Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra informatiky

Zneužívání osobních dat a možnosti jejich ochrany

Bakalářská práce

Autor: Zdeněk Tomášek

Studijní program: B1801 Specializace v pedagogice

Studijní obor: Informatika se zaměřením na vzdělání
Základy techniky se zaměřením na vzdělání

Vedoucí práce: Ing. Mgr. Josef Šedivý, Ph.D.

Hradec Králové Duben 2016

Univerzita Hradec Králové

Přírodovědecká fakulta

Zadání bakalářské práce

Autor:	**Zdeněk Tomášek**
Studijní program:	B 1801 Specializace v pedagogice
Studijní obor:	Informatika se zaměřením na vzdělávání Základy techniky se zaměřením na vzdělávání
Název práce:	**Zneužívání osobních dat a možnosti jejich ochrany**
Název práce AJ:	Misuse of personal data and the posibility of their protection
Cíle a metody práce:	Cílem této práce je provést rozbor potencionálních útoků na osobní data, jejich zneužití skrze sociální sítě a informační systémy, poukázat na to, jak snadno jsou informace o určitém člověku dostupné a seznámit s možným bezpečnostním rizikem. Dále sestavit dotazník na danou problematiku, který by měl za úkol zjistit, zda si klasický uživatel internetu uvědomuje, co všechno na internetu zveřejňuje a navrhnout možnou ochranu osobních dat a předcházet možným útokům nebo sledování.
Garantující pracoviště:	Katedra Informatiky Přírodovědecké fakulty UHK
Vedoucí práce:	Ing. Mgr. Josef Šedivý, Ph.D.
Konzultant:	
Oponent:	Ing. Petr Voborník, Ph.D.
Datum zadání práce:	26. 11. 2015
Datum odevzdání práce:	

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, z kterých jsem vycházel.

V Hradci Králové dne Jméno a příjmení

Poděkování

Děkuji Ing. Mgr. Josefu Šedivému, Ph.D. za odborné vedení a cenné rady, které mi při zpracování práce poskytl. Současně bych chtěl poděkovat své přítelkyni za podporu, pomoc a toleranci při tvorbě této práce.

Anotace

Tomášek, Z. *Zneužívání osobních dat a možnosti jejich ochrany*. Hradec Králové, 2016. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradce Králové. Vedoucí bakalářské práce Ing. Mgr. Josef Šedivý, Ph.D. 56 s.

Cílem této práce je provést rozbor potencionálních útoků na osobní data, jejich zneužití skrze sociální sítě a informační systémy, poukázat na to, jak snadno jsou informace o určitém člověku dostupné a seznámit s možným bezpečnostním rizikem. Dále sestavit dotazník na danou problematiku, který by měl za úkol zjistit, zda si klasický uživatel internetu uvědomuje, co všechno na internetu zveřejňuje a navrhnout možnou ochranu osobních dat a předcházet možným útokům nebo sledování.

Klíčová slova:

Zneužívání osobních informací, Sociální sítě, Bezpečnostní rizika, Ochrana osobních informací

Annotation

Tomášek, Z. *Misuse of personal data and the possibility of their protection.* Hradec Králové, 2015. Bachelor Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor Ing. Mgr. Josef Šedivý, Ph.D. 56 p.

The aim of this work is analyze the potential attacks on a personal data their misuse through Social networking sites and information systems, point out how easily are information about a specific person available and meet with the potential security risk. Additionally assemble a questionnaire on this issue, which was supposed to find out whether if a classic Internet user is aware of what all publish on the Internet and suggest possible protection of the personal data and prevent to potential attacks or monitoring.

Key words:

Misuse of personal information, Social Networks, Security Risks, Protecting Personal Information

Obsah

Úvod

V době novodobých trendů zvaných sociální sítě se setkáváme s velmi rychlými prostředky pro komunikaci a seznámení se s lidmi, které je díky neosobnímu kontaktu a tedy odbourání komunikační bariéry velmi snadné. Často pak zapomínáme na úskalí spojené se zveřejňováním osobních dat na různých serverech.

Uživatel internetu by si tím spíše měl uvědomit, že veškeré informace, sdílené, nahrané nebo napsané na internet, jsou zpětně dohledatelné. Stačí k tomu pouze počítač, připojení k internetu a trochu zručnosti.

Při své závěrečné práci se zaměřuji na potencionální shromažďování a ohrožení těchto osobních informací, které jsou dostupné téměř od každé osoby, jež se dostala do kontaktu s moderními technologiemi (platební karty, kamerové systémy, internet). Dále bych rád uvedl příklady technologií a jejich možnosti sledování osobního života. Neopomenutelným z cílů je také seznámení s legislativní stranou některých útoků a navržení možné obrany poskytované zákony.

Smyslem není řešit či hodnotit danou situaci, ale pouze ji dostatečně shrnout v rámci moderních prostředků a technologií, poukázat na úskalí s touto problematikou spojené a seznámit s možnou alternativní ochranou. Rád bych, aby tato práce upozornila na nebezpečí zneužití osobních dat, které může každému z nás ublížit a nebyla využita jako návod.

Práce je rozdělena do šesti hlavních kapitol. První dvě kapitoly se týkají vymezení základních pojmů s danou problematikou, využití osobních údajů v informačních technologiích a legislativy. Následující dvě se zabývají přímými útoky a zneužívání osobních údajů pomocí internetu a technologií. Pátá kapitola navrhuje možné ochrany a prevence vybraných problémů. V poslední kapitole řeším empirickou část závěrečné práce, jejíž částí je také vyhodnocení dotazníku.

1 Vymezení základních pojmů

Pro lepší pochopení mé práce je nutné si na začátek definovat několik základních pojmů. Nejdůležitější z nich je samotná definice informace.

1.1 Informace

Informace je velmi široký a mnohoznačný pojem, pro který není úplně přesná definice. Informace jako taková pochází z latinského slova *informatio* (představa, obrys), tento termín byl převážně využíván ve smyslu „formulovat myšlenku“. V nejjednodušším tvaru definice můžeme informace chápat jako údaje o reálném prostředí, o jeho stavu a procesech v něm probíhajících, která jsou nesená médiem, jež může být hmotné nebo energetické povahy. [1]

V informačních technologiích tvoří informaci kódovaná data, která jsou za pomoci určité technologie dál šířena, přijímána, uchovávaná nebo zpracována pro další použití. [2]

1.2 Osobní údaje

Osobním údajem se chápe jakákoliv informace týkající se naší osoby. Spojením jednotlivých osobních údajů je možná naše identifikace. Definicí tohoto pojmu se zabývá zákon o ochranu osobních údajů, kde osobní údaj „*je jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují. Tato se považuje za určenou nebo určitelnou, jestliže lze fyzickou osobu přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro její fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.*“ [3] Tudíž jakákoliv osobní informace, která není ve spojení s konkrétní osobou, není osobní údaj. Z toho si můžeme vyvodit například, že pokud uvedeme číslo pojistné smlouvy bez jeho majitele, nejedná se o osobní údaj, ale jen do té doby než přiřadíme číslo pojistné smlouvy klientovy.

1.3 Identifikační údaje

Do této skupiny zahrnujeme všechny údaje, které mohou přesně definovat osoby podle jednotlivých vlastností nebo jiných rysů odlišit jedince od celé skupiny a přesně ho identifikovat. Tento údaj používáme ke zjištění totožnosti. [4]

1.4 Identifikační a kontaktní údaje

Identifikační a kontaktní údaje je množina údajů sloužících a kontaktu současně.

Do identifikačních a kontaktních údajů řadíme tyto: [5]

- Jméno a příjmení
- Datum narození
- Rodné číslo
- Číslo občanského průkazu
- Adresu
- Telefon a emailovou adresu
- Pohlaví
- Rodinný stav
- Vlastní podpis
- Státní příslušnost

1.5 Citlivé osobní údaje

Jedná se o údaje, které jsou nejvíc spojeny s naším soukromím. Špatným zacházením s těmito citlivými údaji může dojít například i k porušování základních lidských práv nebo k diskriminaci. Charakteristika pojmu je uvedena přímo v zákoně takto: *„citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“* [6]

2 Využití osobních údajů v informačních technologiích

S pokročilým vývojem počítačových technologií se pojem soukromí přesunul na jiný stupeň. V minulosti bylo velmi složité sledovat kohokoliv dálkově, aniž by si toho všiml. Nyní však máme dobu, kde kamerové technologie umožňují sejmutí biometrických údajů během několika vteřin a následně je porovnat s databází pohřešovaných nebo trestaných osob na útěku a kontaktovat příslušné orgány.

Dnes je možné značnou část všech lidských aktivit sledovat. Z nich mohou vyvozovat následky nejen bezpečnostní složky, ale například i cílené reklamy pro zlepšení odbytu nabízeného sortimentu. Co se týče osobní komunikace, nyní je těžké odhadnout, zda si zprávu přečetl opravdu jen autor a adresát nebo i nějaká třetí strana.

Starosti nám také mohou dělat úložiště fotek či videí na internetu (Youtube, Instagram, Facebook) Počítačem uložená data, přestože jsou vymazána ze serveru, nejsou nikdy zcela vytracena a budoucí zaměstnavatel si může dohledat kupříkladu vaši fotografii z minulosti a podle toho se rozhodnout o vašem přijetí na pracovní pozici.

2.1 Osobní údaje v IS (Informačních systémech)

Podle Zdeňka Molnára informační systém jako takový je [7], *„soubor lidí, technických prostředků a metod (programů), zabezpečujících sběr, přenos, zpracování, uchování dat, za účelem prezentace informací pro potřeby uživatelů činných v systémech řízení.“*. Nebo podle Petra Sodomky [8], *„Podnikový informační systém vytvářejí lidé, kteří prostřednictvím dostupných technologických prostředků a stanovené metodologie zpracovávají podniková data a vytvářejí z nich informační a znalostní bázi organizace, sloužící k řízení podnikových procesů, manažerského rozhodování a správě podnikové agendy.“*

Z těchto definic můžeme vyvodit, že informační systém tvoří počítačový hardware, který obsluhuje speciálně navržený software, k němuž patří lidé, využívající tento software a provádějící procesy, jež vykonávají za účelem sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení. [9]

2.2 Zákon o ochraně osobních údajů v informačních systémech

Zákon č. 256/1992 Sb. byl jedním z prvních a významnějších v České republice v oblasti ochrany osobních údajů. Byl schválen v roce 1992, s ním byly oficiálně předneseny některé pojmy z informatiky a stanoveny základní pravidla v nakládání s osobními údaji. Tento zákon můžeme považovat za předchůdce nového zákona 101/2000 Sb. [10]

Zákony o ochraně osobních údajů, jakož i mezinárodní předpisy o ochraně osobních údajů, vždy upravují pouze některé formy a způsoby používání osobních údajů. Obecný právní pojem v českém právním řádu, který „pokrývá" prakticky všechny formy a způsoby používání osobních údajů, je „*nakládání s osobními údaji*". Některé formy nakládání s osobními údaji podléhají zákonu o ochraně osobních údajů, tyto formy se nazývají „*zpracováním osobních údajů*". Až na některé výjimky není zpracování osobních údajů zakázáno, jsou pro ně pouze stanoveny podmínky. Společensky nepřijatelné formy a způsoby nakládání s osobními údaji jsou odpovídajícími právními předpisy považovány za správní delikty nebo dokonce za trestné činy. Postih neoprávněného nakládání s osobními údaji jako trestného činu podle ustanovení *„§178 trestního zákona*" již není považován za součást ochrany osobních údajů. [11]

2.3 Právo na zapomnění

Určité řešení jak ochránit citlivé údaje, jež nedopatřením nebo vydíráním unikly na internet, označujeme za takzvané právo na zapomnění či právo být zapomenut. Slouží k ochraně osobnosti před stránkami, které mohou ovlivnit její pověst. Přesněji můžeme říci, že při vyhledání svého jména bychom neměli být ve výsledcích internetových dotazů v internetovém vyhledávači např. Google, Seznam, Centrum.

Evropský soudní dvůr v roce 2014 rozhodl, že Evropané mohou po webových vyhledávačích požadovat, aby ve výsledcích vyhledávání neodkazovaly na některé citlivé údaje. Google vede například reporting o vyřízených žádostech o odstranění obsahu z vyhledávání. [12]

Podle statistik zveřejněné společností Google od 29. června 2014 bylo v celé Evropě přijato 1 449 498 žádostí o odstranění webových adres a z toho 429 172

jich bylo přijato a odstraněno. Z České republiky bylo přijato 19 236 žádostí a z toho 3 995 jich bylo vyřešeno. [13]

3 Narušení a zneužívání osobních dat na internetu

S rostoucím počtem osobních údajů na internetu roste i riziko jejich zneužívání. Tuto problematiku popsal Karel Neuwirt [14]. „*Fantastické možnosti informačních technologií poskytují nepřebernou škálu jejich využití, usnadňují a zkvalitňují život dnešní společnosti. Ruku v ruce však poskytují nástroje na možné omezování práv a svobod občanů, např. tím, že dávají nebývalé možnosti uchovávání dat a informací o občanech, jejich snadné a rychlé dostupnosti. Není v možnostech jednotlivců sledovat jakými cestami, komu a k jakému účelu jsou údaje o nich poskytovány. Vzniká reálné nebezpečí vzniku orwelovského světa „Velkého bratra", který ví o občanovi vše a sleduje jej na každém kroku*.“ Zde autor shrnul všechny kladné, ale i záporné stránky nakládání s osobními údaji v informačních technologiích a potencionální hrozby.

3.1 Počítačová kriminalita

Jedná se o novodobý fenomén. Můžeme se s ním setkat prakticky kdykoliv, jedná se o využití počítače a internetu za účelem poškození či odcizení dat fyzické osobě či společnosti. Počítačová kriminalita je v současnosti považována za trestnou činnost využívající veřejné sítě jako nástroje k páchání běžných podvodů. Internet slouží zejména jako možnost širšího oslovení potencionálních obětí a současně, jako anonymizační prvek v rámci provedeného podvodu. [15]

3.2 Druhy počítačové kriminality

3.2.1 Spam

Spam je asi nejrozšířenější a nejznámější druh počítačové kriminality, který však není z pohledu zákona nijak trestán. Jde o rozesílání nevhodných a nechtěných emailů, které obsahují převážně nabídku některého zboží, jedná se převážně o komerční obsah. Můžeme se s ním setkat například i v diskusních fórech, kdy takzvaný „spamer“ umístí reklamu například na webovou stránku či produkt z ní pod článek, který s tím vůbec nesouvisí. Spam může být použit pro šíření trojských koní, virů nebo pornografie. O tuto problematiku se více zajímá Úřad pro ochranu osobních údajů, který provádí dozor na dodržování zákonem

stanovených povinností při zpracování osobních údajů, vede registr povolených zpracování osobních údajů, přijímá podněty a stížnosti občanů na porušení zákona, poskytuje konzultace v oblasti ochrany osobních údajů. [16]

3.2.2 Hoax

Jedná se o fenomén nynější doby. Hojně se vyskytuje a rychle šíří po internetu v podobě poplašných, klamných nebo nebezpečných řetězových zpráv. Souvisí nejčastěji s různými druhy aktuální problematiky společnosti od politiky přes informatiku až k prosbám o pomoc. Využívá neznalosti uživatelů, kteří tuto informaci převážně prostřednictvím emailu sociálních sítí rychle sdílí. Lidé zprávu pokládají za pravdu a věří jejich pravosti, čímž podněcují důvěru i v ostatních uživatelích, jimž hoax zašlou.

