VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ANALÝZA RIZIKOVÉHO CHOVÁNÍ UŽIVATELŮ SOCIÁLNÍ SÍTĚ FACEBOOK

ANALYSIS OF RISK BEHAVIOUR OF SOCIAL NETWORK FACEBOOK USERS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JAN ONDRA
AUTHOR

VEDOUCÍ PRÁCE — doc. RNDr. JIŘÍ KROPÁČ, CSc.
SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ondra Jan

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Analýza rizikového chování uživatelů sociální sítě Facebook

v anglickém jazyce:

Analysis of Risk Behaviour of Social Network Facebook Users

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

HINDLS, R., S. HRONOVÁ a J. SEGER. Statistika pro ekonomy. 6. vyd. Praha: Professional Publishing, 2006. 415 s. ISBN 80-86419-99-1.
KOZÁK, J., J. ARLT a R. HINDLS. Úvod do analýzy ekonomických časových řad. 1. vyd. Praha: VŠE, 1994. 208 s. ISBN 80-7079-760-6.
KROPÁČ, J. Statistika B. 2. vyd. Brno: FP VUT, 2009. 151 s. ISBN 978-80-214-3295-6.
SEGER, J. Statistika v hospodářství. 1. vyd. Praha: ETC Publishing, 1998. 636 s. ISBN 80-86006-5.

Vedoucí bakalářské práce: doc. RNDr. Jiří Kropáč, CSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 26.05.2013

Abstrakt

Tématem této bakalářské práce je analýza chování uživatelů internetové sociální sítě Facebook z hlediska bezpečnosti. Tato analýza bude provedena na základě vlastního dotazníkového šetření. První část práce je věnována teoretickým východiskům z oboru statistiky, sociologického výzkumu a zásad bezpečného využívání internetu. Druhá část práce obsahuje praktickou realizaci sociologického průzkumu a dotazníkového šetření včetně statického zpracování získaných dat a vyvození závěrů a doporučení.

Abstract

Theme of this bachelor's thesis is analysis of Facebook social network users' behaviour from the security aspect. This analysis will be performed based on self created question-form. First part of this bachelor's thesis is dedicated to theoretical resources of statistics, sociological research and principles of safe use of internet. Second part of this bachelor's thesis contains practical implementation of sociological research and question-form including statistical processed of observed results and drawn of conclusions and recommendations.

Klíčová slova

Statistika, statistická analýza, sociologický průzkum, dotazníkové šetření, Facebook, bezpečnost, internet

Key words

Statistics, statistic analysis, sociological research, question-form, Facebook, security, internet

Bibliografická citace mé práce

ONDRA, J. *Analýza rizikového chování uživatelů sociální sítě Facebook*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 66 s. Vedoucí bakalářské práce doc. RNDr. Jiří Kropáč, CSc..

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 22. května 2013

.....

podpis studenta

Poděkování

Děkuji vedoucímu své bakalářské práce doc. RNDr. Jiřímu Kropáčovi, CSc. za odborné vedení, cenné rady a připomínky při zpracování bakalářské práce. Rád bych poděkoval Vlastimilovi Veselému za významnou pomoc při vytváření elektronické verze dotazníku. Dále bych chtěl poděkovat rodině a všem, kteří mě během mého studia a psaní bakalářské práce podporovali.

Obsah

Úvod

Během posledních několika let se u nás sociální síť Facebook stala doslova fenoménem. Svůj profil má na této sociální síti již většina lidí, u skupiny mladých lidí je na Facebooku téměř každý. Uživatelé využívají Facebook nejen ke komunikaci s přáteli a známými, ale začali jej využívat také pro „mapování“ vlastního života. Na svém profilu zveřejňují, co se v jejich životě událo, kam a kdy pojedou na dovolenou či do jaké školy chodí.

Tato sociální síť se stala místem, kde mohou uživatelé komunikovat se starými známými, které by za normálních okolností nepotkali, seznámit se s novými lidmi nebo zjistit, co je nového v životě jejich přátel. Každá mince má však dvě strany. Na jednu stranu je Facebook věcí prospěšnou, která lidem mnohé věci v každodenním životě ulehčuje, na stranu druhou je však místem, kde uživatelům hrozí nebezpečí toho, že jejich osobní údaje a data budou zneužita.

Může se jednat o případy, kdy je bezpečnost uživatelova účtu prolomena a jeho osobní data či fotografie jsou šířeny bez souhlasu majitele. Mohou však nastat mnohem vážnější případy. V poslední době se stále více začínají objevovat případy, kdy je uživatel, či jeho majetek v reálném světě napaden, či nějakým způsobem poškozen a to na základě informací zveřejněných na uživatelově profilu na Facebooku. Uveřejnění informace o tom, že následující týden stráví uživatel na dovolené, totiž není pouhou skutečností, kterou se majitel účtu snaží vyjádřit, jak moc se na dovolenou těší, ale je zároveň oznámením, že jeho byt či dům bude následující týden prázdný. Přibývá případů, kdy byly domy či byty lidí vykradeny potom, co majitel nezodpovědně oznámil svou nepřítomnost na sociální síti. Když si dále uvědomíme, jaké nebezpečí hrozí dětem, když uveřejňují, kam chodí do školy, či kde tráví volný čas, zjistíme, že otázka bezpečnosti chování uživatelů sociální sítě Facebook je problémem, který je třeba řešit.

Cíl a metodika práce

Hlavním cílem práce je za použití metod sociologického výzkumu zmapovat chování českých uživatelů sociální sítě Facebook z hlediska bezpečnosti a rizikovosti jejich chování.

Dílčí cíle práce byly definovány následovně:

a) určit, která skupina uživatelů se na Facebooku chová nejrizikověji a hrozí jí tak největší potenciální nebezpečí;
b) jakých největších chyb, z hlediska bezpečnosti, se dopouští nejohroženější skupina uživatelů sociální sítě Facebook;
c) jak se z hlediska bezpečnosti chovají uživatelé, kteří působí v informačních technologiích a mají tak vyšší znalosti v oblasti bezpečného chování na sociálních sítích, resp. na internetu obecně. Jak rizikové je jejich chování v porovnání s ostatními uživateli?;

Práce bude obsahovat teoretická východiska ze tří oblastí a to sice ze sociologického průzkumu, kde bude definováno, jak potřebná data získat, statistiky, kde bude popsáno, jak získaná data zpracovat a poslední část teoretických východisek bude věnována sociálním sítím s důrazem na sociální síť Facebook a na pravidla bezpečného chování na internetu.

1 Teoretická východiska práce

1.1 Statistika

1.1.1 Statistická jednotka, statistický znak, základní soubor

Při statistickém zkoumání se zajímáme o hromadné jevy a procesy, které se vyskytují u velkého množství prvků. Tyto zkoumané prvky nazýváme ***statistickými jednotkami***, které jsou elementárními jednotkami při statistickém pozorování Příkladem statistické jednotky může být např. osoba, událost či organizace.

Statistický znak vyjadřuje vlastnosti statistické jednotky. Pokud tedy např. zvolíme jako statistickou jednotku pracovníka průmyslové výroby, statistické znaky pro tuto jednotku budou mzda, počet let praxe, věk apod. (Hindls, Seger a Hronová, 2002, s. 13-14).

Základní soubor je množina všech statistických jednotek, u nichž zkoumáme příslušné statistické znaky. Počet všech jednotek statistického souboru nazýváme rozsah statistické souboru, tento rozsah může být konečný i nekonečný, zpravidla je ale velký. Základní soubor obvykle označujeme písmenem Z (Novovičová, 1999, s. 10).

1.1.2 Výběrový soubor

Jelikož rozsah základního souboru je často velmi velký, provádí se šetření pouze na vybrané části základního souboru, tuto vybranou část nazýváme výběrovým souborem.

Výběrový soubor je podmnožina základního souboru Z a obsahuje tedy pouze ty prvky (statistické jednotky) základního souboru, na kterých provádíme šetření. Výsledky získané z výběrového souboru pak slouží k provádění úsudku o celém základním souboru (Blatná, 2007, s. 6).

Prvky ze základního souboru lze vybírat a tím vytvářet výběrový soubor dvěma způsoby:

Reprezentativní výběr – jedná se o takový výběr, kdy je získaný výběrový soubor podobný souboru základnímu. Při vhodném výběru prvků ze základního souboru výběrový soubor velmi správně vystihuje vlastnosti základního souboru. Při nevhodném

výběru prvků však získáváme velmi zkreslené informace. Existuje zde však také riziko, kdy jsou prvky ze základního souboru vybrány úmyslně tak, aby sloužili ke klamání veřejnosti.

Náhodný výběr – náhodným výběrem se dá označit takový výběr prvků ze základního souboru, kde výběr prvků proběhne náhodně a to tak, že každý prvek základního souboru má stejnou možnost být vybrán. Takový výběr je označován také jako tzv. *nezávislý výběr* (Kropáč, 2009, s. 3).

1.1.3 Datový soubor a jeho charakteristiky

Datovým souborem označujeme hodnoty zkoumaného statistického znaku na prvních výběrového souboru. Jako rozsah datového souboru poté rozumíme jako počet těchto hodnot.

Zkoumáme-li u každé statistické jednotky pouze jeden statistický znak, nazýváme získaný datový soubor jako datový soubor jednorozměrný. Pokud u každé statistické jednotky zjišťujeme dva, nebo více statistických znaků, mluvíme o *dvourozměrném* resp. *vícerozměrném datovém souboru* (Kropáč, 2009, s. 3-4).

U datového souboru kvantitativních znaků jsou základními charakteristikami výběrový průměr, výběrový rozptyl a výběrová směrodatná odchylka.

Výběrový průměr získáme pomocí vzorce:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} xi \tag{1.1}$$

Výběrový rozptyl:

$$s^2 = \frac{1}{n-1}\left[\sum_{i=1}^{n} x_i^2 - n \cdot \bar{x}^2\right] \tag{1.2}$$

Výběrová směrodatná odchylka:

$$s = \sqrt{s^2} \tag{1.3}$$

Z těchto základních charakteristik je nejdůležitější výběrový průměr $\bar{x}$. Tato charakteristika je však citlivá na extrémně vysoké, nebo naopak velmi nízké hodnoty v datovém souboru. Z toho důvodu se v případech, kdy jsou v datovém souboru obsaženy tyto extrémní rozdíly hodnot, užívají další charakteristiky, které nejsou citlivé k odlehlým hodnotám (Kropáč, 2009, s. 6).

1.1.4 Testy statistických hypotéz

Statistickou hypotézou rozumíme předpoklad o hodnotě určitého parametru či tvaru rozdělení zkoumaného znaku. Pokud například předpokládáme, že průměr prvků základního souboru se rovná určité konkrétní hodnotě, vyslovili jsme určitou hypotézu o parametru základního souboru, v tomto případě o průměru. O správnosti, či nesprávnosti hypotézy by bylo možno rozhodnout šetřením všech prvků základního souboru, avšak takovéto šetření bývá většinou neekonomické a často také technicky neproveditelné, proto tomuto šetření podrobíme pouze vybranou určitou část základního souboru – výběrový soubor. Na tomto výběru poté zjišťujeme, zda je vyslovená hypotéza správná, nebo nesprávná. Tento proces ověřování správnosti hypotézy nazýváme *testováním hypotéz* (Hindls, Seger a Hronová, 2002, s. 133).

Statistickou hypotézu, o jejíž přijetí či zamítnutí rozhodujeme, nazýváme *nulovou hypotézou* a označujeme ji jako H_0. Proti této hypotéze stavíme H_0 stavíme jinou hypotézu, tzv. *alternativní hypotézu* H_1, která nějakým způsobem popírá tvrzení, formulované pomocí nulové hypotézy (Kropáč, 2009, s. 30).

Test statistických hypotéz provádíme pomocí následujícího postupu:

*1. Stanovení hypotéz***.** Stanovíme nulovou hypotézu H_0 a proti ní stanovíme alternativní hypotézu H_1.

2. Zvolíme tzv. testové kritérium. Testové kritérium je statistika, tedy funkce náhodného výběru X, označujeme ji obecně G. Z datového souboru x vypočteme její realizovanou hodnotu, tu značíme g.

3. Sestrojení kritického oboru. Zvolíme číslo α (zpravidla volíme 0,05 nebo 0,01), nazýváme jej hladinou významnosti. Následně určíme kritický obor W_α . Při platnosti

nulové hypotézy H_0 se v tomto kritickém oboru realizuje nejvýše 100α% hodnot testového kritéria G.

4. Vypočteme hodnotu testového kritéria.

5. Formulujeme závěr testu. Pokud realizovaná hodnota g leží v kritickém oboru W_α, zamítáme nulovou hypotézu a přijímáme hypotézu alternativní. Pokud hodnota g neleží v kritickém oboru W_α přijímáme nulovou hypotézu a zamítáme hypotézu alternativní. Přijetí nulové hypotézy však není důkazem její správnosti, značí pouze, že tato hypotéza nebyla vyvrácena. Při testování mohou nastat dva druhy chyb. Chyba první druhu nastane v případě, že nulová hypotéza H_0 platí, ale je odmítnuta na základě testu. Chyba druhého druhu nastává v situaci, kdy platí hypotéza H_1, ale na základě testu jsme přijali H_0 (Hindls, Seger a Hronová, 2002, s. 135-136).

1.1.5 Dvourozměrné datové soubory kvalitativních znaků

Jak již vyplývá z názvu, jedná se o ty datové soubory, jež jsou tvořeny z pozorovaných hodnot dvou znaků kvalitativního typu, tedy můžeme je vyjádřit slovy. Někdy tyto znaky nazýváme také *kategoriální*, protože po vytřídění jejich variant vznikají skupiny neboli kategorie.

Kontingenční tabulka

K hodnocení znaků nám slouží tzv. ***kontingenční tabulka***. Jedná se o tabulku dvourozměrnou, v jejímž záhlaví se nacházejí varianty znaku prvního a v prvním sloupci tabulky varianty znaku druhého. Jednotlivá pole (buňky) tabulky pak zobrazují tzv. *simultánní četnosti*, které označujeme n_{ij} a které nám značí počet pokusů, při kterých došlo k výskytu varianty A_i u zkoumaného znaku *A*, a zároveň se vyskytla varianta B_i u zkoumaného znaku *B*. V posledním sloupci kontingenční tabulky se nachází řádkové součty, označené $n_{i\bullet}$,které vyjadřují celkový počet opakování pokusu u kterých nastala *i*-tá varianta znaku *A*. Poslední řádek tabulky zobrazuje sloupcové součty $n_{\bullet j}$, které udávají celkový počet opakování pokusu, u kterých se vyskytla *j*-tá variantu znaku B. Tyto řádkové resp. sloupcové součty označujeme jako *marginální četnosti*. Pokud tyto četnosti dělíme počtem opakování experimentu *n*, získáváme odhady *simultánních pravděpodobností* resp. *marginálních pravděpodobností*, které

označujeme $\hat{p}_{ij}$ resp. $\hat{p}_{i\bullet}$ a $\hat{p}_{\bullet j}$. Při testu nezávislosti dvou kvalitativních znaků A, B používáme u kontingenční tabulky k nalezení **testového kritéria** tento vztah:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{(n_{ij} - n\hat{p}_{ij})^2}{n\hat{p}_{ij}} \tag{1.4}$$

Pro nalezení **kritického oboru** u kontingenční tabulky použijeme tento vztah:

$$W_\alpha = \{\chi^2 : \chi^2 \geq \chi^2_{1-\alpha}\big((r-1)(s-1)\big)\} \tag{1.5}$$

Nalezením testového kritéria však pouze zjistíme, zda jsou testované znaky závislé, či nikoliv. K vyjádření velikosti této závislosti využijeme tzv. ***Cramérův koeficient kontingence***, určený následujícím vztahem:

$$V = \sqrt{\frac{\chi^2}{n(m-1)}} \tag{1.6}$$

Cramérův koeficient kontingence nabývá hodnot v intervalu (0, 1), kde nula reprezentuje úplnou nezávislost testovaných znaků a hodnota jedna jejich úplnou závislost. Čím více se hodnota koeficientu blíží k jedné, tím je velikost závislosti zkoumaných znaků vyšší. (Kropáč, 2009, s. 66-68).

Čtyřpolní tabulka

Zvláštním typem kontingenční tabulky je tzv. ***čtyřpolní tabulka***, kterou použijeme v případě, že oba zkoumané kvalitativní znaky, A i B, jsou alternativního typu, tedy mohou nabývat pouze dvou variant.

