Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Krádež virtuální identity

Bakalářská práce

Lucie Nevludová

Školitel: Mgr. Jakub Kothánek, LL.M.

České Budějovice 2019

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Lucie Nevludová
(jméno, příjmení, tituly)

Obor – zaměření studia: Aplikovaná informatika

Katedra/ústav PřF JU, kde bude práce vypracována a obhájena: UAI
Školitel: Mgr. Jakub Kothánek
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF JU: .....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: .....
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce: Krádež virtuální identity

Úkoly práce:

- Vytvořit literární rešerši na téma krádež virtuální identity.
  1. Analyzovat problematiku spojenou s pojmem krádež identity.
  2. Identifikovat metody, kterými se získávají informace pro krádež virtuální identity.
  3. Zmapovat právní důsledky týkající se krádeže virtuální identity plynoucí z platné legislativy (v době vypracování práce).

Cíle práce:

- Hlavní cíl: Navrhnout metodiku pro předcházení krádeže virtuální identity na základě vlastního výzkumu.
- Dílčí cíl: Konfrontovat navrženou metodiku s osobou (obětí), které byla v minulosti virtuální identita odcizena a získat od ní zpětnou vazbu (např. formou rozhovoru, či dotazníkového šetření).

Upřesnění hlavního cíle práce: Student v rámci praktické části práce provede vlastní výzkum, který bude spočívat v provedení sociálního experimentu. Jeho podstatou bude zjištění míry důvěřivosti cílové skupiny osob při otevírání neznámých zdrojů pod záminkou simulace důvěryhodného prostředí. Výsledek experimentu poté bude vyhodnocen základními statistickými metodami.

Základní doporučená literatura:

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-18-8.

Financování práce .....

Školitel práce .....podpis: .....

U externích vedoucích fakultní garant práce .....podpis: .....

Garant oboru bak. studia (nepožaduje se u oboru biologie) .....podpis: .....

Vedoucí katedry/ústavu PřF JU, kde proběhne obhajoba.....podpis: .....

Případný souhlas vedoucího ústavu AV .....podpis: .....

V Českých Budějovicích dne 25.2.2019 Podpis studenta .....

Bibliografické údaje

Nevludová L., 2019: Krádež virtuální identity. [Virtual Identity Theft. Bc. Thesis, in Czech] – 81 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Bakalářská práce je zaměřena na téma krádež virtuální identity. V teoretické části práce jsou vysvětleny pojmy týkající se identity osoby. Dále jsou vybrány a popsány některé kybernetické útoky, které se krádeže identity týkají. Zmíněny jsou také informace týkající se zákonného pohledu na toto téma. Praktická část obsahuje metodiku pro předcházení krádeže virtuální identity, metodika je zpracována na základě sociálního experimentu. Navržená metodika je konfrontována s osobou, které byla v minulosti virtuální identita odcizena.

Klíčová slova

Krádež identity, odcizení identity, kybernetické útoky, zvýšení zabezpečení

Annotation

The bachelor thesis is focused on virtual identity theft. In the theoretical part of this thesis are explained terms related to the identity of the person. In addition, some cyber attacks related to identity theft are selected and described. Information regarding the legal perspective on this topic is also mentioned. The practical part of the thesis contains a methodology for preventing theft of virtual identity, the methodology is based on a social experiment. The methodology is confronted with a person whose virtual identity was previously stolen.

Key words

Identity theft, identity fraud, cyber attacks, security increase

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracovala samostatně pouze s využitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 9. prosince 2019 Podpis.....

Poděkování

Chtěla bych poděkovat Mgr. Jakubu Kothánkovi, LL.M., vedoucímu mé bakalářské práce, za odborné rady a čas věnovaný při konzultacích. Mé poděkování také patří Doc. RNDr. Ivě Dostálkové, Ph.D. za pomoc se zpracováním statistické analýzy. Dále bych chtěla poděkovat paní Mgr. Bohdaně Majerové za odbornou konzultaci jazykové stránky práce. V neposlední řadě bych také chtěla poděkovat své rodině a přátelům za trpělivost a podporu během celého studia.

Obsah

Úvod

Krádež a zneužití cizí identity nepředstavuje ve své podstatě nový jev, prostřednictvím informačních technologií ale nabyl nových a někdy taktéž závažnějších forem.

S příchodem informačních technologií tato trestná činnost začala nabírat nových rozměrů. Společně s obrovským rozvojem v tomto oboru vzniklo mnoho dalších možností pro potencionální útočníky. Virtuální identita obsahuje aspekt osobní a sociální identity stejně jako běžná identita. Na rozdíl od sociální identity, kde si ztrátu identifikačních dokumentů uvědomíme velice rychle, zcizení virtuální identity zjistíme často až ve chvíli, kdy útočník nějakým způsobem poškodí nás nebo někoho z našeho okolí. V dnešní době se čím dál tím více setkáváme s odcizením sociálních účtů nebo přijímáním e-mailů s podvodnými údaji či odkazy na podvodné stránky.

Tato práce je zaměřena na seznámení s nejčastějšími pojmy a kybernetickými technikami, které se týkají krádeže identity. Práce by měla ve čtenáři vzbudit pocit, že virtuální identitu je nutné chránit minimálně stejně, jako chrání svou sociální identitu, se kterou vystupuje například na úřadech.

Cílem práce je vytvořit rešerši na téma krádež virtuální identity. V práci jsou vysvětleny pojmy týkající se identity, krádeže identity a základní informace o několika metodách, které útočníci využívají pro krádež identity. Zároveň jsou stručně zpracovány informace týkající se zákonného pohledu na toto téma.

Součástí práce je praktická část, ve které je zpracována statistická analýza a metodika pro předcházení krádeže virtuální identity. Metodika je zpracována na základě sociálního experimentu, ve kterém se zjišťuje míra důvěřivosti cílové skupiny osob při otevírání neznámých zdrojů pod záminkou simulace důvěryhodného prostředí. Navržená metodika je následně konfrontována s osobou, které byla v minulosti virtuální identita odcizena.

1 Sociální a virtuální identita

V minulosti se k prokazování identity používaly listinné dokumenty – zejména občanský průkaz, řidičský průkaz, rodný list nebo cestovní pas. Zaznamenání ztráty nebo odcizení dokumentu bylo otázkou relativně krátké doby.

V dnešní době jsme téměř přestali vystupovat osobně, potvrzení naší identity probíhá pravidelně prostřednictvím kódů a hesel. Naše virtuální (resp. elektronická) identita existuje uložená „někde“ v databázi, a tak je možné, že informace o identitě získá někdo jiný. Skutečnost, že nám byla virtuální identita zcizena, zjistíme většinou až ve chvíli, kdy jsme poškozeni my, nebo někdo z našeho virtuálního okolí. V některých případech útočník nestihne provést své plány a díky obezřetnosti a pohotovosti další možné oběti nakonec nedojde k poškození žádné osoby. [9] [10]

1.1 Identita

Identita (latinsky *identitas*, odvozené od slova *idem* – stejný) neboli totožnost je pojem používaný v případě, že porovnávané objekty, osoby nebo jevy je možné zaměnit. Takováto záměna je možná pouze v případě, že mezi vlastnosti porovnávaných objektů je možné pomyslně položit znaménko rovnosti. Vždy by mělo platit, že vše, co lze vypovědět o jedné entitě, lze vypovědět taktéž o entitě druhé. [1, s. 37 – 38]

1.1.1 Identita osoby

Pokud se hovoří o identitě osoby, jedná se o kombinaci biologických i psychických, vrozených i získaných, individuálních i specifických vlastností a schopností vnímat sám sebe. Identita je ztělesněním našeho vlastního já, z čehož vyplývá, že každý z nás je totožný právě a jen sám se sebou. [1, s. 39] Sociální (resp. fyzická) identita osoby je unikátní, na světě neexistuje člověk, který by měl shodnou sociální identitu s někým dalším (např. DNA jednovaječných dvojčat je také odlišná – projevují se zde drobné mutace a odlišnosti). [5, s. 271]

Během svého života může každá osoba přijmout různé identity, někteří dokonce používají několik zcela rozdílných identit zároveň. Může se jednat o osoby spojené se zpravodajskou nebo kriminální činností, pracovníky bezpečnostních služeb pracující s krytím, dále také o herce nebo umělce. [1, s. 39]

V kriminalistice se z praktických důvodů rozlišují pojmy identita a shodnost. Identita osoby je v čase neměnná a je jednoznačná. Osoba shodná sama se sebou je pouze v jednom jediném časovém okamžiku, jelikož dochází k neustálému pozměňování fyziologickými procesy – např. nemoc, stárnutí, změna váhy nebo rozdílné znalosti. V obou případech jde ale o jednu a tutéž identickou osobu. [1, s. 40]

1.2 Identifikace

Pod pojmem identifikace je myšlen proces určení identity osoby, jevu nebo systému. Jinak řečeno jde o proces, jehož cílem je určit, zda porovnávané objekty jsou identické či nikoliv. Obecná identifikace je velice rozmanitý rozhodovací proces, ve kterém je třeba porovnávat vlastnosti, vztahy nebo funkce objektu. Tento rozhodovací proces by měl být realizován v konečném čase – konečné posloupnosti rozhodovacích kroků. [1, s. 40]

Dříve byl pojem identifikace spojován zejména s vojenskými a bezpečnostními aplikacemi. Ve vědeckém odvětví byl tento pojem spojován zejména s kriminalistickými a forenzními disciplínami. [1, s. 33]

Identifikaci je z kriminalistického hlediska možné dělit do dvou skupin – individuální a skupinová. [1, s. 35] U individuální identifikace se jedná o identifikační vlastnosti, které umožňují přesně identifikovat konkrétní objekt. Existuje tedy známý vztah mezi kriminalistickou stopou a konkrétním objektem, který stopu vytvořil. Skupinová, nebo také druhová identifikace, zahrnuje vlastnosti, kterými je možné identifikovaný objekt zařadit do určité skupiny objektů. [11, s. 44]

1.2.1 Identifikace osoby

Identifikace osoby je specifický případ obecné identifikace, kde člověk může být objektem i subjektem identifikace. V tomto případě lze uvažovat pojmy vnější a vnitřní identifikace (sebeidentifikace). U vnější identifikace jde o stanovení fyzické identity člověka, naopak vnitřní identifikací rozumíme nalezení a vnímání vlastní sociální, filosofické nebo psychologické identity. [1, s. 44]

Faktory zabezpečení

Je třeba vědět, zda daná osoba je tou osobou, za kterou se vydává, nebo zda ta určitá osoba nezneužívá identitu někoho jiného ke svému prospěchu. [1, s. 35]

Osobu můžeme identifikovat podle tří základních faktorů (přístupů): osoba něco zná, něco má nebo čím je. V případě, kdy osoba „něco zná“, prokazuje svou znalost (např. heslo, postup). Přístup „něco má“ znamená vlastnictví určité věci danou osobou (např. karta, klíč). A nakonec, pokud osoba „něčím je“, znamená to, že má určité biometrické charakteristiky (např. otisk prstu, otisk oční duhovky, hlas) nebo má nějaké chování. [12] [18]

Další pro identifikaci osoby je kontextový faktor. Tento faktor zahrnuje informace o místu uživatele pomocí ověřitelné polohy, času autentizace, zařízení nebo IP adresy, kterou osoba používá. [8]

1.2.2 Identifikátor

Identita je většinou reprezentována jednoznačným identifikátorem ve vybrané množině. Identifikátor je informace, která poskytuje možnost pro vzájemné odlišení jednotlivých entit stejné třídy objektů. [13]

Identifikátor se může dělit dle původu identifikátoru na přirozený (např. jméno) a umělý (např. identifikační číslo). Dále je možné dělit identifikátory dle vypovídající hodnoty identifikátoru na významový, který nese dodatečnou informaci (např. rodné číslo – nese informaci data narození a pohlaví) a bezvýznamový, který nenese jinou informaci než unikátnost (např. číslo zákaznické karty). [7, s. 125]

Virtuální identita používá jako identifikátor uživatelské (resp. přihlašovací) jméno, které zajišťuje jednoznačnou identifikaci uživatele v rámci aplikace, webové stránky nebo v nějakém softwaru. [14]

1.3 Autentizace

Autentizace (řecky *authentikos*, latinsky *authenticus* – skutečný, původní) znamená ověření identity nějakého subjektu. Jedná se o bezpečnostní opatření, které zajišťuje ochranu před falšováním identity. [12] Autentizace je jednoznačné určení uživatele, který přistupuje k systému. Cílem autentizace je zajištění znalosti identity komunikujícího uživatele. [15] Na základě důkazů, podle některého z výše uvedených faktorů, dochází k potvrzení identity subjektu. [12]

Ověření identity se vykonává prostřednictvím vnitřních mechanismů systému, nejčastěji databázového serveru. V databázi je uložena informace o uživateli (uživatelském jménu) a jemu příslušném heslu. Tato informace bývá v databázi šifrována. [15]

Příkladem autentizace může být přihlášení pomocí hesla do e-mailu. Vždy probíhá ověření, zda je zadané heslo správné (neboli, zda odpovídá heslu, které je uloženo v databázi k danému uživatelskému jménu). Autentizaci je možné provést také prostřednictvím vlastnictví nebo určité vlastnosti. [16]

1.4 Autorizace

Autorizací se rozumí proces, během kterého dochází k ověření přístupových oprávnění uživatele vstupujícího do informačního systému. Podstatou autorizace je ověřit, zda uživatel má právo přistupovat k určitému obsahu nebo provést určitou akci. Procesu autorizace velice často předchází autentizace. Cílem tohoto procesu je udělení souhlasu pro přístup nebo provedení určité akce, nebo odmítnutí požadavku. [15]

Například uživatel, který je přihlášený jako uživatel jsemjohndoe s e-mailovou adresou jsemjohndoe@seznam.cz může přistupovat pouze k e-mailům jemu směrovaným. E-maily, které byly směrovány na adresu jsemjohndoe1@seznam.cz nemá možnost číst (za předpokladu, že tento e-mail není vlastněn stejnou osobou).

1.5 Údaje

Pojmem údaj se označuje sdělení o konkrétním stavu jedné či více entit – jedná se o určité informace, např. údaje (resp. informace) o osobě. [24]

Osobní údaje

Nařízení Evropské unie o ochraně osobních údajů GDPR (viz kapitola 6.1 GDPR) definuje osobní údaje jako veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo nebo nepřímo identifikovat. Tuto identifikaci je možné provést odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. [3, s. 20] [17]

Osobní údaje je možné považovat za aktivum uživatele, které je vytvořeno identitou a chováním jedince. Toto aktivum je využíváno jako výměna za vyšší kvalitu služeb a produktů. Osobní údaje se používají v online platformách pro personalizaci služeb. [3, s. 20]

Mezi nejčastější osobní údaje patří např. jméno, adresa, pohlaví, věk, datum narození, rodné číslo, e-mailová adresa, IP adresa, fotografie, vzdělání a další. [17]

Citlivé osobní údaje

Pod pojmem citlivý osobní údaj se podle GDPR rozumí osobní údaj, který vypovídá o národnostním, rasovém nebo etnickém původu, náboženském nebo politickém vyznání, členství v odborových organizacích, trestních deliktech nebo pravomocném odsouzení, zdravotním stavu, osobních údajích dětí nebo genetickém údaji subjekt údajů. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. [17] [19]

Za citlivé jsou tyto údaje označeny proto, že mohou subjekt samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. [19]

Přihlašovací údaje

Přihlašovací údaje jsou údaje, které slouží k identifikaci uživatele na internetu. Skládají se nejčastěji z uživatelského jména a hesla. Během autentizace k účtu pomocí přihlašovacích údajů uživatel prokazuje znalost těchto údajů. Tyto údaje jsou vytvářeny uživatelem nebo institucí. [20]

1.6 Data

Data jsou získané a zachycené údaje, které popisují realitu. Jsou to zaznamenaná fakta nebo se jedná o výsledky pozorování reality, poznatky, informace, znalosti nebo vědomosti. Tato fakta jsou zaznamenaná dohodnutým způsobem (např. v konkrétním formátu) a mají určitý smysl. Data existují a jsou uložena na různých paměťových médiích nebo nosičích (např. papír, pevný disk, CD nebo paměťová karta). Pokud data projdou zpracováním a dostanou určitou strukturu, vytvoříme z dat informace. [21]

V informatice se pojem data používá jako označení pro čísla, text, zvuk, obraz, popřípadě jiné smyslové vjemy reprezentované v podobě vhodné pro zpracování počítačem. [4, s. 2]

Z hlediska práce s daty se rozlišují dva typy dat. Nestrukturovaná data jsou nejčastěji uložena v dokumentech, někdy také ale v podobě multimédií (obrázku, videa či zvuku). V těchto datech je obtížné vyhledávání. Naopak data strukturovaná jsou typicky uložena v nějaké databázi, ve které existují určité elementy dat s danou hierarchií (např. pole → záznam →

relace → databáze). Díky strukturovanému uložení je možné snadno vybírat pouze data, která uživatel v dané situaci potřebuje. [4, s. 2]

Na počítačích se dnes skladuje více informací než kdykoliv dříve a tyto informace mají velkou cenu. Uživatel si často neuvědomuje, že jeho počítač a jeho data jsou ohroženější než kdykoliv předtím. Dokonce v případě, kdy uživatel nebude mít na počítači žádné osobní informace, žádné finanční údaje a nic, co by někoho mohlo jakkoliv zajímat, počítač i v takovém případě může být zneužit k útoku na někoho jiného. [6, s. 41]

1.6.1 Digitální stopa

Během jakékoliv činnosti uživatele ve virtuálním světě – např. při použití vyhledávače, návštěvou webové stránky, nákupem přes internet – se tato data ukládají a vytvářejí tzv. digitální stopu. Tato stopa je tvořena vyhledatelnými informacemi, na základě kterých je možno zjistit nemálo informací o určité osobě. Digitální stopu vytváří nejen uživatel svou činností, ale je vytvářena také činností jeho přátel. [22] [23]

Digitální stopu je možné eliminovat např. mazáním cookies (data, která slouží k rozlišování jednotlivých uživatelů, ukládají se do nich uživatelské předvolby), používáním anonymního okna, které zajistí neukládání cookies a historie nebo rozmazáním, které uživatel zajistí tak, že používá několik různých účtů, které nic nespojuje. Ze všeho nejdůležitější je nutná obezřetnost uživatele při publikování informací o své osobě. [25] Je rozšířeno známé pravidlo, které říká, že informace, která se na internetu jednou objeví, už nikdy nezmizí. [26]

2 Krádež virtuální identity

Krádeží virtuální identity lze označit situaci, během které útočník převezme kontrolu nad virtuální identitou oběti. Jedná se o podvodné jednání, při kterém se útočník vydává za oběť, nejčastěji s cílem získat finanční prostředky, důležité informace nebo jiné výhody. [9] [27]

Na pojem krádež virtuální identity lze pohlížet ze dvou různých pohledů. První pohled zahrnuje vnímání tohoto pojmu některými uživateli internetu. V případě, kdy je uživateli odcizen zejména profil na sociální síti, ale útočník tento profil nijak nevyužívá, je pouze v jeho držení. Uživatel tuto situaci označuje jako krádež identity (účtu na dané webové stránce nebo v aplikaci), přičemž útočník identitu oběti prozatím pouze získal.

