Tvorba e-learningu na ochranu informací na sociálních sítích

Marcel Sedlář

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Marcel Sedlář**
Osobní číslo:	**A18542**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Tvorba e-learningu na ochranu informací na sociálních sítích**
Téma práce anglicky:	**The Creation of E-learning for Information Protection on Social Networks**

Zásady pro vypracování

1. Uveďte základní terminologii související s tématem práce.
2. Rozeberte nejpoužívanější sociální sítě a hrozby s nimi spojené.
3. Zaměřte se na bezpečnost a na rizikové chování na sociálních sítích.
4. Vytvořte pravidla bezpečného chování.
5. Navrhněte e-learning.

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

Seznam doporučené literatury:

1. MCCARTHY, Linda a Denise WELDON-SIVIY. Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online. Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.
2. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
3. A. RUSSELL, Matthew a Mikhail KLASSEN. Mining the Social Web. 3rd edition. Sebastopol: O’Reilly Media, 2019. ISBN 978-1-49198504-5.
4. TIPTON, Harold a Micki KRAUSE NOZAKI, ed. Information Security Management Handbook. 6th edition. Boca Raton (Florida): CRC Press, 2012. ISBN 978-1-4398-9315-9.
5. BAILEY, Matthew, ed. Complete Guide to Internet Privacy, Anonymity & Security. 2nd edition. Nerel Online, 2015. ISBN 978-3-9503093-3-1.

Vedoucí bakalářské práce: **Ing. Dora Kotková, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **15. ledna 2021**
Termín odevzdání bakalářské práce: **19. května 2021**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 14.5.2021

Marcel Sedlář v.r.
podpis studenta

ABSTRAKT

Bakalářská práce je zaměřena na bezpečnost na sociálních sítích a tvorbu výukového e-learningu. Teoretická část rozebírá nejčastěji využívané sociální sítě a popisuje nejběžnější hrozby. Praktická část je zaměřena na bezpečnost, na rizikové chování na internetu, na nastavení sociálních sítí a na tvorbu pravidel chování. Výstupem bakalářské práce je e-learningu, který tyto pravidla shrne a představí je uživateli.

Klíčová slova: sociální sítě, ochrana dat, ochrana soukromí na internetu, vytěžování sociálních sítí, tvorba e-learningu

ABSTRACT

The bachelor thesis is focused on security on social networks and the creation of educational e-learning. The theoretical part analyzes the most commonly used social networks and describes the most common threats. The practical part is focused on security, risky behavior on the Internet, setting up social networks, and creating rules of conduct. The output of the bachelor's thesis is e-learning, which summarizes these rules and introduces them to the user.

Keywords: social networks, data protection, internet privacy protection, datamining of social networks, creation of e-learning

Poděkování:

Chtěl bych poděkovat Ing. Doře Kotkové, Ph.D. jako vedoucí této práce za její odborné vedení, poskytnutí pomoci, rad a věcných připomínek.

Dále bych chtěl poděkovat všem dobrovolníkům, kteří ve svém volném čase absolvovali e-learning a za poskytnutí zpětné vazby.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **8**
I TEORETICKÁ ČÁST **9**
1 SOCIÁLNÍ SÍTĚ **10**
1.1 HISTORIE SOCIÁLNÍCH SÍTÍ 10
1.2 MODERNÍ SOCIÁLNÍ SÍTĚ 11
1.2.1 Facebook 11
1.2.2 Twitter 12
1.2.3 Reddit 14
1.2.4 Instagram 15
1.2.5 Další sociální sítě 16
2 ZNEUŽITELNOST OSOBNÍCH INFORMACÍ NA SOCIÁLNÍCH SÍTÍCH **17**
2.1 CHRÁNĚNÉ OSOBNÍ INFORMACE 17
2.2 INFORMACE SDÍLENÉ UŽIVATELEM 18
2.3 ZPŮSOBY VYUŽITÍ INFORMACÍ 19
2.3.1 Hledání zaměstnání 19
2.3.2 Krádež identity 20
2.3.3 Stalking 21
2.3.4 Vyhledávání potenciálních cílů pro krádeže 22
2.4 PŘÍKLADY ZNEUŽITÍ INFORMACÍ ZE SOCIÁLNÍCH SÍTÍ 23
2.4.1 Pokus o krádež vozidla 23
2.4.2 Účast na zakázané akci 23
2.4.3 Ztráta invalidního důchodu 23
3 ZÁSADY TVORBY E-LEARNINGU A ROZDĚLENÍ NA FÁZE **25**
3.1 KROKY TVORBY E-LEARNINGU 25
II PRAKTICKÁ ČÁST **28**
4 TVORBA E-LEARNINGU **29**
4.1 VYTYČENÍ CÍLŮ 29
4.1.1 Představení, jaké informace o sobě poskytujeme 29
4.1.2 Ukázka, jak lze informace zneužít 29
4.1.3 Představení opatření 30
4.2 PŘÍPRAVA MATERIÁLŮ 30
4.3 CÍLOVÁ SKUPINA 30
4.4 PŘEDÁNÍ INFORMACÍ 31
4.5 NÁVRH OSNOVY 31
4.6 VOLBA NÁSTROJŮ 32
4.7 TVORBA PROTOTYPU 33
4.7.1 Prototyp 33
4.7.2 Získání zpětné vazby 33
4.8 REALIZACE E-LEARNINGU 34
4.8.1 Vzhled a úprava 34
4.8.2 Titulní strana 35

4.8.3 Hlavní menu s výběrem kapitol 35
4.8.4 Úvod a první téma 36
4.8.5 Kvíz 36
4.8.6 Sdělování informací na sociálních sítích 38
4.8.7 Zneužití informací 38
4.8.8 Hledání zaměstnání 39
4.8.9 Krádež identity 40
4.8.10 Stalking 42
4.8.11 Identifikace potencionální oběti krádeže 43
4.8.12 Případy využití informací na sociálních sítích v praxi 43
4.8.13 Pokus o krádež automobilu 44
4.8.14 Krádež identity 44
4.8.15 Účast na zakázané akci 44
4.8.16 Nastavení a ochrana informací 45
4.8.17 Nastavení Facebooku 45
4.8.18 Nastavení Instagramu 46
4.8.19 Pravidla chování na sociálních sítích 47
4.8.20 Předposlední a poslední slide 48
4.9 DOLADĚNÍ E-LEARNINGU 48
4.10 PUBLIKOVÁNÍ E-LEARNINGU 49
ZÁVĚR 50
SEZNAM POUŽITÉ LITERATURY 51
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 55
SEZNAM OBRÁZKŮ 56
SEZNAM PŘÍLOH 57

ÚVOD

S rozvojem internetu přišel též rozvoj nových způsobů komunikace. Jedním z nich jsou i sociální sítě. Ty nám umožňují navázat kontakty s lidmi, prezentovat se na internetu, chlubit se úspěchy či sdílet své názory. Sociální sítě jsou v jisté míře součástí života většiny lidí a v dohledné době tomu tak zůstane.

S jejich rozmachem však přišla předtím nevídaná možnost poskytnout ostatním lidem náhled do našeho soukromého života. Takové možnosti předtím neexistovaly a lidé začali sdílet detaily ze svého života, které by se předtím na veřejnost nedostaly. Detaily, ač na první pohled nevýznamné, mohou sdělit informace, o kterých neuvažujeme jako o podstatných, avšak dokáží vyzradit více, než si člověk původně přál. S důslednou metodikou může pak cizí člověk tyto informace zneužít proti jejich majiteli. Zneužití takových informací může pak způsobit majiteli škodu, o které předtím neuvažoval a která může mít vážné následky.

Neopatrnost, s jakou lidé sdělují své osobní informace, je častým jevem na sociálních sítích a není výsadou pouze jedné skupiny lidí. Citlivé informace o svém osobní životě sdělují všechny věkové kategorie, lidé z různých sociálních vrstev, lidé s rozdílnou ekonomickou situací a s různou úrovní vzdělání. Fotografie, videa či komentáře, to vše lidé sdělují a vystavují na svých profilech, nehledě na to, co tyto příspěvky sdělují navíc, mimo původní záměr.

Hlavní cílem této bakalářské práce je vytvořit e-learning, který poukáže na tyto problémy, a předvést, jaké informace se dají z profilů na sociálních sítích dostat a jakým způsobem je lze zneužít proti majiteli. Dalším cílem je pak ukázat, jakým způsobem lze tyto informace chránit před veřejností, jak se na sociálních sítích chovat, na co si dávat pozor, co a jakým způsobem zveřejňovat, aby nedošlo ke zneužití.

V první kapitole teoretické části práce bude probrána historie sociálních sítí a jejich použití v moderní době. Další kapitola se pak věnuje informacím sdíleným na sociálních sítích a jakým způsobem se dají využít ze strany útočníka. Poslední kapitola teoretické části se věnuje teorii tvorby e-learningu. Celá praktická část práce se pak věnuje všem krokům tvorby e-learningu. Od základního návrhu až po jeho kompletaci.

I. TEORETICKÁ ČÁST

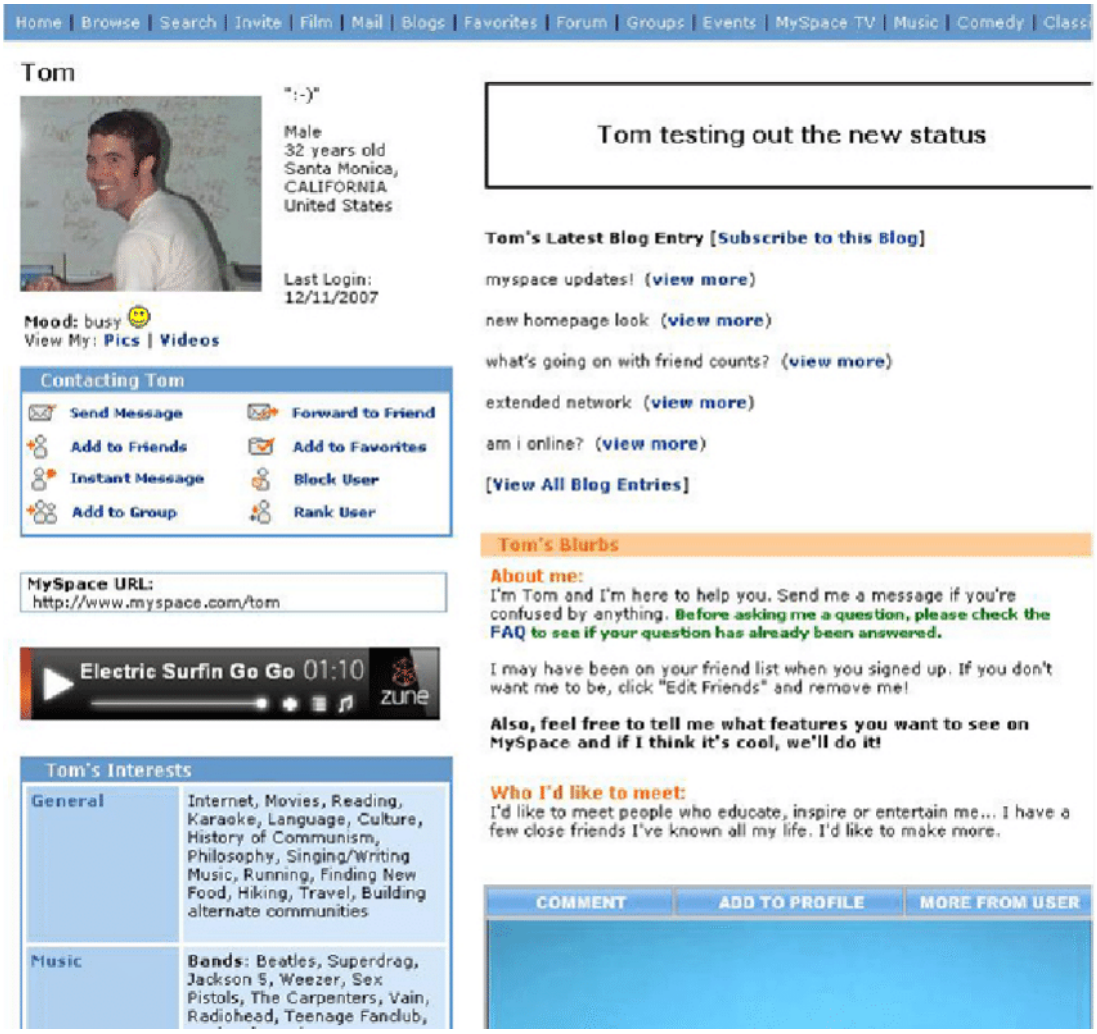
1 SOCIÁLNÍ SÍTĚ

Sociální sítě jsou počítačové sítě umožňující sdílet nápady, myšlenky a informace skrz síť kontaktů a komunit. Sociální sítě jsou konstruované tak, aby uživatel získal možnost rychlého způsobu komunikace a sdílení informací s okolím. Mezi takové informace mohou patřit textové příspěvky, komentáře, fotky, videa, dokumenty, zprávy a jiné. [1] [2]

1.1 Historie sociálních sítí

K prvnímu výskytu sociální sítích došlo během rozmachu internetu v 90. letech 20. století. V této době se začaly objevovat první blogy a předchůdci sociálních sítí, které naznačily budoucí podobu sociálních sítí. Jednou z prvních sociálních sítí by se dal označit web SixDegrees.com z roku 1997. Tento web umožňoval uživatelům přidat do seznamu kontaktů rodinu, přátelé, spolupracovníky a jiné osoby. Uživatelé mohli sdílet obsah a využívat tento web k posílání zpráv ostatním uživatelům. Další sociální síť byla Friendster z roku 2001. Tato sociální síť umožňovala podobně jako SixDegrees vytvářet kontakty, sdílet obsah jako fotky a videa, vytvářet události a další. [3]