U čtyřpolní tabulky lze k testování nezávislosti znaků A a B využít zjednodušeného vzorce testového kritéria (4), tento jednodušší výraz má tuto podobu:

$$\chi^2 = n\frac{(n_{11}\cdot n_{22} - n_{12}\cdot n_{21})^2}{n_{1\bullet}\cdot n_{\bullet 1}\cdot n_{2\bullet}\cdot n_{\bullet 2}} \tag{1.7}$$

Kritický obor pro hladinu významnosti α vypočítáme dle následujícího vztahu:

$$W_\alpha = \{\chi^2 : \chi^2 \geq \chi^2_{1-\alpha}(1)\} \tag{1.8}$$

Toto testové kritérium se doporučuje použít při dostatečně velkých výběrech, ideálně pokud je n>40. Pokud není tato podmínka splněna, používá se tzv. *Fisherův faktoriální test.* K vyjádření velikosti závislosti zkoumaných znaků můžeme využít Cramérův koeficient kontingence, jehož výpočet je u čtyřpolní tabulky shodný jako u kontingenční tabulky, použijeme tedy vztah (1.6) (Kropáč, 2009, s. 71).

1.2 Sociologický výzkum

Sociologický výzkum je jedním z druhů vědeckého výzkumu, který lze definovat jako složitou, záměrnou poznávací činnost, v níž je prováděné systematické studium reálnou skutečností s přesně vymezenými metodologickými postupy a prostředky. Jako sociologický výzkum poté označujeme takový vědecký výzkum, jehož předmětem jsou různé sociologické jevy. Jako sociologický jev můžeme označit všechno to, co souvisí se společností lidí. Sociologickým jevem tedy rozumíme například skupinu lidí, organizaci, ale také jakoukoliv vlastnost či chování jedince, skupiny či celku (Malátek a Polanský, 1998, s. 7; Gabrielová, 2012, s. 53).

1.2.1 Etapy sociologického výzkumu

Realizaci sociologického výzkumu lze rozdělit do tří základních fází, jde o fázi přípravnou, fázi sběru empirického materiálu a fázi zpracovávání a zobecňování empirických údajů.

Přípravná fáze

První fází výzkumu je fáze přípravná. V této etapě provádíme teoretické analýzy zkoumaného problému. Do této analýzy zahrnujeme studium vývoje problému, naše dosavadní znalosti o problému, formulujeme hypotézy a definujeme také, jak a jakými metodami budeme daný problém řešit.

Obecně lze říci, že tato fáze by měla přinést odpovědi na tyto otázky:

- **CO** bude zkoumáno, jaký je předmět výzkumu?
- **PROČ** bude zkoumáno, za jakým účelem je výzkum prováděn?
- **KDY** bude zkoumáno, v jakém časovém období proběhne výzkum?
- **KDE** bude zkoumáno, v jakém místě bude výzkum realizován?

Výstupem teoretické analýzy je pak tzv. *úvodní studie*, která obsahuje všechny dosud známé poznatky o daném problému a formuluje také cíle výzkumu. V rámci přípravné etapy se provádí také předvýzkum, někdy nazývaný také pilotní studie, jehož cílem je zejména ověření vhodnosti navrhované techniky sběru dat a organizační náročnosti realizace výzkumu. Přípravná fáze je velmi důležitou fází výzkumu, protože její špatné, popřípadě nedostatečné provedení může přivodit problémy v dalších etapách výzkumu, proto by jí měla být přikládána dostatečná pozornost a význam (Gabrielová, 2012, s. 55; Veselá, 2006, s.15).

Fáze sběru empirického materiálu (Realizační fáze)

Fáze sběru empirického materiálu nebo také *realizační fáze* je další etapou při provádění sociologického výzkumu. Spočívá v samotné realizaci sběru dat, který závisí na charakteru zkoumaného problému a zvolené problematice. V této fázi jsou získaná data také podrobována kritice z pohledu úplnosti, relevantnosti a validity, tedy zda data skutečně zobrazují přesně ten problém, který nás zajímá. Fáze sběru materiálu je náročná zejména po organizační stránce (Gabrielová, 2012, s. 56).

Fáze zpracování a zobecňování empirických údajů (Vyhodnocovací fáze)

Poslední fází výzkumu je *fáze zpracování a zobecňování empirických údajů*, někdy nazývána *fází vyhodnocovací*. Hlavní náplní práce v této etapě je roztřídění empirického materiálu a jeho následné zpracování za účelem zjištění skutečností definovaných pomocí hypotéz. Při tomto zpracování a následném posuzování dat se zpravidla využívá statistických metod.

Výstupem sociologického výzkumu je pak *závěrečná zpráva*, která shrnuje všechny fáze provádění výzkumu. Závěrečná zpráva by měla obsahovat vymezení problému, popis a postup použití dané metodiky a vlastní výsledky, které by neměly

obsahovat pouze závěry a výsledky výzkumu, ale také doporučení a opatření pro případné zlepšení stavu zkoumaného problému (Gabrielová, 2012, s. 56).

1.2.2 Výzkumné metody

Základní metody, používané při sociologickém výzkumu, za pomoci kterých lze získávat požadovaná data a informace jsou pozorování, rozhovor a dotazník či anketa. Mezi další metody patří studie písemných dokumentů, škálování, ale mezi výzkumné metody patří i experiment, nebo práce s filmem či videem (Gabrielová, 2012, s. 57).

Z toho důvodu, že v této práci bude využit dotazník, popis ostatních výzkumných metod bude vynechán.

Dotazník

Dotazník je soubor písemných, záměrně položených otázek, které mají směřovat ke stanovenému cíli. Dotazník vyplňuje odpovídající sám. (Gabrielová, 2012, s. 59)

Mezi pozitiva dotazníku patří především jednoznačná formulace otázek, dostatek času na vyplnění dotazníku a promyšlení odpovědí pro dotazovaného a hromadné zpracování výsledků. Dotazník je proto kvalitativně nejproduktivnější technikou, protože jeho prostřednictvím lze získat velké množství informací za relativně krátké časové období. Kladem dotazníku je také důvěra respondenta v udržení anonymity.

Mezi negativní stránky při použití dotazníkového šetření patří zejména to, že respondent nemusí položené otázce přesně porozumět, v důsledku toho mohou nastat odpovědi nejasné či nepřesné. Písemná odpověď také nemusí vždy obsahovat pouze vlastní názory respondenta, je zde možnost ovlivnění ze strany např. rodinných příslušníků, spolupracovníků (Malátek a Polanský, 1998, s. 41).

Vzhled dotazníku a forma zadání otázek by měla být taková, aby byl respondent k vyplnění dotazníku sám motivován a dotazník si získal jeho zájem. Dotazník by proto měl splňovat několik základních podmínek a pravidel.

Rozsah dotazníku – nadměrné množství otázek oslabuje ochotu respondenta k vyplnění a snižuje tak věrohodnost poskytovaných odpovědí. Proto by měl být rozsah

dotazníku vhodně zvolen. Zdaleka totiž neplatí pravidlo, že čím více otázek bude položeno, tím objektivnější výsledky budou dosaženy.

Grafická a stylistická úprava – špatná stylistická úprava a gramatické chyby nejen, že zkreslují srozumitelnost a smysl otázek, ale tyto chyby také výrazně snižují zájem dotazovaného spolupracovat. Při vytváření dotazníku by neměla být opomíjena také jeho grafická podoba a úprava, je vhodné použít výrazně členěný a prostorově vhodně uspořádaný text, vhodně zvolit font a vyvarovat se také nezvyklých formátů papíru. Velký formát totiž evokuje představu velkého množství otázek a velké časové náročnosti dotazníku. Nejvhodnějším formát je proto formát A4. Ve spojitosti se zvoleným formátem bychom se měli pokusit vypracovat dotazník v takové podobě, aby se na to zvolený formát dal vhodně umístit a vyvarovali se situaci, kdy se například poslední otázka dotazníkového šetření nachází na nové straně.

Uspořádání a obtížnost otázek – otázky by měly být uspořádány tak, aby podporovaly zájem dotazovaného, proto je vhodné na začátek pokládat otázky zajímavé s možností jednoduché odpovědi. Otázky složitější by měly být pokládány až ve střední, resp. na závěr dotazníku. Součástí dotazníku by měly být i tzv. identifikační otázky, které se netýkají přesně cíle výzkumu, ale jde o otázky, u kterých jsou zjišťovány charakteristiky respondenta (např. věk, pohlaví). Tyto otázky mohou být zařazeny i na konci dotazníku (Malátek a Polanský, 1998, s. 42-44; Buriánek, 1988, s. 20).

1.3 Sociální sítě a Facebook

1.3.1 Sociální sítě a jejich historie

Vývoj sociálních sítí začal v USA již v polovině 90. let minulého století. Jednalo se o sítě, které využívali zejména studenti. Už u prvních z nich se objevovaly první profily a skupiny přátel.

V současné době se sociální sítě staly skutečným fenoménem. Počty jejich uživatelů dosahují milionů a už se nezaměřují pouze na studenty, ale na celou veřejnost. Studentů je však na sociálních sítích stále téměř polovina (Kulhánková a Čamek, 2010, s. 9-11).

1.3.2 Facebook

Facebook, který je dostupný prostřednictvím adresy *Facebook.com*, byl vytvořen a v prvotní fázi jeho fungování určen výhradně pro studenty Harvardské univerzity, kdy k identifikaci přihlašovaných využíval e-mailové domény univerzity. Postupem času byly do Facebooku přidávány další univerzity. Nejprve byly přidány školy tzv. „Břečťanové ligy" (Ivy League), do které patří osm elitních soukromých univerzit, poté přibývaly školy další. Okruh možných uživatelů stále rostl a to až do té podoby, ve které Facebook známe dnes, tedy jako veřejně přístupný každému. Facebook je největší sociální sítí na světě, počet jeho uživatelů je vyčíslen na 900 milionů.

Jedním z důvodů, proč se stal Facebook tak úspěšným a oblíbeným a díky čemuž se dokázal odlišit od jiných sociálních sítí, bylo zavedení tzv. „Vybraných příspěvků". Jedná se o funkci, která slouží k zobrazování aktuální aktivity přátel. Když tedy někdo přidá na Facebook například novou fotografii, je tato fotografie v podstatě okamžitě zobrazena ve „Vybraných příspěvcích" jeho přátel (Kulhánková a Čamek, 2010, s. 9-11).

Ve spojitosti s touto sociální sítí lze však také narazit na několik problémů v systému fungování a v pravidlech této služby. Některé z nich jsou popsány v následujícím odstavci.

Na Facebooku je možné (na rozdíl například od Twitteru) nalézt poměrně velké množství profilů malých dětí a to i přesto, že jsou tím porušována stanovená pravidla. Minimální věk pro možnou registraci a založení profilu na této sociální síti je totiž stanoven na 13 let. Informace o věku uživatele však není žádným způsobem ověřována a tak je v podstatě registrace umožněna komukoliv, kdo při registraci účtu uvede svůj věk vyšší než 13. Důsledkem tohoto faktu je to, že české děti mají běžně založen profil na Facebooku v páté třídě základní školy, ačkoliv jejich věk požadovanou hranici 13 let nepřesáhl. Děti si v tomto věku neuvědomují možná rizika a nebezpečí a bez zábran navazují nové kontakty, sdílejí informace, poskytují osobní údaje či zveřejňují osobní fotografie.

Dalším problémem je mj. i to, že se jedná o zahraniční společnost, jejíž hlavní sídlo je v USA, tudíž její aktivity podléhají americkému právu. Dalším faktem s tímto problémem souvisejícím je pro uživatele z České republiky zdlouhavé řešení problémů,

nehledě na to, že řešení problémů probíhá pouze v angličtině (Eckertová a Dočekal, 2013, s. 28-29).

1.4 Bezpečné chování na internetu

Server *Cesivsiti*.cz provedl rozsáhlé šetření zabývající se chováním českých uživatelů na internetu, některé poznatky z výsledků toho projektu jsou shrnuty v tomto odstavci. V České republice je počet uživatelů internetu vyčíslen na 6,3 milionu lidí, přičemž polovina z tohoto počtu je ve věku mezi 15 a 44 roky. U věkové skupiny 16 až 65 let využívá Internet a jeho služby plných 80%, dvě třetiny z tohoto počtu ho využívají denně. U mladší generace internet využívá prakticky každý. Trendem v dnešní době jsou tzv. smartphony, neboli chytré telefony, které umožňují přístup k Internetu prakticky odkudkoliv. Chytrý telefon k připojení k Internetu používá v Česku již každý třetí uživatel. To jen potvrzuje soudobý trend, že se Internet stále více přeměňuje v Internet „mobilní“. Uživatelé Internet nejvíce využívají k získávání informací o produktech a službách, následuje získávání informací pro studium a k práci, na třetím místě figuruje sledování videí. Průměrný český uživatel stráví týdně na Internetu 15 hodin, přičemž osm hodin se věnuje hledání informací, pět hodin zábavě a dvě hodiny týdně stráví průměrný český uživatel internetu nakupováním. Internet dnes tedy není pouze zdrojem informací, ale také místem, kam se chodí uživatel bavit. A čím mladší uživatelé jsou, tím více zábavy na Internetu hledají (Eckertová a Dočekal, 2013, s. 25).

1.4.1 Uživatelé internetu

Uživatelé internetu by se z pohledu jejich chování a přístupu k Internetu dali rozdělit na následující skupiny:

Uživatelé ve věku 14-19 let – Uživatelé v tomto věku dnes již nerozlišují hranici mezi online a offline světem, vyrůstali s Internetem a je pro ně běžné mít Internet neustále s sebou a mít možnost připojit se k němu odkudkoliv. Internet je pro ně především nástrojem zábavy. Na rozdíl od starších uživatelů využívají v nebývalé míře sociální sítě. Spolu se současným trendem rozvoje Internetu a informačních technologii obecně se dolní hranice uživatelů Internetu stále snižuje, proto již nikoho nezarazí, když již dvanáctileté děti umí pracovat s počítačem, respektive internetem. Právě tato skupina je pro její nízký věk skupinou na internetu nejohroženější.

Uživatelé ve věku 19-29 let – Tito uživatelé zacházejí s Internetem podstatně sofistikovaněji, jsou k němu kritičtější. Internet neberou ve svém životě tak „samozřejmě“, jako uživatelé mladší. Sociální sítě však využívá tato věková skupina ve stejné míře, jako skupina mladších uživatelů.

Uživatelé ve věku 30-44 let – U této věkové skupiny již nalézáme velké rozdíly ve využívání internetu, jde totiž o věkovou skupinu, u které se Internet objevil až v jejich vyšším věku a tato generace se musela s Internetem naučit žít. Řada z těchto lidí se s Internetem sžít nedokázala a jeho využívání pro ně není tak samozřejmé. Sociální sítě velmi často nevyužívají, jedním z důvodů je to, že neví, jakým způsobem je využívat a ovládat, další důvod je prostý, jednoduše nevidí žádný důvod, proč sociální sítě využívat.

Uživatelé ve věku 45-65 let – Internet je u této věkové skupiny využíván omezeněji, převládá nedůvěra a také strach z neužití. Na sociálních sítích se uživatelé této věkové skupiny téměř nevyskytují (Eckertová a Dočekal, 2013, s. 24-25).

1.4.2 Pravidla internetového provozu

Z důvodu, že Internet je velmi proměnlivý a charakter jeho služeb a produktů je velice časově omezený, univerzální návod na bezpečné chování v podstatě neexistuje. Základní pravidla by se však dala shrnout do podoby desatera, které je uváděno na adresách *www.seznamsebezpecne.cz* a *www.bezpecnyinternet.cz*. Tato pravidla jsou určena zejména pro skupinu na Internetu nejohroženější, tedy pro děti a mládež. Většina pravidel je však uplatnitelná i u dospělé populace.

Desatero má tuto podobu:

- Nedávej nikomu adresu ani telefon. Nevíš, kdo se skrývá za monitorem.
- Neposílej nikomu, koho neznáš, svou fotografii a už vůbec ne intimní.
- Udržuj hesla k e-mailu i jinam v tajnosti, nesděluj je ani blízkému kamarádovi.
- Nikdy neodpovídej na neslušné, hrubé nebo vulgární maily a vzkazy.
- Nedomlouvej si schůzku na Internetu, aniž bys o tom řekl někomu jinému.
- Pokud narazíš na obrázek, video nebo e-mail, který tě šokuje, opusť webovou stránku.
- Svěř se dospělému, pokud tě stránky uvedou do rozpaků nebo vyděsí.

- Nevěř každé informaci, kterou na Internetu získáš.
- Když se s někým nechceš bavit, nebav se. (Eckertová a Dočekal, 2013, s. 36).

1.4.3 Bezpečné heslo

Tato kapitola, věnovaná bezpečnému hesla čerpala informace ze serveru *Technet.cz* a z *Finexpert.cz* a ze serveru *Bezpecnyinternet.cz.* K zabezpečení našich internetových účtů a tím i k zabránění zneužití našich osobních údajů můžeme jako uživatelé přispět volbou správného a bezpečného hesla. Bezpečné heslo by mělo dodržovat tato dvě základní pravidla:

- Délka hesla by měla být minimálně 8 znaků, ideální je však použít znaků 14.
- Heslo by mělo obsahovat různé typy znaků, malá i velká písmena, číslice, interpunkční znaménka a speciální znaky.