Z pohledu legislativy se jedná o krádež identity až v případě, kdy jako první dojde k získání identity útočníkem a následně dojde ještě ke zneužití takto získané identity. Právo krádež identity kvalifikuje jako dvoustupňový trestný čin. [28]

2.1 Odcizení

Odcizení identity uživateli, tudíž získání identity útočníkem, se v anglické terminologii označuje jako *Identity theft*. Získat kontrolu nad danou identitou může útočník dočasně nebo trvale. Cíle k získání cizí identity mohou být různé, např. se může jednat o poškození osoby, získání finančních prostředků (např. prodání profilu, vylákání financí), získání informací a další. [2, s. 318]

Pokud se útočníkovi nepodaří získat přihlašovací údaje, je možné, že stáhne veškerá dostupná data z profilu oběti a tato data následně využije k založení duplicitního profilu oběti. Jedná se o tzv. klonování profilů. Falešný profil je často od skutečného téměř k nerozeznání a uživatelé často nepoznají, že se jedná o duplicitní profil. [29] Následně tímto falešným profilem útočník oslovuje přátele oběti. Také tento přístup je možné označit za krádež identity. [10]

Získat identitu může útočník dalšími mnoha způsoby, které jsou blíže popsány v kapitole 3 Kybernetické útoky.

2.2 Zneužití

V případě, že útočník některý z výše uvedených cílů vykoná, jedná se již o zneužití získané identity. Tento krok se v anglické terminologii označuje jako *Identity fraud*. Od této chvíle se již jedná z pohledu práva platného v České republice o trestný čin. [28]

3 Kybernetické útoky

Kybernetická kriminalita (zkráceně kyberkriminalita) je kriminalita, která probíhá v kybernetickém prostoru. Tento prostor je virtuální prostředí, které nemá začátek ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je. [30] Útočník může neoprávněně získat virtuální identitu oběti několika způsoby, mezi které patří fyzický útok (odcizení počítače, odcizení disku), napadení zevnitř (zaměstnanci firmy, rodinou), napadení zvenčí (odposlech, neoprávněný vstup) a manipulační techniky (phishing, pharming, podvodné webové stránky). [9]

3.1 Sociální inženýrství

Sociální inženýrství, jinak řečeno sociotechnika, nelze považovat přímo za kybernetický útok, ale je předpokladem pro to, aby byla řada kybernetických útoků úspěšná. Jde o ovlivňování, přesvědčování nebo manipulaci osob s cílem donutit je provést určitou akci, nebo od nich získat informace, které by za jiných okolností neposkytli.

Smyslem sociálního inženýrství je vyvolat v uživateli dojem, že situace, ve které se nachází je jiná, než tomu ve skutečnosti je. [31] Řada útočníků využívá sociální inženýrství k tomu, aby získala informace nebo data a dále je využila. Taktéž policie v určité podobě využívá k získání informací, např. pro získání přístupu do telefonu, sociální inženýrství. [2, s. 186]

Pro útočníka je jednodušší uvést uživatele v omyl, během kterého sám prozradí heslo, než využívat technické přístupy nebo nástroje. Mnohdy dochází k dlouhodobému působení útočníka na uživatele, přičemž útočník následně využívá důvěřivosti, ochoty, strachu nebo neopatrnosti uživatele.

Sociální inženýrství je vedeno zpravidla třemi způsoby:

1) sběr volně dostupných dat o cíli útoku (oběti) – digitální stopa, informace v novinách a další,
2) fyzický útok, během kterého se snaží útočník získat co nejvíce informací zevnitř společnosti,
3) psychologický útok. [2, s. 186 – 188]

Mezi nejčastější metody, které využívají sociálního inženýrství, patří například podvodný e-mail nebo falešná webová stránka, prohledávání webu, nabídka vyzkoušení služby online a další. [2, s. 188]

Pro snížení rizika útoku s využitím sociálního inženýrství je třeba zvyšovat povědomí uživatelů o možných hrozbách. Znalost a zkušenost uživatelů ztěžuje pachatelům útok. [2, s. 192]

3.2 Malware

Pojem malware je zkratkou anglických slov *malicious software*, což v překladu znamená škodlivý software. Tímto pojmem je možné označit jakýkoliv software, který se využívá k narušení standardní činnosti počítačového systému, zjištění informací, nebo je využit k získání přístupu k počítačovému systému. [2, s. 204] [32]

Malware může mít různou podobu, často je pojmenován dle činnosti, kterou provádí. Jeden malware může plnit několik funkcí současně. Například se může sám dále šířit pomocí e-mailových příloh a získávat data z napadeného počítačového systému, nebo může data na napadeném počítači poškodit či smazat. [2, s. 204]

Malware je možné šířit například e-mailem, přenosovými médii, stažením z internetu a spuštěním souboru nebo může být uložen přímo na webových stránkách. [2, s. 212 – 215]

Dnes se používá primárně pojem malware, dříve se používaly jednotlivé názvy dle konkrétního software. Níže budou zmíněny pouze ty, které se týkají krádeže identity. [2, s. 204]

Vir

Vir je program nebo škodlivý kód, který se sám připojí k jinému existujícímu spustitelnému souboru nebo dokumentu. Tyto programy jsou často schopny šířit se bez nutnosti zásahu a tudíž i bez vědomí uživatele. [33] Vir se reprodukuje ve chvíli, kdy dojde ke spuštění infikovaného souboru nebo otevření dokumentu.

Některé viry ničí počítačové systémy, jiné se pouze v co největším počtu usídlí a tyto počítačové systémy následně využijí k cílenému útoku. [2, s. 207 – 208]

Červ

Počítačoví červi někdy bývají označováni za viry. Červi ale, na rozdíl od virů, nepotřebují žádný spustitelný soubor, dokáží se šířit samostatně. Napadený počítačový systém je následně využíván k dalšímu odesílání kopií sebe sama dalším uživatelům pomocí síťové komunikace. Tyto programy jsou schopny analyzovat bezpečnostní slabiny v zabezpečení informačního systému. [2, s. 208] [33]

Trojský kůň

Pojmem trojský kůň (anglicky *trojan horse* nebo *trojan*) je označován počítačový program, který obsahuje skryté funkce, s jejichž užitím uživatel nesouhlasí nebo o nich neví. Tyto funkce jsou potenciálně nebezpečné pro další fungování systému. Trojský kůň může samostatně vypadat jako neškodný program, nebo může být připojen k bezpečným programům nebo aplikacím. Na rozdíl od virů není schopen se replikovat ani šířit bez interakce uživatele. Pokud je trojský kůň aktivován, může být využit k mazání, blokování, modifikaci, kopírování dat nebo například k narušování běhu počítačového systému. [2, s. 208]

Keylogger

Keylogger nebo keystroke logger je program, který je schopen zaznamenat jednotlivé stisky kláves na napadeném počítačovém systému. Tento záznam je uložen a následně zaslán útočníkovi. Nejčastěji se využívá k zaznamenání přihlašovacích údajů k účtům, ke kterým nic netušící uživatel přistupuje. [2, s. 210] [34]

3.3 Phishing

Pojem phishing, někdy do češtiny překládán jako rhybaření, označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli (uživatelské jméno, heslo, PIN). Toto jednání má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem – k tomu využívá sociálního inženýrství. [2, s. 246]

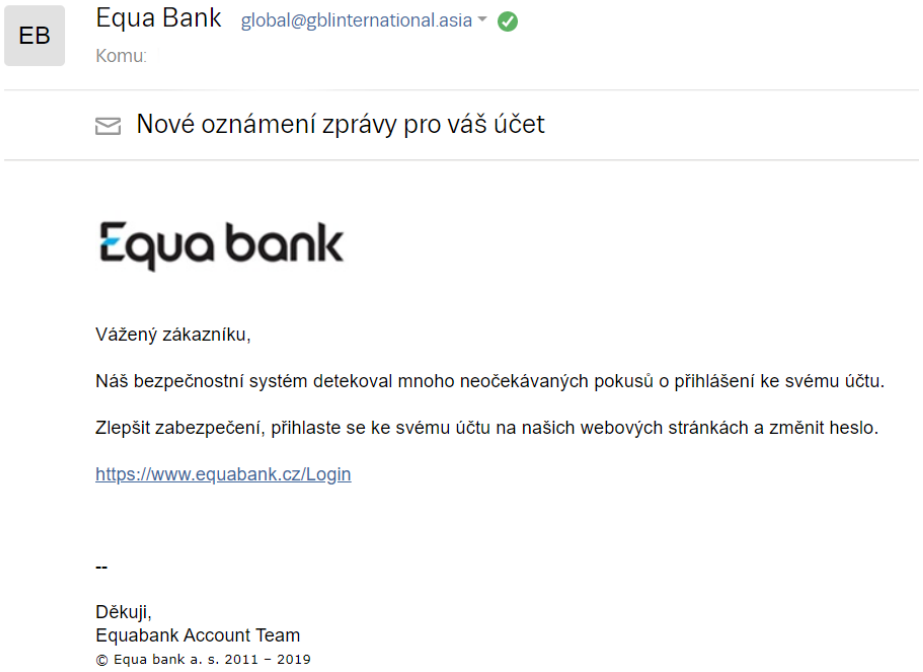
Phishingový útok není žádnou novinkou, první záznamy jsou z poloviny 90. let minulého století. Masově se tento útok začal rozšiřovat až počátkem tohoto století. [35]

O původu tohoto slova jsou dvě teorie, z nichž jedna tvrdí, že slovo vzniklo undergroundovou úpravou slova fishing – česky rybaření. [35] Jedni z prvních útočníků (resp. hackerů) byli známí jako *phreaks*, což je označení, které se váže k průzkumu experimentování a studiu

telekomunikačních systémů. Písmeno „f“ bylo zaměněno za dvojici písmen „ph“, jakožto spojení vedoucí z propojení pojmů **p**hreak a **h**acker. [36] Druhá teorie předpokládá, že se jedná o zkratku z **p**assword **h**arvesting f**ishing** – česky sběr hesel rybařením. Slovo fishing bylo zřejmě zvoleno z důvodu podobnosti s rybařením. Útočník rozešle e-maily na mnoho náhodných adres (jako když rybáři hodí své sítě do vody) a čeká na to, kdo se nachytá a sdělí mu důvěrné informace. [35]

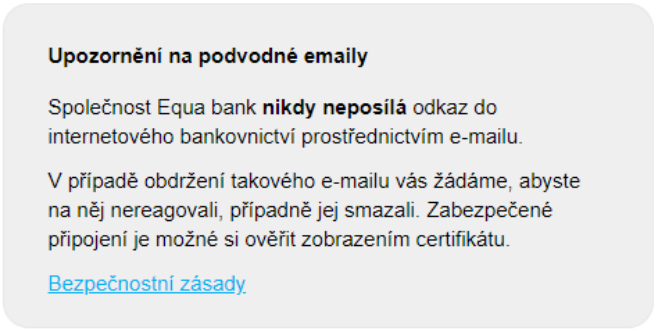
Phishing má několik základních znaků:

- snaží se vyvolat dojem, že byl odeslán organizací, která po svých klientech požaduje zadání důvěrných informací. Toho se snaží docílit grafickou podobou e-mailu nebo třeba zfalšováním adresy odesílatele,
- text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti a další,
- v textu zprávy je odkaz, který na první pohled vypadá, že směřuje na stránky organizace. Při bližším zkoumání uživatel zjistí, že ve skutečnosti odkazuje na podvodné webové stránky (viz kapitola 3.4 Podvodné webové stránky), které mohou vypadat téměř identicky s oficiálními stránkami. [35]



Obrázek 1 – Phishingový e-mail [Zdroj: vlastní]

Výše uvedené znaky jsou pro phishingový útok často využívány, ale není možné určit jednotný postup, jelikož každý útočník má svou vlastní taktiku a následuje vlastní postupy. [35]



Obrázek 2 – Equa bank upozornění pro zákazníky [75]

Útočník se nejčastěji snaží získat údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům. Nemusí se jednat pouze o bankovní účty, ale jde o jakékoliv účty, zejména organizací, kde může docházet k manipulaci s penězi nebo může útočník jakýmkoliv způsobem zneužít služby. Příkladem mohou být PayPal, eBay, Skype, Google a Facebook. [35]

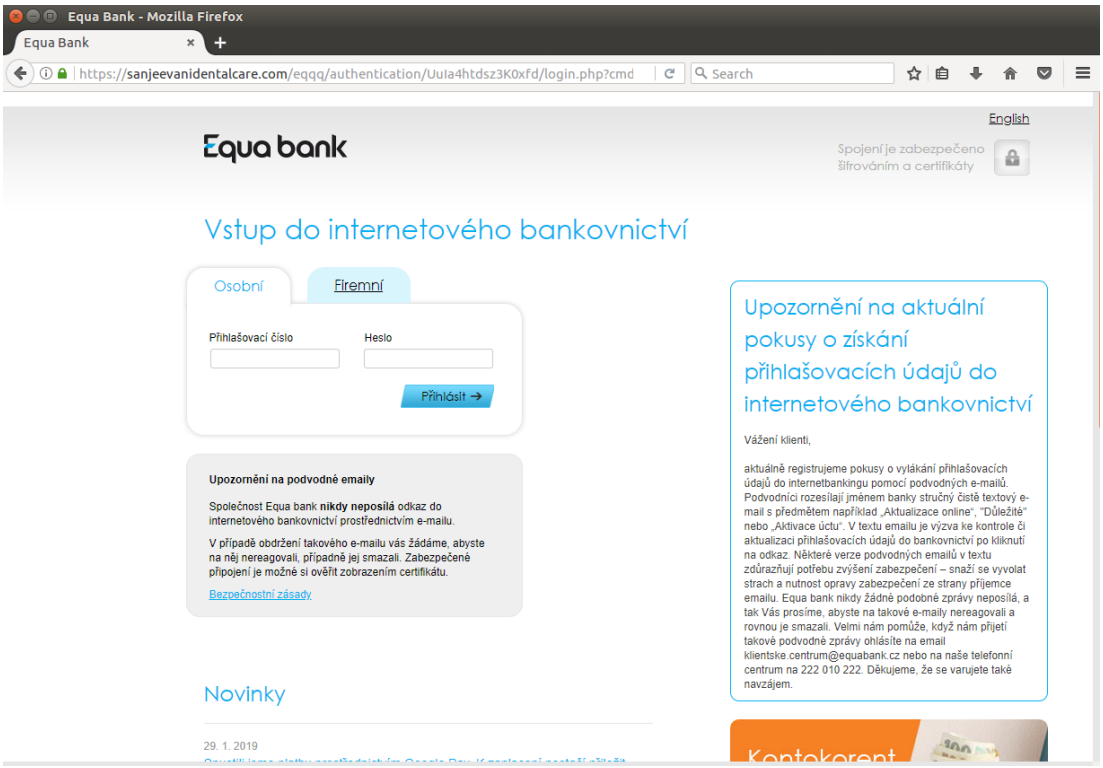
V reálném světě bychom mohli phishing provádět různými způsoby. Ve virtuálním světě je možné během krátkého času a s minimální námahou rozeslat podvodné zprávy velkému počtu potenciálních obětí. [2, s. 246]

Pharming

Jedná se o nebezpečnější a sofistikovanější formu phishingu. Tento útok je veden na DNS server (Domain Name Server), na kterém dochází k předkladu doménového jména na IP adresu. Ve chvíli, kdy uživatel zadá jméno webové stránky do prohlížeče, dojde k přesměrování na podvrženou IP adresu, nikoliv na IP adresu originálního serveru. Tento typ útoku je možné provádět bez jakékoliv přítomnosti malware v počítači.

Útočník naopak použije k napadení počítače malware zejména v případě, kdy lze předpokládat menší míru zabezpečení. Tento malware změní soubor hostitele s cílem odklonit a přesměrovat uživatele na falešnou webovou stránku.