Na tuto problematiku poukazuje český server HOAX.CZ, jež analyzuje, hledá tyto klamné zprávy a ukládá je do své databáze, ke kterým má přístup uživatel. [17]

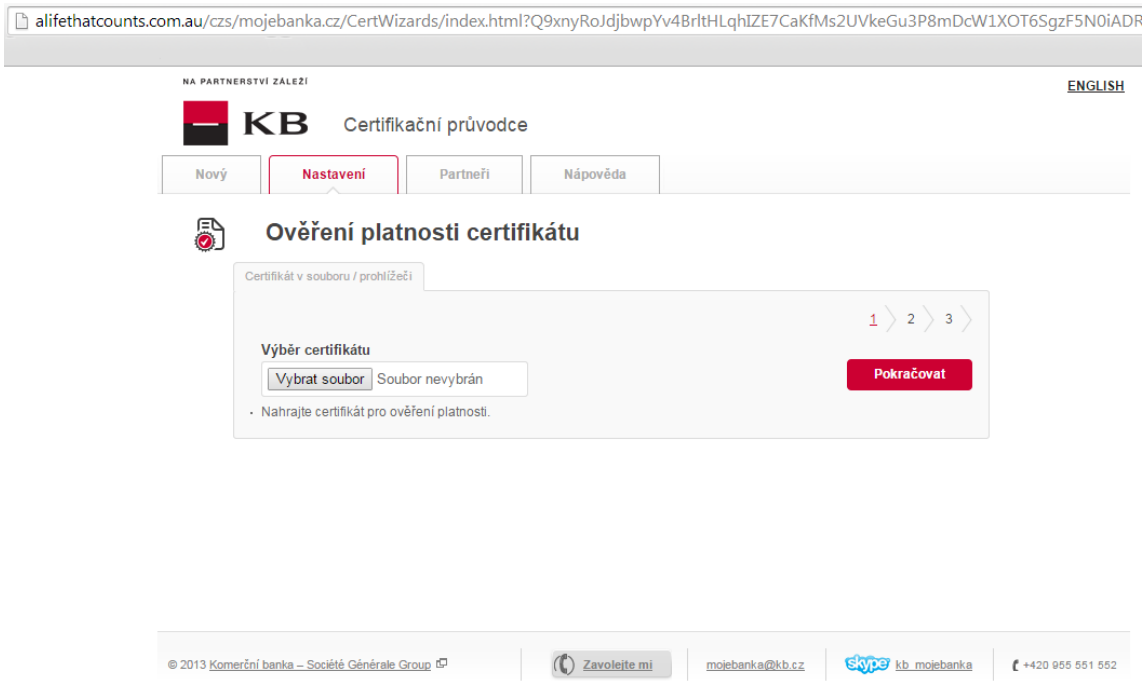
Trestnost takového protiprávního jednání ošetřuje Trestní zákoník §357 (šíření poplašné zprávy), ale jen v případě pokud je pachateli prokázán úmysl takového jednání. [18]

3.2.3 Phishing

Jedná o podvodné emailové útoky, které si kladou za cíl vymámit z uživatele citlivé informace například k platebním kartám včetně PINu nebo různé přihlašovací údaje k různým účtům. Podrobně tento problém definoval James Lance [19], *„způsob odeslání falšovaného e-mailu příjemci, který klamavým způsobem napodobuje legální instituci s úmyslem vyzvědět od příjemce důvěrné informace jako číslo platební karty nebo heslo k bankovnímu účtu. Takový e-mail většinou navádí uživatele, aby navštívil nějaké webové stránky a zadal zde tyto důvěrné informace…. Stránky této instituci samozřejmě nepatří a výsledkem je ukradení vašich důvěrných údajů za účelem finančního zisku.“*

Jako příklad si můžeme uvést zprávu z 3. února 2015 z informačního serveru aktuálně.cz, kde byl prostřednictvím emailu uživatelům rozeslán podvodný email pro přihlášení do internetového bankovnictví u Komerční banky, kde podvodné stránky převzali designovou podobu výše zmíněné banky a požadovaly potvrzení platnosti certifikátu. Banka ihned po odhalení útoku varovala své klienty. Z následujícího Obrázku č. 1 můžeme vypozorovat, že vizuální stránka je velice

zdařilou kopií. Avšak pokud se podíváme na webovou adresu, zjistíme, že nesouhlasí s webovou stránkou Komerční banky. [20]



Obrázek č. 1 - Fiktivní webová stránka Komerční banky pro získání přihlašovacích údajů
Zdroj: http://zpravy.aktualne.cz/finance/hackeri-miri-na-klienty-komercni-banky-chteji-pristupy/r~44c33b16ab9211e498be002590604f2e/

3.2.4 Pharming

Jedná se o inovativní formu phishingu. Tato podvodná technika napadne DNS server dané přihlašovací společnosti, což způsobí přesměrování klienta na podvodnou stránku. Zde pak klienta požádají o zadání všech přihlašovacích hesel a kódů. Pokud tak klient učiní, mohou se neoprávnění uživatelé přihlásit do internetového bankovnictví pod jeho jménem. Pokud klient nemá nastaveno další zabezpečení (např. potvrzování transakcí pomocí autorizační SMS nebo klientský certifikát), mohou mu nepozorovaně převést peníze z jeho účtu. [21]

3.2.5 Sniffing

Sniffing, v překladu „*čenichat*“, je technologie pro zachytávání dat nebo komunikace v rámci lokální počítačové sítě. Používá se například při diagnostice sítě nebo zjištění používaných služeb a protokolů.

Sniffing tímto způsobem plnohodnotně zastává činnost spywaru (špionáž dat) či keyloggeru (zjištění hesel). Software, za jehož pomoci je sniffing úspěšně vykonáván, se jmenuje sniffer. [22] Proti tomuto útoku se lze bránit například šifrováním komunikace na internetu.

Tato činnost je trestná podle § 182Porušení tajemství dopravovaných zpráv. Pokud pachatel použije získaná data jen pro vlastní účely, je těžko vysledovatelný a tedy téměř nepostihnutelný. [23]

3.2.6 Carding

Tento pojem v sobě ukrývá zneužití platebních karet při jejich použití v online platbách. Do tohoto útoku zahrnujeme prosté odcizení platební karty, krádež čísla platební karty, PIN kódu, nebo také zkopírování karty pomocí speciálního zařízení přidělané přímo na bankomat s kamerou pro snímání PIN kódu. Tyto zjištěné údaje pachatel nahraje na svou padělanou platební kartu. Tato činnost se nazývá „*skimming*“. [24]

3.2.7 Vishing

Jedná se o takzvaný „*voice phishing*“ tedy o vylákání údajů od lidí pomocí telefonních služeb. V tomto případě může oběť kontaktovat osoba, která se představí například jako pracovník banky nebo kontaktuje osobu SMS zprávou či emailem s číslem, na které se má obratem ozvat kvůli kupříkladu nevysvětlitelným platebním transakcím.

„Hrozbou budoucnosti je také takzvaný vishing, který k odcizení informací využívá telefonní služby místo chybného webového linku. Při této formě phishingu přijmou uživatelé telefonát informující o potížích s jejich kreditní kartou. Hovor vybízí oběť, aby následně po telefonátu volala na zadané číslo a vyřešila tak problém se svou kreditní kartou. Na daném čísle je oběť vyzvána k zadání čísla své kreditní karty nebo jiných detailů svého bankovního účtu. Často je telefonní služba využívána jenom k proniknutí spyware do telefonu. Když si představíme, že business přes telefonní služby je dnes již běžnou záležitostí, tak to zavání vishingovou epidemií.“[25]

Tomuto nepříjemnému napadení se lze vyhnout tak, že budeme ignorovat podezřelé SMS či emaily s výzvou o zavolání, nebo dokonce přeposlání SMS s číslem karty a PINem na údajné číslo. Můžeme například použít přímo infolinku banky pro zjištění více informací.

3.3 Facebook jako potencionální nebezpečí

3.3.1 Historie

Tato síť byla založena v únoru roku 2004 studentem Harvardovy univerzity Markem Zuckerbergem, kterou nedokončil. Původně tuto síť založil pro lepší seznámení nových spolužáků na univerzitě. Postupně se rozšiřovala i na jiné univerzity a instituce od roku 2006 mohl facebook používat každý starší 13 let. Společnost Facebook své peníze vydělává především pomocí reklam, které jsou přesně cílené na jednotlivé zájmy uživatele a jeho chování na sociální síti.[26]

3.3.2 Skutečný Facebook v dnešní době

Facebook jako největší a nejpopulárnější sociální sít shromažďuje od roku 2006 osobní údaje 1,65 miliardy svých uživatelů, z toho 72% dospělých uživatelů denně navštěvuje Facebook, počet denně aktivních uživatelů je 890 milionů z toho jen v Evropě je aktivních 233 milionů. Průměrný čas strávený uživatelem denně na Facebooku je 21 minut a země s nejvíce aktivními uživateli je Kanada. Podle statistik má každá žena průměrně 166 přátel a každý muž 145 přátel a 83% z nich má v přátelích rodiče. 27% právě jedoucích řidičů sledují dění na Facebooku. [27]

K Facebooku se lze připojit i pomocí mobilních zařízení například přes aplikaci Facebook Mobile, což umožňuje uživatelům být kdykoliv a kdekoliv, kde je přístup k internetu, online, sdílet své vzpomínky jako jsou fotky či videa a komunikovat s přáteli. Populárnost Facebooku vzrůstala s jeho funkcionalitou. Každý z uživatelů určitě uvítá přehledné uživatelské rozhraní s výběrem jazyka a hezkým příjemně působícím klidným, modrým designem, jednoduché vyhledávání známých lidí, ať už kamarádů, nebo známe osobnosti a chatování. Dalšími klady jsou sdílení fotografií z dovolené, videí, vkládaní odkazů, vytváření vlastních událostí, na které lze přizvat své přátele, dále nám Facebook nabízí mnoho aplikací, jako jsou asi nejrozšířenější hry, porovnávání fotek s přáteli, time managment a propojení například s YouTube.

3.3.3 Potencionální nebezpečí

Na hlavní stránce Facebooku můžeme narazit na slogan „*Facebook byl, je a bude zdarma.*“, ale po přečtení Podmínek použití Facebooku, Zásady používání dat a Používání souborů cookies napadne mnoho lidí, že Facebook nechce za používání žádné peníze, ale za využívání všech služeb, které poskytuje, chce úplný přístup ke

všem osobním informacím, fotkám, videím, vaší GPS poloze a nárokuje si vlastnictví na tyto údaje.

Zde na nás můžou číhat potencionální bezpečnostní rizika, jako je kopírování, nebo zneužití osobních údajů. Množství dat, které sdílíme na sociální síti mohou využívat třetí strany (reklamní společnosti), které velmi účinně cílí reklamu a sledují náš pohyb na internetu pomocí souborů cookies bez jejich povolení ve vašem prohlížeči se na Facebook nepřihlásíte.

Dále Facebook mohou používat lidé, jako jsou násilníci, zloději, nebo pedofilové, kteří pomocí sociálních sítí vyhledávají svou potencionální oběť. Díky informacím si oběť můžou vytipovat například sdílením údajů, kde a s kým se právě nachází, tím se tomuto riziku vystavují. Tyto všechny údaje, které o sobě sdílíme, můžeme ochránit pomocí nastavení soukromí, bohužel průzkum Tatjany Taraszow na kolektivu z roku 2010 poukazuje na to, že 22,1% mladých lidí ve věku 13 až 30 let mají svůj profil zcela veřejně přístupný bez nastavení soukromí. [28] Což je sice malé procento uživatelů, ale když si to přepočtem na počet uživatelů používající Facebook dojdeme k ohromujícímu číslu.

Zde bych uvedl výběr několika důležitých usnesení o podmínkách používání Facebooku: [29], [30], [31]

„**Souhlasíte s přenesením a zpracováním svých osobních údajů ve Spojených státech amerických.**“(Podmínky použití: bod 17. Zvláštní ustanovení pro uživatele mimo Spojené státy americké, které nám jasně říká, že sdílené informace jsou odesílány do Spojených států amerických)

„**Informace, které o vás obdržíme, používáme pro spolupráci se službami a funkcemi, jež poskytujeme vám a ostatním uživatelům**“(Zásady používání dat: Informace, které o vás získáváme.)

„**Informace o zařízení.**

Podle oprávnění, která jste udělili, shromažďujeme informace z počítačů, telefonů a dalších zařízení, na která instalujete nebo v nichž používáte naše Služby, a také informace o těchto zařízeních. Informace získané z různých zařízení můžeme sdružovat, abychom mohli snadněji poskytovat konzistentní služby ve všech zařízeních. Tady je několik příkladů informací, které o zařízeních shromažďujeme:

- Atributy, jako je operační systém, verze hardwaru, nastavení zařízení, názvy a typy souborů a softwaru, výkon baterie, síla signálu a identifikátory zařízení.
- Umístění zařízení, včetně konkrétních zeměpisných umístění, například prostřednictvím GPS, Bluetooth nebo signálů Wi-Fi.
- Informace o připojení, například název mobilního operátora nebo poskytovatele internetových služeb, typ prohlížeče, jazyk a časové pásmo, číslo mobilního telefonu, IP adresa.“

„**Sdílení vašeho obsahu a informací**

- K obsahu chráněnému právy k duševnímu vlastnictví, jako jsou fotografie a videa (obsah podléhající duševnímu vlastnictví, DV), nám výslovně udělujete následující oprávnění, v souladu s vaším nastavením soukromí a nastavením aplikací: udělujete nám nevýhradní, přenosnou, převoditelnou, celosvětovou bezúplatnou (royalty-free) licenci na použití veškerého obsahu podléhajícího DV, který zveřejníte na Facebooku nebo v návaznosti na něj (Licence k DV).

  Tato licence k DV končí, jakmile svůj obsah podléhající DV odstraníte ze svého účtu, s výjimkou případů, kdy jste tento obsah sdíleli s ostatními (pokud jej také oni neodstranili).
- Jestliže obsah podléhající DV odstraníte, bude odstraněn obdobným způsobem, jako při přesunutí do Koše v počítači. Berete však na vědomí, že odebraný obsah může existovat v záložních kopiích po přiměřeně dlouhou dobu (nebude však dostupný ostatním).

Pro shrnutí tohoto bodu, cokoliv vytvoříte a umístíte na sociální síť, se okamžitě vzdáváte práva na duševní vlastnictví a Facebook může a využívá vaši tvorbu ke komerčnímu využití.