Obecně lze říci, že ideální bezpečné heslo by mělo obsahovat velký počet znaků a mělo by v něm být použito co nejvíce typů znaků. Platí také, že čím méně typů znaků je v hesle obsaženo, tím delší by heslo mělo být, např. řada náhodných 15 čísel je jako heslo bezpečnější, než osmiznakové heslo, které obsahuje různé typy znaků.
Při tvorbě bezpečného heslo bychom se měli vyvarovat těchto základních chyb a omylů:

- Jako heslo v žádném případě nepoužívat svoje jméno, datum narození, či podobný osobní údaj, obecně nepoužívat žádná smysluplná slova.
- V hesle by se neměly objevovat řady znaků, opakující se znaky, nebo ta písmena, která leží na klávesnici vedle sebe.

Heslo bychom měli pravidelně měnit a to i v případě, že se jedná o heslo bezpečné. Zvláště to platí například pro přihlašování k bankovním účtům. Pro více internetových služeb bychom měli také používat různá hesla, není tedy bezpečné pro všechny služeb využívat pouze jedno heslo. Heslo bychom neměli žádným způsobem zaznamenávat, ani sdělovat jiným osobám.

2 Praktická část práce

Cílem této práce je analýza rizikového chování uživatelů sociální sítě Facebook, práce se pokouší odpovědět na otázku do jaké míry se uživatelé Facebooku chovají rizikově a tím se vystavují možnému nebezpečí zneužití jejich osobních údajů a dat. Jako prostředek ke zjištění odpovědi na tuto otázku bylo použito dotazníkové šetření.

2.1 Hypotézy

Základní hypotézu můžeme definovat takto:

Chování českých uživatelů na sociální síti Facebook je rizikové.

Tato základní hypotéza může být rozdělena na několik dílčích hypotéz, pomocí kterých se snažíme odpovědět na hypotézu základní. Zvláštní důraz je kladen na hypotézu závislosti znalosti informačních technologií uživatele a jeho chování, resp. to, zda uživatelé, kteří studují či pracují v oblasti informačních technologií, vykazují bezpečnější chování z hlediska rizika zneužití dat.

Dílčí hypotézy byly formulovány takto:

1. Uživatelé působící v oblasti informačních technologií používají silnější hesla než ostatní uživatelé.
2. Většina uživatelů využívá stejné heslo k více účtům.
3. Většina uživatelů používá funkci automatického zapamatování hesla.
4. Veřejně přístupné účty se u uživatelů, působících v informačních technologiích, objevují méně, než u ostatních uživatelů.
5. Uživatelé mladší 18 let přijímají přátelství od neznámých uživatelů častěji, než uživatelé jiní.
6. Nebezpečné aplikace a hry využívají nejčastěji uživatelé mladší 18 let.
7. Uživatelé jsou si vědomi nebezpečí zneužití jejich osobních údajů a dat.
8. Uživatelé mladší 18 let častěji uveřejňují důvěrné osobní informace a data.
9. Uživatelé s vysokým počtem přátel přijímají častěji přátelství od neznámých uživatelů.
10. Nejvíce času denně stráví na Facebooku uživatelé ve věku 10-18 let.

2.2 Přípravná fáze sociologického výzkumu

V rámci přípravné fáze sociologického výzkumu musíme získat odpovědi na několik základních otázek týkající se samotné pozdější realizace tohoto sociologického šetření.

2.2.1 Úvodní studie

Cílem úvodní studie bylo zjištění, zda jsou mnou připravené otázky vhodné a zda jsou navrhované možnosti odpovědi u zavřených otázek dostatečné a tedy zda tyto možnosti otázek dobře pokrývají šíři možné odpovědi respondenta. Toto ověření bylo prováděno formou nestrukturovaného rozhovoru a účastníci studie byli lidé z mého okolí.

Tato úvodní studie přinesl pozitivní výsledek, tedy navrhované otázky bylo, po drobných úpravách, možné využít při samotné realizaci sociologického šetření. Jediný problém, který se vyskytl při úvodní studii, ale i během samotného výzkumu nesouvisí s konstrukcí či metodikou výzkumu, ale spočívá v tom, že někteří respondenti na některé otázky nechtějí odpovědět v obavách, aby jejich odpověď nebyla zneužita. Při pozdějším sběru dat dokonce někteří respondenti odmítli odpovědět úplně a to právě z tohoto důvodu. Na jednu stranu tento problém komplikoval sběr dat, na stranu druhou je však toto chování pochopitelné a z pohledu bezpečnosti osobních údajů správné.

2.2.2 Cílová skupina

Sociologický výzkum byl určen výhradně pro uživatele sociální sítě Facebook. Výzkum byl určen pro tuto sociální síť zejména proto, že tato sociální síť je zdaleka nejpoužívanější a nejvíce navštěvovanou sociální sítí u nás. Dalším důvodem byla rozdílnost podoby jednotlivých sociálních sítí. Z důvodu specifického zaměření na pouze jednu z těchto sítí bylo možno upravit pokládané otázky podle podoby a charakteru této sociální sítě. Z jiných pohledů nebyla cílová skupina omezena, tedy byla určena pro všechny věkové kategorie, pro muže i ženy.

2.2.3 Technika sběru dat

Vzhledem k tématu celého výzkumu a vzhledem k cílové skupině, pro kterou byl výzkum určen, byl jako vhodný prostředek ke sběru dat použit dotazník. Ostatní techniky by samozřejmě šli využít také, ale dotazník byl pro mnou realizovaný výzkum technikou nejefektivnější a to jak z pohledu zpracování dat, tak z časové a organizační náročnosti výzkumu. Dotazníkové šetření bylo realizováno pouze v elektronické podobě, sběr dat formou tištěné podoby dotazníku použit nebyl a to jednak z důvodu organizační i časové náročnosti tohoto způsobu a také z důvodu určení dotazníku specifické cílové skupině, tedy uživatelům sociální sítě Facebook. Elektronická podoba dotazníku byla k respondentům distribuována zejména právě prostřednictvím sociální sítě Facebook a to jednak sdílením tohoto dotazníku mezi uživateli samotnými, ale také umístěním dotazníku do skupin na této sociální síti. Dalšími místy, na kterých byl dotazník umístěn, byla diskusní fóra zabývající se problematikou sociálních sítí, resp. informačních technologií obecně. Zvolení elektronické podoby dotazníku se ukázalo jako vhodné, jelikož byl získán poměrně velký vzorek dat a to v relativně krátkém čase a s velmi nízkými náklady na tvorbu i distribuci dotazníku.

2.2.4 Podoba a konstrukce dotazníku

Konstrukce dotazníku spočívala nejprve ve formulaci otázek a následně k jejich vhodnému seřazení v rámci doporučeného řazení. První část dotazníku je věnována bezpečnosti hesla uživatele, další část tomu, jak moc je uživatel důvěřivý k anonymitě. Třetí část se věnuje tomu, jaká data je o sobě uživatel ochoten zveřejnit. Poslední část dotazníku se zaměřuje na otázky doplňující, v úplném závěru se nabízí možnost pro respondenta uvést svoji e-mailovou adresu a být po skončení výzkumu informován o výsledku. Rozsah dotazníku, obtížnost a seřazení otázek, ale i grafická úprava dotazníku byla zvolena tak, aby měl dotazník co největší efektivitu.

Dotazník měl následující podobu: (Pro potřeby textového zobrazení byla podoba dotazníku lehce upravena, u otázek, u kterých nejsou uvedeny možnosti odpovědi, bylo možno zvolit z odpovědí ANO či NE)

Prosím, vyplňte tento dotazník, který byl zpracován jako součást bakalářské práce

Dotazník se zabývá analýzou chování uživatelů sociální sítě Facebook, zejména pak jejich bezpečností na této sociální síti.

1. Kolik znaků má vaše heslo?
1-5, 6-9, 10-15, 15 a více

2. Jaké znaky obsahuje vaše heslo?
Velká písmena, Malá písmena, Číslice, Speciální znaky

3. Používáte stejné heslo také k jiné službě na internetu?

4. Využíváte na svém osobním počítači funkce automatického uložení hesla?

5. Přihlašujete se ke svému profilu na veřejných místech?

6. Je váš profil veřejně přístupný? (Jeho obsah mohou zobrazit i ti uživatelé, které nemáte v přátelích)

7. Pokud vás o přátelství požádá neznámý uživatel, přijmete?

8. Využíváte na Facebooku aplikace (popř. hry), které používaje vaše osobní údaje?

9. Jste si vědom nebezpeční zneužití vašich osobních údajů?

10. Uveřejňujete na svém profilu své skutečné jméno?

11. Uveřejňujete na svém profilu svoje telefonní číslo?

12. Uveřejňujete na svém profilu adresu vašeho bydliště?

13. Zveřejňujete prostřednictvím svého profilu osobní fotografie?

14. Pracujete (popř. studujete) v oblasti IT?

15. Vaše pohlaví? MUŽ/ŽENA

16. Kolik přátel máte na Facebooku?
0-100, 101-200, 201-300, 301-500, 501 a více

17. Váš věk?
10-18, 19-25, 26-35, 36-45, 46 a více

18. Kolik hodin (průměrně) denně na Facebooku strávíte?
0-1, 1-2, 2-4, 4 a více

V případě zájmu o výsledky průzkumu můžete napsat svoji e-mailovou adresu:

Děkuji za vyplnění dotazníku.

Dotazník byl realizován jako webová stránka na adrese http://bp-dotaznik.8u.cz. Jako nástroj pro tvorbu dotazníku byl využit skriptovací programovací jazyk PHP a to především z důvodu možnosti uložení výsledků ve vhodné požadované podobě. Výsledky byly ukládány do souboru s název *vysledky.php* a to v podobě tabulky, kdy každý řádek představuje jednoho respondenta. Odpovědi byly převedeny do číselné podoby z důvodu pozdějšího zpracování. Bylo použito číselného převodu odpovědi ve formě – 0 pro možnost „NE“, 1 pro možnost „ANO“, obdobně pro otázky z více možnými odpověďmi.

2.2.5 Využití Microsoft Excel 2007, Microsoft Visual Basic

K následnému statistickému zpracování byl využit Microsoft Excel 2007. K filtrování dat byl využit programovací jazyk Microsoft Visual Basic, který je součástí programu Microsoft Excel 2007 a je určen mimo jiné právě k práci s daty z tohoto programu. Data by bylo možno filtrovat také pomocí funkce Filtr, resp. Souhrn integrované v programu Excel, ale řešení za pomoci Microsoft Visual Basic dovoluje pohodlnější a přehlednější výsledek dotazu. Další důvod proč bylo využito pro řešení Microsoft Visual Basic je ten, že v případě změny zdrojových dat lze dojít k novému výsledku prostým opětovným spuštěním naprogramovaného algoritmu, kdežto při použití integrovaných funkcí Filtr, resp. Souhrn by bylo třeba hodnoty manuálně upravovat a přepočítávat a tak by se integrace změny zdrojových dat stala velmi časově náročnou.

Algoritmus vytvořený ve Microsoft Visual Basic, který filtruje potřebná data, pracuje tak, že v cyklu (konkrétně je použit cyklus Do...Until, tedy „opakuj tyto příkazy, dokud neplatí tato podmínka“) algoritmus prochází řádek po řádku zdrojových dat a každý řádek prověřuje z pohledu požadovaných kritérií. Pokud konkrétní řádek vyhovuje (např. v sloupci R, obsahuje číslo 1 – což značí kladnou odpověď na otázku číslo 14 a zároveň ve sloupci G obsahuje číslo 0 – což označuje negativní odpověď na otázku číslo 3), přičte se k proměnné určující počet vyhovujících řádků, resp. záznamů jednička. Cyklus probíhá tak dlouho, dokud nenarazí na prázdný řádek („Until Buňka.Range=””). Použití tohoto cyklu tak zaručuje univerzálnost algoritmu, lze ho použít na jakýkoliv počet záznamů. Po ukončení cyklu dochází k vypsání proměnné, která označuje počet řádků, vyhovujících danému požadavku. Algoritmus se pro konkrétní úlohy mění pouze v požadovaných kritériích na zkoumaný řádek, jeho princip

však zůstává nezměněn. Výpis proměnné, resp. proměnných je realizován do příslušných buněk příslušné tabulky, hodnoty jsou tedy vypisovány přímo do buněk pracovního listu Microsoft Excel. Z takto vyplněné tabulky je poté vytvořen graf a to užitím integrované funkce Microsoft Excel – Vytvoření grafu. Při změně vstupních dat je změna výsledného grafu jednoduchá, opětovně se spustí algoritmus, který upraví hodnoty, vyhovující požadovanému kritériu dle nově zadaných dat, a automaticky se změní i grafické znázornění těchto dat. Integrace změn vstupních dat je proto velice rychlá a časově nenáročná.

2.3 Statistické vyhodnocení získaných dat

2.3.1 Bezpečnost hesla

Dílčí hypotéza č. 1: Uživatelé působící v oblasti informačních technologií používají silnější hesla než ostatní uživatelé.

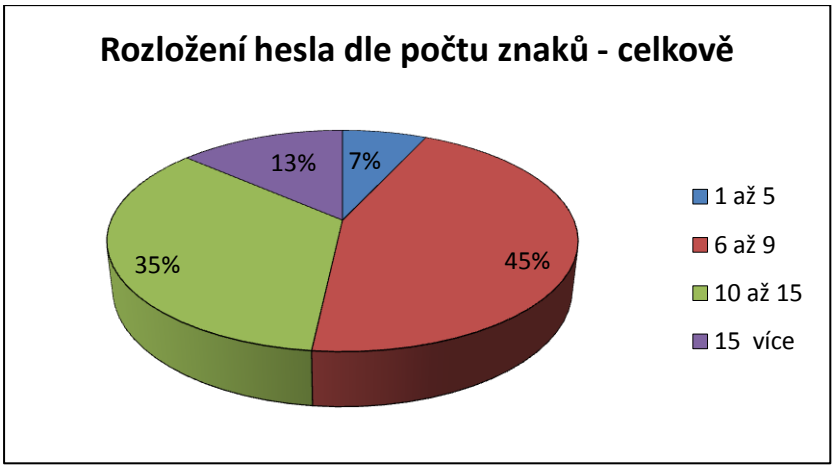
Předpokladem je, že uživatelé působící v oblasti informačních technologií budou používat lepší a silnější hesla než uživatelé jiní, a to z důvodu, že jakožto lidé, kteří se zajímají o informační technologie, by měli mít větší přehled o nebezpečí na internetu a o nebezpečí užití slabých hesel a proto by logicky tato hesla neměli využívat a tím se vystavovat zbytečnému riziku.

Výsledky rozložení hesla dle počtu znaků jsou zachyceny v následující tabulce a graficky zobrazeny na uvedených grafech.

Tab. č. 1: Rozložení hesla dle počtu znaků

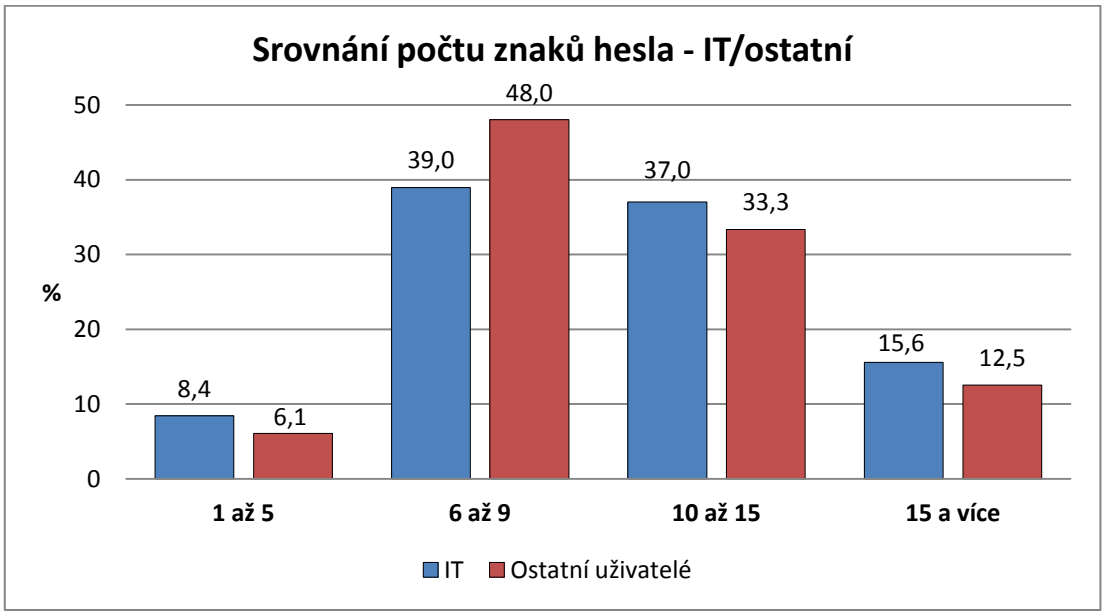
Počet znaků	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
1 až 5	30	0,07	13	0,08	17	0,06
6 až 9	194	0,45	60	0,39	134	0,48
10 až 15	150	0,35	57	0,37	93	0,33
15 a více	59	0,14	24	0,16	35	0,13
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)



Graf č. 1: Rozložení hesla dle počtu znaků – celkově

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)



Graf č. 2: Srovnání počtu znaků hesla – IT/ostatní

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Jak můžeme z tabulky, resp. z grafů vyčíst, v celkovém pohledu uživatelé nejvíce používají heslo v délce 6 až 9 znaků, používá ho 45% všech respondentů. Tato délka hesla není z hlediska bezpečnosti dostačující, ale zaručuje již relativní bezpečnost. 7% ze všech respondentů však využívá heslo naprosto nedostatečné délky a to kratší než 5 znaků. Pozitivním zjištěním však je, že téměř polovina všech respondentů, konkrétně 48%, využívá heslo dostatečné délky, 13% dotazovaných dokonce používá heslo delší než 15 znaků, které můžeme označit již jako velmi bezpečné. Pokud porovnáme délku hesla u uživatelů působících v IT a uživatelů ostatních, vidíme, že u uživatelů z oblasti informačních technologií jsou více používána delší hesla.