Webové stránky se velice podobají originálním stránkám, často jsou zcela k nerozeznání. Útočník získá přihlašovací údaje ve chvíli, kdy se s nimi uživatel autentizuje na podvržených webových stránkách. Tento typ útoku je realizován zejména na stránkách internetového bankovnictví. [2, s. 263]



Obrázek 3 – Podvodná stránka Equa bank [Zdroj: vlastní]

Spearing

Spearing nebo spear phishing (anglicky *spear* – oštěp) je forma phishingového útoku, ve kterém se na rozdíl od nahodilého phishingu jedná o přesně cílený útok. [69] Cílem útoku bývá konkrétní organizace, skupina nebo jedinec. Útočník usiluje o získání konkrétních dat nebo informací. [2, s. 264]

Existuje speciální případ, ve kterém útočník cílí svůj útok na nejvyšší management a jiné vysoké cíle z hlediska byznysu. Tento typ útoku se označuje jako whaling (anglicky *whale* – velryba). [37]

Vishing

Pojem vishing představuje telefonický phishing (anglicky *voice phishing*). V tomto případě útočník používá techniky sociálního inženýrství a snaží se vylákat citlivé informace od uživatele. Útočník se záměrně představuje pod falešnou identitou, například jako zástupce skutečných bank či jiných institucí. Během hovoru může útočník zjistit osobní a citlivá data oběti. [2, s. 265]

Smishing

Smishing je založen na podobném principu jako vishing, ale k získání informací jsou používány SMS zprávy. Prostřednictvím této metody se útočník snaží uživatele přimět zaplatit částku, nebo navštívit webovou stránku. Na webové stránce se využívá zranitelnosti počítačového systému, na jejímž základě dochází k instalaci malware, nebo k vyzvání uživatele k zadání citlivých údajů. [2, s. 266] [38]

3.4 Podvodné webové stránky

Uživatel se s podvodnými stránkami může setkat zejména prostřednictvím navštívení odkazu z phishingového útoku, během kterého mylně předpokládá, že se nachází na oficiální stránce organizace (viz obrázek 3). Dále se na internetu uživatel může setkat s webovými stránkami, které prezentují výhru pro uživatele nebo nabízejí zboží za velmi výhodné ceny. V případě podvodných stránek se využívá sociálního inženýrství spolu s důvěřivostí a neopatrností uživatelů. [2, s. 266]

Takovéto stránky mohou například sloužit k instalaci virů nebo trojských koní do uživatelova počítače. [39] Útočník se buďto zaměřuje na vylákání citlivých osobních údajů, nebo přímo požaduje po uživateli určité finanční prostředky. Uživatel zadává své citlivé údaje dobrovolně, jelikož tyto údaje útočník po uživateli požaduje zadat pro přihlášení, dokončení registrace, doručení výhry nebo zboží. Získané údaje následně útočník může využít například pro přístup k dalším službám. [2, s. 266] [39]

3.5 Sniffing

Pojem sniffing označuje metodu nelegálního odposlechu dat procházejících počítačovou sítí při komunikaci mezi poskytovanou službou a počítačovým systémem prostřednictvím tzv. snifferu. [2, s. 294] Sniffer neboli analyzátor paketů je počítačový program, pomocí kterého je možné zachytávat a zaznamenávat komunikaci v počítačové síti. [40]

Sniffing je možné také označit jako monitoring provozu sítě. V případě, že správce monitoruje síť, nejedná se o nelegální činnost, jelikož tím udržuje a spravuje počítačovou síť. O nelegální činnost se jedná v tom případě, že osoba provádí tuto činnost bez souhlasu a vědomí uživatele. Z dat zachycených během monitoringu sítě je útočník schopen zjistit citlivé informace. [2, s. 294]

3.6 Prolamování hesel

Jde o proces, během kterého útočník získává hesla k počítačovému systému. K prolamování hesel je možné použít různé postupy, mezi které patří:

- hádání hesel na základě určitých znalostí o uživateli – tyto informace útočník může získat například: ze sociálních sítí, digitální stopy nebo různých diskuzních fór, na které uživatel přispívá. Tyto informace může útočník získat také díky využití sociálního inženýrství, [2, s. 274]
- slovníkový útok, během kterého útočník zadává hesla ze slovníku, seznam slov uživatelova mateřského jazyka, popřípadě kombinací těchto slov, [70]
- zadávání nejčastěji používaných hesel. Mezi nejčastěji používaná hesla patří 123456, 123456789, qwerty, password, 111111. Tato hesla útočník prolomí téměř ihned, [42]
- hádání hesel hrubou silou (anglicky *brute force*). Útočník zkouší všechny kombinace hesel z dané abecedy (použité znaky a symboly). Pokud útočník zná název účtu (přihlašovací jméno) a maximální délku hesla, vždy nalezne správnou kombinaci. Tento postup ale bývá často velice časově náročný,
- vyžádání hesla od administrátora, během kterého se útočník vydává za oprávněného uživatele, předstírá, že heslo zapomněl a snaží se heslo obnovit,
- odchytávání hesel na základě nešifrované, nebo nedostatečně šifrované síťové komunikace mezi počítačovým systémem a uživatelem,
- hledání hesel v souborech dat uložených systémem – cookie soubory. [2, s. 274 – 276]

4 Možnosti zvýšení zabezpečení

Na zabezpečení počítačových systémů se v dnešní době klade větší důraz než před pár lety. Zvýšit zabezpečení svých virtuálních účtů může uživatel hned několika způsoby. Názory na sílu zabezpečení jednotlivými způsoby se velice často liší, proto bych se na některé možnosti chtěla zaměřit v rámci praktické části.

4.1 Heslová politika

Jedná se o pravidla pro hesla, která se doporučují, nařizují nebo vyžadují. Heslová politika zahrnuje zejména požadavky na minimální sílu hesla. Heslo se označuje za silné nebo slabé podle toho, jak obtížné je heslo uhádnout. Útočník může různými způsoby dosáhnout prolomení hesla (viz kapitola 3.6 Prolamování hesel). [43]

Odolnost neboli síla závisí na délce hesla – čím je heslo delší, tím více narůstá počet možných kombinací, tento nárůst je exponenciální. Na sílu hesla mají vliv také použité znaky, které jsou pro dané heslo zvoleny. Uživatel si vybírá ze znaků malých a velkých písmen, číslic a symbolů (tzv. speciálních znaků). [41] Bezpečnostní experti se podle webu Infosec Resources shodují, že použití malých a velkých písmen, je základem pro zvýšení síly hesla. [44]

Útočníci si schraňují databázi odcizených a prolomených hesel, ze kterých jsou schopni zjistit nejčastější hesla a způsoby jejich tvoření. [43] Nejodolnější vůči uhodnutí jsou hesla tvořená náhodně strojově generovanou posloupností znaků, která mají nejvyšší míru entropie. Jejich nevýhodou je, že jsou těžko zapamatovatelná a náchylnější k chybám a překlepům při jejich vyplňování uživatelem. [41]

Vytvořené heslo podle průzkumu, který prováděl Avast na přelomu roku 2018/2019, často obsahuje osobní údaje a informace, které lze snadno dohledat na profilech na sociálních sítích, čímž ulehčí útočníkovi práci s odcizením jejich účtu. Nejčastěji se v heslech objevuje jméno uživatele nebo jméno člena rodiny, jméno domácího mazlíčka nebo datum vlastních narozenin. [45]

Podle doporučení Avastu je při vytváření hesel důležité si pamatovat následující pravidla: Kdykoliv je to možné, měla by hesla obsahovat alespoň 16 znaků, v ideálním případě by měla obsahovat čísla a speciální znaky, jejich text by neměl souviset s vámi ani se službou, do níž chrání přístup. [46]

S minimálním počtem 12 a doporučeným počtem 16 znaků se s Avastem shodují také další weby na internetu. [45] Pokyny pro digitální identitu NIST, SP 800-63B Digital Identity Guidelines, obsahují informaci, že v případě, kdy si uživatel vytváří heslo sám, mělo by být minimálně 8 znaků dlouhé. Uživatelé by měli mít možnost vytvářet hesla tak dlouhá, jak chtějí, ale zároveň by délka měla být v rozumných mezích (udává se povolit uživateli zadat až 64 znaků, někdy i více). [47]

Některé weby nebo aplikace vyžadují změnu hesla každých 90 dní. Podle webu SpyCloud je pravděpodobné, že během roku 2020 bezpečnostní experti začnou toto nastavení zpochybňovat. V případě, že je uživatel nucen si každých 90 dní heslo změnit, útočníci mohou po uplynutí tří měsíců stále dokola zkoušet vkládat hesla z databáze prolomených hesel. Tímto způsobem je hodně pravděpodobné, že dříve nebo později se k účtu útočník dostane. [48]

Stejné heslo na více účtech

Přesně tak, jako je snadné pro uživatele si zapamatovat a používat pouze jedno heslo na více účtech, je snadné pro útočníka toto zjištěné heslo zkusit použít na několik z nich. [49] Podle průzkumu Avastu používá téměř polovina Čechů (přesněji 45 %) stejné heslo pro více účtů, čímž vystavují své účty nebezpečí napadení. Téměř všichni z těchto respondentů si jsou vědomi toho, že je toto jednání rizikové. [46] Webová stránka The Star Online udává dokonce informaci, že šest osob z deseti používá stejné heslo na více účtech. [50]

Podle zprávy z webu Yubico z roku 2019, týkající se stavu zabezpečení hesel a ověřování, používá 51 % osob pět hesel v průměru napříč pracovními a osobními účty. [51] Nejen na základě těchto průzkumů, ale také podle doporučení dalších webů, je velice důležité, aby uživatel nepoužíval stejné heslo na dvou a více účtech.

4.2 Správce hesel

Správce hesel (anglicky *password manager*) je samostatná aplikace, rozšíření webového prohlížeče, nebo správce zabudovaný přímo v operačním systému, který umožňuje ukládat stovky silných a jedinečných hesel. Uživatel si musí zapamatovat pouze jedno hlavní heslo, po jehož zadání se otevírá šifrovaná databáze hesel. [73] Největší rozdíl mezi aplikacemi bývá v uložení hesel. Některé aplikace ukládají všechna hesla lokálně na počítač, další je ukládají na servery, jiné používají obě tyto varianty. Hlavní heslo by mělo být unikátní, silné a uživatel by si jej, tak jako ostatní hesla, neměl nikde zaznamenávat. [55]

Existuje mnoho webových stránek a aplikací, mezi kterými si uživatel může správce hesel vybírat. Příkladem může být český Sticky Password, dále pak LastPass nebo 1Password. [56]

4.3 Vícefaktorová autentizace

Informační systém potřebuje znát identitu uživatele, který k němu přistupuje. Je potřeba zajistit úroveň jistoty, která potvrzuje, že přistupující uživatel je tím, za koho se vydává. Dříve stačilo přihlášení jménem a heslem, ale následně, zejména s nástupem elektronických bankovních aplikací, bylo třeba úroveň jistoty zvýšit. [18]

Vícefaktorová autentizace (anglicky *multi-factor authentication – MFA*) je metoda ochrany přístupu k prostředku (např. webu, informačnímu systému), založená na kombinaci více zabezpečovacích faktorů, zmíněných v kapitole 1.2.1 Identifikace osoby. [18] Jakékoliv heslo může být kompromitováno, ale útočník se do dané služby nepřihlásí, pokud nemá přístup k zařízení nebo účtu zajišťujícímu druhý kanál. V dnešní době se nejčastěji jedná o kombinaci jména a hesla společně s jednorázovým kódem odeslaným na telefonní číslo uživatele – tento postup se často označuje jako dvoufázové ověření. [52]

Znalost

Jedná se o cokoliv, na co je uživatel schopen si vzpomenout. Typickým příkladem je jméno a heslo (PIN), dále například nakreslení znaku/gesta nebo osobní otázky. Do této skupiny patří také vygenerované jednorázové kódy.

Vlastnictví

Vlastnictví zahrnuje zjednodušeně to, co lze nosit v kapse nebo peněžence. Jedná se o hardwarové tokeny (RSA SecurID, Vasco DIGIPASS), platební karty, mobilní telefony a SIM karty (ověření zpětným voláním nebo SMS zprávou s jednorázovým kódem).

Biometrie

Biometrie zahrnuje charakteristiky svého nositele. Jedná se o otisk prstu, sken očnice, rozpoznávání obličeje, přihlášení hlasem. Speciální kategorií je charakteristika „jsem člověk“, která se využívá například v CAPTCHA mechanismu – obecně tam, kde řešení je jednoduché, ale špatně algoritmizovatelné. [18]

4.4 Další možnosti

4.4.1 Zabezpečené připojení

HTTP (anglicky *HyperText Transfer Protocol*) je způsob pro přenos webových stránek. HTTP spojení nezaručuje, že obsah, který uživatel uvidí v prohlížeči, odpovídá tomu obsahu, který vytvořila příslušná webová stránka. Během cesty od webového serveru dané stránky k prohlížeči uživatele je možné data číst nebo upravit výsledek, aniž by to návštěvník zaregistroval. [53]

HTTPS (anglicky *HyperText Transfer Protocol Secure*) je šifrovaná varianta internetového protokolu HTTP. Protokol HTTPS umožňuje zabezpečený přístup k webovému serveru tím, že veškerou přenášenou komunikaci šifruje algoritmem SSL nebo TLS. Šifrování komunikace je důležité při přenášení citlivých informací (např. číslo kreditní karty, heslo k účtu). Uživatel by měl kontrolovat zabezpečené připojení nejen na stránkách elektronického bankovnictví. [71]

Pro zvýšení bezpečnosti vyžaduje prohlížeč komunikující přes HTTPS tzv. certifikát. Certifikát musí být podepsaný certifikační autoritou, což zaručuje pravost certifikátu. V případě, že by certifikát nebyl platný, zobrazí se uživateli v prohlížeči oznámení ve smyslu, že nelze ověřit certifikát. [54]

4.4.2 Propojené účty

Uživatel má možnost propojit si službu třetí strany (např. sociální síť, aplikaci) s účtem, např. na Google nebo Facebooku. Toto propojení následně uživateli může umožnit zpřístupnění dalších funkcí, nebo uživateli poskytuje rychlejší a snadnější přihlášení do dané služby, jelikož se na této stránce již nemusí registrovat. [57]

4.4.3 Antivirový systém

Antivirový systém, zkráceně antivirus, je program, který chrání počítač před napadením od řady různých druhů škodlivých programů. Uživatel často navštěvuje různé odkazy, na kterých se může nacházet škodlivý program, tudíž může dojít ke snadnému napadení nechráněného počítače. Někdy se může objevit malware, který napadá počítač přímo přes chybu operačního systému nebo prohlížeče. Po nainstalování antiviru a navštívení určité stránky může být

uživatel upozorněn, že stránka, na kterou chce přistoupit, je nebezpečná. Poté je na zvážení uživatele, zda této webové stránce věří či nikoli. [58]

4.4.4 Aktualizace

Pro bezpečnost uživatelských účtů je důležitá také aktualizace jednotlivých zařízení a aplikací. V případě, kdy je v operačním systému nebo v aplikaci bezpečnostní chyba, jsou zařízení a účty náchylnější k napadení útočníkem. Chyby mohou mít vliv nejen na bezpečnost, ale také na funkčnost zařízení. Po zjištění chyby vydávají výrobci aktualizace s opravami, uživatel je upozorněn na možnost aktualizace a následně se čeká na schválení stažení této aktualizace. V některých systémech a aplikacích je možné nastavit automatickou aktualizaci. [59]

4.4.5 Uzamykání účtu

Některé aplikace mají implementovanou politiku účtů, která je schopna dočasně nebo trvale uzamknout účet, pokud se uživatel opakovaně chybně přihlašuje během krátkého časového úseku. Uživatel následně musí čekat předem stanovený čas, než se mu účet znovu zpřístupní pro další přihlašování, nebo se účet může trvale uzamknout z důvodu podezření na bezpečnostní událost. Pro další přístup uživatel, v případě trvalého uzamknutí účtu, potřebuje pomoc organizace nebo administrátora pro odblokování účtu. [60] [61]

Přítomnost tohoto nastavení je podle pokynů pro digitální identitu NIST, SP 800-63B Digital Identity Guidelines, dobré znát, protože následně podle toho může uživatel upravovat délku hesla. [47]

5 Následky krádeže identity

Následky krádeže identity mohou být závislé na tom, zda útočník odcizil identitu uživatele nebo firmy. V případě, že byla odcizena identita uživatele, může útočník zneužít kontakty zejména k dalším útokům, falešně komunikovat s přáteli a požadovat po nich finanční prostředky, předávat lživé informace nebo prostřednictvím účtu pomlouvat a hanit jiné osoby a další.

Pokud se jedná o odcizení účtu firmy, firemních skupin nebo firemních produktů, může útočník cílit na finanční prostředky nebo na poškození reputace firmy, což může vést až k tak velkým škodám, že dojde ke krachu firmy.

Schneier ve vztahu k datům uvedl, že s nimi útočník může dělat tři základní věci: krást je (narušení důvěrnosti), měnit je (narušení celistvosti) nebo bránit vlastníkům v přístupu k nim (narušení dostupnosti). [2, s. 185] [62]

6 Legislativa

Často se kyberkriminalita považuje za nový druh kriminality, nicméně se na značnou část využívají a přenášejí notoricky známé druhy protiprávního jednání. Příkladem může být podvod, porušování autorských práv, šikana nebo krádež. Existují ale taktéž určité typy jednání, u kterých označení za trestný čin může být obtížnější, nebo dokonce nemožné, jelikož se může jednat pouze o nemorální či nechtěné jednání.

Virtuální svět se pro mnoho z nás stává čím dále tím významnějším. Mnohdy to vypadá, že uživatel přestal přemýšlet o možných rizicích a hrozbách, na které by v sociálním světě přišel téměř automaticky a zachoval by se zcela jinak. Současně zdánlivě slušní lidé v reálném světě se ve virtuálním prostředí projevují bez jakýchkoliv morálních nebo legálních zábran. Například osoba, která by v reálném světě nic neukradla, ve světě virtuálním nemá problém krást nebo porušovat práva chráněná zákonem. Tato skutečnost by mohla být způsobena zejména zdánlivě nekonečnými možnostmi „nových technologií“. [2, s. 181]

Marc Goodman v roce 2012 uvedl, že „*schopnost jedince ovlivnit masy, právě díky těmto technologiím, roste exponenciálně. Exponenciálně roste jak v oblasti ‚dobrého, tak zlého účelu‘*“. Tento růst názorně prezentoval na vývoji zločinu loupeže, kdy v minulosti docházelo k loupežnému přepadení jednotlivci nebo malými skupinami. *„K zásadní „inovaci“ došlo v okamžiku loupežného přepadení celého vlaku, ve kterém cestovalo 200 lidí.“* Internet umožňuje výraznější rozsah útoku jedné osoby na více uživatelů, kdy v případě Sony Playstation bylo přibližně 100 milionů poškozených osob. *„Kdy v historii lidstva mohl jedinec okrást 100 milionů lidí? Ale nejde jen o krádeže…“*. [2, s. 182]

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn či zabit.	Bez rizika fyzické újmy
Zisk	Průměrně 3–5 tisíc USD.	Průměrně 50–500 tisíc USD.
Pravděpodobnost dopadení	Dopadeno 50–60 % útočníků.	Dopadeno cca 10 % útočníků.
Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených útočníků.	Z dopadených útočníků dojde k soudnímu projednávání pouze u 15 % útočníků a z nich je odsouzeno jen 50 %.
Trest	Průměrně 5–6 let, pokud pachatel při loupeži nikoho nezranil.	Průměrně 2–4 roky.

Obrázek 4 – Porovnání loupeže a kybernetického útoku [2, s. 182]

Z pohledu práva je krádež identity považována za dvoustupňový trestný čin. Nejprve musí útočník získat cizí virtuální identitu a následně ji zneužije (viz kapitola 3 Krádež identity).