Touto kapitolou jsem chtěl informovat o možnostech s potencionálním ohrožením dat, nebo dokonce uživatelů nejen této sociální sítě, ale všech sociálních sítí, které jsou dostupné širší veřejnosti. Je samozřejmě na nás, co vše veřejně sdílíme, ale v některých případech bychom si měli promyslet důsledky, které by to pro nás nebo pro naše okolí mohlo přinést.

3.4 Social Engineering

V českém překladu se tento druh kriminality nazývá sociální inženýrství. Jedná se o techniku manipulace uživatelů, nebo klientů bez jejich vědomí prostřednictvím klamání za účelem provedení akce, nebo získání informací na úrovni toho, že si útočník vytvoří sociální důvěru a využije jejich city, emoce, záliby, koníčky atp. Zkouší různé psychologicky založené triky.

S budováním sociálního inženýrství se můžeme setkat prakticky kdykoliv, známým příkladem jsou podvodní výběrčí nedoplatků za plyn, elektřinu a vodu, nebo také pochybné firmy, které se zabývají poradenstvím a tuto techniku využívají takovým způsobem, že si klienta „vygooglí" a najdou si jeho zájmy, koníčky a vše co ho baví. To vše jim pomůže při následné komunikaci s klientem a vyvolání falešného pocitu přátelství, kdy klient bude důvěřovat plně poradci. [32]

3.5 Krádež identity v kybernetickém světě

Krádeží identity se útočníci zajímají už od dob, kdy zjistili, že to může být velmi výdělečné. V současnosti se však pozměnila její podoba. Místo fyzického vydávání se za určitou osobu, kde se museli ukrást různé dokumenty či provést změnu vzhledu je jednodušší se tou osobou stát online díky tomu, že přes internet nikdo neví, jak doopravdy vypadáte.[33]

Prostředků pro krádež identity je spousta, některé jsme si vyjmenovali výše, v nynější době se nejčastěji stávají oběti těchto odcizení dat lidé, nebo skupiny, které mají veřejné profily na sociálních sítích. Většinou je to za účelem zesměšnění, nebo marketingového boje mezi firmami a v neposlední řadě k trestné činnosti.

Takového jednání se považuje jako trestný čin a je možné proti tomuto podat trestní oznámení na tyto usnesení v trestním zákoníku: [34]

§ 182 - Porušení tajemství dopravovaných zpráv

§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

§ 232 - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Ukradení identity můžete poznat například podle toho, že na sociální síti objevíte velmi podobnou kopii vašeho profilu, včetně fotografií, příspěvků a bude se snažit kontaktovat vaše přátele. Nebo se můžete tzv. „vygooglit“ a zjišťovat informace sami o své osobě, nebo firmě.

3.6 Kybernetický stalking

Pojem stalking jako takový si můžeme vyložit jako opakované a stupňované obtěžování nebo pronásledování, které se může projevovat v různých formách.

Novinkou v éře ICT je takzvaný kyberstalking, který využívá online komunikátorů k systematickému zasílání obtěžujícího, zastrašujícího a nenávistného obsahu vybraným uživatelům. Oběti tohoto typu útoku jsou obtěžovány pomocí spamu, zanechávání hanlivých vzkazů na chatu, zasíláním klamných zpráv a virů. K získávání kontaktů na jednotlivé uživatele slouží diskusní skupiny, sociální sítě, informační systémy (škol, podniků apod.), diskusní fóra a email. [35], [36]

Kyberstalker může využít například k hanobení uživatele krádež identity a založit identický profil oběti, kde ji osočuje, vyjadřuje za ni její názory a kontaktuje přátele.

4 Technologie narušení soukromí a monitoringu

4.1 Data mining

Data mining, neboli dolování dat přímo z databáze informačního systému, který shromažďuje informace o uživatelích. Jedná se o analytický pojem z oblasti Business Inteligence a podrobný popis takzvaných „dolování dat“ můžeme najít v České terminologické databázi knihovnictví a informačních věd: Technologie vyhledávání, modelování a prezentace předem neznámých informací, příp. znalostí a vztahů mezi daty v rozsáhlých databázích a datových skladech. Analýzy se odvozují přímo z obsahu dat, nikoliv na základě hypotéz či dotazů uživatele. Využívají se techniky umělé inteligence (neuronové sítě, rozpoznávání, samoučící se algoritmy), jež mohou být kombinovány s technikami statistického a

matematického modelování (klasifikační pravidla nebo stromy, regrese, shluková analýza) a s nástroji OLAP (on-line analytické zpracování). [37]

Data mining tedy umožňuje pomocí speciálních algoritmů automaticky objevovat v datech strategické informace. Je to analytická technika pevně spjatá s databázemi, jako velmi kvalitním zdrojem pro tyto speciální analýzy. Data mining slouží manažerům k objevování nových skutečností, které pomáhají zaměřit jejich pozornost na podstatné faktory podnikání. [38] Tato vydolovaná data mohou být i v podobě citlivých informací a jejich použitím lze například získat informace o tom, jaké má zvyklosti uživatel, který se pohybuje internetem a umožňuje přesnou a cílenou reklamu, či jeho sledování chování na internetu.

4.2 Mobilní telefony jako prostředek pro sledování

Mobilní telefony v dnešní době nejsou žádnou raritou, nýbrž se stali spotřebním zbožím, trendem či doplňkem k oblečení. Tyto telefony představují skvělý prostředek pro komunikaci a ze spojení s moderní technologií a operačním systémem dostáváme jako celek malý a výkonný počítač, v nynější době nazývaný Smarthphone, neboli chytrý telefon, který můžeme využívat nejen k telefonování, ale i k brouzdání po internetu s použitím Wi-Fi nebo mobilní sítě, pořizování fotografií a stahování různých aplikací.

Od počátků mobilních telefonů se s nimi spojoval i pojem odposlechy hovorů, nebo sledování SMS zpráv. V raných počátkách standardu GSM (Globální systém pro mobilní komunikaci) bylo téměř nemožné prolomit zabezpečení tohoto protokolu, později se šifrovací standardy prolomily. Pro dešifrování GSM komunikace je ale zapotřebí profesionální odposlechové vybavení v řádech několika tisíc korun a navíc odposlechy jsou vedeny jako trestný čin. Legální odposlech může nařídit soud. [39]

Nynější doba nabízí široké spektrum pro sledování činnosti na chytrých telefonech a tou jsou aplikace pod hromadným názvem SPY software, tedy špionážní software. K instalaci takovéto aplikace může dojít nejméně dvěma způsoby. První způsob je takový, že se vám útočník dostane fyzicky k mobilnímu telefonu a nainstaluje vám škodlivý software. Instalace takového softwaru zabere několik málo minut. Druhá možnost stáhnutí a nainstalování SPY softwaru do mobilního telefonu je, že si majitel telefonu dotyčnou aplikaci nevědomky stáhne sám například s jinou aplikací, aktualizací, nebo se může skrývat v MMS zprávě.

Jakmile je úspěšně provedena instalace, SPY aplikace běží na telefonu skrytě, telefon nevykazuje žádné změny ve funkčnosti a majitel nemá téměř žádnou šanci zjistit, že má takovýto software ve svém zařízení. Aplikace pro toto sledování jsou dostupné ke stažení na internetu a netají se ani jejich použití, cena takovéto aplikace se pohybuje od 20$ za měsíc a jsou kompatibilní pro všechny možné operační systémy chytrých telefonů (Android, Windows, iPhone, Blackberry atd.) bez rozdílů značek mobilních telefonů. [40], [41]

Aplikace plní převážně tyto úlohy: [42]

- Odposlech hovorů v reálném čase
- Ukládání hovorů ve skrytých souborech
- Poslech okolí, dálkové zapnutí mikrofonu
- Zachycení SMS, MMS a emailových zpráv i v případě, že oběť zprávu smaže
- Zachycení všech multimediálních souborů (fotky, videa, emaily, soubory)
- Monitoring GPS polohy
- Možnost zapnutí kamery na dálku
- Zachytávání hesel k emailovým nebo aplikačním účtům (gmail.com, Hotmail.com, Facebook, Google+, Skype)

Tato technologie může být využívána například v rodičovské kontrole, zabezpečení v případě krádeže nebo napadení. Dále je mohou využívat firmy pro nezákonné sledování zaměstnanců, zhrzený zamilovaný partner, stalker, nebo jiný sociální zvrhlík.

4.3 Bezpečnostní kamery

Bezpečnostní kamery, jak už název vypovídá, jsou kamery sloužící k ochraně osob a majetku, který je součástí EZS (Elektronického zabezpečovacího systému). V nynější době kamerové systémy zasahují největší částí do narušení soukromí sledováním činnosti osob a pomocí speciálních algoritmů jsou schopny vyhodnotit podle biometrických údajů a mimiky potencionální možné nebezpečí a zavčas varovat příslušné orgány.

Analýza osob podle biometrických údajů obličeje je nejméně nákladným a zároveň efektivním procesem při použití kvalitních bezpečnostních kamer a softwarového vybavení. Metoda pomocí otisků prstů není tak přesná kvůli tomu, že dvě procenta populace nemá jedinečný otisk prstu, DNA testy jsou velmi přesné,

ale finančně náročné a zdlouhavé a skenování duhovky je velmi složité pro masové využití. [43]

V rušném městě se nachází několik stovek a v Praze i dva tisíce kamer pro sledování dění na ulicích či ke kontrole dopravní infrastruktury. Na jednu stranu tento systém velmi efektivně usnadňuje práci policie a jiných bezpečnostních složek, na druhou stranu tato technologie zásadně narušuje soukromí lidí, kteří ani nemusí vědět, že jsou sledováni a vyhodnocování systémem. Pomocí tohoto systému lze pak předvídat s velkou přesností jednotlivé úkony sledovaného, a stát pak může mít pod úplnou kontrolou své občany, nebo marketingové firmy lépe cílit reklamu podle toho kam se člověk dívá, nebo podle jeho nálady. [44], [45]

4.4 Technologie GPS

Global positioning system, neboli česky Globální polohovací systém, je družicový systém pro určení vaší polohy kdekoliv na zemském povrchu, bez ohledu na počasí a na dobu, kdy ho používáte s přesností na několik metrů či centimetrů. V roce 1973 byl původně sestrojen Ministerstvem obrany Spojených států pro vojenské námořnické účely. V průběhu let se systém vyvíjel a rozšiřoval do dalších odvětví jako je letectvo, kosmonautika, či veřejný sektor a začátkem roku 2000 se stal plně funkčním a dostupným po celém světě. [46]

Nyní kolem naší planety obíhá celkem 32 satelitů ve výšce 20 200 kilometrů, kde se pohybují rychlostí 3,8 km/s, GPS lokace se využívá skoro ve všech zařízeních pro snadnou lokalizaci polohy a následné navigace, například automobilový průmysl tuto technologii využívá v podobě navigačního hardwaru s displejem umístěného za čelním sklem auta, další možností použití systému je turistika. V dnešní době chytrých telefonů nenarazíme na mobilní telefon, který tuto technologii nevyužívá se spojením dalších aplikací, jako jsou například mapy. [47]

GPS systém je pouze pasivní technologií, tzn. použitá technologie pro lokalizaci pouze data přijímá. Hlavním důvodem je vojenský původ systému, pro který by bylo nepřípustné, aby byl zpětně lokalizován nepřítelem. Dále GPS pro svou funkčnost nepotřebuje přístup k internetovému spojení. [48]

S touto geolokační technologií mohou přijít i nemilé úskalí, například zpráva z roku 2007 z vojenské základy v Iráku, kde letka helikoptér Apache byla po přistání vyfocena vojáky přímo na letišti. Tyto fotky následně umístili vojáci na

internet a z metadat útočníci zjistili přesnou polohu základny na kterou zahájili minometný útok, při kterém byly zničeny čtyři helikoptéry. To se odehrálo pomocí tzv. „Geotaggingu“ jedná se o anglický termín o předání geografické informace k různým médiím, jako jsou například fotografie. Tyto informace většinou zahrnují zeměpisnou délku a šířku, kde byla fotografie pořízena, technologii samotnou v sobě může ukrývat fotoaparát, nebo mobilní telefon. Tuto funkci lze v nastavení zařízení vypnout. [49]

Tato technologie velmi usnadňuje vykonávání různých aktivit, ale také vybízí ke spoustě otázkám týkajících se našeho narušení soukromí a jestli lze přes satelitní síť kohokoliv a kdykoliv sledovat a ukládat si data o jeho pohybu.

5 Možné návrhy na zabezpečení soukromí

V předešlých odstavcích byly podrobně vysvětleny různé možnosti zneužití osobních údajů, dat a citlivých informací. Následující kapitola se bude věnovat ochraně těchto důležitých dat, bohužel neexistuje jednotná rada na předcházení všech takovýchto útoků a zneužívání, ale existují různé ochranné metody a postupy pro jednotlivé činy, které narušují soukromí.

S hlavní takovouto metodou se už na základní škole seznamují děti a tou je tzv. počítačová gramotnost, jedná se o soubor schopností a dovedností, které se zaměřují na práci s počítačem, využití v životě a porozumění internetového světa. Toto považuji za základní pilíř při obraně našich osobních údajů.

5.1 Všeobecné zásady pro ochranu soukromí

Těmito zásadami se výhradně zajímá Úřad pro ochranu osobních údajů (UOOU), který vytváří rady a řeší různé kauzy v oblasti ochrany osobních dat i na internetu a vydává různé propagační letáky do škol.

Zde bych uvedl souhrnný seznam rad podle UOOU: [50]

- každý, kdo si nárokuje vaše osobní údaje, musí mít váš souhlas k jejich využití
- pozorně si pročítat dokumenty a jejich dodatky, které podepisujeme ve většině dokumentů je malým písmem, že data poskytnuté firmě budou dále použita pro marketingové účely. To může mít za následky nevyžádané telefonáty s nabídkou půjček, parfému atp.

- máte právo na výpis osobních údajů, které o vás subjekt získává. Pokud zjistíte, že data jsou nepravdivé či neúplné, máte nárok na opravu, blokování, doplnění, nebo na vymazání.
- je zakázáno pořizování kopií vašich osobních údajů (občanský průkaz, cestovní doklady) bez vašeho souhlasu, nebo souhlasu soudu
- pro evidenci vstupu do budovy je plně dostačující vaše jméno a příjmení v některých možných případech i číslo občanského průkazu, nebo služební průkaz. Nikdy nesmí být požadováno vaše rodné číslo.
- pokud vaše data ukládáte na nějaké záznamové zařízení je nutno například před případným prodejem vymazat důkladně data
- při zasílání vašich osobních údajů pomocí elektronického komunikátoru dbejte na to, že komunikační prostředky mohou být odposlouchávány neoprávněnou osobou
- v případě sledování prostoru kamerovým systémem jste povinni vědět o tom, že je s vámi prováděn záznam. Záznamové kamery nesmí nainstalovány v intimních prostorách, jako jsou toalety, sprchy, převlékárny.

5.2 Možnosti ochrany soukromí na internetu

V prostředí internetového nákupu, registrace do fóra, ankety, dotazníky, nebo jiné služby se setkáváme s nutností zadávat své osobní údaje. Obchod s osobními údaji není žádná novinka, existují velké databáze osobních údajů prodávané v aukcích, a proto se vyplatí umět zacházet s těmito daty.

