Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Rizika používání sociálních sítí - analýza a návrh zabezpečení

Diplomová práce

Autor: Vojtěch Krčil
Studijní obor: Informační management, im2

Vedoucí práce: Ing. Karel Mls, Ph.D.

Hradec Králové duben 2016

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 30. dubna 2016 ……

Bc. Vojtěch Krčil

Poděkování

Rád bych tímto poděkoval Ing. Karlu Mlsovi, Ph.D. a Mgr. Jiřímu Havigerovi, Ph.D. za cenné rady při tvorbě této diplomové práce.

Anotace

Diplomová práce se zabývá především analýzou bezpečnostních rizik na sociálních sítích u studentů základních škol, středoškolských gymnázií a středních škol se zaměřením na IT v Královéhradeckém kraji. Pro lepší pochopení praktické části diplomové práce jsou v teoretické části vysvětleny základní pojmy a hlavní sociální sítě. V praktické části byly vytvořeny na základě poznatků z teoretické části hypotézy, které slouží k identifikaci nejčastějších rizik a rizikových skupin na sociálních sítích. Všechny výsledky zkoumaných hypotéz slouží pro vytvoření návrhu na zlepšení bezpečnostní situace u žáků zmíněných škol.

Annotation

Title: Risks in the use of social networks – analysis and proposal for security improvement

Diploma Thesis primarily focuses on analysis of security risks on social networks for students of upper primary schools, secondary grammar schools and secondary schools with a focus on IT in Kralovehradecky region. For a better understanding of the practical part of thesis, theoretical part of thesis explains the basic concepts and main social networks. In the practical part of thesis there have been created hypotheses based on knowledge gained from the theoretical part, which are used to identify the most common risks and risk groups on social networks. All the results of the examined hypotheses are used to create a list of principles to improve the security situation.

Obsah

Úvod

V současné době jsou sociální sítě nejpoužívanější internetovou službou. Uživatelé po celém světě jsou ke svým oblíbeným sociálním sítím připojeni téměř nepřetržitě. Sociální sítě představují velice užitečný a univerzální nástroj, díky kterému má uživatel možnost komunikace a sdílení různých aktivit s určitou, jím zvolenou skupinou lidí. Mezi hlavní přínosy sociálních sítí patří především zábava, komunikace, vzdělání, ale také marketing a propagace firmy či fyzické osoby.

Existuje obrovské množství sociálních sítí, proto budou rozebrány ty sociální sítě, které jsou v rámci zkoumaných skupin lidí nepoužívanější. K zjištění nejpoužívanějších sociálních sítí byl použit pilotní výzkum, z kterého vyplynulo, že nejpoužívanějšími sociálními sítěmi jsou Facebook, Youtube, Instagram a několik dalších sociálních sítí, které budou podrobněji představeny v dalších částech diplomové práce.

Sociální sítě jsou mocným a užitečným nástrojem, nicméně na nich existuje obrovské množství hrozeb, které jsou popsány u nejpoužívanějších sociálních sítí. Uživatelé se často setkávají s internetovou šikanou (kyberšikanou), zneužitím osobních údajů a dalšími negativními jevy, před kterými je třeba se chránit. Aby se předešlo těmto hrozbám a negativním jevům, je podrobně rozebráno i zabezpečení a ochrana soukromí uživatelů.

Předmětem výzkumu v praktické části diplomové práce je zabezpečení tří nejpoužívanějších sociálních sítí a setkání uživatelů s negativními jevy na různých sociálních sítích. Cílem výzkumu je zjistit nedostatky v zabezpečení uživatelských účtů na nejpoužívanějších sociálních sítích a dopady těchto nedostatků na samotné uživatele. Výsledky výzkumu pomohou k identifikaci rizikových skupin a nejčastějších rizik na sociálních sítích.

Dále je v praktické části diplomové práce navrhnuto řešení, které má za úkol zvýšit povědomí uživatelů v raném věku o zabezpečení a hrozbách sociálních sítí, protože právě těmto dvěma tématům je v dnešní době vhodné věnovat velkou pozornost. Zvýšením povědomí uživatelů a určením pravidel, jakými se řídit při používání sociálních sítí by se měl snížit výskyt negativních zkušeností uživatelů se sociálními sítěmi, jako je například kyberšikana, kyberstalking, zneužití osobních údajů a další.

Pro lepší pochopení výsledků v praktické části jsou v teoretické části představeny základní pojmy, nejpoužívanější sociální sítě, jejich zabezpečení a využití.

1. Co jsou sociální sítě

1.1. Sociální síť

Sociální síť je internetová služba, která slouží uživatelům k vytvoření osobního, či firemního profilu. Takovýto profil je podle nastavení uživatele a použité sociální sítě veřejný, nebo z části veřejný a umožňuje svému vlastníkovi, nebo správci, navazovat virtuální vztahy s ostatními uživateli. Sociální síť pak umožňuje propojeným uživatelům vzájemnou komunikaci, sdílení informací, fotografií, videí, odkazů, událostí a mnoho dalších aktivit. Existuje velké množství sociálních sítí, které se liší především v zaměření na určité funkční požadavky uživatelů. [1]

Pro firmy jsou sociální sítě velmi účinným a používaným marketingovým nástrojem pro propagaci firmy a nabízených produktů. Sociální sítě jsou součástí každodenního života a v několika případech byly také použity jako důkaz při soudním sporu, kde byla použita jako důkaz fotografie, nebo komunikace mezi uživateli. [2]

Sociální sítě jsou často označovány jako nová generace internetových služeb, tzv. web 2.0. Principem této nové generace World Wide Webu (www) je vytváření obsahu uživateli. Mezi hlavní představitele webu 2.0 patří právě sociální sítě jako Facebook, YouTube a Twitter spolu s blogy a wiki. [3]

1.2. Využití sociálních sítí - uživatel

Sociální sítě se v posledních letech staly každodenní součástí životů jejich uživatelů. Jak již bylo řečeno, existuje spousta sociálních sítí s různými možnostmi využití.

1.2.1. Facebook

Pravděpodobně nejuniverzálnější sociální sítí je Facebook. Jedná se o celosvětově nejpoužívanější sociální síť, která nabízí po registraci uživatelům velké množství funkcí. Mezi hlavní funkce patří vytvoření osobního profilu, sdílení informací, vytváření událostí, aplikace, hraní her a především komunikace s lidmi nejen textovými, ale i hlasovými zprávami a videohovory. [4]

1.2.2. Google+

Velkou výhodou Google+ je propojení jednotlivých služeb poskytovaných společností Google, nicméně se tato sociální síť netěší takové oblíbenosti jako funkčně podobný Facebook. Google+ poskytuje především vytvoření osobního profilu, sdílení informací a sledování určitých komunit či lidí. Nicméně díky již zmíněné propojenosti všech služeb Google je velice snadné z rozhraní Google+ přejít na email, mapy, obchod s aplikacemi, osobní Google disk, Hangouts (zpráva, hovor a videohovor s přáteli) a další užitečné služby. Přechod je také možný na další sociální síť společnosti Google, kterou je oblíbený YouTube. [5]

1.2.3. YouTube

Další sociální sítí společnosti Google je YouTube. Jedná se o oblíbenou sociální síť, ve které má uživatel, kromě jiného, možnost sledovat a sdílet videa. Uživatel s vytvořeným profilem (kanálem) má možnost vytvoření seznamu videí, svá nahraná videa, oblíbená videa a odběry ostatních kanálů. Úvodní stránka pak uživateli nabízí videa podle toho, jaká v minulosti navštívil, nebo jaká odebírá. Nepřihlášený uživatel může videa pouze sledovat. YouTube je velice oblíbená sociální síť což dokazuje fakt, že má přes miliardu uživatelů. [6]

1.2.4. Twitter

Twitter je na oficiálních stránkách popsán jako „okno do světa“. Je popsán právě takto, protože umožňuje vidět uživatelům novinky, které jejich sledovaní přátelé, oblíbené osobnosti, nebo firmy zveřejní („tweetnou“) na svém profilu. Uživatel má dále možnost psát své vlastní „tweety“, kterými se dělí o novinky ze svého života s lidmi, kteří ho sledují. [7]

1.2.5. LinkedIn

Cílem této sociální sítě je propojení profesionálů z celého světa. Uživateli nabízí vytvoření profilu ve formě životopisu s pracovními a studijními úspěchy. Propojením pak uživatel získá obrovskou síť lidí, nové pracovní příležitosti a informace, které mu mají pomoci k osobnímu růstu v jeho profesní oblasti. [8]

1.2.6. Ask.fm

Poslední blíže představenou sociální sítí je Ask.fm. Ask.fm je specifická svým Q&A (otázka a odpověď) formátem. Jedná se o jednoduchý princip, kde uživatel může položit jinému uživateli otázku a naopak na položené otázky odpovědět. Uživatelům slouží především pro položení otázek, na které nemají odvahu se zeptat osobně. [9]

1.2.7. Další sociální sítě

Kromě výše zmíněných je dobré zmínit ještě některé sociální sítě, které jsou zajímavé svojí funkcionalitou a oblíbeností. Velmi oblíbenou sociální sítí je Instagram, který slouží uživatelům pro sdílení fotografií a videí. Jedná se především o mobilní aplikaci, webová verze nenabízí některé funkce. [10]

Mezi seznamovací sociální sítě patří Badoo, Tinder a české líbimseti. Mezi další specifické sociální sítě patří také Foursquare. Ten slouží pro sdělení aktuálního místa, kde tráví uživatel čas, a doporučení zajímavých míst. Obsahuje herní prvky, díky kterým je vidět oblíbenost jednotlivých míst. [11]

1.3. Využití sociálních sítí – firmy a instituce

Sociální sítě nejsou zajímavé pouze pro běžné uživatele. Čím dál větší pozornost jim věnují firmy i instituce, které využívají velké uživatelské základny k propagaci vlastní věci a dalším aktivitám popsaným v této podkapitole.

1.3.1. Firmy

Jelikož sociální sítě každodenně navštěvují milióny lidí, mají obrovský potenciál pro firmy z hlediska marketingu. Do marketingu na sociálních sítích investují nemalé částky a propagují tak své služby a produkty. Pro propagaci používají většinou více než jednu sociální síť. Běžně se jedná o Facebook, YouTube, Instagram a Twitter. Díky sociálním sítím firmy nezískávají pouze nové zákazníky, ale i nové pracovníky. Pro získání nových pracovníků firmy často využívají sociální síť LinkedIn, která umožňuje HR (human resources) specialistům vidět životopis uchazeče přímo na jeho profilu. [12]

Další užitečné využití sociálních sítí pro firmy je uživatelská podpora. Z výzkumu společnosti Microsoft vyplynulo, že sociální sítě jsou druhou nejdůležitější technologií, která manažerům pomáhá k úspěchu na trhu. Používání sociálních sítí firmou zlepšuje kvalitu služeb a spokojenost zákazníků. To podporuje i fakt, že sociální sítě používá 24% českých firem, kde největší podíl mají firmy nad 250 zaměstnanců (40%). Nejrozšířenějšími sociálními sítěmi u firem je podle ČSÚ (Český statistický úřad) Facebook a LinkedIn. Facebook především kvůli největší koncentraci uživatelů a možnosti vytvoření firemního profilu. Facebook dále umožňuje firmám placenou reklamu na jejich stránkách s garancí určitého dosahu uživatelů. LinkedIn je oblíbený kvůli možnosti náboru nových zaměstnanců. [12, 13]

Přestože je podíl českých firem na sociálních sítích téměř čtvrtina, oproti vyspělým zemím české firmy zaostávají. Za rok 2014 české firmy po Rumunsku, Polsku a Lotyšku využívaly sociální sítě nejméně. Nicméně nárůst oproti roku 2013 byl 6,8%, což značí, že českým firmám dochází důležitost sociálních sítí v podniku. [12]

1.3.2. Instituce

Pro instituce platí podobné využití jako pro firmy, nicméně oproti firmám se zaměřují spíše na komunikaci a informování uživatelů. Vzdělávací instituce mohou využívat sociální sítě jako e-learningové kurzy. Příkladem e-learningové sociální sítě je Duolingo, kde má uživatel možnost se naučit cizí jazyk formou hry. [14]

1.4. Nebezpečí sociálních sítí

Jak je vidět v předchozích kapitolách, sociální sítě jsou velice užitečným nástrojem jak z pohledu uživatele, tak z pohledu firmy. Nicméně existuje i stinná stránka sociálních sítí, a tou je závislost, zneužití osobních údajů a další nepříjemnosti, kterým uživatel musí čelit. Konkrétní negativní jevy, se kterými se uživatel může setkat, jsou popsány u jednotlivých sociálních sítí. [15]

1.5. Shrnutí

V této úvodní kapitole byl představen pojem sociální síť a její využití jak z pohledu běžného uživatele, tak z pohledu firmy nebo instituce. Díky těmto základním znalostem bude lépe porozuměno další kapitole, ve které budou představeni hlavní zástupci světových sociálních sítí.

2. Sociální sítě

Po představení pojmu sociální síť a nastínění využití sociálních sítí budou představeny nejvýznamnější zástupci. Jako první bude představena sociální síť Facebook, která je světově nejrozšířenější. Dále budou představeny další oblíbené sociální sítě.

2.1. Facebook

Facebook je celosvětovým fenoménem. Jedná se o nejpoužívanější sociální síť, která měla v září roku 2015 v průměru 1,01 miliardy aktivních uživatelů. Úkolem Facebooku je dát lidem možnost sdílet informace a dělat tak svět více propojeným. Lidé používají Facebook aby mohli zůstat v kontaktu s přáteli a rodinou, zjistili co je nového ve světě a sdíleli to, na čem jim záleží. [16]

Informace pro zpracování této podkapitoly byly získány z oficiálních stránek Facebooku [4]a centra nápovědy Facebooku. [17]

2.1.1. Vznik Facebooku

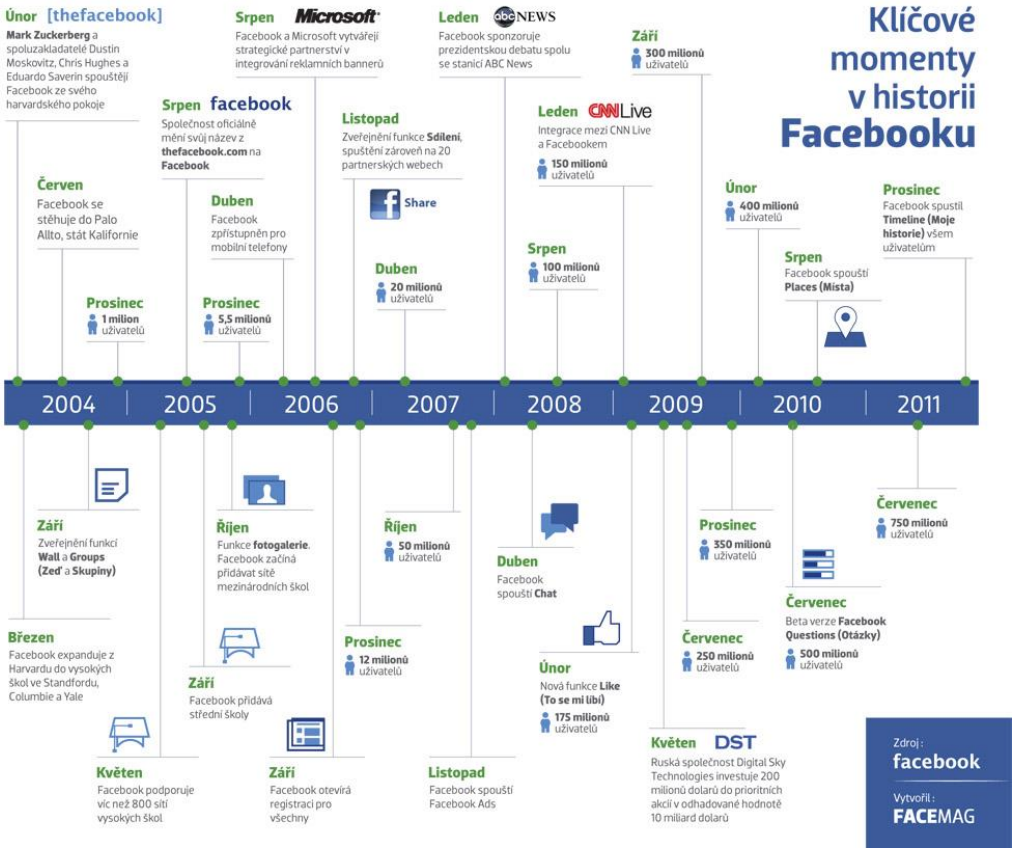
Facebook byl založen studentem Harvadu Markem Zuckerbergem a jeho spolužáky Eduardem Saverinem, Dustinem Moskovitzem a Chrisem Hughesem. Jejich původním projektem byl Facemash, který se v mnohém podobal dnešnímu Tinderu. Jednalo se o výběr přitažlivější studentky/studenta ze dvou možností. Aby tento projekt mohl vůbec začít, byla potřeba databáze studentů Harvardu. Tu Zuckerberg získal tak, že se naboural do sítě Harvardu. Projekt byl spuštěn 28. 10. 2003 a odstaven o několik dní později úředníky Harvardu z důvodu zneužití osobních údajů. Mark Zuckerberg byl obviněn z porušení bezpečnosti, autorských práv a práv jednotlivce za krádeže snímků studentů, použitých na stránkách Facemash. V důsledku těchto obvinění čelil Zuckerberg vyloučení z Harvardské university, nicméně všechna obvinění byla stažena a Zuckerberg dostal pouze podmíněné vyloučení po dobu půl roku. [18]

Nové stránky pod názvem Thefacebook Zuckerberg spustil 4. 2. 2004. Název Thefacebook vznikl podle názvu seznamovacích letáků amerických studentů. 10. 2. 2004 čelil obvinění od tří studentů Harvardu, Camerona Winklevosse, Tylera Winklevosse a Divya Narendra, že jejich nápad ukradl. Jednalo se jim o velkou podobnost projektů HarvardConnection, na kterém s dvojčaty Winklevossovými a Narendrou pracoval, a Thefacebook. Všechny spory však byly vyřešeny mimosoudní cestou a Zuckerberg zaplatil minimálně 65 miliónů dolarů odškodné. TheFacebook byl původně pouze pro studenty Harvardu ale postupem času se Zuckerberg rozhodl zaměstnat několik svých spolužáků a expandovat na další univerzity a vysoké školy. V roce 2004 vstoupil do společnosti investor Sean Parker, který navrhl odkoupení domény facebook.com za 200 000 dolarů. Společnost tak dostala nové jméno Facebook. [18]

Celý příběh Marka Zuckerberga a vzniku Facebooku byl zachycen ve snímku "The Social Network" režiséra Davida Finchera. Od tohoto filmu se však firma Facebook i samotný Mark Zuckerberg distancovali. [19]

2.1.2. Vývoj Facebooku

4. 2. 2014 Facebook oslavil už desáté výročí od vzniku. Facebook prošel mnoha změnami a dosáhl na několik historických milníků. Hlavní momenty v historii Facebooku od založení do roku 2012 jsou zobrazeny na obrázku číslo 1. Pomineme-li založení Facebooku, je zde vidět mnoho funkčních novinek jako například zavedení funkce zeď, skupiny, like (to se mi líbí), sdílení a místa. Mezi hlavní milníky období do roku 2012 však patří otevření registrací pro všechny uživatele v září roku 2006, spuštění chatu v dubnu roku 2008 a spuštění nové verze profilu, tzv. Timeline, všem uživatelům v prosinci roku 2011. [20]



Obrázek 1: Klíčové momenty v historii Facebooku [20]

Rok 2012 byl pro Facebook důležitý, protože se mu podařilo získat sociální síť Instagram, kterou odkoupil v dubnu za 1 miliardu dolarů. V květnu téhož roku Facebook vstoupil na burzu. Posledním velkým milníkem roku 2012 bylo říjnové dosažení miliardy aktivních uživatelů. [21, 22]

V červenci roku 2013 používalo mobilní verzi Facebooku více než 100 milionů lidí a v srpnu Facebook spustil internet.org, který má za úkol zajistit přístup k internetu na celém světě. [21, 23]

Na přelomu ledna a února roku 2014 Facebook spustil iOS aplikaci Facebook Paper, což byla aplikace, která sloužila jako noviny, nebo magazín pro zařízení od firmy Apple. 4. 2. 2014 Facebook oslavil desáté výročí od založení a při té příležitosti nabídl uživatelům tzv. Lookback, což umožnilo uživateli prohlédnout si video automaticky vytvořené z příspěvků, které vložil za posledních 10 let. V únoru 2014 přišla ještě jedna důležitá událost pro Facebook, tou bylo odkoupení mobilní aplikace WhatsApp za 16 miliard dolarů. V březnu 2014 Facebook odkoupil další společnost, tentokrát Oculus VR, Inc., což je vedoucí společnost v oblasti virtuální reality. Mezi hlavní funkce, které byly spuštěny v roce 2014, patří Safety Check a Rooms. [16]

V dubnu roku 2015 bylo v Messengeru umožněno uživatelům provádět videohovory. V červnu Facebook spustil tzv. Moments, což zachycuje momenty sdílené uživatelem na Facebooku s určitým přítelem. V srpnu 2015 bylo spuštěno live video pro veřejné příspěvky a koncem tohoto měsíce dosáhl Facebook dalšího velkého milníku, když oznámil, že v jeden den použila Facebook více než jedna miliarda lidí. [16]

2.1.3. Software Facebooku

Jelikož Facebook operuje s velkým množstvím dat, některé tradiční přístupy a technologie nejsou praktické. Úkolem vývojářů Facebooku je zajistit hladký běh služby pro více než miliardu aktivních uživatelů. [24]

LAMP

Základním stavebním kamenem je LAMP software, což je open-source software skládající se v případě Facebooku z operačního systému Linux, webového serveru Apache, databázového systému MySQL a skriptovacího programovacího jazyku PHP. Nicméně vývojáři Facebooku tyto jednotlivé části neustále vylepšují a rozšiřují o nové služby, díky kterým je aplikace mnohem výkonnější. Pro zrychlení běhu aplikace používá Facebook také Memcached a další služby a systémy. [24]

Memcached

Memcached je hojně používaným softwarovým řešením pro větší weby na internetu. Díky Memcached má Facebook rychlejší přístup k informacím. Důvodem je vytvoření cache vrstvy mezi webovými servery a MySQL servery. Vytvořením této vrstvy se zrychlí přístup k databázi, který je obvykle pomalý. Stejně jako tomu bylo u balíčku LAMP, i u Memcached Facebook udělal nespočet optimalizací pro zlepšení výkonu. [24]

HipHop pro PHP

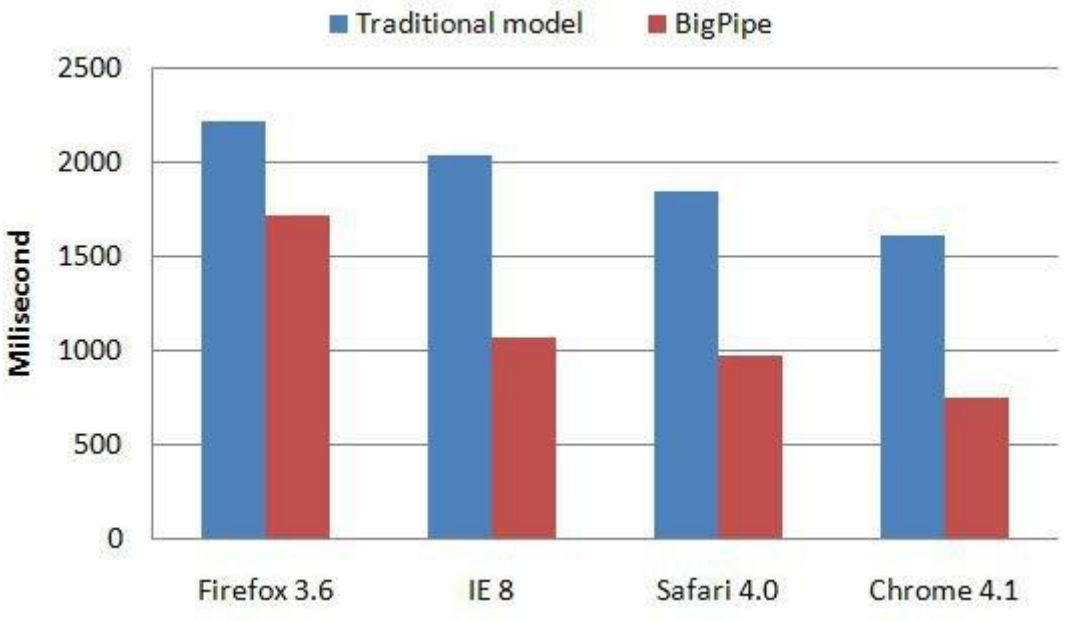
Hlavním cílem Facebooku je být rychlý a výkonný. K tomu slouží právě i HipHop, díky kterému se podařilo redukovat využití CPU na webových serverech Facebooku přibližně o 50%. HipHop funguje jako překladač kódu z PHP do vysoce optimalizovaného C++ kódu. [25]

Haystack

Haystack slouží jako sklad jakýchkoliv objektů, nicméně Facebook jej používá především jako výkonné uložiště fotografií, kterých je na Facebooku obrovské množství. Každá fotografie je uložena ve čtyřech různých rozlišeních. [24]

BigPipe

BigPipe je systém, který generuje webové stránky po takzvaných pagelets, což jsou jednotlivé části webové stránky. U úvodní stránky Facebooku to jsou části jako například chat, události, novinky s příspěvky a aplikace. Výhodou je menší chybovost, kdy při chybě například načtení chatu se zbytek pagelets načte v pořádku. Jednotlivé pagelets mohou být načteny zároveň v různých stádiích načtení. Za pomoci tohoto systému se stránky v jakémkoliv prohlížeči načtou rychleji. Výsledky srovnání mezi použitím BigPipe a tradičním modelem načtení jsou zobrazeny na grafu číslo 1. [24, 26]



Graf 1: Rychlost načtení stránek [26]

Cassandra

Apache Cassandra je distribuovaný systém pro práci s velkým množstvím dat, který je bezchybný. Jedná se o úložný systém z rodiny NoSQL, který Facebook využívá při hledání v doručených zprávách. Kromě Facebooku Cassandru používá i například Digg. [24]

Scribe

Scribe je logovací systém, který slouží Facebooku interně k mnoha účelům. Byl vytvořen pro rychlé zpracování přihlášení do Facebooku a pro automatické řízení nových přihlášení podle potřeby. Nových přihlášení tak mohou být stovky. [24]

Hadoop a Hive

Hadoop je implementace, která umožňuje provádět kalkulace na obrovském množství dat. Hive pochází přímo od Facebooku a lze pomocí něj zasílat SQL dotazy na Hadoop. Tím usnadňuje práci s Hadoop lidem bez větších programátorských zkušeností. [24]

Varnish

Varnish funguje jako http akcelerátor, který může fungovat jako load balancer, nebo cache obsahu, který je doručen uživateli velmi rychle. Facebook používá Varnish pro fotky a profilové obrázky a jako většina softwaru co Facebook používá je open source. [24]

Thrift

Facebook používá velké množství programovacích jazyků, jako například PHP, Java, C++ nebo Erlang pro chat. Thrift byl vyvinut jako rámec pro komunikaci mezi těmito jednotlivými jazyky. [24]

Gatekeeper

Facebook má dále systém Gatekeeper, který mu umožňuje spustit různý kód pro různé skupiny uživatelů. Toto umožňuje Facebooku lepší testování nových vlastností systému a například aktivaci nových funkcí, či služeb pouze pro zaměstnance Facebooku. Gatekeeper umožňuje také tzv. „dark launches“, což je spuštění určitého elementu, nebo funkce na pozadí tak, že si toho uživatel nevšimne. Toto slouží pro testování funkcí před oficiálním spuštěním. [24]

2.1.4. Funkcionalita Facebooku

Funkce Facebooku jsou dostupné pouze pro řádně registrovaného a přihlášeného uživatele. Pro ostatní uživatele bez zájmu vytvořit osobní profil nabízí možnost vytvoření stránky pro celebritu, skupinu nebo společnost. Tato funkce je však dostupná i z uživatelského profilu, proto bude charakterizována v jednom z následujících bodů.