6.1 GDPR

Zkratka GDPR (General Data Protection Regulation) označuje obecné nařízení Evropské unie (EU) 2016/679 na ochranu osobních údajů. Toto nařízení je vytvořeno s cílem posílit a sjednotit ochranu dat pro všechny občany EU. Cílem GDPR je chránit a hájit práva občanů EU proti neoprávněnému zacházení s jejich daty, včetně osobních údajů. Toto nařízení je v celé EU jednotně účinné od 25. května 2018. [63]

GDPR v České republice nahradilo směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a související zákon č. 101/2000 Sb., o ochraně osobních údajů. [65] Nařízení věnuje speciální pozornost zpracování zvláštních kategorií osobních údajů, kterými jsou citlivé osobní údaje (viz kapitola 1.5 Údaje). [64]

6.2 Zákon 40/2009

Zákon 40/2009 Sb., trestní zákoník. *„Čin je trestný, jen pokud jeho trestnost byla zákonem stanovena dříve, než byl spáchán.“* [66]

§ 182 Porušení tajemství dopravovaných zpráv

Útočník by mohl být v případě sniffingu (viz kapitola 3.5 Sniffing) odsouzen podle § 182 zákona č. 40/2009 Sb., trestního zákoníku. [2, s. 294] V tomto případě dochází k nelegálnímu odposlechu a záznamu telekomunikačního provozu. [66 §182] Současně dochází k zásahu do Listiny základních lidských práv a svobod, která ve čl. 13 zajišťuje každému tajemství listovních a jiných písemností a záznamů. [67]

Tento útok je možné kvalifikovat podle § 182 odst. 1, nebo v případě, že by útočník odchycené informace zneužil, mohl by být čin kvalifikován podle § 182 odst. 2, ve kterém je navíc stanoveno, že takového tajemství (resp. informace) zneužije. Pachateli hrozí trest odnětí svobody až na dvě léta nebo zákaz činnosti. Vždy je třeba prokázat úmysl útočníka. [2, s. 294] [28]

§ 209 Podvod

§ 209 trestního zákoníku v prvním odstavci stanovuje, že: *„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“*, přičemž podle šestého odstavce je trestná také příprava. [66 §209]

Tento paragraf by bylo možné použít na útoky jako je phishing, pharming nebo podvodné stránky. Podvod je dokonán obohacením se. Vytvoření repliky webové stránky a získání přihlašovacích jmen by bylo možné kvalifikovat podle § 209 odst. 6 jako přípravu či pokus o podvod § 209. [2, s. 269] [66 §209]

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

V prvním odstavci § 230 trestního zákoníku je vymezeno, že *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“*. [66 § 230]

Pokud útočník prolomí byť jednoduché heslo, už se jedná o překonání bezpečnostního opatření. Nemusí dojít ke krádeži dat, v tomto případě zcela postačí, že si útočník zajistil přístup k cizímu počítači, např. pomocí malware, který infikoval počítač. Přesněji § 230 odst. 3 by byl použit v případě, že by se prokázal úmysl útočníka s cílem získat sobě nebo někomu jinému neoprávněný prospěch. [2, s. 263 – 269]

V případě podvodných stránek by se § 230 trestního zákoníku mohl kvalifikovat ve chvíli, kdy by se útočník pokusil na základě získaných přístupových údajů o neoprávněný přístup do jiného účtu uživatele. [28] [66 §230]

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

V případě § 231 trestního zákoníku je třeba, aby soud prokázal úmysl útočníka spáchat trestný čin porušení dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2, kdy útočník nakládá se zařízením nebo jeho částí (softwarem, databází hesel), která umožňuje

spáchat jeden z výše uvedených trestných činů. V případě prokázání úmyslu bude útočník potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.

Odnětí svobody až na tři léta, zákaz činnosti nebo propadnutí věci hrozí v případě, že spáchá trestný čin jako člen organizované skupiny, nebo pokud získá takovým činem pro sebe nebo pro někoho jiného značný prospěch (> 500 000 Kč). Odnětí svobody na šest měsíců až pět let hrozí pachateli, pokud pro sebe nebo pro někoho jiného získá činem prospěch velkého rozsahu (> 5 000 000 Kč). [66 §231]

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

Tento paragraf se týká odpovědnosti konkrétních osob, které nakládají s důležitými údaji a způsobí ztrátu nebo změnu počítačových dat. Kvalifikovat tento trestný čin může soud už v případě, pokud se jedná o hrubou nedbalost vyplývající ze zaměstnání či funkce. V případě, že vlivem hrubé nedbalosti vznikne značná škoda (> 500 000 Kč), může být dotyčný potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci. Pokud vznikne škoda velkého rozsahu (> 5 000 000 Kč), může být pachatel potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci. [28] [66 §232]

7 Statistická analýza

Součástí praktické části bakalářské práce je vytvoření sociálního experimentu, na jehož základě bude zjištěna míra důvěřivosti cílové skupiny osob při otevírání neznámých zdrojů pod záminkou simulace důvěryhodného prostředí. Podle výsledků a pozorování během sociálního experimentu bude následně zpracována metodika předcházení krádeže virtuální identity.

7.1 Zpracování

Vytvořila jsem dotazník pro cílovou skupinu osob – jedná se o osoby, které mám v ‚přátelích' na sociální síti Facebook, případně o přátele mých přátel. V rámci experimentu jsem vytvořila důvěryhodné prostředí (dotazník), ale toto prostředí jsem se pokusila schovat za nedůvěryhodné prostředí. Odkaz pro vyplnění dotazníku jsem „schovala" za zkrácenou URL, aby potencionálním respondentům nebylo ihned jasné, že se jedná o důvěryhodné a zabezpečené prostředí. Text odesílané zprávy byl navrhnut tak, aby lákal uživatele k přístupu na daný odkaz.

7.1.1 Počet přístupů

Webová stránka Bitly (https://bitly.com/) umožňuje zkrácení odkazu a současně také počítání počtu kliknutí na odkaz pro danou webovou stránku. Tuto funkci jsem využila k tomu, abych zjistila, kolikrát bylo na odkaz s dotazníkem přistoupeno. Web poskytuje v reálném čase statistiku počtu přístupů na vytvořený odkaz. Dále umožňuje vlastní nastavení části odkazu. Zde jsem pro zajímavost zvolila vlastní nastavení a čekala, zda slovo „dotazník" v odkazu někdo uvidí, nikdo takový se nenašel. Použitý odkaz: http://bit.ly/d0t4zN1k.

Pro zjištění počtu přístupů jsem navíc použila stránku Blasze (http://blasze.com/), přes kterou jsem byla schopna zjišťovat IP adresu uživatele. Tento krok navíc jsem použila z důvodu, abych byla schopna určit počet unikátních IP adres, ze kterých uživatelé přistoupili. Jeden uživatel může na odkaz kliknout vícekrát, každé kliknutí se započítá do statistiky. Pokud bych neznala IP adresu, nebyla bych schopna určit, zda stejný počet uživatelů přistoupil a současně vyplnil dotazník. Použitý odkaz: http://blasze.tk/K6UJ57.

Odkazy jsem před odesláním zprávy testovala na více zařízeních, ale nepodařilo se mi vytvořit problémovou situaci, která nastala až při odeslání přátelům celkem u 11 respondentů. Těmto respondentům jsem odeslala náhradní odkaz, prostřednictvím kterého přistupovali už pouze na dotazník, nikoliv přesměrováním přes web pro trackování IP adres.

Skript pro výpis unikátních IP adres

Web Blasze nevypisuje uživateli žádnou statistiku, rozhodla jsem se proto pro vytvoření jednoduchého skriptu (viz příloha 2 – Skript), abych nemusela počítat jednotlivé IP adresy a současně mezi adresami hledat, které z nich jsou unikátní a které duplicitní.

Zobrazila jsem si zdrojový kód webové stránky Blasze a uložila jej do souboru vstup.txt. Tento soubor je ve skriptu následně načítán a jsou zpracována data, která se v něm nacházejí. Pro zachování ochrany osobních údajů tento soubor není přiložen jako součást práce. Zjednodušila jsem si práci tím, že v tabulce se IP adresa nachází vždy ve druhém sloupci.

Skript vypisuje celkový počet přístupů a počet unikátních IP adres. Jelikož se jedná o skript, ze kterého data potřebuji získat pouze jednou, nechala jsem si vypsat počet adres pouze do konzole.

Obrázek 5 – Výstup do konzole [Zdroj: vlastní]

Zde by mohl nastat problém, pokud by více osob přistoupilo v rámci jedné IP adresy (např. v rámci domácnosti, veřejné sítě). Počet problémů a počet unikátních IP adres odpovídá počtu vyplněných dotazníků, proto jsem se touto možností dále nezabývala.

7.1.2 Dotazník

Pro účely sběru dat jsem využila aplikaci Google Forms. Formuláře od Google umožňují rozsáhlé uživatelské nastavení a vyplněné dotazníky jsou viditelné ihned. Současně je možné data z dotazníku vyexportovat a dále s nimi pracovat. Dotazník v plném znění viz příloha 1 – Dotazník.

7.1.3 Zpráva

Odesílaná zpráva měla v uživateli vzbouzet zvědavost, měla být jednoduchá a ideálně měla vypadat jako zpráva, kterou by mohl útočník použít. Cílové skupině osob byl odeslán text ve znění:

Ahoj, koukni na tuto stránku http://bit.ly/d0t4zN1k určitě tě to bude také zajímat! :)

Kdybych tuto zprávu posílala znovu, tak bych místo slova „koukni“ použila „podívej se“. Pokud by útočník používal například překladač, s větší pravděpodobností by jeho přeložená zpráva obsahovala slovo „podívej se“.

7.1.4 Statistika

Z vyplněných dotazníků jsem zjišťovala závislosti mezi získanými informacemi, abych v případě, kdy se mezi některými proměnnými prokáže souvislost, mohla na základě těchto informací vytvořit metodiku.

Pro získání této informace byl použit test nezávislosti v kontingenční tabulce, tzv. Pearsonův chí-kvadrát test. Nulovou hypotézou v tomto testu je tvrzení, že náhodné veličiny X a Y jsou nezávislé. Předpokládejme, že veličina X nabývá I hodnot a veličina Y nabývá J hodnot. [72]

		X					
		x_1	x_2	…	x_i	…	x_I
Y	y_1						
	y_2						
	…						
	y_j				p_{ij}		
	…						
	y_J						

Pravděpodobnost, že nastane případ x_i a současně y_j , označíme p_{ij} a za předpokladu nezávislosti je tato pravděpodobnost rovna součinu pravděpodobností, že nastane případ x_i (označíme p_i) bez ohledu na veličinu Y a že nastane případ y_j (označíme p_j) bez ohledu na veličinu X. Nulovou hypotézu tedy lze přepsat do tvaru $p_{ij} = p_i p_j$. Násobíme-li p_{ij} počtem pozorování, obdržíme četnosti očekávané (anglicky *expected*) za předpokladu nezávislosti obou proměnných, tedy za platnosti nulové hypotézy.

Z experimentu jsme obdrželi sledované (anglicky *observed*) četnosti. Pokud platí nulová hypotéza, jsou obě četnosti totožné.

Vytvoříme novou náhodnou veličinu $S = \sum_{i=1}^{I}\sum_{j=1}^{J}\frac{(observed_{ij}-expected_{ij})^2}{expected_{ij}}$.

Veličina *S* má přibližně χ^2 rozdělení s počtem stupňů volnosti (*I*-1)(*J*-1). S hodnotou křivky hustoty χ^2 rozdělení je spojena veličina *P* (dosažená hladina významnosti, anglicky *significance level*), $P \in < 0, 1 >$. [72]

Čím vyšší je hodnota χ^2, tím nižší je hodnota *P*. *P* se srovnává s hladinou významnosti testu α (zde rovno 0.05). Pokud je $P < \alpha$, zamítáme nulovou hypotézu na hladině α. Hladina významnosti označuje pravděpodobnost, že jsme se dopustili chyby menší nebo rovné α.

Pokud nelze nulovou hypotézu zamítnout, pak ji nezamítáme, v praxi to interpretujeme jako nezávislost mezi veličinami *X* a *Y*. [74]

7.2 Vyhodnocení

V této podkapitole se zaměřím na samotné vyhodnocení získaných informací a dat v rámci sociálního experimentu.

7.2.1 Počet přístupů

Počtem přístupů je označen počet kliknutí uživatelů na odkaz zaslaný ve zprávě. Z rozdílu v počtu přístupů na web s trackováním (125) a v celkovém počtu přístupů Blasze (73) je možné usuzovat, že dalším lidem se zobrazila chyba webové stránky. Všem, kteří mě kontaktovali s problémem, jsem odeslala nový odkaz, ostatní se nijak nevyjádřili. Tento rozdíl může být také způsoben opakovaným pokusem respondentů zobrazit webovou stránku znovu poté, co se jim poprvé zobrazila chyba.

Bitly statistika

Počet přístupů na web s trackováním	125
Počet přístupů na dotazník (nový odkaz)	15
Celkový počet přístupů Bitly	**140**

Tabulka 1 – Počet přístupů Bitly

Blasze statistika

Počet unikátních IP adres	53
Celkový počet přístupů Blasze	**73**

Tabulka 2 – Počet přístupů Blasze

Mělo by platit, že každý respondent, který přišel na stránku, dotazník vyplnil. Celkový počet problémů se zastavil na čísle 11, počet přístupů s unikátní IP adresou byl 53 a počet vyplněných dotazníků byl 64.

Z reakcí byla nejčastější otázka „co to je“, která se v některých případech lišila slovosledem nebo použitím jiného slova např. „co tam je“. Další nejčastější reakcí byla otázka, zda odkaz „není vir“. V jednom případě došlo k nemožnosti uživatele přistoupit na odkaz s trackováním na základě nastavení bezpečnostní politiky firmy, z jehož počítače se respondent snažil na web přistoupit.

V případě, kdy by byla uvažována situace, že stejný počet osob, jako je počet přístupů na web s trackováním (125 – viz tabulka 1), by chtěl přistoupit na dotazník, tak by se počet dotazů dal vyjádřit zlomkem 1/10. Neboli že každý desátý uživatel se nad zprávou pozastavil a zaslal dotaz, zda se nejedná o spam, nebo zda tento odkaz byl odeslán mou osobou.

Pokud by tato informace byla uvažována podle počtu vyplněných dotazníků, jednalo by se o lepší poměr, jednalo by se o každého pátého uživatele.

Celkem odesláno zpráv	112
Celkový počet přístupů	213
Celkem vyplněno dotazníků	64
Celkem reakcí (dotazů)	12

Tabulka 3 – Celková statistika

Ze získaných dat je možné odvodit, že osoby, které mají dokončené středoškolské vzdělání ukončené maturitou, nebo vysokoškolské, si dávali větší pozor na zprávy než osoby s dokončeným základním vzděláním nebo se střední školou ukončenou výučním listem.

Ve dvou případech z celkového počtu dotazů (12) mě uživatelé kontaktovali na jiném kanále, než na Facebooku. Jeden dotaz mi přišel na Instagram, druhý na soukromý e-mail.

Dokončené vzdělání	**Počet dotazů**	**Vyplněných dotazníků**
Základní škola	0	5
Střední škola ukončena výučním listem	0	11
Střední škola ukončena maturitou	6	33
Vysokoškolské – bakalář	3	9
Vysokoškolské – magistr, inženýr	3	6

Tabulka 4 – Počet dotazů v závislosti na dokončeném vzdělání

7.2.2 Statistika

Ze získaných dat bylo prokázáno několik závislostí, a to závislost krádeže virtuální identity a používání různého hesla, krádeže identity a používání vícefaktorové autentizace, krádeže identity a kontroly zabezpečeného připojení. Krádež virtuální identity byla zjišťována na základě otázky „Byla někdy Vaše osobní data ve virtuálním světě napadena nebo ukradena? (může se jednat o zneužití dat, profilů na sociálních sítích, dalších webových stránkách a účtech)“ z dotazníku.

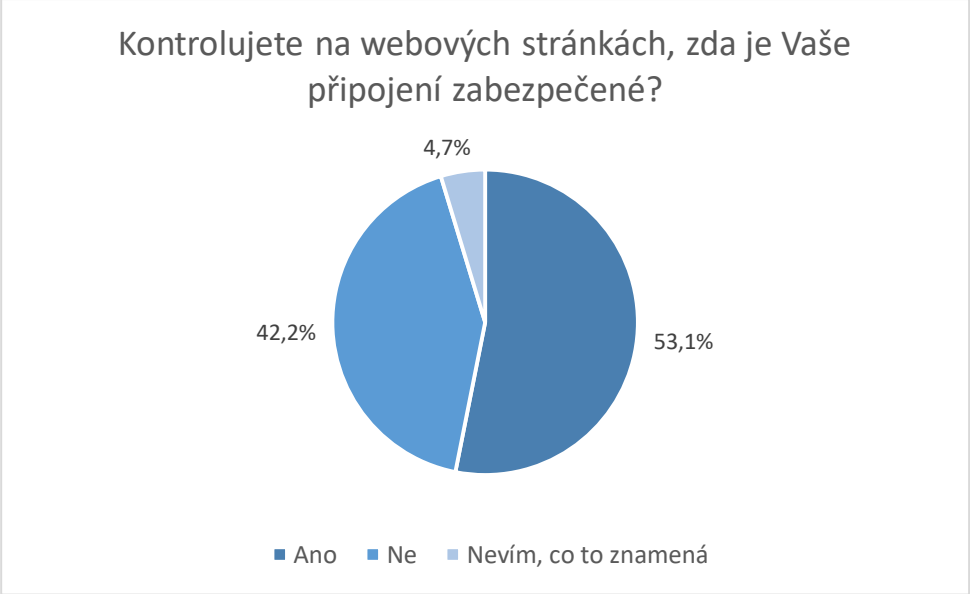
Závislost mezi krádeží identity a věkem ($\chi^2(1) = 0{,}102582, P = 0{,}748753$), vzděláním ($\chi^2(4) = 4{,}94376, P = 0{,}293117$), pohlavím ($\chi^2(1) = 0{,}039385, P = 0{,}842689$), délkou hesla ($\chi^2(15) = 12{,}6885, P = 0{,}626345$), změnou hesla ($\chi^2(5) = 8{,}89350$, $P = 0{,}113388$) nebo složitostí hesla ($\chi^2(9) = 11{,}1251, P = 0{,}267233$) se ze získaných dat neprokázala. Ve všech těchto případech nebyla zamítnuta nulová hypotéza o nezávislosti mezi proměnnými.