5.2.1 Registrace

Při registraci na nějakou webovou službu byste si důkladně měli promyslet, komu dáváte k dispozici vaše osobní údaje. Většina formulářů pro registraci má označena textová okna, která jsou nutná pro registraci při tomto vyplňování je nutno vyplnit jen nezbytné údaje. Pro nevyžádané reklamní sdělení či spamy je namístě si vytvořit několik emailových schránek například pro nákupy, běžnou komunikaci a práci. Posledním důležitým faktorem při registraci je „silné“ heslo, nepoužívejte lehce odhadnutelná hesla (password, heslo, 123456789, atd.…), ale využijte například generátory hesel nebo celé věty s kombinací různých speciálních znaků či velkých a malých písmen. Důležité je také nemít jedno heslo k více službám a jednou za tři měsíce ho obměnit. [51]

5.2.2 Stahování

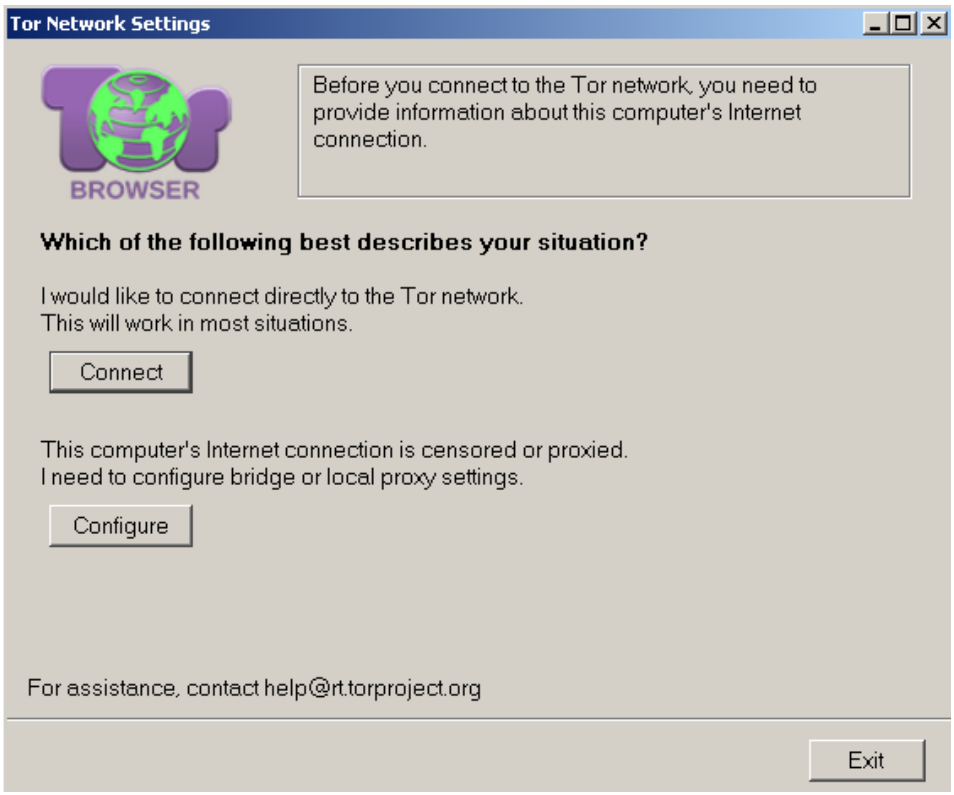
Je dobré si při stahování různých souborů, obrázků, her a filmů prověřit jejich původ a také dávat pozor na koncovky souborů, například vir rozesílaný po facebooku, který nabádal ke stažení obrázku s koncovkou .exe, což značí spustitelný program v operačním systému MS Windows a takovýchto virů na webových uložištích je spousta. Dále toto riziko přináší stahování pornografie, nelegální kopie multimédií a softwaru.

5.2.3 Historie

Všechny dostupné prohlížeče v dnešní době mají funkci uchovávání historie prohlížení internetu a ukládání hesel. Tyto funkce lze vypnout, ale jejich zapnutí vám umožní lépe vyhledávat stránky, které jste navštívili a nemusíte si pamatovat desítky hesel. Ovšem toto ukládání se dá zneužít. Proti tomuto zneužití nesmíme vystavovat zařízení (mobil, stolní počítač, notebook, tablet) bez dozoru. Dále když přistupujeme na internet z veřejného počítače (kavárna, škola, knihovna) je lepší využít funkci prohlížeče nazvané „anonymní okno", či „anonymní prohlížení“, jelikož všechny informace z vašeho surfování po internetu, které si prohlížeč zaznamenává po zavření anonymního okna smazány. [52]

5.2.4 Anonymita online

Pod tímto pojmem si můžeme představit surfování po internetu, kdy za sebou nenecháme žádnou vysledovatelnou stopu (ip adresu, jméno počítače), k tomuto úkonu může sloužit anonymizační síť Tor, která nám zajistí pomocí proxy serverů novou identitu, plně otevřený internet a deep web (zakázaný internet, kde se na stránkách zakázané státy propaguje různé násilí nebo obchody s nelegálními věcmi), na síť Tor se lze připojit po stáhnutí „Tor Browser“ jedná se o prohlížeč, u kterého můžeme zvolit při každém spuštění náš problém a podle toho se nastaví (viz. Obrázek č. 2).



Obrázek č.2 Možnosti připojení k Tor síti
Zdroj: vlastní

5.2.5 Spam

Obrana proti nevyžádané poště je velmi nespecifická, první možnou obranou je nastavení emailového filtru na příchozí emaily. Pokud se jedná o emaily firmy, které jste dali souhlas se zasíláním propagačních materiálů, tak lze tuto volbu zrušit prostým kliknutím, nebo zasláním emailu o tom, že nechcete dostávat tyto emaily. Další možností je vytvoření tzv. spamového emailu, který budete využívat jen pro účely registrace na internetové služby.

5.2.6 Vylákání osobních údajů

Ve třetí kapitole byly zmíněny možnosti útoků a vymámení osobních dat pomocí phishingu, pharmingu, sniffingu, cardingu a vhishingu. Proti těmto útokům se lze bránit pouze, pokud budeme ostražití při vyplňování důležitých údajů pod nějakou výzvou ať už skrz emailovou korespondenci nebo telefonátem. Nejlépe na tyto podněty nereagovat vůbec.

5.2.7 Reklamy

Pomocí cookies a získaných osobních dat o nás a našem pohybu po internetu webové stránky a vyhledávače přizpůsobují reklamy přímo na uživatele. Při načítání webové stránky se tak spolu s obsahem musí načítat i několik reklam,

které značně mohou zpomalovat internet. Proti těmto marketingovým záležitostem nám mohou pomoci programy třetích stran (viz. Obrázek č. 3), které se přímo dají nainstalovat jako modul do prohlížeče jedním takovýmto modulem je „AdBlock Plus“ lze ho nainstalovat do většiny nejpoužívanějších prohlížečů. Do internetového prohlížeče lze nainstalovat i rozšíření, které chrání před sledovacími systémy a různými aplikacemi třetích stran tento modul se jmenuje „Ghostery“.

Obrázek č . 3 Vlevo stránka s vypnutým AdBlockem, vpravo stránka se zapnutým modulem
Zdroj: Printscreen z http://www.zive.cz/

5.3 Možnosti ochrany soukromí na sociálních sítích

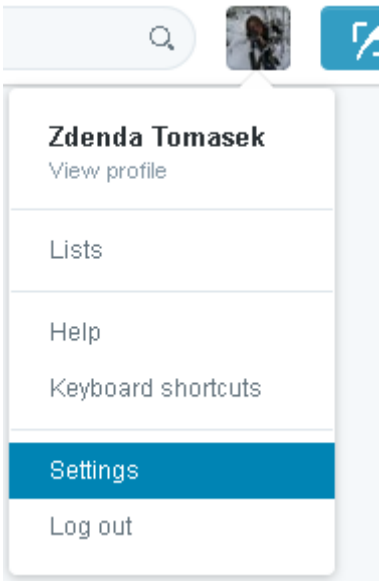
Následující dvě sociální sítě, kterým bych se chtěl věnovat. Z hlediska zabezpečení osobních údajů jsou největší a nejpopulárnější a někteří lidé nevyužívají jejich potencionální zabezpečení a tak vystavují svůj profil veřejně.

5.3.1 Twitter

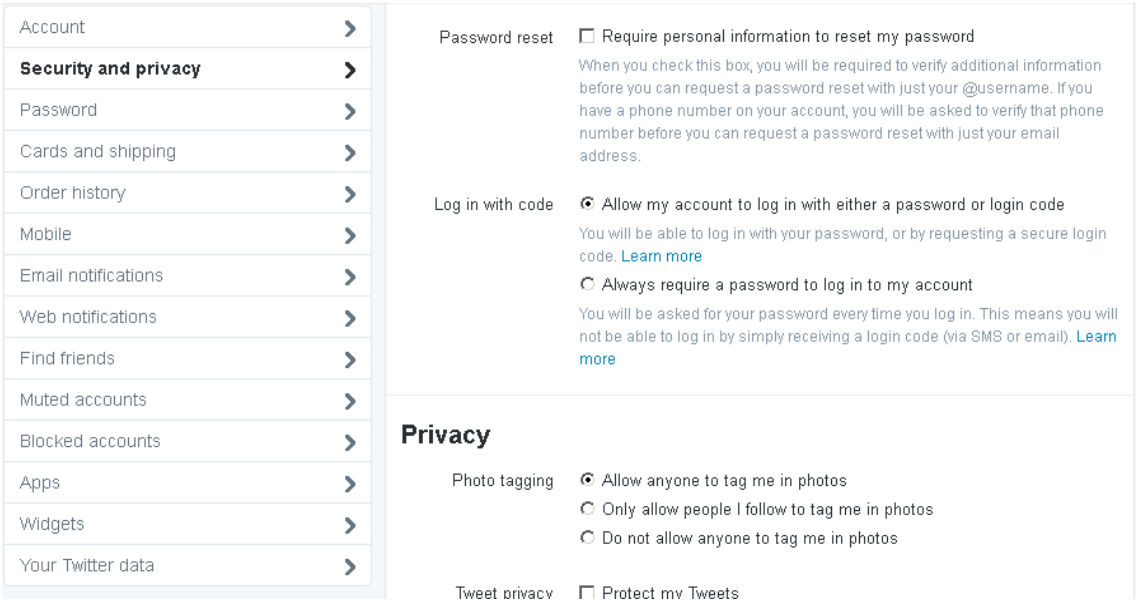
Pro nastavení soukromí na sociální síti Twitter.com si najedeme kurzorem do pravého horního rohu na naši profilovou fotku a levým tlačítkem myši rozbalíme kontextovou nabídku, kde jako předposlední máme „Settings“ (viz. Obrázek č. 4). Po stisknutí se nám zobrazí stránka s celkovým nastavením našeho profilu rozděleného vlevo do několika bloků. Pro nastavení soukromí zvolíme možnost druhou ze shora „Security and privacy“, kde nás nejvíce bude zajímat položka soukromí „Privacy“ (viz. Obrázek č. 5).

Zde máme mnoho možností, jak zabezpečit své soukromí lze si nastavit označování na fotografiích povolení všem označovat mou osobu na fotografiích, povolit jen lidem, které následuji, nebo zákaz označování na fotografiích.

Další možností je své příspěvky zveřejnit jen pro sebe. Dále zde máme zveřejnění lokace příspěvku zde je možno povolit či nikoliv. Dalšími možnostmi jak zabezpečit svůj profil je možnost zveřejnit příspěvek jen pro sebe, dále je zde zveřejnění lokace příspěvku zde je možné povolit či nikoliv, následuje možnost, jak vás lidé mohou najít, zde jsou dvě možnosti, které mohou být zaškrtnuté současně. Následující důležité nastavení se týká zpráv, které vám mohou zaslat jedinci, které nenásledujete.



Obrázek č. 4 Kontextová nabídka s možností nastavení
Zdroj: Printscreen z https://twitter.com/

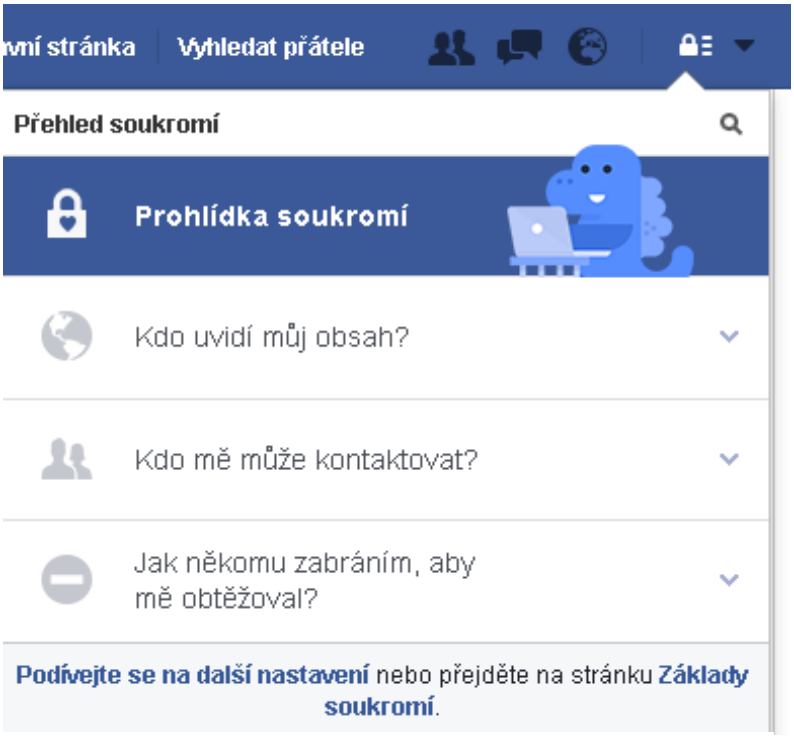


Obrázek č. 5 Možnost nastavení bezpečnosti a soukromí
Zdroj: Printscreen z https://twitter.com/settings/security

5.3.2 Facebook

Tato sociální síť, na rozdíl od konkurenčního Twitteru, má v nastavení soukromí o mnoho více možností úprav vašeho veřejného profilu, navíc veškeré nastavení jsou lokalizované do Českého jazyka. Zde bych představil některé důležité nastavení soukromí, které by měl zvážit každý uživatel sociální sítě. Facebook má pro nastavení soukromí velmi intuitivního průvodce, který vás provede celou řadou nastavení.

Do nastavení soukromí se lze dostat dvěma způsoby, oba plní tu samou funkci. První způsob nám zobrazí intuitivního průvodce pro prohlídku soukromí, nalezneme ho v pravém horním rohu jako ikonu visacího zámku (viz. Obrázek č. 6).