Profil

Registrací se uživateli automaticky vytvoří uživatelský profil, kde má uživatel možnost vyplnění základních osobních údajů, nahrání profilové a úvodní fotografie, a přidání příspěvků na svojí Timeline.

Úvodní fotografie je vidět pouze na profilu daného uživatele, zatímco profilový obrázek slouží i jako prezentace uživatele, protože je zobrazen u každé aktivity uživatele a ve vyhledávání pod jeho jménem. Rozměry profilového obrázku jsou 160 x 160 pixelů a úvodního obrázku 828 x 315 pixelů.

Timeline je součástí profilu a jedná se o časově seřazené příspěvky přidané uživatelem, nebo uživateli, kteří daného uživatele v příspěvku označili. Příspěvky jsou řazeny od nejnovějších po nejstarší. Příspěvkem se rozumí jakékoliv video, fotka, textový stav nebo životní událost. Při vytváření jednotlivých příspěvků má uživatel možnost nastavení soukromí pro zobrazení daného příspěvku. Třemi základními volbami soukromí příspěvků je Veřejný (příspěvek může vidět kdokoliv), Přátelé (příspěvek vidí pouze přátelé uživatele) a Jenom já (příspěvek vidí pouze uživatel, který ho přidal). Další možností u příspěvků je přidání určitých pocitů či aktivit, se kterými se uživatel chce podělit s přáteli. Zatímco u životní události může uživatel vytvořit a sdílet cokoliv, u pocitů a aktivit tomu tak není. Uživatel má možnost velkého výběru aktivit, nemá však možnost přidání své vlastní. Nicméně pokud by se uživatel chtěl například podělit o to, že se kouká na film Forrest Gump, stačí mu napsat první slovo a vyhledávač mu již nabídne odkaz na film, který může sdílet. Odkazem na jednotlivé aktivity jsou pak existující ověřené stránky na Facebooku.

Po zveřejnění příspěvku má uživatel možnost základních operací s jednotlivými příspěvky jako je úprava, smazání, změna data, přidání polohy, označení přátel a skrytí na Timeline. Dále má uživatel možnost u příspěvků přidávat komentáře ve formě textu, samolepky, nebo fotografie. Posledními funkcemi je označení příspěvku „To se mi líbí“ a sdílení daného příspěvku.

Kromě Timeline, které je nastavené jako výchozí zobrazení na profilu, má uživatel možnost přepínat mezi dalšími kartami, které poskytují uživateli určité funkce nebo informace. Hlavními kartami jsou Informace, kde uživatel vidí své zaměstnání, rodinný stav, studia, bydliště a další informace. Dále Přátelé, se kterými je uživatel ve spojení a Fotky. Mezi další oddíly na uživatelském účtu patří videa, oznámení polohy, skupiny, poznámky, recenze a oblíbené filmy, sporty, hudba, TV pořady, knihy a další stránky.

Poslední možností profilu je nastavení určitých oprávnění pro obsah Timeline. Zabezpečení Timeline a celého uživatelského profilu na Facebooku bude rozebráno v kapitole o zabezpečení osobního profilu.

Novinky

Novinky jsou zobrazeny uživateli na hlavní stránce v prostřední části. Na začátku stránky má uživatel možnost přidání nového příspěvku, stejně jako tomu bylo u Timeline. Tyto dvě funkce jsou propojeny, pokud uživatel přidá cokoliv na hlavní stránku, příspěvek se zobrazí i na jeho Timeline a naopak. Funkce Novinky však zobrazuje i ty příspěvky, které přidávají lidé, stránky, nebo skupiny, které uživatel sleduje, nebo je jejich členem. Jakmile se uživatel spřátelí s určitým uživatelem, automaticky ho sleduje, to však lze změnit na profilu daného uživatele, nebo u příspěvku, který přidal. Uživatel má možnost zrušení sledování nejen uživatele, ale i stránky, ze které pro něj nezajímavé či obtěžující příspěvky pocházejí. Jako u všech příspěvků má pak uživatel možnost komentovat, „lajkovat" a sdílet. Specifická je možnost nahlásit a uložit příspěvek, nebo zapnout upozornění pro příspěvek. Zapnutím upozornění bude uživatel vědět o jakékoliv aktivitě (to se mi líbí, komentář, sdílení), která se v rámci příspěvku děje.

Přátelé

Přátelé jsou nejen pro Facebook důležití. Jedná se o skupinu lidí, se kterými je uživatel propojen, a sdílí s nimi informace a jiný obsah. Facebook nabízí vyhledání přátel pomocí emailové adresy, prohledá kontakty z emailu uživatele a pokud se některý z kontaktů shoduje s emailem uživatele Facebooku, navrhne ho jako přítele. Pro vyhledání přátel je možné použít i vyhledávání na hlavní stránce, nebo návrhy Facebooku, které jsou zobrazeny podle počtu společných přátel, lokace a dalších faktorů. Pokud si uživatel nepřeje být nikým neznámým přidán jako přítel, má možnost nastavit, že mu žádost o přátelství mohou poslat pouze přátelé jeho přátel. Uživatel však musí potvrdit žádost o přátelství, do té doby nejsou uživatelé propojeni, pouze ho daný uživatel může sledovat, což lze také zakázat tím, že v nastavení uživatel zvolí, že ho mohou sledovat pouze přátelé.

Jakmile uživatel schválí přátelství, je možné s novým přítelem komunikovat prostřednictvím chatu a vidět všechny příspěvky, které měl přístupné pouze pro přátele v závislosti na nastavení profilu.

Přátelé jsou automaticky rozřazeni podle určitých faktorů. Kromě možnosti vidět všechny přátele může uživatel zobrazit pouze nedávno přidané přátele, přátele, kteří mají narozeniny v blízké době, přátele z vysoké nebo střední školy, z místa pobytu nebo z rodného města. Kromě těchto automaticky vytvořených skupin má uživatel možnost přátele dělit i do dalších skupin, které může sám vytvářet a spravovat. V těchto skupinách má pak možnost nastavit různá oprávnění. Jedním z předem vytvořených seznamů je seznam Blízcí přátelé. Uživatel pak dostává upozornění o aktivitách těchto členů skupiny.

Pro odebrání přátel má uživatel dvě možnosti. První možností je nalezení profilu uživatele, kterého chce z přátel odstranit, ve vyhledávači na hlavní stránce. Druhou možností je vyhledat uživatele na svém profilu v seznamu přátel.

Fotky

Další z hlavních funkcí Facebooku jsou Fotky. Díky této funkci má uživatel možnost nahrávat a sdílet fotografie, nebo celá alba na svůj osobní profil. Do jednoho alba lze nahrát až 1000 fotografií. Facebook nabízí i možnost nahrání fotek ve vysokém rozlišení. Pokud uživatel chce své fotografie uložit na svůj profil ve vysokém rozlišení, stačí mu zaškrtnout pole Vysoké rozlišení při nahrávání fotografií. Kromě přehlednosti je dobré fotografie třídit do alb i z důvodů bezpečnosti. Je totiž možné, aby různá alba měla různá oprávnění. Tak může uživatel například nastavit, aby rodinné fotografie z dovolené viděli pouze členové rodiny. Fotografie uživatel, stejně jako příspěvky, může nahrát i na profil uživatele, kterého má v přátelích.

S nahranou fotografií má uživatel možnost různých operací. Kromě tradičního označení To se mi líbí, komentáře a sdílení má možnost základních úprav fotografie jako je otočení doleva, otočení doprava a hlavně označení osob na fotografii. Tato funkce umožňuje uživateli označit uživatele, se kterými na fotografii je, nebo se kterými chce fotografii sdílet. Označená fotografie se pak zobrazí všem označeným osobám na jejich Timeline. Limit označených osob nebo stránek na jedné fotografii je 50.

Facebook používá software na rozpoznání obličejů, které jsou na fotografii. Tento software porovnává rysy obličeje určité osoby a vypočítá tak jedinečné číslo, podle kterého pak navrhuje uživatele k označení. Mezi tyto rysy patří vzdálenost mezi očima, ušima a nosem. Díky tomuto softwaru se tak uživateli dostane pomoci při označování, jelikož mu bude nabídnuta osoba pro označení na daném obličeji. Tato funkce lze vypnout v nastavení Timeline a označování.

Videa

Podobnou funkcí jako Fotky jsou Videa. Po nahrání videí je automaticky vytvořeno album Videa, ve kterém jsou všechna videa, která uživatel nahrál. Možné je však i přidat videa do jednotlivých, již vytvořených alb. Facebook podporuje velké množství video formátů jako například nejrozšířenější 3gp, avi, divx, mkv, mov, mp4, mpeg a mnoho dalších. Doporučenými formáty jsou mp4 a mov. Facebook poskytuje možnost nahrání videí v HD kvalitě. Omezením je maximální délka 45 minut a velikost 1,75 GB.

Facebook také nabízí živé vysílání, což jsou videopříspěvky od ověřených stránek, uživatelů nebo známých osobností, které má uživatel v přátelích, nebo je sleduje. Po celou dobu uživatel vidí živé komentáře a počet sledujících. Všechny komentáře a celé video po skončení vysílání zůstane na Timeline uživatele, který jej vytvořil. Živá vysílání mají maximální délku 30 minut a je důležité, aby uživatel měl dostatečný signál, proto se doporučuje vysílat pouze tehdy, pokud je uživatel připojen na Wi-Fi nebo alespoň 4G mobilní připojení. [27]

Chat

Facebook je především sociální síť pro propojení lidí. Pro komunikaci mezi propojenými lidmi slouží chat. Chat funguje jako instant messaging funkce, která umožňuje uživatelům komunikovat v reálném čase. Při komunikaci mají uživatelé k dispozici přívětivé uživatelské rozhraní, které jim umožňuje lehce využívat další funkce spojené s konverzací. Mezi tyto funkce patří zaslání fotografie, souboru nebo samolepky. Samolepky jsou vytvořené animace a obrázky, které může uživatel přidat do svého chatu a používat je při konverzaci. Tyto samolepky je možné získat z obchodu se samolepkami na Facebooku, kde jsou všechny zdarma.

Chat nabízí nejen přenos textových zpráv, ale i hlasový hovor a videohovor. Další možností je přidání dalších uživatelů do chatu a vytvoření tak skupinové konverzace, ve které probíhá konverzace v reálném čase mezi všemi účastníky chatu. Posledními funkcemi je možnost vypnutí chatu a blokace zpráv od daného uživatele. U každé zprávy je vidět, zda si jí příjemce přečetl nebo ne.

Tyto možnosti má uživatel i v globálním nastavení chatu, kde má možnost určit skupiny lidí, pro které bude chat zapnut nebo naopak vypnut. Další možností globálního nastavení je vypnutí celého chatu, skrytí postranního panelu s chatem, vypnutí videohovorů a volání, vypnutí zvuků chatu a skrytí nabízených her v horní části panelu chatu. Chat je spojen s funkcí Zprávy, která nabízí další možné operace s konverzacemi.

Zprávy

Zprávy jsou úzce spjaté s chatem a dávají uživateli možnost několika nových operací s konverzacemi. Kromě klasického zasílání a přijímání textových zpráv, multimediálních zpráv a souborů, má uživatel možnost zobrazení všech fotografií a textů v celé konverzaci s daným uživatelem. Ve zprávách má uživatel dále možnost vymazání jednotlivých zpráv i celé konverzace. Všechny zprávy jsou rozděleny do několika kategorií, z nichž hlavními jsou Nejnovější, Žádosti zpráv a Archivováno. Výchozí kategorií jsou nejnovější zprávy, které uživatel obdržel nebo odeslal. V kategorii Žádosti zpráv jsou zprávy od uživatelů, se kterými uživatel není nijak propojen. V archivovaných zprávách jsou ty zprávy, které uživatel sám zvolil archivovat. Pro ovládání zpráv a chatu slouží klávesové zkratky a mezi hlavní patří ALT+G pro hledání konverzací a ALT+M pro novou zprávu.

Události

Pomocí funkce Události může uživatel organizovat události, reagovat na pozvánky na události a sledovat, na jaké události se chystají přátelé. Události, na které se uživatel přihlásil, jsou seřazeny podle data a uživatel má tak přehled o tom, jaké události jsou nadcházející. Pro ještě větší přehled funkce Události nabízí kalendář, ve kterém jsou události uživatele uloženy. Kromě událostí, na které se přihlásil, jsou v kalendáři uloženy narozeniny všech přátel, kteří mají na svém profilu vyplněný datum narození. Upozornění na nadcházející události a narozeniny z aktuálního dne uživatel dostává v pravém sloupci na hlavní stránce. Kromě nadcházejících událostí si uživatel může prohlédnout i události, které již uplynuly.

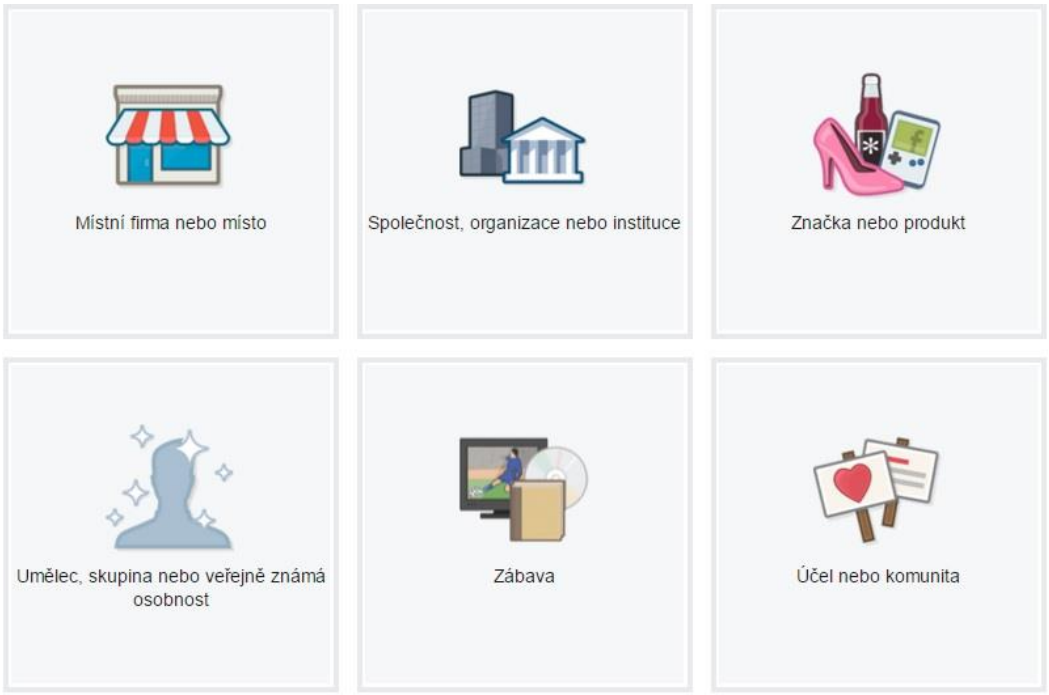
Na samotné stránce vytvořené události má každý uživatel možnost zvolit, zda se zúčastní akce, nebo má o akci pouze zájem. V těchto dvou případech budou uživateli chodit upozornění o nové aktivitě v rámci události. Pokud uživatel zvolí, že nemá zájem o událost, žádné upozornění mu již nebude chodit a to ani, když je pozvaný. Když je uživatel nerozhodný, zda se nějaké události zúčastnit, může mu pomoci pravý panel, kde lze vidět profilové obrázky přátel, kteří se zúčastní. Dále je zde vidět celkový seznam všech účastníků události. Pod panelem se zúčastněnými má uživatel možnost pozvat své přátelé.

Každý uživatel má možnost vytvořit si svou vlastní událost. Existují dva hlavní typy událostí. První je událost veřejná, kterou vidí všichni a druhou je událost soukromá, kterou vidí pouze ti uživatelé, kteří obdrželi pozvánku. Při vytváření pak uživatel zvolí název a fotku události, místo konání, čas konání a popis. Tyto údaje vidí pak každý uživatel, který má přístup do události. Dále má uživatel možnost zvolit, jestli pozvaní přátelé mohou zvát další hosty. Tato možnost je pouze při vytváření soukromé události, protože na veřejnou událost přístup není omezen. Maximální počet osob, které může jeden uživatel pozvat je 500.

Stránky

Stránky slouží pro propagaci firmy, značky, osobnosti nebo organizace. Díky stránkám mohou komunikovat se svými fanoušky, kteří označili danou stránku tlačítkem „To se mi líbí“. Stejně jako tomu je u profilu, i na stránky může uživatel (správci) vkládat příspěvky, vytvářet události, přidávat aplikace a vše je zobrazeno na Timeline dané stránky. Uživatelé, kteří jsou fanoušky této stránky, vidí její příspěvky na své hlavní stránce v novinkách. Seznam svých oblíbených stránek uživatel vidí na levé straně své hlavní stránky.

Vytvořit stránku může kdokoliv, nicméně pro stránku, která bude reprezentovat firmu, společnost, organizaci nebo osobnost, musí být oficiálním zástupcem. Při vytvoření stránky má uživatel na výběr z možností na obrázku číslo 2.



Obrázek 2: Volba typu stránky [4]

Kromě účelu a komunity je vždy třeba vybrat ze seznamu kategorií, do kterých daná skupina spadá. Například u možnosti Společnost, organizace nebo instituce to jsou kategorie Cestování/volný čas, Jídlo/nápoje, Malá firma, Politická strana, Vzdělání a mnoho dalších. Po výběru kategorie a zadání názvu je správce stránky vyzván, aby vyplnil informace o stránce, odkaz na web, adresu na Facebooku, profilový obrázek a přidal stránku mezi své oblíbené, aby se mu zobrazovala v levém sloupci na hlavní stránce a měl ke stránce snadný přístup. Poslední možností při vytváření stránky je identifikace preferovaného okruhu uživatelů stránky. Správce má možnost nastavit lokaci, věk, pohlaví a zájmy lidí, se kterými se chce spojit.

Jakmile je stránka vytvořena, správce má možnost přejít na nastavení, kde má širokou škálu různých nastavitelných prvků stránky. V obecném nastavení má správce možnost nastavit viditelnost stránky, kdo může na stránce zveřejňovat příspěvky, možnost kontaktovat stránky přes zprávy, věkové a územní omezení pro uživatele, filtr vulgárních výrazů, pořadí komentářů a další užitečná nastavení, mezi kterými nechybí ani stažení, sloučení a smazání stránky.

Dalším zajímavým nastavením je nastavení rolí u stránky. Správce může dát některému z uživatelů jednu z pěti rolí s různými oprávněními. Správce může provádět veškeré operace, které stránka poskytuje. Editor má možnost upravovat stránku, posílat zprávy, vytvářet reklamy a může zobrazit přehledy. Moderátor stránky může reagovat na komentáře na stránce a odstranit je, odesílat zprávy jménem stránky a prohlížet přehledy. Inzerent může vytvářet reklamy a prohlížet přehledy. Analytik může pouze prohlížet přehledy. Pro všechny role platí, že vidí, kdo přidal příspěvek nebo komentář.

Facebook poskytuje také placenou propagaci stránky. Pro propagaci stačí správci zvolit možnost propagovat stránku a vybrat cílový okruh uživatelů, kteří mají být osloveni, rozpočet a trvání propagace. Při výběru cílového okruhu správce určí lokaci, zájmy, věk a pohlaví uživatelů. Rozpočet je maximální denní částka, která je do propagace investována. Čím je částka vyšší, tím více odhadovaných fanoušků přibyde. Odhady jsou určeny z průměrné úspěšnosti reklam, proto mohou být matoucí. Jako poslední správce zvolí trvání propagace a platbu. Kromě celé stránky je možné propagovat i jednotlivé příspěvky.

Skupiny

Skupiny slouží uživatelům jako soukromý prostor, díky kterému mají možnost mezi sebou komunikovat a sdílet informace, dokumenty nebo fotografie. Uživateli jsou jeho oblíbené skupiny zobrazeny v levém sloupci pod stránkami na hlavní stránce, kde má možnost spravovat své skupiny, ale také prohlížet skupiny přátel, místní skupiny a doporučené skupiny. Ve skupině, které je uživatel již členem má možnost vidět diskuzi, která je ve formě příspěvků, členy skupiny, události skupiny, fotky a soubory.

Skupinu může vytvořit kdokoliv a nastavit jí jedno ze tří možných nastavení soukromí. Skupina je pak vytvořena jako veřejná, tajná, nebo uzavřená. Zatímco veřejné skupiny jsou přístupné pro kohokoliv, tajné a uzavřené jsou přístupné pouze pro jejich členy. Hlavním rozdílem mezi tajnou a uzavřenou skupinou je takový, že u tajné skupiny uživatel nevidí informace o skupině, nemůže zažádat o vstup do skupiny a skupina se mu nezobrazuje ve vyhledávání. V případě uzavřené skupiny uživatel vidí základní informace jako název skupiny, popis, uživatelé ve skupině, a může skupinu vyhledat a požádat o členství, které schvaluje správce skupiny. Kromě výběru soukromí skupiny uživatel při vytváření vyplní už pouze název skupiny a jména členů. Vyplnění popisu, tagů, úprava obrázku a další nastavení uživatel nastavuje přímo na stránce vytvořené skupiny, na kterou je ihned po vytvoření přesměrován.

Aplikace

Poslední hlavní funkcí, která je přístupná v levé části hlavní strany, jsou aplikace. Aplikace vytváří vývojáři třetích stran, nicméně vytvořit si je může kdokoliv. Vytvořené aplikace má uživatel možnost umístit na své stránky. Společně s vytvořenou aplikací se vytvoří i karta, u které je možné měnit pořadí například tak, že bude zobrazena hned za kartou s informacemi. K dispozici je možnost spolupráce s jedním z marketingových vývojářů Facebooku. Externí vývojáři se musí řídit Zásadami platformy Facebook pro vytváření a provozování aplikací na Facebooku. Všechny informace, které aplikace shromáždí, jsou umístěny na serverech vývojářů a Facebook za ně není odpovědný. Pokud by uživatel chtěl některé informace odebrat, musel by kontaktovat přímo vývojáře.

Hlavní podíl aplikací na Facebooku vytvořených třetími stranami mají hry. Pro přehlednost bylo vytvořeno Centrum aplikací a her, kde má uživatel možnost vyhledávat podle názvu, kategorie, oblíbenosti a mnoha dalších parametrů. Mezi nejoblíbenější hry na začátku roku 2016 patřily Candy Crush Soda Saga, Farm Heroes Saga a kulečníkový simulátor 8 Ball Pool.

Po výběru aplikace se uživatel dostane na její stránku, kde může vidět video, nebo obrázky z aplikace. Uživatel má dvě možnosti, spustit hru, nebo ji odeslat na mobilní zařízení, na které mu přijde upozornění, že hra je připravena ke spuštění. Při spuštění aplikace uživatel automaticky souhlasí se zpracování osobních údajů uvedených na svém profilu. Seznam všech je nevýrazným písmem zobrazen v části pod možností spuštění hry.

Funkcionalita aplikací, ale především her, často časem uživatele přinutí k propagaci hry na svém profilu, popřípadě k zaslání určitého finančního objemu. Facebook nabízí vrácení peněz do šedesáti dnů od původní transakce, pokud se uživatel stal obětí podvodu falešné, nebo neautorizované aplikace.

Další funkce

Facebook neustále přidává nové funkce, ty hlavní již byly představeny, nicméně existuje ještě mnoho dalších. Mezi oblíbenou funkci patří Lokality. Tato funkce umožňuje uživateli přidat k příspěvku polohu. Tato funkce je pro nezletilé uživatele v jejich výchozím nastavení vypnuta a po zapnutí této funkce je nezletilý neustále upozorňován na aktivitu této funkce. Každý uživatel má možnost vidět historii svých uvedených poloh.

Dalším typem funkcí, které jsou u uživatelů velice oblíbeny, jsou tvorby videí k různým speciálním dnům. Mezi takové patří Přehled roku a Friends Day Video. Užitečnou novou funkcí je služba „Jste v bezpečí?“. Tato služba umožní uživatelům během katastrofy rychle sdělit přátelům, že jsou v pořádku.

Pro firmy je velice užitečnou funkcí Nabídka. Tato funkce umožňuje firmám vytvoření nabídky. Jedinou podmínkou je, že stránka musí mít více, než 50 označení To se mi líbí. Pro vytvoření nabídky správce stránky vyplní pouze název, popis, datum konce nabídky a limit počtu uplatnění dané nabídky.

Poslední zmíněnou užitečnou funkcí pro firmy je Hodnocení a recenze. Jedná se o hodnocení dané stránky pomocí hvězdiček. Hodnocení funguje tak, že se vytvoří průměr ze všech veřejných hodnocení, které stránka získala a funguje jako ukazatel kvality dané stránky.

2.1.5. Mobilní aplikace

Facebook

Mobilní aplikací, která obsahuje většinu funkcí aplikace webové je Facebook. Tato aplikace je dostupná v několika verzích podle toho, na které platformě běží. Funkcionalita chatu je v mobilní verzi rozdělena a poskytuje ji aplikace Messenger. Tyto dvě aplikace jsou propojeny a uživatel je mezi nimi automaticky přesměrováván. Další výhodou používání mobilní aplikace Facebook je vyšší rychlost než u mobilní verze stránek dostupných na adrese m.facebook.com.

Messenger

Jak již bylo řečeno, Messenger slouží uživatelům mobilních zařízení jako chat a zaznamenal více než miliardu instalací. [28] Aplikace Messenger poskytuje uživateli stejné funkce jako chat ve webové verzi. Dále nabízí uživatelům možnost posílání SMS zdarma svým přátelům díky synchronizaci kontaktů. Messenger je dostupný i ve verzi pro chytré hodinky Apple Watch, ve které je možné číst zprávy a posílat rychlé reakce (To se mi líbí, aktuální poloha, hlasové klipy, samolepky).

Facebook Pages Manager

Tato aplikace umožňuje uživateli prostřednictvím tabletu, nebo smartphonu spravovat až 50 stránek na Facebooku. Aplikace umožní uživateli, který je správcem stránky, posílat zprávy, zobrazovat přehledy, sdílet obsah a kontrolovat aktivity na stránce.

2.1.6. Hrozby

Facebook je nejpoužívanější sociální sítí s velkou uživatelskou základnou a proto je také velice oblíbený mezi různými jedinci, kteří se snaží nějakým způsobem poškodit uživatele. Hrozeb a rizikových jevů je na Facebooku veliké množství.

Spam

Velice častým způsobem kontaktování osob s nevyžádaným obsahem a žádostmi je spam. Obětí spamu se může stát uživatel, který zobrazí škodlivý odkaz, nainstaluje škodlivý software nebo jeho přihlašovací údaje k osobnímu účtu na Facebooku získají podvodníci.