Krádež virtuální identity a kontrola zabezpečeného připojení

V případě získaných dat pro proměnné, krádež virtuální identity a kontrola zabezpečeného připojení, vyšla hodnota jen o málo větší než kritická hodnota $\chi^2(2) = 5{,}99, P = 0{,}05$. Hodnoty kontroly zabezpečeného přístupu odpovídají odpovědím respondentů na otázku „Kontrolujete na webových stránkách, zda je Vaše připojení zabezpečené?“. V této otázce byla možnost odpovědí „Ano“, „Ne“ a „Nevím, co to znamená“. Počet stupňů volnosti je spočten podle vzorce jako $df = (2-1)(3-1)$, výsledkem jsou 2 stupně volnosti. Chí-kvadrát test pro tyto dvě proměnné je $\chi^2(2) = 6{,}00937, P = 0{,}049554$.

Pokud by se z odpovědí vypustila možnost „Nevím, co to znamená“, hodnota p-value by vyšla ještě nižší, $\chi^2(1) = 5{,}95076, P = 0{,}014711$, protože tuto možnost zvolily pouze tři osoby.

V tomto případě vyšla závislost proměnné krádeže virtuální identity v závislosti na kontrole zabezpečeného připojení. Očekávalo se méně osob, kterým virtuální identita byla ukradena a zároveň kontrolují zabezpečené připojení. Znamená to tedy, že podle dat respondenti, u kterých byla virtuální identita ukradena, kladou větší důraz na kontrolu zabezpečeného připojení.

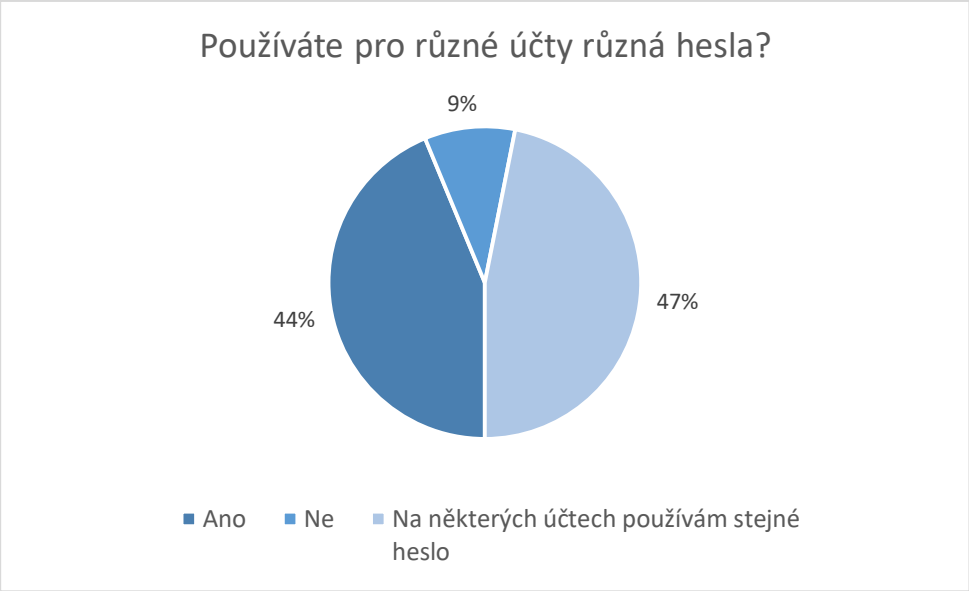


Graf 1 – Kontrola zabezpečeného připojení

Krádež virtuální identity a používání různých hesel pro různé účty

Ze získaných dat pro proměnné krádež virtuální identity a používání různých hesel pro různé účty se podle kritické hodnoty $\chi^2(2) = 5{,}99, P = 0{,}05$ a získané hodnoty $\chi^2(2) = 6{,}24590, P = 0{,}044027$ zamítla nezávislost. V tomto případě se na rozdíl od kontroly zabezpečeného přístupu prokázalo, že v případě, kdy uživatel nepoužívá různá hesla na různých účtech, existuje větší pravděpodobnost, že jeho účet bude odcizen nebo zneužit. Podle očekávaných a získaných hodnot byl rozdíl v počtu uživatelů, kteří používají stejná hesla na více účtech, a jejich virtuální identita jim byla odcizena.

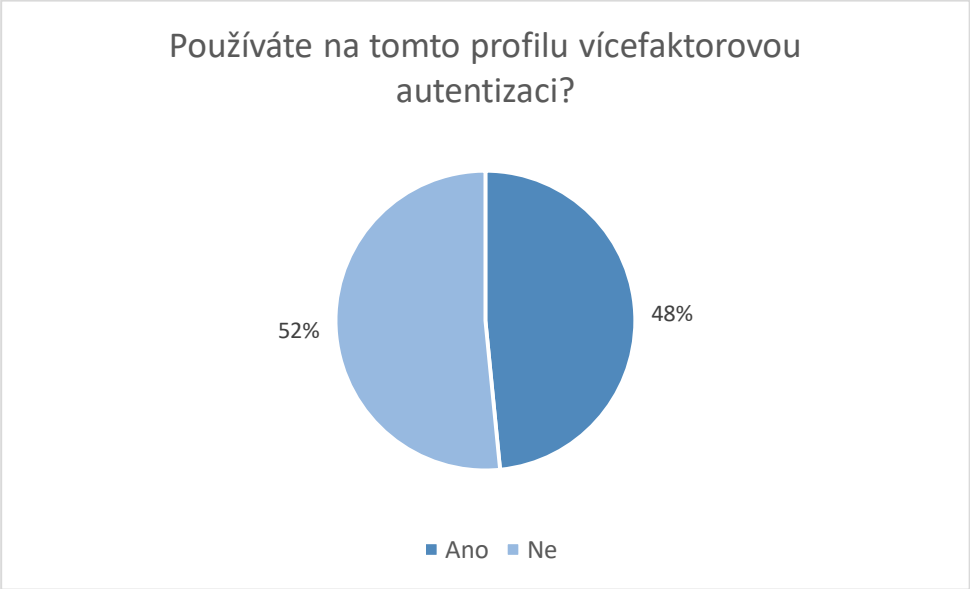
V teoretické části práce v kapitole 4.1 Heslová politika bylo na základě průzkumu Avastu uvedeno, že 45 % Čechů používá stejné heslo na více účtech. Získaná data z dotazníku tuto informaci potvrzují, jelikož respondenti v dotazníku odpovídali téměř v identickém procentuálním rozdělení.



Graf 2 – Používání stejných hesel na více účtech

Krádež virtuální identity a používání vícefaktorové autentizace

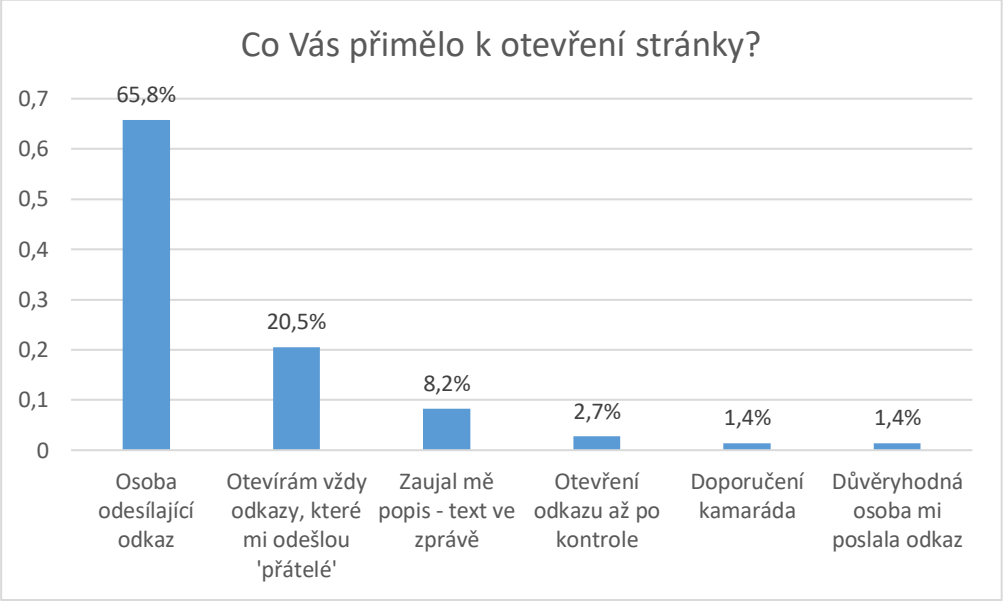
Poslední případ, ve kterém byla zamítnuta nulová hypotéza, je mezi proměnnými krádež virtuální identity a používání vícefaktorové autentizace. V tomto případě je jeden stupeň volnosti, jehož kritická hodnota je $\chi^2(1) = 3{,}84, P = 0{,}05$. Hodnota p-value pro tyto dvě proměnné nabyla nejnižší hodnoty, $\chi^2(1) = 4{,}43824, P = 0{,}035142$. Nulová hypotéza byla zamítnuta, z dat se ukázal rozdíl mezi očekávanými a naměřenými hodnotami. Očekávalo se méně osob, které nepoužívají vícefaktorovou autentizaci a virtuální identita jim byla ukradena. Použití vícefaktorové autentizace pomáhá uživatelům zabezpečit jejich účty.



Graf 3 – Používání vícefaktorové autentizace

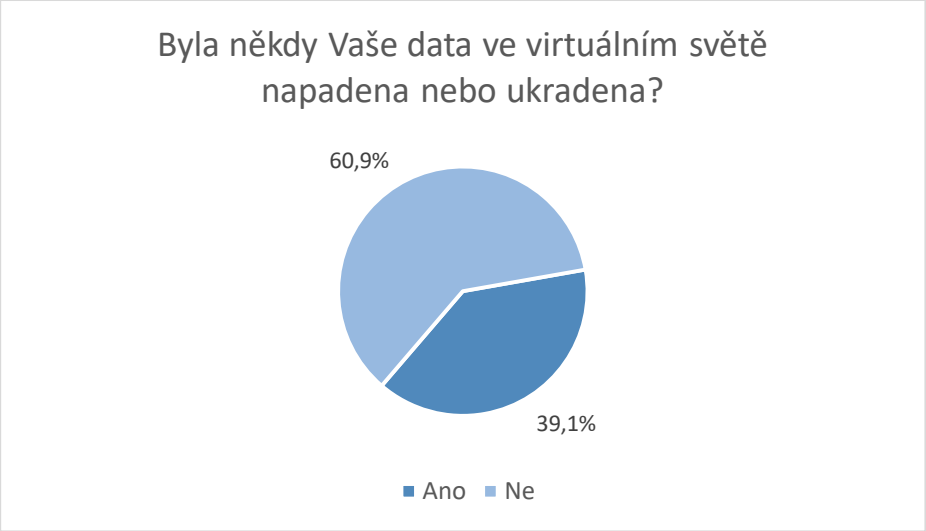
7.2.3 Dotazník

Jak bylo zmíněno v kapitole 3.4 Podvodné webové stránky, využití sociálního inženýrství spolu s důvěřivostí a neopatrností uživatelů v případě podvodných stránek, dalo by se toto tvrzení potvrdit také u respondentů, kterým byl dotazník odeslán. Více než polovina respondentů, přesněji 65,8 %, označila možnost „Osoba odesílající odkaz“ jako odpověď na otázku „Co Vás přimělo k otevření stránky“. V tomto případě by zvolení této odpovědi mohlo souviset jak s důvěřivostí, protože se domnívali, že odkaz jsem odeslala já, tak také s neopatrností, jelikož v mnohých případech jsem s respondenty nebyla již dlouhou dobu v kontaktu.



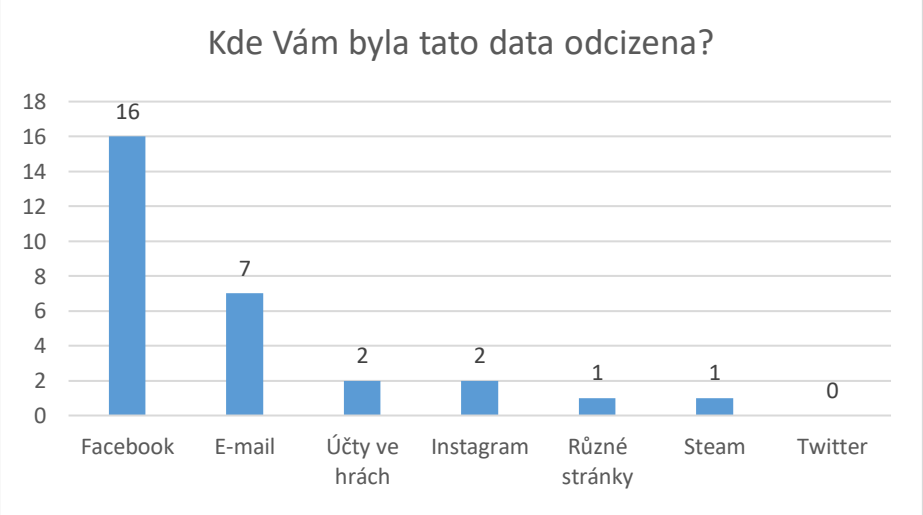
Graf 4 – Důvod otevření odkazu

Procento uživatelů, kteří se ve virtuálním světě setkali s napadením nebo ukradením identity, se zastavilo téměř na 40 %. Tento počet mi přijde vysoký, ale může být ovlivněn také tím, že pouze pár dní před začátkem rozeslání dotazníku jsem se setkala se dvěma případy mých „přátel“, kterým byla virtuální identita odcizena, jejich identita byla také zneužita.



Graf 5 – Zkušenost respondentů s krádeží identity

Nejčastější stránkou, na které respondentům byla identita odcizena, je Facebook, který označilo celkem 16 z 25 respondentů. V tomto výsledku se zřejmě projevila skutečnost, že Facebook je podle webu Statista označen za nejpopulárnější sociální síť. Sociální sítě byly řazeny na základě počtu aktivních uživatelů. [68] Facebook označil dokonce dvakrát větší počet respondentů než druhý v pořadí e-mail.

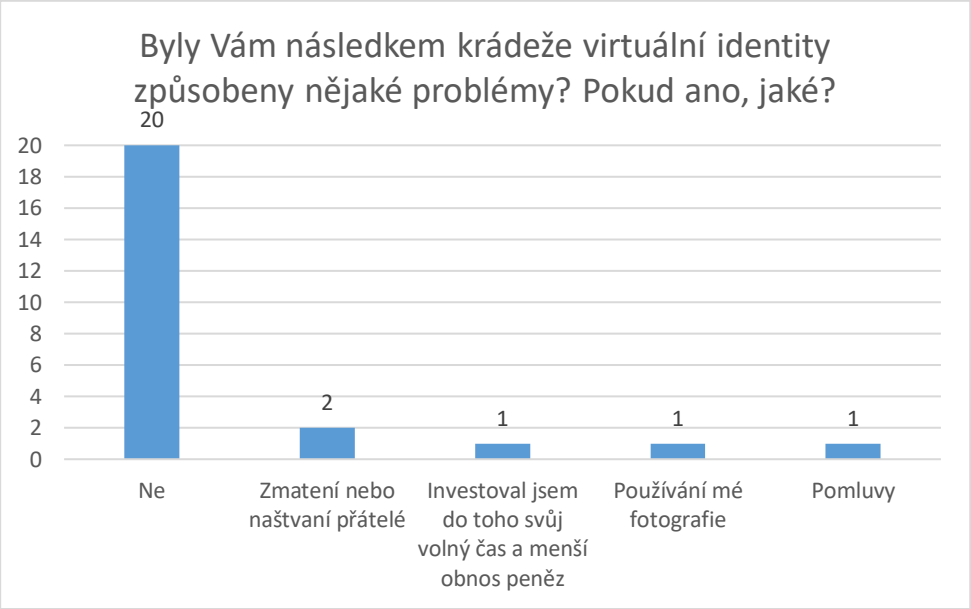


Graf 6 – Nejčastější weby, kde se respondenti setkali s krádeží identity

Respondenti v otázce „Jak jste napadení řešil/a?“ měli možnost vypisovat jakýkoliv text. Data jsem prošla a zoptimalizovala, jelikož například možnost „změna hesla“ a „změnou hesla“ se podle grafu v Google Formulářích jevila jako rozdílná, podstatou jde ale o stejná řešení. Respondenti v téměř 65 % řešili krádež identity změnou hesla. Kontaktování podpory a nahlášení problému by se dalo označit za jedno řešení, pro názornost dat jsem tato dvě řešení nechala rozdělené.

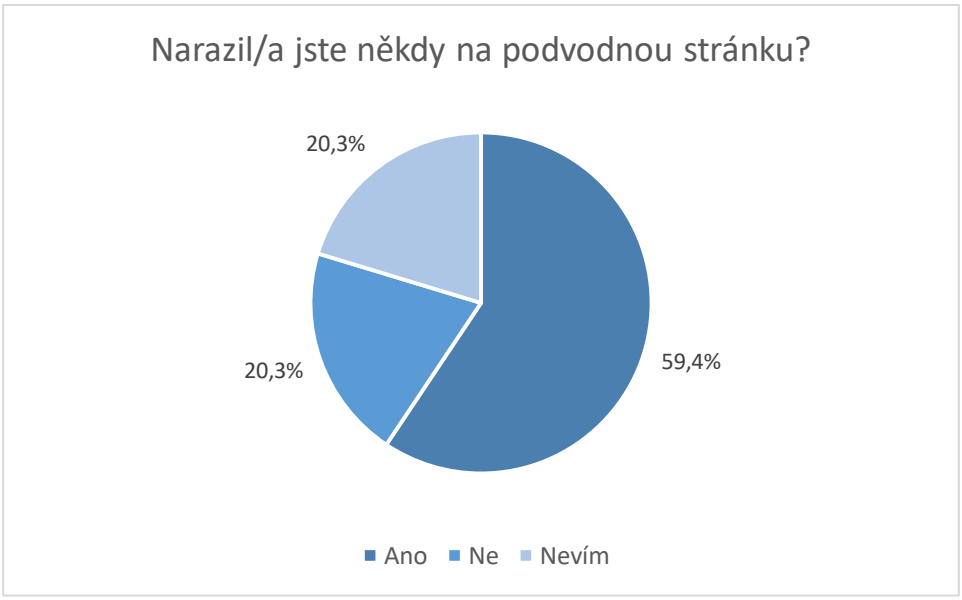
Graf 7 – Řešení respondentů při krádeži identity

Téměř žádnému respondentovi nebyl krádeží identity způsoben problém. Pouze 5 z 25 respondentů se s nějakým problémem setkali, což je určitě povzbuzující číslo. Největší problém by mohl být čas a peníze respondenta a poté také pomluvy.