Obrázek č. 6 Průvodce pro nastavení soukromí
Zdroj: Printscreen z https://www.facebook.com/

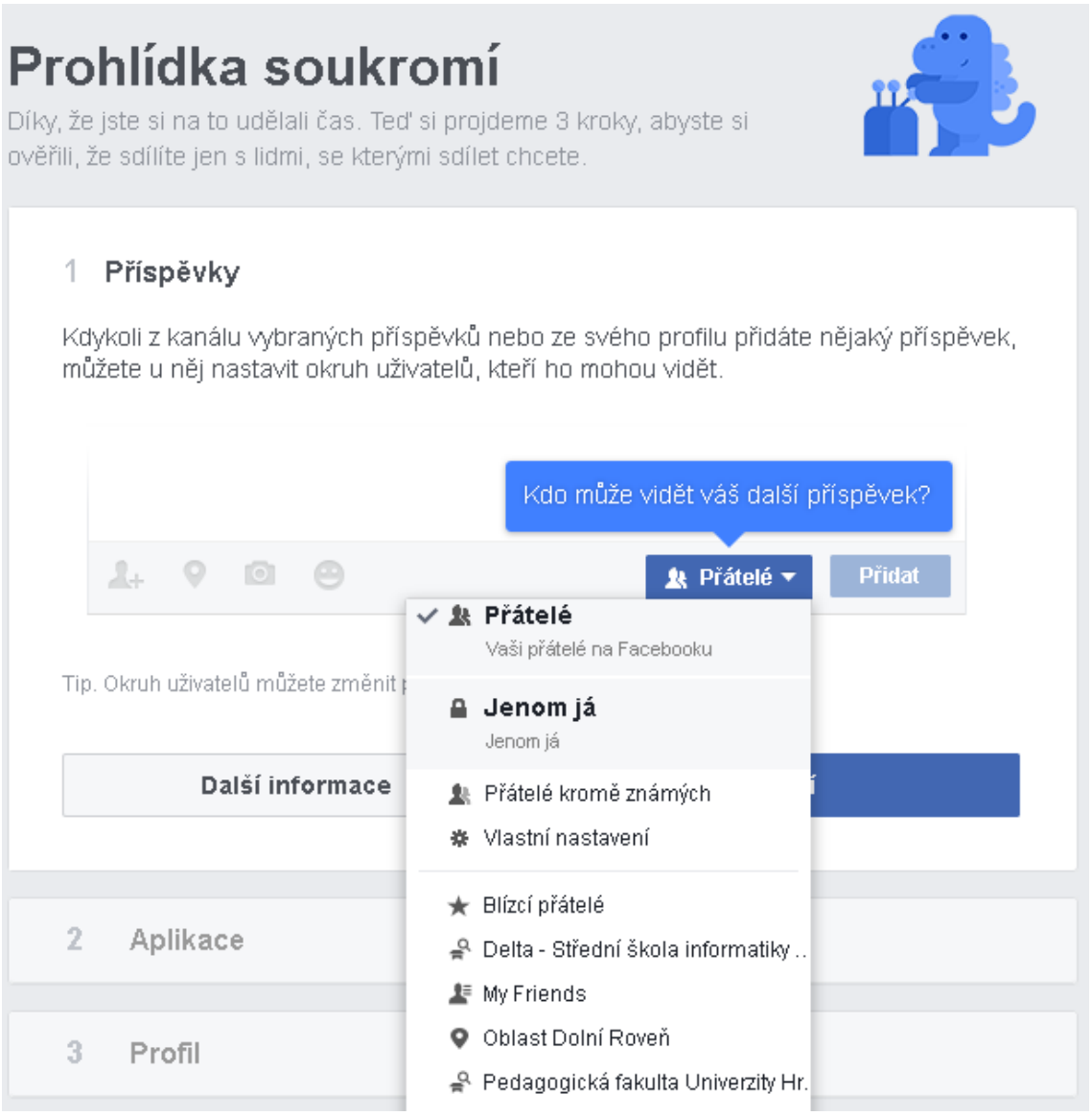
Po kliknutí na nabídku Prohlídka soukromí se zobrazí intuitivní průvodce, který ve třech krocích umožní nastavit naše základní nastavení soukromí. Prvním krokem je nastavení příspěvků, aneb „kdo může náš příspěvek zobrazit“. Zde jsou tři základní možnosti a jedna rozšiřující možnost komu umožníme, aby náš příspěvek na zdi viděl.

Veřejný – umožní zobrazit příspěvek komukoli, kdo zobrazí náš profil

Přátelé – váš sdílený obsah uvidí pouze lidé, které máte přidány do přátel

Jenom já – po tomto nastavení veškeré příspěvky, které publikujete, můžete vidět pouze vy

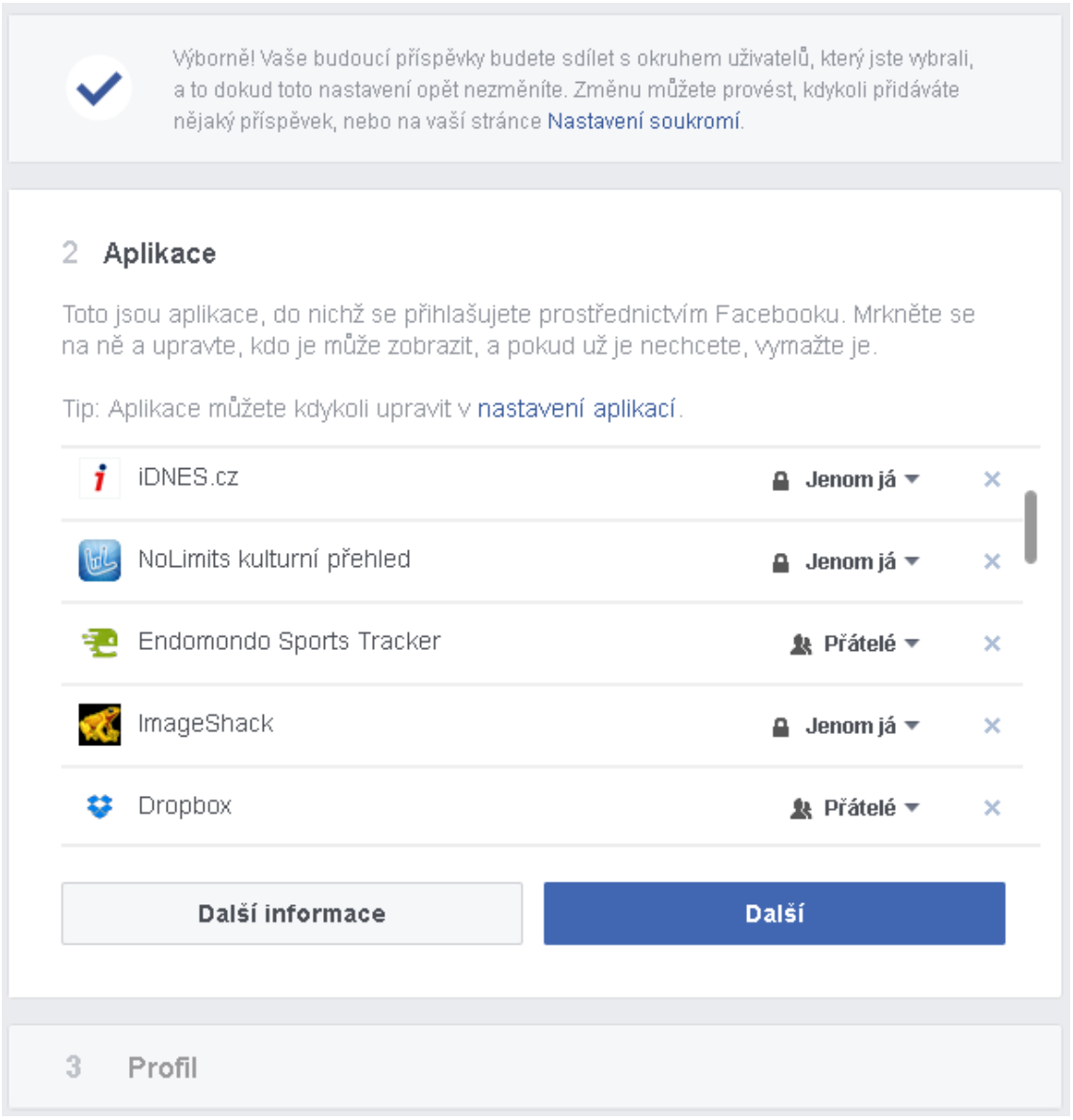
Další možnosti – v těchto možnostech si můžete úpravy, kdo uvidí váš příspěvek velmi specifikovat například vlastním nastavením, kde můžete přímo vypsat přátele, kterým se příspěvky můžou, nebo naopak nesmí zobrazovat. Dále je možnost nastavit zobrazení příspěvků podle lokality, nebo podle skupin přátel, které máte vytvořeny.



Obrázek č. 7 Možnosti nastavení zobrazování příspěvků
Zdroj:Printscreen z https://www.facebook.com

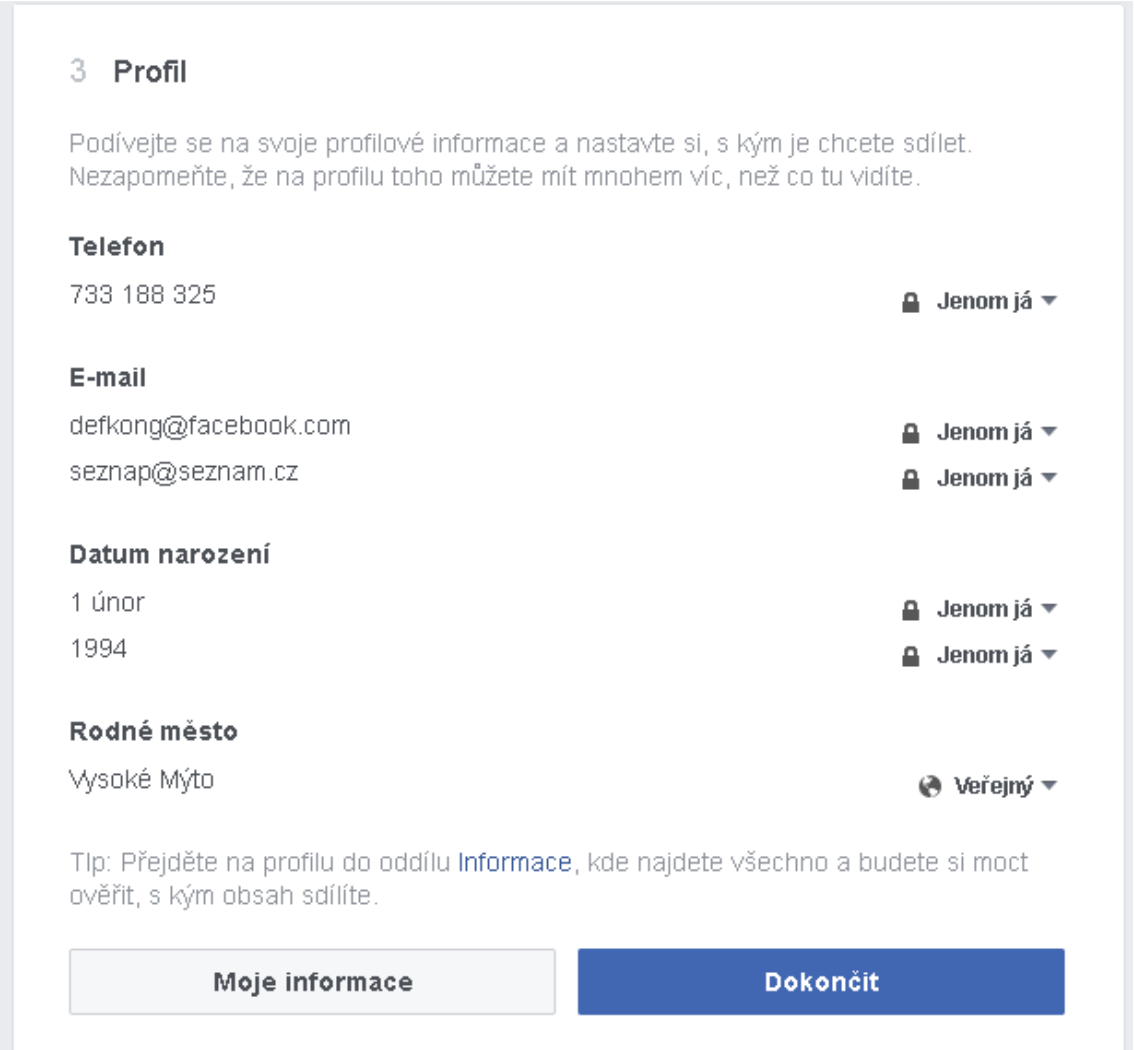
Po nastavení tohoto modulu klikneme na tlačítko další a přesuneme se do druhého kroku s nastavením aplikací. Zde můžeme nalézt souhrnný seznam aplikací, do nichž se přihlašujeme prostřednictvím Facebooku. Aplikace se netýkají pouze tzv. „Facebook aplikací“, ale i jiných webových domén, které mají pro

ulehčení přihlášení nabídku „přihlášení pomocí Facebooku". Zde si nastavíme, kdo může prohlížet aplikace, které využíváme podobně jako v nastavení příspěvků.



Obrázek č. 8 Nastavení zobrazování aplikací, které využíváme
Zdroj: Printscreen z https://www.facebook.com

Poslední třetí krok se zabývá nastavením profilu, kde najdeme profilové informace a můžeme si nastavit, s kým je chceme sdílet. Způsoby, jakými lze provést nastavení jsou stejné, jako v předchozích krocích. V tomto průvodci jsou jen základní nastavení, proto nás dále upozorňuje, že pokud chceme vidět vše, co s kým sdílíme, musíme do oddílu Informace. Následuje tlačítko Dokončit, po kterém jsme vyzváni pro častou kontrolu s kým obsah facebooku sdílíme a pro kontrolu dalšího nastavení soukromí navštívit Nastavení.