Na předchozí sociální sítě pak v roce 2003 navázala síť MySpace. Tato sociální síť umožňovala tvorbu vlastního profilu, seznamu přátel a kontaktů a posílání zpráv. Umožňovala přidávat obsah na zeď profilu uživatele a stala se tak předlohou pro ostatní sociální sítě. V roce 2006 se stala nejnavštěvovanější internetovou stránkou na světě a měla víc než 100 milionů unikátních uživatelů každý měsíc. Síť MySpace stála na počátku obrovského rozmachu sociálních sítí a otevřela cestu dalším, dnes populárním sítím. [3]



Obrázek 1. Profil zakladatele sítě MySpace Thomase Andersona v roce 2007 [4]

1.2 Moderní sociální sítě

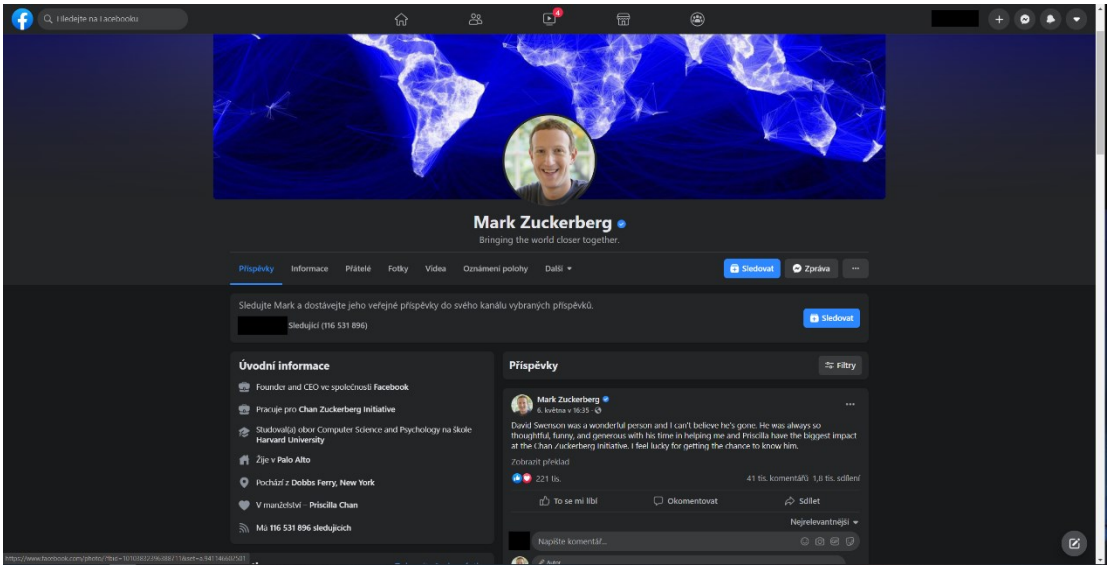
Na úspěch MySpace navázalo mnoho dalších sociálních sítí, které fungují dodnes. Zde jsou uvedeny informace a přehled o dnes nejvíce používaných sociálních sítích.

1.2.1 Facebook

Facebook je sociální síť, na které má každý uživatel vlastní profil, kde si udržuje seznam kontaktů, sdílí příspěvky na své zdi v podobě komentářů, videí, obrázků. Profily si zde taktéž zakládají slavné osobnosti, politici či firmy. Příspěvky lze dále sdílet, hodnotit či komentovat.

Facebook byl založen v roce 2004 trojicí studentů na Harvardu – Markem Zuckerbergem, Eduardem Saverinem a Dustinem Moskovitzem. Původně sloužil Facebook studentům Harvardu, kteří mohli navzájem sdílet fotografie, osobní informace o svém životě

či rozvrhy. Postupně se stránka rozšířila mezi studenty dalších univerzit a v červnu roku 2004 měla stránka už zaregistrováno přes 250 000 studentů z různých škol. Ještě ten rok byla přidána možnost komentovat a psát zprávy na zeď ostatních uživatelů a první společnosti začaly platit za reklamy na stránce. V roce 2005 bylo sdílení fotografií rozšířené o možnost označovat ostatní uživatele na fotografiích a na konci roku bylo umožněno se zaregistrovat i studentům mimo USA. V roce 2006 se Facebook otevřel široké veřejnosti a začal tak prudký nárust uživatelské základny. Facebook překonal MySpace co do počtu měsíčních uživatelů v roce 2008 a od té doby je nejpopulárnější sociální sítí.[5]



Obrázek 2. Facebookový účet Marka Zuckerberga (Vlastní)

Facebook za svou existenci měl několikrát problémy s ochranou soukromých záležitostí svých uživatelů. V roce 2007 Facebook spustil projekt Beacon. Pokud si uživatel zakoupil něco od reklamních partnerů, byl tento nákup zobrazen na zdi uživatele. Uživatelé tento projekt označili za zásah do soukromí a Facebook projekt opustil. Mezi další případy patří incident, kdy 14 milionům uživatelů se na profilu objevily příspěvky, jež uživatelé nastavili jako soukromé. Podle stránky Alexa, která se zabývá návštěvností internetových stránek, je Facebook aktuálně 7 nejnavštěvovanější stránkou na světě. [5] [6]

1.2.2 Twitter

Twitter je sociální síť, která však uplatňuje jiný přístup k uživatelům než Facebook. Zatímco Facebook slouží k vytvoření profilu prezentující uživatele na internetu, kde si uživatel přidává přátele, plánuje akce, zveřejňuje informace o svém osobním životě, hlavním záměrem Twitteru je zveřejňovat krátké zprávy a názory. Uživatel zveřejňuje tzv. Tweets,

což jsou krátké zprávy s maximální délkou 280 znaků. Předmětem takových zpráv jsou často různá oznámení, komentáře k aktuálnímu dění, infomační sdělení a jiné. Uživatelé si nepřidávají ostatní uživatel jako přátele, ale provádí sledování ostatních uživatelů. Pokud uživatele sledujete, jeho příspěvky se budou zobrazovat na vaší domovské stránce. Tyto příspěvky pak může uživatel nadále sdílet, komentovat či tzv. lajknout, čímž dá uživatel najevo svůj souhlas s obsahem.

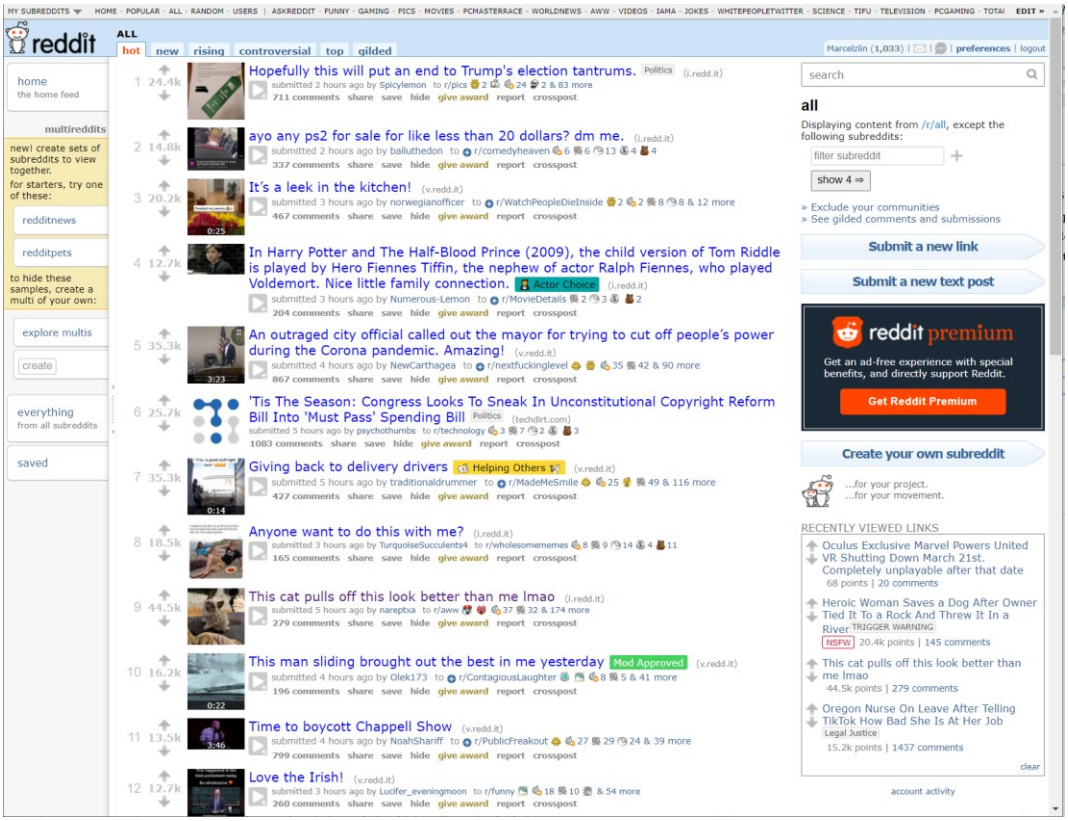
Obrázek 3. – Účet na Twitteru (Vlastní)

Twitter byl vytvořen jako interní projekt firmy Odeo v roce 2006. Byl vytvořen Evanem Williamsem a Christopherem Stonem, ke kterým se později přidal Jack Dorsey. Projekt začal jako forma SMS zpráv zdarma s aspekty sociálních sítí. Představen veřejnosti byl v roce 2007. Maximální délka zprávy v té době byla 140 znaků. V roce 2008 začal Twitter díky americkým prezidentským volbám získávat na popularitě. Možnost rychle posílat aktuální zprávy ohledně dění okolo voleb velkému počtu uživatelů se stala příhodnou pro množství zpravodajských stanic a webů. I samotní prezidenští kandidáti využívali Twitter jako jednoduchý způsob komunikace směrem ke svým příznivcům. V roce 2010 pak Twitter uzavřel smlouvu s poskytovateli reklam a začal zviditelňovat reklamní prohlášení. Během následujících let pak popularita Twitteru dále rostla a v roce 2017 byl zvýšen limit znaků jednoho Tweetu ze 140 na 280 znaků. Podle stránky Alexa je Twitter aktuálně 45 nejnavštěvovanější stránkou na světě. [6] [7]

1.2.3 Reddit

Reddit není tradiční sociální sítí. Je spíše kombinací sociální sítě a komunitního fóra. Podstatou redditu je sdružování skupin o různých zájmech. Reddit se dělí na takzvané subreddity které jsou označeny r/jménosubredditu. Subreddit je specificky zaměřený na určené téma a funguje jako fórum pro dané téma. Mezi příklady lze uvést r/movies, který je zaměřený na diskusi o filmech, r/games, který je zaměřený na diskuze o hrách, r/funny, kde uživatelé zasílají vtipné, obrázky, videa a jiné a dále například r/science, kde uživatelé diskutují na téma nových vědeckých poznatků. Subreddity mohou být taktéž velmi specificky zaměřené. Například r/retrofuturism se zaměřuje na umělecká díla, která jsou ve stylu představ budoucnosti z 50/60 let. Jsou zde i subreddity na citlivější témata. Jedním z příkladů je r/depression, kde lidé sdílí svoje problémy s depresemi. Každý uživatel redditu má svůj vlastní účet, který spravuje. Lze k němu přiřadit některé informace jako svoji fotografii a základní informace o jeho osobě. Neslouží však jako Facebook k navazování kontaktů. Procházet reddit lze buďto anonymně a bez registrace, to však slouží pouze k prohlížení stránky, nebo se zaregistrovat jako uživatel. Uživatel pak může začít odebírat jednotlivé subreddity a vybrané příspěvky z nich se mu budou zobrazovat na hlavní stránce. Jednotlivé příspěvky mohou obsahovat téměř cokoliv. Ať již textové příspěvky, obrázky, videa, či odkazy na jiné webové stránky. Příspěvky lze hodnotit buď pozitivně nebo negativně, psát k nim komentáře a ty následně taktéž hodnotit. Historie uživatele je dostupná všem ostatním uživatelům včetně příspěvků, historie komentování, historie hodnocení příspěvku. To vše je volně přístupné a informace lze dohledat i více než 10 let nazpět. Reddit tedy nenabízí uživateli svůj účet udělat neveřejný. Uživatelé tedy často zakládají účty na jedno použití, pokud mají otázky ohledně citlivějších záležitostí.

Reddit byl vytvořen dvojicí studentů Stevem Huffmanem a Alexisem Ohanianem v roce 2005. Byl zamýšlen jako prostor pro sdílení odkazů na internetu. Postupně došlo k nárustu uživatelské základny a reddit byl v roce odkoupen v roce 2006 za 20 milionů dolarů společností Condé Nast a roce 2011 byl oddělen jako samostatná společnost. V roce 2008 bylo umožněno uživatelům zakládat vlastní subreddity. V roce lednu 2011 překročil reddit 1 miliardu návštěv za měsíc. Podle stránky Alexa je Reddit aktuálně 45 nejnavštěvovanější stránkou na světě. [6][8]



Obrázek 4. Úvodní stránka Reddit (Vlastní)

1.2.4 Instagram

Instagram je sociální síť založená primárně na sdílení fotografií a videí. Instagram se nesnaží přímo konkurovat ostatním sociálním sítím, ale zaměřuje se spíše na sdílení zážitků uživatelů. Uživatelé mohou pořídit fotografie a videa, ty pak přes zabudované filtry upravit a sdílet je na svém profilu. Nabízí taktéž možnost tzv. Stories, což je série fotografií a videí dokumentující určitou událost. Po 24 hodinách po nahrání jsou tyto Stories automaticky smazány z účtu uživatele. Instragram funguje na podobném principu jako Twitter, kdy uživatel sleduje ostatní uživatele a obsah, který sdílejí se uživateli zobrazuje na hlavní stránce. Příspěvky dalších uživatelů lze podobně jako na Facebooku „lajkovat“ a vyjádřit tak, že se příspěvek líbí. Hlavní platformou Instagramu jsou mobilní telefony, díky kterým uživatelé snadno sdílejí své fotky a videa.