8% uživatelů působících v IT však využívá nejslabší formu hesla, tedy délku kratší než 5 znaků. V porovnání s ostatními uživateli je tento údaj vyšší, konkrétně o 2%. Z důvodu, že výsledky obou skupin uživatelů se v žádném místě příliš neodlišují, si troufám tvrdit, že fakt, že uživatel studuje či pracuje v informačních technologiích, neovlivňuje délku jeho hesla. Rozhodujícím faktorem při uživatelově volbě hesla je dle pak mého názoru spíše povaha konkrétního člověka a to, jak moc je konkrétní jedinec opatrný a obezřetný.

Bezpečnost hesla určuje samozřejmě nejen jeho délka, ale i to, z jakých znaků je heslo složeno. Toto rozdělení je zachyceno v následující tabulce. Pro větší přehlednost jsou varianty seřazeny podle oblíbenosti užívání od nejvíce používané varianty po variantu užívanou nejméně.

Tab. č. 2: Varianty použitých znaků v hesle uživatele

Varianta	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
Písmena a čísla	110	0,25	39	0,25	71	0,25
Malá písmena a čísla	106	0,24	30	0,19	76	0,27
Pouze malá písmena	69	0,16	11	0,07	58	0,21
Kombinace všeho	37	0,09	24	0,16	13	0,05
Pouze čísla	32	0,07	10	0,06	22	0,08
Malá písmena, čísla a speciální znaky	15	0,03	8	0,05	7	0,03
Velká písmena a čísla	14	0,03	8	0,05	6	0,02
Pouze velká písmena	14	0,03	6	0,04	8	0,03
Písmena	10	0,02	6	0,04	4	0,01
Velká písmena, čísla a speciální znaky	7	0,02	5	0,03	2	0,01
Pouze speciální znaky	7	0,02	2	0,01	5	0,02
Velká písmena a speciální znaky	5	0,01	3	0,02	2	0,01
Malá písmena a speciální znaky	4	0,01	1	0,01	3	0,01
Písmena a speciální znaky	2	0,00	1	0,01	1	0,00
Čísla a speciální znaky	1	0,00	0	0,00	1	0,00
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Z tabulky vidíme, že nejvíce používanou variantou užitých znaků v heslech uživatelů je kombinace písmen a čísel, tuto možnost volí 25% všech uživatelů. Druhou kombinací, která dosahuje téměř stejného počtu využívání (24%) je kombinace pouze malých písmen a čísel. Nejsilnější možnou kombinaci, tedy užití písmen, čísel i speciálních znaků využívá 9% uživatelů, přičemž u uživatelů z oblasti IT je to dokonce 16%, u ostatních uživatelů 5%. Tento fakt ukazuje na to, že uživatelé působící v oblasti informačních technologií si více uvědomují důležitost použití různých znaků v hesle. Ostatní uživatelé naopak využívají oproti uživatelům z IT o 16% více heslo složené pouze z malých písmen, které je z hlediska bezpečnosti velmi slabé. Z používaných variant znaků v hesle tedy vyplývá, že lidé z oblasti IT volí z tohoto pohledu hesla bezpečnější, než ostatní uživatelé.

K tomu, abychom mohli potvrdit či vyvrátit hypotézu o tom, že uživatelé působící v oblasti informačních technologií používají silnější a bezpečnější hesla je však třeba porovnat závislost délky hesla a toho, z jakých znaků je heslo složeno. Bezpečné heslo je totiž takové, které je bezpečné z obou těchto pohledů, jeho délka je dostatečná a zároveň je složeno z různých znaků.

Následující kontingenční tabulky zobrazují závislost délky hesla a jeho znakového složení. Hodnoty v tabulkách jsou pro přehlednost uvedeny v procentech. První kontingenční tabulka zobrazuje výsledky pouze těch uživatelů, kteří působí v informačních technologiích.

Tab. č. 3: Závislost délky hesla a použitých znaků v hesle – uživatelé působící v IT

Délka hesla / Znaky v hesle	1 až 5	6 až 9	10 až 15	15 a více	Celkem
Písmena a čísla	0,65	10,39	12,34	1,95	25,32
Malá písmena a čísla	0,00	12,99	5,19	1,30	19,48
Pouze malá písmena	0,00	4,55	1,95	0,65	7,14
Vše	0,00	2,60	9,09	3,90	15,58
Pouze čísla	0,00	2,60	1,95	1,95	6,49
Ostatní varianty	7,79	5,84	6,49	5,84	25,97
Celkem	**8,44**	**38,96**	**37,01**	**15,58**	**100,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Druhá kontingenční tabulka zachycuje výsledku u uživatelů, kteří v oblasti informačních technologií nepůsobí.

Tab. č. 4: Závislost délky hesla a použitých znaků v hesle – ostatní uživatelé

Délka hesla / Znaky v hesle	1 až 5	6 až 9	10 až 15	15 a více	Celkem
Písmena a čísla	1,79	12,54	9,68	1,43	25,45
Malá písmena a čísla	1,79	14,70	9,32	1,43	27,24
Pouze malá písmena	0,72	11,47	7,17	1,43	20,79
Vše	1,08	0,36	1,43	1,79	4,66
Pouze čísla	0,36	4,66	2,15	0,72	7,89
Ostatní varianty	0,36	4,30	3,58	5,73	13,98
Celkem	**6,09**	**48,03**	**33,33**	**12,54**	**100,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Pokud z těchto kontingenčních tabulek vyjádříme procentuální zastoupení silných hesel, tedy těch, jejichž délka je alespoň 8 znaků a které jsou složeny alespoň ze dvou různých znaků, dostáváme tyto výsledky:

- uživatelé, kteří studují, či pracují v oblasti informačních technologií, užívají silné bezpečné heslo v 70,13% případů.
- ostatní uživatelé užívají silná hesla v 50,36% případů.
- v celkovém souhrnu užívá silné heslo 54,50% všech uživatelů.

Tyto výsledky dokazují, že uživatelé, působící v informačních technologiích užívají silná hesla přibližně o 20% více, než ostatní uživatelé. Slabé heslo tedy mezi uživateli z informačních technologií užívá přibližně 30%, kdežto u ostatních uživatelů je slabé heslo využíváno bezmála v 50% případů.

Na základě zjištěných výsledků potvrzujeme dílčí hypotézu č. 1. Uživatelé, kteří působí v oblasti informačních technologií totiž opravdu používají bezpečnější hesla častěji, než ostatní uživatelé.

2.3.2 Závisí znaková skladba hesla na jeho délce?

Pro zjištění odpovědi na tuto otázku, je třeba tuto závislost otestovat pomocí testu nezávislosti dvou kvalitativních znaků. Průběh testu je popsán v 1.1.4., konkrétní vztahy pro výpočet charakteristik pak v části 1.1.5.

Zkoumaný znak A: Znaková skladba hesla.

Zkoumaný znak B: Délka hesla.

1. Definujeme nulovou, resp. alternativní hypotézu:

Nulová hypotéza H_0: Zkoumané znaky jsou nezávislé, znaková skladba hesla není ovlivněna jeho délkou.

Alternativní hypotéza H_1: Zkoumané znaky jsou závislé, znaková skladba hesla je jeho délkou ovlivněna.

2. Hodnota testového kritéria $\chi^2 \doteq 77{,}81$

3. Kritický obor na 5%-ní hladině významnosti: $W_\alpha = \{\chi^2 : \chi^2 \geq 24{,}996\}$

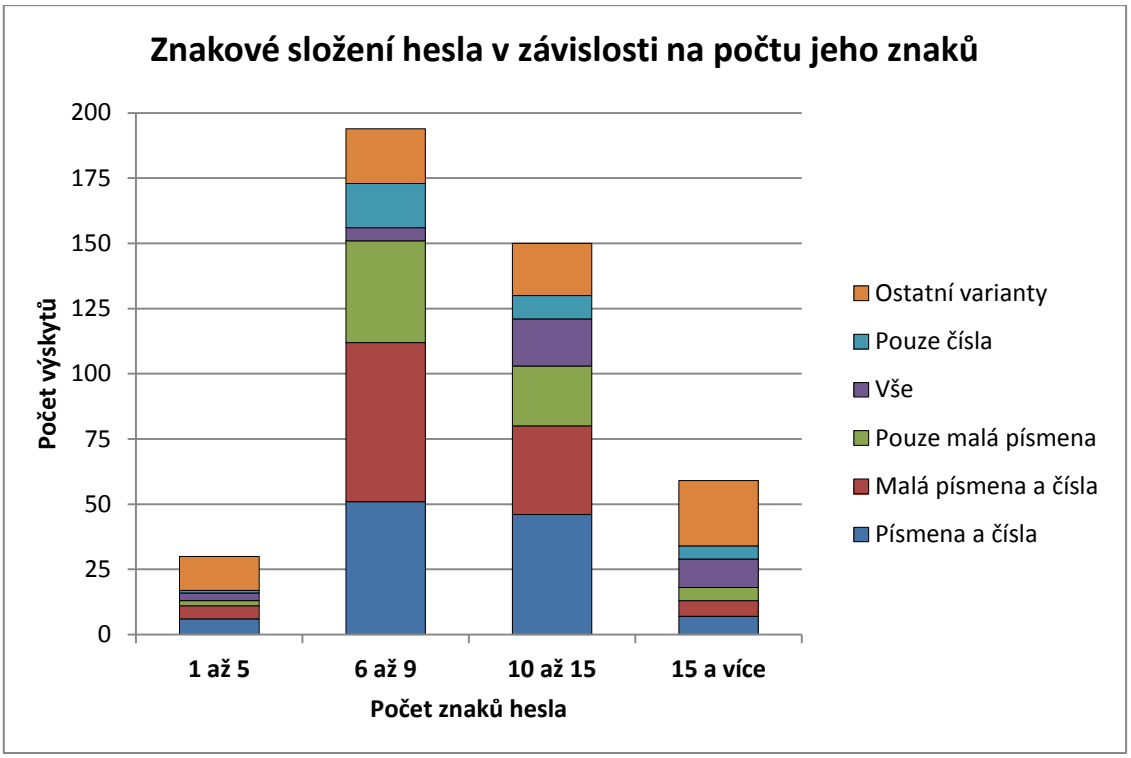
4. Závěr testu. Protože se hodnota testového kritéria v kritickém oboru realizovala, zamítáme na 5%-ní hladině významnosti nulovou hypotézu H_0 a přijímáme alternativní hypotézu H_1. S 5%-ní možností omylu lze tedy říci, že zkoumané znaky, tedy skladba hesla a jeho délka jsou na sobě závislé, délka hesla tedy ovlivňuje jeho znakové složení. Závislost znakového složení hesla na jeho délce je zobrazena na následujícím grafu, který rovněž dokazuje, že znakové složení hesla se mění v závislosti na jeho délce.

K vyjádření těsnosti této závislosti využijeme Cramérův koeficient kontingence, tento koeficient vypočteme dle (1.6) v části 1.1.5.

Hodnota Cramérova koeficientu kontingence $V = 0{,}433$.

Hodnota koeficientu značí, že mezi délkou hesla a jeho znakovým složením existuje nízká až střední závislost.

Závislost znakového složení hesla a jeho délky je zachycena na grafu č. 3. Na grafickém znázornění vidíme, že znakové složení hesla se opravdu mění v závislosti na jeho délce, čímž se nám potvrzuje výsledek zjištěný pomocí testu nezávislost dvou kvalitativních znaků.



Graf č. 3: Znakové složení hesla v závislosti na počtu znaků

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

2.3.3 Použití stejného hesla k více účtům

Dílčí hypotéza č. 2: Většina uživatelů využívá stejné heslo k více účtům.

Charakteristikou, která přímo nesouvisí s bezpečností hesla samotného, ale ovlivňuje bezpečnost uživatelských účtů je využívání stejného hesla u více účtů. O této charakteristice hovoří hypotéza č. 2. Tím, že uživatelé používají stejné heslo na více místech, podstupují riziko toho, že pokud bude jejich heslo prolomeno, útočník bude mít přístup ke všem účtům uživatele, u kterých bylo toto heslo použito. Proto se doporučuje používat různá hesla pro různé účty. Výsledky této charakteristiky jsou zobrazeny v následující tabulce.

Tab. č. 5: Používání stejného hesla k více účtům

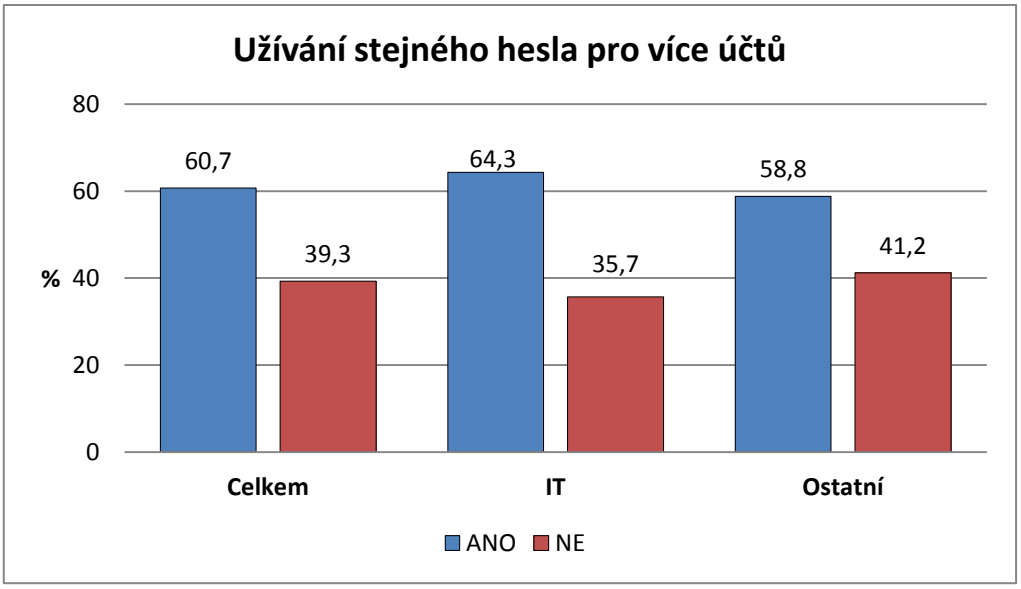
Hodnota	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	263	0,61	99	0,64	164	0,59
NE	170	0,39	55	0,36	115	0,41
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Jak vidíme, stejné heslo pro přihlašování k více internetovým službám používá 61% uživatelů. Toto číslo je poměrně vysoké, přihlédneme-li k faktu, že tito uživatelé (když ne všichni, tak alespoň část z nich) využívají toto heslo všude, tzn. i u služeb jako například bankovní účet či email, jejichž zneužití by mnohdy mělo pro uživatele fatální následky. Srovnání uživatelé působících v IT a uživatelů ostatních přineslo překvapivý výsledek. Uživatelé z oblasti IT vykazují horší výsledek, stejné heslo k více účtům využívá 64%, u ostatních uživatelů je to pouze 59%.

Výsledky potvrzují hypotézu č. 2, tedy že většina českých uživatelů sociální sítě Facebook používá stejné heslo také k přihlašování k jiné službě.

Graficky jsou výsledky zobrazeny na následujícím grafu.



Graf č. 4: Užití stejného hesla pro více účtů

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

2.3.4 Užívání funkce automatické uložení hesla

Dílčí hypotéza č. 3: Většina uživatelů používá funkci automatického zapamatování hesla.