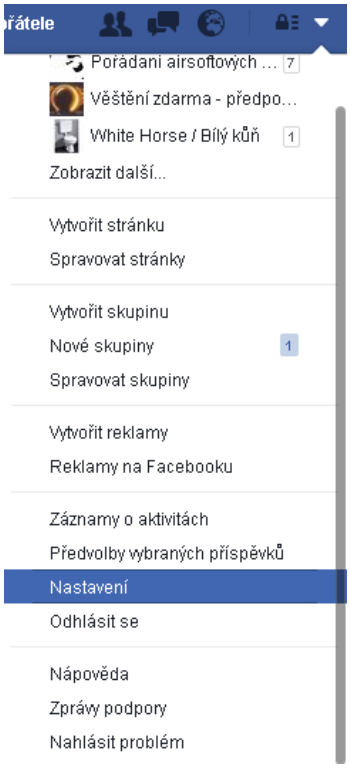


Obrázek č. 9 Nastavení zobrazování profilových informací
Zdroj: Printscreen z https://www.facebook.com

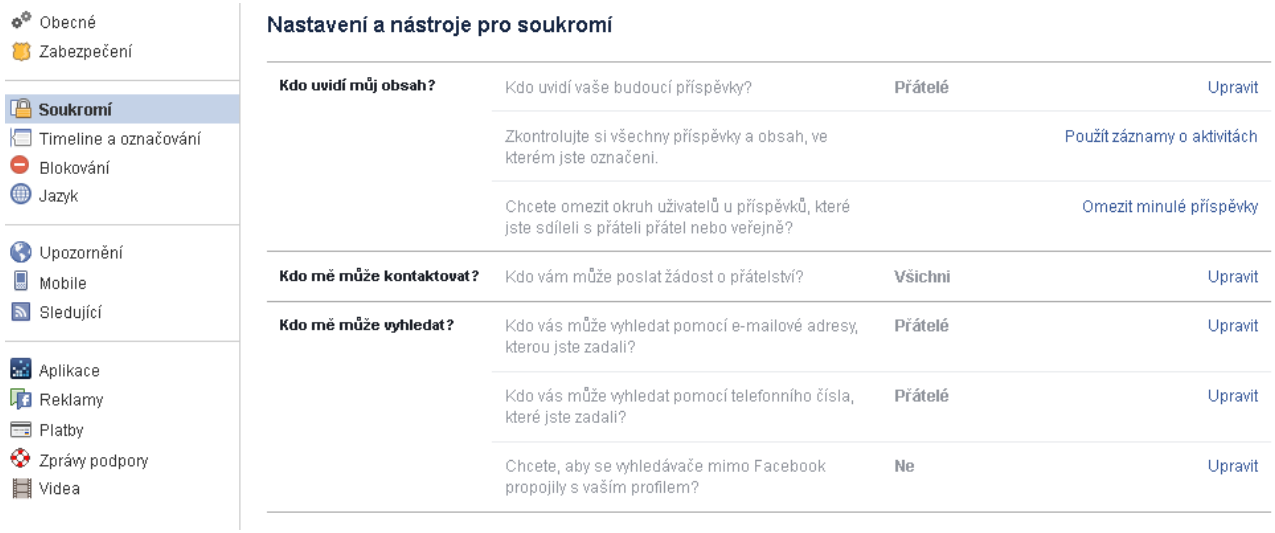
Další možnost nastavení soukromí se ukrývá přímo v nastavení, do kterého se dostaneme z hlavní stránky Facebooku, vpravo nahoře úplně poslední ikona šipka směřující dolů (viz. Obrázek č. 10). Nastavení se nachází jako páté od zdola, kde se nám po kliknutí zobrazí kompletní nastavení naší Facebookové stránky. V tuto chvíli se budeme zabývat pouze nastavením soukromí a ochranou dat, které najdeme v levém menu pod položkami Soukromí, Timeline a označování a Blokování.

Soukromí – pomocí tohoto modulu lze nastavit „Kdo uvidí můj obsah?“, jak už bylo zmíněno výše, jedná se o nastavení toho, kdo může vidět vaše příspěvky. Dále lze nastavit možnosti „Kdo mě může kontaktovat?“, zde jsou pouze dvě možnosti: všichni a přátelé přátel. Jako poslední v tomto modulu je nastavení „Kdo mě může vyhledat?“, jedná se o nastavení, pomocí jakých prostředků vás jiný člověk může

vyhledávat, nalézají se zde tři editovatelné možnosti: podle emailové adresy, telefonního čísla, nebo pomocí jiných internetových vyhledávačů.



Obrázek č. 10 Přehled nastavení Facebooku
Zdroj: Printscreen z https://www.facebook.com



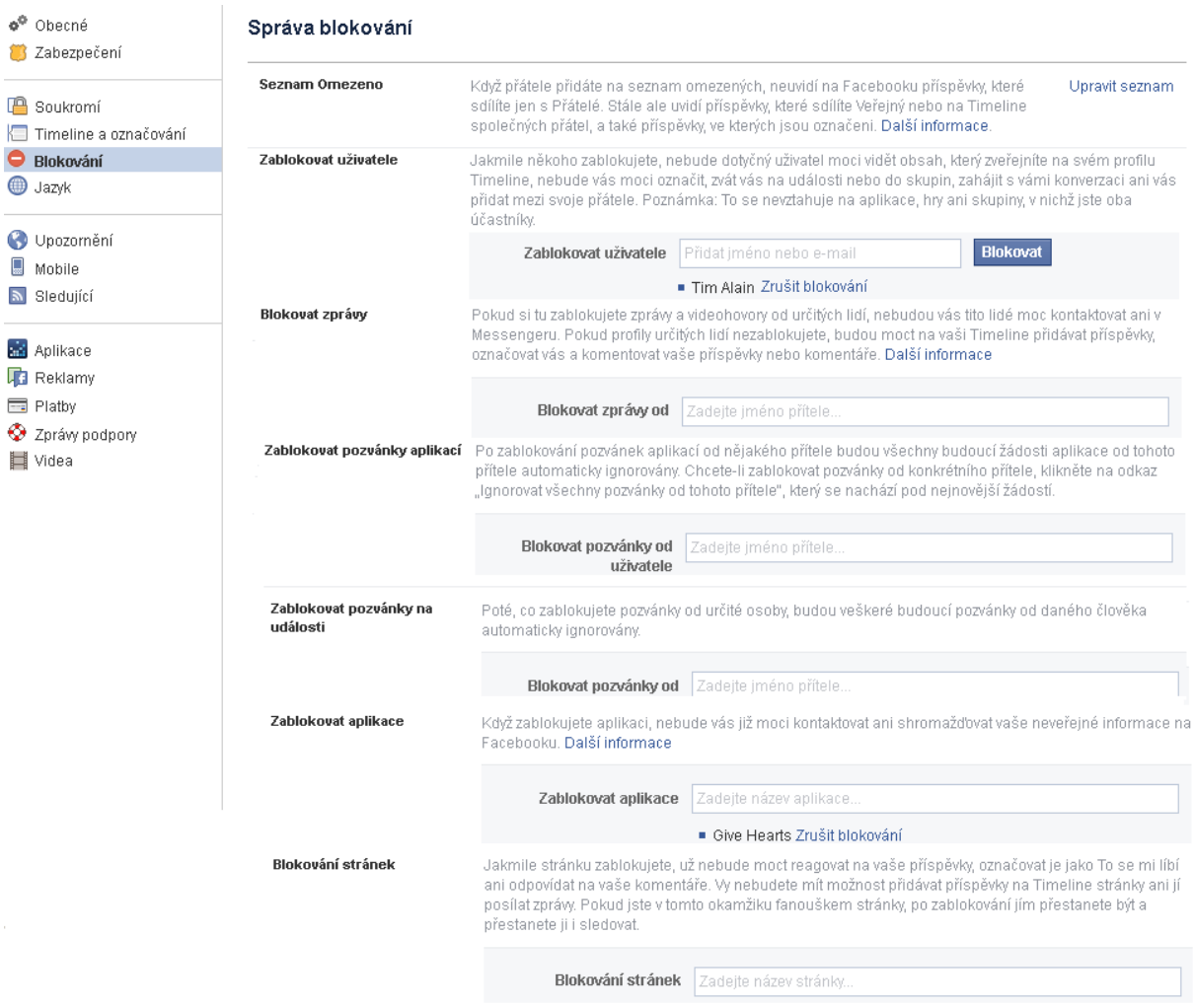
Obrázek č. 11 Nástroje pro nastavení soukromí
Zdroj: Printscreen z https://www.facebook.com/settings?tab=privacy

Timeline a označování – tento modul se rozděluje na tři možnosti nastavení. První možností je „Kdo může přidávat obsah na moji Timeline?“, jedná se o nastavení, kterým nastavíme, kdo může přidat na naši zeď příspěvek a následně můžeme zapnout či vypnout kontrolu příspěvků, ve kterých nás přátelé můžou označit, nebo se pokusí přidat příspěvek na naši zeď.

Druhá možnost nastavení je „Kdo uvidí obsah na mojí Timeline?“, jde o nastavení, se kterým jsme se setkali už výše v průvodci nastavení soukromí s rozšířenou možností, že si můžeme zobrazit profil, buď jak vypadá veřejně, nebo můžeme zobrazit, jak vypadá pro určitého uživatele. Třetí poslední možnost „Jak můžu spravovat označení, která lidé přidají, a návrhy na označení?“ se týká označování v příspěvcích, či fotkách vaší osoby. Zde je také možnost kontroly těchto akcí.

Obrázek č. 12 Možnosti nastavení Timeline a označování
Zdroj: Printscreen z https://www.facebook.com/settings?tab=timeline

Blokování – jedná se o poslední modul, jak už z názvu vypovídá, o blokování uživatelů Facebooku, příchozích zpráv, aplikací, pozvánek na události a stránek. Stačí do textových oken vepsat, co chceme blokovat a potvrdit. Akce je možno vrátit zpět.



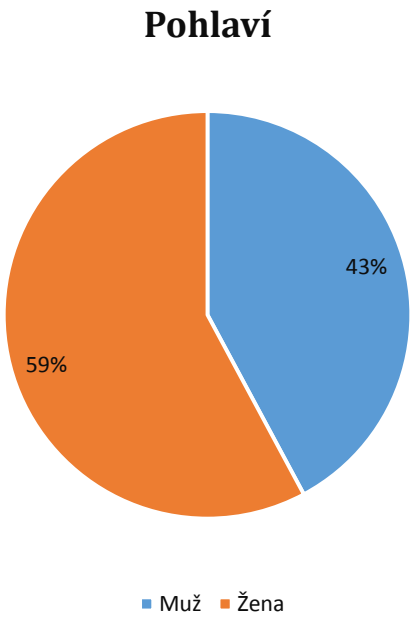
Obrázek č. 13 Možnosti Blokování
Zdroj: Printscreen z https://www.facebook.com/settings?tab=blocking

Je na každém uživateli jakou ochranu svých osobních informací si zvolí. V této kapitole mi šlo především o rozšíření vědomostí a možností v oblasti zabezpečení na sociálních sítích. Postupem času dostává sociální síť Facebook nový kabát, proto se mohou jednotlivé nastavení lišit s předchozími i následujícími verzemi.

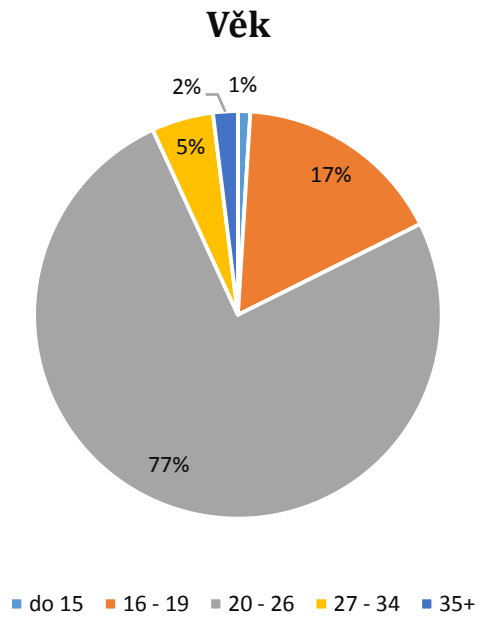
6 Dotazník

Cílem mé závěrečné práce bylo vytvořit dotazník (viz. Příloha č. 1), který by měl zkoumat uvědomění internetových uživatelů o možnostech zneužití osobních dat a o tom zdali znají a využívají možnosti ochrany soukromí a osobních dat na sociálních sítích a internetu celkově.

V dotazníku bylo celkem čtrnáct uzavřených otázek a vyplnilo jej celkem sto dva respondentů. Pro vytvoření a propagaci dotazníku jsem použil server Survio.cz. Cílem bylo získání dat od různých věkových kategorií a sociálních skupin pro zjištění co nejobecnějšího přehledu o dané problematice.

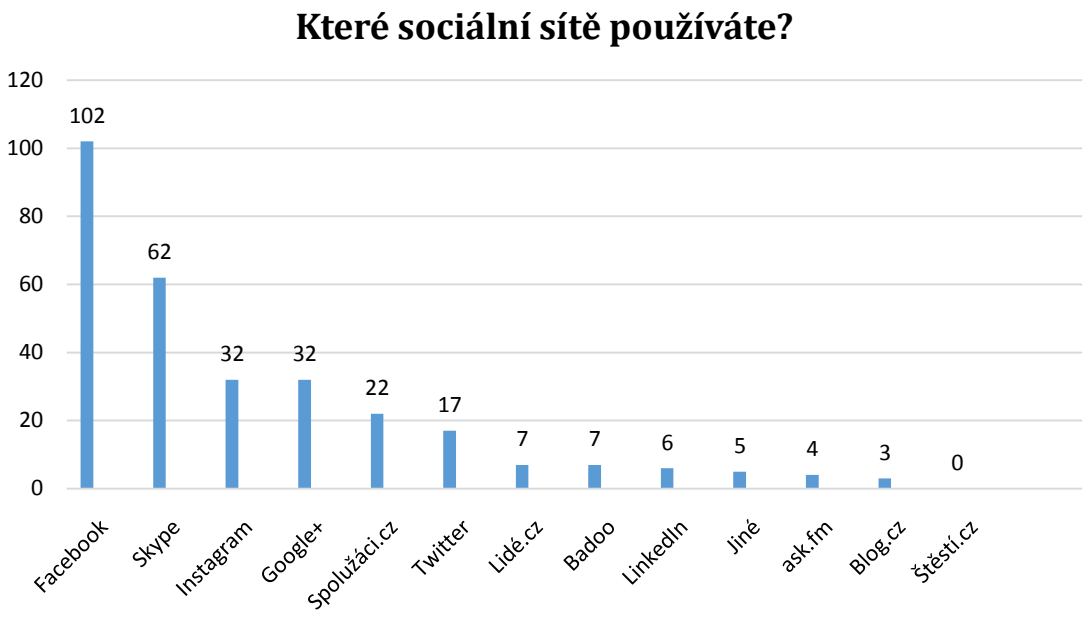


Graf č. 1 Pohlaví



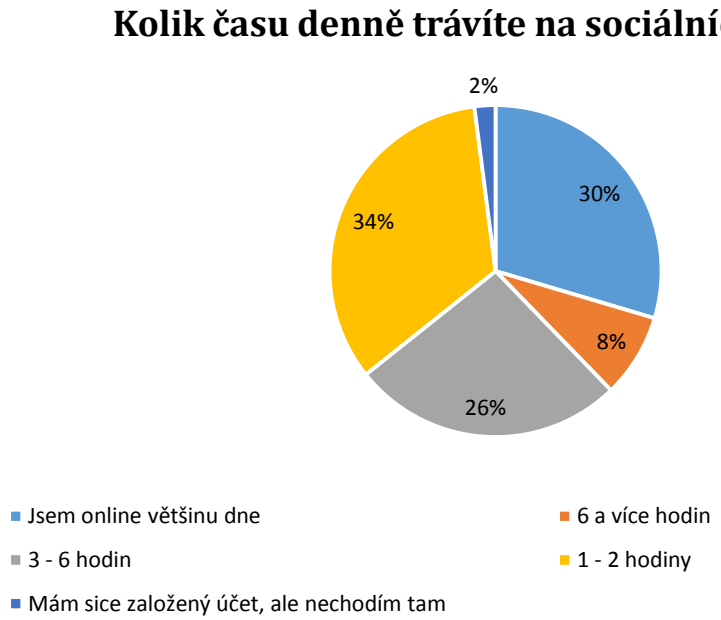
Graf č. 2 Věk

Z těchto dvou prvních grafů můžeme určit, že dotazník vyplnila mírná převaha žen oproti mužům a že se jednalo spíše o mladou generaci dospělých respondentů.