Instagram byl vytvořen Kevinem Systromem a spolu s Mikem Kriegerem jej v roce 6.října 2010 spustil na mobilních telefonech. Do poloviny prosince téhož roku si aplikaci stáhlo přes 1 milion uživatelů. Relativně rychlý růst pak způsobil zájem ze strany investorů a v roce 2012 byl odkoupen společností Facebook za 1 miliardu dolarů a ve stejném roce

byla poprvé spuštěna verze pro prohlížeče v počítači. V roce 2016 spustil Instagram funkci Stories a v roce 2018 dosáhl Instragram 1 miliardy aktivních uživatelů každý měsíc. [9]

1.2.5 Další sociální sítě

V současné době existuje mnoho dalších sociálních sítí. Většina z nich funguje na podobném principu jako výše jmenované, a proto jsou zde uvedeny v krátkém přehledu s popisem.

Pinterest – Je sociální síť zaměřená na sdílení kreativních nápadů mezi uživateli. Tyto nápady zahrnují recepty, dekorace, domácí projekty a jiné. Tyto nápady lze sdílet ve formě obrázků, videí či pomocí jiných audiovizuálních médií. Takové příspěvky se nazývají „Pins“ a uživatel si je může uložit pro pozdější použití. [10]

Snapchat – Aplikace na sdílení fotek a videí podobná Instagramu. Sdílené fotky a videa se nazývají „Snaps“. Snapchat přišel s konceptem sdílení fotek a videí na omezenou dobu. Uživatel může nastavit, jestli jeho příspěvek bude sám smazán a za jak dlouho. Touto funkcí se později inspirovali vývojáři Instagramu. [3]

TikTok – TikTok je aplikace na sdílení krátkých videí. Uživatelé vytváří krátká videa o délce 3-60 vteřin, která následně sdílí na svém profilu. [3]

Tumblr – Tumblr je sociální síť kde uživatelé sdílejí své příspěvky ve formě krátkých blogů. Uživatelé sdílejí příspěvky na různá témata v podobě textových příspěvků, obrázků či videí. Tyto příspěvky se dají hodnotit a komentovat. Oproti Facebooku jsou tyto příspěvky obsáhlejší a týkají se spíše osobních zájmů uživatelů než jejich osobnosti. [11]

Vkontakte – Vkontakte je ruská sociální síť. Jedná se o konkurenci Facebooku, se kterou sdílí podobné funkce. Populární je hlavně v Rusku a východní Evropě. Dostupná je ve více než 90 jazycích včetně češtiny. V česku je málo rozšířená. Jedná se o 22 nejnavštěvovanější stránku na světě. [6]

Existují i další sociální sítě. V kontextu použití v České republice (ČR) jsou však tyto sítě svou velikostí zanedbatelné a není potřeba jim věnovat zvýšenou pozornost.

2 ZNEUŽITELNOST OSOBNÍCH INFORMACÍ NA SOCIÁLNÍCH SÍTÍCH

Tato kapitola je zaměřena na zneužitelnost osobních informací poskytovaných samotným uživatelem. Běžní uživatelé si často nejsou vědomi o existujících rizicích na sociální sítích, a proto nevěnují pozornost obsahu, který na ně přidávají. Uživatelé na sociálních sítí často sdílejí informace o své osobě a nepřemýšlejí nad zneužitelností jejich obsahu. Takového chování pak mohou zneužít jiné osoby pro svůj prospěch či pro poškození daného uživatele.

Informace může útočník získat pomocí několika způsobů. Nejčastějším způsobem je obyčejné prohlížení profilu a získávání relevantních informací o uživateli jako například bydliště, rodinný stav, majetek a další. Existují i pokročilejší způsoby jako například vytěžování informací pomocí počítačových scriptů a jiných technických prostředků. Tyto metody jsou však vyžadují vysoké technické znalosti a nejsou tedy pro většinu útočníků reálně využitelné. [12]

2.1 Chráněné osobní informace

V době nových komunikačních technologií dochází k přenosu velkého množství osobních informací. Tyto informace se dají označit jako tzv. Privacy-sensitive information (PSI) neboli Informace citlivé na soukromí. Takové informace mohou obsahovat Personally identifiable information (PII) či Osobně identifikovatelné informace. PII jsou takové osobní informace, které lze přímo spojit s konkrétní osobou a jejich ochrana je v zájmu každého uživatele, který tyto informace poskytuje provozovatelům sociálních sítí. Subjekt, pracující s osobními daty uživatele, je označen jako správce údajů. Organizace pro hospodářskou spolupráci a rozvoj (OECD) vydala sérii doporučení a principů, jak s těmito informacemi nakládat:

- Princip omezení sběru informací – Měly by být zavedeny omezení na sběr osobních informací a všechna nasbíraná data by měla být získána pouze zákonným způsobem a s vědomím či souhlasem uživatele.
- Princip kvality dat – Všechna data by měla souviset s důvodem sběru informací a měla by být kompletní a aktuální.
- Princip specifikace účelu – Účel, za kterým jsou data sbírána, by měl být sdělen uživateli nejpozději v moment jejich sběru.

- Princip omezení užití – Osobní data by neměla být využita pro jiný účel, než pro který byla původně získána, bez souhlasu uživatele.
- Princip bezpečnostních záruk – Osobní data by měla být chráněna v přiměřeném měřítku proti ztrátě, zničení, nepovolenému přístupu, použití či modifikaci.
- Princip otevřenosti – Správce údajů by měl majitele osobních dat informovat, jakým způsobem jsou data využívána a jak je s nimi nakládáno. Taktéž by měl správce údajů sdělit svoji identitu a adresu, kde jej kontaktovat.
- Princip individuální účasti – Majitel osobních dat by měl být schopen získat svá osobní data od správce údajů či měl by být schopen od něj získat potvrzení, zda taková data má správce údajů k dispozici a měl by být schopen požádat o smazání či omezení nakládání s daty.
- Princip zodpovědnosti – Správce údajů by měl nést odpovědnost za dodržování opatření, která uplatňují zásady uvedené výše. [13]

Všechny tyto body jsou vydaná doporučení OECD a nejsou tedy pro provozovatele sociálních sítí závazné. O tom, jak nakládat s osobními údaji, rozhoduje legislativa jednotlivých států. V případě České republiky se jedná o Zákon č. 110/2019 Sb. – Zákon o zpracování osobních údajů.

2.2 Informace sdílené uživatelem

Uživatelé o sobě na sociálních sítích sdělují různé druhy informací. Výzkum provedený ve Spojených státech amerických (USA) odhalil, které informace o své osobě uživatelé ve věku 12-17 let zveřejňují na Facebooku a jsou volně dostupné na jejich profilu. [14]

- 92 % sděluje na sociálních sítí své skutečné jméno
- 91 % zveřejňuje na sociálních sítí své fotografie
- 84 % sděluje své zájmy a koníčky
- 82 % zveřejňuje datum svého narození
- 71 % má na svém profilu jakou školu navštěvují
- 62 % zveřejňuje zda jsou ve vztahu s jinou osobou
- 53 % zveřejňuje svoji emailovou adresu

- 24 % nahrává na profil videa o sobě
- 20 % zveřejňuje své telefonní číslo [14]

Všechny tyto informace mohou být dostupné všem uživatelům sociální sítě, pokud uživatel tyto informace nenastavil jako soukromé. Z těchto informací se dá postupně nasbírat dostatečné množství materiálu, které útočník může zneužít proti uživateli. [14]

2.3 Způsoby využití informací

Informace, které útočník získává, lze zneužít proti uživateli sociální sítě několika způsoby. Některé útoky se zaměřují na osobu samotného uživatele, kterého se pokoušejí poškodit. Jedním z takových útoků je například stalking neboli nebezpečné pronásledování osoby. U jiných metod se snaží útočník na úkor uživatele obohatit. Příkladem může být krádež identity, kdy se útočník vydává za uživatele a snaží se získat přístup k jeho prostředkům. Zde je uveden přehled různých způsobů zneužití informací získaných z profilů na sociálních sítích.

Informace, které uživatel poskytuje, však nemusí být pouze zneužity k trestným účelům. Mohou poskytnout informace i lidem, kteří se o nás chtějí dozvědět co nejvíce za účelem poznání naší osoby. Příkladem mohou být potencionální zaměstnavatelé.

Taktéž mohou informace ze sociálních sítí sloužit složkám státní správy, která je může použít při dokazování.

2.3.1 Hledání zaměstnání

Informace sdílené na internetu nemusí být zneužity pouze útočníky k poškození uživatele. Zaměstnavatelé velmi často při hledání nových kandidátů procházejí jejich sociální sítě, aby zjistili informace o potencionálních zaměstnancích. Tyto informace pak hrají důležitou roli při rozhodujícím výběru.

Průzkum provedený na toto téma zjistil, že 70 % zaměstnavatelů prohledává sociální sítě kandidátů na práci. Dále pak průzkum zjišťoval, jaké informace nejčastěji zaměstnavatele zajímají: [15]

- 58 % hledalo informace, zda kandidát splňuje kvalifikace k danému pracovnímu místu
- 50 % zajímalo vystupování kandidáta na sociální sítích

- 34 % jaké informace o kandidátovi sdělují ostatní uživatelé
- 22 % aktivně hledá důvody, které vylučují zaměstnání kandidáta [15]

Stejný průzkum dále zjišťoval, jaké informace poskytnuté na sociální síti rozhodují o odmítnutí kandidáta:

- Kandidát sdílel nevhodné či urážlivé komentáře, fotografie a videa
- Kandidát se často objevoval na fotografiích s alkoholem či drogami
- Kandidát vykazoval důkazy o trestné činnosti
- Kandidát lhal o svojí kvalifikaci
- Kandidát se nevhodně a urážlivě vyjadřoval na adresu svého bývalého zaměstnavatele
- Kandidát sdílel citlivé informace o svém bývalém zaměstnavateli
- Kandidát měl špatné vyjadřovací schopnosti
- Jméno, jakým se kandidát prezentoval na sociálních sítích, nebylo vhodné [15]

Uživatel sociální sítě může o sobě snadno sdílet informace, které snižují jeho šance při hledání zaměstnání. Monitorování sociálních sítí ze strany zaměstnavatele je dnes běžné, a proto musí uživatel dávat pozor na to, co sdílí a udržovat určitou úroveň profesionality, která jej bude v takových situacích reprezentovat.

2.3.2 Krádež identity

Jedním z běžných způsobů zneužití informací proti uživateli je krádež identity. Jedná se o poměrně jednoduchou metodu, kdy útočník vytvoří falešný profil vyhlédnutého uživatele a vydává se za něj. K tomu, aby byla šance na úspěch co nejvyšší, musí útočník vytvořit co nejvěrohodnější profil. K vytvoření takového profilu, v první fázi útoku, musí útočník důkladně prohledat všechny stopy po uživateli na internetu a ty správně sestavit. Tyto informace může útočník získat o uživateli na různých sociálních sítích, internetových seznamkách či fórech. Mezi informace, které může získat patří fotografie osoby, datum narození či místo pobytu. Dále pak může na falešný profil přidat fotografie, které uživatel přidal na svůj vlastní profil, či fotografie, na kterých byl označena od jiných uživatelů. Takové fotografie mohou dodat falešnému profilu větší věrohodnost. Další krokem je sběr detailů o životě uživatele. Znalost koníčků a zájmů uživatele opět pomáhá důvěryhodnosti

profilu. Informace o tom, kde uživatel pracoval či studoval mohou útočníkovi pomoct. V této fázi taktéž útočník sbírá informace o okolí uživatele. Snaží se získat přehled o jeho rodině, přátelích a známých s cílem určit nejvhodnější cíl pro provedení útoku. Takto vyhlédnutá oběť je pak cílem podvodu ze strany útočníka. [16] [17]

Po sestavení falešného profilu útočník přejde do druhé fáze útoku. V případě krádeže identity je nejčastějším typem útoku podvod za cílem vylákání peněz z osob blízkých uživateli. Útočník, vydávající se za uživatele, kontaktuje člena rodiny, některého z přátel či známých uživatele s tím, že potřebuje peníze. Útočník předstírá, že se uživatel dostal do finanční nouze a potřebuje nutně pomoct. V tento moment se útočníkovi hodí všechny informace, které se mu v první fázi podařilo získat. Pokud útočník má například znalost, kde uživatel pracuje, může předstírat, že byl propuštěn z práce a dostal se tak do finančních potíží. Úspěch útoku pak už jen záleží na důvěřivosti oběti a na schopnosti útočníka přesvědčit oběť o tom, že situace je skutečná. Pokud oběť uvěří, že uživatel má opravdu problémy, tak útočníkovi vydávajícímu se za uživatele zašle peníze. Útočník pak přeruší komunikaci a peníze převede pryč z účtu. Může se stát, že útočník se pokusí oběť znovu kontaktovat a požádat o další peníze. Každý takový pokus je však riskantnější a hrozí jeho odhalení. [16] [17]

Jinou možností je, že vyhlédnutá oběť útočníkovi neuvěří a kontaktuje skutečného uživatele. V takovém případě, již nemá dále smysl pro útočníka pokračovat v útoku, neboť uživatel, za kterého se vydává, varuje své kontakty o možném útoku a nahlásí falešný profil správci sítě.