Adware

Adware je typ softwaru, který monitoruje aktivitu uživatele a na základě získaných údajů uživateli nutí reklamu. Často tento software změní domovskou stránku a v rámci Facebooku zobrazuje bannery s reklamou. Adware je často spojován se spywarem, rozdíl je takový, že spywarové programy jsou instalovány bez vědomí uživatele a shromažďují a odesílají informace o uživateli. [29]

Malware

Malware je software, který může provádět jménem uživatele akce jako odesílání zpráv a aktualizace stavu. Dále může provádět sběr informací o účtu a může být použit i k získání přístupu k účtu. Na Facebooku se malware nejčastěji šíří skrze „šokující“ videa sdílená na různé stránky nebo návštěvou stránek, které nabízejí speciální funkce a stažení doplňku pro prohlížeč. Mezi nejčastější nabízené podvodné funkce a doplňky patří změna barvy profilu a odebrání Timeline.

Příkladem využití malware je případ z roku 2014, kdy bylo zjištěno, že podvodníci využili tento škodlivý software pro získání bitcoinů (virtuální měna). Uživatel obdržel soukromou zprávu od napadeného účtu s nakaženým softwarem, který sice neshromažďoval žádná data, ale využíval výpočetní výkon napadeného počítače k získání virtuální měny. [30]

Phishing

Phishing je technika, kterou používají podvodníci k získání citlivých dat uživatele. Na Facebooku se jedná většinou o zadání přihlašovacích údajů do formuláře na falešné stránce. Často jsou tyto stránky pro běžného uživatele k nerozpoznání od oficiálních stránek. Dalšími častými informacemi, které se podvodníci snaží získat, jsou informace k internetovému bankovnictví a kreditní kartě.

Sharebaiting

Sharebaiting nutí uživatele sdílet určitý obsah pod falešným příslibem určité odměny. Odměnou může být například možnost sledování momentálně nedostupného videa, nebo možnost výhry nějaké ceny.

Podvody využívající samospuštění XSS

Cross-site scripting (XSS) je vektorový útok, který využívá bezpečnostních chyb ve skriptech a používá se ke krádeži citlivých informací, pomocí kterých podvodník využívá účet uživatele především k finančním podvodům, spamu a rekrutování dalších lidí. Nejčastěji se o podvod typu XSS jedná, pokud uživatele osloví jeho přítel, který se již stal obětí XSS podvodu s tím, že ví, jak napadnout cizí účet na Facebooku. Tuto zprávu píše již podvodník, který se účtu přítele zmocnil a snaží se, aby uživatel vložil škodlivý kód do konzoly JavaScriptu. [31]

ClickJacking

Clickjacking je podvodníky využíván tak, že je na Facebook umístěn falešný objekt, který přiměje uživatele udělat akci, kterou udělat nechtěl. Jedná se například o umístění neviditelného tlačítka „To se mi líbí“ na jiné, viditelné tlačítko. Díky neviditelnému tlačítku uživatel označí daný příspěvek (stránku) že se mu líbí, přitom tuto akci provést nechtěl.

Škodlivé aplikace

Aplikace na Facebooku žádají uživatele, aby jim umožnily přístup k určitým informacím. Škodlivé aplikace však požadují více informací, než je k jejich funkci potřeba. Získané informace zneužívají k přístupu k uživatelskému účtu, následnému zveřejňování nežádoucích příspěvků pod jménem napadeného uživatele a dalších nekalých aktivit.

Krádež přístupového tokenu

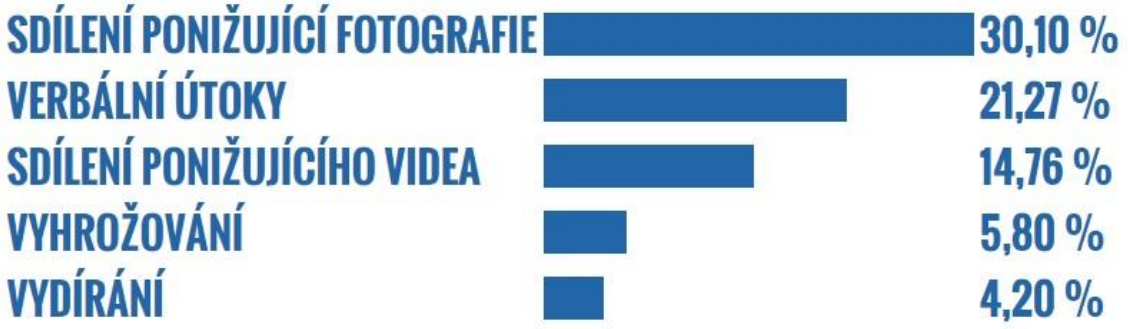
Pomocí přístupového tokenu aplikace získávají oprávnění přidávat příspěvky jménem uživatele. Přístupové tokeny jsou obsaženy v URL adrese Facebooku a podvodníci tyto údaje získávají tak, že je uživatel vloží na určitý podvodný web. Mezi hlavní triky, na které se podvodníci snaží nalákat uživatele, je možnost získat více fanoušků na stránky, změnit barvu Facebooku, zjistit, kdo si zobrazil uživatelův profil, nebo možnost zobrazit nějaké šokující video. Po získání přístupového tokenu podvodníci šíří spam.

Kyberšikana

Kyberšikana je záměrné agresivní chování, které útočník, nebo skupina útočníků provádí prostřednictvím elektronických médií. Kyberšikana se v největším množství týká dnešních dětí. [32]

Jelikož jsou sociální sítě hlavním komunikačním prostředkem dnešní doby, je vhodné předpokládat, že kyberšikana probíhá i na těchto sociálních službách. Konkrétně Facebook má největší uživatelskou základnu a možností kyberšikany je zde mnoho. Mezi hlavní typy kyberšikany patří verbální urážky prostřednictvím zpráv a komentářů, úprava a zveřejnění kompromitujících fotografií nebo zveřejnění osobních informací uživatele. Skupinovou formou kyberšikany na Facebooku může být vyloučení z určitých skupin, konverzací, událostí či hromadné vymazání uživatele z přátel. [32]

Výzkum „České děti a Facebook“ za rok 2015, který uskutečnilo Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s firmami Seznam.cz, Vodafone, Policií ČR a Sdružením Linka bezpečí zjistil, že z celkového počtu 1248 respondentů ve věku od 8 do 17 let ze všech regionů ČR se 30 % setkalo s kyberšikanou ve formě sdílení ponižující fotografie, 21 % s verbálními útoky, 15 % se sdílením ponižujícího videa, 6 % s vyhrožováním a 4 % s vydíráním. [33]



Graf 2: Typy kyberšikany u dětí ve věku 8 - 17 let [33]

Kyberstalking

Kyberstalking je pronásledování a opakované, stupňované obtěžování v různé intenzitě prostřednictvím informačních a komunikačních technologií. Útočník se často pomocí zpráv na Facebooku a odesílání žádostí o přátelství snaží opakovaně kontaktovat oběť, které po navázání kontaktu často vyhrožuje. Některé incidenty z oblasti kyberstalkingu zahrnují výhružky nejen oběti, ale i její rodině, přátelům či spolupracovníkům. Výhružkou může být například zveřejnění určité informace, nebo fotografie, kterou útočník o oběti získal. Dále chování kyberstalkera zahrnuje útok na data nebo osobní vlastnictví oběti, sbírání informací o oběti, odloučení oběti od společnosti a nabádání ostatních uživatelů v obtěžování oběti. Mezi kyberstalkery se nejčastěji řadí obdivovatelé a bývalí partneři. [34]

Kybergrooming

Mezi další velice nebezpečný jev patří kybergrooming. Kybergroomer je osoba, která se snaží s obětí sblížit pomocí online komunikace. Po určitém čase se však kybergroomer začne zajímat o sexuální život oběti a snaží se výměnou získat materiály se sexuálním podtextem (sexuální fantazie, nahé fotografie). Po získání těchto materiálů se snaží domluvit s obětí osobní schůzku s úmyslem zneužití oběti. Kybergroomer je často pedofil, který zaměřuje svoji pozornost na nezletilé děti. Facebook je kvůli velké koncentraci mladých lidí ideálním místem pro kybergroomery. [35]

Další hrozby

Na sociálních sítích a především Facebooku existuje mnoho dalších hrozeb, které mohou nějakým způsobem poškodit uživatele. Jednou z nich je hrozba zneužití osobních údajů. Právě osobní informace, které uživatel sdílí na svém profilu, může kdokoliv zneužít například ke stalkingu a dalším výše uvedeným hrozbám.

Mezi další hrozby především u nezletilých uživatelů patří sexting. Sexting je posílání a přijímání textových zpráv, fotografií nebo videí se sexuálním obsahem. Sexting využívají kybergroomeři k získání nahých fotografií nebo videí uživatele, kterého následně vydírají k osobní schůzce. [36]

Poslední zmíněnou hrozbou je flaming, který je charakterizován jako zbytečně agresivní a nepřátelské chování uživatele, který většinou uráží, nadává, nebo dokonce vyhrožuje jinému uživateli. [37]

2.1.7. Soukromí

Facebook v závislosti na službách, které uživatel využívá, shromažďuje spoustu informací. Tyto informace Facebook využívá k vylepšení svých služeb a následně je sdílí s dalšími uživateli. Celá kapitola je zpracována pomocí stránky o soukromí na Facebooku. [38]

Shromažďované informace

Facebook shromažďuje obsah zpráv či jiné komunikace s ostatními uživateli. Dále také informace o tom, jak uživatel využívá služby včetně typu obsahu, propojení, frekvenci a dobu trvání určitých aktivit uživatele. Mezi informace, které Facebook shromažďuje, patří i informace uvedené při registraci.

Shromažďovány nejsou pouze informace o samotném uživateli, ale i o uživatelích a skupinách, se kterými je uživatel ve spojení. Mezi tyto informace patří například fotografie, které s daným uživatelem někdo sdílel, a informace o nich. Dále veškerá interakce uživatele s propojenou skupinou a informace poskytované při nahrávání, synchronizaci nebo importu ze zařízení.

Z důvodu konzistence služeb Facebook shromažďuje data o zařízení využívající služby Facebooku podle oprávnění, které uživatel nastavil. Mezi informace o zařízení patří například operační systém, verze hardwaru, nastavení zařízení, výkon baterie, síla signálu, umístění zařízení a informace o připojení (název mobilního operátora, poskytovatel internetových služeb, prohlížeč, jazyk, časové pásmo, telefonní číslo a IP adresa zařízení).

Pokud uživatel využívá služby Facebooku k nákupu nebo finančním transakcím, jsou shromažďovány informace o daném nákupu či transakci (číslo platební karty, informace o platbě a účtu, fakturační informace, doprava a kontaktní údaje).

Facebook také shromažďuje informace, které uživatel poskytne při použití webů a aplikací třetích stran, které využívají služby Facebooku. Mezi takové informace patří informace o navštívených webech, použití služeb Facebooku na těchto webech a aplikacích, ale také informace, které vydavatel webu poskytuje uživateli.

Posledním typem informací, které Facebook shromažďuje, jsou informace od externích partnerů a od společností, jejichž vlastníkem nebo provozovatelem je Facebook.

Využití shromážděných informací

Facebook shromážděné informace využívá k poskytnutí a podpoře svých služeb. Na základě získaných informací personalizuje obsah pro uživatele a poskytuje mu návrhy. Kromě stránek, skupin a přátel Facebook umožňuje navrhovat uživatele pro označení na fotografii podle rysů obličeje. Tuto funkci však musí mít uživatel povolenou v nastavení profilu.

Informace o poloze Facebook využívá například k poskytnutí funkce pro oznámení polohy a vyhledání událostí nebo nabídek z okolí uživatele.

Dále jsou informace využívány pro komunikaci s uživatelem. Jedná se například o marketingové nabídky, informace o službách, informace o novinkách a odpovědi na dotazy uživatele. Marketingové nabídky a reklamy jsou díky získaným informacím relevantní podle zájmů uživatele.

Díky získaným informacím se Facebook snaží zlepšovat zabezpečení například pomocí nahlášení obsahu, které je vysvětleno v podkapitole o zásadách zabezpečení. Nejen k zabezpečení ale i k vytváření reklam a služeb Facebook využívá soubory cookie, pixelové tagy a další technologie.

Sdílení informací

Každý uživatel má možnost vybrat skupiny uživatelů, se kterými bude sdílet různé množství informací. Pokud uživatel sdílí některé informace veřejně, jsou dostupné všem uživatelům, dokonce i těm, kteří služby Facebooku nevyužívají. V případě, že uživatel okomentuje příspěvek jiného uživatele, komentář je zobrazen okruhu uživatelů, které vybral vlastník příspěvku. To samé platí pro označení příspěvku „To se mi líbí“. Dále má uživatel možnost sdílet obsah, na kterém je jiný uživatel se svým okruhem uživatelů.

Uživatel, který využívá aplikace a externí weby dává možnost provozovatelům těchto služeb získat informace o tom, co sdílí a zveřejňuje. Dále tyto služby mohou získat údaje jako je uživatelské jméno, id uživatele, věk, zemi, seznam přátel a informace sdílené s přáteli z veřejného profilu uživatele.

Veškeré informace jsou sdíleny v rámci všech společností pod Facebookem a v případě změny vlastnictví mohou být všechny informace o uživatelích převedeny na nového vlastníka.

Facebook spolupracuje s externími partnery a zákazníky, kterým poskytuje informace o uživatelích výměnou za služby, které podporují podnikání Facebooku. Tito partneři musí dodržovat přísné podmínky pro zacházení se získanými daty.

Sdílené informace má uživatel možnost spravovat v prostředí Facebooku pod záložkou Záznamy o aktivitách. Zde vidí své aktivity seřazeny od nejnovější po nejstarší a u každé aktivity okruh lidí, kteří danou aktivitu vidí. Veškeré informace přidružené k účtu si může uživatel stáhnout v jednom souboru pomocí nástroje Stahování informací.

V případě vymazání Facebookového účtu se Facebook zavazuje smazat všechen obsah, který uživatel zveřejnil. Nicméně informace, které o uživateli sdílí jiní uživatelé, smazány nebudou.

Globální zacházení s informacemi

Veškeré zacházení s daty z Evropské unie Facebook provádí v souladu s předpisy US-EU a US-Swiss Safe Harbor, které jsou stanoveny Ministerstvem obchodu. Na webu https://safeharbor.export.gov je možné společnost Facebook najít na seznamu certifikovaných společností. Právě díky programu Safe Harbor Facebook řeší spory s uživateli prostřednictvím organizace TRUSTe. Nicméně Facebook jak již bylo řečeno, může poskytovat osobní informace uživatelů všem společnostem, které jsou součástí Facebooku a třetím stranám. Dále Facebook může přenést informace získané v rámci Evropského hospodářského prostoru i do zemí mimo tento prostor podle podmínek popsaných v této kapitole. Případné změny zásad Facebook oznamuje v předstihu tak, aby mohli uživatelé reagovat dříve, než budou pokračovat ve využívání služeb. [39, 40]

2.1.8. Zásady zabezpečení

Aby uživatel předešel hrozbám na Facebooku, musí dbát na zabezpečení. Hlavním předpokladem pro bezpečnější používání sociálních sítí je uvážlivé chování uživatelů a zabezpečení osobního profilu, které bude blíže rozvedeno společně s dalšími způsoby zvýšení zabezpečení uživatelů na sociálních sítích v následující podkapitole.

Bezpečné chování

Bezpečné chování na sociálních sítích spočívá především v rozmyslu uživatele předtím, než provede nějakou akci. Některé škodlivé odkazy lze snadno identifikovat a uživatel tak může zabránit dalším bezpečnostním problémům. Dále by si každý uživatel měl pečlivě chránit své heslo, které by neměl nikdy sdílet a používat na jiném webu. Nemělo by se jednat o heslo, které je snadno uhodnutelné. Důležitým aspektem k ochraně přihlašovacích údajů je zabezpečený a nesdílený emailový účet. Pro útočníka je jednoduché získat heslo na Facebook, pokud má přístup k emailu uživatele. Dalším důležitým pravidlem je odhlášení od Facebooku, pokud uživatel sdílí počítač s dalšími osobami. Odhlásit se dá i vzdáleně přímo ze sekce Nastavení zabezpečení u osobního profilu uživatele, kde je vidět kdy, kde, a z jakého zařízení a prohlížeče byl uživatel přihlášen ke svému profilu. Po nalezení má uživatel možnost odhlášení z daného zařízení. Mezi poslední důležitá pravidla bezpečného chování patří nahlášení podezřelého obsahu, potvrzení žádosti o přátelství pouze známým lidem a úprava nastavení soukromí.

Nahlášení obsahu

Každý uživatel má možnost anonymně nahlásit pro něj nějakým způsobem podezřelý, nebo hanlivý obsah. Facebook nahlášený obsah kontroluje a ten obsah, který porušuje Podmínky používání služby Facebook nebo Zásady komunity odstraňuje. I obsah, který neporušuje podmínky a zásady na Facebooku může být pro uživatele nepříjemný, proto má možnost přizpůsobit si, jaký obsah se mu zveřejňuje. [41]

Antivirová ochrana

Dalším předpokladem pro zvýšení ochrany uživatele je přítomnost antivirového softwaru na zařízení, ze kterého uživatel přistupuje ke svým sociálním sítím.

Facebook ve spolupráci se společnostmi Microsoft McAfee, TrendMicro, Sophos a Symantec spolupracuje na odhalení škodlivého obsahu na Facebooku porovnáváním URL blacklistu, který kontroluje každý den trilióny kliků, a databázemi škodlivých odkazů výše uvedených společností pro zajištění větší úrovně zabezpečení. [42]

Centrum prevence šikany

Centrum prevence šikany je součástí Facebooku a jeho cílem je i podle názvu prevence kyberšikany. Facebook pomocí mnoha nástrojů bojuje ve spolupráci s Yale Center of Emotional Intelligence s šikanou a jejími následky. Centrum prevence šikany dává uživatelům informace o tom, jak využít bezpečnostní funkce Facebooku a jak se správně chovat v případě setkání s kyberšikanou. [43]

Facebook dále spolupracuje s různými organizacemi jako například Cyberbullying Research Center, Wired Safety, A Thin Line a dalšími organizacemi a kampaněmi, které mají za úkol zvýšit bezpečnost na internetu.

2.1.9. Zabezpečení osobního profilu

Přehled soukromí

Základní možnosti nastavení soukromí je možné spravovat pomocí Prohlídky soukromí. Díky této funkci má uživatel možnost pomocí průvodce projít nastavení soukromí u příspěvků, aplikací a profilu. U příspěvků má uživatel možnost změnit výchozí nastavení pro viditelnost přidaných příspěvků pro určité okruhy uživatelů (například pouze pro přátele, nebo určitou skupinu přátel). U prohlídky nastavení soukromí aplikací uživatel vidí všechny aplikace, do nichž se přihlašuje prostřednictvím svého Facebookového profilu. U každé aplikace v seznamu má uživatel, stejně jako u příspěvků, možnost nastavit viditelnost. Dále také odstranit danou aplikaci a všechny související příspěvky aplikace. Facebook však po zobrazení dalších informací varuje, že aplikace může mít stále k dispozici údaje, které uživatel v aplikaci sdílel i po odstranění. Posledním krokem je prohlídka soukromí informací sdílených na osobním profilu. V tomto kroku uživatel vidí informace, které má uvedené na svém Facebookovém profilu a okruhy uživatelů, se kterými tyto informace sdílí. Tyto okruhy může stejně jako u příspěvků a aplikací měnit.

Další položky přehledu soukromí umožňují uživateli zobrazit záznam o jeho aktivitách a zobrazit jeho Facebookový profil tak, jak ho vidí lidé, které nemá v přátelích. Tato funkce je užitečná pro kontrolu nastavení soukromí. Další možností nastavení soukromí je volba okruhu uživatelů, kteří mohou uživateli odeslat žádost o přátelství. Posledním základním nastavením soukromí je blokování uživatelů. Pro zamezení jakéhokoliv kontaktu s určitým uživatelem stačí zadat jeho jméno do textboxu a vybraného uživatele zablokovat. Uživatel má možnost všechny blokované uživatele zobrazit a případné blokování zrušit.

Nastavení a nástroje pro soukromí

Kromě nastavení a funkcí dostupných v Přehledu soukromí má uživatel možnost v rozšířeném nastavení využít další funkce a nástroje pro soukromí. Jedním z těchto nástrojů je omezení nastavení soukromí pro starší příspěvky sdílené na osobním profilu uživatele. Použitím tohoto nástroje se obsah, který uživatel sdílel veřejně, omezí pouze na přátele uživatele. Obsah na profilu uživatele pak budou moci vidět pouze jeho přátelé, popřípadě označené osoby a jejich přátelé. Dále je nastavení soukromí rozšířeno o volbu okruhu uživatelů, kteří mohou uživatele vyhledat pomocí telefonního číslo nebo emailu. Posledním nastavením soukromí je volba propojenosti Facebookového profilu s vyhledávači. Pokud se uživatel rozhodne mít tuto funkci zapnutou, jeho osobní profil bude zobrazován ve výsledcích vyhledávání různých vyhledávačů. Vypnutím této funkce již uživatelský účet nebude propojen s vyhledávači, nicméně určitou dobu trvá, než se osobní profil přestane ve výsledcích vyhledávání zobrazovat.

Nastavení Timeline a označování

Z hlediska soukromí je důležité i nastavení Timeline a označení. Facebook poskytuje uživatelům možnost zvolit, kdo může přidávat obsah na jejich Timeline a kdo obsah na Timeline uvidí. Velice užitečnou funkcí je kontrola příspěvků, v kterých je uživatel označen a mají být zveřejněny na Timeline uživatele. Povolením této funkce uživatel dostane upozornění pokaždé, když ho někdo označí v příspěvku a má možnost se rozhodnout, zda daný příspěvek na svou Timeline přidá nebo ho skryje. Pokud je uživatel již označen, má v nastavení možnost zvolit okruh uživatelů, kteří budou přidáni k příspěvku. Další užitečnou funkcí je kontrola označení. Zapnutím této funkce uživatel podobně jako v předchozím případě dostane upozornění a může schválit nebo zamítnout označení, které provedl nějaký uživatel, který není v jeho seznamu přátel.

Blokování

Stejně jako v přehledu soukromí má i zde uživatel možnost blokovat uživatele. Navíc zde uživatel může zablokovat pouze zprávy od určitého uživatele, nebo uživatele přidat do seznamu Omezeno. Lidem v tomto seznamu jsou přístupné pouze veřejné příspěvky uživatele. Dále uživatel může zablokovat pozvánky na události nebo pozvánky k aplikacím od určitého přítele. Kromě blokace uživatelů a omezení přátel má uživatel možnost blokovat i aplikace.

Nastavení Zabezpečení

Velice důležitým nastavením je nastavení zabezpečení. Facebook poskytuje uživatelům různé funkce zabezpečení. První taková funkce upozorní uživatele, že se někdo připojil k jeho účtu z nového zařízení nebo prohlížeče. Upozornění může uživatel dostávat i prostřednictvím emailu. Pro přihlášení z nového zařízení nebo prohlížeče existuje také další funkce, která nepřihlásí uživatele, dokud nebude ověřen pomocí bezpečnostního kódu. Touto funkcí se zamezí přihlášení jiného uživatele k cizímu účtu. V nastavení zabezpečení je možné také spravovat seznam zařízení, na kterých je uživatel přihlášen a seznam pověřených kontaktních osob, které po případné smrti uživatele mohou spravovat jeho profil. Pokud uživatel nechce, aby po jeho smrti kdokoliv jeho profil spravoval, má možnost volby odstranění účtu, ke kterému dojde po úmrtí uživatele. Dalším seznamem, který si uživatel volí, jsou důvěryhodné kontakty. Mezi takové kontakty patří blízcí přátelé, na které se může uživatel obrátit, pokud má problém s přihlášením ke svému účtu a ti mu sdělí bezpečnostní kód pro přihlášení. Facebook dále dává uživatelům možnost vložit svůj OpenPGP veřejný klíč na jejich profil. Tyto klíče mohou být použity pro zašifrování emailů odeslaných z Facebooku na preferovaný emailový účet uživatele. [44]

Facebook poskytuje uživateli možnost svůj účet dočasně deaktivovat. Pokud se uživatel pro tuto možnost rozhodne, jeho osobní profil nebude přístupný žádným uživatelům. Některé sdílené informace však mohou být stále některým uživatelům přístupné. Jedná se především o zprávy s daným uživatelem, který tyto zprávy stále vidí. Veškeré informace, které má uživatel uvedeny v profilu, jsou uloženy pro případ, že by se uživatel rozhodl účet znovu aktivovat. Pokud uživatel ví, že už nikdy nebude chtít získat přístup ke svému profilu, má možnost požádat o jeho kompletní odstranění. Proces odstranění účtu může trvat až 90 dní, nicméně po tuto dobu nemají ostatní uživatelé k daným informacím uživatele přístup. Záznamy protokolů a další záznamy Facebook může z technických důvodů uchovávat, ale již neobsahují žádné osobní identifikátory uživatele.

Aplikace

Aplikace a hry jsou jednou z velmi využívaných funkcí Facebooku, který poskytuje uživatelům možnost správy a nastavení oprávnění jednotlivých aplikací. Zatímco údaje jako je jméno a příjmení, profilový obrázek, úvodní fotka, pohlaví, sítě, uživatelské jméno a uživatelské ID jsou přístupné pro všechny aplikace, u ostatních informací, jako je seznam přátel, vztahy, narozeniny, zaměstnání, rodné město, označení to se mi líbí a mnoho dalších informací má uživatel možnost zvolit, zda je bude aplikaci poskytovat. Aplikace může uživatel také vymazat ze svého profilu. Facebook však varuje, že aplikace může stále obsahovat poskytnuté informace.

Další nastavení profilu

Uživatelé Facebooku mají možnost si také zvolit, jestli umožní sledování svého profilu. Sledování zajistí uživatelům vidět příspěvky, které uživatel zveřejní. Dále také spravovat nastavení upozornění a zvuky v rámci Facebooku. Další užitečnou funkcí je nastavení plateb a reklamy. Kromě dalších základních nastavení jako je změna jména, uživatelského jména, emailu a hesla poskytuje Facebook ještě další možnosti nastavení, které již nejsou úzce spjaté se zabezpečením.

2.2. Instagram

Další sociální sítí, která spadá pod společnost Facebook je Instagram. Tato aplikace vyšla 6. října 2010 a byla dostupná pouze pro platformu Apple, nyní je dostupná i pro platformy Android a Windows phone. Zakladatelem je Kevin Systrom, který na projektu spolupracoval s Mikem Kriegerem, kteří Instagram prodali společnosti Facebook v dubnu roku 2012 za miliardu dolarů. [45, 46]

Pro zpracování této kapitoly byl využit osobní profil [10] a nápověda aplikace Instagram. [47]

2.2.1. Funkcionalita Instagramu

Fotografie a videa

Hlavní funkcí Instagramu je sdílení fotografií a videí. Každý uživatel má možnost při přidání fotografie nebo videa využít jednoho z mnoha filtrů pro úpravu. Kromě filtrů má uživatel možnost upravit jas, kontrast, sytost, strukturu, barvu a další vlastnosti fotografie nebo videa, které se chystá nahrát.

Na Instagramu bylo možné nahrávat fotografie a videa pouze ve čtvercovém formátu, to však od verze aplikace 7.5 neplatí a Instagram při nahrání multimédia umožňuje uživateli vybrat mezi formátem krajina a portrét. [48]

Dále Instagram nabízí možnost instalace funkcí Boomerang a Layout. První jmenovaná funkce umožňuje uživateli vytvářet a sdílet minividea. Díky funkci Layout může uživatel přidat více fotografií do jednoho příspěvku na Instagramu. V posledním kroku před zveřejněním obsahu uživatel může přidat místo, označit lidi a přidat popisek, ve kterém jsou často používány hashtagy.