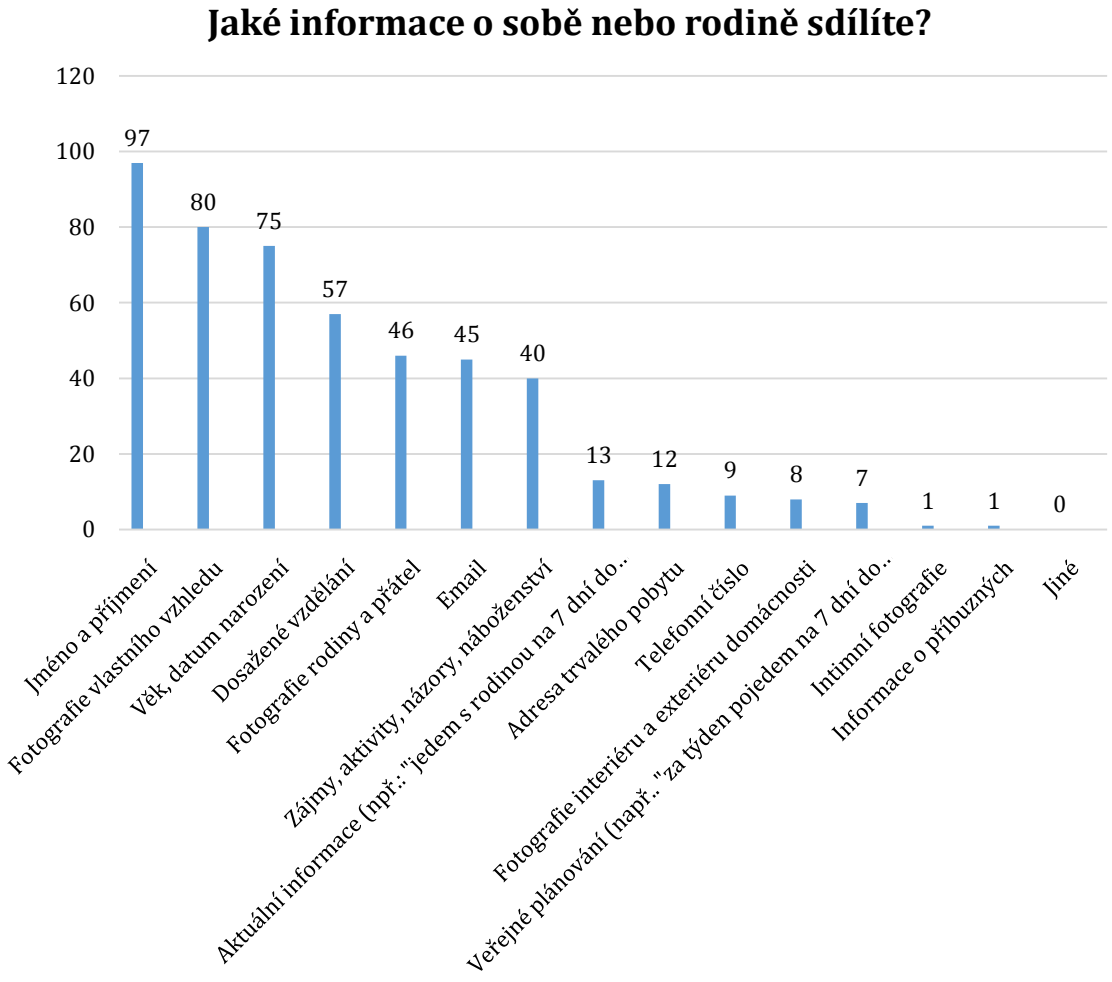
Graf č. 3 Používání sociálních sítí

Z tohoto grafu můžeme určit, že 100% dotázaných využívá sociální síť Facebook k další nejpoužívanější sociální síti patří Skype, který primárně sloužil jako komunikátor, ale postupně se rozrostl do nynější podoby. Mezi jinými možnostmi dotázaní uváděli například, ruskou sociální síť ВКонтакте (VKontakte), Vinted a Snapchat.



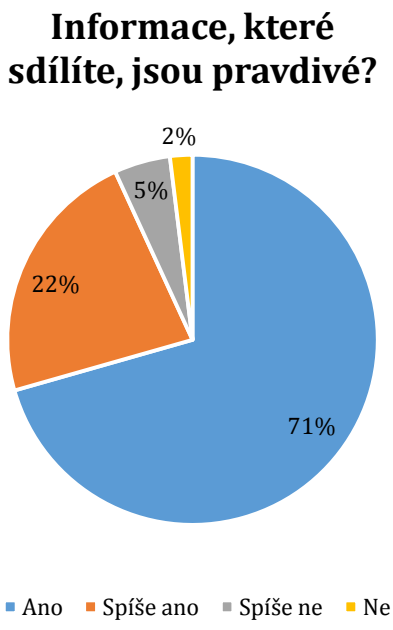
Graf č. 4 Čas trávený na sociálních sítích

Z Grafu č. 4 můžeme vysledovat a dopočítat, že zhruba 64% dotázaných svůj všední den věnuje z jedné třetiny sledováním dění na sociálních sítích. Samozřejmě musíme brát v potaz, přihlášení uživatelů na mobilních zařízeních, kde jsou prakticky aktivní i přes noc a systém kontrolující, zdali vám nepřišla zpráva, nebo upozornění.

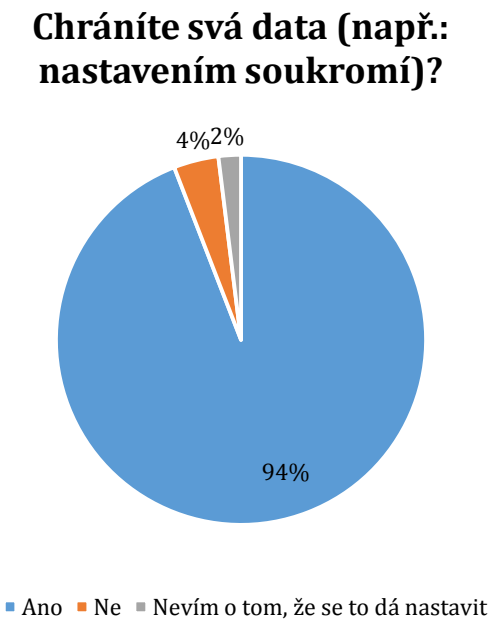


Graf č. 5 Sdílení informací

Z tohoto grafu můžeme jasně vidět, které osobní údaje respondenti sdílí v rámci sociálních sítí. Jedná se o známku toho, že osobní informace jsou jako celek vystaveny pro možnou další manipulaci, nebo zneužití.

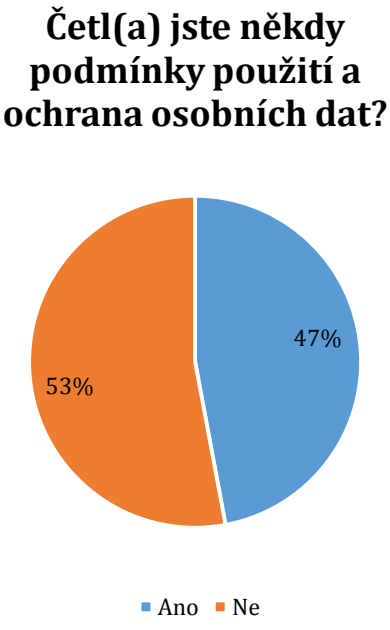


Graf č. 6 Pravdivost informací

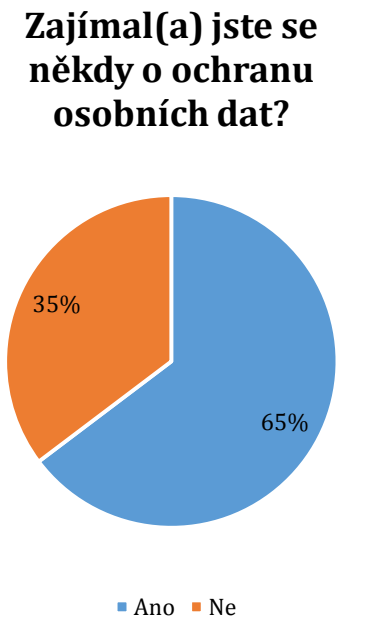


Graf č. 7 Využití nastavení soukromí

Tyto dva grafy nám sdělují, že informace, které sdílíme, jsou z většiny pravdivé a následně vidíme, že většina respondentů využívá nastavení soukromí na sociální síti. Bohužel se v takovém počtu najdou i tací, kteří vůbec toto zabezpečení nevyužívají, nebo o něm nevědí.

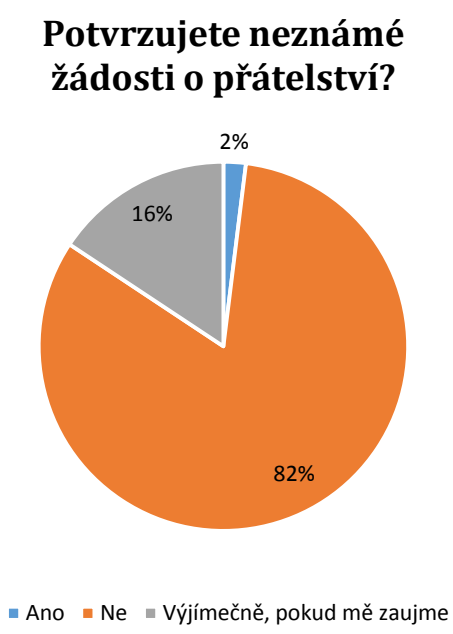


Graf č. 8 Použití a ochrana osobních dat

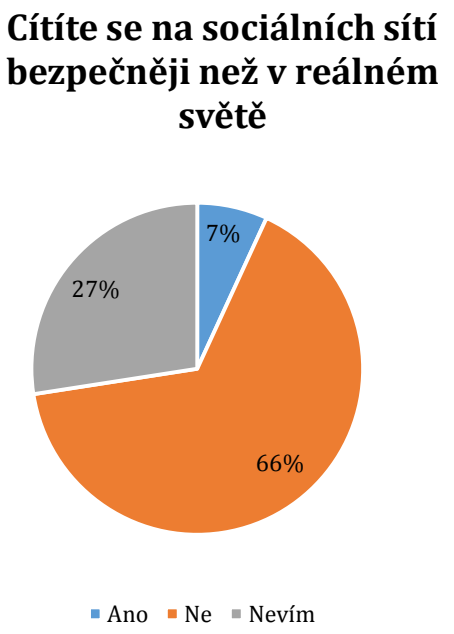


Graf č. 9 Zájem o ochranu osobních dat

Tyto dva grafy jsou v celku pozitivní vzhledem k tomu, že skoro 50% respondentů si dalo práci s přečtením podmínek použití a ochranu osobních dat na sociálních sítích a dále, že polovina dotázaných se o tuto problematiku zajímá.



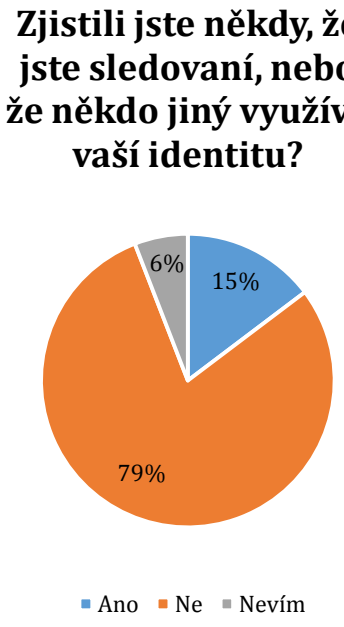
Graf č. 10 Potvrzení žádosti o přátelství



Graf č. 11 Pocit bezpečnosti

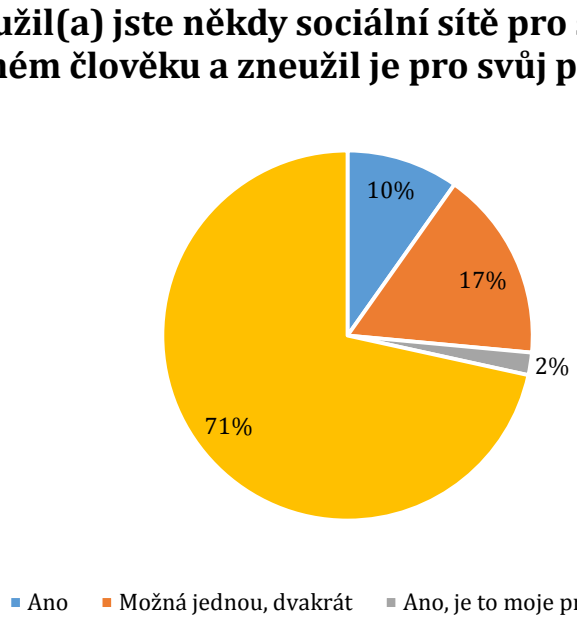
Značná část dotazovaných v Grafu č. 10 vyplnila, že si potvrzuje přátelství od uživatelů, které vlastně vůbec nezná, ale nějakým způsobem ho zaujmou. U mužů může jít o ženy, které mají atraktivní profilovou fotografii a u žen fotky svalnatých mužských postav. Přidáním této osoby se vystavují riziku vystavení svých informací nebezpečnému uživateli. V Grafu č. 11 nás může zarazit, že 27% dotazovaných nedokáže říci, jestli se cítí bezpečně na sociální síti.

Graf č. 12 Úvaha o úniku osobních dat na internetu



Graf č. 13 Zjištění o sledování nebo využívání

V takto položených otázkách z grafů č. 12 a 13 jsem chtěl zjistit, jestli se respondenti zamýšleli nad ohrožením díky zveřejnění osobních údajů, které uvedli v otázce zaměřenou na to, co sdílí a dále, jestli se už někdy se zneužitím přímo setkali. Z odpovědí jednoznačně vyplívá, že velká část o problematice uvažovala, ale našli se i někteří, které to vůbec nezajímá a dále, že se poměrná část respondentů setkala se sledováním, nebo využitím jejich identity někým jiným.



Graf č. 14 Využitá sběru dat

Na tomto posledním grafu můžeme vidět značné procento respondentů, kteří využili, nebo využívají informace ze sociálních sítí pro své vlastní potřeby.

Závěr

Ohrožení osobních údajů se může týkat každého z nás a je jen na nás, jaké prostředky použijeme pro prevenci a ochranu našich citlivých informací. Jedná se především o předání počítačové a internetové gramotnosti mladším i starším ročníkům a vést je k možnostem zabezpečení našich dat.