Krádež identity může naplnit skutkovou podstatu následujících trestných činů:

- § 182 Trestního zákoníku – Porušení tajemství dopravovaných zpráv
- § 230 Trestního zákoníku – Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Trestního zákoníku – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat [18]

2.3.3 Stalking

Web policie ČR popisuje stalking neboli nebezpečné pronásledování následovně: „Nebezpečným pronásledováním (známějším pod pojmem stalking) rozumíme úmyslné, zlovolné a systematické pronásledování a obtěžování jiné osoby, které snižuje kvalitu života

a ohrožuje její bezpečnost. Cílem je navázání a udržování kontaktu s pronásledovanou osobou i přes její zjevný nesouhlas. Přímým následkem je závažné narušování soukromí, osobní svobody a lidské důstojnosti oběti, v závažných případech poškození duševního a tělesného zdraví.“ [19]

Pokud takové pronásledování probíhá přes internet, používá se název cyberstalking. Existuje několik způsobů, jakým se může projevovat. Mezi nejčastější projevy cyberstalkingu podle provedené studie patří:

- Psaní nevyžádaných soukromých zpráv oběti
- Kontaktování osob v okolí oběti s cílem ji pomluvit či získat o ní osobní informace
- Rozšiřování lží o oběti po internetu
- Publikování soukromých informací o oběti
- Přesvědčování jiných osob, aby oběť kontaktovali
- Krádež identity oběti a vydávání se za ni s cílem oběť poškodit
- Zveřejňování citlivých fotografií oběti [20]

Cyberstalking může být pouze součástí klasického stalkingu. Útočník může na sociálních sítích získat například informace o pohybu oběti. Takové informace pak může využít k vyhledání oběti a pronásledovat ji fyzicky.

Nebezpečné pronásledování je kvalifikováno jako trestný čin v § 354 Trestního zákoníku – Nebezpečné pronásledování. [19]

2.3.4 Vyhledávání potenciálních cílů pro krádeže

Uživatelé na sociálních sítích často sdílejí osobní fotografie či videa, na kterých je zachycen i jejich osobní majetek. Na fotografiích mohou být mobilní telefony, televize, notebooky, šperky či jiné cennosti. Další informace, které uživatel může na sociální sítích sdělovat, se týkají toho, kde se zrovna nachází. Na sociálních sítích mohou nevědomě sdílet informace kdy odchází z domu, jak dlouho jsou v práci nebo kdy se vrací. Uživatelé taktéž na sítích oznamují, kam jdou večer do klubu či kdy odjíždí na dovolenou a jak dlouho na ní budou.

Ze všech těchto informací může potenciální zloděj sestavit seznam majetku uživatele a jeho denní rozvrh. To pak může z uživatele udělat cíl majetkové trestné činnost, kdy zloděj

využije příležitost a v tobě nepřítomnosti uživatele se mu vloupá do domu a odnese si z něj cennosti a další majetek. [21]

2.4 Příklady zneužití informací ze sociálních sítí

V praxi dochází ke zneužití informací na sociálních sítích poměrně často. Tyto informace mohou posloužit však nejen zlodějům, ale i správním orgánům. Níže jsou uvedené některé příklady související se sdílením informací na sociálních sítích od ledna 2021.

2.4.1 Pokus o krádež vozidla

Majitel veteránu jej nabídl k prodeji přes sociální sítě. Jednalo se o historický Mercedes v odhadované hodnotě okolo 300 000 Kč a majitel inzerát umístil do 3 facebookových skupin. Majitel popsal stav vozidla a přiložil k němu i několik fotografií. Na některých fotografiích však bylo vidět i číslo garáže, ve které se vozidlo nacházelo. Toho využili zloději, kteří se o 2 dny později pokusili do garáže vloupat. Vozidlo se v ten moment nacházelo v servisu a zloději tedy ukradli jen nářadí v celkové hodnotě 35 tisíc korun. Policie v souvislosti s případem varovala před zveřejňováním informací na sociálních sítích. Podle informací se zloděje zodpovědné s krádeží zatím nepodařilo dopadnout. [22]

Případ ilustruje nejjednodušší způsob zneužití informací ze sociálních sítí. Zloději využili pouze informace, které majitel veřejně poskytnul v inzerátu a na svém profilu.

2.4.2 Účast na zakázané akci

V rámci nařízení spojených s pandemií v roce 2021 došlo k uzavření barů a restaurací. Docházelo však organizaci nelegálních akcí, kde se vyskytovalo větší množství účastníků. Při jedné takové akci došlo k policejnímu zásahu a restaurace byla uzavřena. Jeden z účastníků však nechtěl přestat a vydal se na další nelegální akci. O své účasti na akci pak informoval na sociálních sítích. Policie pak provedla zásah i proti této akci. Všichni účastníci byli nahlášeni správní orgánům pro podezření z přestupku. [23]

2.4.3 Ztráta invalidního důchodu

Sedmačtyřicetiletá žena, která podstoupila několik operací páteře, měla z důvodů bolesti a snížené mobility uznán nárok na invalidní důchod. Žena však pokračovala ve volnočasových aktivitách včetně účasti na plesech a zájezdům k moři. Fotky z těchto akcí pak zveřejňovala na Facebooku. Posudkový lékař pak na základě fotek ze sociální sítě

v posudku rozhodl, že žena své potíže nadhodnocuje. Správa sociálního zabezpečení pak na základě tohoto posudku snížila dotyčné stupeň invalidity. Tím žena ztratila nárok na invalidní důchod. [24]

Uvedené příklady dokazují, že informace poskytnuté uživatelem na sociálních sítí nemusí být zneužity pouze pro trestnou činnost, ale mohou být taktéž využity správními orgány proti uživateli.

3 ZÁSADY TVORBY E-LEARNINGU A ROZDĚLENÍ NA FÁZE

Při tvorbě e-learningu, stejně jako při tvorbě jakéhokoliv vzdělávacího materiálu, musí autor postupovat metodicky a být dobře připraven na každý krok tvorby. E-learning funguje samostatně. Musí tedy jednoznačně předat informace uživateli bez zásahu autora. Kvalita získaných informací tedy přímo souvisí s kvalitou zpracování E-learningu. [25]

Metodika postupu vypracování e-learningu probíhá v několika fázích. V první fázi probíhá příprava a získávání informací a seznámení se s jejich obsahem. Důležitou částí této fáze je získání kvalitních zdrojů. Druhá fáze se soustředí na cíle a strukturu e-learningu. V této části je zvolena cílová skupina, je určeno, jakým způsobem jsou předány informace a navržena osnova. Zde je dobré vytvořit prototyp e-learningu. V další fázi je provedena realizaci tvorby. Volba vhodných nástrojů a návrh vizuální stránky e-learningu probíhá v této části. Poslední fázi je publikační fáze. Zde je uveden e-learning do ostrého provozu. Na základě zpětné vazby lze pak provádět menší úpravy.

3.1 Kroky tvorby e-learningu

Pro lepší rozvržení práce při tvorbě e-learningu je dobré si fáze rozdělit na menší kroky, které na sebe přirozeně navazují. Takto rozvržená práce pomáhá navýšit přehlednost práce. [26]

Krok 1 – Zjištění problému a nastavení cílů

V prvním kroku je zjištěno, s jakým problémem se v e-learningu bude pracovat. Zjišťuje se, čeho se chce dosáhnout a jaký výstup by e-learning měl mít. [26]

Krok 2- Příprava materiálů

Ve druhém kroku je provedeno studium dané problematiky. Dochází k vyhledání vhodných materiálů pro práci a ty jsou upraveny tak, aby vyhovovaly potřebám e-learningu. Důležité je dobře porozumět problematice a rozhodnout o tom, které informace obsažené v materiálech jsou podstatné pro uživatele. [26]

Krok 3 – Vymezení cílové skupiny

V tomto kroku je určeno, pro koho je e-learningu vytvořen. E-learning uzpůsobený jedné skupině nebude vhodný pro skupinu druhou. E-learning vytvořený pro zaměstnance u výrobní linky nelze vytvořit se stejnou strukturou a se stejným způsobem podání informací

jako pro zaměstnance v kanceláři. Důležité je taktéž zohlednit různé věkové skupiny. Každá věková skupina reaguje na přijímaní informací jiným způsobem. [26]

Krok 4 – Určení, jakým způsobem předáme informace

Tento krok přímo navazuje na krok předchozí. Po vymezení cílové skupiny je zjištěno, jak daná skupina reaguje na přijímání informací a podle toho jsou připraveny podklady. [26]

Krok 5 – Návrh osnovy

Při návrhu osnovy e-learningu je důležité dávat pozor na přirozenou návaznost. V první části je představen problém. Pro lepší demonstraci problému je dobré navázat, k jakým následkům může dojít. Po představení následků je předvedeno řešení. [26]

Krok 6 – Volba nástrojů na realizaci e-learningu

Zde je rozhodnuto se, jakým způsobem je realizován e-learning. Je vybrán způsob, jakým dojde k předání informací. Lze použít dedikovanou internetovou stránku, prezentaci či seminář. Taktéž je proveden výběr technických nástrojů pro provedení. Je dobré volit takové nástroje, se kterými je autor již seznámen. Dojde tím k úspoře času, který by bylo jinak nutno vložit do studování nových metod. [26]

Krok 7 – Tvorba prototypu

V tomto kroku dochází k ověření použití funkčnosti zvolených nástrojů a otestování rozvržení e-learningu. Dochází zde taktéž k prvotnímu návrhu vizuální stránky. V prototypové fázi lze e-learning otestovat na testovací skupině, která nám přinese zpětnou vazbu. [26]

Krok 8 - Realizace e-learningu

Po vytvoření prototypu a seznámením s pracovními nástroji probíhá realizace finální podoby samotného e-learningu. Touto dobou je již známa kompletní vize nad osnovou a vizuální stránkou e-learningu. [26]

Krok 9 – Doladění detailů

V tomto kroku dochází ke konečným úpravám. Oprava gramatiky či doladění vizuální stránky e-learningu. Opravy by neměly být rozsáhlé, v opačném případě hrozí, že bude nutno se vrátit o několik kroků nazpět. [26]

Krok 10 – Publikování e-learningu

V posledním kroku dochází ke zveřejnění e-learningu. Zpětnou odezvu, která bude získána od uživatelů, lze využít pro další opravy a úpravy e-learningu. Po publikování jsou prováděny pravidelné revize e-learningu a aktualizace informací, které obsahuje. [26]

Všechny tyto kroky slouží k optimalizaci tvorby a navazují na sebe tak, aby došlo k maximalizaci efektivity. Dále pomáhají k vytvoření přirozeného pracovního postupu, který zajistí, že finální produkt bude ucelený a všechny jeho aspekty budou vytvářet dobrý dojem.

II. PRAKTICKÁ ČÁST

4 TVORBA E-LEARNINGU

Praktická část práce se bude zaobírat tvorbou konceptu e-learningu. Cílem této části je zpracovat následující body:

- Vytyčení cílů, jakých chceme s e-learningem dosáhnout
- Připravit vhodné materiály, ze kterých budeme čerpat informace pro e-learning
- Vymezení cílové skupiny uživatelů, na které bude e-learning zamířen
- Návrh osnovy, která bude v e-learningu použita
- Tvorba prototypu a zkouška na dobrovolnících se zpětnou vazbou
- Tvorba finální verze e-learningu

Výsledkem práce bude e-learning, který uživateli předá informace o sociálních sítích a poučí jej, jak se na sociálních sítích chovat.

4.1 Vytyčení cílů

Sociální sítě jsou v dnešní době běžnou částí života většiny lidí. Jejich používání však s sebou přináší rizika. Tato rizika již byla představena v teoretické části bakalářské práce a cílem praktické části je tyto informace zpracovat a zakomponovat do e-learningu. V prvním kroku tvorby e-learningu proto dojde k vytyčení cílů, kterých chce e-learning dosáhnout.

4.1.1 Představení, jaké informace o sobě poskytujeme

Prvním cílem je představení informací, jaké o sobě uživatelé sociálních sítí poskytují. Uživatelé často sdílí o sobě informace, o kterých neví, jaká jejich hodnota. Ukázka, jaké informace o sobě poskytujeme je tedy dobrým startovním bodem pro e-learning. Zná-li uživatel jejich hodnotu, je větší šance, že bude uživatel opatrnější při jejich sdělování.

4.1.2 Ukázka, jak lze informace zneužít

Druhým cílem je ukázka způsobů, jak lze zneužít informace, které o sobě uživatelé poskytují. Ukázka takových způsobů pomáhá uživatelům představit si skutečná rizika při umísťování informací na sociální sítě. První částí bude představení potenciálních hrozeb, které sdílené informace představují a ve druhé části bude ukázka zneužití informací v praxi. Praktické příklady velmi dobře demonstrují nebezpečí a uživatel e-learningu získá cenné informace.

4.1.3 Představení opatření

Posledním cílem je představit uživatelům sociálních sítí možnosti ochrany osobních informací. Cílem je naučit uživatele, jak se na sociálních sítích chovat, jaké informace může sdělovat a na jaké věci si dát pozor. Dále je pak cílem představit, jaká nastavení na ochranu soukromí poskytují samotné sociální sítě, a kde se dají aktivovat.

Bude-li e-learning splňovat všechny cíle, uživatelé, kteří jej budou využívat, budou po jeho absolvování mít potřebné znalosti na ochranu svých informací.

4.2 Příprava materiálů

Při přípravě materiálů se bude postupovat podle vytyčených cílů. Vhodné materiály a zdroje pro tento e-learning lze najít ve formě literatury a vědeckých prací. Dalším zdrojem mohou být články na webových stránkách či zprávy z novin a zpravodajských webů.