Vyhledávání

V srpnu roku 2015 Instagram překonal hranici 400 miliónů aktivních uživatelů, kteří každý den sdílejí přes 80 miliónů fotografií. Pro třídění takového velkého množství fotografií má uživatel možnost přidání hashtagu v popisku příspěvku, podle kterého je možné najít určitý obsah. [49]

Dalšími možnostmi vyhledávání je vyhledávání lidí podle jména, uživatelského jména na Instagramu, nebo podle různých míst, která Instagram uživateli nabídne na základě geografické polohy.

Profil

Oproti profilu na Facebooku je ten Instagramový velice jednoduchý. Uživatel má možnost zobrazit fotografie, které sdílel, nebo fotografie, na kterých je označený. Uživatel má možnost zobrazit interaktivní mapu fotek, která zobrazuje na mapě fotografie uživatele podle místa, kde byla fotografie pořízena.

Dále uživatel vidí vedle své profilové fotografie počet příspěvků, počet lidí, které sleduje a počet lidí, kteří sledují jeho.

Sledování a aktivita

Pro odběr veřejného obsahu sdíleného určitým Instagramovým profilem je nutné začít daný profil sledovat. Pokud profil není nastaven jako soukromý, odběr příspěvků a možnost zobrazení profilu proběhne ihned. Pokud je však profil nastaven jako soukromý, je třeba vyčkat na potvrzení žádosti o sledování, která je odeslána majiteli profilu. Veškerý odebíraný obsah je pak zobrazen v časové posloupnosti na hlavní stránce Instagramu uživatele.

Veřejný obsah, nebo obsah, který sleduje, může uživatel okomentovat, nebo označit srdcem a vyjádřit tak, že se mu příspěvek líbí. Veškeré aktivity, jako je okomentování, označení srdcem a sledování má uživatel možnost vidět v aktivitách. Jedná se o aktivity uživatelů vůči příspěvkům uživatele. Uživatel může také sledovat aktivitu uživatelů, které sleduje.

Instagram Direct

Poměrně novou funkcí, kterou Instagram nabízí, jsou zprávy nazvané Direct. Tato funkce umožňuje komunikaci mezi uživateli pomocí zpráv. Kromě klasických textových zpráv umožňuje i výměnu fotografií.

2.2.2. Soukromí a zabezpečení

Nastavení soukromí na Instagramu je oproti Facebooku velice jednoduché. Uživatel si může zvolit, zda svůj účet bude mít soukromý, nebo veřejný. Zapnutím soukromého účtu uvidí příspěvky uživatele pouze ti lidé, kterým uživatel schválí sledování jeho účtu. Ovlivněni tím jsou pouze lidé, které uživatel nemá na svém profilu jako sledující. Aktuálně sledujících se změna tohoto nastavení nedotkne a i nadále uvidí veškerý obsah, který uživatel sdílí. Z toho důvodu je důležité, aby si uživatel nastavil účet jako soukromý hned po registraci.

Ohledně bezpečnosti na Instagramu platí pravidlo „zablokovat a ignorovat“. Uživatel má možnost jiného uživatele zablokovat a přerušit tak veškerou komunikaci mezi těmito uživateli.

2.2.3. Osobní údaje

Instagram o svých uživatelích shromažďuje stejně jako Facebook velké množství osobních údajů a dalších informací. Mezi údaji, které uživatel poskytuje Instagramu přímo je uživatelské jméno a heslo, emailová adresa, informace uvedené na profilu (popis, profilový obrázek, telefonní číslo), veškerý uživatelský obsah (fotografie, komentáře, označení) a komunikace.

2.3. YouTube

YouTube se od svého vzniku v roce 2005 neustále vyvíjí a nabízí stále nové funkce. V současné době se jedná o nejnavštěvovanější videoportál na světě. YouTube je zařazen do sociálních sítí díky propojení obrovské komunity lidí, umožnění komunikace a navázání spojení mezi jednotlivými lidmi. V roce 2006 se stala novým majitelem YouTube společnost Google, která YouTube koupila za 1,65 miliardy dolarů. Popularitu dokazují statistiky, které uvádí, že YouTube má více než miliardu diváků po celém světě, kteří sledují každý den stovky miliónů videí a vytvoří tak miliardy zhlédnutí. [50, 51, 52]

Celá kapitola byla zpracována s využitím osobního profilu na oficiálních stránkách sociální sítě YouTube [53] a nápovědy YouTube. [54]

2.3.1. Funkcionalita YouTube

YouTube poskytuje uživatelům mnoho funkcí, tou hlavní však zůstává nahrávání a přehrávání videí. Pro plné využití všech funkcí a sociální prvků YouTube však uživatel musí být přihlášen.

Videa

YouTube poskytuje kvalitní a intuitivní přehrávač videí, který umožní uživateli základní operace s videem. Mezi tyto operace patří pozastavení videa, přechod na další video, volba hlasitosti, režimu obrazu (klasický režim, režim kino, na celou obrazovku) a základní nastavení videa. V nastavení videa uživatel může zvolit rychlost přehrávání, viditelnost poznámek ve videu a vypnutí nebo zapnutí automatického přehrávání. Hlavním nastavením je však nastavení kvality obrazu, kde má uživatel možnost volby rozlišení videa, které závisí na kvalitě nahraného videa a rychlosti uživatelova připojení k internetu. YouTube ve výchozím nastavení mění kvalitu videa automaticky podle velikosti videopřehrávače. YouTube podporuje videa ve vysokém rozlišení 4K, která jsou přenášena rychlostí 2160p a poskytuje tak velice čistý a detailní obraz. U každého videa jsou zobrazeny popisné informace, které se uživatel, který video nahrál, rozhodl zveřejnit. Uživatel má možnost přidávat videa do vlastních seznamů videí, které si může uložit a přehrát tak najednou skupinu všech oblíbených videí. Stejně tak může přidávat svá vlastní videa do seznamů a vytvářet tak nové seznamy videí. [55]

Každý přihlášený uživatel má také možnost videa nahrávat. Po nahrání videa uživatel zvolí název videa, popis, štítky a miniaturu videa. Miniatury videa jsou vytvořeny automaticky z určitých částí videa. Ověřený uživatel má možnost vytvoření vlastních miniatur a dalších funkcí. Základní informace o videu má uživatel možnost přeložit do jiných jazyků sám, nebo získat překlad od profesionálních překladatelských služeb. V dalším nastavení videa uživatel volí, zda povolit komentáře u videa, zda uživatelé mohou zobrazit hodnocení u videa, kategorii videa, licenci a vlastnictví práv. Posledním nejdůležitějším nastavením je soukromí. Uživatel má možnost vybrat, zda bude video soukromé (zobrazí se pouze tomu, kdo ho vytvořil), veřejné (bude přístupné komukoliv), nebo neveřejné (zobrazí se pouze uživatelům, kteří vlastní přímý odkaz na video).

YouTube nově také poskytuje uživatelům funkci živého vysílání. Tato funkce je stejně jako přidání miniatur videí dostupná pouze pro ověřené uživatele. Uživatel může zahájit živé vysílání okamžitě a YouTube automaticky zvolí rozlišení, snímkovou frekvenci a další informace nezbytné pro spuštění živého vysílání. Druhou možností je využití funkce plánování události, která poskytne uživateli volbu soukromí, času zahájení, a další rozšiřující informace. Po spuštění přímého přenosu má uživatel možnost komunikovat se svými diváky prostřednictvím živého chatu. Živý chat je po ukončení přímého přenosu zobrazen jako komentáře pod videem a je možné jej kdykoliv v nastavení vypnout.

Úprava videí

Po přidání videa má uživatel možnost jej upravit díky nástrojům, které vidí pod přidaným videem, nebo ve studiu pro autory v rámci správy videí. Upravovat může nejen základní informace o videu, ale díky nástroji pro vylepšení také video jako takové. Na videu může upravit jas, kontrast, sytost, teplotu barev, zpomalení, zrychlení a další volitelná nastavení. U videa může uživatel také zvolit jeden z mnoha filtrů a speciálních efektů pro rozmazání obličeje nebo určité části videa. Pro méně zkušené uživatele YouTube poskytuje automatickou opravu videa, která opraví světla, barvy a stabilizaci, která odstraní roztřesené pohyby kamery. Video je také možné oříznou nebo otočit o 90°. Pro složitější úpravy videa má uživatel možnost využít editor videa YouTube, který umožňuje například kombinovat několik videí dohromady, přidat text, přechod mezi určitými snímky, přidat fotografie a další užitečné funkce pro tvorbu videa.

Kromě vylepšení kvality videa má uživatel možnost přidání nekomerční hudby do videa. Seznam skladeb je uživateli zobrazen podle oblíbenosti, nicméně uživatel má možnost daný seznam seřadit podle hudebního žánru, nebo specifickou skladbu hledat pomocí názvu.

Další užitečnou funkcí úpravy videa je přidání poznámek do videa. Umístění poznámky a její podobu si volí uživatel sám. Posledními užitečnými funkcemi je přidání titulků v určitém jazyce a přidání karty. Karta je interaktivní prvek, který po kliknutí odkáže uživatele na předem nastavené URL.

Domovská stránka, trendy a odběry

Domovská stránka přihlášeného a nepřihlášeného uživatele se liší především v typu zobrazovaných videí. Zatímco nepřihlášenému uživateli jsou zobrazena populární videa specifická pro celou populaci, uživateli přihlášenému se zobrazují různé kategorie pro něj relevantních videí. Přihlášený uživatel například vidí seznam videí, která si již pustil a doporučená videa na základě obsahu, který uživatel přehrával v minulosti. Dále uživatel vidí výběr videí z kanálů, které odebírá. Kanály, které uživatel odebírá a jejich videa má možnost zobrazit v kategorii odběry, kde jsou videa od všech odběrů seřazeny podle časové posloupnosti od nejnovějších po nejstarší. Seznam kanálů, které uživatel odebírá, má k dispozici v hlavním menu na levé straně. Poslední položkou stejnou jak pro přihlášené, tak pro nepřihlášené uživatele, jsou trendy. Jedná se o videa, která jsou na YouTube v danou chvíli nejsledovanější.

Kanál

Kanál slouží jako profil uživatele, kde může sdílet svá videa, vidí své seznamy videí a další popisné informace. Podobně jako tomu je u většiny profilů na sociálních sítích si uživatel může zvolit profilový obrázek a úvodní fotografii, která bude zobrazena všem návštěvníkům jeho kanálu. Pomocí třídění videí do seznamů videí je pro návštěvníky snadnější orientace v různých typech videí uživatele.

V nastavení kanálu má uživatel možnost volby různých nastavení. Jedná se například o již zmíněné vkládání vlastních miniatur, možnost nabízet placený obsah, možnost označit videa jako neveřejná a soukromá, aktivace přímých přenosů, možnost použít v popisu odkazy na různé sponzory a partnery, aktivace delšího obsahu videí a především aktivace zpeněžení videí. Pro využití těchto funkcí je potřeba splnit několik předpokladů. Těmi základními je mít kanál ověřený a v dobrém stavu. Kanál lze ověřit pomocí zadání mobilního čísla, na které uživateli přijde ověřovací kód, kterým potvrdí, že se jedná opravdu o něho. Kanál v dobrém stavu je takový kanál, který neporušuje pokyny pro komunitu a autorská práva kvůli obsahu.

Jakmile uživatel disponuje ověřeným kanálem v dobrém stavu, může využít výše zmíněné funkce. Například základní délku nahraného videa může z 15 minut navýšit až na 11 hodin, kde maximální velikost videa je 128 GB. Při velikosti videa nad 20 GB je třeba mít aktuální verzi internetového prohlížeče.

Pro zpeněžení obsahu musí uživatel navíc být partnerem YouTube. Aby se uživatel mohl stát partnerem YouTube musí nahrávat původní kvalitní videa, která jsou relevantní pro inzerenty a obsah musí splňovat smluvní podmínky a pokyny pro komunitu YouTube. Dále se uživatel musí seznámit s materiály o autorských právech a zpeněžení musí být dostupné v dané zemi, ve které uživatel působí. V České republice tato funkce dostupná je, stejně jako v dalších více než šedesáti zemích. Po aktivaci zpeněžení má uživatel možnost u vhodných videí aktivovat vydělávání peněz reklamou. Aby uživatel mohl videa zpeněžit, musí obsah vytvořit on, nebo mít oprávnění ho komerčně využít. Oprávnění musí být schopen v případě nutnosti doložit. Aktivace zpeněžení se provádí při nahrávání videa, je však možné tuto akci provést i poté, co je video nahráno. Hodnota příjmů závisí na několika faktorech. Těmi hlavními je typ a cena reklam, které budou zobrazeny u videí uživatele. Dalšími faktory je například počet zhlédnutí a délka videa. Nejvíce vydělávajícím člověkem v současné době je Švéd Felix Kjellberg, který vystupuje pod jménem PewDiePie. Jeho roční příjmy se pohybují okolo 12 miliónů dolarů. [56]

Aby uživatel mohl inkasovat příjmy z reklam, musí propojit svůj účet YouTube s AdSense, což je služba od společnosti Google, která zobrazuje relevantní reklamy k obsahu u jednotlivých videí. Pro vyplacení příjmů z AdSense musí uživatel dosáhnout určitých hranic. V následující tabulce jsou zobrazeny jednotlivé finanční hranice v různých měnách pro jednotlivé aktivity uvedené v hlavičce sloupců. [57]

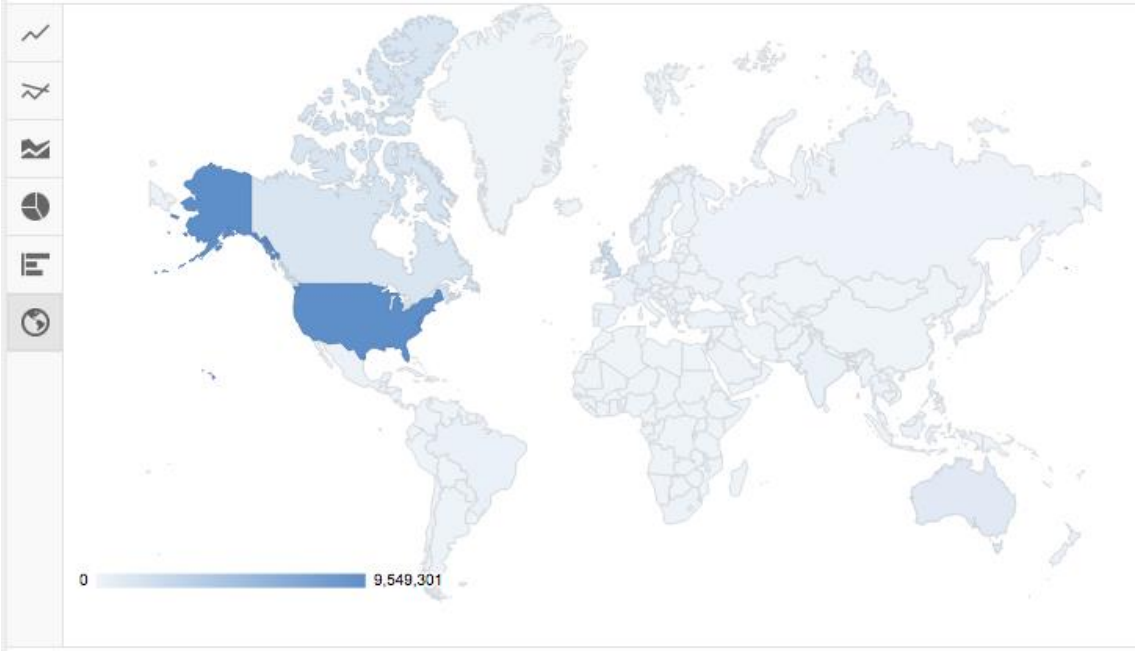
Hranice	Zadání daňových údajů	Ověření adresy	Zadání platební metody	Platba	Zrušení
Americký dolar (USD)	0 $	10 $	10 $	100 $	10 $
Euro (EUR)	není stanovena	10 EUR	10 EUR	70 EUR	10 EUR
Britská libra (GBP)	není stanovena	10 £	10 £	60 £	10 £
Australský dolar (AUD)	není stanovena	15 A$	15 A$	100 A$	15 A$
Kanadský dolar (CAD)	0 C$	10 C$	10 C$	100 C$	10 C$
Česká koruna (CZK)	není stanovena	200 Kč	200 Kč	2 000 Kč	200 Kč

Tabulka 1: Hranice platby AdSense [58]

Analytics

Nástroj YouTube Analytics poskytuje uživateli možnost sledovat, jak se jeho kanálu podle aktuálních metrik a přehledů daří. Uživatel se tak může dozvědět například celkovou dobu sledování jeho videí, zdroje návštěvnosti, demografické údaje, celkový počet zhlédnutí, poměr líbí se/nelíbí se, míru udržení publika a další užitečné informace. K dispozici má například také srovnání jednotlivých videí. Veškeré informace jsou graficky interpretovány pomocí přehledných grafů různých typů (spojnicový, výsečový, sloupcový, skládaný plošný). Velice užitečným přehledem je přehled tržeb. Pomocí tohoto přehledu má uživatel možnost zobrazit například odhadované tržby za vybrané období a v rámci vybrané oblasti. Dále odhadované tržby z různých typů reklam, odhadované transakční tržby a tržby z YouTube Red.

Uživatel má také k dispozici interaktivní mapu, pro sledování demografických údajů. Oblasti, kde se dané video zobrazuje nejvíce, jsou označeny tmavší barvou.



Obrázek 3: Interaktivní mapa YouTube Analytics [59]

Další funkce

Kromě výše zmíněných hlavních funkcionalit a doplňkových sociálních funkcí, jako jsou komentáře, sdílení a další, YouTube poskytuje další zajímavé inovativní funkce a služby. Za zmínku stojí například služba YouTube Red i přes fakt, že zatím není v České republice dostupná. Jedná se o novou placenou službu, která umožní uživatelům uložit si oblíbená videa na mobilních zařízeních a sledovat je později offline bez reklam. Dále bude poskytovat obsah, který bude dostupný pouze v této službě. Hlavní tváří této nové služby je již zmíněný Felix Kjellberg.

2.3.2. Autorská práva

Autorská práva jsou pro komunitu nahrávající obsah na YouTube velice důležitá. Poskytují jím ochranu jimi vytvořeného originálního obsahu. Vlastník má tak výhradní práva k používání jeho videa. YouTube poskytuje několik nástrojů a informací pro správu autorských práv. Vlastník má možnost podat stížnost pomocí formuláře pokud má dojem, že jeho video chráněné autorskými právy bylo na YouTube publikováno bez jeho svolení. Pokud je nějaké video již zablokováno a uživatel se domnívá, že zablokování bylo neoprávněné, má možnost podat protioznámení, které bude vyřízeno do deseti pracovních dnů. Pokud uživatel ve videu použije materiál, který je chráněn autorským právem, může být vznesen požadavek na umístění videa do systému Content ID. Takový materiál (například zvuk) může být zablokován, nebo může být příjem z reklam přesměrován na vlastníka autorských práv k danému materiálu. [60]

Jakmile uživatel poruší autorská práva nebo pokyny pro komunitu, hrozí mu, že přijde o statut kanálu v dobrém stavu a tím pádem i o funkce, které jsou podmíněné tímto stavem. Při uvalení tří sankcí na uživatele je jeho účet ukončen. Jednotlivé porušení autorského práva lze řešit osobní žádostí na osobu, která vznesla požadavek na odstranění videa a má možnost požadavek stáhnout. V jiném případě sankce vyprší po šesti měsících, pokud během této doby uživatel absolvuje Školu autorského práva a nebude vůči němu uvalena žádná další sankce za porušení autorského práva. Stav účtu vzhledem k autorským právům je vidět ve stavu a funkcích kanálu. [60]

Pro udělení oprávnění k použití díla určitému uživateli tvůrci používají licenci Creative Commons. Tato licence umožňuje uživateli používat daný obsah označený jako CC BY i ke komerčním účelům ve svých videích. Možnost označit videa licencí Creative Commons mají pouze ti uživatelé, kteří mají účet v dobrém stavu. Další možností pro použití materiálu chráněného autorskými právy je využití principu „fair use“. Tento princip se používá především v USA, kde jej lze uplatnit při komentáři, průzkumu, výuce, kritice nebo zpravodajství. Přesná pravidla se pro jednotlivé země liší a ve většině případů je použití tohoto principu posuzováno soudem. [60, 61]

2.3.3. Zabezpečení

YouTube jakožto velice oblíbená a rozšířená sociální síť, která poskytuje interakci mezi uživateli, je stejně jako Facebook v některých případech zneužívána k obtěžování, kyberšikaně a dalším negativním jevům. YouTube poskytuje určité rady, zásady a nástroje pro vypořádání se s jednotlivými negativními jevy na jejich sociální síti.

Obtěžování a kyberšikana

Obtěžování a kyberšikana v prostředí YouTube probíhá ve většině případů prostřednictvím komentářů. Uživatel má možnost komentáře, které již překročily určitou hranici, nahlásit a YouTube takové komentáře odstraní. Pokud kyberšikana přichází výhradně od určitých osob, má uživatel možnost komentáře vymazat a dané uživatele zablokovat. Zablokovaný uživatel nebude nadále moci přidávat komentáře k žádnému z videí uživatele, ani ho kontaktovat pomocí soukromé zprávy. Pokud obtěžování nebo kyberšikana vystupňuje do vážné podoby, je uživateli doporučeno nahlásit to příslušnému státnímu orgánu.

Nevhodný obsah

Prvním typem nevhodného obsahu je nahota a sexuální obsah. Sexuální obsah typu pornografie a fetišistická videa na YouTube nejsou povolena. Videa, která obsahují nahotu, nebo jiný erotický obsah nemusí být nutně smazána, pokud je primární účel videa vzdělávací, dokumentární, vědecký nebo umělecký. Taková videa mohou podléhat věkovému omezení a jejich obsah při zapnutí funkce omezeného režimu není uživateli zobrazen.

Dalším typem nevhodného obsahu je násilný nebo explicitní obsah. U tohoto obsahu platí podobná pravidla jako u předchozího nevhodného obsahu. U některých videí je nevyhnutelné, že obsah je násilný nebo explicitní. Odstranění takového obsahu však lze předejít vhodným popisem a doplňujícími informacemi, které sdělí uživateli, proč je obsah videa svým způsobem nevhodný. Jako v přechozím případě může takový obsah podléhat věkovým omezením. V souvislosti s násilnými videi YouTube přísně zakazuje veškeré teroristické propagandy a celkově zakazuje jakékoliv teroristické organizaci používat YouTube.

Posledním typem je škodlivý nebo nebezpečný obsah. Kromě již zmíněného zákazu teroristických propagand prostřednictvím videí YouTube se považuje za škodlivý nebo nebezpečný obsah například výroba bomby, užívání tvrdých drog nebo nebezpečné hry, při kterých hrozí smrt. Zakázána jsou také videa, která nabádají uživatele k páchání násilných činů. Důraz YouTube klade především na škodlivý nebo nebezpečný obsah, ve kterém vystupují nezletilé osoby.

Pomluvy a výhružky

YouTube umožňuje uživatelům vyjádřit jejich svobodné myšlení, nepodporuje však pomluvy a výhružky. Jedná se především o nevhodný obsah, který je zaměřený vůči určité skupině lidí na základě rasy, postižení, pohlaví, věku, sexuální orientace nebo náboženství. Za závažné se považují výhružky pod fyzickým napadením jedince nebo určité skupiny lidí.

Předstírání identity

YouTube netoleruje kanály nebo videa, která mají za účel napodobit určitý, již existující obsah a vydávat se za něj. Takový obsah je po nahlášení automaticky odstraněn. Kanály a videa, která napodobují určitou společnost, mohou čelit právní stížnosti, kterou má vlastník původního obsahu možnost podat prostřednictvím právních formulářů pro nahlášení.

Spam, klamavé postupy a podvody

YouTube řeší veškeré formy podvodů, spamy a výhružky. Podvodné praktiky a spam se týká především snahy zvýšit počet zhlédnutí, označení „líbí se“ nebo komentářů. Videa a účty, u kterých se prokáží takovéto praktiky, jsou smazány. Penalizována jsou také videa s klamným obsahem, metadaty a zavádějícími nebo sexuálně provokativními miniaturami. Vydírání se považuje za vážný přečin a uživatel, který se stane obětí vydírání, by měl obsah nebo účet nahlásit a informovat příslušné bezpečnostní složky.

Bezpečnost mladistvých

Mladiství jsou na YouTube zastoupeni ve velkém procentu. Jejich ochrana a bezpečnost je pro YouTube důležitá. Proto pokud je identifikován jakýkoliv nevhodný obsah, ve kterém vystupují mladiství, je účet vlastníka obsahu pozastaven a obsah je smazán. Dále je takový případ ohlášen organizaci NCMEC, která spolupracuje s policejními a bezpečnostními složkami.

YouTube poskytuje mladistvým několik zásad pro jejich bezpečnost. Užitečným případem je zde pravidlo „babičky“, které mladistvým uživatelům říká, aby nenahrávali obsah, který by nemohli ukázat babičce nebo třeba budoucímu zaměstnavateli. Dalším užitečným tipem je používání funkcí zabezpečení YouTube.

Nastavení ochrany soukromí a bezpečnosti

YouTube nabízí několik nástrojů pro ochranu soukromí a bezpečnosti uživatelů. Mezi hlavní patří funkce Omezený režim. Pokud je tato funkce zapnutá, uživateli se nezobrazuje obsah, který je potenciálně nevhodný. Často je tato funkce využívána jako forma rodičovské kontroly. Tato funkce funguje na úrovni webového prohlížeče nebo zařízení, proto je nutné tuto funkci nastavit na všech zařízeních, ze kterých se daný uživatel přihlašuje ke svému osobnímu profilu na YouTube.

Další užitečnou funkcí je změna nastavení soukromí u jednotlivých videí, které uživatel nahrává. Videa mohou být veřejná, neveřejná nebo soukromá. Veškerá videa jsou defaultně nastavena jako veřejná a může si je prohlédnout kdokoliv. Proto je vhodné tomuto nastavení věnovat pozornost a u videí nastavit soukromí na neveřejná, pokud uživatel chce, aby k videu měli lidé přístup pouze prostřednictvím přímého odkazu, nebo soukromá, pokud uživatel chce, aby si obsah mohl zobrazovat pouze on.

Další funkce pro podporu zabezpečení je moderování komentářů a blokování uživatelů. Moderováním komentářů se rozumí odstranění, nahlášení, nebo skrytí nevhodných komentářů.

Nahlášení obsahu

Veškerý nevhodný obsah, definovaný výše, má uživatel možnost nahlásit. YouTube do 24 hodin ověří, zda se opravdu jedná o nevhodný obsah a pokud ano, obsah odstraní a případně zablokuje účet majitele obsahu, nebo na video udělí věková omezení. Nahlásit, stejně jako video, lze i nepřípustný komentář nebo celý kanál.

Nahlásit lze i videa nebo účet, který vyjadřuje myšlenky se sebevražednými sklony. YouTube navádí uživatele, kteří mají podezření na takovéto chování u některého z jiných uživatelů, aby navštívili stránku www.befrienders.org, kde je uveden seznam organizací, které se zabývají prevencí sebevražd.