Další charakteristikou, která může ohrozit bezpečnost uživatele je využívání funkce automatického uložení hesla. Užívání této funkce je předmětem dílčí hypotézy č. 3. Tuto funkci uživatelé většinou využívají pouze na svých osobních počítačích, ke kterým mají přístup pouze oni sami a osoby jim blízké. Může se však stát, že se k počítači dostane člověk naprosto neznámý a zneužije údaje uživatele. Mnohdy se také stává, že uživatelé tuto funkci použijí „omylem“, například při přihlašování k sociální síti na veřejných počítačích. Uživatel, který s počítačem pracuje po těchto uživatelích, se tak dostane do osobního profilu předchozího uživatele. V nejlepším případě situace končí prostým odhlášením, či napsáním vtipné zprávy či statusu na adresu nezodpovědnosti uživatele, ale může se stát, že uživatel, který se zapomněl odhlásit, se stane obětí mnohem závažnějšího útoku a přijde o svá soukromá, citlivá data. To, jak respondenti odpověděli na otázku týkající se automatického uložení hesla, vidíme v následující tabulce.

Tab. č. 6: Užívání funkce automatického uložení hesla

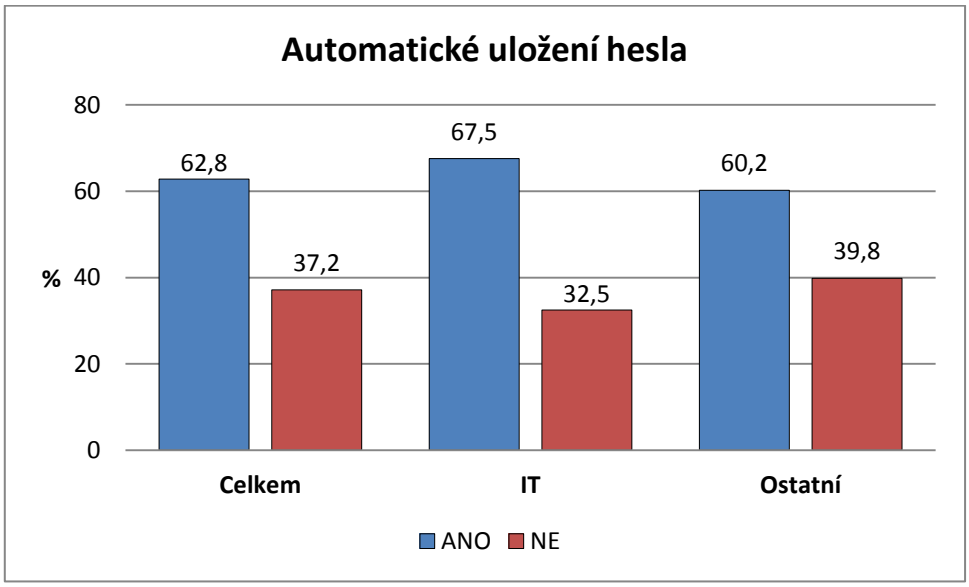
Hodnota	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	272	0,63	104	0,68	168	0,60
NE	161	0,37	50	0,32	111	0,40
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Funkci automatického uložení hesla používá 63% všech uživatelů. S přihlédnutím k faktu, že 61% uživatelů používá jedno hesla k přihlašování k více internetovým službám, je třeba poukázat na riziko toho, že může nastat ten případ, že potencionální útočník získá heslo ke všem uživatelovým účtům, včetně e-mailu, či bankovního účtu, a to pouze tím, že heslo zjistí „bez práce“ na základě automaticky uloženého hesla neopatrného uživatele. Opět překvapivé jsou výsledky skupiny uživatelů, kteří působí v IT. Ti totiž využívají funkci automatického uložení hesla více, než uživatelé ostatní, tuto funkci využívá 68% těchto uživatelů. Skutečnost, že 63%

procent uživatelů využívání funkce automatického zapamatování hesla, potvrzuje tvrzení dílčí hypotézy č. 3, většina uživatelů totiž opravdu využívá funkci automatického uložení hesla.

Grafické znázornění toho, jak je funkce automatického uložení hesla využívána vidíme na následujícím grafu.



Graf č. 5: Automatické uložení hesla

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Dle zjištěných výsledků můžeme říci, že automatické uložení hesla stejně jako užívání stejného hesla pro více účtů je využíváno velkou částí uživatelů a to i přesto, že kombinace těchto dvou faktorů negativně ovlivňuje bezpečnost uživatele.

Na závěr části, věnující se bezpečnosti hesla je třeba říci, že se v současné době stále více setkáváme s předepsanou minimální délkou i znakovou skladbou hesla při vytváření účtu nejen na sociálních sítích, čímž je uživatel dotlačen k užívání silného hesla. Jak tento trend roste, snižuje se počet užívaných slabých hesel, v budoucnu se proto dá očekávat, že uživatelé budou, i když ne mnohdy ze své vlastní iniciativy, ale přesto – používat silná a bezpečná hesla.

2.3.5 Veřejná přístupnost profilu

Dílčí hypotéza č. 4: Veřejně přístupné účty se u uživatelů, působících v informačních technologiích, objevují méně, než u ostatních uživatelů.

Veřejně přístupný profil je jedním z klíčových aspektů z pohledu bezpečnosti osobních údajů. Pokud totiž uživatel takovýto profil využívá, všichni ostatní uživatelé (i ti, které uživatel s veřejným účtem nemá v přátelích), mohou vidět vše, co neopatrný uživatel na sociální síti zveřejňuje, tedy nejen všechny osobní údaje, které o sobě uživatel zadal, ale také například fotky, videa a další data, která by měla zůstat soukromými a důvěrnými. Logicky se proto dá předpokládat, že uživatelé veřejný profil využívat nebudou, zvláště Ti, kteří působí v oblasti informačních technologií a proto jsou si, díky svým znalostem z této oblasti, více vědomi nebezpeční zneužití osobních dat.

Četnosti, resp. relativní četnosti výskytu použití nezabezpečeného účtu jsou shrnuty v následující tabulce.

Tab. č. 7: Veřejná přístupnost profilu

Hodnota	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	77	0,18	31	0,20	46	0,16
NE	356	0,82	123	0,80	233	0,84
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

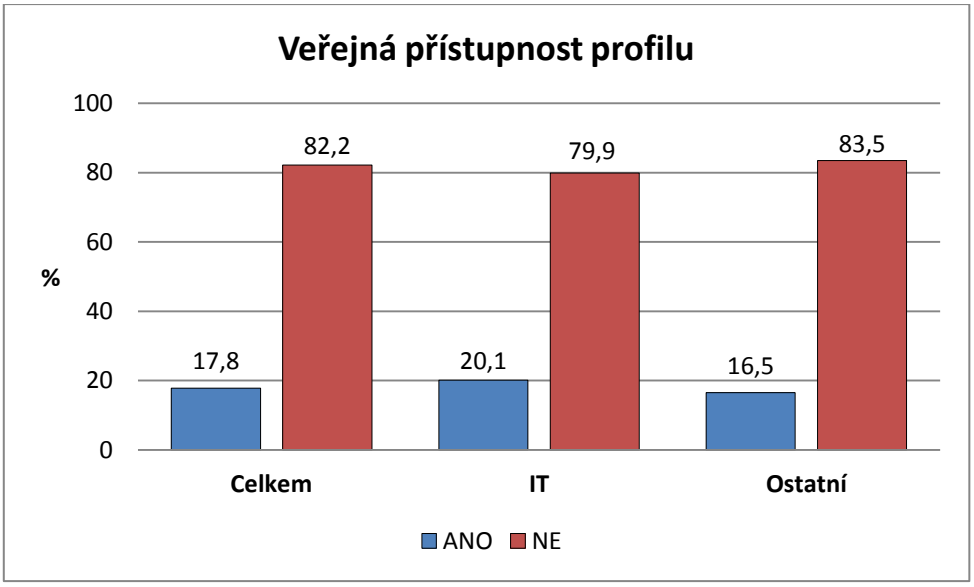
(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Výsledky přinesly nečekaný výsledek, nejen, že v celkovém pohledu využívá nezabezpečený profil celých 18% uživatelů, ale u uživatelů působících v informačních technologiích je to dokonce plných 20%, u ostatních uživatelů je veřejný profil využíván u 16% účtů. Tato čísla jsou dle mého názoru opravdu alarmující, jelikož přibližně každý pátý profil může být zobrazen naprosto cizím uživatelem a osobní údaje a data uložená na tomto profilu tak mohou být zneužita. Pracovní hypotézu č. 4, která tvrdí, že uživatelé z oblasti informačních technologií využívají nezabezpečené účty méně, s ohledem na výsledky pozorování zamítáme. Toto vysoké využívání nezabezpečeného účtu u uživatelů, působících v informačních technologiích, si lze jen

těžko vysvětlit. Uživatelé se tak totiž dobrovolně vystavují vysokému riziku narušení jejich bezpečnosti a zneužití jejich osobních údajů a dat. A ani to nejbezpečnější heslo je proti tomu neubrání.

Vzhledem ke zjištěným skutečnostem, odmítáme tvrzení hypotézy č. 4, uživatelé, kteří působí v oblasti IT totiž veřejný profil využívají více, než uživatelé ostatní.

Výsledky jsou znázorněny na následujícím grafu.



Graf č. 6: Veřejná přístupnost profilu

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

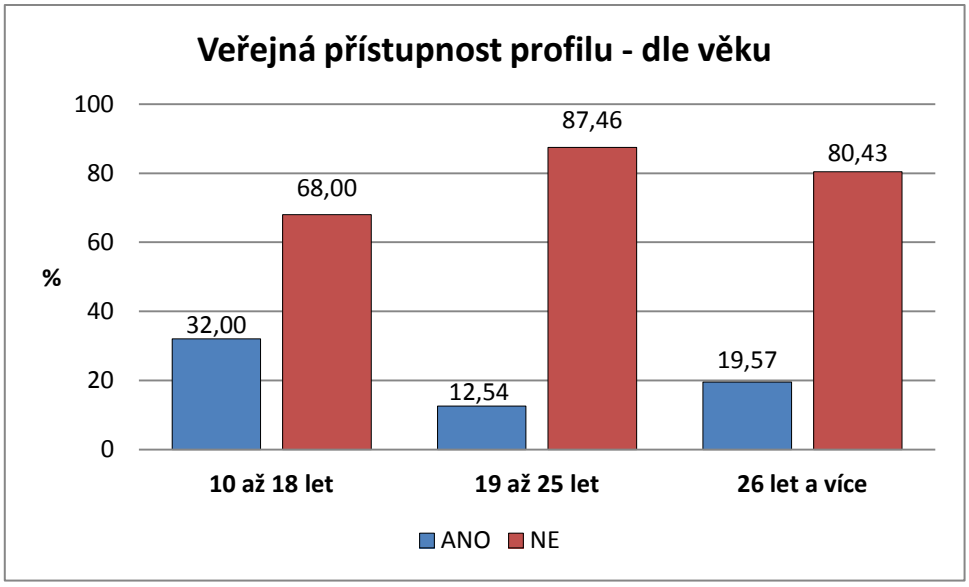
Srovnáním, které se v souvislosti s veřejnou přístupností profilu nabízí, je srovnání z pohledu věku uživatele. Využívání nezabezpečeného profilu je totiž nejrizikovější pro děti, tedy pro uživatele ve věku 10-18. Pro ostatní skupiny je veřejná přístupnost profilu také riziková, ale u dětí, kterým hrozí další nebezpečí ze strany únosců, deviantů atd., je využívání této možnosti rizikové ještě mnohem více. Případy, kdy bylo dítě napadeno či uneseno na základě informací z jeho profilu na sociální síti, totiž bohužel přibývají. Jaké výsledky byly pro otázku týkající se veřejného profilu zaznamenány u jednotlivých věkových skupin, můžeme vidět na grafu, který následuje.

Tab. č. 8: Veřejná přístupnost profilu – dle věku

Hodnota	10 až 18 let		19 až 25 let		26 let a více	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	32	0,32	36	0,13	9	0,20
NE	68	0,68	251	0,87	37	0,80
Celkem	**100**	**1,00**	**287**	**1,00**	**46**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Výsledky přinesly bohužel negativní zjištění, a to sice takové, že veřejný profil je u dětí využíván mnohem častěji, než u jiných věkových skupin. Uživatelé ve věku 10-18 používají veřejný profil ve 32% případů. Toto zjištění je s přihlédnutím na nebezpeční, které dětem hrozí, opravdu alarmující. Výsledky jsou graficky znázorněny na následujícím grafu. Z důvodu toho, že respondentů ve věku 35 až 45 let, resp 45 let a více bylo velmi málo a jejich výsledky jsou proto zkreslující, byly tito respondenti shrnuti do společné skupiny 26 let a více.



Graf č. 7: Veřejná přístupnost profilu – dle věku

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

2.3.6 Přijetí přátelství od neznámého uživatele

Přijetí přátelství od neznámého uživatele je další ze skutečností, která negativně ovlivňuje bezpečnost uživatelů a zvyšuje riziko zneužití jejich osobních údajů a dat. Nikdy totiž uživatel, který takovéto přátelství přijímá, nemůže mít jistotu, že neznámý

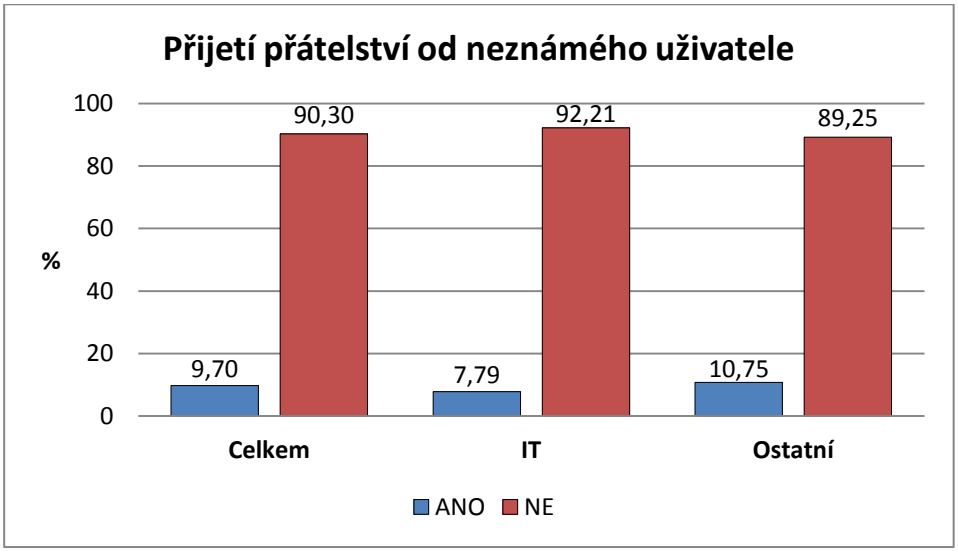
uživatel se s ním nesnaží spřátelit ve snaze zneužití osobních dat, či jiného druhu útoku. Přátelství bychom měli přijímat pouze od uživatelů, které dobře známe. Následující tabulka obsahuje výsledky respondentů na otázku, zda přijmou přátelství od neznámého člověk.

Tab. č. 9: Přijetí přátelství od neznámého uživatele

Hodnota	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	42	0,10	12	0,08	30	0,11
NE	391	0,90	142	0,92	249	0,89
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Jak můžeme z tabulky vyčíst, 10% všech respondentů je ochotno přijmout riziko a přijmout přátelství od neznámého člověka. Uživatelé z oblasti informačních technologií jsou toto riziko ochotni přijmout v 8% případů, ostatní uživatelé přijmou přátelství od neznámého člověka v 11% případů. Výsledky jsou graficky znázorněny na následujícím grafu.



Graf č. 8: Přijetí přátelství od neznámého uživatele

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Opět se nabízí srovnání, jak se liší výsledky pro jednotlivé věkové skupiny. Toto srovnání je předmětem dílčí hypotézy č. 5.

Dílčí hypotéza č. 5: Uživatelé mladší 18 let přijímají přátelství od neznámých uživatelů častěji, než uživatelé jiní.

Stejně jako veřejná přístupnost profilu je i přijetí přátelství od neznámých uživatelů nejrizikovějších pro děti a to ze stejných důvodů. Výsledky pro jednotlivé skupiny jsou zaznamenány v následující tabulce.