Pro první vytyčený cíl si jsou volbou zdroje zabývající se problematikou sdílených informacích na sociálních sítí. Dobrým zdrojem mohou být vědecké práce se statistikami, které získávají informace od samotných uživatelů. Díky tomu lze získat přehled, jaké informace o sobě uživatelé dobrovolně sdělují.

Pro druhý cíl představení, jakými způsoby se dají informace zneužít, lze použít materiály v podobě novinových a zpravodajských článků. Skutečné případy z praxe nejlépe ukazují zranitelnost uživatelů a vytváří dobrý odstrašující příklad.

Pro poslední cíl představení opatření jsou dobrým zdrojem manuály a nastavení samotných sociálních sítí. V nich lze získat informace, jaké bezpečnostní prvky jsou součástí sociálních sítí, kde je najdeme, jak je aktivujeme a co jejich aktivace dělá. Pro rady uživatelům, jak se na sociálních sítí chovat, lze použít literaturu a vědecké práce na téma chování na sociálních sítí. Zde lze najít zdroje informací, jak se má člověk prezentovat na sítích, a co o sobě nemá sdělovat.

Velkou část těchto zdrojů je možno získat využitím zdrojů použitých při psaní teoretické části práce. Většina zdrojů již pokrývá problematiku stanovených cílů a lze je přizpůsobit k použití v e-learningu.

4.3 Cílová skupina

Určení cílové skupiny e-learningu je důležité z důvodu dalšího postupu při jeho tvorbě. Jak již bylo řečeno v teoretické části, každá skupina reaguje na získávání informací

jinak. Jeden způsob zpracování e-learningu, který je určen pro mladé uživatele, nemusí být vhodný pro uživatele starší.

E-learning bude určen pro především pro osoby do 25 let. Důvodů výběru této cílové skupiny je několik:

- V posledních letech se objevuje stále více sociálních sítí. Mladí lidé tak často využívají několik takových sítí naráz a na každé z nich sdělují své osobní informace
- Mladiství mají menší přehled o následcích svého chování, jsou náchylnější k tomu, aby se stali cílem zneužití informací
- Autor práce je v přibližně stejné věkové kategorii jako cílová skupina. Může se tak snadněji vžít do role cílové skupiny a zpracovat e-learning takovým způsobem, který danou skupinu osloví

Výhodou zvolené cílové skupiny je to, že můžeme mezi ni e-learning snadno rozšířit díky internetu. Problém může představovat fakt, že cílová skupina nemusí mít o e-learning zpočátku zájem. Důležité tedy je cílovou skupinu upoutat. Alternativou může být zavedení e-learningu na školách. Škola jej rozšíří mezi studenty a ti jej absolvují. Překážkou může být při tomto způsobu navázaní spolupráce se školou.

E-learning lze zároveň použít i na uživatele starší, kteří však nemají s internetem takové zkušenosti a nemají přehled o tom, jaká nebezpečí se na internetu mohou nacházet. Jedná se tedy především o uživatele ve věkové kategorii nad 60 let. Takovým uživatelům lze předat informace formou příkladů z praxe.

4.4 Předání informací

Předání informací probíhá pomocí dvou základních způsobů. Prvním způsobem je samotný text. Ten musí být jednoduchý a dostatečně výstižný. E-learning obsahuje co nejmenší množství textu potřebného k předání důležitých informací. Tímto dochází k zajištění toho, že uživatel e-learningu nebude příliš zahlcen. Pro sekci nastavení sociálních sítí pak došlo k přidání demonstrativních obrázků, které ukazují doporučené nastavení.

4.5 Návrh osnovy

Návrh osnovy je velmi důležitým krokem při tvorbě e-learningu. Správně navržená osnova musí na sebe přirozeně navazovat a udržet pozornost uživatele. Bez takové

návaznosti hrozí, že se uživatel v e-learningu ztratí a nezachová si v paměti předané informace. Návrh osnovy v e-learningu je následující:

- V první části e-learningu je uživatel seznámen se sociálními sítěmi a tím, co se na nich nejběžněji zveřejňuje. Tato část je spíše informační, většina uživatelů je jejich aktivními uživateli a zná je z osobních zkušeností
- Ve druhé části jsou detailněji představeny informace zveřejňované na sociálních sítích. Cílem je poukázat, na jaké informace je důležité si dát pozor při zveřejňování. Tato část by měla uživatele naučit na co si dávat pozor a měla by mu to poskytnout snadno zapamatovatelným způsobem
- Ve třetí části je uvedeno, jakým způsobem se informace ze sociálních sítí dají zneužít. E-learning vysvětlí, jak zneužití takových informací probíhá, jaké postupy útočník využívá a co je útočníkovým cílem
- Ve čtvrté části dojde u představení příkladů zneužití informací ze skutečného života. Tato část slouží jako názorný příklad toho, co se může stát při tom, když si uživatel nedává na sociálních sítích pozor
- V poslední části je uživateli sděleno, jak se může na sociálních sítích bránit zneužití informací. Je mu ukázáno, jak si sociální sítě nastavit, aby k jeho informacím měly přístup pouze schválené osoby a taktéž je uživatel poučen, jaké informace by o sobě neměl na sociálních sítích zveřejňovat

Takto navržená osnova postupně poskytuje informace o problematice. Nejdříve uživatele seznámí s problémem, poté jej vystaví následkům problému, a nakonec mu poskytne řešení. Uživatel si tak uloží informace a v nejlepším možném případě se bude chovat opatrněji na sociálních sítích. E-learning tak splní svůj účel.

4.6 Volba nástrojů

Po zvážení všech možností bylo rozhodnuto, že nejlepší nástrojem na vytvoření e-learningu bude aplikace na tvorbu prezentací Powerpoint od společnosti Microsoft. Volba na tento nástroj padla z několika důvodů:

- Autor je s tímto nástrojem dobře seznámen a umí jej využívat
- Nabízí širokou paletu nástrojů, jak e-learning vylepšit

- Powerpoint je nainstalován na většině počítačů a dá se zabudovat i na webové stránky. E-learning tak bude snadno rozšiřitelný

Možnosti Powerpointu z něj dělají nejvhodnější nástroj pro tvorbu e-learningu. Jeho volba tedy dělá vzhledem k úkolu největší smysl.

4.7 Tvorba prototypu

Tvorba prototypu je důležitým krokem při vytváření e-learningu. Pomáhá nám dát všechny předtím navržené kroky do prvního uceleného návrhu, ze kterého se bude nadále vycházet. Je to taktéž první krok, ve kterém je možno získat zpětnou vazbu na dosud vytvořené materiály. To umožní upravit kurz, kterým se e-learning ubírá a doplnit jej o dalším informace.

4.7.1 Prototyp

Nejdříve je nutné pro demonstraci e-learningu vytvořit vhodný prototyp. Jako prototyp nám bude sloužit prezentace, která se bude řídit podle předtím navržených kroků. V tomto případě musí e-learning splňovat:

- Vytyčené cíle. Cílem je uživatele informovat o nebezpečí zneužití soukromích informací na sociálních sítích a poučit jej, jak se chránit
- Použijeme informace získané z materiálů zvolených ve druhém kroku
- E-learning je důležité přizpůsobit cílové skupině, tedy uživatelům do věku 25 let.
- Je důležité dodržovat osnovu

Tento prototyp bude tedy reflektovat výsledný e-learning. Při jeho tvorbě lze získat potřebné zkušenosti pro další práci na projektu e-learningu.

4.7.2 Získání zpětné vazby

Po vytvoření prototypu je dalším krokem nalezení dobrovolníků, kteří absolvují kurz. Tím lze získat první reakce na e-learning a informace o tom, co na něm dále upravit. Skupina dobrovolníků byla v případě tohoto kurzu vybrána z řad studentů Univerzity Tomáše Bati. Po absolvování e-learningu došlo ze strany dobrovolníků k následující zpětné vazbě:

- Rozšíření e-learningu o možnosti krádeže hesel (například pomocí spamu)
- Více grafů a statistik

- Zařadit do e-learningu informace pro rodiče
- Jeden účastník uvedl, že zná příklad krádeže identity ze svého okolí
- Většina účastníků uvedla, že si nemyslí, že by na sociálních sítích zveřejňovali o sobě příliš informací
- Všichni účastníci potvrdili, že si budou dávat více pozor na to, co zveřejňují

Poskytnutá zpětná vazba je velmi cenným zdrojem informací. Všechny poskytnuté body budou vzaty v úvahu při tvorbě finálního produktu. Ukázalo se taktéž, že e-learninge splnil svůj cíl, tedy poučit uživatele o nebezpečí a změnit jeho chování tak, aby si dával větší pozor.

4.8 Realizace e-learningu

Po splnění všech předchozích kroků nastává hlavní část tvorby e-learningu, a to samotná realizace. Realizace se bude se řídit navrženou osnovou a bude použit zvolený nástroj Microsoft Powerpoint.

4.8.1 Vzhled a úprava

Pro e-learning byl zvolen jednoduchý grafický styl. Jedná se bílé pozadí s několika jednoduchými geometrickými tvary. Volba na tento styl padla z důvodu, protože neodvádí pozornost uživatele od textu a není náročný na oči.

Pro font slov byl vybrán Franklin Gothic. Jedná se o jednoduchý bezpatkový font. Volba na tento font padla, protože je to opět font, který není náročný na čtení a je na první pohled přívětivý. Pomáhá tak udržovat pozornost a neodrazuje uživatele.

E-learning je doplněn o jednoduché ilustrační obrázky. Tyto obrázky slouží k upoutání pozornosti uživatele a k tomu, aby e-learning byl graficky zajímavější.

Navigace je řešena na všech stránkách e-learningu pomocí navigačních tlačítek ve spodní části stránek. Jsou do tlačítka další strana, předchozí strana a domů. Tlačítko domů vezme uživatele do hlavního menu s přehledem kapitol.

Většina snímků je doplněná o jednoduché animace textu. Tyto animace jsou nastaveny tak, aby se text postupně za sebou automaticky objevoval. Cílem těchto animací je, aby uživatel nebyl zahlcen velkým množstvím informací naráz.

4.8.2 Titulní strana

První stránkou e-learningu je titulní strana. Jedná se o jednoduchou stránku pouze s názvem tohoto e-learningu.

Obrázek 5. Úvodní strana e-learningu (Vlastní)

První strana je jednoduchá a jejím cílem je jasně předat zprávu o tom, na jaké téma následující e-learning bude.

4.8.3 Hlavní menu s výběrem kapitol

Druhou stranou e-learningu je hlavní menu s výběrem kapitol. Rozložení stránky je jednoduché pro snadnou přehlednost.

Obrázek 6. Hlavní menu s výběrem kapitol (Vlastní)

Tento snímek má 2 hlavní úkoly. Tím prvním je vytvořit domovskou stránku na kterou se může uživatel odkázat a odkud může snadno přeskočit na téma, které ho zajímá. Druhým úkolem je funkce jednoduchého přehledu obsahu. Uživateli to předá informaci, co může od e-learningu čekat.

4.8.4 Úvod a první téma

Na další straně čeká uživatele jednoduchý úvod. V něm mu je vysvětleno, co jej v e-learningu čeká a co se v něm naučí.

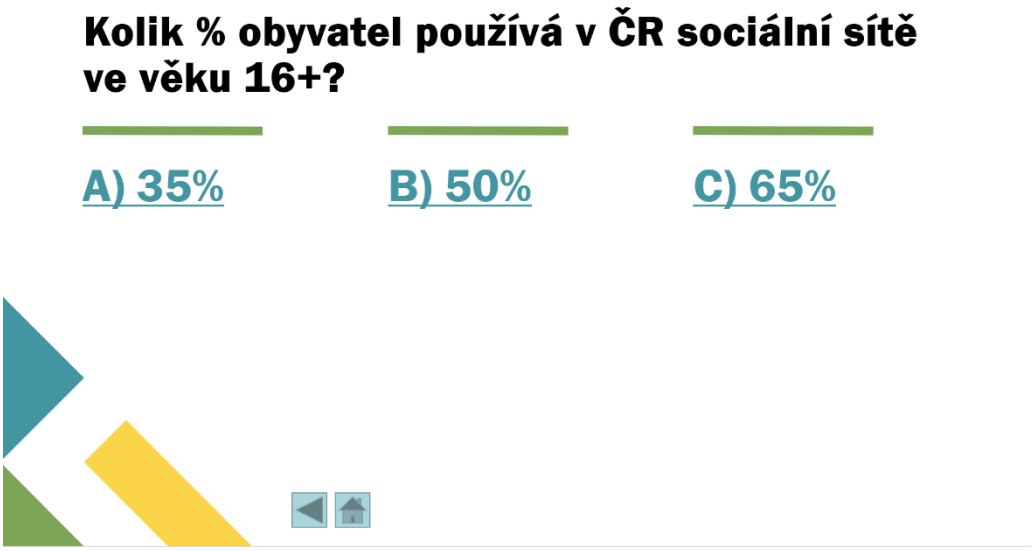
První kapitola e-learningu začíná úvodem do sociálních sítí. Tato část obsahuje pár úvodních slov na toto téma.

Obrázek 7. Snímek s úvodem do sociálních sítí (Vlastní)

Tato část slouží jako úvod do sociálních sítí. Obsahuje základní informace o jejich využití a statistiky užívání sociálních sítí v ČR. Tyto informace slouží k probuzení zájmu u uživatele o dané téma. Zároveň slouží k vytvoření prvního dojmu e-learningu a jako nápověda, jak bude celý e-learning probíhat.