2.3.4. Ochrana soukromí a osobních údajů

Každý uživatel má právo na své soukromí. Pokud tedy jakýkoliv uživatel toto právo porušuje sdílením citlivých informací o uživateli prostřednictvím videa, uživatel má dvě možnosti na řešení problému. Prvním krokem by mělo být kontaktování majitele videa a požádání jej o odstranění. Pokud uživatel nesouhlasí, nebo nereaguje, může uživatel oslovit YouTube. YouTube určí, zda má obsah být odebrán na základě jedinečné identifikace uživatele podle vzhledu, hlasu, jména a příjmení, čísla bankovního účtu nebo jiných osobních kontaktních údajů. Pokud je žádost oprávněná, YouTube kontaktuje majitele videa s oznámením o porušení ochrany osobních údajů a dá uživateli 48 hodin na odstranění videa, nebo všech osobních údajů. [62]

Aby uživatelé předcházeli takovýmto situacím, měli by dodržovat určité zásady pro ochranu osobních údajů. Hlavními zásadami je vhodné promyšlení zveřejnění osobních údajů a získání svolení od osob zahrnutých ve videu. Dále by uživatel neměl nikomu sdělovat své heslo.

Shromažďované informace

YouTube respektive Google shromažďuje podobně jako Facebook velké množství informací. Kromě osobních údajů zadaných při registraci to jsou i informace získané při používání služeb. Mezi takové informace patří informace o zařízení, z kterého se uživatel přihlašuje, vyhledávací dotazy, informace o hovorech daného čísla, informace o poloze a další informace. YouTube využívá k identifikaci prohlížeče a zařízení uživatele soubory cookie a podobné technologie. [63]

Veškeré shromážděné informace YouTube používá k vývoji vlastních služeb a k zobrazení relevantních výsledků. Osobní údaje má Google dostupné ve všech svých službách. Může tak například nastavit jméno, které uživatel nastavil při registraci služby Gmail, ve všech ostatních službách včetně YouTube. Google může veškeré informace použít i v reklamním kontextu. Toto však má uživatel možnost v nastavení omezit a nastavit tak, aby se například jeho profilový obrázek nezobrazoval v reklamách. [63]

Sdílení informací

Obecně Google neposkytuje osobní informace uživatelů společnostem, organizacím ani jednotlivcům. Výjimkou může být situace, kdy uživatel ke sdílení dá osobní souhlas. Další výjimkou jsou právní důvody nebo účel externího zpracování. Externím zpracováním se rozumí poskytnutí informací spřízněným společnostem, které pro firmu Google zpracovávají informace na základě předem daných pokynů a v souladu se zásadami ochrany osobních údajů. Společnost Google se zavazuje k zajištění ochrany osobních údajů i v případě prodeje, sloučení, nebo akvizice společnosti. [63]

Zabezpečení informací

Před neoprávněným přístupem k osobním informacím společnost Google chrání uživatele několika způsoby. Mnoho služeb šifruje pomocí zabezpečeného protokolu SSL, poskytuje dvoufázové ověření přihlášení k účtu a provádí pečlivé kontroly zpracování informací, aby se předešlo neoprávněnému přístupu do systému Google. Přístup k osobním informacím mají pouze zaměstnanci společnosti Google, smluvní partneři a zástupci, pro které jsou tyto údaje nezbytné pro zpracování. [63]

2.4. Google+

Další sociální sítí firmy Google je Google+. Tato sociální síť byla vytvořena jako konkurence pro Facebook, nicméně není tak úspěšná jako Facebook a nedosahuje ani takové popularity jako druhá sociální síť společnosti Google YouTube. Funkčnost služby Google+ je v mnoha směrech stejná jako u Facebooku, pouze se určité funkce liší názvem nebo specifickou funkcionalitou. Mezi odlišnou funkcionalitu se dá považovat komunikace. Google+ totiž oproti Facebooku poskytuje komunikaci samostatně jako oddělenou službu nazvanou Hangouts, která poskytuje uživatelům komunikaci prostřednictvím textových zpráv, telefonního hovoru a videohovoru. [5, 64, 65]

Velkou výhodou Google+ je propojení s ostatními službami a funkcemi společnosti Google. Přímo v panelu Google+ má uživatel možnost přejít na služby Hangouts, Gmail, Google Play, YouTube, Google Drive a mnoho dalších služeb, pro které se uživatel nemusí znovu přihlašovat.

Zásady ochrany osobních údajů jsou v tomto případě stejné jako u YouTube, proto je zbytečné je zde rozebírat znovu. [63]

2.5. Twitter

Twitter je dalším specifickým typem sociální sítě, která má za úkol umožnit uživatelům sdílet myšlenky a informace s ostatními uživateli. Jedná se o oblíbenou mikroblogovací službu, která měla k 31. 12. 2015 více než 320 miliónů aktivních uživatelů měsíčně. Jack Dorsey založil Twitter v roce 2006 a v současnosti působí ve firmě jako CEO. [66]

Twitter je poměrně jednoduchým nástrojem, který umožňuje uživatelům podělit se o svoji myšlenku, kterou musí zformulovat do délky maximálně 140 znaků. Postupem času bylo uživatelům umožněno přidat kromě textové zprávy i obrázek, gif, dokonce i jednoduchý dotazník pro krátkou anketu. Myšlenkám, které uživatelé sdílí na twitteru se říká „tweety“. [67, 68]

Uživatelé tuto sociální síť používají především pro získávání informací o celebritách, sportovcích, společnostech a lidech, o které se zajímají. Pro získávání informací stačí uživateli začít daný Twitterový účet sledovat a všechny příspěvky, které sledovaný účet přidá, budou zobrazeny na hlavní stránce uživatele. Uživatel může na „tweety“ reagovat a oslovit sledované uživatele přímo pomocí zpráv. Vzhledem k obrovskému množství „tweetů“ se používají hashtagy, které stejně jako u Instagramu slouží jako filtr podle názvu kategorií. [67, 68]

Při ponechání výchozího nastavení může „tweety“ uživatele vidět kdokoliv, dokonce i když nemá svůj Twitterový účet. Zapnutím funkce chráněných „tweetů“ jsou veškeré tweety viditelné pouze pro ty, kteří uživatele sledují. Další základní možností zabezpečení je zákaz přijímání zpráv od uživatelů, kteří uživatele nesledují. [67]

2.6. Ask.fm

Cílem sociální sítě Ask.fm je pomoci uživatelům v konverzaci pomocí otázek a odpovědí. Tato poměrně nová sociální síť vznikla v červnu roku 2010. Přestože Ask.fm vznikla v Lotyšsku, hlavní sídlo má v Irsku. Tato sociální síť si získala mnoho obdivovatelů, ale i kritiků po celém světě. V současné době má přibližně 150 miliónů aktivních uživatelů měsíčně a je dostupná ve 150 zemích po celém světě. Populární je tato sociální síť především díky možné anonymitě dotazů, které uživatelé mohou pokládat jinému uživateli. Právě anonymnost dotazů byla často zneužívána a vedla často ke kyberšikaně, která může vést i k sebevraždě. [69, 70]

V srpnu roku 2014 byla tato kontroverzní sociální síť odkoupena společností InterActiveCorp (IAC), která se zavázala zvýšit zabezpečení a ochranu soukromí uživatelů. Chce toho docílit díky investicím do lepšího detekčního systému a rozšířením týmu pracovníků, kteří budou schopni vyřešit stížnosti ohledně bezpečnosti a soukromí během 24 hodin. IAC najala také specialistku na ochranu dětí na internetu Annie Mullins, a také Catherine Davis Teitelbaum, která dříve pracovala na bezpečnostní politice firmy Yahoo.com. [71]

Důsledkem těchto změn byla nová bezpečností politika Ask.fm, která má za úkol chránit děti před kyberšikanou. Uživatel má nově možnost si zvolit, zda bude přijímat anonymní otázky, které jsou však kontrolovány detekčním systémem a v případě nalezení nevhodného obsahu řešeny pracovníky IAC. Další novinkou v zabezpečení je nové Centrum bezpečnosti, které poskytuje uživatelům mnoho nástrojů a tipů ohledně zabezpečení. [70, 71]

2.7. Další sociální sítě

V konkurenci Facebooku je velice těžké se prosadit, proto jsou vytvářeny sociální sítě, které mají specializaci na určitou oblast. Mezi takové sociální sítě patří například LinkedIn, který spojuje odborníky v určitém oboru a pomáhá jim tak k navázání profesionální spolupráce. Často je využíván společnostmi pro získání nových pracovníků. Pro jednotlivce je to skvělá příležitost pro vytvoření svého profesního profilu, který se podobá životopisu a který může pomoci uživateli získat zajímavé pracovní místo v oboru. [72]

Další specifickou sociální sítí je Foursquare. Tato sociální síť pomáhá uživatelům najít oblíbená místa, která si jejich komunita oblíbila. Foursquare poskytuje také funkci check-in, která umožní uživateli sdělit polohu v reálném čase. Tato funkce se stala velice populární a v roce 2014 byla pro tuto funkci vytvořena samostatná aplikace Swarm, která obsahuje herní prvky, díky kterým je pro uživatele zajímavější. [73]

Dalším specifickým odvětvím sociálních sítí jsou seznamky. Mezi takové sociální sítě patří především Badoo a Tinder. Cíl těchto aplikací je vytvořit pro uživatele příjemné prostředí, ve kterém se mohou seznámit s ostatními uživateli. Potenciálním rizikem tohoto typu sociální sítí může být kyberstalking a kybergrooming. [74, 75]

Posledním zmíněným typem jsou herní sociální sítě. Nejvýznamnějším zástupcem v tomto odvětví sociálních sítí je Twitch.tv. Tato sociální síť umožňuje svým uživatelům odebírat a sledovat oblíbené hry nebo hráče v živém vysílání nebo záznamech. [76]

2.8. Shrnutí

Existuje obrovské množství sociálních sítí s mnoha různými zaměřeními a využitími. Nejvýznamnějšími sociálními sítěmi jsou Facebook a YouTube, které byly v této kapitole rozebrány podrobně. Velká část popisu těchto sociálních sítí byla zaměřena na hrozby, které plynou z používání sociálních sítí, a možné postupy a nástroje, které slouží k prevenci a odstranění těchto hrozeb. Velmi oblíbenou sociální sítí je také Instagram. Mezi nejkontroverznější sociální sítě se dá bezesporu zařadit Ask.fm. Z těchto důvodů budou právě tyto sociální sítě předmětem výzkumu a navrhovaného řešení.

3. Výzkum

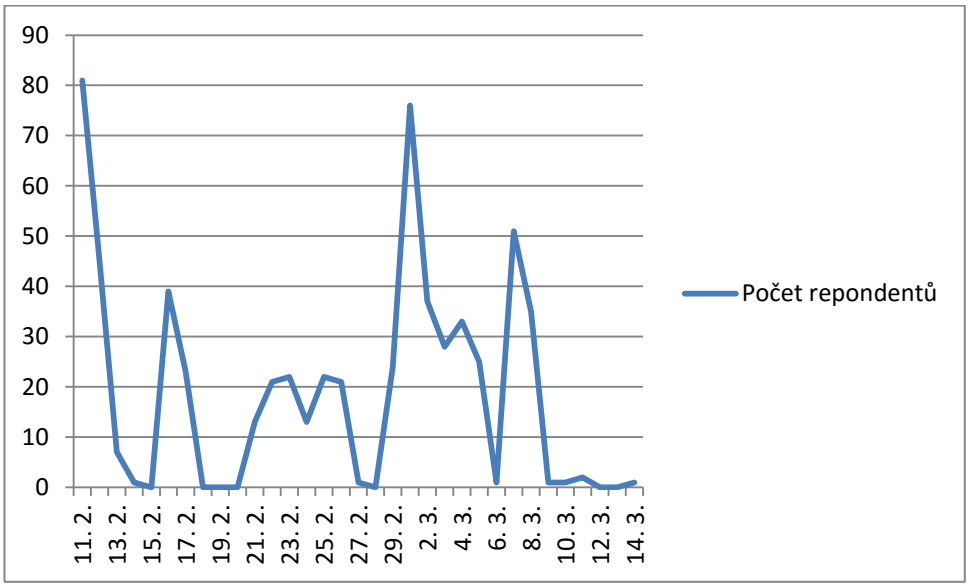
3.1. Metodika výzkumu

Před vytvořením hlavního dotazníku byl vytvořen pilotní dotazník. Jeho hlavním úkolem bylo zjistit, jaké sociální sítě uživatelé ve vybraných školách používají a jak znají pojmy kyberšikana, kyberstalking a kybergrooming. Hlavní dotazník byl přizpůsoben výsledkům z pilotního dotazníku.

3.1.1. Tvorba a šíření dotazníku

Hlavní dotazník obsahuje 30 otázek, které byly vytvořeny na základě poznatků z bakalářské práce, teoretické části diplomové práce a pilotního dotazníku. Otázky byly vytvořeny tak, aby pomohly určit rizikové skupiny respondentů a rizikové jevy, se kterými se respondenti setkávají.

Dotazník byl vypracován pomocí Google formulářů a šířen pomocí metody sněhové koule. Pro šíření dotazníku byli vybráni studenti, kteří odpovídají cílové skupině. Tito studenti byli požádáni o šíření dotazníku s ostatními studenty, kteří splňují podmínky cílové skupiny. Kromě studentů byli osloveni i kantoři, kteří na vybraných školách vyučují a mají možnost dotazník šířit mezi studenty. Oslovení počátečních studentů a kantorů bylo rozděleno do několika vln pro zajištění rovnoměrně rozdělených dat. [77]



Graf 3: Vývoj počtu respondentů v čase

3.1.2. Předzpracování dat

V první fázi byla odstraněna duplicitní data (méně než 0,5 %) a data nesprávně vyplněná (méně než 1 %). V druhé fázi byla odstraněna data, která byla nesmyslná (méně než 1,5 %). Jednalo se například o odpovědi u otázek, které uživatel nepoužívající konkrétní sociální síť nemohl smysluplně zodpovědět. V poslední fázi byla upravena data, která byla zadána špatně, ale vyplýval z nich jasný formát správné odpovědi (méně než 0,5 %). Celkový počet odpovědí 624 byl tak redukován na počet 610.

Pro ulehčení zpracování nasbíraných dat bylo provedeno kódování. Dichotomické proměnné byly zakódovány pomocí nul a jedniček. Chybějícím údajům byla přiřazena hodnota 999. Kódování se provádělo pomocí vnořených IF funkcí v programu Microsoft Excel 2010.

Pro otázku "Kolik přátel máte na Facebooku?" byly vytvořeny skupiny podle počtu přátel pro další analýzu dat. Otázky s možností výběru více než jedné odpovědi byly rozděleny podle jednotlivých možností na samostatné otázky s dichotomickými proměnnými. Aby bylo možné testování určitých hypotéz, pro jednotlivé rozdělené otázky ohledně sdílení byla vytvořena souhrnná proměnná Počet_sdílení, jejíž hodnotou byla suma hodnot rozdělených otázek ohledně sdílení. Obdobným způsobem byla vytvořena proměnná Počet_hrozeb, jejíž hodnota byla sumou hodnot proměnných o lehkém zneužití dat, vážném zneužití dat, kyberstalkingu a kyberšikaně.

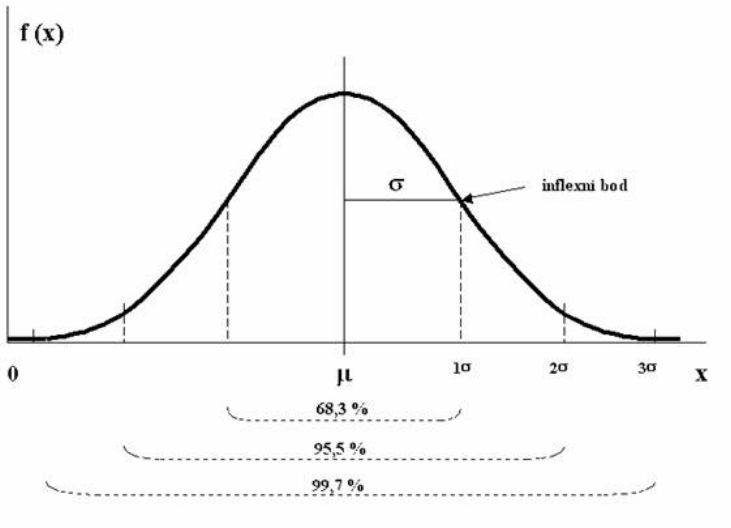
Při předzpracování dat v SPSS byly jednotlivým otázkám přiřazeny správné datové typy, typy proměnných, desetinná místa a hodnota chybějících údajů. Dále byly odstraněny otázky, které byly v MS Excel rozděleny na jednotlivé otázky s nominálními proměnnými. Pro přehlednost byly upraveny názvy otázek, respektive sloupců, se kterými se dále pracovalo.

3.1.3. Statistické metody analýzy dat

Veškeré operace s daty byly prováděny v programu Microsoft Excel 2010 a IBM SPSS Statistics verze 22. Pro základní popsání vzorku byly použity frekvenční tabulky a tabulky četností. Pro analýzu dat byly použity metody testu chí-kvadrátu, Mann-Whitneyův test, korelace a test pro podíl u jednoho výběru. Hladina významnosti α byla stanovena na hodnotu 0,05. Metoda T-testu nebyla použita, protože nebyla potvrzena normalita rozdělení.

Test normality

Normální (Gaussovo) rozdělení je jedním z nejdůležitějších rozdělení spojitých náhodných veličin. Právě normální rozdělení dat je podmínkou pro použití T-testu a dalších parametrických statistických testů. Dvěma hlavními parametry normálního rozdělení je střední hodnota μ a směrodatná odchylka σ. Pro normální rozdělení pak platí, že 68,3 % hodnot se nachází v intervalu <μ - σ, μ + σ>. Dále platí, že 95,5 % se nachází v intervalu <μ - 2σ, μ + 2σ> a 99,7 % se nachází v intervalu <μ - 3σ, μ + 3σ>. [78]



Graf 4: Normální rozdělení [79]

Zjistit, zda se jedná o normální rozdělení, je možné několika způsoby. Prvním způsobem je použití histogramu, P-P grafu nebo Q-Q grafu. Druhým způsobem je použití jednoho z testů pro ověření normality (Kalmogorovův-Smirnovův, Shapirův-Wilkův, Lillieforsův a další). Pro otestování, zda lze rozdělení dat považovat za normální byl použit Shapirův-Wilkův test, který je součástí IBM SPSS Statistics verze 22. Z testu plyne, že ani jedna z proměnných nemá normální rozdělení, proto nelze použít studentův T-test.

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Kolik_přátel_máte_na_Facebooku	,173	574	,000	,927	574	,000
Jaké_heslo_máte_na_Facebooku_nastavené	,326	574	,000	,829	574	,000
Jakou_školu_navštěvujete	,218	574	,000	,800	574	,000
Jak_dlouho_používáte_Facebook	,127	574	,000	,968	574	,000
Kolik_hodin_na_sociálních_sítích	,167	574	,000	,843	574	,000
Z_jakého_důvodu_jste_přestali_používat_sociální_sít	,272	574	,000	,788	574	,000

Tabulka 2: Test normality

Test chí-kvadrát nezávislosti

χ^2 test nezávislosti je založen na porovnání teoretických a empirických četností a vychází z kombinační tabulky. Používá se pro testování nezávislosti proměnných $X_1, X_2, \dots, X_r$ a $Y_1, Y_2, \dots, Y_s$, s, r ≥ 2, kde r je index řádku a s je index sloupce. V kombinační tabulce je pro každé políčko tabulky vypočítána kromě empirické hodnoty také očekávaná hodnota. Pokud se tyto četnosti liší pouze nahodile, platí nulová hypotéza H_0: $\pi_{ij} = \pi_i . \pi_{.j}$ pro všechny dvojice i, j pro i = 1, 2, 3, …, r a j = 1, 2, 3, …, c. V případě nezávislosti obou proměnných nastane shoda obou četností a bude potvrzena alternativní hypotéza H_1: $\pi_{ij} \neq \pi_i . \pi_{.j}$ pro alespoň jednu dvojici i, j pro i = 1, 2, 3, …, r a j = 1, 2, 3, …, c. Významnost neshody empirických a očekávaných četností je měřená χ^2 statistikou a nulová hypotéza je podle výsledné χ^2 statistiky zamítnuta nebo potvrzena podle zvolené hladiny významnosti α. Testové kritérium G χ^2 testu nezávislosti se stupni volnosti df = (r - 1)(c - 1) se vypočítá podle vzorce:

$$G = \sum_{i=1}^{r} \sum_{j=1}^{s} \frac{(n_{ij} - n'_{ij})^2}{n'_{ij}}$$

Kritickou hodnotu $\chi^2_{1-\alpha;k}$ lze získat pomocí funkce CHINV v programu Microsoft Excel 2010. Je určena kvantilem χ^2 rozdělení pro dané stupně volnosti na hladině významnosti α. Podle prvního rozhodovacího pravidla pak platí, že se nulová hypotéza H_0 zamítá na hladině významnosti, pokud $\chi^2 > \chi^2_{1-\alpha;k}$. Pokud platí, že $\chi^2 < \chi^2_{1-\alpha;k}$ H_0 nelze zamítnout. [80]

X/Y	Y_1	Y_2	…	Y_n	$\sum_j$
X_1	n_{11}	n_{12}	⋮	n_{1n}	$n_{1.}$
X_2	n_{21}	n_{22}	⋮	n_{2n}	$n_{2.}$
⋮	⋮	⋮	⋮	⋮	⋮
X_m	n_{m1}	n_{m2}	…	n_{mn}	$n_{m.}$
$\sum_i$	$n_{.1}$	$n_{.2}$	…	$n_{.n}$	n

Tabulka 3: Kontingenční tabulka [81]

Předpokladem pro použití χ^2 testu je, že žádná teoretická četnost nesmí být menší než 1 a zároveň maximálně 20% teoretických četností může obsahovat hodnotu menší než 5. Pokud se jedná o kombinační tabulku 2x2 mělo by být n > 40. Pokud je n < 20 by měl být použit Fisherův test a pro 20 < n < 40 je třeba upravit kritérium χ^2 podle Yatesovy rovnice. [80]

V programu IBM SPSS Statistics verze 22 jsou kontingenční tabulky přístupné pod položkou Analyze ⟶ Descriptive Statistics ⟶ Crosstabs. Uživatel zvolí, jaké proměnné umístí do řádků a do sloupců a stisknutím tlačítka Statistics… zobrazí dialogové okno, kde má možnost vybrat několik různých statistik. Zaškrtnutím položky Chi-square uživatel vybere test χ^2.

Binomický test

Binomický test je test pro podíl u jednoho výběru, který testuje rovnost parametru π s binomickým rozdělením a předem dané hodnoty π_0. Nulová hypotéza je ve tvaru H_0: $\pi = \pi_0$. Alternativní hypotézy jsou H_1: $\pi \neq \pi_0$, H_1: $\pi > \pi_0$ a H_1: $\pi < \pi_0$. Při testování se používá aproximace na normované normální rozdělení. [82, 83]

V programu IBM SPSS Statistics verze 22 je testována alternativní hypotéza H_1: $\pi > \pi_0$ a test pro podíl u jednoho výběru je přístupný pod položkou Analyze ⟶ Nonparametric Tests ⟶ Legacy Dialogs ⟶ Binomial.... V dialogovém oknu má uživatel možnost zadat hodnotu π_0, která bude testována, a podle které bude vypočítána minimální hladina významnosti, od které se nulová hypotéza H_0 zamítá. [83]

Mann-Whitneyův test

Jak již bylo řečeno, pro některé testy je potřeba, aby data měla normální rozdělení. Pro data, u kterých nelze předpokládat normální rozdělení pravděpodobností, se používají neparametrické testy. Síla neparametrických testů není tak vysoká jako u parametrických testů.

Mann-Whitneyův pořadový test se používá pro porovnání dat, u kterých nelze předpokládat normální rozdělení. Pomocí Mann-Whitneyova testu se porovnávají dva různé výběrové soubory pro hodnocení nepárových pokusů. Testuje se nulová hypotéza, která říká, že obě skupiny vzorků mají stejné rozdělení pravděpodobností. V prvním kroku testu je všem měřením pro $x_1, x_2, x_3, \ldots, x_{n1}$ a pro $y_1, y_2, y_3, \ldots, y_{n2}$ přiřazena pozice podle velikosti vzestupně. Seřazeným hodnotám se říká směsný výběr, který se značí písmenem z a platí pro něj, že $z_1 < z_2 < z_3 < \ldots < z_n$ kde $n = n_1 + n_2$. Všem hodnotám z je přiřazeno pořadí (1, 2, ..., n). Při shodě určitých hodnot je pořadí vypočítáno jako jejich průměr. Výpočet samotné testovací statistiky je pak dán vzorcem $U_A = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_A$, kde R_A je součet všech pořadí hodnot veličiny X a vzorcem $U_B = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_B$, kde R_B je součet všech pořadí hodnot veličiny Y. Menší hodnota U je následně použita jako testové kritérium pro porovnání s kritickou hodnotou Mann-Whitneyova testu pro zvolenou hladinu významnosti α. Nulová hypotéza se zamítá, jestliže $U < U_{(\alpha,n_1,n_2)}$. Jestliže $U > U_{(\alpha,n_1,n_2)}$ nulovou hypotézu nelze zamítnout. [84, 85]

V programu IBM SPSS Statistics verze 22 jsou kontingenční tabulky přístupné pod položkou Analyze ⟶ Nonparametric Tests ⟶ Legacy Dialogs ⟶ 2 Independent Samples....

Korelace

Pro řešení nelineárních závislostí mezi náhodnými proměnnými byl použit Spearmanův koeficient korelace, protože zachycuje kromě lineárních vztahů také rostoucí nebo klesající vztahy mezi proměnnými. Výhodou Spearmanova koeficientu korelace (r) je odolnost vůči odlehlým hodnotám, protože pracuje s pořadím pozorovaných hodnot. Výpočet se provádí pomocí vzorce $r_{sp} = 1 - \frac{6 \sum D_i}{n(n^2-1)}$ kde D_i je rozdíl mezi pořadím hodnot x_i a y_i u korelačních dvojic a n je počet korelačních dvojic. Výsledná hodnota r nabývá hodnot od -1 do 1. Pro hodnotu -1 platí nepřímá nezávislost, pro hodnotu 0 nezávislost a pro hodnotu 1 platí přímá závislost mezi proměnnými. Výsledná hodnota r je pak porovnána s kritickými hodnotami Spearmanova korelačního koeficientu pro zvolené α a dané n. Pokud platí, že $|r_{sp}| > r_{sp(\alpha,n)}$, koeficient pořadové korelace je významný na zvolené hladině významnosti α. Pokud platí, že $|r_{sp}| < r_{sp(\alpha,n)}$, koeficient pořadové korelace na zvolené hladině významnosti α významný není. [86]

3.2. Cílová skupina

Cílovou skupinou byli studenti základních škol, středoškolských gymnázií a středních škol s IT zaměřením v Královéhradeckém kraji. Celkem se výzkumu zúčastnilo 624 studentů z prvního až čtvrtého ročníku výše zmíněných středních škol a z šestého až devátého ročníku základních škol.

3.3. Cíl výzkumu

Hlavním cílem výzkumu bylo poukázat na situaci ohledně zabezpečení sociálních sítí u studentů základních škol, středoškolských gymnázií a středních škol s IT zaměřením. Zkoumány byly především zkušenosti respondentů s různými hrozbami, které jsou pro sociální sítě typické. Mezi hlavní zkoumané hrozby patří zneužití osobních údajů, kyberšikana a kyberstalking.