Graf 8 – Problémy způsobené krádeží identity

Další otázka v dotazníku, na kterou odpovídali všichni respondenti, byla „Narazil/a jste někdy na podvodnou stránku?“. Pro tuto proměnnou také nebyla prokázána závislost s krádeží virtuální identity. *P*-value nabyla vyšší hodnoty než je stanovená hladina významnosti $\chi^2(2) = 1{,}91156, P = 0{,}384512$.

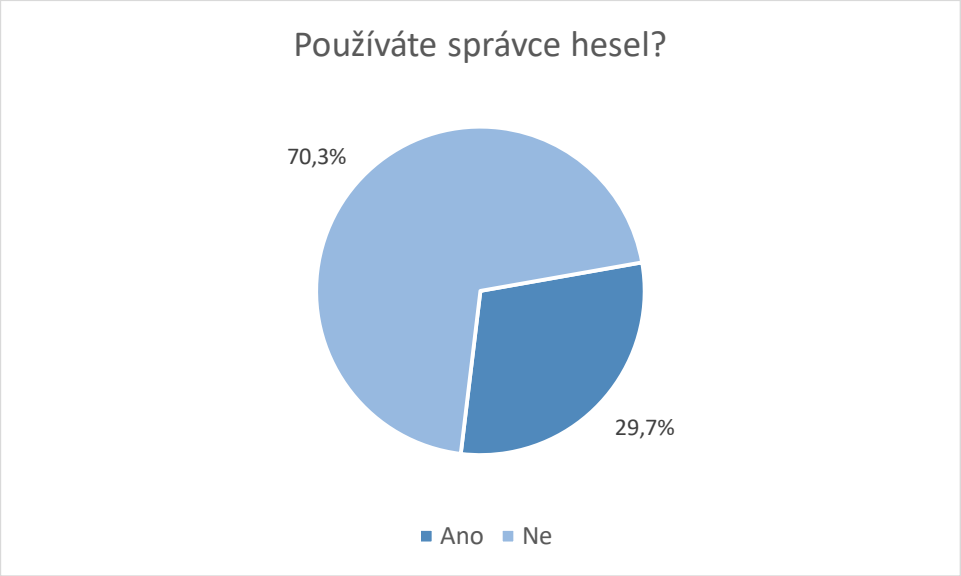


Graf 9 – Zkušenost respondentů s podvodnými stránkami

Nejčastěji osoby podvodnou stránku jednoduše opustily, druhou nejčastější odpovědí bylo „zavření prohlížeče“ – to by se dalo považovat za stejnou reakci. Pokud uživatelé nahlásí stránku administrátorovi, mohou tím napomoci upozornit případné další možné oběti těchto stránek.

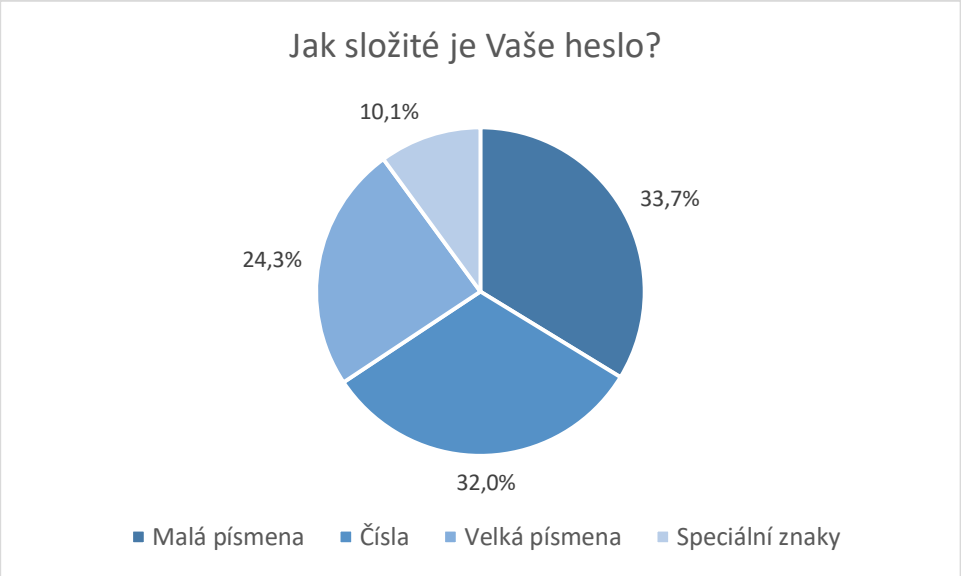
Graf 10 – Reakce respondenta po zjištění, kdy navštívil podvodnou stránku

Konečná získaná data ukazují, že téměř 30 % respondentů používá správce hesel. Toto procentuální rozložení se zdá poměrně pravděpodobné. Jelikož během zpracování bylo toto rozdělení téměř 50:50, tak mi tento výsledek přišel poměrně zajímavý. Navíc jsem se tedy zeptala některých respondentů, jestli by mi prozradili, jak na tuto otázku odpověděli. Jedna skupina respondentů mi oznámila, že „ANO“, používají správce hesel. Když jsem se zeptala, jakou aplikaci k tomu používají, tak mi odpověděli, že žádnou aplikaci, ale nechávají si ukládat hesla do manageru hesel v prohlížeči. Zde je tak jako u správce hesel potřeba, aby si uživatel zjistil, kde jsou jeho hesla ukládána a podle toho do daného prohlížeče ukládal hesla, či nikoliv.



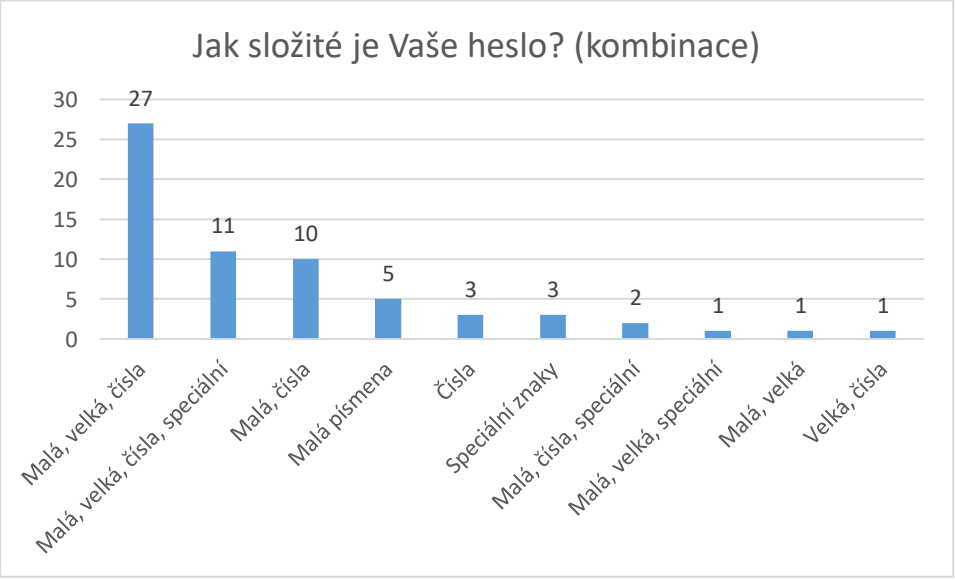
Graf 11 – Používání správce hesel

Z grafu níže je vidět, že respondenti při vytváření hesla nejčastěji používají malá písmena a čísla. Méně často pak používají velká písmena a pouze 10 % respondentů používá v uvažovaném hesle speciální znaky.



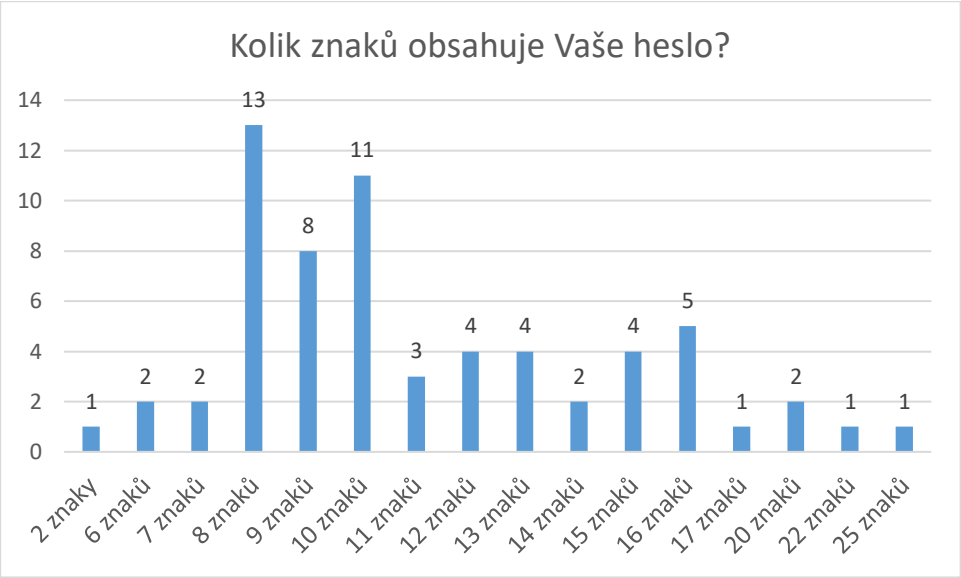
Graf 12 – Složitost hesla

Nejčastěji heslo respondentů obsahovalo malá, velká písmena a čísla. Druhou nejčastější kombinací je podle některých zdrojů nejlepší kombinace, a to malá a velká písmena, čísla a speciální znaky. Obě tyto varianty obsahují základ, který je uveden na webu Infosec Resources (viz kapitola 4.1 Heslová politika).



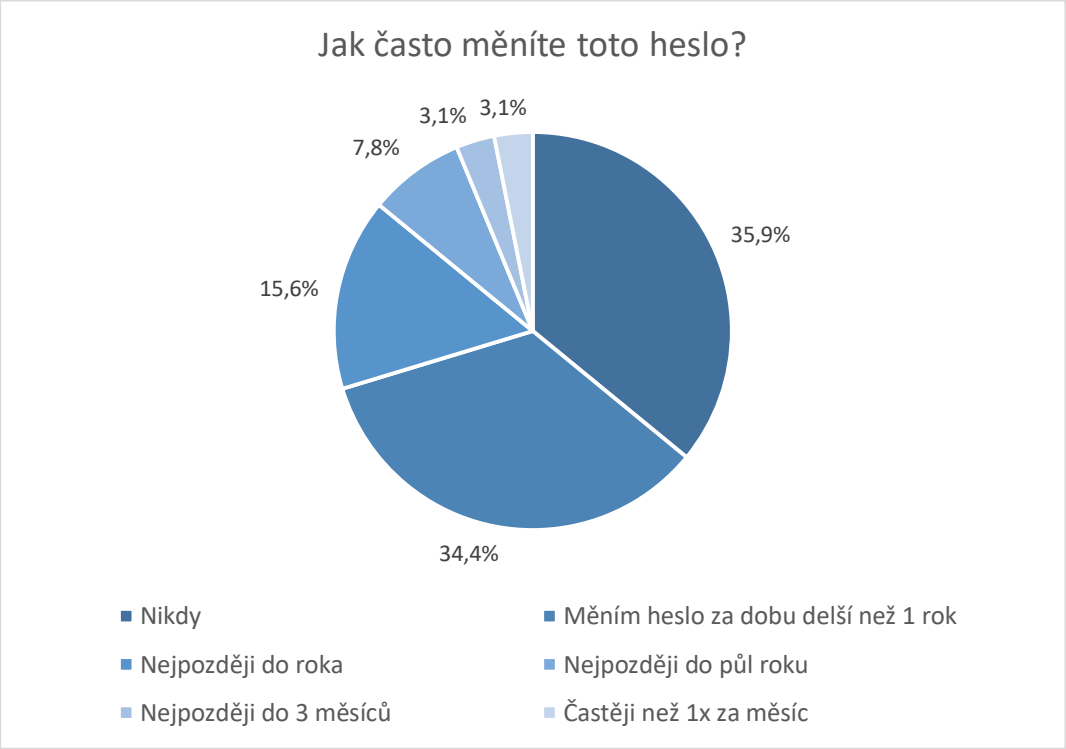
Graf 13 – Složitost hesla (kombinace)

Respondenti u otázky na délku hesla měli možnost vyplnit číslici, kolik znaků jejich heslo obsahuje. Dva znaky budou určitě nějaký překlep respondenta. Nejčastější počet znaků je 8, tento počet je často používán jako minimální možný počet znaků. Podle kapitoly 4.1 Heslová politika je uživateli doporučeno 16 znaků. Jelikož se mezi krádeží virtuální identity a počtem znaků závislost neprokázala, toto doporučení nad získanými daty není možné potvrdit.



Graf 14 – Počet znaků v hesle

70 % respondentů nemění své heslo nikdy, nebo jej mění za delší dobu než 1 rok. Také v tomto případě se na získaných datech neprokázala závislost s krádeží identity. Zajímavé je, že dva respondenti odpověděli, že své heslo mění častěji než 1x za měsíc. Jelikož podle výsledků už nyní mnozí respondenti nevyužívají pravidelnou změnu hesla, tak předpověď z webu SpyCloud, že během roku 2020 bezpečnostní experti začnou toto nastavení pravidelné změny hesla zpochybňovat, mi přijde velice reálná.



Graf 15 – Změna hesla

8 Metodika

Hlavním cílem práce je navržení metodiky pro předcházení krádeže virtuální identity na základě sociálního experimentu z kapitoly 7 Statistická analýza.

8.1 Obecné

Níže navržená metodika se týká zejména případů, kdy se útočník snaží o odcizení již vytvořeného profilu. V případě vytvoření duplicitního profilu bohužel uživatel nemá mnoho šancí, jak krádeži identity předcházet. Jedná se o metodiku založenou na výsledcích sociálního experimentu, současně je ale většina z uvedených bodů zmiňována na mnohých webových stránkách, které se zabývají krádežemi virtuální identity.

Určení hodnoty aktiva

Facebook pro respondenty často nemá takovou hodnotu aktiva jako jiný účet (např. elektronické bankovnictví). Proto by si uživatel měl stanovit, jakým aktivem je pro něj účet na dané stránce nebo v aplikaci. Měl by se zamyslet nad tím, co by pro něj znamenala případná kompromitace účtu a jaké problémy by mohlo zjištění přístupových údajů útočníkem způsobit. Zjištění hesla na účet e-mailu může mít pro útočníka větší cenu, než by se na první pohled mohlo zdát, jelikož na tento účet může zažádat o obnovu hesla na jiném účtu. Také tuto skutečnost by měl uživatel v rámci určení hodnoty aktiva brát v úvahu.

Uživateli postačí jednoduché určení, zda pro něj má účet hodnotu vysokou, normální nebo nízkou. Ideálně by se měl řídit všemi níže zmíněnými body. Případně by měl na základě určení hodnoty aktiva dodržovat více či méně z bodů metodiky popsaných níže.

Používání unikátního hesla, správce hesel

Uživatel by měl používat na každém účtu jiné heslo. Jelikož mnoho uživatelů má několik desítek účtů, může se tento bod jevit jako velice náročný. Uživatel má možnost použít různé mnemotechnické pomůcky na zapamatování, případně by mohl problém zapamatování velkého počtu hesel za uživatele vyřešit správce hesel, kde stačí zapamatování si pouze jednoho „hlavního“ hesla. Uživatel by měl mít unikátní hesla minimálně na účtech, které pro něj mají vysokou hodnotu aktiva.

Používání vícefaktorové autentizace

Na účtech, které to umožňují, by měl uživatel používat vícefaktorovou autentizaci. Nejčastěji aplikace a weby umožňují vícefaktorovou autentizaci prostřednictvím zaslání jednorázového kódu na uživatelem předem zadané telefonní číslo.

Kontrola zabezpečeného přístupu

Uživatel by měl kontrolovat, zda jím navštívená stránka umožňuje zabezpečený přístup. Neměl by na weby, které neposkytují zabezpečené připojení zadávat žádné citlivé údaje, jelikož by mohly být odcizeny útočníkem.

Kontrola odkazů

Uživatel by neměl otevírat hned každý odkaz, který mu někdo zašle. V případě, že odkaz otevře, tak by měl zkontrolovat, zda je přesměrován na web, na který měl odkaz vést. Zde by uživatel mohl narazit na problém, kdy mu je odeslán v textu odkaz, ale web na který se dostane, je odlišný.

V případě, že uživateli přijde zkrácený odkaz, např. Bitly, je třeba si zkontrolovat, na jaký web a kam má být uživatel přesměrován. Přímo Bitly má možnost zjistit cíl přesměrování přidáním znaménka plus na konec odkazu. Další stránky, které umožňují zjištění cíle odkazu, jsou např. https://www.expandurl.net/ nebo https://unshorten.me/.

Kontrola aktivity

Kontrola aktivity na daném profilu by mohla odhalit nesrovnalosti a uživatel by tak mohl zareagovat na krádež identity ještě dříve, než jeho profil bude zneužit. Kontrolou aktivity je také myšleno zpozornění uživatele v případě, že mu přijde oznámení o kontrole přihlášení.

Informovanost

Důležitá je také informovanost osob o možných rizicích, se kterými se na internetu uživatel může setkat. Nejen weby, které se často setkávají s krádeží identity, ale také ostatní weby nebo firmy by měly preventivně upozorňovat uživatele na možná rizika. Vedení firmy může na různých webových stránkách vyzkoušet, zda je jejich firma náchylná ke zranitelnosti na určitý typ kybernetických útoků. Například je možné vyzkoušet zranitelnost firmy na phishingové útoky: https://www.infosecinstitute.com/iq/phishing/phishing-risk-test/.

Obezřetnost

Tak jako kdykoliv jindy by neměl uživatel zapomenout být obezřetný. Pokud mu někdo nikdy nenapsal, s tou osobou se téměř nezná a teď mu píše, že ho něco bude zajímat, měl by uživatel zpozornět.

Kontaktování osoby

Pokud uživatel zaregistruje neočekávané chování nebo neočekávanou zprávu, měl by se ujistit, zda zpráva opravdu byla odeslána danou osobou. Před otevřením odkazu by měl kontaktovat osobu buď na stejné stránce, na jiném komunikačním kanálu, položením otázky, na kterou osoba dokáže odpovědět, nebo konstatováním informace, kterou s největší pravděpodobností znají jen dané osoby.