4.8.5 Kvíz

E-learning taktéž obsahuje několik jednoduchých kvízových otázek. Tyto otázky slouží k oživení e-learningu a upoutání pozornosti uživatele. Jejich cílem není zkoušet znalosti uživatele.



Obrázek 8. Kvízová otázka (Vlastní)

První kvízovou otázkou je odhad užití sociálních sítí v populaci ČR. Všechny možnosti jsou zvoleny tak, aby mohly být správnou odpovědí a žádná z nich příliš nevybočuje. Uživatel zvolí možnost kliknutím. Po kliknutí je přenesen na příslušnou stránku s vyhodnocením odpovědi.

Obrázek 9. Odpověď na kvíz (Vlastní)

Uživatel je jednoduše informován, zda odpověděl dobře nebo špatně a je mu taktéž prezentována možnost se správnou odpovědí.

4.8.6 Sdělování informací na sociálních sítích

Po úvodu do sociálních sítí se další část e-learningu věnuje informacím, které jsou na sociálních sítích sdíleny. Tato část e-learningu má hlavně poučnou úlohu. Slouží k tomu, aby se již při čtení uživatel zamyslel nad tím, co na sociálních sítích sděluje.

Obrázek 10. Sdílení informací (Vlastní)

Tato kapitola obsahuje výčet běžných informací, které lidé sdělují na sociálních sítích. Je zde taktéž obsažena další kvízová otázka. Tato otázka se zabývá problematikou veřejného sdělování polohy na sociálních sítích.

4.8.7 Zneužití informací

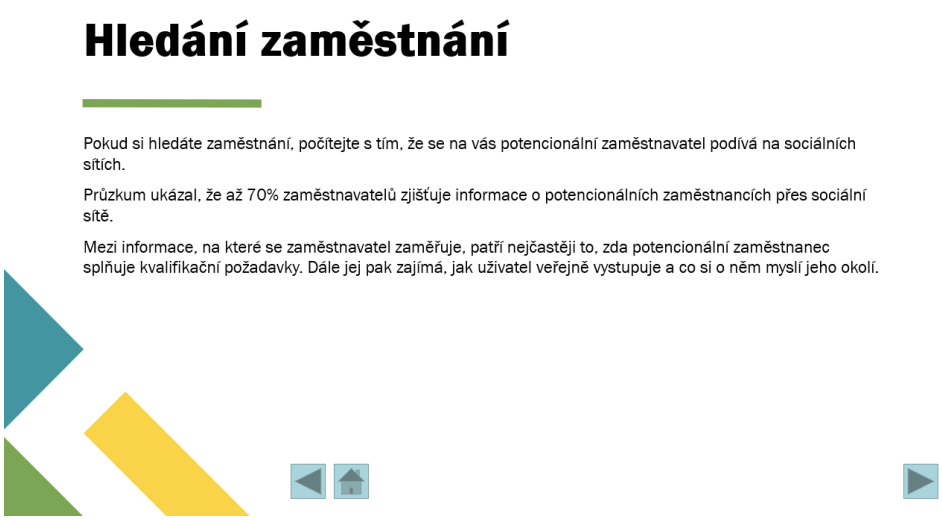
Důležitou částí e-learningu je část zabývající se zneužitím informací poskytovaných uživatelem na sociálních sítích. Úkolem této kapitoly je poučit o množství nebezpečí, která se na sociálních sítích objevují. Zároveň tato část slouží k postrašení uživatele, aby si uvědomil nebezpečí těchto skutečností.

Obrázek 11. Úvod do zneužití informací (Vlastní)

Kapitola je koncipována jako seznam častých způsobů zneužití informací. Začíná se od nejméně vážných a postupně k závažnějším situacím. Každý příklad je koncipován tak, že nejdříve je uživatel informován o tom, co se může stát. Poté je nabídnuto řešení v podobě tipů, jaké informace se k těmto útokům dají využít a jak se tedy chránit.

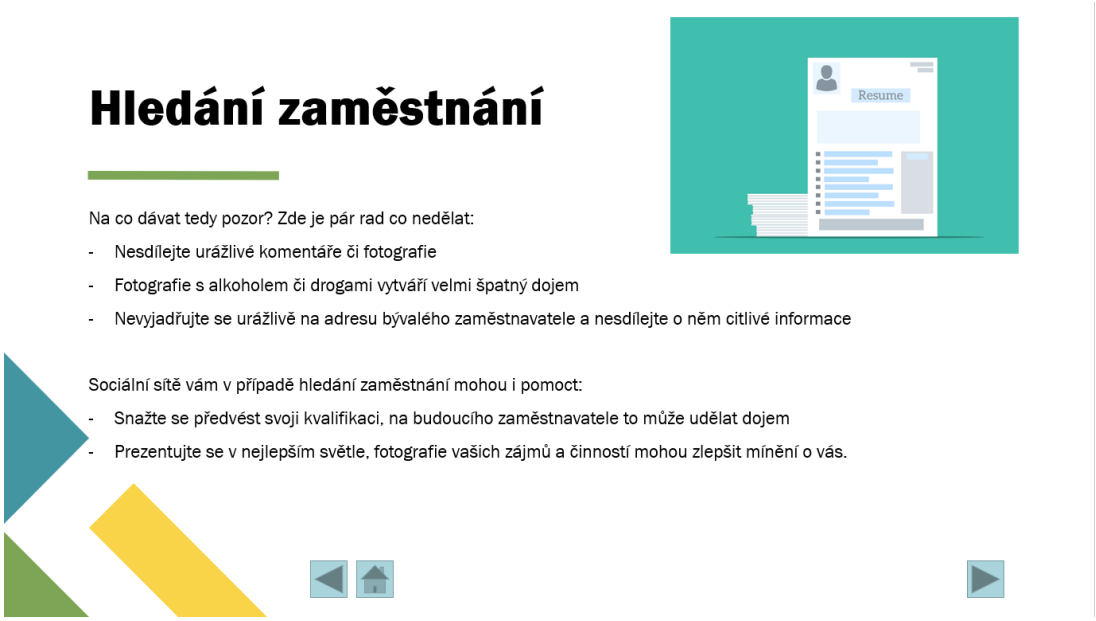
4.8.8 Hledání zaměstnání

Prvním způsobem využití informací proti uživateli je hledání zaměstnání. Většina zaměstnavatelů při procházení kandidátů kontroluje jejich profily na sociálních sítích. Upozornění na tuto skutečnost je tedy dobrým začátkem pro tuto kapitolu.



Obrázek 12. Snímek zabývající se hledáním zaměstnání (Vlastní)

Toto téma bylo zvoleno na začátek, protože je z pohledu uživatele téměř neškodné a slouží jako dobrý příklad toho, co o nás sociální sítě sdělují. Dále pak tento případ připomíná, že sociální sítě jsou naším obrazem na internetu a často vytváří důležitou část prvního dojmu o nás samotných.

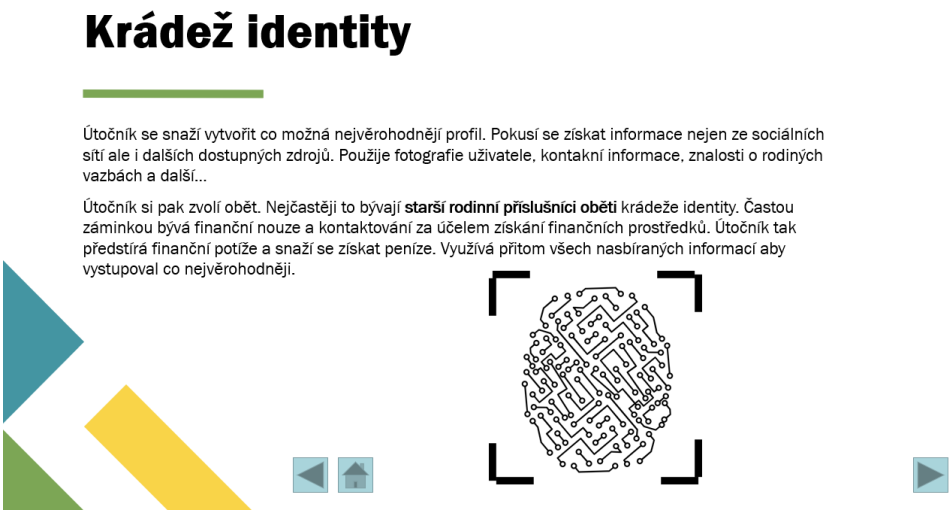


Obrázek 13. Rady u hledání zaměstnání (Vlastní)

Druhá část nabízí konkrétní rady ohledně sdílení informací, týkající se tohoto příkladu. Vycházejí ze zjištění, kterých bylo dosáhnuto v teoretické části této práce.

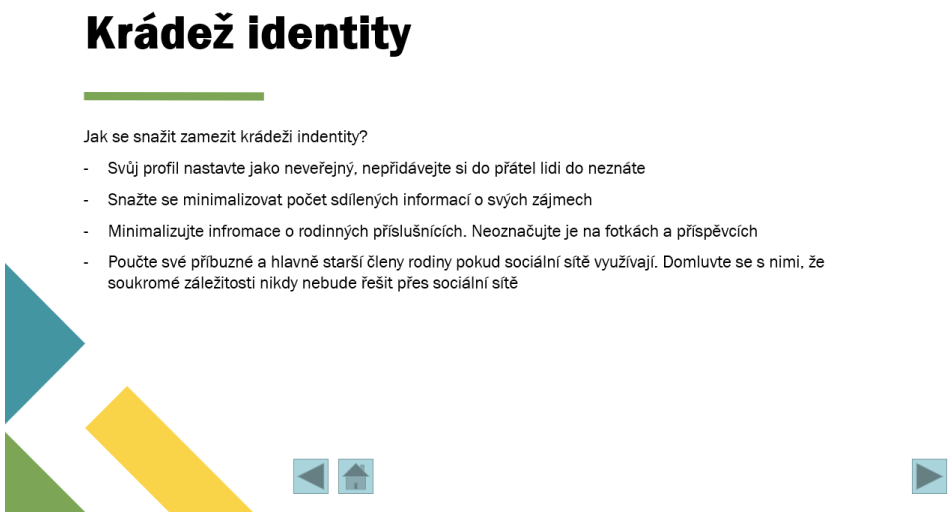
4.8.9 Krádež identity

Druhým uvedeným příkladem zneužití informací je krádež identity. Krádež identity není jen problémem sociálních sítí, ale představuje zde poměrně známý úkaz. Tento příklad se zaměřuje, jak krádež identity nejčastěji probíhá a co je jím nejčastějším cílem.



Obrázek 14. Snímek krádež identity (Vlastní)

Cílem tohoto příkladu je poučit uživatele o tom, jakým způsobem se krádež identity často uplatňuje. Důležité je upozornění, že cílem často není samotný uživatel, ale jeho rodinní příslušníci, a to hlavně starší generace. Uživatel by si měl z této části odnést to, že útok může hrozit i jeho nejbližšímu okolí.

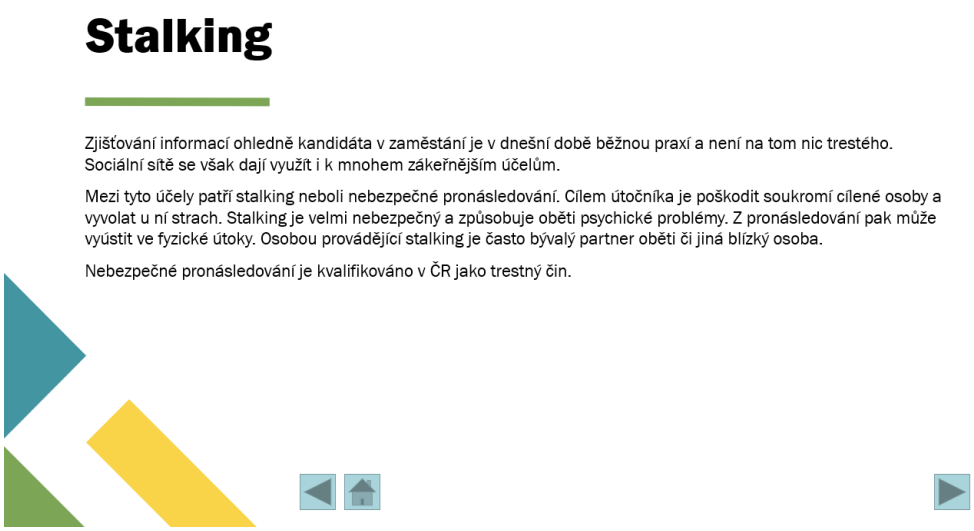


Obrázek 15. Rady u krádeže identity (Vlastní)

Snímek, který se zabývá opatřeními proti krádeži identity upozorňuje hlavně na to, aby uživatel měl svůj profil na sociálních sítích nastaven jako neveřejný a nedával tak přístup cizím lidem k informacím. Upozorňuje taktéž na to, aby nesdílel informace o svých příbuzných a rodinných vztazích. Snímek zároveň naléhá na uživatele, aby poučil o těchto situacích své příbuzné.