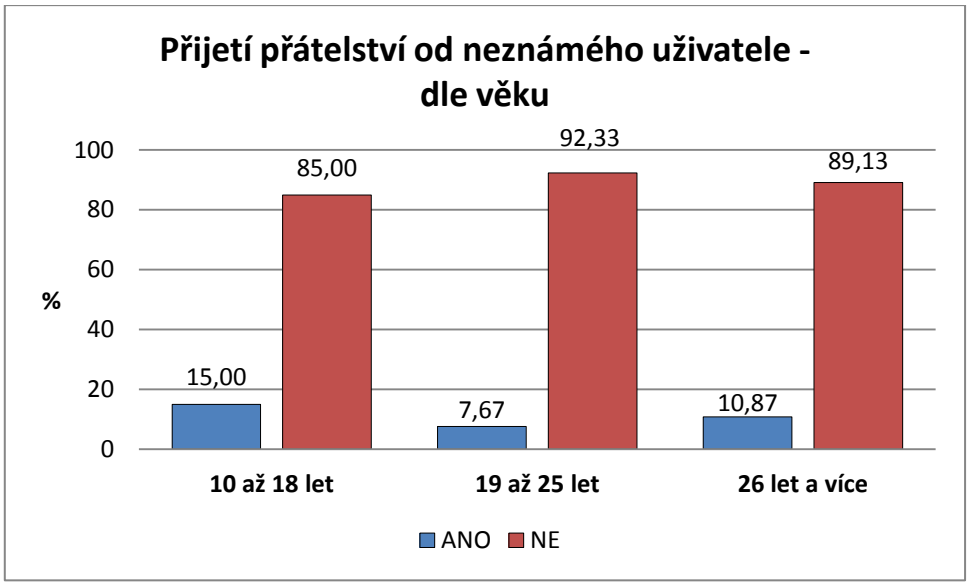
Tab. č. 10: Přijetí přátelství od neznámého – dle věku

Hodnota	10 až 18 let		19 až 25 let		26 let a více	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	15	0,15	22	0,08	5	0,11
NE	85	0,85	265	0,92	41	0,89
Celkem	**100**	**1,00**	**287**	**1,00**	**46**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Zjištěné výsledky jsou bohužel opět negativní, jelikož nejvyšší procento přijetí přátelství od neznámého uživatele bylo zaznamenáno u dětí. Děti přijímají přátelství od neznámého uživatele v 15% případů. Tento výsledek je možno, s přihlédnutím na nebezpečí hrozící dětem, považovat za výsledek znepokojivý. Způsobem, jak do budoucna bezpečnost chování dětí zlepšit, je zvýšená prevence a to především ze strany rodičů. K seznámení dětí s riziky hrozícím jim na Facebooku respektive na celém internetu by měly pomáhat také školy a další organizace, ale největší vliv na děti mají jejich rodiče, proto by snaha o zlepšení informovanosti a obezřetnosti dětí, měla začínat právě u rodičů.

Na základě výše popsaných zjištění, potvrzujeme tvrzení dílčí hypotézy č. 5, uživatelé ve věku 10 až 18 let přijímají přátelství od neznámých uživatelé častěji, než ostatní uživatelé. Výsledky jsou znázorněny na následujícím grafu.



Graf č. 9: Přijetí přátelství od neznámého – dle věku

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

2.3.7 Využívání aplikací a her, které pracují s osobními údaji

Na Facebooku se můžeme setkat s velkou spoustou aplikací a her, které pracují s osobními údaji. Při jejich prvním použití je uživatel vyzván, aby potvrdil použití svých údajů a dat aplikací. Z důvodu toho, že uživatel nemá jistotu, co přesně se s jeho údaji děje a kde jsou zaznamenány a použity, používání těchto aplikací a her se nedoporučuje. Používáním těchto aplikací mohou být údajů uživatele zneužity a to bez jeho vědomí.

Kolik uživatelů takovéto aplikace a hry využívá, je zobrazeno v následující tabulce.

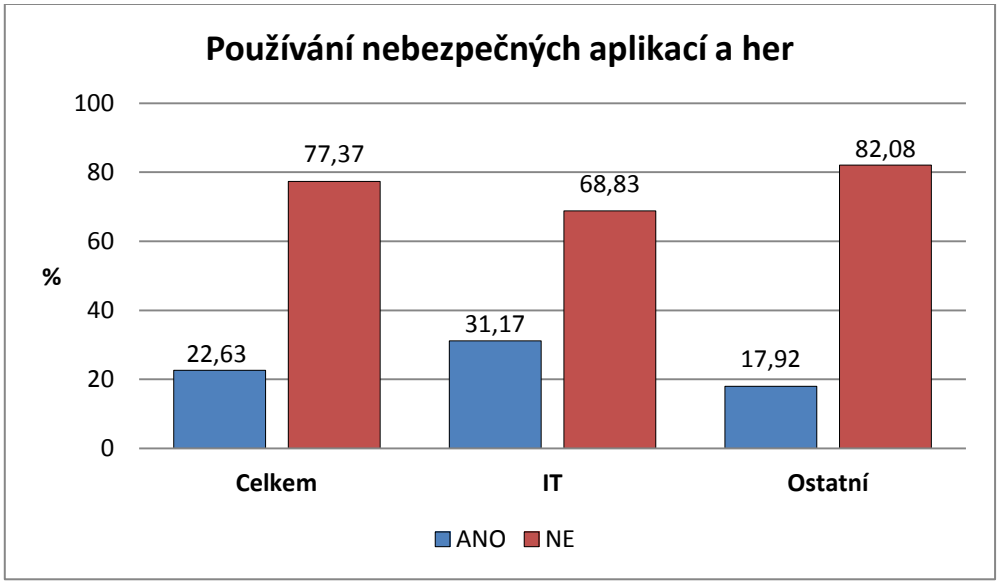
Tab. č. 11:Využívání aplikací a her

Hodnota	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	98	0,23	48	0,31	50	0,18
NE	335	0,77	106	0,69	229	0,82
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Z tabulky můžeme zjistit, že aplikace a hry, pracující s osobními daty uživatele využívá 23% uživatelů. V oblasti informačních technologií je to 31%, ostatní uživatelé takovéto aplikace používají v 18% případů. Riziko zneužití údajů prostřednictvím

aplikací není tak vysoké jako u jiných charakteristik, ale i přesto je to další z činností, kterými uživatelé snižují bezpečnost svých údajů. Grafické znázornění výsledků vidíme na následujícím grafu.



Graf č. 10: Využívání aplikací a her

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Znovu se můžeme ptát, jak se tyto výsledky mění pro jednotlivé věkové skupiny. O tom hovoří dílčí hypotéza č. 6.

Dílčí hypotéza č. 6: Nebezpečné aplikace a hry využívají nejčastěji uživatelé mladší 18 let.

Jak často využívají potencionálně nebezpečné aplikace a hry jednotlivé věkové skupiny vidíme na následující tabulce.

Tab. č. 12: Využívání aplikací a her – dle věku

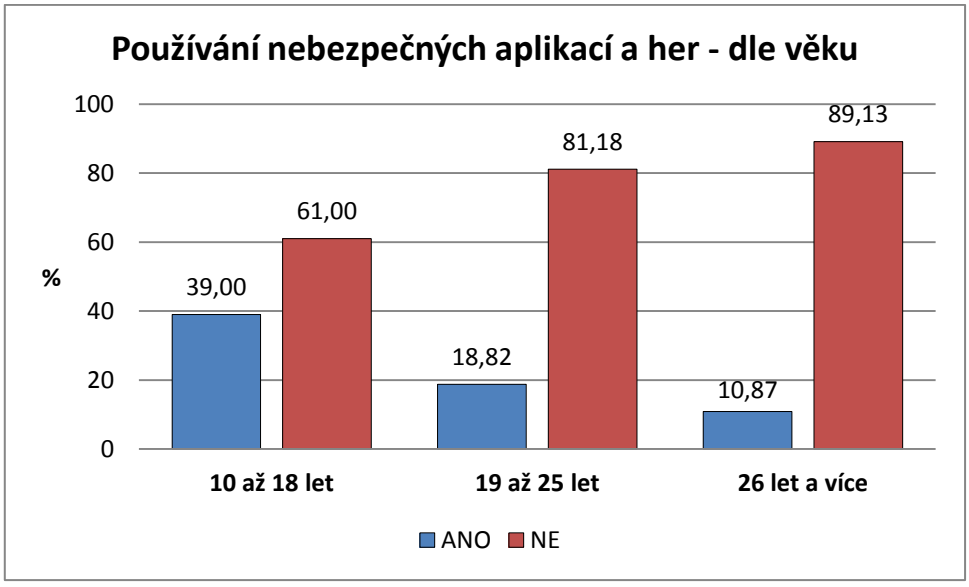
Hodnota	10 až 18 let		19 až 25 let		26 let a více	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	39	0,39	54	0,19	5	0,11
NE	61	0,61	233	0,81	41	0,89
Celkem	**100**	**1,00**	**287**	**1,00**	**46**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Na základě výsledků můžeme prohlásit, že nejvíce jsou aplikace a hry využívány dětmi, důvod je zřejmý, děti se jednoduše chtějí bavit a tyto aplikace a hry využívat. Často tak v touze po nové hře odsouhlasí použití osobních údajů aplikací. Čím starší uživatelé jsou, tím tyto aplikace a hry využívají méně.

Dané výsledky potvrzují hypotézu č. 6, nebezpečné aplikace a hry opravdu nejvíce využívány u věkové skupiny 10-18 let.

Grafické znázornění výsledků je zobrazeno na následujícím grafu.



Graf č. 11: Využívání aplikací a her – dle věku

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

2.3.8 Jsou si uživatelé vědomi nebezpečí zneužití osobních údajů?

Dílčí hypotéza č. 7: Uživatelé jsou si vědomi nebezpečí zneužití jejich osobních údajů a dat.

Dotazníková otázka číslo 9 zjišťovala, zda si je respondent vědom nebezpečí zneužití jeho osobních údajů. Cílem otázky bylo zjistit, kolik uživatelů je přesvědčeno, že jejich osobní data nemohou být zneužita. Tedy kolik uživatelů naprosto důvěřuje bezpečnosti svého profilu a nebojí se na svém profilu uveřejnit jakoukoliv informaci. Výsledky jsou zachyceny v následující tabulce.

Tab. č. 13: Vědomí možnosti zneužití údajů

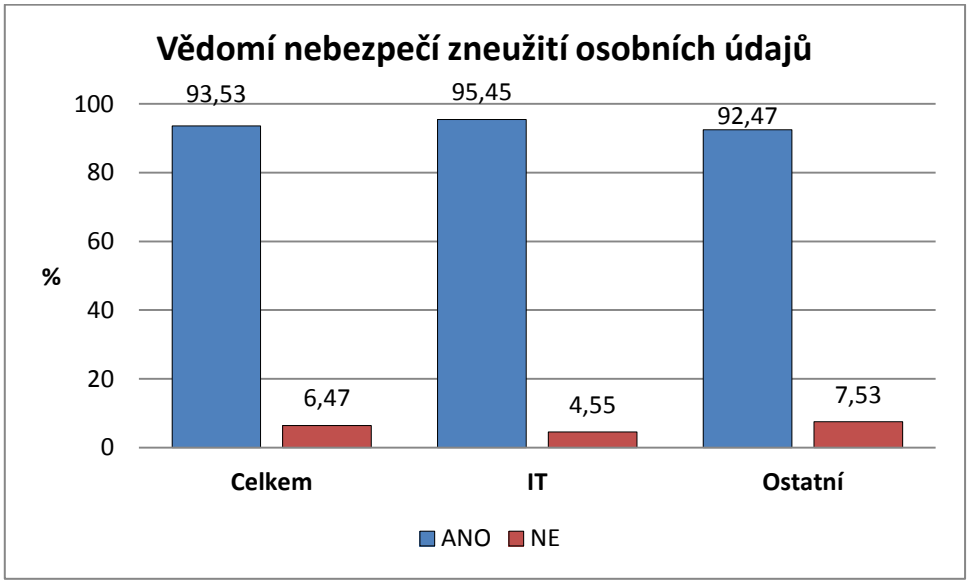
Hodnota	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
ANO	405	0,94	147	0,95	258	0,92
NE	28	0,06	7	0,05	21	0,08
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Je vidět, že drtivá většina uživatelů, konkrétně 94% si je vědoma nebezpečí zneužití jejich osobních údajů.

Tvrzení dílčí hypotézy č. 7 tak nepřijímáme, ne všichni uživatelé jsou si vědomi toho, že jejich data mohou být zneužita.

Při porovnání výsledků uživatelů působící v informačních technologiích a uživatelů ostatních, můžeme říci, že uživatelé z oblasti IT vykazují lepší výsledky, avšak rozdíl není nijak výrazný. Graficky jsou výsledky interpretovány na následujícím grafu.



Graf č. 12: Vědomí možnosti zneužití údajů

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

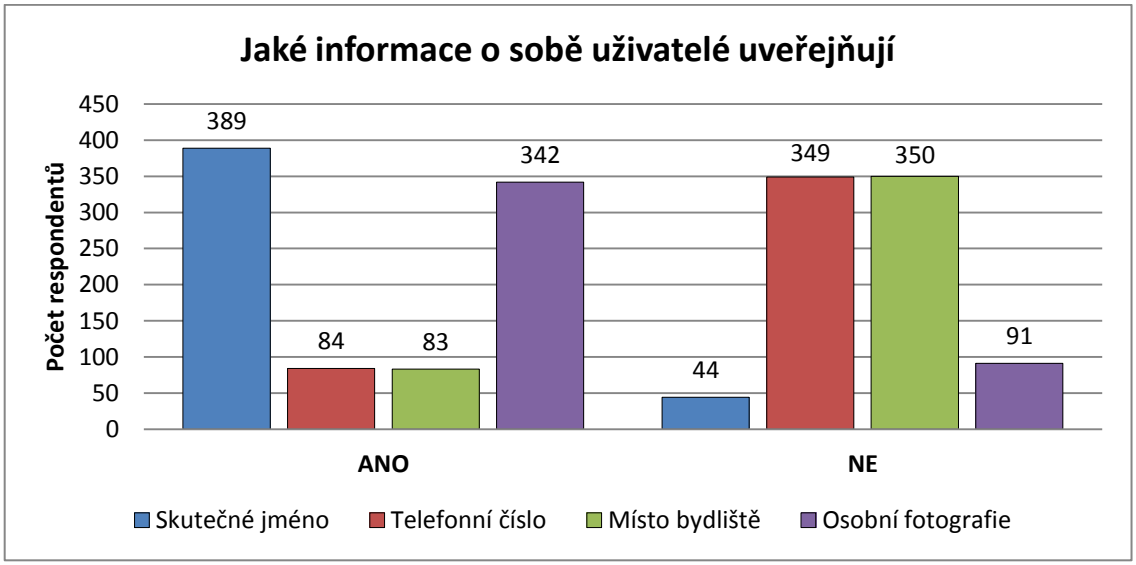
2.3.9 Jaká data o sobě uživatelé uveřejňují

Osobní údaje a data, která o sobě uživatelé na sociálních sítích uveřejňují, jsou na jednu stranu věcí, která plně zapojuje uživatele do dění na sociální sítí a umožňuje

mu plně využít všechny možnost, které mu sociální síť nabízí. Tím, že například uvede bydliště, systém mu doporučí profily uživatelů se stejným bydlištěm. Pokud uvede školu, na které studoval, díky této informaci umožní sociální síť spojit se s dřívějšími spolužáky a kamarády, kteří navštěvovali stejnou školu.

Těchto funkcí, které jsou založeny na uveřejněných informací uživatele je mnohem více, sociální síť v dnešní podobě je schopna pracovat s mnoha údaji, od zveřejnění zaměstnavatele, po vytvoření míst, kde se uživatel v poslední době nacházel na základě zadaných souřadnicí GPS, či jmen těchto destinací. Zveřejňování osobních údajů a dat je tedy na jednu stranu věcí pro uživatele prospěšnou, díky těmto datům může vést „plnohodnotný" život na sociální síti. Z pohledu bezpečnosti však zveřejňování osobních údajů představuje nebezpečí a riziko pro uživatele. Na základě těchto dat může totiž potenciální útočník zjistit, kde uživatel bydlí, jakou navštěvuje školu, či zda se chystá na dovolenou a jeho byt či dům tak bude v daném termínu prázdný.