O aktuální problematiku jsem se velice zajímal, ještě než jsem si ji zvolil jako téma k závěrečné práci, proto jsem čerpal i z vlastních ověřených pramenů a ze zkušenostní. Systémy pro sběr a uchovávání osobních dat se dále rozšiřují a zlepšují, proto jsem se snažil svou práci vést v duchu nynějších aktuálních informací.

Svou práci jsem pojal jako popis různých možností, jak získat a zneužívat osobní údaje pomocí sociálních sítí a jiných technologií a dále jsem vyjmenoval možnou ochranu osobních dat v sociálních sítích, jako je Facebook a Twitter. Cílem této práce bylo provést rozbor potencionálních útoků na osobní data a jejich zneužití skrze sociální sítě a informační systémy, dále poukázat na to, jak jsou osobní data snadno dostupná jiným uživatelům internetu a seznámení s možným bezpečnostním rizikem a navrhnout možnou ochranu. Poslední cíl mé práce bylo sestavit dotazník, kterým měl za úkol zjistit povědomí uživatelů internetu o tom, co zveřejňují a jestli si uvědomují jisté riziko s tím spojené.

Myslím, že vytýčené cíle mé závěrečné práce byly splněny a z dotazníku jsem zjistil, že uživatelé sdílí velké množství informací, ale většina z mých respondentů se zajímá a zabezpečuje své údaje pomocí nástrojů pro ochranu soukromí.

Použitá literatura

1. **BAWDEN DAVID a ROBINSON LYN.***Introduction to information science*. London: Facet publishing, 2012, 351 s. ISBN 978-1-55570-861-0.

2. **CEJPEK, Jiří.***Informace, komunikace a myšlení: úvod do informační vědy*. Praha: Karolinum, 1998.219 s. ISBN 80-7184-767-4.

3. **Zákon č. 101/2000 a) Sb. o ochraně osobních údajů a o změně některých zákonů** [online]. 2000 [cit. 2016-05-16]. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-101

4. **MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK**. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). str. 21 ISBN 978-80-7357-322-5.

5. **MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK**. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). str. 23 ISBN 978-80-7357-322-5.

6. **Zákon č. 101/2000 b) Sb. o ochraně osobních údajů a o změně některých zákonů** [online]. 2000 [cit. 2016-05-16]. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-101

7. **MOLNÁR, Zdeněk.***Podnikové informační systémy*. Vyd. 2., přeprac. V Praze: České vysoké učení technické, 2009. str. 13 ISBN 978-80-01-04380-6.

8. **SODOMKA, Petr.***Informační systémy v podnikové praxi*. Brno: ComputerPress, 2006. str. ISBN 80-251-1200-4.

9. **APICS.***APICS Dictionary* [online]. Chicago: APICS, 2013 [cit. 2016-05-16]. Dostupné z: http://www.apics.org/dictionary/dictionary-information?ID=2012.0

10. **ZADRAŽILOVÁ, Iva.***Nebezpečí zneužití osobních informací v době globálního monitoringu s přihlédnutím k možnostem ochrany soukromí* [online]. Brno, 2009 [cit. 2016-05-16]. Dostupné z: http://is.muni.cz/th/6943/ff_m/Diplomova_prace.pdf. Diplomová práce. Masarykova univerzita. Vedoucí práce PhDr. Michal Lorenz.

11. **OPLETALOVÁ, Vendula.***OCHRANA OSOBNÍCH ÚDA JŮ V INFORMAČNÍM SYSTÉMU* [online]. Brno, 2007 [cit. 2016-05-16]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=1102. Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Vedoucí práce JUDr. TOMÁŠ SOUKUP.

12. **Patria.***Právo být zapomenut" již rok platí i v Česku* [online]. 2015 [cit. 2016-05-16]. Dostupné z: https://www.patria.cz/pravo/2906800/pravo-byt-zapomenut-jiz-rok-plati-i-v-cesku.html

13. ***Google: Transparency Report*** [online]. 2014 [cit. 2016-05-16]. Dostupné z: https://www.google.com/transparencyreport/removals/europeprivacy/

14. **NEUWIRT, Karel.***Informační společnost ve zdravotnictví a elektronické karty - II* [online]. [cit. 2016-05-17]. Dostupné z: http://www.zdrav.cz/web/mpz/mpz4704__v__neuwirt_k__inf_sys.htm

15. **Policie ČR.***Počítačová kriminalita* [online]. [cit. 2016-05-17]. Dostupné z: http://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

16. **Úřad pro ochranu osobních údajů**. *Úřad* [online]. [cit. 2016-05-17]. Dostupné z: https://www.uoou.cz/urad/ds-1059/p1=1059&cookiesAllowed=1

17. **HOAX.***Co je to hoax* [online]. 2000 [cit. 2016-05-17]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

18. **Zákony od centrum.cz.***Trestní zákoník: § 357* [online]. [cit. 2016-05-17]. Dostupné z: http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-10-dil-6-paragraf-357

19. **JAMES, Lance.***Phishing bez záhad*. Praha: Grada, 2007. str. 28 ISBN 978-80-247-1766-1.

20. **Aktuálně.cz.***Hackeři míří na klienty Komerční banky, chtějí přístupy* [online]. 2015 [cit. 2016-05-17]. Dostupné z: http://zpravy.aktualne.cz/finance/hackeri-miri-na-klienty-komercni-banky-chteji-pristupy/r~44c33b16ab9211e498be002590604f2e/

21. **Bezpecný internet**. *Phishing a pharming* [online]. [cit. 2016-05-17]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

22. **Správa sítě: slovník pojmů.***Sniffing* [online]. [cit. 2016-05-18]. Dostupné z: http://www.sprava-site.eu/sniffing/

23. **Zákony od centrum.cz.***Trestní zákoník: § 182* [online]. [cit. 2016-05-18]. Dostupné z: http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-2-dil-2-paragraf-182

24. **Policie ČR.***SKIMMING* [online]. [cit. 2016-05-18]. Dostupné z: http://www.policie.cz/clanek/skimming.aspx

25. **ŠAFÁŘ, Daniel.***Phishing a další formy útoku.* In: *ITBIZ* [online]. 2008 [cit. 2016-05-18]. Dostupné z: http://www.itbiz.cz/phishing-check-point

26. **ŠKOPEK, Pavel.***Komunikace českých parlamentních stran na internetové sociální síti Facebook* [online]. Plzeň, 2012 [cit. 2016-05-18]. Dostupné z: https://otik.uk.zcu.cz/bitstream/handle/11025/12698/BAKALARSKA%20PRACE%20-%20PAVEL%20SKOPEK.pdf?sequence=1. Bakalářská. Západočeská univerzita v Plzni. Vedoucí práce PhDr. Přemysl Rosůlek, Ph.D.

27. **Digital Marketing Ramblings: DMR.***200 Amazing Facebook Statistics (April 2016): Facebook stats* [online]. 2016 [cit. 2016-05-18]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/3/

28. **TATJANA, Taraszow.**Disclosureofpersonal and contactinformation by youngpeople in socialnetworkingsites: Ananalysisusing Facebook profiles as anexample. In: *International Journalof Media &CulturalPolitics*. 2010, str. 89 ISSN 1740-8296 (Print); ISSN 2040-0918 (Online).

29. **E-Bezpečí.***Stručný přehled vybraných podmínek užívání Facebooku* [online]. 2013 [cit. 2016-05-18]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/socialni-sit/587-struny-pehled-vybranych-podminek-uivani-facebooku

30. **Facebook.***Zásady používání dat* [online]. 2015 [cit. 2016-05-18]. Dostupné z: https://www.facebook.com/privacy/explanation

31. **Facebook.***Prohlášení o právech a povinnostech* [online]. 2015 [cit. 2016-05-18]. Dostupné z: https://www.facebook.com/legal/terms/

32. **PCWorld.***Co je sociální inženýrství?: 1. díl*[online]. 2012 [cit. 2016-05-19]. Dostupné z: http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-1-dil-44361

33. **Bezpečný internet.***Krádež identity a jak se jí bránit* [online]. [cit. 2016-05-19]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

34. **E-bezpečí.***Krádež identity* [online]. 2012 [cit. 2016-05-19]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/502-krade-identity

35. **E-bezpečí.** *Co je to stalking a cyberstalking* [online]. 2008 [cit. 2016-05-19]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23

36. **Eprávo.***Cyberstalking* [online]. 2013 [cit. 2016-05-19]. Dostupné z: http://www.epravo.cz/top/clanky/cyberstalking-91552.html

37. **KTD - Česká terminologická databáze knihovnictví a informační vědy.***Data mining* [online]. [cit. 2016-05-17]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00000/00/000000088.htm

38. **PETR, Pavel.***Data Mining*. Vyd. 3. Pardubice: Univerzita Pardubice, 2010-. str. 7 ISBN 978-80-7395-325-6.

39. **Technologie pro mobilní komunikaci.***Historie systému GSM* [online]. [cit. 2016-05-24]. Dostupné z: http://tomas.richtr.cz/mobil/bunk-gsm.htm

40. **PROBIN.***Způsoby odposlechu mobilní komunikace* [online]. [cit. 2016-05-24]. Dostupné z: http://www.probin.cz/zpusoby-odposlechu-mobilni-komunikace

41. **Mobil.Idnes.cz.** *Odposlech mobilů je opět snazší. Kvůli chybám v letitém protokolu* [online]. 2015 [cit. 2016-05-24]. Dostupné z: http://mobil.idnes.cz/odposlech-mobilu-protokol-ss7-dkz-/mob_tech.aspx?c=A141228_215236_mob_tech_vok

42. **Spyera.***Spyphone Android App* [online]. [cit. 2016-05-24]. Dostupné z: http://spyera.com/cs/android-%C5%A1pion%C3%A1%C5%BEn%C3%AD-app/

43. **CHIP.***Dozor prostřednictvím rozpoznávání tváří* [online]. 2012 [cit. 2016-05-24]. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/vydani/r-2012/chip-07-2012/dozor-rozpoznavani-tvari/

44. **KIVI - Knihovnictví a informační věda informuje.***Hrozba univerzálního monitoringu* [online]. [cit. 2016-05-24]. Dostupné z: http://www.phil.muni.cz/kivi/smarda/hum.html

45. **Praha.Idnes.cz.***V Praze bude více kamer, doplní je i program na rozpoznávání tváří* [online]. 2016 [cit. 2016-05-24]. Dostupné z: http://praha.idnes.cz/v-praze-bude-vice-kamer-ale-take-program-na-rozpoznavani-tvari-p6n-/metro.aspx?c=A160210_180621_praha-metro_lupo

46. **GPS - Stránka o satelitní navigaci.***GPS* [online]. [cit. 2016-05-25]. Dostupné z: http://gps.slansko.cz/

47. **Pavel Škopek.***Techbox: jak funguje GPS, které vás dovede k vašemu cíli?* [online]. Mobilenet, 2013 [cit. 2016-05-25]. Dostupné z: https://mobilenet.cz/clanky/techbox-jak-funguje-gps-ktere-vas-dovede-k-vasemu-cili-11200

48. **SVĚTANDROIDA.***Jak funguje zaměření polohy pomocí GPS?* [online]. 2015 [cit. 2016-05-25]. Dostupné z: https://www.svetandroida.cz/gps-princip-201503

49. **Tomáš Slavíček.***Geotagging: Druhá strana mince* [online]. DIGIarena.cz, 2012 [cit. 2016-05-25]. Dostupné z: http://digiarena.e15.cz/geotagging-druha-strana-mince

50. **Úřad pro ochranu osobních údajů.***Zásady ochrany osobních údajů* [online]. [cit. 2016-05-25]. Dostupné z: https://www.uoou.cz/zasady-ochrany-osobnich-udaju/ds-2615/p1=2615

51. **Jak na internet.***Ochrana osobních údajů* [online]. [cit. 2016-05-25]. Dostupné z: http://www.jaknainternet.cz/page/1183/ochrana-osobnich-udaju/

52. **Dsl.cz**. *Jak si chránit soukromí na internetu (2): Webové prohlížeče* [online]. [cit. 2016-05-25]. Dostupné z: http://www.dsl.cz/jak-na-to/jak-si-chranit-soukromi-na-internetu-webove-prohlizece

Seznam obrázků

Seznam grafů

Přílohy

Příloha č. 1 Dotazník

Zneužívání osobních dat a možnosti jejich ochrany

1) Pohlaví
    - Muž
    - Žena
2) Věk
    - Do 15
    - 16 – 19
    - 20 – 26
    - 27 – 54
    - 55+

3) Které sociální sítě používáte? (lze zaškrtnout více odpovědí)

- ☐ Facebook
- ☐ Twitter
- ☐ Skype
- ☐ Instagram
- ☐ Google+
- ☐ Linkedln
- ☐ Badoo
- ☐ Ask.fm
- ☐ Spolužáci.cz
- ☐ Lidé.cz
- ☐ Blog.cz
- ☐ Štěstí.cz
- ☐ Jiné:

4) Kolik času denně trávíte na sociálních sítích?

- o Jsem online většinu dne
- o 6 a více hodin
- o 3 – 6 hodin
- o 1 – 2 hodiny
- o Mám sice založený účet, ale nechodím tam

5) Jaké informace o sobě nebo rodině sdílíte (lze zaškrtnout více odpovědí)

- Jméno a příjmení
- Věk, datum narození
- Adresa trvalého pobytu
- Telefonní číslo
- Email
- Dosažené vzdělání
- Zájmy, aktivity, názory, náboženství
- Fotografie vlastního vzhledu
- Fotografie rodiny a přátel
- Fotografie interiéru a exteriéru domácnosti
- Intimní fotografie
- Informace o příbuzných
- Aktuální informace (např.: "jedem s rodinou na 7 dní do Alp")
- Veřejné plánování (např.. "za týden pojedem na 7 dní do Alp")
- Jiné:

6) Informace, které sdílíte, jsou pravdivé?

- Ano
- Spíše ano
- Spíše ne
- Ne

7) Chráníte svá data (např.: nastavením soukromí)?

- Ano
- Ne
- Nevím o tom, že se to lze nastavit

8) Četl(a) jste někdy podmínky použití a ochrana osobních dat?

- Ano
- Ne

9) Zajímal(a) jste se někdy o ochranu osobních dat?
    - Ano
    - Ne
10) Potvrzujete neznáme žádosti o přátelství?
    - Ano
    - Ne
    - Výjimečně, pokud mě zaujme
11) Cítíte se na sociálních sítích bezpečněji než v reálném světě?
    - Ano
    - Ne
    - Nevím
12) Přemýšlel(a) jste někdy o tom, že vás pomocí vámi uveřejněných informací může někdo sledovat, nebo o vás sbírat informace?
    - Ano
    - Ne
    - Nevím, nikdy jsem o tom nepřemýšlel(a)
13) Zjistil(a) jste někdy, že jste sledován, nebo že někde jiný využívá vaší identitu?
    - Ano
    - Ne
    - Nevím
14) Využil(a) jste někdy sociální sítě pro sběr dat o jiném člověku a zneužil je pro svůj prospěch?
    - Ano
    - Možná jednou, dvakrát
    - Ano, je to má práce
    - Ne