3.4. Hypotézy

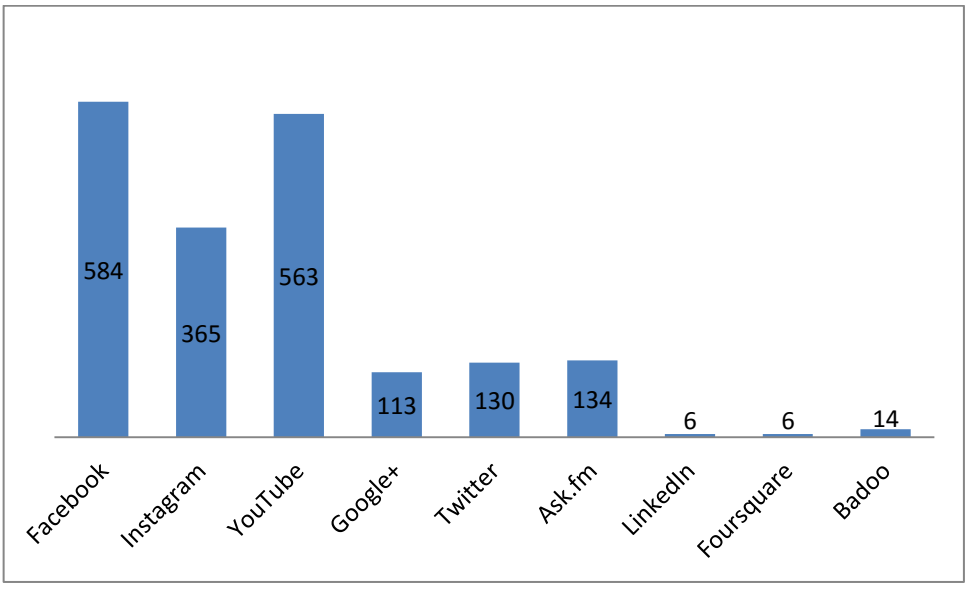
Vzhledem k většímu počtu testovaných hypotéz jsou graficky a tabulkově zobrazeny pouze vybrané hypotézy a statistiky. Důležité údaje a výsledky v ostatních hypotézách jsou interpretovány slovně. Vzhledem k nepovinnému vyplnění u některých otázek a následným filtrům při zpracování mají některé hypotézy rozdílnou velikost zkoumaného vzorku. Vzorek je však vždy vybrán tak, aby byl reprezentativní. Z tohoto důvodu byly vynechány veškeré hypotézy vztahující se ke kybergroomingu.

3.4.1. Popis vzorku

Rozdělení vzorku podle pohlaví je poměrně vyrovnané (338 mužů a 272 žen). Větší počet mužů je zapříčiněn především nepoměrem můžu a žen na středních školách s IT oborem (164 mužů a 26 žen). Respondenti byli rozděleni také podle místa bydliště, kde podle očekávání největší procentuální zastoupení mělo velké město nad 5000 obyvatel. 27,9 % respondentů uvedlo jako své bydliště malé město. Vesnici uvedlo jako své bydliště 29,8 % respondentů.

Šíření dotazníku bylo prováděno tak, aby byl vzorek rovnoměrně rozdělený podle typu školy, kterou respondenti navštěvují, a ročníku, který na dané škole aktuálně studují. Procentuálně tak bylo studentů základních škol 31,8 %, středoškolských gymnázií 37 % a středních škol s IT zaměřením 31,1 %. Počty respondentů v jednotlivých ročnících se lišily pouze nepatrně.

Řešené hypotézy byly přizpůsobeny pro nejpoužívanější sociální sítě, které byly zjištěny pomocí pilotního dotazníku. Výsledky pilotního dotazníku a hlavního dotazníku se v otázce používání různých sociálních sítí neliší, nejpoužívanějšími sociálními sítěmi jsou v obou případech Facebook a YouTube následovaný Instagramem.



Graf 5: Jaké sociální sítě aktivně využíváte?

3.4.2. Závislost na pohlaví

První skupinou hypotéz jsou hypotézy, které testují závislost určitých proměnných na pohlaví. Všechny tři hypotézy jsou řešeny pomocí χ^2 testu nezávislosti.

H_1: Ženy se stávají častěji oběťmi lehkého i vážného zneužití osobních údajů, kyberšikany a kyberstalkingu.

Pro možnost otestování této hypotézy byla vytvořena proměnná Počet_hrozeb, která v sobě zahrnovala lehké a vážné zneužití osobních údajů, kyberšikanu i kyberstalking. Jednotlivé negativní jevy byly zkoumány i samostatně.

Testována byla nulová hypotéza, která říkala, že osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na pohlaví.

		Počet_hrozeb					
		0	1	2	3	4	Total
Pohlaví	Muž	214	84	27	11	2	338
	Žena	141	47	37	29	18	272
Total		355	131	64	40	20	610

Tabulka 4: Kontingenční tabulka H_1

V tabulce číslo 4 je vidět kontingenční tabulka, která je výstupem programu IBM SPSS verze 22. V řádcích tabulky je pohlaví, kterému odpovídají četnosti jednotlivých hodnot proměnné Počet_hrozeb ve sloupcích. Z tabulky lze vyčíst velký rozdíl v prvním sloupci, který říká, že se respondent na sociálních sítích nesetkal s žádnou z testovaných hrozeb. Jelikož byly všechny zahrnuté otázky povinné, počet respondentů je 610. Pro testování této hypotézy byl použit test χ^2 nezávislosti (viz tabulka číslo 5).

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	41,266[a]	4	,000
Likelihood Ratio	43,248	4	,000
Linear-by-Linear Association	31,776	1	,000
N of Valid Cases	610		

Tabulka 5: Test χ^2 nezávislosti H_1

Z tabulky číslo 5 vyplývá, že nulová hypotéza se na hladině $\alpha = 0{,}05$ při čtyřech stupních volnosti zamítá. Přijímá se tak alternativní hypotéza H_1, která říká, že ženy se stávají častěji oběťmi lehkého i vážného zneužití osobních údajů, kyberšikany a kyberstalkingu.

Jak již bylo řečeno, testovány byly i jednotlivé hrozby samostatně a všechny dílčí nulové hypotézy se na hladině $\alpha = 0{,}05$ při čtyřech stupních volnosti zamítají. Signifikance je podle Pearsonova χ^2 testu u lehkého zneužití osobních údajů 0,027, u vážného zneužití osobních údajů 0,016, u kyberšikany a kyberstalkingu je signifikance rovna 0,000.

H_2: Ženy jsou častěji ochotny odsouhlasit přístup k osobním údajům po spuštění aplikace.

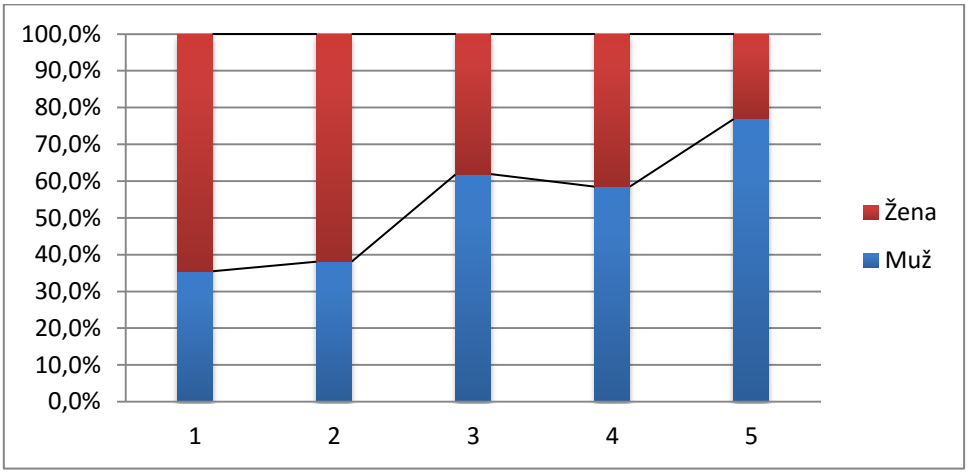
V rámci nepovinné otázky zda jsou respondenti ochotni odsouhlasit přístup k osobním údajům po spuštění aplikace na Facebooku bylo zaznamenáno 13 chybějících hodnot, proto je celkový počet respondentů u této hypotézy 597. Z těchto 597 respondentů bylo ochotno odsouhlasit přístup 56,9 % mužů a 43,1 % žen.

Testována byla nulová hypotéza, která říkala, že odsouhlasení přístupu k osobním údajům po spuštění aplikace není závislé na pohlaví. Nulovou hypotézu nelze zamítnout, protože signifikance Pearsonova χ^2 testu nezávislosti (0,636) je větší než zvolená hladina významnosti $\alpha = 0,05$ při jednom stupni volnosti.

H_3: Muži mají nastavené silnější heslo než ženy.

Otázka zabývající se sílou hesla byla nepovinná, proto je celkový počet snížen o chybějící hodnoty na 590. Testována byla nulová hypotéza, která říkala, že síla hesla není závislá na pohlaví. Nulová hypotéza byla zamítnuta na základě Pearsonova χ^2 testu na hladině významnosti $\alpha = 0,05$ při čtyřech stupních volnosti. Výsledná signifikance měla hodnotu 0,000.

Na ose x grafu číslo 6 jsou hodnoty 1, 2, 3, 4, 5, které reprezentují jednotlivé odpovědi v dotazníku a jsou seřazeny podle síly hesla. Hodnota 1 je tedy nejméně silné heslo (krátké zapamatovatelné) a hodnota 5 je nejsilnější heslo (Složené z písmen, číslic a speciálních znaků). Z grafu je evidentní rostoucí tendence procentuálního zastoupení mužů v závislosti na rostoucí síle hesla.



Graf 6: Závislost síly hesla na pohlaví

3.4.3. Vliv sdílení na bezpečnost

Tato skupina dvou hypotéz zkoumá vliv sdílení osobních údajů na bezpečnost uživatelů. Pro potvrzení nebo vyvrácení daných hypotéz byl použit χ^2 test nezávislosti a korelace.

H_4: Oběťmi zneužití dat a kyberšikany a kyberstalkingu jsou lidé, kteří sdílejí více informací.

Stejně jako u H_1 byla použita proměnná Počet_hrozeb, která zahrnuje všechny výše zmíněné hrozby. Všechny zahrnuté otázky použité pro testování hypotézy jsou povinné, proto je celkový počet zkoumaných respondentů 610. Testována byla nulová hypotéza, která říkala, že osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na množství sdílených informací. Na základě Pearsonova χ^2 testu nelze nulovou hypotézu na hladině významnosti $\alpha = 0,05$ při df = 28 stupních volnosti zamítnout. Výsledná signifikance měla hodnotu 0,356.

Otestovány byly i jednotlivé hrozby samostatně a všechny dílčí nulové hypotézy nelze na hladině $\alpha = 0,05$ při čtyřech stupních volnosti zamítnout, jelikož je signifikance podle Pearsonova χ^2 testu u všech testů větší než 0,05.

H_5: Čím větší město respondenti uvedli jako bydliště, tím více osobních údajů sdílí.

Testována byla nulová hypotéza H_0: Osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na množství sdílených informací. Aby tato hypotéza mohla být otestována, bylo potřeba vytvořit proměnnou Počet_sdílení, která byla sumou jednotlivých položek, které respondent sdílel. Obě otázky zahrnuté v této hypotéze jsou povinné, proto je celkový počet respondentů 610.

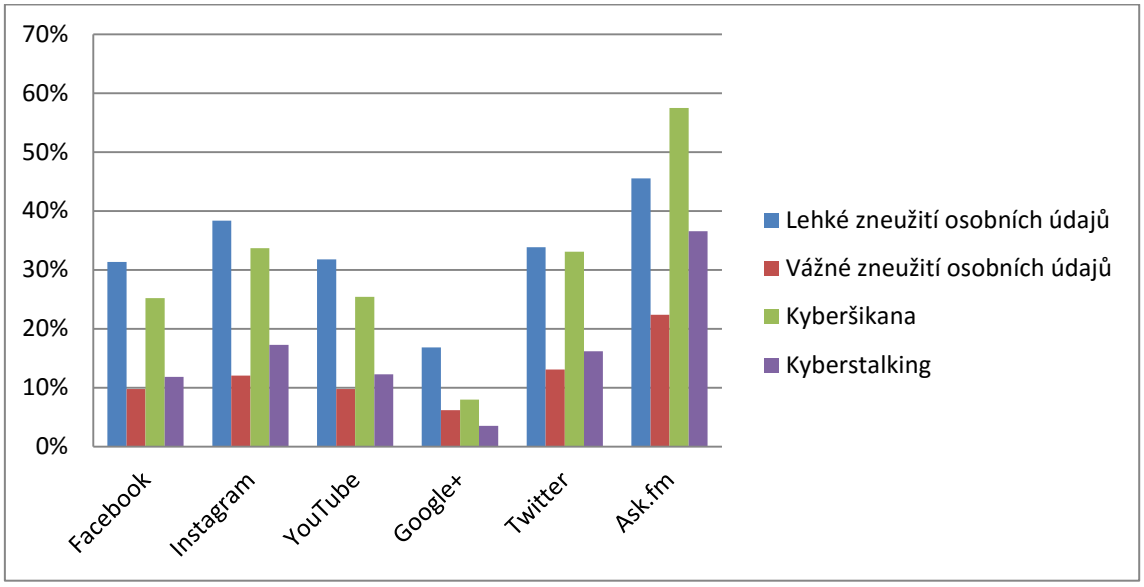
Pro otestování této hypotézy byla použita korelace. Z tabulky číslo 6 vyplývá, že Spearmanův korelační koeficient je roven 0,034 a signifikance 0,313. Nulovou hypotézu proto nelze na hladině $\alpha = 0,05$ zamítnout. Z toho vyplývá, že nelze prokázat závislost mezi místem bydliště a množstvím sdílených údajů.

			Počet_sdílení	Místo_Vašeho_bydliště?
Kendall's tau_b	Počet_sdílení	Correlation Coefficient	1,000	,034
		Sig. (2-tailed)		,313
		N	610	610
	Místo_Vašeho_bydliště?	Correlation Coefficient	,034	1,000
		Sig. (2-tailed)	,313	
		N	610	610
Spearman's rho	Počet_sdílení	Correlation Coefficient	1,000	,041
		Sig. (2-tailed)		,317
		N	610	610
	Místo_Vašeho_bydliště?	Correlation Coefficient	,041	1,000
		Sig. (2-tailed)	,317	
		N	610	610

Tabulka 6: Korelace H_5

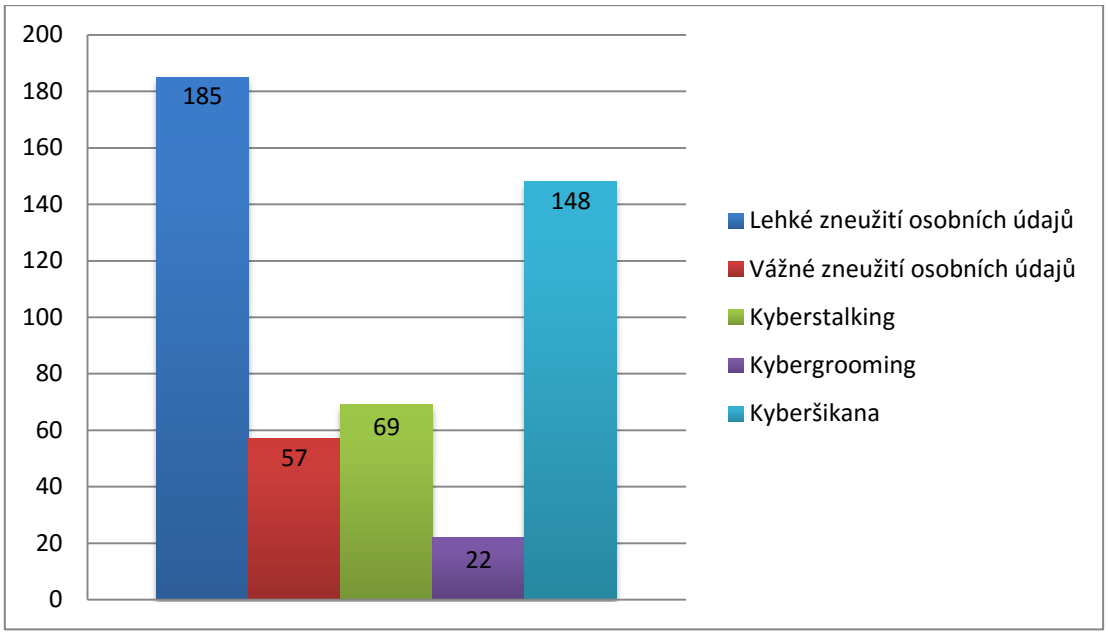
3.4.4. Faktory ovlivňující míru zneužití osobních údajů, kyberšikany a kyberstalkingu

V této podkapitole je testována skupina hypotéz, které souvisejí s lehkým a vážným zneužitím osobních údajů, kyberšikanou a kyberstalkingem. Zahrnuta měla být i hrozba kybergroomingu, nicméně počet lidí, kteří se s touto hrozbou setkali, byl pouze 23, proto by pro některé otázky byl tento vzorek nereprezentativní. Vzhledem k získaným znalostem při tvorbě bakalářské práce na obdobné téma a teoretické části diplomové práce jsou určité hypotézy zaměřeny na sociální síť Ask.fm, která je známá velkým výskytem kyberšikany (viz graf číslo 7).



Graf 7: Procentuální zastoupení hrozeb u jednotlivých sociálních sítí

Kvůli závažnosti tohoto tématu a velkému výskytu jednotlivých hrozeb mezi respondenty je tato skupina hypotéz nejpočetnější. Například s kyberšikanou se setkalo 148 respondentů, což je téměř čtvrtina všech dotázaných (viz graf číslo 8).



Graf 8: Počet výskytů jednotlivých hrozeb u respondentů

H_6: Uživatelé sociální sítě Ask.fm se častěji stávají oběťmi kyberšikany.

Všechny otázky použité pro testování hypotézy jsou povinné, proto je celkový počet zkoumaných respondentů 610. Testována byla nulová hypotéza, která říkala, že osobní zkušenost s kyberšikanou není závislá na používání sociální sítě Ask.fm. Z výstupů IBM SPSS bylo zjištěno, že se s kyberšikanou setkala více než polovina respondentů, kteří používají Ask.fm.

Na základě Pearsonova χ^2 testu se nulová hypotéza na hladině významnosti $\alpha = 0{,}05$ při jednom stupni volnosti zamítá. Výsledná signifikance měla hodnotu 0,000 a lze tak přijmou alternativní hypotézu H_6.

H_7: Uživatelé sociální sítě Ask.fm se častěji stávají oběťmi kyberstalkingu.

Tato hypotéza se liší od předchozí pouze v použití jiné proměnné, nicméně kyberstalking je odlišnou a velmi nebezpečnou hrozbou, proto je dobré udělat hypotézu samostatně a otestovat její správnost. Testována byla nulová hypotéza, která říkala, že osobní zkušenost s kyberstalkingem není závislá na používání sociální sítě Ask.fm. Výsledky u této hypotézy jsou ještě více jednoznačné, protože z celkového počtu 69 respondentů, kteří se setkali s kyberstalkingem, jich 49 používá Ask.fm, což je 71 %.

Výsledek je evidentní, byl však proveden Pearsonův χ^2 testu nezávislosti, podle kterého se nulová hypotéza na hladině významnosti $\alpha = 0{,}05$ při jednom stupni volnosti zamítá. Výsledná signifikance měla hodnotu 0,000 a lze tak přijmou alternativní hypotézu H_7.

H_8: Uživatelé se slabým heslem se častěji stávají oběťmi zneužití osobních údajů, kyberšikany a kyberstalkingu.

Testována je nulová hypotéza H_0: Osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na síle hesla. Pro otestování této hypotézy byla použita proměnná Počet_hrozeb a otázka ohledně nastavení hesla na Facebooku. Jelikož právě otázka ohledně nastavení hesla není povinná, obsahuje hypotéza některé chybějící hodnoty. Celkový počet respondentů zahrnutých v testování hypotézy je tak 590.

Na základě Pearsonova χ^2 testu se nulová hypotéza na hladině významnosti $\alpha = 0{,}05$ při 16 stupních volnosti zamítá. Výsledná signifikance měla hodnotu 0,000.

Otestovány byly opět i jednotlivé hrozby samostatně pomocí Mann-Whitneyova neparametrického testu, který určil, že se všechny dílčí nulové hypotézy na hladině $\alpha = 0{,}05$ při 16 stupních volnosti zamítají, jelikož výsledná signifikance Mann-Whitneyova testu je u všech testů 0,000.

H_9: Studenti, kteří používají rozdílná skupinová oprávnění, se stávají méně často oběťmi kyberšikany, kyberstalkingu a zneužití osobních údajů.

Testována je nulová hypotéza H_0: Osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na používání rozdílných skupinových oprávnění na Facebooku. Pro otestování této hypotézy byla použita proměnná Počet_hrozeb a otázka o používání rozdílného skupinového oprávnění na Facebooku, která není povinná, proto obsahuje hypotéza některé chybějící hodnoty. Celkový počet respondentů zahrnutých v testování hypotézy je 602.

Na základě Pearsonova χ^2 testu nelze nulovou hypotézu na hladině významnosti $\alpha = 0{,}05$ při čtyřech stupních volnosti zamítnout, protože výsledná signifikance měla hodnotu 0,136.

Otestovány byly i jednotlivé hrozby samostatně a všechny dílčí nulové hypotézy nelze na hladině $\alpha = 0{,}05$ při čtyřech stupních volnosti zamítnout, jelikož je signifikance u všech testů větší než 0,05.

H_{10}: Uživatelé s více přáteli jsou častěji oběťmi kyberšikany, kyberstalkingu a zneužití osobních údajů.

Testována je nulová hypotéza H_0: Osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na množství přátel na Facebooku. Pro otestování této hypotézy byla použita proměnná Počet_hrozeb a proměnná s vytvořenými kategoriemi podle počtu přátel na Facebooku. Jelikož uvedení počtu přátel na Facebooku nebyla povinná otázka, obsahuje hypotéza některé chybějící hodnoty. Celkový počet respondentů zahrnutých v testování hypotézy je 594.

Na základě Pearsonova χ^2 testu nezávislosti se nulová hypotéza na hladině významnosti α = 0,05 při 20 stupních volnosti zamítá. Výsledná signifikance měla hodnotu 0,000.

Otestovány byly opět i jednotlivé hrozby samostatně pomocí Mann-Whitneyova neparametrického testu, který určil, že se všechny dílčí nulové hypotézy na hladině α = 0,05 při 20 stupních volnosti zamítají, jelikož výsledná signifikance Mann-Whitneyova testu je u všech testů 0,000.

H_{11}: Uživatelé, kteří používají sociální sítě častěji, se stávají více oběťmi kyberšikany a kyberstalkingu.

Testována je nulová hypotéza H_0: Osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na množství hodin strávených na sociálních sítích denně. Pro otestování této hypotézy byla použita proměnná Počet_hrozeb a otázka ohledně denní porce času stráveného na sociálních sítích. Všechny zahrnuté otázky jsou povinné, proto je počet zkoumaných respondentů 610.

V tomto případě se jedná o hypotézu, která pro své potvrzení potřebuje dva testy korelací. Jeden pro kyberšikanu a druhý pro kyberstalking. Spearmanův korelační koeficient je v případě kyberšikany roven 0,344 a signifikance 0,000. Pro kyberstalking vyšel korelační koeficient 0,220 a signifikance 0,000. Jelikož je korelační koeficient v obou případech kladný, platí přímá závislost proměnných. Nulová hypotéza se proto na hladině α = 0,05 zamítá. Platí tedy, že čím častěji uživatelé používají sociální sítě, tím více se stávají oběťmi kyberšikany a kyberstalkingu.

H_{12}: Uživatelé, kteří přidávají svá vlastní videa, se častěji stávají oběťmi kyberšikany, kyberstalkingu a zneužití osobních údajů.

Testována je nulová hypotéza H_0: Osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na přidávání vlastních videí na YouTube. Pro otestování této hypotézy byla použita proměnná Počet_hrozeb a otázka, která zjišťovala, zda uživatelé přidávají svá vlastní videa na YouTube. Otázka vztahující se k sociální sítí YouTube nebyla povinná, proto je celkový zkoumaný počet respondentů 595.

Na základě Pearsonova χ^2 testu se nulová hypotéza na hladině významnosti α = 0,05 při čtyřech stupních volnosti zamítá. Výsledná signifikance měla hodnotu 0,005. Platí tedy alternativní hypotéza H_{12}.

Testovány byly i jednotlivé hrozby samostatně. Hypotézy o kyberšikaně, kyberstalkingu a lehkém zneužití osobních údajů se na hladině $\alpha = 0{,}05$ při čtyřech stupních volnosti zamítají. Hypotézu o vážném zneužití osobních údajů nelze na hladině $\alpha = 0{,}05$ při čtyřech stupních volnosti zamítnout. Signifikance je podle Pearsonova χ^2 testu u lehkého zneužití osobních údajů 0,010, u vážného zneužití osobních údajů 0,177, u kyberšikany 0,000 a u kyberstalkingu je signifikance rovna 0,013.

3.4.5. Znalosti respondentů

V další skupině hypotéz jsou testovány především znalosti respondentů. Získané výsledky budou užitečné pro navržení možného řešení vylepšení prevence negativních jevů na sociálních sítích.

Z kombinace dvou otázek o soukromí Instagramu vyplývá, že 40,3 % uživatelů Instagramu si myslí, že mají svůj profil nastavený jako soukromý, přesto že neměnili nastavení soukromí. Jelikož je soukromý profil na Instagramu defaultně vypnutý, uživatelé kteří nastavení soukromí neměnili, mají Instagramový profil veřejný.

Kombinací dalších dvou otázek zabývajících se přístupem k osobním údajům v rámci aplikací na Facebooku bylo zjištěno, že 56,4 % respondentů netuší, že spuštěním aplikace dávají Facebooku automaticky svolení k přístupu k jejich osobním informacím. Jedná se o respondenty, kteří uvedli, že používají aplikace na Facebooku a zároveň uvedli, že nejsou ochotni odsouhlasit přístup aplikací k jejich osobním údajům. Spuštěním aplikace však uživatel automaticky dává aplikaci přístup k jeho osobním údajům. Je tak vidět, stejně jako v předchozí popisné statistice, velká neinformovanost respondentů.

H_{13}: Nadpoloviční většina respondentů ví, že registrací na Facebooku potvrzují souhlas s Podmínkami použití a zároveň potvrzuje přečtení dokumentu Zásady používání dat, včetně části Použití souborů cookie.

Testována je nulová hypotéza H_0: Polovina respondentů ví, že registrací na Facebooku potvrzují souhlas s Podmínkami použití a zároveň potvrzuje přečtení dokumentu Zásady používání dat, včetně části Použití souborů cookie. Pro otestování této hypotézy byl použit binomický test pro jeden výběr. Zkoumaná otázka není povinná, proto se v ní vyskytují chybějící hodnoty. Celkový počet respondentů, se kterým se pracuje, je 601.

Nulová hypotéza se pro testovanou hodnotu 0,5 zamítá na hladině významnosti $\alpha = 0{,}05$. Hodnota výsledné signifikance byla 0,000 (viz tabulka číslo 7).

		Category	N	Observed Prop.	Test Prop.	Exact Sig. (2-tailed)
Víte_že_registrací_na_Facebooku_potvrzujete_souhlas	Group 1	0	196	,33	,50	,000
	Group 2	1	405	,67		
	Total		601	1,00		

Tabulka 7: Binomický test H_{13}

Alternativní hypotéza H_{13} se přijímá, jelikož bylo zjištěno, že 67 % respondentů ví, že registrací na Facebooku potvrzují souhlas s Podmínkami použití a zároveň potvrzuje přečtení dokumentu Zásady používání dat, včetně části Použití souborů cookie.

H_{14}: Více než polovina respondentů by i přes rizika zneužití dat nadále používala sociální sítě.