Nastavená bezpečnostní politika

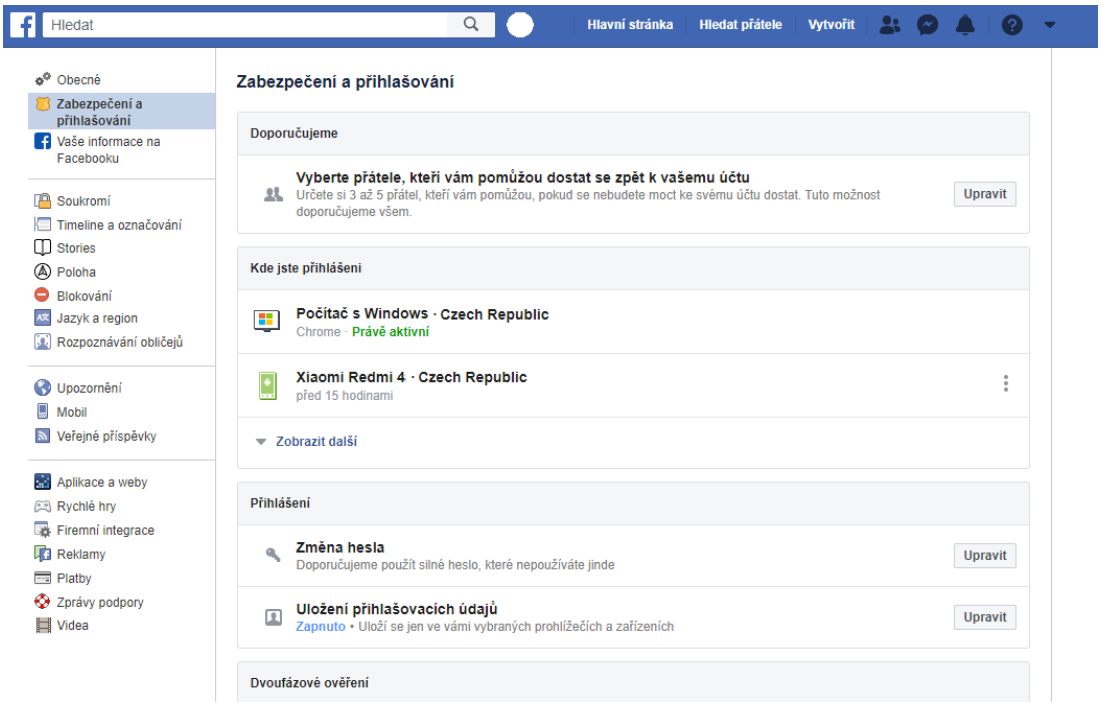
Měla by být nastavena bezpečnostní politika, zejména u firem, jejichž zaměstnanci mají možnost přistupovat na různé weby na internetu. Setkala jsem se s jedním případem, kdy nastavení bezpečnostní politiky firmy zabránilo respondentovi k přístupu na web odesílaný ve zprávě.

8.2 Zabezpečení sociální sítě Facebook

Jelikož se nejčastěji s krádeží identity setkali uživatelé na Facebooku, rozhodla jsem se, že v rámci metodiky představím možnosti nastavení zabezpečení, která tato sociální síť umožňuje. Krádeži identity formou vytvoření duplicitního profilu může uživatel částečně předcházet nastavením soukromí. Na Facebooku má možnost zkontrolovat, jaké informace o něm vidí jakýkoliv jiný uživatel internetu.

Níže popsané a zobrazené návody se týkají nastavení Facebooku na počítači, v mobilní verzi nastavení bude mít uživatel možnosti zabezpečení identické nebo velice podobné. Současně většina sociálních sítí a některé webové stránky, jako je např. e-mail, mají obdobné možnosti zabezpečení.

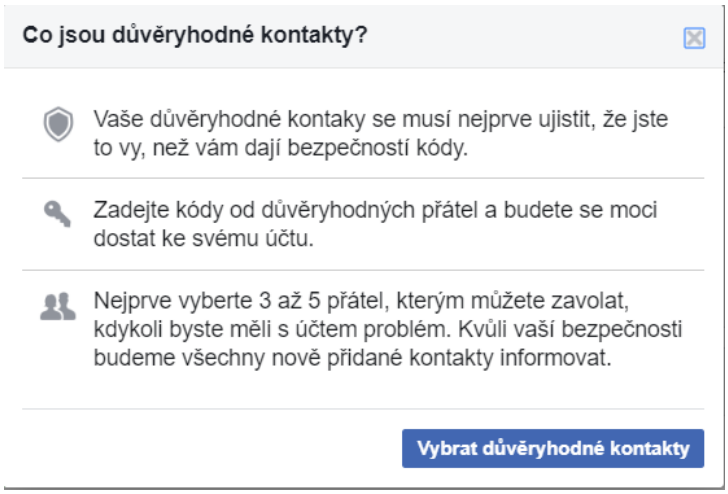
Odkaz na níže popsané možnosti zabezpečení je dostupný na adrese: https://www.facebook.com/settings?tab=security.



Obrázek 6 – Facebook zabezpečení [76]

Jako první možnost, která je uživateli Facebooku při nastavování zabezpečení zobrazena a dokonce doporučována je **Vyberte přátele, kteří vám pomůžou dostat se zpět k vašemu účtu**. Uživatel má možnost vybrat některé ze svých přátel a označit je jako tzv. důvěryhodné kontakty. Po zvolení minimálně tří profilů daných přátel je těmto osobám odeslána informace, že jste si je zvolili jako důvěryhodný kontakt.

Pro opětovné získání přístupu ke svému účtu na Facebooku se uživatel dostane pomocí kliknutí na odkaz *Zapomněli jste účet?* na přihlašovací stránce. Zde zadá svou e-mailovou adresu nebo telefonní číslo a klikne na *Pokračovat*. Dále zvolí možnost *Zobrazit moje důvěryhodné kontakty* a zde napíše celé jméno jednoho nebo více ze svých důvěryhodných kontaktů. Důvěryhodný kontakt získá přihlašovací kód, který následně uživatel může použít pro přístup ke svému účtu.



Obrázek 7 – Facebook důvěryhodné kontakty [76]

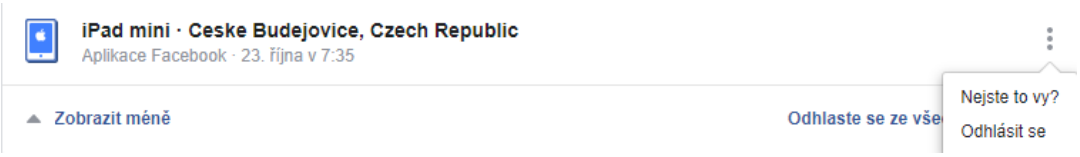
Kde jste přihlášeni, je možnost kontroly všech zařízení, ke kterým je daný profil přihlášen. Pokud některé z těchto zařízení nebo míst nepoznáváte, je třeba tuto skutečnost řešit. Nabízí se tři možnosti:

- *Odhlásit se ze všech zařízení*
- *Odhlásit se*
- *Nejste to vy?*

Pokud uživatel zvolí možnost *Odhlásit se ze všech zařízení*, dojde k odhlášení ze všech zařízení, ke kterým byl nebo je daný profil přihlášen.

Možnost *Odhlásit se* umožní uživateli odhlásit se pouze od jednoho daného zařízení. Pokud se z tohoto zařízení bude uživatel někdy chtít přihlásit, bude muset zadat přihlašovací údaje znovu.

Poslední možností je *Nejste to vy?*, která uživateli zobrazí čas, místo a zařízení, ze kterého připojení proběhlo. Pokud tuto aktivitu uživatel nepoznává, může zvolit možnost *Zabezpečit účet*, během kterého proběhne kontrola nastavení. Facebook následně vyhodnotí, jaké změny proběhly, a současně nabídne uživateli zobrazení posledních změn účtu.

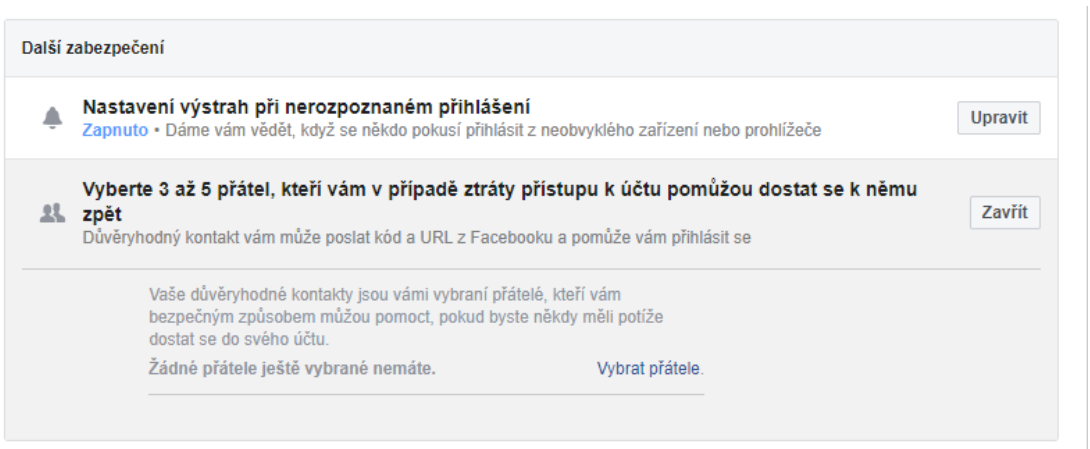


Obrázek 8 – Facebook, kde jste přihlášeni? [76]

Možnost **Přihlášení** umožňuje uživateli *Změnit heslo* a *Uložení přihlašovacích údajů*. Pokud uživatel zvolí Uložení přihlašovacích údajů, tak při příštím přihlášení v tomto prohlížeči nebude muset zadávat heslo.

Dvoufázové ověření umožňuje uživateli nastavit si, že v případě, kdy Facebook zaznamená přihlášení z nerozpoznaného zařízení, bude uživatel požádán o zadání bezpečnostního kódu, nebo potvrzení v jiném zařízení nebo aplikaci. Bezpečnostní kód uživatel získá prostřednictvím SMS s přihlašovacím kódem. Facebook umožňuje uživateli vygenerovat si tzv. kód pro obnovení. Uživatel získá 10 unikátních kódů a každý z nich může pro přihlášení použít právě jednou. Potvrdit přihlášení může uživatel pomocí bezpečnostní aplikace (např. Google Authenticator, LastPass nebo Duo Mobile). V nabídce *Ověřená přihlášení* uživatel kontroluje seznam zařízení, na kterých nebude muset použít přihlašovací kód. *Hesla k aplikacím***,** jako jsou např. Xbox, Spotify nebo Skype, ke kterým se uživatel přihlašuje přes Facebook (viz kapitola 4.4.2 Propojené účty), umožňují nastavení speciálního hesla pro konkrétní aplikaci.

Další zabezpečení se týkají *Nastavení výstrah při nerozpoznaném přihlášení*, kdy uživatel dostane upozornění na přihlášení z neobvyklého zařízení nebo prohlížeče a již výše zmiňovaného výběru důvěryhodných kontaktů.



Obrázek 9 – Facebook, další zabezpečení [76]

Pokročilé zabezpečení umožňuje nastavení *Šifrované e-mailové komunikace, Obnovení externích účtů* a *Zobrazení nejnovějších e-mailů z Facebooku*.

9 Konfrontace metodiky

Dílčím cílem je konfrontace navržené metodiky. Pro tuto část bakalářské práce jsem zvolila metodu rozhovoru. Rozhovor jsem vedla se slečnou Monikou, které byla v minulosti ukradena identita na sociální síti Instagram.

Pořízený záznam rozhovoru nebyl sdílen s nikým jiným než s autorem a vedoucím bakalářské práce. Záznam byl na základě slovní dohody ihned po kompletaci práce vymazán. Autentický přepis rozhovoru je použit jako součást dílčího cíle praktické části práce. Oběť krádeže virtuální identity je identifikována pouze křestním jménem.

Kde byla Tvoje identita ukradena?

„Na Instagramu. Ale poslední dobou mám problém s e-mailem, je zajímavé, že když jdu na e-mail přes telefon a chci si poslat něco do práce, tak začnu psát svoje jméno a začnou mi vyjíždět e-maily, kde je napsaný můj e-mail a pod ním je přesměrování na jiný e-mail. Já nevím, co to je. Pro jistotu jsem si tedy na tomto e-mailu změnila heslo, ale celkově mě to děsí, protože kdybych špatně klikla, tak to odešlu na jiný e-mail. Když počáteční písmena e-mailu zadávám přes notebook, tak mi tam nic nenaskočí, jen přes ten telefon mi tam začnou vyskakovat nějaký e-maily. Přijde mi to děsivý, protože jsou tam koncovky ‚ru' podobné těm, které mi právě ukradli Instagram, tam vlastně byla stejná koncovka."

Přijdou Ti body v metodice srozumitelné?

„Jo, věděla bych, co mám dělat."

Myslíš si, že by sis metodiku přečetla, kdybych s Tebou na tuto metodiku nedělala rozhovor? Myslíš, že bys měla důvod metodiku číst (třeba i proto, že už Ti identita byla ukradena)?

„Když bych to začala číst, tak bych to asi přečetla do konce. Ale já jsem taková, že moc nečtu odkazy, takže si myslím, že bych si to přečetla až potom, co by se mi krádež identity stala. To je případ právě i s tím Instagramem, kdy jsem začala pročítat různé blogy a tak, abych věděla co a jak dál. Preventivně asi ne, nejsem ten typ, který by to četl. Ale když teď vím, že něco takového existuje, tak bych na to možná odkázala někoho, u koho bych si myslela, že by si účet měl víc zabezpečit."

Našla jsi na daných webech informace, co máš dělat?

„Byly tam blogy, které radily, co máš dělat, když máš odcizený účet, jak kontaktovat Instagram. Informace jsem sice nějaké našla, ale účet mi to vlastně nevrátilo. Ale odkaz na článek jsem posílala jedné holce, které díky tomu účet vrátili. Možná jí to vrátili, protože na tom účtě měla hodně sledujících."

Jaké body jsi dodržovala/nedodržovala u odcizeného účtu?

„Nepoužívala jsem tam nic, bylo mi to celkem jedno. Věděla jsem, že se mi to může stát, ale bylo mi to jedno. Potom, co se to stalo, tak jsem si tam nastavila několik ověření, které mám možnost nastavit. Na účtech mám vícefaktorové ověření, ale hesla mám všude stejné."

Z dat vyšlo, že uživatelé, kteří se setkali s krádeží identity, ve větším počtu kontrolují, zda je web, na který přistupují, zabezpečen. Víš, co to je a kontroluješ Ty osobně zabezpečený přístup?

„Moc to nekontroluju, ale prohlížeč mě upozorňuje, že stránka, na kterou chci přistoupit, není zabezpečená, jestli tam chci opravdu vstoupit. Ale sama od sebe to nekontroluju. Na přístup do elektronického bankovnictví nejčastěji používám aplikaci, tam nic takového není."

Jak jsi zjistila, že Ti byla identita odcizena? Zjistila jsi to Ty, nebo někdo jiný?

„Zjistila jsem to vlastně já, bylo to shodou okolností v době, kdy jsem byla v práci. Nacvakala jsem si tam odkaz instagram.com/můjProfil a ten profil mi to nechtělo najít. Přišlo mi to strašně divný, proč se tam nemůžu dostat. Po práci jsem si klikla na aplikaci a dalo mi to vytvořit nový profil přes e-mail. Tak jsem dala přihlásit a viděla jsem úplně jiný Instagram. Začala jsem to vyhledávat a tím, jak jsem se proklikla přes Facebook, kde jsem sdílela z Instagramu fotky, tak se mi zobrazil úplně jiný profil s jiným jménem. Pak jsem si zkontrolovala e-mail, kde vlastně ty e-maily byly přečtený. Byl tam e-mail s žádostí o změnu hesla, o změnu e-mailu. Takže se mi někdo naboural i na e-mail."

Jsi schopna určit hodnotu aktiva, kterou pro Tebe daný účet má?

„Pro mě je všechno důležitý, já jakožto ‚závislák' na telefonu a aplikacích si myslím, že pro mě to má všechno vysokou hodnotu. Tím, jak na Instagramu byly fotky a určité vzpomínky, tak mě to mrzelo. Na tom profilu vlastně zůstaly všechny moje fotky, tak jsem se bála, aby někomu z mého účtu nepsali. Bála jsem se toho, co se stane. Díky nahlášení několika mých přátel nakonec ten profil zrušili."

Je nějaký bod v metodice, který Tě zaujal?

„Všechno jsem asi slyšela a některé body splňuji. Třeba právě u toho e-mailu jsem hned zjišťovala aktivitu, jestli někdo neodesílá něco z mého e-mailu nebo jestli tam není nastavené přeposílání na jiný e-mail."

Je nějaký bod, který bys v metodice očekávala, ale chybí Ti tam?

„Já si myslím, že je tam všechno."

Co z toho (pokud něco) dodržuješ teď jinak, na rozdíl od toho, kdy Ti byla identita ukradena?

„Vícefaktorové ověření, změnila jsem heslo, prodloužila jsem ho a přidala tam různé znaky. Aktivitu kontroluji až od té doby, kdy mi byla identita ukradena. Odkazy neotevírám skoro vůbec, první co udělám, tak to neotevírám. Vím, jak je to na Facebooku, kde ti posílají virové odkazy a prostě to nechci otevírat. To samé u e-mailu, když mi někdo, koho neznám, posílá odkaz. A když mi někdo, koho znám pošle odkaz, tak se zeptám a až po komunikaci s daným člověkem to otevřu, ale neotevírám to hned. Nezáleží na tom, jestli to byl odkaz se zprávou, nebo ne. Mám e-mail, přes který komunikuji a pak záložní, na který se mi některé zprávy přeposílají a měly by mi tam přijít informace, kdyby byly zase nějaké problémy."

Po přečtení metodiky, myslíš si, že budeš něco dodržovat/budeš si dávat na něco větší pozor?

„Snažím se dávat si co největší pozor. Změna si myslím, že nebude moc velká. Různé hesla jsem si zkoušela dávat, ale pak jsem měla ten problém, že jsem je všechny zapomínala. Nechtěla jsem si to někam zapisovat, tak mám teď jedno heslo."

Ukládáš si hesla do prohlížeče?

„Záleží na jakou stránku. Dneska třeba jsem si objednávala reklamní předměty a byla jsem si je vyzvedávat, tak tam jsem si heslo třeba do prohlížeče uložila. Ale u Facebooku, bankovnictví, tam si to nenechávám uložený, tam mi to přijde nebezpečné."