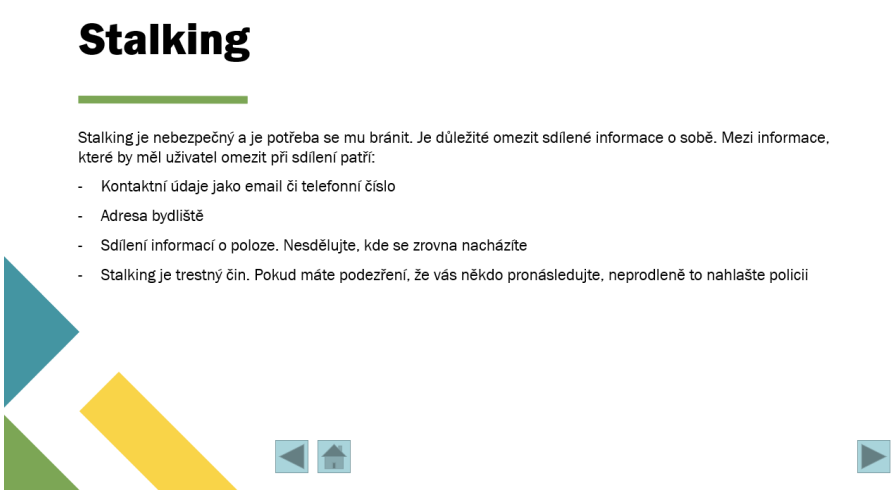
4.8.10 Stalking

Stalking nebo taktéž nebezpečné pronásledování bylo zvoleno jako příklad proto, že sociální sítě jej velmi snadno umožňují. Lidé na sociálních sítích často sdílí informace o svém soukromí a často i o jejich pohybech. Zdůraznění toho, že sociální sítě hrají ve stalkingu důležitou roli je tedy důležitou součástí e-learningu.



Obrázek 16. Snímek zabývající se stalkingem (Vlastní)

Pro lepší představu o tom, jakým způsobem se stalking projevuje, je součástí e-learningu i seznam toho, jak útočník postupuje. Mezi důležité body patří to, že útočníkem bývá často někdo z blízkého okolí a to, že stalking často nekončí jen u internetu, ale může přejít i do skutečného života. Součástí tématu je i kvíz na téma statistik ohledně stalkingu.



Obrázek 17. Rady u stalkingu (Vlastní)

Část zabývající se opatřeními proti stalkingu se věnuje hlavně problematice sdělování polohy a kontaktní údajů. Apeluje na to, aby uživatelé nesdíleli na sociálních sítích údaje jako telefonní číslo, email a další. Varuje taktéž před sdílením údajů o poloze. Mezi ně patří adresa bydliště, ale i informace o tom, kde se zrovna uživatel nachází.

4.8.11 Identifikace potencionální oběti krádeže

Posledním příkladem zneužití informací ze sociálních sítí je metoda identifikace potencionálních cílů krádeže. Není výjimečné, že pachatelé si na sociálních sítí vyhledávají potencionální cíle pro vykradení domů. Procházejí profily uživatelů a hledají známky větších finančních hotovostí a drahého majetku.

Obrázek 18. Snímek zabývající se výběrem potencionálních obětí (Vlastní)

Součástí e-learningu je popis, jak probíhá zákrok ze strany pachatele. Rady, které e-learning poskytuje uživatelům, se zaměřují hlavně na to, aby uživatel nesdílel informace o svém majetku a dával si pozor na to, co fotí. Dále pak radí dávat si pozor na zveřejňování adresy bydliště, denního rozvrhu a budoucích plánů.

4.8.12 Případy využití informací na sociálních sítích v praxi

Čtvrtá kapitola e-learningu se zabývá příklady zneužití informací ze sociálních sítí v praxi. Cílem je ukázat uživateli, že hrozby na sociálních sítích jsou skutečné a mohou nastat. Tato část slouží opět k tomu, aby se uživatel zamyslel nad svým chováním na sociálních sítích a dával si pozor co na nich sděluje.

4.8.13 Pokus o krádež automobilu

Detaily tohoto případu jsou již rozebrány v teoretické části práce. Příklad byl zvolen proto, že demonstruje, jak málo stačí potencionálnímu pachateli k získání všech potřebných informací. Zároveň ukazuje, že i když nebyla krádež vozu úspěšná, pachatel stále ukradl vybavení v nezanedbatelné finanční hodnotě.

Obrázek 19. Slide pokus o krádež automobilu (Vlastní)

4.8.14 Krádež identity

Tento příklad byl zvolen pro ukázku o pokus krádeže identity. Cílem bylo ukázat, že pokusy o krádež identity se nevyhnou ani známým osobám. Případ demonstruje pokus o podvod ve velkém měřítku. Cílem byl zpěvák a jeho fanoušci, mohlo tedy dojít k značné škodě. Případ zároveň ukazuje relativně rychlou odezvu ze strany sociální sítě. Když zpěvák výzvu zveřejnil tak došlo k masovému udání falešného účtu a provozovatel sociální sítě rychle na tento podmět reagoval. [27]

4.8.15 Účast na zakázané akci

Tento případ je taktéž popsán v teoretické části. Cílem tohoto příkladu je ukázat, že to, co uživatel sdílí, nemusí být nutně využito ke kriminální činnosti, ale i jako důkaz pro správní orgány.

4.8.16 Nastavení a ochrana informací

Poslední kapitola e-learningu se věnuje představení možností nastavení sociálních sítí z hlediska ochrany soukromí. Cílem je poučit uživatele o tom, jaké možnosti mu nabízí samotné sociální sítě z hlediska ochrany dat. Tato část je koncipována jako manuál. Důležité je, aby tato část byla co nejvíce jednoduchá a přehledná, aby uživatel mohl snadno následovat jednotlivé kroky.

Obrázek 20. Úvodní slide do poslední části e-learningu (Vlastní)

4.8.17 Nastavení Facebooku

První část se věnuje nastavení Facebooku. Uživateli je představeno, jak bude po doporučeném nastavení jeho stránka vypadat pro cizí uživatele a pak mu je poskytnut manuál pro tato nastavení.

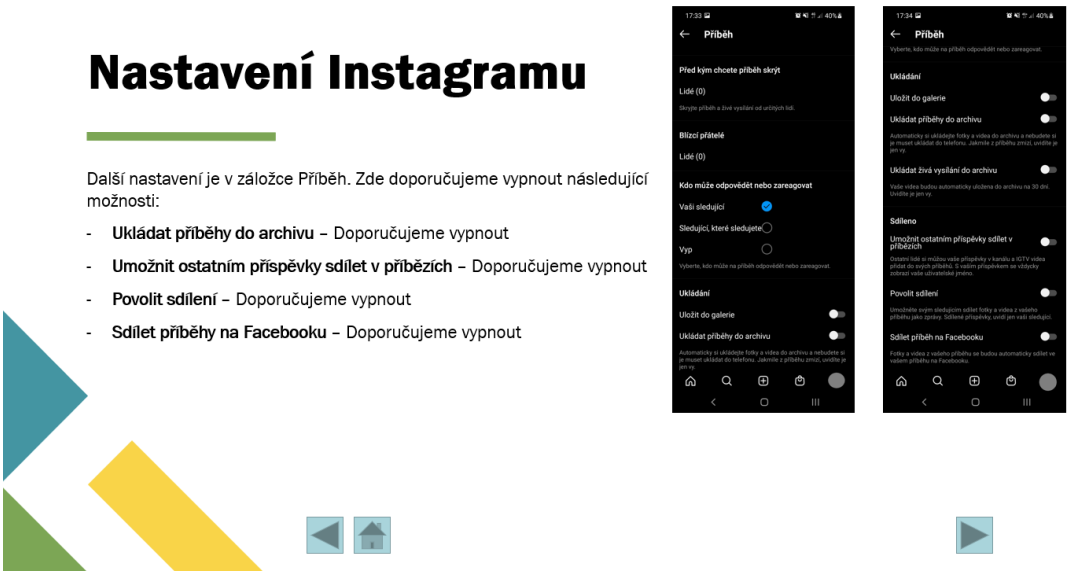
Manuál je jednoduchý a popisuje jednotlivé kroky. Ukazuje, kam má uživatel kliknout, aby se dostal do správného nastavení a popisuje, které záložky nastavení jsou v zájmu uživatele a pak prochází jednotlivé body nastavení a zároveň doporučuje, jakým způsobem tyto záložky nastavit. Jednotlivé kroky jsou doplněny o obrázky se zvýrazněním zájmových položek. To proto, aby byla zvýšena přehlednost celého nastavení a zároveň bylo jasné, jak je nastavit.

Obrázek 21. Slide představující možnosti nastavení Facebooku (Vlastní)

Doporučené nastavení sociální sítě silně omezuje počet položek, které jsou viditelné pro ostatní uživatele. Vzhledem k tomu, že e-learning je určen převážně pro mladistvé, je přísné nastavení vcelku žádoucí.

4.8.18 Nastavení Instagramu

Nastavení Instagramu má stejné cíle jako nastavení Facebooku. Jediným rozdílem je, že manuál je určen pro mobilní aplikaci. Instagram je primárně aplikací mobilní, a proto je vytvořen manuál právě pro tuto platformu.

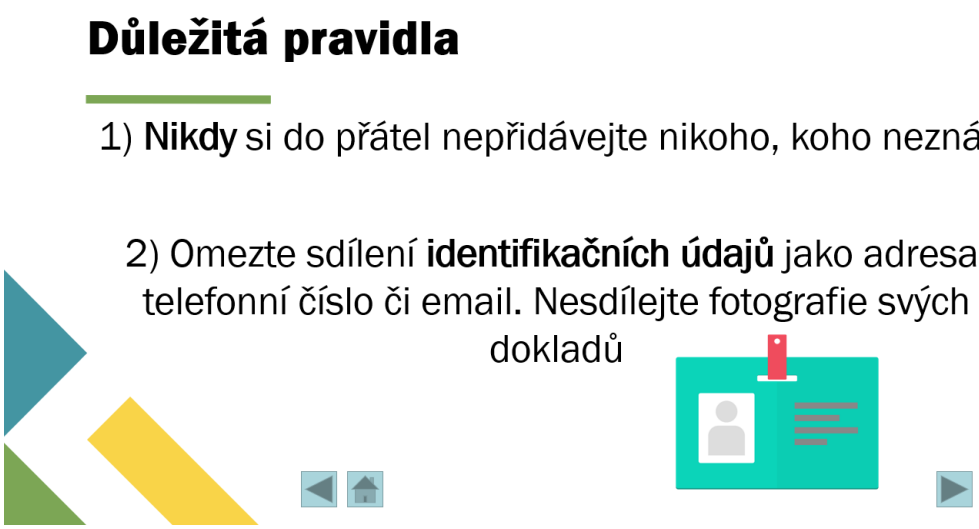


Obrázek 22. Slide představující možnosti nastavení Instagramu (Vlastní)

Jediným rozdílem mezi manuály nastavení Facebooku a Instagramu je ten, že doplňkové fotografie manuálu zabírají méně místa. To umožňuje snadno dát na slide více informací o nastavení a celkově tak zkrátit délku této části. Rozsah této části je tedy oproti předchozí zhruba o polovinu kratší.

4.8.19 Pravidla chování na sociálních sítích

Poslední součástí e-learningu je sestavení pravidel pro uživatele. Pravidla vycházejí ze všech probraných situací a snaží se apelovat na uživatele, aby se jimi řídil. [28] [29]



Obrázek 23. Pravidla chování na sociální síti (Vlastní)

Vybraná pravidla pro e-learning a důvod jejich volby pro něj jsou popsána následovně:

- Nikdy si do přátel nepřidávejte nikoho, koho neznáte.

Toto pravidlo bylo vybráno za účelem toho, že ten, kdo má přístup k účtu jako přítel, má mnohem větší přístup k informacím o uživateli a má tak víc možností, jak tyto znalosti zneužít.

- Omezte sdílení identifikačních údajů jako adresa, telefonní číslo či email. Nesdílejte fotografie svých dokladů.
- Nesdílejte informace o svém denním rozvrhu a budoucích plánech.

Tyto pravidla byla zvolena, aby si uživatel pamatoval nesdílet informace o své poloze. Ta se dá zneužít mnoha způsoby včetně stalkingu, a proto je dobré, se těmto informacím vyhnout.

- Nechlubte se svým majetkem a finanční situací. Cennosti při fotografování ukliďte mimo záběr.

Toto pravidlo slouží jako prevence proti tomu, aby se uživatel pokud možno nestal cílem ze strany zlodějů a přímo navazuje na předchozí 2 pravidla. Lidé mají často potřebu se chlubit, a proto jim je potřeba připomenout, že se tyto informace dají zneužít a mohou z nich udělat cíl pro krádež.

- Nesdílejte informace o rodinných vztazích.

Pravidlo o sdílení informací o rodinných příslušnících slouží hlavně jako prevence před krádeží identity a ochranou svých bližních.

- Nesdílejte fotografie z akcí, kde dochází ke konzumaci alkoholu.
- Nepomlouvejte na sociálních sítí svoji práci, spolupracovníky či další uživatele. Snažte se na nich vystupovat s respektem.

O informace o svých potencionálních zaměstnancích se zajímá většina zaměstnavatelů. Tyto pravidla připomínají uživateli, že na sociálních sítích reprezentuje sám sebe širokému množství lidí a měl by tak dávat pozor na to, jakým způsoben vystupuje.

- Pravidelně kontrolujte, zda nejste označeni na fotkách a příspěvcích jiných uživatelů. Můžou o vás vyzradit to, co nechcete.

Poslední pravidlo je pro uživatele velmi důležité. Ačkoliv má plnou kontrolu nad svým profilem, tak to neplatí o profilech svých přátel a ostatních uživatelů. Na sociálních sítích se mohou objevit příspěvky, které na něj mohou snadno prozradit množství nechtěných informací. Uživatel by měl proto pravidelně kontrolovat, zda se takové příspěvky o něm někde nenachází.

4.8.20 Předposlední a poslední slide

Předposlední slide obsahuje shrnutí částí e-learningu a zdůrazňuje důležitější body. Poslední slide pak obsahuje poděkování a rozloučení s uživatelem.

4.9 Doladění e-learningu

V tomto kroku dochází k doladění posledních detailů ohledně e-learningu. Cílem je opravit gramatiku, vizuální detaily a další. E-learning byl v tomto případě odeslán několika dobrovolníkům k zaslání zpětné vazby k finálnímu produktu.