Přehled toho, jaké informace o sobě uživatelé dobrovolně uveřejňují, zachycuje následující graf:



Graf č. 13: Informace zveřejňované uživateli

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

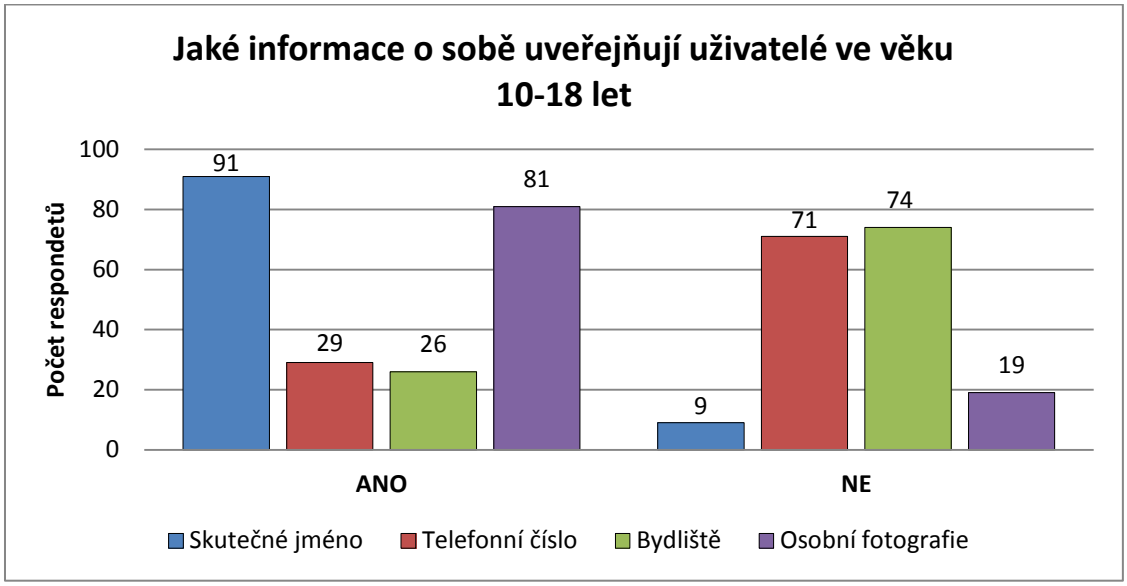
Z grafu můžeme vidět, že skutečné jméno je údajem, které na svých profilech uveřejňuje 389 respondentů, tedy 90%. Skutečné jméno je tedy údajem, u kterého uživatelé necítí velké riziko zneužití, a proto jej drtivá většina z nich používá. Další

informací, kterou uživatelé ve většině poskytují, jsou osobní fotografie. K jejich zveřejňování se přihlásilo 342 respondentů, což činí 79%. U osobních fotografií však již nastává větší riziko zneužití, než u skutečného jména. Pouze ze znalosti jména potencionální útočník příliš údajů nezíská, kdežto z osobních fotografií může získat poměrně velký počet informací, začínaje podobou vlastníka účtu a konče vzhledem jeho bytu či domu poškozeného. Naopak dvě informace, které si uživatelé velmi chrání, jsou telefonní číslo a místo bydliště, tyto dvě informace poskytuje téměř stejný počet respondentů a to 19%. Ostatních 81% tyto informace neuveřejňuje. Z toho můžeme soudit, že uživatelé jsou si vědomi toho, že tyto informace jsou informace velmi důvěrné a proto je nezveřejňují. Tento výsledek však není příliš pozitivní, jelikož téměř každý pátý uživatel takovou informaci zveřejní, čímž opět snižuje svou bezpečnost a dobrovolně poskytuje potencionálnímu útočníkovi více informací.

Zajímavou charakteristikou, která se v souvislosti s uveřejňováním informací nabízí, je uveřejňování informací u dětí, tedy u uživatelů mladších 18 let. O tomto problému hovoří hypotéza č. 8.

Dílčí hypotéza č. 8: Uživatelé mladší 18 let častěji uveřejňují důvěrné osobní informace a data.

Odpovědí na tuto otázku je následující graf, který tento problém zachycuje. Respondentů mladších 18 let bylo přesně 100.



Graf č. 14: Informace zveřejňované uživateli ve věku 10-18 let

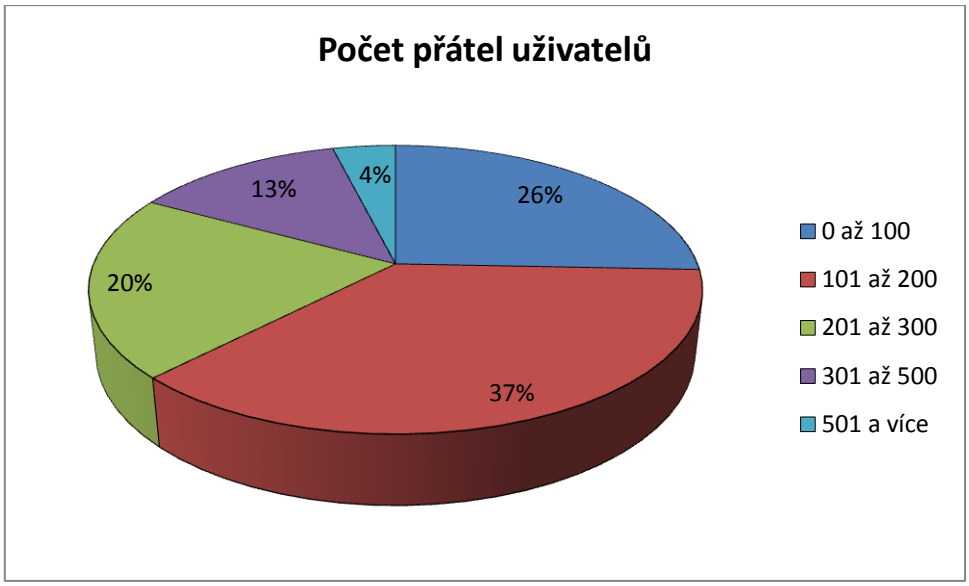
(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Ve srovnání s celkovými výsledky uživatelé ve věku do 18 let vykazují horší výsledky, tedy že důvěrné informace poskytují častěji. Již tato skutečnost není dobrou zprávou, s přihlédnutím na věk těchto uživatelům a na specifická nebezpečí, která právě této skupině hrozí. Nejvíce odlišné výsledky, bohužel v negativním slova smyslu, tito uživatelé vykazují právě u dvou nejosobnějších informací, tedy u telefonního čísla a místa bydliště. Oproti celkovým 19% procentům u obou těchto faktorů u všech uživatelů, telefonní číslo zveřejňuje 29% dětí a místo bydliště 26% dětí. Tato čísla bohužel potvrzují, že děti si nejsou tolik vědomi nebezpečí, které jim na sociálních sítích, potažmo na celém internetu může hrozit a že lehkovážně poskytují i ty nejosobnější informace. Jediným způsobem, jak tento fakt omezit je zlepšit přístup rodičů a vysvětlit dětem nebezpečí, kterému se nevědomky a mnohdy zbytečně vystavují. Tento fakt tedy přijímá hypotézu č. 8 – uživatelé ve věku 10-18 skutečně uveřejňují důvěrné informace častěji.

2.3.10 Doplňující otázky – počet přátel

Počet přátel, v prostředí sociálních sítí myšleno jako počet uživatelů, které konkrétní uživatel označí jako své přátelé. Přátelé pak mohou vidět nejen aktivitu a data uživatele, ale také s ním například sdílet události, či komunikovat prostřednictvím chatu, který je integrován přímo na sociální síti. Vzhledem k tomu, že přátelé na sociální síti mohou vidět všechnu aktivitu a data uživatele, logicky vyplývá, že by uživatelé měli jako přátele označovat pouze osoby, které dobře znají osobně. Počet přátel na Facebooku by tedy mohl odpovídat počtu lidí, které uživatel zná osobně z reálného světa. Často tomu však tak není, můžeme se setkat s uživateli, jejichž seznam přátel je opravdu rozsáhlý, ne výjimečně může přesáhnout dokonce číslo 1000. V honbě za vysokým počtem přátel si však tito uživatelé jako své přátele označují i osoby, které osobně znají jen velmi málo, nebo je neznají vůbec. Toto jednání bylo popsáno již v části této práce, týkající se přijetí přátelství od neznámého člověka. Vysoký počet přátel tedy v některých případech může znamenat zvýšené riziko toho, že mezi svými přáteli má uživatel osobu, která chce jeho data zneužít, či na uživatele nějakým způsobem zaútočit či ho ohrozit.

Jak respondenti na otázku týkající se počtu jejich uživatelé na Facebooku odpověděli, zobrazuje následující graf.



Graf č. 15: Počet přátel uživatelů

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Jak můžeme na grafu vidět, uživatelé mají nejčastěji mezi 101 až 200 přáteli, k tomuto počtu přátel se přihlásilo 37% procent všech respondentů. 17% všech respondentů má ve svých profilech více, než 301 přátel. 4% všech mají dokonce více než 501 přátel. Pozitivním zjištěním je, že většina uživatelů má počet přátel nižší, než 200. Tento počet je dle mého názoru v pořádku, neboť při tomto počtu je vysoká šance, že uživatel zná všechny své přátele na sociální síti také v reálném životě. Naopak počet přátel vyšší jak 301 bych označil už jako rizikový, většinou totiž člověk nemá v reálném světě tolik známých a kamarádů, ale záleží samozřejmě na konkrétním člověku. Počet přátel vyšší než 501 však již považuji za rizikový, šance, že se v přátelích objevují již osoby uživateli zcela neznámé a tím potenciálně nebezpečné, je dle mého názoru velmi vysoká. Celkově bych však tuto charakteristiku hodnotil pozitivně, většina uživatelů si, jak mohu z vlastní zkušenosti potvrdit, do přátel přidává opravdu jen ty osoby, které dobře zná z reálného života.

Jak již bylo naznačeno výše, u uživatelů s vysokým počtem přátel hrozí riziko, že se v jejich přátelích nacházejí neznámé osoby, tedy že jsou tito uživatelé ochotni přijímat přátelství od neznámých osob. K vyšetření této závislost bylo použito řešení pomocí následující čtyřpolní tabulky, která daný problém zobrazuje. Jako vysoký počet přátel byl označen počet větší, než 301. Tato charakteristika je předmětem hypotézy č. 9.

Dílčí hypotéza č. 9: Uživatelé s vysokým počtem přátel přijímají častěji přátelství od neznámých uživatelů.

Tab. 14: Závislost vysokého počtu přátel a přijetí od neznámého

Přijetí od neznámého / Vysoký počet přátel	ANO	NE	Celkem
ANO (vyšší, než 301)	9	65	74
NE (nižší, než 301)	33	326	359
Celkem	**42**	**391**	**433**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Z tabulky vyplývá, že 9 respondentů uvedlo vysoký počet přátel a zároveň je ochotno přijmou přátelství od neznámého uživatele. V procentuálním vyjádření to znamená, že 21% uživatelů, kteří jsou ochotni přijmout přátelství od neznámého má zároveň vysoký počet přátel, tito uživatelé se tak vystavují vysokého riziku.

K otestování nezávislosti zkoumaných znaků, tedy vysokého počtu přátel a přijetí přátelství od neznámého uživatele využijeme test nezávislosti dvou kvalitativních znaků. (část 1.1.4)

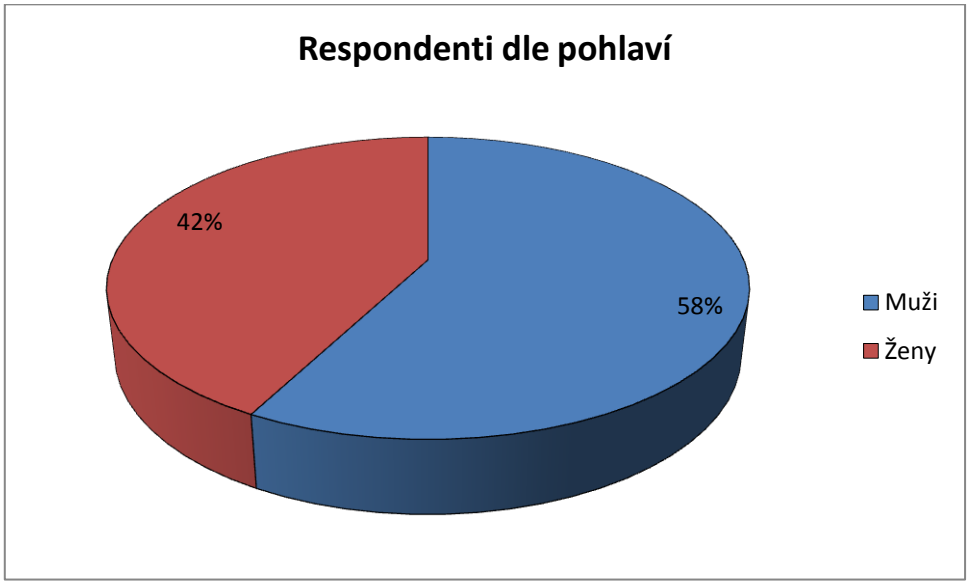
Zkoumaný znak A: Vysoký počet přátel uživatele
Zkoumaný znak B: Přijetí přátelství od neznámého uživatele
1. Definujeme nulovou, resp. alternativní hypotézu:
Nulová hypotéza H_0: Zkoumané znaky jsou nezávislé, vysoký počet přátel neovlivňuje ochotu uživatele přijmout přátelství od neznámého uživatele.
Alternativní hypotéza H1: Zkoumané znaky jsou závislé, vysoký počet přátel ovlivňuje ochotu uživatele přijmout přátelství od neznámého uživatele.
2. Hodnota testového kritéria $\chi^2 \doteq 0{,}6179$
3. Kritický obor je $W_\alpha = \{\chi^2 : \chi^2 \geq 3{,}841\}$
4. Závěr testu. Protože se hodnota testového kritéria v kritickém oboru nerealizovala, zamítáme na 5%-ní hladině významnosti alternativní hypotézu H_1 a přijímáme nulovou hypotézu H_0. S 5%-ní možností omylu lze tedy prohlásit, že znaky A a B jsou na sobě

nezávislé, vysoký počet přátel tedy neovlivňuje ochotu uživatele přijímat přátelství od neznámých uživatelů.

Dle zjištěných výsledků dílčí hypotézu č. 9 nepřijímáme, uživatelé s vysokým počtem přátel nepřijímají přátelství od neznámých uživatelů častěji, než uživatelé jiní.

2.3.11 Doplňující otázky – pohlaví a věk uživatele

Počet žen i mužů na sociálních sítích, resp. na Facebooku je téměř vyrovnaný, stejně jako v reálném světě. Podle údajů Českého statistického úřadu z ledna 2012, je na českém Facebooku 51% žen a 49% mužů. To, jaké bylo složení dle pohlaví u respondentů mého dotazníkového šetření, zobrazuje následující graf.

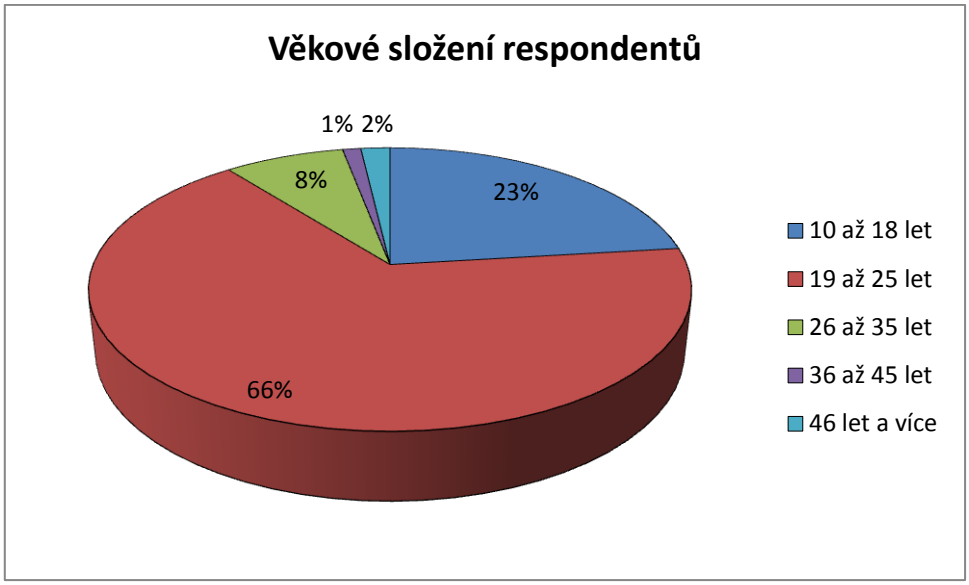


Graf č. 16: Respondenti dle pohlaví

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Jak je z grafu patrno, mnou realizované dotazníkové šetření, vyplnilo 58% mužů a 42% žen. Rozdíl oproti celkovému údaji si vysvětluji tím, že v důsledku menšího vzorku dat vzniklo v tomto ohledu statistické zkreslení. Při větším počtu vzorků dat by se tato hodnota měnila a konvergovala by k celkovému údaji, tedy 51% žen a 49% mužů.

Další statistickou otázkou, která byla v rámci dotazníku položena, byl dotaz na věk respondenta. Dá se předpokládat, že sociální síť Facebook využívají zejména mladí lidé, počet mladých lidí bude navíc umocněn tím, že nezanedbatelný počet respondentů byli lidé z mého okolí, kteří jsou mi blízcí věkem, čímž může být způsobeno lehké statistické zkreslení v podobě vyššího zastoupení mladých lidí. Věkové složení respondentů představuje následující graf.



Graf č. 17: Respondenti dle věku

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Výsledky ukazují, že většina respondentů patří do věkové skupiny 19-25 let. Zastoupení této skupiny je v porovnání s výsledky všech uživatelů sociální sítě Facebook v České republice, které uvádí Český statistický úřad, vyšší a to z důvodů, které jsou popsány nad grafem.