Testována je nulová hypotéza H_0: Polovina respondentů by i přes rizika zneužití dat nadále používala sociální sítě. Pro otestování této hypotézy byl použit stejně jako v předchozím případě binomický test pro jeden výběr. Celkový počet respondentů je 610, protože zkoumaná otázka byla v dotazníku povinná.

Nulová hypotéza se pro testovanou hodnotu 0,5 zamítá na hladině významnosti $\alpha = 0{,}05$. Hodnota výsledné signifikance byla 0,000. Alternativní hypotéza H_{14} se zamítá, jelikož bylo zjištěno, že 76 % respondentů by bylo ochotno přestat používat sociální sítě, kdyby ohrožovaly jejich soukromí. Přijímá se alternativní hypotéza, která říká, že přes rizika zneužití dat by nadále používala sociální sítě méně než polovina respondentů.

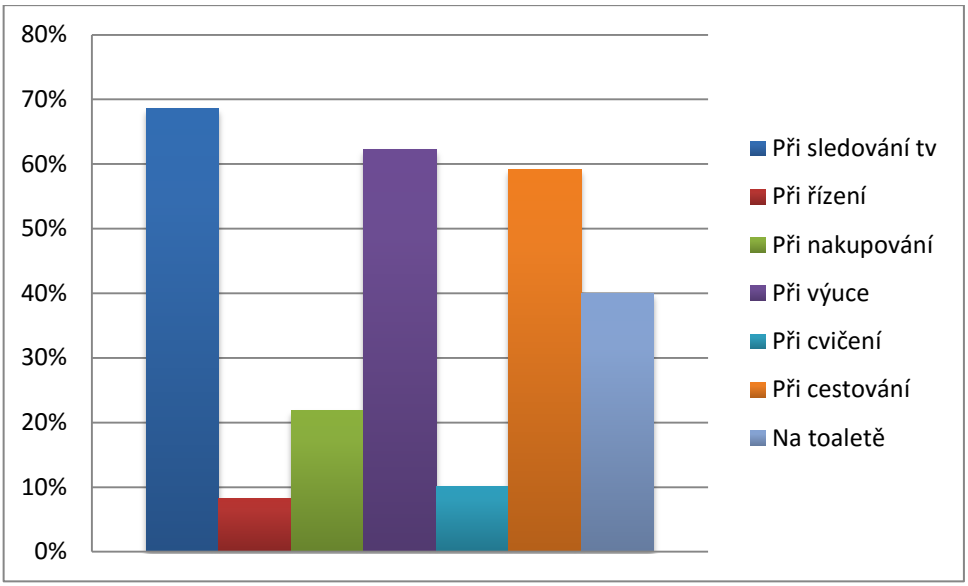
3.4.6. Chování respondentů

V poslední skupině hypotéz jsou ty hypotézy, které zkoumají chování studentů a má význam je testovat z hlediska bezpečnosti a návrhu možného řešení.

H_{15}: Více než polovina studentů používá sociální sítě při hodinách ve škole.

Testována je nulová hypotéza H_0: Polovina studentů používá sociální sítě při hodinách ve škole. Pro otestování této hypotézy byl použit binomický test pro jeden výběr. Celkový počet respondentů je 610, protože zkoumaná otázka byla v dotazníku povinná.

Nulová hypotéza se pro testovanou hodnotu 0,5 zamítá na hladině významnosti $\alpha = 0{,}05$. Hodnota výsledné signifikance byla 0,000. Přijímá se alternativní hypotéza H_{15}, protože sociální sítě při výuce používá 62 % respondentů (viz graf číslo 9)



Graf 9: Při jakých aktivitách používáte sociální sítě?

Z grafu číslo 9 lze vyčíst, že nejnižší procento má používání sociálních sítí při řízení. Tato statistika je však zkreslena faktem, že velké procento respondentů nevlastní řidičský průkaz, a tak nemohou používat sociální sítě při řízení. Aby byla tato statistika relevantní, bylo by potřeba zahrnout otázku, která by zjistila, zda uživatel vlastní řidičský průkaz. Formulace otázky byla inspirována výzkumem serveru creditdonkey.com. [87]

H_{16}: Uživatelé základních škol používají Ask.fm nejvíce.

Testována je nulová hypotéza H_0: Používání sociální sítě Ask.fm nezávisí na škole, kterou respondent navštěvuje. Pro otestování této hypotézy byla použita proměnná Používám_Ask.fm a otázka, která zjišťovala typ školy, kterou respondent studuje. Všechny zahrnuté otázky byly v dotazníku povinné, proto je počet zkoumaných respondentů u této hypotézy 610.

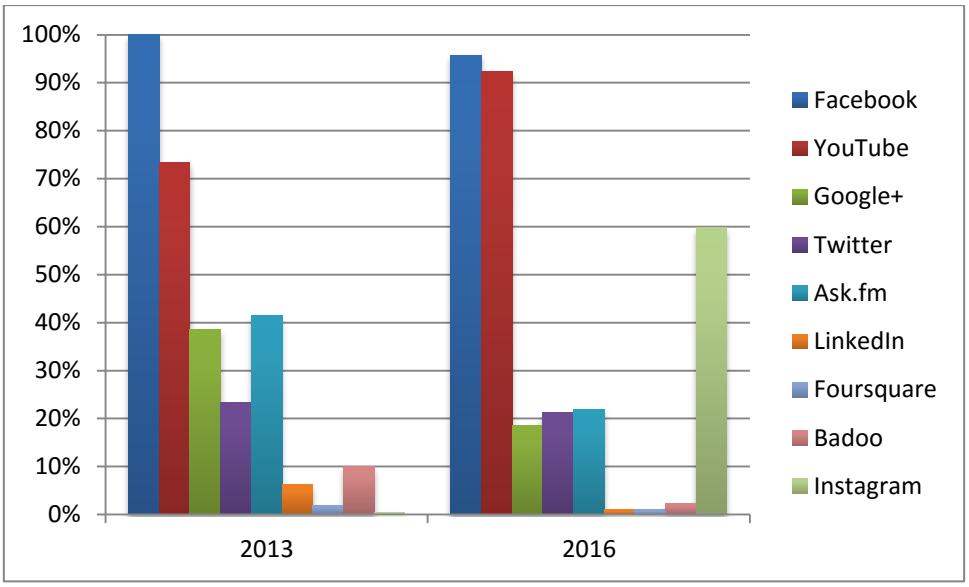
Na základě Pearsonova χ^2 testu se nulová hypotéza na hladině významnosti $\alpha = 0{,}05$ při dvou stupních volnosti zamítá. Výsledná signifikance měla hodnotu 0,000. Platí tedy alternativní hypotéza H_{16}, která říká, že studenti základních škol používají sociální síť Ask.fm více, než studenti z jiných typů škol.

3.5. Porovnání údajů s rokem 2013

Pro porovnání výsledků respondentů středoškolských gymnázií s výsledky z roku 2013 byla data vyfiltrována tak, aby obsahovala pouze odpovědi žáků středoškolských gymnázií. Pro porovnání byly vybrány pouze vybrané statistiky. Pro popis vzorku byly použity frekvenční tabulky, které potvrdily porovnatelné rozdělení respondentů.

3.5.1. Popularita sociálních sítí

V roce 2013 bylo v předvýzkumu zjištěno, že Facebook používá všech 30 dotázaných respondentů. Proto byl hlavní dotazník zaměřen na uživatele Facebooku, a proto je v grafu číslo 10 zastoupení Facebooku u respondentů v roce 2013 100 %. Dále protože nebyla sociální síť Instagram tolik známá, nebyla v roce 2013 zahrnuta jako jedna ze zaškrtávacích odpovědí. Uživatelé však měli možnost Instagram uvést do textového pole pod položkou Jiné.

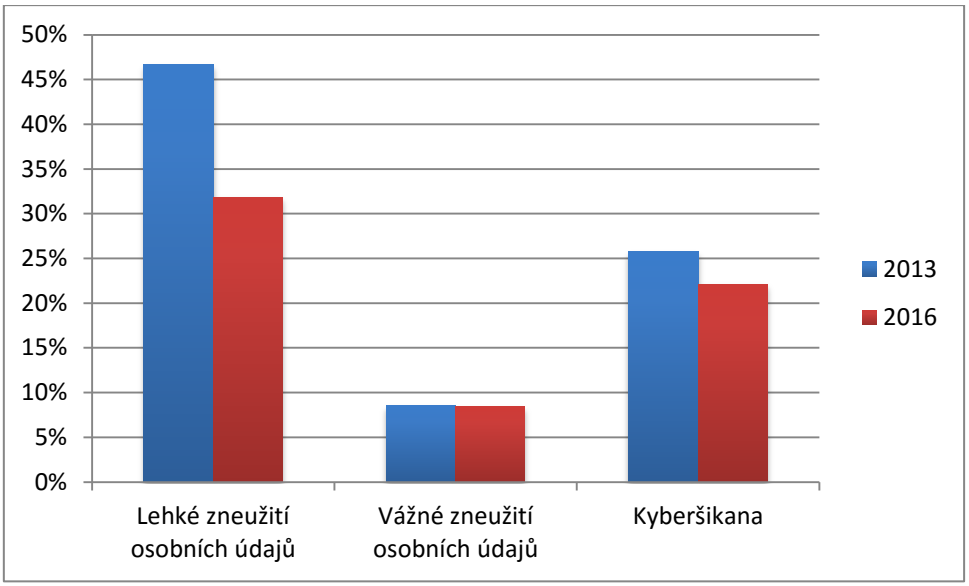


Graf 10: Srovnání používání sociálních sítí v letech 2013 a 2016

Z grafu lze vidět znatelné rozdíly v používání určitých sociálních sítí. Oproti roku 2013 uživatelé více používají především YouTube a Instagram. Naopak úbytek uživatelů je vidět především u sociální sítě Google+ a Ask.fm. U sociální sítě Ask.fm by odliv uživatelů mohl být způsoben častým výskytem kyberšikany.

3.5.2. Hrozby na sociálních sítích

Další porovnávanou oblastí jsou osobní zkušenosti respondentů s negativními jevy na sociálních sítích. V roce 2013 byly zkoumány hrozby lehkého a vážného zneužití osobních údajů a kyberšikana. Pro porovnání tedy nebudou zahrnuty hrozby kyberstalkingu a kybergroomingu, které byly zahrnuty v této diplomové práci.



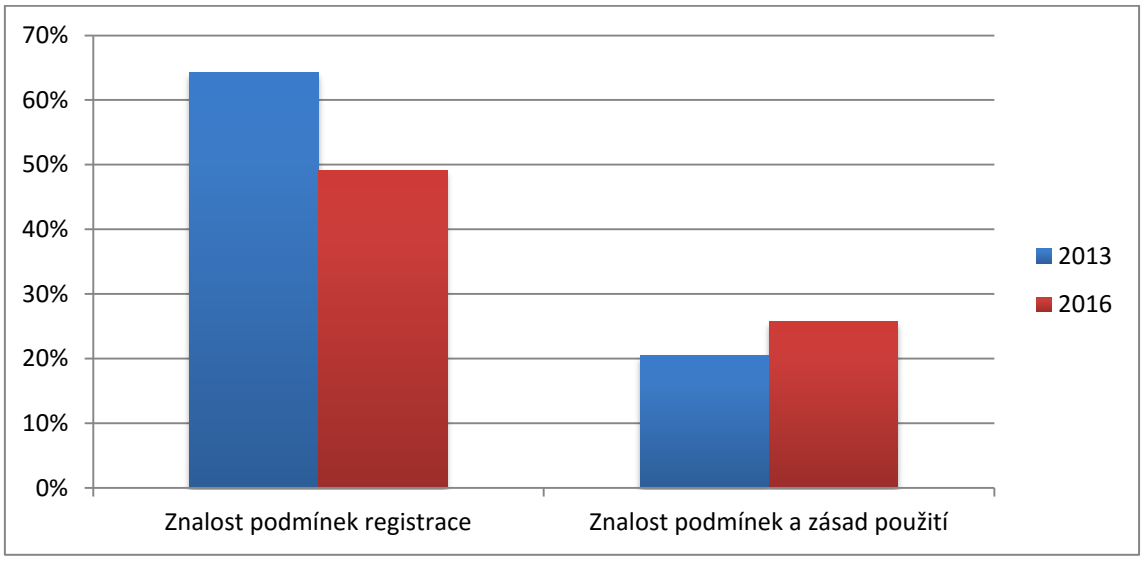
Graf 11: Srovnání výskytu negativních jevů na sociálních sítích v letech 2013 a 2016

Na grafu číslo 11 lze vidět, že situace u studentů středoškolských gymnázií v královéhradeckém kraji se zlepšila, nicméně výskyt negativních jevů je stále poměrně vysoký. Snížil se především výskyt lehkého zneužití osobních údajů. S kyberšikanou se nadále setkává více než 20% dotázaných respondentů.

Stejně jako v roce 2013 byla na hladině významnosti $\alpha = 0{,}05$ potvrzena hypotéza, která říkala, že se uživatelé sociální sítě Ask.fm častěji stávají oběťmi kyberšikany. V roce 2013 se s kyberšikanou setkalo 47 uživatelů, kteří používají Ask.fm. V roce 2016 to bylo 23 uživatelů.

3.5.3. Znalosti respondentů

Jako poslední budou porovnány znalosti respondentů. Porovnány mohly být pouze otázky vztahující se k Facebooku, jelikož ostatní otázky v roce 2013 nebyly zahrnuty.



Graf 12: Srovnání znalostí respondentů v letech 2013 a 2016

Na grafu číslo 12 je vidět, že méně respondentů v roce 2016 ví, že registrací na Facebooku potvrzují souhlas s Podmínkami použití a zároveň potvrzují přečtení dokumentu Zásady používání dat, včetně části Použití souborů cookie. Naopak přibližně o 5 % respondentů více v roce 2016 tvrdí, že se seznámili s obsahem Podmínek použití a Zásad použití dat na Facebooku.

Dále byla porovnána hypotéza, která říká, že nadpoloviční většina respondentů netuší, že spuštěním aplikace dávají Facebooku automaticky svolení k přístupu k jejich osobním informacím. V roce 2013 byla tato hypotéza přijata na hladině významnosti $\alpha = 0{,}05$. Podíl respondentů, kteří nevěděli, že spuštěním aplikace dávají Facebooku svolení k přístupu k jejich osobním informacím byl 70,4 %. V roce 2016 to bylo 53,3 % a nulová hypotéza nemohla být na hladině významnosti $\alpha = 0{,}05$ zamítnuta, proto nebyla výše zmíněná alternativní hypotéza prokázána.

3.6. Shrnutí výsledků

Dosažené výsledky byly zaměřeny na studenty základních škol, středoškolských gymnázií a středních škol se zaměřením na IT v Královéhradeckém kraji. Výsledný vzorek, se kterým se pracovalo, byl 610 respondentů, což lze považovat za reprezentativní vzorek. K zjištění kvality a vyváženosti vzorku byly zpracovány popisné statistiky, které zjistily, že jsou respondenti rovnoměrně rozděleni podle školy a ročníku, který navštěvují. Dále byli uživatelé poměrně rovnoměrně rozděleni podle pohlaví a bydliště. Testované hypotézy byly vytvořeny tak, aby pomohly určit rizikové oblasti na sociálních sítích.

Hypotézy byly rozděleny do skupin podle zkoumaných oblastí. V první skupině byla testována závislost pohlaví na určité oblasti zabezpečení. Z výsledků vyplývá, že ženy se stávají častěji oběťmi lehkého i vážného zneužití osobních údajů, kyberšikany a kyberstalkingu. Dále bylo potvrzeno, že muži mají nastavené silnější heslo než ženy. Naopak závislost pohlaví na odsouhlasení přístupu k osobním údajům po spuštění aplikace na Facebooku nebyla prokázána.

V druhé skupině byl testován vliv sdílení osobních informací na sociálních sítích na bezpečnost. U obou testovaných hypotéz této skupiny nešlo zamítnout nulovou hypotézu. Bylo tak zjištěno, že osobní zkušenost se zneužitím osobních údajů, kyberšikanou a kyberstalkingem není závislá na množství sdílených informací. Na základě druhé hypotézy nebylo prokázáno, že množství sdílených informací závisí na velikosti města, které respondenti uvedli jako své bydliště.

Třetí skupina byla skupinou s nejvíce hypotézami, jelikož se zabývala faktory ovlivňující míru zneužití osobních údajů, kyberšikany a kyberstalkingu. Tato skupina hypotéz poskytla informace, které budou důležité při tvorbě určitých doporučení pro zvýšení bezpečnosti na sociálních sítích. Bylo zjištěno, že uživatelé sociální sítě Ask.fm se stávají častěji oběťmi kyberšikany a kyberstalkingu. Dále bylo potvrzeno, že uživatelé se slabým heslem se častěji stávají oběťmi zneužití osobních údajů, kyberšikany a kyberstalkingu. Naopak hypotéza, která říkala, že studenti, kteří používají rozdílná skupinová oprávnění, se stávají méně často oběťmi kyberšikany, kyberstalkingu a zneužití osobních údajů byla zamítnuta. Potvrzena byla přímá závislost osobní zkušenosti se zneužitím osobních údajů, kyberšikanou a kyberstalkingem na množství přátel na Facebooku. Dále bylo zjištěno, že uživatelé, kteří používají sociální sítě častěji, se stávají více oběťmi kyberšikany a kyberstalkingu. V poslední hypotéze bylo zjištěno, že uživatelé, kteří přidávají svá vlastní videa, se častěji stávají oběťmi kyberšikany, kyberstalkingu a zneužití osobních údajů. Pokud by se však tato hypotéza rozdělila na čtyři samostatné hypotézy podle jednotlivých hrozeb, bylo by zjištěno, že osobní zkušenost s vážným zneužitím osobních údajů není závislá na přidávání vlastních videí na YouTube. Pro ostatní hrozby byla závislost potvrzena.

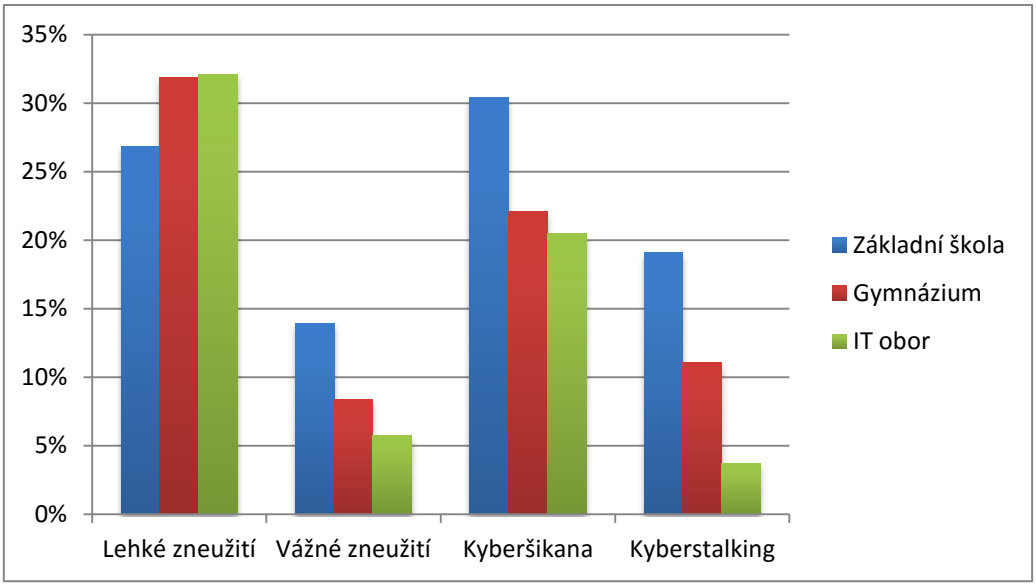
V další skupině byly testovány znalosti respondentů v rámci zabezpečení sociálních sítí. Bylo zjištěno, že 56,4 % většina respondentů netuší, že spuštěním aplikace dávají Facebooku automaticky svolení k přístupu k jejich osobním informacím. Dále si 40,3 % respondentů myslí, že profil na Instagramu mají soukromý, přestože však neměnili nastavení soukromí, soukromý ho mít nemohou. Dále bylo potvrzeno, že nadpoloviční většina respondentů ví, že registrací na Facebooku potvrzuje souhlas s Podmínkami použití a zároveň potvrzuje přečtení dokumentu Zásady používání dat, včetně části Použití souborů cookie. Dále by více než polovina respondentů byla ochotna přestat používat sociální sítě, kdyby ohrožovaly jejich soukromí. Tato skupina posloužila jako ukázka nedostatečné informovanosti respondentů v rámci základních nastavení zabezpečení na sociálních sítích.

V poslední skupině hypotéz bylo potvrzeno, že více než polovina studentů používá sociální sítě při hodinách ve škole. Dále také, že studenti základních škol používají sociální síť Ask.fm více než respondenti ostatních typů škol. Především druhá hypotéza je zásadní, protože bylo potvrzeno, že uživatelé sociální sítě Ask.fm se stávají častěji oběťmi kyberšikany a kyberstalkingu.

Dále byly srovnány vybrané aktuální výsledky s výsledky z bakalářské práce, která byla vytvořena v roce 2013. Jelikož byla bakalářská práce zaměřena pouze na studenty středoškolských gymnázií v Královéhradeckém kraji, byla data z aktuálního průzkumu vyfiltrována tak, aby obsahovala pouze studenty středoškolských gymnázií. Oproti roku 2013 respondenti více používají sociální sítě YouTube a Instagram. Naopak sociální sítě Google+ a Ask.fm používají respondenti o něco méně. Dále v porovnání s rokem 2013 výrazně kleslo u studentů lehké zneužití dat a mírně klesl výskyt kyberšikany. Obě hrozby však jsou nadále v poměrně velkém procentuálním zastoupení.

4. Návrh řešení

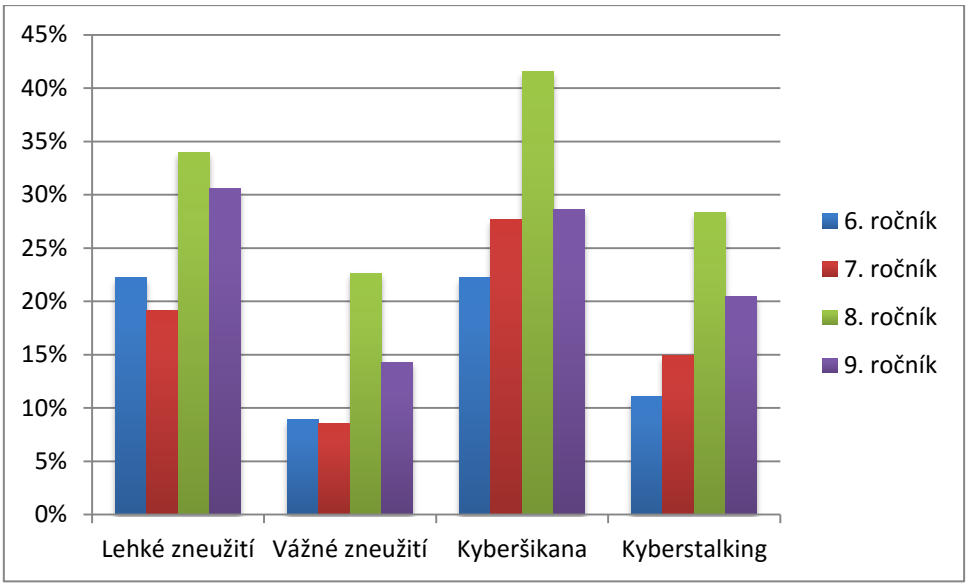
Výsledky výzkumu poukázaly na časté výskyty rizikových jevů na sociálních sítích u studentů základních škol, středoškolských gymnázií a středních škol se zaměřením na IT. Na grafu číslo 13 je vidět, že respondenti ze základních škol se nejčastěji setkávají se všemi hrozbami kromě lehkého zneužití osobních údajů.



Graf 13: Procentuální výskyt hrozeb u jednotlivých typů škol

Navrhované řešení proto bude cíleno především na studenty základních škol. Je vhodné, aby nezletilí žáci, kteří používají sociální sítě, věděli, jaká rizika na ně na sociálních sítích čekají a jak se proti nim bránit.

V dnešní době je naprosto běžné, že žáci na druhém stupni používají jednu nebo více sociálních sítí. Na grafu číslo 14 je vidět, že se s rizikovými jevy nejčastěji setkávají žáci osmých a devátých tříd. Nicméně negativní zkušenost s některou z hrozeb má i velké procento žáků šestých ročníků, proto by bylo vhodné informovat žáky o rizikových jevech na sociálních sítích už v šestém ročníku.



Graf 14: Procentuální výskyt hrozeb u jednotlivých ročníků základní školy

Informování žáků o problémech by mohlo probíhat v rámci zvaných přednášek expertů na bezpečnost na sociálních sítích. Další možností by bylo zahrnutí internetové bezpečnosti do předmětu informatiky, nebo zavedení nového předmětu s názvem například „Internetová bezpečnost“, který by připravil žáky na hrozby nejen sociálních sítí, ale internetu obecně.

Jako podpůrné prostředky pro zlepšení povědomí o bezpečnosti by ve třídách, nebo na chodbách základní školy mohly být vyvěšeny infografiky informující o různých hrozbách se stručným návodem jak těmto hrozbám čelit. Vhodné infografiky na základní rizikové jevy na sociálních sítích a internetu jsou zpracovány v rámci projektu e-bezpečí, který získal cenu evropské prevence za rok 2015. [88]

Kromě velice výstižných a graficky dobře zpracovaných materiálů projekt e-bezpečí poskytuje online poradnu, interaktivní DVD a online kurzy zdarma. Právě z tohoto projektu by měli učitelé čerpat, aby mohli předat žákům užitečné informace, které jim pomohou se ochránit před rizikovými jevy na internetu. Projekt e-bezpečí obsahuje akreditované školení pro učitele v rámci DVPP (Další vzdělávání pedagogických pracovníků) a pořádá výše zmíněné semináře o bezpečnosti pro žáky druhého stupně základních škol. Délka takového semináře je 2 x 45 minut a cena tohoto semináře je 2940 Kč plus cestovné a je kvalitní formou prevence rizikových jevů na sociálních sítích. [89]

Závěr

Sociální sítě jsou v současné době každodenním nástrojem v životě velkého počtu především mladých lidí. V teoretické části této práce byly představeny nejpoužívanější sociální sítě, jejich funkcionalita a využití. Zvláštní pozornost byla věnována hrozbám a zabezpečení na jednotlivých sociálních sítích. Je důležité, aby si lidé uvědomovali, že na sociálních sítích existuje mnoho hrozeb, které mohou mít katastrofální důsledky, a že je třeba se proti těmto hrozbám bránit.

Hrozbami a bezpečnostními opatřeními se zabývá praktická část této diplomové práce. Zkoumána byla situace na základních školách, středoškolských gymnáziích a středních školy se zaměřením na IT v Královéhradeckém kraji. Pomocí vhodných kontaktů a šíření dotazníků pomocí metody sněhové koule se podařilo nasbírat kvalitní reprezentativní vzorek respondentů.

Podle nabytých poznatků z teoretické části a osobních zkušeností byly vytvořeny hypotézy, které byly analyzovány a zjistily bezpečnostní situaci na sociálních sítích u respondentů. Bylo zjištěno, že se velká část respondentů setkala s negativními jevy jako je zneužití osobních údajů, kyberšikana a kyberstalking. Dále bylo potvrzeno, že uživatelé sociální sítě Ask.fm se často stávají oběťmi kyberšikany a kyberstalkingu. Testovány byly i znalosti respondentů v oblasti zabezpečení sociálních sítí. Na základě výsledků ze zkoumaných hypotéz bylo navrženo možné řešení pro zlepšení bezpečnostní situace u respondentů.