Jednou z úprav na e-learningu bylo v části manuálu nastavení sociálních sítí pořízení nových verzí fotodokumentace. Původní fotodokumentace obsahovala fotografie stránek v tzv. světlé verzi stránek. Stránky měly bílé pozadí a kvůli tomu došlo ke splynutí obrázků s pozadím e-learningu. Na základě zpětné vazby pak byla pořízena nová fotodokumentace, kdy u webové stránky Facebooku a aplikace Instagramu bylo přepnuto na tmavý mód a díky tomu nyní obrázky v manuálu mnohem lépe vyniknou.

Dále došlo k obecné úpravě časování animací, gramatických chyb, překlepů a ostatních nedodělků.

4.10 Publikování e-learningu

Posledním krokem je publikování e-learningu. E-learning byl publikován mezi cílovou skupinu uvedenou v kroku 3. Účastníci obdrželi e-learning a absolvovali jej. Poté byli požádáni o zaslaní zpětné vazby. Někteří účastnici se již zúčastnili testování prototypu. Tito uživatelé uvedli následující:

- Změny oproti prototypu jsou pozitivní. Vizuální stránka je lepší
- Byl vylepšen způsob předání informací

Všichni uživatelé pak poskytli další zpětnou vazbu, která se zabírá e-learningem celkově a uvedli následující

- Vizuální stránka obdržela pozitivní zpětnou vazbu. Zvolené vizuální prvky nejsou rušivé
- Informace, které e-learning poskytuje jsou poučné. Uživatelé uvedli, že se přiučili novým faktům
- Délka e-learningu je dostačující. Není příliš dlouhý na to, aby byl unavující, a zároveň předá informace v dostatečném množství
- Uživatelé by ocenili větší množství obrázků pro zvýšení atraktivity
- Fotodokumentace nastavení by měla být větší. Některé prvky jsou špatně čitelné

Tato zpětná vazba byla pak následně zpracována a na jejím základě došlo k dalším vylepšením e-learningu.

Celkově uživatelé hodnotili e-learningu pozitivně a uvedli, že informace v něm obsažené budou při budoucím používaní sociálních sítí brát v potaz.

ZÁVĚR

Cílem bakalářské práce bylo seznámit s ochranou soukromí na sociálních sítích. V teoretické části jsme se seznámili s dnes běžně používanými sociálními sítěmi a jejich způsobem fungování. V další části jsme prošli informace sdílené na sociálních sítích. V této došlo k seznámení s informacemi, jaké lidé běžně sdělují a pak, jakým způsobem se tyto informace dají zneužít. Součástí byl i přehled dnes nejčastějších způsobů, kterými lze takto informace zneužít. Byla zde vysvětlena metodika útoků na uživatele i jejich cíle a následky. Pro demonstraci pak bylo zvoleno několik příkladů zneužití ze skutečného života. Poslední část teorie této seminární práce se věnovala tvorbě e-learningu. Došlo zde k popisu základních postupů při jeho tvorbě.

Cílem praktické části práce byla tvorba e-learningu. Tvorba probíhala v souladu s kroky zmíněnými v teoretické části. Došlo k základnímu vytyčení cílů, přípravě materiálů, volbě cílové skupiny a návrhu osnovy. Všechny tyto základní kroky slouží k vytvoření ucelené představy o podobě e-learningu a z nich pak vychází celý zbytek práce. Praktická část pak pokračovala tvorbou konceptu v podobě prototypu, který byl předveden dobrovolníkům, kteří poskytli zpětnou vazbu. Zpětná vazba byla pak nadále zpracována a sloužila jako jeden z podkladů při výrobě samotného e-learningu. Samotná tvorba e-learningu probíhala v programu Microsoft Powerpoint, kvůli jeho přizpůsobitelnosti. Popis jednotlivých slidů představil jejich cíl a roli v rámci celého e-learningu. Jednotlivé stránky e-learningu jsou vytvořeny tak, aby předaly uživateli co největší množství informací, pokud možno co v nejkompaktnější podobě. Informace obsažené v e-learningu představují to nejdůležitější z toho, co si má uživatel zapamatovat. Tato část práce je pak doplněna o fotodokumentaci, která slouží k vytvoření lepší představy o podobě e-learningu a pro demonstraci myšlení autora práce. Předposledním krokem byla úprava e-learningu. Zde došlo pouze k minimálním změnám na finálním produktu. V posledním kroku došlo ke zveřejnění e-learningu v cílové skupině. Na základě zpětné vazby potom došlo k dalším úpravám e-learningu.

E-learning představuje problematiku sdílení informací na sociálních sítích a cílem je uživatele poučit. Ze zpětné vazby vyplývá, že se tohoto cíle podařilo dosáhnout a uživatelé si z e-learningu nějaké informace odnesli.

SEZNAM POUŽITÉ LITERATURY

[1] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[2] Definition of social media. *Webster's Dictionary* [online]. [cit. 2020-11-29]. Dostupné z: https://www.merriam-webster.com/dictionary/social%20media

[3] The Evolution of Social Media: How Did It Begin, and Where Could It Go Next? *Maryville University* [online]. [cit. 2020-11-29]. Dostupné z: https://online.maryville.edu/blog/evolution-social-media/

[4] GOODLINGS, Lewis. *Screenshot of Tom ANDERSON's profile page* [online]. In:. 2011 [cit. 2020-11-29]. Dostupné z: https://www.researchgate.net/publication/289077180_The_Dilemma_of_Closeness_and_Distance_A_Discursive_Analysis_of_Wall_Posting_in_MySpace

[5] HALL, Mark. Facebook. *Brittanica* [online]. [cit. 2020-11-29]. Dostupné z: https://www.britannica.com/topic/Facebook

[6] The top 500 sites on the web. *Alexa* [online]. [cit. 2020-12-02]. Dostupné z: https://www.alexa.com/topsites

[7] HOSCH, William a Michael RAY. Twitter. *Britannica* [online]. 2009 [cit. 2020-11-29]. Dostupné z: https://www.britannica.com/topic/Twitter

[8] MACALE, Sherilynn. A rundown of Reddit's history and community. *The Next Web* [online]. 11.10.2011 [cit. 2020-12-02]. Dostupné z: https://thenextweb.com/socialmedia/2011/10/14/a-rundown-of-reddits-history-and-community-infographic/

[9] BLYSTONE, Dan. The Story of Instagram: The Rise of the #1 Photo-Sharing Application. *Investopedia* [online]. 6.6.2020 [cit. 2020-12-02]. Dostupné z: https://www.investopedia.com/articles/investing/102615/story-instagram-rise-1-photo0sharing-app.asp

[10] MENG, Andrew. WHAT IS PINTEREST, AND HOW DOES IT WORK? *Infront Webworks* [online]. 14.1.2019 [cit. 2020-12-03]. Dostupné z: https://www.infront.com/blog/what-is-pinterest-and-how-does-it-work/

[11] OCHS, Josh. What is Tumblr? Parent and Teacher Guide. *Smart Social* [online]. 29.8.2019 [cit. 2020-12-03]. Dostupné z: https://smartsocial.com/what-is-tumblr-parent-teacher-guide/

[12] RUSSELL, Matthew a Mikhail KLASSEN. *Mining the Social Web*. 3rd edition. Sebastopol: O'Reilly Media, 2019. ISBN 978-1-491-98504-5.

[13] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Organizace pro hospodářskou spolupráci a rozvoj* [online]. [cit. 2021-04-03]. Dostupné z: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[14] MADDEN, Mary, Amanda LENHART, Sandra CORTESI, Urs GASSER, Maeve DUGGAN, Aaron SMITH a Meredith BEATON. *Teens, Social Media, and Privacy* [online]. Washington, 2013 [cit. 2020-12-03]. Dostupné z: https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/

[15] More Than Half of Employers Have Found Content on Social Media That Caused Them NOT to Hire a Candidate, According to Recent CareerBuilder Survey. *CareerBuilder* [online]. 9.8.2018 [cit. 2020-12-04]. Dostupné z: http://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey

[16] RAFTER, Dan. Social Media Identity Theft: How to Protect Yourself. *LifeLock* [online]. 22.10.2020 [cit. 2020-12-03]. Dostupné z: https://www.lifelock.com/learn-internet-security-social-media-behavior-leads-identity-theft.html

[17] RAHIM SOOMRO, Tariq. *Identity Theft and Social Media* [online]. Dubaj, 2018 [cit. 2020-12-03]. Dostupné z: https://www.researchgate.net/publication/323185128_Identity_Theft_and_Social_Media. Shaheed Zulfikar Ali Bhutto Institute of Science and Technology.

[18] Krádež identity. *Internetem bezpečně* [online]. 2016 [cit. 2020-12-04]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[19] Nebezpečné pronásledování (stalking). *Policie České republiky* [online]. [cit. 2020-12-04]. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-nebezpecne-pronasledovani-stalking.aspx

[20] MCCARTHY, Linda a Denise WELDON-SIVIY. *Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.

[21] FOSTER, Matthew. Is The Way We Use Social Media Leaving Us Vulnerable To Burglary? *Social Media Week* [online]. 11.5.2015 [cit. 2020-12-04]. Dostupné z: https://socialmediaweek.org/blog/2015/05/social-media-leaving-us-vulnerable-burglary/

[22] JEŽEK, Tomáš. Veterána k prodeji nafotil před vlastní garáží, za pár hodin přišli zloději. *Idnes* [online]. MAFRA, 12.1.2021 [cit. 2021-04-03]. Dostupné z: https://www.idnes.cz/auto/zpravodajstvi/veteran-prodej-inzerat-foto-garaz-zlodeji-chyba-mercedes-socialni-site.A210108_114658_automoto_taj

[23] BARBORA, Sedlářová. Policie zasahovala v otevřených barech. Účastníci se chlubili na webu. *Idnes* [online]. MAFRA, 20.3.2021 [cit. 2021-04-03]. Dostupné z: https://www.idnes.cz/praha/zpravy/praha-otevrene-bar-restaurace-kokain.A210320_135225_praha-zpravy_bse

[24] EVA, Zahradnická. Pozor na sociální sítě. Přišla o invalidní důchod kvůli fotkám na Facebooku. *Idnes* [online]. MAFRA, 9.2.2021 [cit. 2021-04-03]. Dostupné z: https://www.idnes.cz/zpravy/domaci/invalidni-duchod-facebook-pater.A210208_202635_domaci_ldv

[25] HUHTANEN, Akseli. The design book for online learning. *FITech Network University* [online]. 2019 [cit. 2020-12-07]. Dostupné z: https://fitech.io/app/uploads/2019/09/The-Design-Book-for-Online-Learning-v-1.4.1-EN-web.pdf

[26] 10 Crucial Steps in the eLearning Development Process. *Vyond* [online]. 13.1.2020 [cit. 2020-12-07]. Dostupné z: https://www.vyond.com/resources/10-crucial-steps-in-the-elearning-development-process/

[27] Václav Noid Bárta obětí podvodníka: Krádež identity i tahání peněz z fanoušků! *Blesk* [online]. CZECH NEWS CENTER, 21.4. 2020 [cit. 2021-5-9]. Dostupné z: https://bit.ly/3uy4z7T

[28] BAILEY, Matthew, ed. *Complete Guide to Internet Privacy, Anonymity & Security*. 2nd edition. Nerel Online, 2015. ISBN 978-3-9503093-3-1.

[29] TIPTON, Harold a Micki KRAUSE NOZAKI, ed. *Information Security Management Handbook*. 6th edition. Boca Raton (Florida): CRC Press, 2012. ISBN 978-1-4398-9315-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká republika
OECD	Organizace pro hospodářskou spolupráci a rozvoj
USA	Spojené státy americké

SEZNAM OBRÁZKŮ

Obrázek 1. Profil zakladatele sítě MySpace Thomase Andersona v roce 2007 [4] ...11
Obrázek 2. Facebookový účet Marka Zuckerberga (Vlastní) 12
Obrázek 3. – Účet na Twitteru (Vlastní) 13
Obrázek 4. Úvodní stránka Reddit (Vlastní) 15
Obrázek 5. Úvodní strana e-learningu (Vlastní) 35
Obrázek 6. Hlavní menu s výběrem kapitol (Vlastní) 35
Obrázek 7. Snímek s úvodem do sociálních sítí (Vlastní) 36
Obrázek 8. Kvízová otázka (Vlastní) 37
Obrázek 9. Odpověď na kvíz (Vlastní) 37
Obrázek 10. Sdílení informací (Vlastní) 38
Obrázek 11. Úvod do zneužití informací (Vlastní) 39
Obrázek 12. Snímek zabývající se hledáním zaměstnání (Vlastní) 39
Obrázek 13. Rady u hledání zaměstnání (Vlastní) 40
Obrázek 14. Snímek krádež identity (Vlastní) 41
Obrázek 15. Rady u krádeže identity (Vlastní) 41
Obrázek 16. Snímek zabývající se stalkingem (Vlastní) 42
Obrázek 17. Rady u stalkingu (Vlastní) 42
Obrázek 18. Snímek zabývající se výběrem potencionálních obětí (Vlastní) 43
Obrázek 19. Slide pokus o krádež automobilu (Vlastní) 44
Obrázek 20. Úvodní slide do poslední části e-learningu (Vlastní) 45
Obrázek 21. Slide představující možnosti nastavení Facebooku (Vlastní) 46
Obrázek 22. Slide představující možnosti nastavení Instagramu (Vlastní) 46
Obrázek 23. Pravidla chování na sociální síti (Vlastní) 47

SEZNAM PŘÍLOH

P1 CD se souborem E-learning Ochrana soukromí na sociálních sítích