2.3.12 Počet hodin denně strávených na Facebooku

Další otázkou, zařazenou v závěru dotazníku, byla otázka týkající se počtu hodin strávených na Facebooku denně. V následující tabulce jsou zapsány výsledky dané

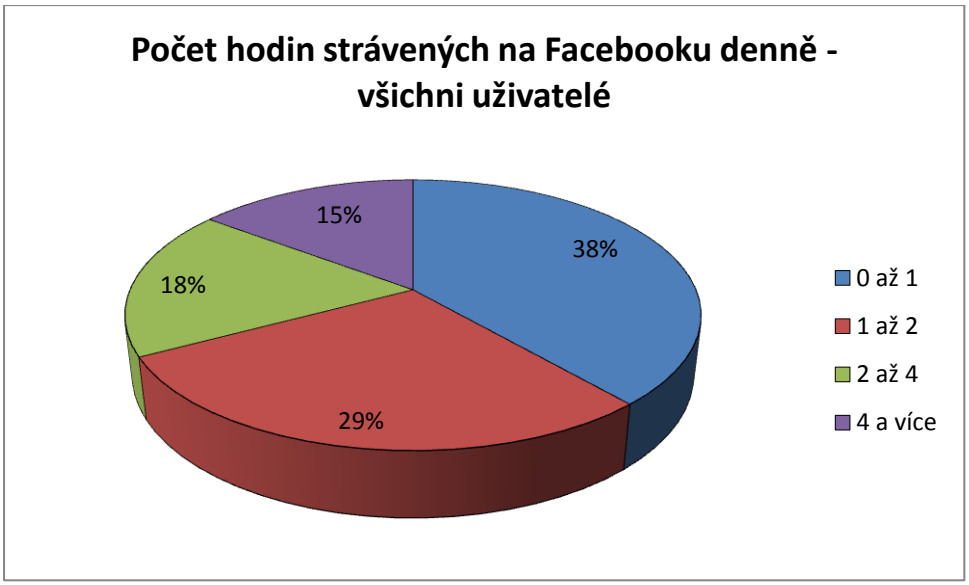
otázky, pro zajímavost je do tabulky začleněno také srovnání počtu hodin strávených denně na Facebooku u uživatelů, kteří působí v oblasti informačních technologií a u uživatelů ostatních.

Tab. č. 15: Počet hodin strávených na Facebooku denně

Počet hodin strávených na Facebooku denně	Všichni uživatelé		IT		Ostatní	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
0 až 1	164	0,38	68	0,44	96	0,34
1 až 2	122	0,28	42	0,27	80	0,29
2 až 4	77	0,18	24	0,16	53	0,19
4 a více	70	0,16	20	0,13	50	0,18
Celkem	**433**	**1,00**	**154**	**1,00**	**279**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Graficky je počet hodin strávených na Facebooku denně pro všechny uživatele zobrazen na následujícím grafu.



Graf č. 18: Počet hodin strávených na Facebooku denně

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Jak vidíme, 38% uživatelé na Facebooku stráví maximálně jednu hodinu denně. Toto zjištění je pozitivní, Facebook není doposud pro většina lidí nezbytnou „součástí života“. 16% respondentů však uvedlo, že na Facebooku tráví více, než 4 hodiny denně,

což představuje již výrazné ovlivnění volného času a může předpovídat u daného jedince závislost na sociálních sítích, či na internetu obecně. Při porovnání uživatelů z oblasti informačních technologií a uživatelů ostatních můžeme prohlásit, že uživatelé, působící v informačních technologiích, tráví denně na Facebooku méně času, než uživatelé jiní.

V současné době je stále více diskutován fakt, že děti a mladí lidé tráví na Facebooku, či obecně na internetu značné množství času. O tomto faktu mluví hypotéza č. 10.

Dílčí hypotéza č. 10: Nejvíce času denně stráví na Facebooku uživatelé ve věku 10-18 let.

Jak se liší doba strávená na Facebooku denně dle věku, znázorňuje následující tabulka.

Tab. č. 16: Vztah mezi věkem uživatele a počtem hodin na Facebooku denně

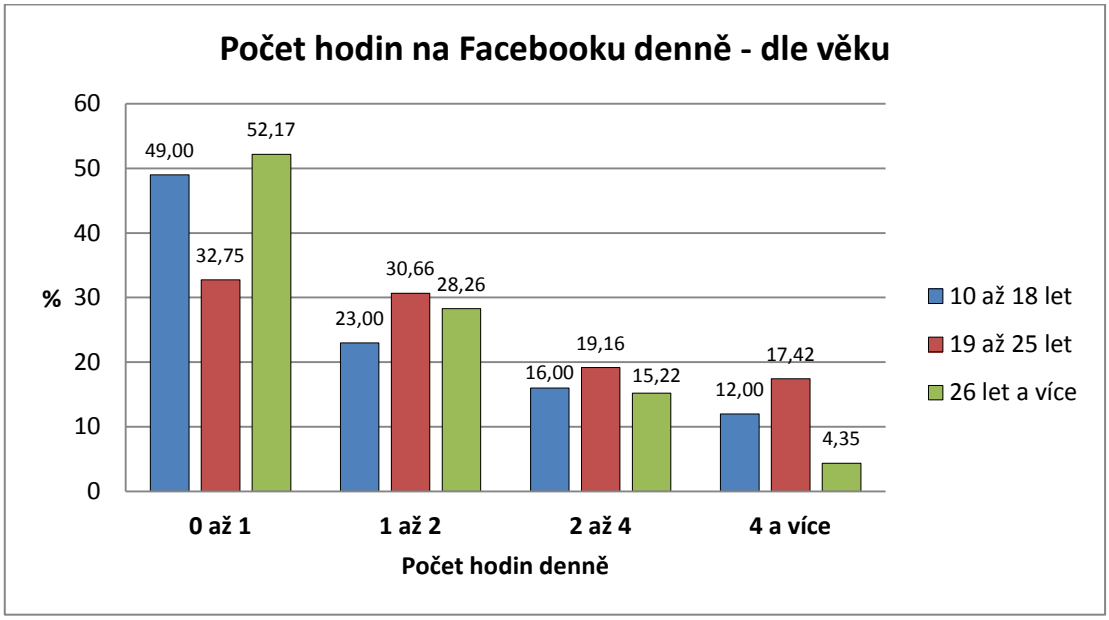
Věk uživatele / Počet hodin	10 až 18 let		19 až 25 let		26 let a více	
	Četnost	Relativní četnost	Četnost	Relativní četnost	Četnost	Relativní četnost
0 až 1	49	0,49	94	0,33	24	0,52
1 až 2	23	0,23	88	0,31	13	0,28
2 až 4	16	0,16	55	0,19	7	0,15
4 a více	12	0,12	50	0,17	2	0,05
Celkem	**100**	**1,00**	**287**	**1,00**	**46**	**1,00**

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

Dle výsledků vidíme, že nejvíce času na Facebooku tráví uživatelé ve věku 19 až 25 let. Více než 4 hodiny tráví na této sociální síti denně více než 17% z nich, 36,5% uživatelů v tomto věku tráví denně na Facebooku více, než 2 hodiny. U uživatelů starších je patrné, že na sociální síti stráví méně času, převládají nízké doby, více než 4 hodiny denně pak u internetu, resp. sociální sítě tráví pouze 3% z těchto uživatelů.

Na základě zjištěných faktů odmítáme tvrzení hypotézy č. 10. Nejvíce času na Facebooku totiž netráví uživatelé ve věku 10-18 let, jak hypotéza č. 10 tvrdí, ale uživatelé ve věku 19-25 let.

Výsledky jsou znázorněny na následujícím grafu.



Graf č. 19: Počet hodin na Facebooku denně – dle věku

(Zdroj: Vlastní dotazníkové šetření; Zpracování: Vlastní)

2.3.13 Vyhodnocení dotazníkového šetření

Na základě výsledků dílčích hypotéz přijímáme tvrzení hypotézy základní, chování uživatelů na sociální síti Facebook je rizikové.

Průzkumu se zúčastnilo 433 respondentů. Mužů bylo 250, žen 183. Respondentů, kteří studují či pracují v oblasti informačních technologií bylo 154, ostatních respondentů bylo 279.

O výsledcích práce budou informování respondenti, kteří o tuto možnost projevili zájem a uvedli svoji e-mailovou adresu. Těchto respondentů bylo 135.

3 Návrhy řešení a doporučení

Dílčím cílem, který si práce vytyčila, bylo určit, která skupina uživatelů se na Facebooku chová nejrizikověji a hrozí jí tak největší potenciální nebezpečí.

Na základě výsledků výzkumu můžeme prohlásit, že nejvíce potencionálně ohroženou skupinou je jednoznačně skupina uživatelů ve věku 10-18 let. Tito uživatelé totiž vykazují téměř ve všech sledovaných ukazatelích nejrizikovější chování.

Dalším dílčím cílem práce bylo zjistit, jakých největších chyb z hlediska bezpečnosti, se dopouští nejohroženější skupina uživatelů sociální sítě Facebook

Nejohroženější skupina uživatelů, tedy věková skupiny ve věku 10-18 let, se největších chyb dopouští bohužel u těch ukazatelů, které lze označit jako velmi rizikové. Největších chyb se uživatelé ve věku 10-18 let dopouští především v těchto ukazatelích:

- využívání veřejného účtu
- přijetí přátelství od neznámého člověka
- poskytování důvěrných informací, jako je telefonní číslo či místo bydliště

U těchto ukazatelů vykazují uživatelé ve věku 10-18 let nejvíce rizikové chování v porovnání s ostatními věkovými skupinami. Všechny tyto charakteristiky naznačují, že poměrně vysoké procento dětí se na sociální síti Facebook chová velmi nezodpovědně a vystavují se zbytečně vysokému riziku. Dle mého názoru je jedním z důvodu takového chování neznalost a nevědomost dětí o nebezpečích, které jim na sociální síti mohou hrozit.

Opatřením, jak změnit uvažování a především chování dětí, je jednoznačně prevence.

Největší vliv na chování dětí mají jejich rodiče, proto by právě oni měli být těmi, kteří své děti informují o rizicích a nebezpečích, které jim na sociální síti, respektive na celém internetu hrozí. Dalším místem, kde by děti měly být o nebezpečí informovány, jsou školy a další organizace.

Důležitost takové prevence umocňuje fakt, že bohužel stále přibývá případů, kdy bylo dítě uneseno, či jinak napadeno a to na základě informací, které uveřejnilo na svém profilu. Pokud dítě naprosto veřejně oznamuje informace nejen o tom, jak se

jmenuje a jak vypadá, ale také kde bydlí, kam chodí do školy či jaké má telefonní číslo, potencionální útočník může tyto informace velmi snadno zneužít a dítě na základě těchto informací napadnout. Proto by měla být prevenci kladena dostatečná pozornost a důležitost, protože může nejen ochránit data dítěte, ale v mnoha případech mu i zachránit život.

Dále se práce snažila odpovědět na otázku, jak se z hlediska bezpečnosti chovají uživatelé, kteří působí v informačních technologiích a mají tak vyšší znalosti v oblasti bezpečného chování na sociálních sítích, resp. na internetu obecně. V souvislosti s tímto dílčím cílem si také práce vytyčila odpovědět na otázku, jak rizikové je chování těchto uživatelů v porovnání s ostatními uživateli.

Výsledek výzkumu je takový, že uživatelé, kteří působí v oblasti informačních technologií, vykazují stejné a v několika ohledech dokonce i horší chování než uživatelé ostatní.

Uživatelé z oblasti informačních technologií kladou větší důraz na bezpečnost hesla, kde vykazují jasně lepší výsledky než ostatní uživatelé. V ostatních ukazatelích se však chování těchto uživatelů nijak neliší od chování ostatních uživatelů.

Řešením, jak chování lidí zlepšit, je opět prevence, tedy informovat a poukázat na rizika, která jim hrozí. Tyto informace o rizicích, která uživatelům na sociálních sítích hrozí by měly být zveřejňovány nejen na internetu na specializovaných internetových portálech, ale také na místech, kde se tyto informace dostanou k široké veřejnosti, tedy v novinách, či televizním vysílání.

Doporučení pro samotné uživatele je vyvarovat se zveřejňování více informací než je nutné. Na profilu by se tak neměly objevovat informace o zájmech, majetku či zaměstnání uživatele. Zároveň by měl být kladen důraz na využívání bezpečného hesla.

Závěr

Výzkum bohužel prokázal, že chování mnoha uživatelů je velmi rizikové a uživatelé se vystavují vysokému nebezpečí zneužití jejich osobních dat a údajů.

Dle mého názoru závažným problémem, který tato práce potvrdila a který je v poslední době ve společnosti stále více diskutován, je velmi rizikové chování dětí na sociální síti Facebook. Velká část dětí se na Facebooku chová nezodpovědně, ať už jde o poskytování důvěrných osobních údajů, či například o přijímání přátelství, od zcela neznámých uživatelů. Tímto chováním se, nutno říci, že často zbytečně, vystavují nebezpečí zneužití jejich osobních údajů a dat.

Práce však odhalila rizikové chování nejen u dětí, ale i u ostatních uživatelů. Bezpečnost osobních dat na sociální síti je faktorem, který může uživatel svým chováním ovlivnit, proto by mělo být v zájmu každého jednotlivce, aby jeho chování bylo co nejbezpečnější.

Smyslem této práce je upozornit uživatele na možná nebezpečí a změnit jejich přístup k Facebooku a hlavně chování na této sociální síti. Facebook totiž rozhodně není místem, kde bychom mohli naprosto klidně uveřejňovat informace, ale naopak místem, kde mohou být naše informace zneužity.

Pokud by tato práce změnila pohled na Facebook a zlepšila chování alespoň jednoho uživatele, považoval bych ji za úspěšnou a přínosnou.

Seznam použité literatury

BEZPECNYINTERNET. Desatero bezpečného internetu. *Bezpecnyinterne.cz* [online]. ©2012 [cit. 2013-05-02]. Dostupné z: http://www.bezpecnyinternet.cz/deti/rady-pro-tebe/desatero-bezpecneho-internetu.aspx

BLATNÁ, Dagmar, 2007. *Statistika a pravděpodobnost*. 3. vyd. Praha: Bankovní institut vysoká škola, 114 s. ISBN 978-80-7265-109-2.

BURIÁNEK, Jiří, 1988. *Metody a techniky sociologického výzkumu.* Praha: Státní pedagogické nakladatelství, 137 s.

CESIVSITI. Češi v síti 2011. *Cesivstiti.cz* [online]. ©2009–2013 [cit. 2013-05-02]. Dostupné z: http://cesivsiti.cz/tags/češi2011

ČESKÝ STATISTICKÝ ÚŘAD. Uživatelé Facebooku. *Czso.cz* [online]. ©2013 [cit.2013-05-06]. Dostupné z: http://www.czso.czcsu/redakce.nsf/i/uzivatele_facebooku

ECKERTOVÁ, Lenka a Daniel DOČEKAL, 2013. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 224 s. ISBN 978-80-251-3804-5.

FINEXPERT. Jak si vytvořit bezpečné heslo. *Finexpert.e15.cz* [online]. ©2013 [cit. 2013-05-02]. Dostupné z: http://finexpert.e15.cz/jak-si-vytvorit-bezpecne-heslo

GABRIELOVÁ, Alena, 2012. *Základy sociologie, sociální komunikace a sociologického výzkumu.* Kladno-Kročehlavy: Vyšší odborná škola územně-správní a jazyková škola s právem státní jazykové zkoušky, 80 s. ISBN 978-80-904859-3-8.

HINDLS, R., J. SEGER a S. HRONOVÁ, 2002. *Statistika pro ekonomy*. Brno: Professional Publishing, 415 s. ISBN 80-86419-26-6

KROPÁČ, Jiří, 2009. *Statistika B: jednorozměrné a dvourozměrné datové soubory, regresní analýza, časové řady.* 2. vyd. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, v, 145 s. ISBN 978-80-214-3984-9.

KULHÁNKOVÁ, Hana a Jakub ČAMEK, 2010. *Fenomén facebook.* Kladno: BigOak, 128 s. ISBN 978-80-904764-0-0.

NOVOVIČOVÁ, Jana, 1999. *Pravděpodobnost a matematická statistika.* Praha: České vysoké učení technické, 154 s. ISBN 80-01-01980-2.

MALÁTEK, Vojtěch a Dušan POLONSKÝ, 1998. *Metody sociologického výzkumu.* Karviná: Slezská univerzita, 92 s. ISBN 80-7248-015-4.

SEZNAMSEBEZPECNE. Desatero. *Seznamsebezpecne.cz* [online]. ©1996–2011 [cit. 2013-05-02]. Dostupné z: http://www.seznamsebezpecne.cz/desatero

TECHNET. Jak si vytvořit bezpečné heslo a nebýt za hlupáka. *Technet.idnes.cz* [online]. ©1998–2013 [cit. 2013-05-02]. Dostupné z: http://technet.idnes.cz/jak-si-vytvorit-bezpecne-heslo-a-nebyt-za-hlupaka-fbo-

VESELÁ, Jana, 2006. *Sociologický výzkum a jeho metody.* 2.vyd. Pardubice: Univerzita Pardubice, 92 s. ISBN 80-7194-847-0.

Seznam obrázků a grafů

Seznam tabulek

Seznam příloh

Příloha č. 1: CD se získanými daty z dotazníkového šetření a jejich zpracování pomocí Microsoft Visual Basic.