Diplomová práce je v určitém směru pokračováním a rozšířením bakalářské práce z roku 2013, která zkoumala bezpečnostní situaci na sociálních sítích u respondentů navštěvujících středoškolská gymnázia v Královéhradeckém kraji. Proto byly z aktuálních dat vyfiltrovány respondenti, kteří navštěvují středoškolské gymnázium a byly porovnány výsledky. Z výsledků kromě jiného plyne, že ubylo lehkého zneužití osobních údajů a mírně ubylo výskytů kyberšikany, nicméně výskytů je stále mnoho, proto byl vytvořen seznam doporučení pro prevenci negativních jevů na sociálních sítích.

Pro zlepšení situace ohledně bezpečnosti byla vytvořena určitá doporučení. Navrhované řešení by počítalo se školením pedagogů druhého stupně základních škol, kteří by nabyté znalosti uplatňovali v hodinách informatiky, nebo nově zavedených hodinách internetové bezpečnosti. Dále by škola v rámci projektu e-bezpečí měla zajistit pro žáky semináře vedené experty. Jako podpůrné materiály by ve školách měly být vyvěšeny infografiky informující o hrozbách internetu.

Diplomová práce již zabírá poměrně rozsáhlou oblast, nicméně není možné výsledky vztáhnout na celou populaci České republiky. Jako další zajímavou oblast zkoumání bych proto považoval rozšíření výzkumu na základní školy v celé České republice.

Seznam použité literatury

1. HAVLOVÁ, Jaroslava. sociální síť. In: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha: Národní knihovna ČR, 2003 [cit. 2016-01-08]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000015947&local_base=KTD
2. Sociální sítě. *Aktuálně.cz* [online]. 3. 7. 2011 [cit. 2016-01-08]. Dostupné z: http://wiki.aktualne.centrum.cz/datarama/socialni-site/
3. Web 2.0 Definition from PC Magazine Encyclopedia. PCMAG [online]. 2016, [cit. 2016-01-11]. Dostupné z: http://www.pcmag.com/encyclopedia/term/56219/web-2-0
4. ZUCKERBERG, Mark. *Facebook* [online]. 2004 [cit. 2016-01-15]. Dostupné z: https://www.facebook.com
5. GOOGLE. *Google+* [online]. 2013 [cit. 2016-01-15]. Dostupné z: https://plus.google.com/
6. Statistics - YouTube. *YouTube* [online]. 2016 [cit. 2016-01-15]. Dostupné z: https://www.youtube.com/yt/press/statistics.html
7. About Twitter. Twitter [online]. [cit. 2016-01-15]. Dostupné z: https://about.twitter.com/
8. O nás | LinkedIn. LinkedIn [online]. [cit. 2016-01-15]. Dostupné z: https://www.linkedin.com/about-us
9. About Us | About.Ask.fm. Ask.fm [online]. [cit. 2016-01-15]. Dostupné z: http://about.ask.fm/about/
10. Instagram [online]. 2016 [cit. 2016-01-15]. Dostupné z: https://www.instagram.com/
11. ŠKOPEK, Pavel. Foursquare vám nabídne cestovní tipy od přátel. Mobilenet.cz [online]. 2016 [cit. 2016-01-15]. Dostupné z: https://mobilenet.cz/clanky/foursquare-vam-nabidne-cestovni-tipy-od-pratel-29326
12. BUREŠOVÁ, Kamila. České firmy zaostávají ve využívání sociálních sítí. Statistika&My - měsíčník Českého statistického úřadu [online]. 2015 [cit. 2016-01-15]. Dostupné z: http://www.statistikaamy.cz/2015/09/ceske-firmy-zaostavaji-ve-vyuzivani-socialnich-siti/
13. České firmy se vrhly na sociální sítě, už je jich tam čtvrtina. Technologie a komunikace - E15.cz / e-svět[online]. [cit. 2016-01-15]. Dostupné z: http://e-svet.e15.cz/internet/ceske-firmy-se-vrhly-na-socialni-site-uz-je-jich-tam-ctvrtina-1265243

14. Duolingo [online]. 2016 [cit. 2016-01-15]. Dostupné z: https://www.duolingo.com/
15. Rizika sociálních sítí. Jak na Internet [online]. [cit. 2016-01-16]. Dostupné z: http://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/
16. Company Info. Facebook Newsroom [online]. [cit. 2016-01-16]. Dostupné z: http://newsroom.fb.com/company-info/
17. ZUCKERBERG, Mark. *Centrum nápovědy služby Facebook* [online]. 2004 [cit. 2016-01-17]. Dostupné z: https://www.facebook.com/help
18. BELLIS, Mary. Who Invented Facebook?: The history behind the number one social media network Facebook. *About.com: Do more.* [online]. [cit. 2016-01-17]. Dostupné z: http://inventors.about.com/od/fstartinventions/a/Facebook.htm
19. The Social Network. *ČSFD.cz: Česko-Slovenská filmová databáze* [online]. [cit. 2016-01-17]. Dostupné z: http://www.csfd.cz/film/262711-the-social-network/
20. Infografika: Klíčové momenty v historii Facebooku (česky). *Facebook magazín: FaceMag.cz* [online]. 18. 12. 2011 [cit. 2016-01-17]. Dostupné z: http://www.facemag.cz/infografika-klicove-momenty-v-historii-facebooku-cesky/
21. 10 let s Facebookem. První kulaté narozeniny oslavil s miliardou lidí. *Facebook magazín | FaceMag.cz* [online]. 2014 [cit. 2016-01-17]. Dostupné z: http://facemag.cz/facebook-slavi-desate-vyroci-podivejte-se-na-jeho-historii/
22. HOLANOVÁ, Tereza. Facebook vstoupil na burzu. Po naději přišlo zklamání. Aktuálně.cz [online]. 2012 [cit. 2016-01-28]. Dostupné z: http://zpravy.aktualne.cz/ekonomika/svetova-ekonomika/facebook-vstoupil-na-burzu-po-nadeji-prislo-zklamani/r~i:article:745491/
23. Internet.org od Facebooku. Internet.org od Facebooku [online]. [cit. 2016-01-17]. Dostupné z: https://www.internet.org/about?locale=cs_CZ
24. Exploring the software behind Facebook, the worlds largest site | Pingdom Royal. Pingdom Royal | We Love The Internet [online]. [cit. 2016-01-17]. Dostupné z: http://royal.pingdom.com/2010/06/18/the-software-behind-facebook/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+RoyalPingdom+(Royal+Pingdom)
25. ZHAO, Haiping. HipHop for PHP: Move Fast - Facebook pro vývojáře. Vývojáři společnosti Facebook - Facebook pro vývojáře [online]. [cit. 2016-01-17]. Dostupné z: https://developers.facebook.com/blog/post/2010/02/02/hiphop-for-php--move-fast/

26. JIANG, Changhao. BigPipe: Pipelining web pages for high performance. Facebook [online]. [cit. 2016-01-17]. Dostupné z: https://www.facebook.com/notes/facebook-engineering/bigpipe-pipelining-web-pages-for-high-performance/389414033919/
27. Facebook Media - Tips for Using Facebook Live. Facebook [online]. [cit. 2016-01-29]. Dostupné z: https://www.facebook.com/facebookmedia/best-practices/live
28. Messenger – Aplikace pro Android ve službě Google Play. Google Play [online]. [cit. 2016-02-15]. Dostupné z: https://play.google.com/store/apps/details?id=com.facebook.orca
29. AYCOCK, John. Spyware and Adware. Springer Science & Business Media, 2010.
30. Facebook je pro piráty zlatý důl. Novinky.cz - nejčtenější zprávy na českém internetu [online]. 2014 [cit. 2016-02-18]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/340002-facebook-je-pro-piraty-zlaty-dul.html
31. FOGIE, Seth, et al. XSS Attacks: Cross Site Scripting Exploits and Defense. Syngress, 2011. KALLAS, Priit. Facebook Cheat Sheet: Sizes and Dimensions. DreamGrow Digital - Social media marketing [online]. 4. 5. 2011 [cit. 2013-04-17]. Dostupné z: http://www.dreamgrow.com/facebook-cheat-sheet-sizes-and-dimensions/
32. ČERNÁ, Alena, et al. Kyberšikana: Průvodce novým fenoménem. Grada Publishing, as, 2013.
33. České děti a Facebook 2015. Projekt E-bezpečí [online]. 2015 [cit. 2016-02-18]. Dostupné z: http://www.e-bezpeci.cz/facebook2015/
34. BOCIJ, Paul. Cyberstalking: Harassment in the Internet age and how to protect your family. Greenwood Publishing Group, 2004.
35. WACHS, Sebastian; WOLF, Karsten D.; PAN, Ching-Ching. Cybergrooming: Risk factors, coping strategies and associations with cyberbullying.Psicothema, 2012, 24.4: 628-633.
36. MITCHELL, Kimberly J., et al. Prevalence and characteristics of youth sexting: A national study. Pediatrics, 2012, 129.1: 13-20.
37. HOLLAND, Norman. The internet regression. Psychoanalytic Studies e-journal, 1996.
38. Zásady používání dat. Facebook [online]. [cit. 2016-04-19]. Dostupné z: https://www.facebook.com/about/privacy
39. Organization Information. *Safe Harbor* [online]. [cit. 2016-04-19]. Dostupné z: https://safeharbor.export.gov/companyinfo.aspx?id=28012

40. TRUSTe Feedback and Resolution System. *Submit a Report - Watchdog* [online]. [cit. 2016-04-19]. Dostupné z: https://feedback-form.truste.com/watchdog/request

41. Zásady komunity. *Facebook* [online]. [cit. 2016-04-19]. Dostupné z: https://www.facebook.com/communitystandards/

42. The Facebook Anti-Virus Marketplace. In: *Facebook* [online]. 2012 [cit. 2016-04-19]. Dostupné z: https://www.facebook.com/notes/facebook-security/the-facebook-anti-virus-marketplace/10150672849230766

43. Zapojte se do boje proti šikaně. *Facebook* [online]. [cit. 2016-04-19]. Dostupné z: https://www.facebook.com/safety/bullying/

44. Securing Email Communications from Facebook. In: *Facebook* [online]. 2015 [cit. 2016-04-19]. Dostupné z: https://www.facebook.com/notes/protect-the-graph/securing-email-communications-from-facebook/1611941762379302/

45. SENGUPTA, Somini; PERLROTH, Nicole; WORTHAM, Jenna. Behind Instagram's Success, Networking the Old Way. The New York Times. San Francisco, California, USA Retrieved March, 2012, 11: 2013.

46. Instagram. Google Play [online]. [cit. 2016-04-21]. Dostupné z: https://play.google.com/store/apps/details?id=com.instagram.android

47. Centrum nápovědy Instagramu. *Instagram* [online]. [cit. 2016-04-19]. Dostupné z: https://help.instagram.com/

48. VOJTĚCH, Petr. Instagram končí se čtvercovým formátem. *Mobilenet.cz* [online]. 2015 [cit. 2016-04-19]. Dostupné z: https://mobilenet.cz/clanky/instagram-konci-se-ctvercovym-formatem-28008

49. SHEZI, Lungelo. MORE THAN 80 MILLION PHOTOS ARE SHARED ON INSTAGRAM DAILY. In: *Htxt.africa*[online]. 2015 [cit. 2016-04-19]. Dostupné z: http://www.htxt.co.za/2015/09/23/more-than-80-million-photos-are-shared-on-instagram-daily/

50. YouTube overtakes Facebook as the web's biggest social network. Brafton [online]. 2014 [cit. 2016-04-21]. Dostupné z: http://www.brafton.com/news/youtube-overtakes-facebook-webs-biggest-social-network/

51. Google buys YouTube for $1.65 billion. In: *NBC News* [online]. 2013 [cit. 2016-04-19]. Dostupné z: http://www.nbcnews.com/id/15196982/ns/business-us_business/t/google-buys-youtube-billion/#.VxaVBzCLTIV

52. O YouTube. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://www.youtube.com/yt/about/cs/

53. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://www.youtube.com/

54. Nápověda YouTube. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://support.google.com/youtube/?hl=cs#topic=4355266

55. TestTube. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://www.youtube.com/testtube

56. MANDLE, Chris. Forbes names PewDiePie as highest-earning YouTuber with annual income reaching $12m. *The Independent* [online]. 2015 [cit. 2016-04-19]. Dostupné z: http://www.independent.co.uk/news/people/forbes-names-pewdiepie-as-highest-earning-youtuber-with-annual-income-reaching-12m-a6695536.html

57. Reklamy Google. *Google* [online]. [cit. 2016-04-19]. Dostupné z: https://www.google.cz/ads/

58. Hranice platby - Nápověda AdSense. *Google* [online]. [cit. 2016-04-19]. Dostupné z: https://support.google.com/adsense/answer/1709871

59. Základní informace o nástroji YouTube Analytics - Nápověda YouTube. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://support.google.com/youtube/answer/1714323?hl=cs

60. Centrum autorských práv YouTube. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://www.youtube.com/yt/copyright/cs/

61. Poctivé využití (fair use). *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://www.youtube.com/yt/copyright/cs/fair-use.html#yt-copyright-four-factors

62. Pokyny služby YouTube k ochraně osobních údajů. *YouTube* [online]. [cit. 2016-04-19]. Dostupné z: https://www.youtube.com/t/privacy_guidelines

63. Zásady ochrany osobních údajů – Ochrana soukromí a smluvní podmínky. *Google* [online]. [cit. 2016-04-19]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/

64. KARCH, Marziah. What Is Google+. *About Tech* [online]. 2015 [cit. 2016-04-21]. Dostupné z: http://google.about.com/od/p/g/Google-plus.htm

65. Hangouts Google. *Google+* [online]. [cit. 2016-04-19]. Dostupné z: https://hangouts.google.com/

66. Společnost | About. *Twitter* [online]. [cit. 2016-04-19]. Dostupné z: https://about.twitter.com/cs/company

67. *Twitter* [online]. [cit. 2016-04-19]. Dostupné z: https://twitter.com/

68. KWAK, Haewoon, et al. What is Twitter, a social network or a news media?. In:Proceedings of the 19th international conference on World wide web. ACM, 2010. p. 591-600.

69. KENINS, Laura. Latvian Web site at center of cyber-bullying inquiry. News from Latvia, Estonia & Lithuania - The Baltic Times [online]. 14. 11. 2012 [cit. 2013-04-17]. Dostupné z: http://www.baltictimes.com/news/articles/32099/

70. *Ask.fm* [online]. [cit. 2016-04-19]. Dostupné z: https://www.ask.fm/

71. MILLER, Joe. Ask.fm bought by Ask.com and Tinder owner. *BBC* [online]. 2014 [cit. 2016-04-19]. Dostupné z: http://www.bbc.com/news/technology-28776254

72. *LinkedIn* [online]. [cit. 2016-04-19]. Dostupné z: https://www.linkedin.com/

73. About. *Foursquare* [online]. [cit. 2016-04-19]. Dostupné z: https://foursquare.com/about

74. *Poznejte nové lidi na Badoo, Seznamujte se, Chatujte, Flirtujte* [online]. [cit. 2016-04-19]. Dostupné z: https://badoo.com/cs/

75. *Tinder* [online]. [cit. 2016-04-19]. Dostupné z: https://www.gotinder.com/

76. About - Twitch. *Twitch* [online]. [cit. 2016-04-19]. Dostupné z: https://www.twitch.tv/p/about

77. BALTAR, Fabiola; BRUNET, Ignasi. Social research 2.0: virtual snowball sampling method using Facebook. internet Research, 2012, 22.1: 57-74

78. Rovnoměrné a normální rozložení četnosti. *Matematika.cz* [online]. 2014 [cit. 2016-04-19]. Dostupné z: http://www.matematika.cz/rovnomerne-normalni-rozlozeni

79. Pravděpodobnostní rozdělení spojité náhodné veličiny pro základní soubory. *Multimediální pomůcky na VFU* [online]. [cit. 2016-04-19]. Dostupné z: http://cit.vfu.cz/statpotr/POTR/Teorie/Predn2/rozdelZS.htm

80. SKALSKÁ, Hana. Aplikovaná statistika. Vyd. 1. Hradec Králové: Gaudeamus, 2013. ISBN 978-80-7435-320-8.

81. *SlidePlayer - Nahrávejte a Sdílejte své PowerPoint prezentace* [online]. [cit. 2016-04-19]. Dostupné z: http://images.slideplayer.cz/8/2285649/slides/slide_17.jpg

82. Matematická biologie učebnice: Binomický test. *Matematická biologie učebnice* [online]. [cit. 2016-04-19]. Dostupné z: http://portal.matematickabiologie.cz/index.php?pg=zaklady-informatiky-pro-biology--databazove-systemy-v-biomedicine--analyticke-a-statisticke-funkce-sql--statisticke-funkce--binomicky-test

83. Hlavní druhy pravděpodobnostních výběrů. *IAstat - INTERAKTIVNÍ UČEBNICE STATISTIKY* [online]. [cit. 2016-04-19]. Dostupné z: http://iastat.vse.cz/kategorie.htm

84. GraphPad Statistics Guide. *Graphpad.com* [online]. [cit. 2016-04-19]. Dostupné z: http://www.graphpad.com/guides/prism/6/statistics/index.htm?how_the_mann-whitney_test_works.htm

85. Mann-Whitney. *Multimediální pomůcky na VFU* [online]. [cit. 2016-04-19]. Dostupné z: http://cit.vfu.cz/statpotr/POTR/Teorie/Predn4/MannWhit.htm

86. Spearmanův korelační koeficient. *Matematická biologie učebnice* [online]. [cit. 2016-04-19]. Dostupné z: http://portal.matematickabiologie.cz/index.php?pg=aplikovana-analyza-klinickych-a-biologickych-dat--analyza-a-management-dat-pro-zdravotnicke-obory--zaklady-korelacni-analyzy--spearmanuv-korelacni-koeficient

87. Survey: Social Media Usage Statistics. *CreditDonkey* [online]. [cit. 2016-04-19]. Dostupné z: https://www.creditdonkey.com/social-media-usage-statistics.html

88. Materiály pro podporu vyuky. *Projekt E-bezpečí* [online]. [cit. 2016-04-19]. Dostupné z: http://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

89. *Projekt E-bezpečí* [online]. [cit. 2016-04-19]. Dostupné z: http://www.e-bezpeci.cz/

Seznam obrázků

Seznam tabulek

Seznam grafů

Přílohy

Příloha 1: Pilotní dotazník

Pilotní studie - sociální sítě

Tento dotazník je anonymní a pouze pro účely Diplomové práce. Za vyplnění předem moc děkuji.

*Povinné pole

Jaké sociální sítě aktivně využíváte? *

- [ ] Facebook
- [ ] Google+
- [ ] Youtube
- [ ] Twitter
- [ ] LinkedIn
- [ ] Instagram
- [ ] Badoo
- [ ] Tinder
- [ ] Ask.fm
- [ ] Jiné:

Jakou školu navštěvujete? *

- ○ Základní školu - 2. stupeň
- ○ Střední školu - gymnázium
- ○ Střední školu - obor IT

Znáte pojem kyberšikana? *

- ○ Ano
- ○ Ne

Znáte pojem kyberstalking? *

- ○ Ano
- ○ Ne

Znáte pojem kybergrooming? *

- ○ Ano
- ○ Ne

Příloha 2: Hlavní dotazník

Hlavní výzkum - Zabezpečení sociálních sítí

Tento dotazník je anonymní a slouží pouze k účelům Diplomové práce. Za vyplnění předem moc děkuji.

*Povinné pole

Jaké je Vaše pohlaví? *

- ○ Muž
- ○ Žena

Jakou školu navštěvujete? *

- ○ Základní
- ○ Střední - gymnázium
- ○ Střední - IT obor

V jakém jste ročníku? *

- ○ 6. třída ZŠ/1. ročník SŠ
- ○ 7. třída ZŠ/2. ročník SŠ
- ○ 8. třída ZŠ/3. ročník SŠ
- ○ 9. třída ZŠ/4. ročník SŠ

Místo Vašeho bydliště? *

- ○ Vesnice (do 1000 obyvatel)
- ○ Malé město (1001 - 5000 obyvatel)
- ○ Velké město (nad 5000 obyvatel)

Jak dlouho používáte Facebook?
Odpověď vyplňte jako celé číslo. (pokud používáte Facebook 3 roky, vyplňte "3")

Vaše odpověď

Kolik hodin denně strávíte na sociálních sítích? *
Odpověď vyplňte jako celé číslo. (pokud používáte sociální sítě 4 hodiny denně, vyplňte "4", pokud jste online nonstop vyplňte "24")

Vaše odpověď

Stali jste se obětí lehkého zneužití Vašich osobních údajů? *
Například neschválené zveřejnění Vaší fotografie na sociální síti.

- Ne
- Ano

Stali jste se obětí vážného zneužití Vašich osobních údajů? *
Například urážka jiných osob pod Vaším jménem.

- Ne
- Ano

Stali jste se už obětí kyberšikany? *
Kyberšikana je druh šikany, který využívá elektronické prostředky. (sociální sítě) Její nejobvyklejší projevy představuje zasílání obtěžujících, urážejících či útočných zpráv a vytváření stránek dehonestujících ostatní, popřípadě může kyberšikana sloužit k posilování klasických forem šikany, nejčastěji prostřednictvím nahrání scény na mobilní telefon a jejího následného rozeslání známým dotyčného, popřípadě prostřednictvím vystavení na sociálních sítích.

- Ne
- Ano

Kolik přátel máte na Facebooku?
Vyplňte celé číslo. (pokud máte 258 přátel, vyplňte číslo 258)

Vaše odpověď

Používáte rozdílná oprávnění pro skupiny přátel na Facebooku?

- ○ Ne
- ○ Ano

Využíváte aplikace na Facebooku?

Například hry, aplikace na sečtení počtu zpráv s přáteli, různé otázky a dotazníky.

- ○ Ne
- ○ Ano

Jste ochotni odsouhlasit přístup k Vašim osobním údajům po spuštění aplikace na Facebooku?

- ○ Ne
- ○ Ano

Jaké osobní údaje sdílíte veřejně na svém profilu? *

- ☐ Jméno a Příjmení
- ☐ Město
- ☐ Vzdělání
- ☐ Email
- ☐ Partnera, členy rodiny
- ☐ Zaměstnání
- ☐ Telefonní číslo
- ☐ Adresu

Víte, že registrací na Facebooku potvrzujete souhlas s Podmínkami použití a zároveň potvrzujete přečtení dokumentu Zásady používání dat, včetně části Použití souborů cookie?

- ○ Ne
- ○ Ano

Seznámili jste se s obsahem Podmínek použití a Zásad použití dat na Facebooku?

- ○ Ne
- ○ Ano

Jaké heslo máte na Facebooku nastavené?

- ○ Krátké – lehce zapamatovatelné
- ○ Složené pouze z písmen
- ○ Složené pouze z číslic
- ○ Složené z číslic a písmen
- ○ Složené z písmen, číslic a speciálních znaků

Jaké sociální sítě aktivně využíváte? *

- ☐ Facebook
- ☐ Instagram
- ☐ YouTube
- ☐ Google+
- ☐ Twitter
- ☐ Ask.fm
- ☐ LinkedIn
- ☐ Foursquare
- ☐ Badoo
- ☐ Jiné: _____

Při jakých aktivitách používáte sociální sítě? *

- ☐ Při sledování TV
- ☐ Při řízení
- ☐ Při nakupování
- ☐ Při výuce
- ☐ Při cvičení
- ☐ Při cestování
- ☐ Na toaletě
- ☐ Jiné:

Dokázali byste přestat používat Vaši oblíbenou sociální síť, kdyby ohrožovala Vaše soukromí? *

- ○ Ne
- ○ Ano

Z jakého důvodu jste přestali používat určitou sociální síť? *

- ○ Přestala mě bavit
- ○ Ohrožovala mé soukromí
- ○ Kvůli negativní zkušenosti se sociální sítí
- ○ Nepřestal/a jsem používat žádnou sociální síť
- ○ Jiné:

Byli byste ochotni zabezpečit svůj profil na sociální síti, kdybyste dostali návod jak na to? *

- ○ Ne
- ○ Ano

Měnili jste nastavení soukromí na Facebooku?

- ○ Ne
- ○ Ano
- ○ Nevím jak

Měnili jste nastavení soukromí na Instagramu?

- ○ Ne
- ○ Ano
- ○ Nevím jak

Přidáváte svá vlastní videa na YouTube?

- ○ Ne
- ○ Ano

Stalo se Vám, že o Vás unikly citlivé údaje prostřednictvím videa na YouTube?

- ○ Ne
- ○ Ano

Jaký typ videí na YouTube sledujete?

- ☐ Hudební klipy
- ☐ Vzdělávací videa
- ☐ Vlogy
- ☐ Zpravodajství
- ☐ Zábavná videa
- ☐ Videa sdílená přáteli
- ☐ Jiné: _____

Stali jste se už obětí kyberstalkingu? *

Kyberstalking označuje dlouhodobé, opakované, systematické a stupňované pronásledování a obtěžování oběti pomocí sociálních sítí. Kyberstalking zahrnuje například výhrůžky, falešná obviňování, poškozování dat nebo zařízení, krádeže identity či dat, monitorování počítače, sexuální obtěžování a další formy agrese. Pachatel (kyberstalker) nepřestane takto jednat ani poté, co je oběti požádán o přerušení veškerých kontaktů. Je obvyklé, že intenzita obtěžování se stupňuje a postupem času může přejít z virtuálního do reálného světa.

- ○ Ne
- ○ Ano

Stali jste se už obětí kybergroomingu? *

Kybergrooming je termín, který označuje chování uživatelů sociálních sítí, které má v uživateli vyvolat falešnou důvěru a připravit ho na schůzku, jejímž cílem je nezletilou/zletilou oběť pohlavně zneužít. Útočníci jsou tedy často pedofilové.

- ○ Ne
- ○ Ano

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Systémové inženýrství a informatika
Forma: Prezenční
Obor/komb.: Informační management (im2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Krčil Vojtěch	Velká Jesenice 139, Velká Jesenice	I1434

TÉMA ČESKY:

Rizika používání sociálních sítí - analýza a návrh zabezpečení

TÉMA ANGLICKY:

Risks in the use of social networks - analysis and proposal for security improvement

VEDOUCÍ PRÁCE:

Ing. Karel Mls, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cíl práce: Analýza rizik, které plynou z používání sociálních sítí. Určení rizikových skupin na základě dotazníku a návrh pro zlepšení zabezpečení pro dané skupiny.

1.Úvod
2.Sociální sítě
3.Zabezpečení a soukromí
4.Dotazníkový průzkum
5.Návrh pro zlepšení zabezpečení
6.Závěr a shrnutí výsledků

SEZNAM DOPORUČENÉ LITERATURY:

GROSS, Ralph; ACQUISTI, Alessandro. Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005. p. 71-80.
TAYLOR, Robert W.; FRITSCH, Eric J.; LIEDERBACH, John. Digital crime and digital terrorism. Prentice Hall Press, 2014.
WILSON, Robert E.; GOSLING, Samuel D.; GRAHAM, Lindsay T. A review of Facebook research in the social sciences. Perspectives on psychological science, 2012, 7.3: 203-220.
TUCKER, Catherine E. Social networks, personalized advertising, and privacy controls. Journal of Marketing Research, 2014, 51.5: 546-562.
SALZINGER, Suzanne; ANTROBUS, John; HAMMER, Muriel. The First Compendium of Social Network Research Focusing on Children and Young Adult: Social Networks of Children, Adolescents, and College Students. Psychology Press, 2015.

Podpis studenta: ..... **Datum:** 14.10.2015

Podpis vedoucího práce: ..... **Datum:** 14.10.2015