Řekla jsi, že používáš jedno heslo. Takže kdyby někdo zjistil tvoje heslo na tom webu, tak by se Ti mohl dostat vlastně do e-mailu.

„Vlastně nepoužívám jen jedno heslo, používám více variant toho hesla. Jedno jednodušší a druhé složitější. Podle té metodiky by to odpovídalo té hodnotě aktiva."

Znáš možnosti zabezpečení, které nabízejí Instagram a Facebook?

„Potom, co mi ukradli Instagram, tak jsem zjišťovala, jak můžu svůj účet ochránit. Teď tam používám heslo a kód. Mám navíc nějaké speciální kódy, které slouží k ověření, kdyby mi nepřišel kód. To samé mám u Facebooku, ale navíc tam mám přidané přátele, kteří by mi v případě odcizení mohli pomoct s vrácením účtu. Navíc si pamatuju, že jednou mi přišlo upozornění, že se nacházím v Irsku, ale to jen v práci máme tak nastavenou Wi-Fi.“

Vyhodnocení

Na základě rozhovoru jsem zjistila, že slečna Monika od krádeže virtuální identity začala dodržovat téměř všechny body zmíněné v metodice. Zkoušela používat unikátní hesla, momentálně ale používá jedno heslo pro účty, které pro ní mají vysokou hodnotu, pro ostatní účty používá heslo jiné. Zde bych jí na základě výsledků ze statistiky doporučila, aby změnila svá hesla a pro zapamatování využila například některého ze správců hesel.

Co se týká zabezpečeného přístupu, tak věří prohlížeči, který jí podle jejích slov v případě nezabezpečeného webu o této skutečnosti informuje. Tento přístup slečny Moniky by se dal považovat za rizikový, jelikož prohlížeč ji ne vždy musí upozornit.

Navržená metodika se zdá být vzhledem k informacím získaným během rozhovoru obecná, měla by obsahovat všechny důležité body, které by uživatel pro zvýšení zabezpečení svých účtů měl dodržovat.

Závěr

Stále více z nás začíná žít ve virtuálním prostředí a sociální život odsouvají až do druhé řady, což sice není podle mého názoru správné, ale není to předmětem této práce a tak toto konstatování nebudu dále rozvíjet. Mnozí z nich si ale neuvědomují, že tento svět poskytuje nejen možnosti, ale také skrývá různé nástrahy.

Rychlý rozvoj v oblasti informačních technologií přináší uživateli celou řadu novinek, ať jsou to nové možnosti zabezpečení, ale také neustále nové způsoby, jak může dojít ke krádeži virtuální identity. Některá doporučení na zabezpečení se během let postupně upravují, další nová dokonce přibývají. Uživatel má možnost pro zvýšení zabezpečení zvolit kombinaci několika způsobů, kterými bude chránit svou identitu ve virtuálním prostředí. Často se bohužel stává, že začne řešit možnosti zabezpečení až ve chvíli, kdy už je pozdě, protože již ke krádeži jeho virtuální identity došlo. Tato práce by měla ukázat možnosti, jak se chránit dříve, než k takové situaci dojde.

Bakalářská práce je rozdělena na devět kapitol, prvních šest kapitol se věnuje teoretické rovině tématu. V první kapitole jsou vymezeny základní pojmy. Ve druhé kapitole jsem popsala, co to je krádež virtuální reality. Ve třetí kapitole jsou popsané kybernetické útoky. Ve čtvrté kapitole jsou uvedeny způsoby, jak může uživatel zvýšit zabezpečení. V páté kapitole jsem uvedla následky krádeže virtuální reality. V šesté kapitole jsem se věnovala legislativě, tedy mj. GDPR. Snažila jsem se podrobně a precizně shrnout známá fakta a vypracovat návod, který by pomáhal lidem nejen řešit již vzniklou krádež virtuální identity, ale byl (a to hlavně) preventivním nástrojem, aby k takové činnosti docházelo pokud možno co nejméně.

V dalších třech kapitolách se věnuji praktické části: nejprve to byl v sedmé kapitole rozbor získaných odpovědí na dotazník a následné vypracování statistické analýzy. V osmé kapitole jsem popsala metodiku této práce a v deváté kapitole jsem zaznamenala autentickou výpověď osoby, které virtuální identita již byla ukradena.

Během práce jsem měla možnost zjistit, jak důvěřiví, nebo naopak prozíraví, dokáží být uživatelé ve virtuálním prostředí. Při výzkumu se mi potvrdila domněnka, která není moc přívětivá: uživatelé důvěřují osobě ve virtuálním světě, aniž by si ověřili její skutečnou totožnost.

Je důležité, aby se o tématu krádeží identity mluvilo. Čím informovanější a obezřetnější uživatelé jsou, tím více se snižují možnosti útočníků odcizit jejich účet. Samozřejmě na tuto skutečnost útočníci postupně reagují novými a ještě více sofistikovanějšími způsoby. Způsoby, které v současné době ještě neexistují, ale za pár let již budou stejně tak probírané, jako některé dnešní běžné útoky.

Cíle, které byly pro tuto práci stanoveny, a to: zjištění, jak jsou lidé informováni o možnosti napadení a zabezpečení, dále jak mají svá dat a účty zajištěny, zjistit, jak jsou informováni o dalším postupu při krádeži dat – byly splněny. Navržená metodika z kapitoly 8 Metodika se jeví jako obecná vzhledem k získaným informacím z rozhovoru se slečnou Monikou, neboť jednotlivé body metodiky se dají použít na různých webech, zejména na sociálních sítích.

Seznam použitých zdrojů

Knihy

[1] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[2] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

[3] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[4] SKLENÁK, Vilém. Data, informace, znalosti a Internet. Praha: C.H. Beck, 2001. C.H. Beck pro praxi. ISBN 80-717-9409-0.

[5] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 978–80–254–8979–6.

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

[7] BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012. Olomouc: ANAG, 2012. Právo (ANAG). ISBN 978-80-7263-749-2.

Web

[8] GEER, David. Poznejte výhody vícefaktorové autentizace. Computerworld.cz [online]. 12. 8. 2018 [cit. 2019-11-24]. Dostupné z: https://computerworld.cz/securityworld/poznejte-vyhody-vicefaktorove-autentizace-54802

[9] COUFALOVÁ, Denisa. Jak předejít krádeži identity? A lze rozpoznat, že jste se stali obětí takového zločinu? Ušetřeno.cz [online]. 18. 2. 2018 [cit. 2019-02-24]. Dostupné z: https://www.usetreno.cz/kradez-identity/

[10] Krádež identity. INTERNETEM BEZPEČNĚ [online]. [cit. 2019-03-11]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[11] VICHLENDA, Milan. Kriminalistika [online]. Karviná, 2011 [cit. 2019-03-28]. Dostupné z: https://www.sosoom-zlin.cz/media/skripta/kriminalistika.pdf

[12] Autentizace, ověření, identifikace (Authentication). ManagementMania.com [online]. 13. 2. 2018 [cit. 2019-03-12]. Dostupné z: https://managementmania.com/cs/autentizace-identifikace

[13] Trvalý identifikátor. Wikisofia [online]. [cit. 2019-03-28]. Dostupné z: https://wikisofia.cz/wiki/Trval%C3%BD_identifik%C3%A1tor

[14] Uživatelské jméno. ManagementMania.com [online]. 17. 4. 2018 [cit. 2019-01-24]. Dostupné z: https://managementmania.com/cs/uzivatelske-jmeno

[15] Autentizace a autorizace. Trisul.cz [online]. [cit. 2019-04-24]. Dostupné z: http://www.trisul.cz/bezpecnost-autentizace-autorizace/

[16] Autentizace. ITBiz.cz [online]. 13. 9. 2011 [cit. 2019-04-24]. Dostupné z: https://www.itbiz.cz/slovnik/informacni-technologie-it/autentizace

[17] MIHULKOVÁ (KMOŠKOVÁ), Jitka a Martin KORNEL. Co je, co není a co bude osobní údaj podle GDPR. Frank Bold Advokáti [online]. 10. 2. 2018 [cit. 2019-04-12]. Dostupné z: https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdpr

[18] Vícefaktorová autentizace. AMI Praha a.s. [online]. [cit. 2019-03-24]. Dostupné z: https://www.ami.cz/publikujeme/blog/vicefaktorova-autentizace

[19] Citlivé osobní údaje. GDPR.cz [online]. [cit. 2019-11-24]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

[20] Co to jsou přihlašovací údaje a k čemu slouží. Policie České republiky [online]. [cit. 2019-03-21]. Dostupné z: https://www.policie.cz/clanek/co-to-jsou-prihlasovaci-udaje-a-k-cemu-slouzi.aspx

[21] Data. ManagementMania.com [online]. 19. 2. 2018 [cit. 2019-02-28]. Dostupné z: https://managementmania.com/cs/data

[22] Digitální stopa. Jak na Internet [online]. [cit. 2019-02-24]. Dostupné z: https://www.jaknainternet.cz/page/3651/digitalni-stopa/

[23] Digitální stopa. INTERNETEM BEZPEČNĚ [online]. [cit. 2019-02-28]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

[24] Údaj. Wikislovník [online]. [cit. 2019-11-28]. Dostupné z: https://cs.wiktionary.org/wiki/%C3%BAdaj

[25] Digitální stopy. E-Bezpečí [online]. [cit. 2019-02-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

[26] KRATOCHVÍL, Petr. Deset bezpečnostních přikázání. Chip.cz - recenze a testy [online]. 6. 6. 2012 [cit. 2019-01-21]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/vydani/r-2012/chip-05-2012/deset-bezpecnostnich-prikazani/

[27] ŠTOCHL, Jiří. MARUŠKA NOVÁKOVÁ NEBO MARUSKA NOVAKOVA – FALEŠNÉ PROFILY NA SOCIÁLNÍCH SÍTÍCH. INTERNETEM BEZPEČNĚ [online]. 3. 9. 2018 [cit. 2019-03-28]. Dostupné z: https://www.internetembezpecne.cz/5856-2/

[28] Krádež identity a jak se jí bránit. Bezpečný internet [online]. [cit. 2019-11-28]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

[29] KUBEŠ, Jan. Poznáte falešný profil na Facebooku? Dvojklik [online]. [cit. 2019-06-24]. Dostupné z: https://www.dvojklik.cz/poznate-falesny-profil-na-facebooku/

[30] Kyberkriminalita. Prevence kriminality [online]. [cit. 2019-06-28]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

[31] Co je sociální inženýrství? - 2. díl. PC World.cz [online]. 3. 6. 2012 [cit. 2019-02-28]. Dostupné z: https://pcworld.cz/internet/co-je-socialni-inzenyrstvi-2-dil-44372

[32] CO TO JE MALWARE. INTERNETEM BEZPEČNĚ [online]. [cit. 2019-03-21]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/co-to-je-malware/

[33] POČÍTAČOVÉ VIRY, ČERVI A TROJSKÉ KONĚ. INTERNETEM BEZPEČNĚ [online]. [cit. 2019-03-21]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

[34] Keylogger. Avast [online]. [cit. 2019-03-28]. Dostupné z: https://www.avast.com/cs-cz/c-keylogger

[35] CO JE TO PHISHING. HOAX [online]. [cit. 2019-06-24]. Dostupné z: https://www.hoax.cz/phishing/co-je-to-phishing

[36] History of Phishing. Phishing [online]. [cit. 2019-06-24]. Dostupné z: https://www.phishing.org/history-of-phishing

[37] VIOLINO, Bob. Jak správně zabezpečit nejvyšší manažery podniku? Computerworld.cz [online]. 21. 12. 2018 [cit. 2019-06-29]. Dostupné z: https://computerworld.cz/securityworld/jak-spravne-zabezpecit-nejvyssi-manazery-55108

[38] Předpovědi pro rok 2019, 2. část: Mobilní hrozby. Avast Blog [online]. 18. 1. 2019 [cit. 2019-10-28]. Dostupné z: https://blog.avast.com/cs/predpovedi-pro-rok-2019-mobilni-hrozby

[39] KIGUOLIS, Linas. CO JE TO TROJSKÉ KONĚ A JAK JEJ ODSTRANIT. Bezpečnost a novinky o virech [online]. 26. 4. 2016 [cit. 2019-03-28]. Dostupné z: https://odstranitvirus.cz/trojske-kone/

[40] Sniffer. IT Slovník [online]. [cit. 2019-03-28]. Dostupné z: https://it-slovnik.cz/pojem/sniffer

[41] Síla hesla. Wikipedie [online]. [cit. 2019-02-12]. Dostupné z: https://cs.wikipedia.org/wiki/S%C3%ADla_hesla

[42] PICHETA, Rob. How hackable is your password? CNN [online]. 23. 4. 2019 [cit. 2019-11-28]. Dostupné z: https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

[43] Zásady pro bezpečné nakládání s hesly. Interval.cz [online]. [cit. 2019-11-14]. Dostupné z: https://www.interval.cz/clanky/zasady-pro-bezpecne-nakladani-s-hesly/

[44] Password Security: Complexity vs. Length [Updated 2019]. Infosec Resources [online]. 8. 9. 2019 [cit. 2019-11-27]. Dostupné z: https://resources.infosecinstitute.com/password-security-complexity-vs-length/

[45] Slabá hesla používá 95 % lidí v Česku. Avast Press [online]. 2. 5. 2019 [cit. 2019-09-09]. Dostupné z: https://press.avast.com/cs-cz/slaba-hesla-pouziva-95-lidi-v-cesku

[46] LOUDA, Pavel. Stejné heslo pro více účtů využívá polovina Čechů - i když se toho bojí. Computerworld.cz [online]. [cit. 2019-06-24]. Dostupné z: https://computerworld.cz/securityworld/stejne-heslo-pro-vice-uctu-vyuziva-polovina-cechu-55359

[47] Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology [online]. [cit. 2019-11-23]. Dostupné z: https://pages.nist.gov/800-63-3/sp800-63b.html

[48] 2020 Prediction: The Death of the Password Rotation Policy. SpyCloud [online]. [cit. 2019-11-28]. Dostupné z: https://spycloud.com/2020-prediction-the-death-of-the-password-rotation-policy/https://spycloud.com/2020-prediction-the-death-of-the-password-rotation-policy/

[49] 7 způsobů, jak zabránit krádežím identity online. Dr.fone [online]. [cit. 2019-11-24]. Dostupné z: http://global.drfone.biz/cs/vpn/prevent-identity-theft-online.html

[50] What you risk when you use the same password for multiple accounts. The Star Online [online]. 21. 4. 2018 [cit. 2019-11-28]. Dostupné z: https://www.thestar.com.my/tech/tech-news/2018/04/21/what-you-risk-when-you-use-the-same-password-for-multiple-accounts

[51] The 2019 State of Password and Authentication Security Behaviors Report. Yubico [online]. [cit. 2019-11-28]. Dostupné z: https://www.yubico.com/authentication-report/

[52] Správce hesel - nezbytný parťák pro online život. Magazín o SSL/TLS certifikátech a certifikačních autoritách [online]. [cit. 2019-06-24]. Dostupné z: https://blog.sslmarket.cz/inpage/spravci-hesel-nezbytny-partak-uzivatele-internet/

[53] Přechod na HTTPS - má smysl? Je čas.cz [online]. 7. 10. 2015 [cit. 2019-03-18]. Dostupné z: https://jecas.cz/https

[54] Co je HTTPS. Adaptic [online]. [cit. 2019-03-18]. Dostupné z: https://www.adaptic.cz/znalosti/slovnicek/https/

[55] Chrome vs LastPass detailed comparison as of 2019. Slant [online]. [cit. 2019-11-14]. Dostupné z: https://www.slant.co/versus/2550/2823/~chrome_vs_lastpass

[56] KLUSKA, Vladislav. 5 nejlepších služeb pro správu hesel a citlivých údajů. Živě.cz [online]. 6. 2. 2018 [cit. 2019-09-15]. Dostupné z: https://www.zive.cz/clanky/5-nejlepsich-sluzeb-pro-spravu-hesel-a-citlivych-udaju/sc-3-a-191643/default.aspx#part=5

[57] Sociální síť Facebook. FastCentrik [online]. [cit. 2019-11-29]. Dostupné z: https://www.fastcentrik.cz/podpora/manual/zakladni-nastaveni/socialni-site-a-web-identity/facebook

[58] PAULÍK, Tomáš. Proč používat Antivir. ANTIMALWARE.CZ [online]. [cit. 2019-09-09]. Dostupné z: https://www.antimalware.cz/blog/proc-pouzivat-antivir

[59] Proč pravidelně aktualizovat operační systém i další programy? Vím, kam klikám [online]. [cit. 2019-09-24]. Dostupné z: https://www.vimkamklikam.cz/soukromi/proc-pravidelne-aktualizovat-operacni-system-i-dalsi-programy

[60] Brute force – útok na hesla hrubou silou. HackerLab HackingKurzy.cz [online]. 7. 11. 2017 [cit. 2019-11-29]. Dostupné z: https://www.hackingkurzy.cz/blog/brute-force-utok-na-hesla-hrubou-silou/

[61] What is and Account Lockout? Computer Hope's Free Computer Help [online]. [cit. 2019-11-29]. Dostupné z: https://www.computerhope.com/jargon/a/accolock.htm

[62] Co je krádež identity? ESET [online]. [cit. 2019-11-29]. Dostupné z: https://www.eset.com/cz/kradez-identity/

[63] Co je GDPR? GDPR [online]. [cit. 2019-02-29]. Dostupné z: https://www.gdpr.cz/gdpr/

[64] Co považuje GDPR za osobní údaje. GDPR [online]. [cit. 2019-02-25]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

[65] Legislativa - Ochrana osobních údajů. Ministerstvo vnitra České republiky [online]. [cit. 2019-11-27]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/gdpr-web-legislativa-legislativa.aspx

[66] Úplné znení. Trestní zákoník [online]. [cit. 2019-11-27]. Dostupné z: http://www.trestnizakonik.cz/uplne-zneni

[67] Listina základních práv a svobod. Parlament České republiky, Poslanecká sněmovna [online]. [cit. 2019-11-27]. Dostupné z: https://www.psp.cz/docs/laws/listina.html

[68] CLEMENT, J. Global social networks ranked by number of users 2019. Statista [online]. 21. 11. 2019 [cit. 2019-11-28]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[69] Spear phishing je cílený phishing, kterému se lze jen těžko bránit. CleverAndSmart Management Consulting [online]. 26. 9. 2012 [cit. 2019-09-10]. Dostupné z: https://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/

[70] Slovníkový útok. Jak na IT [online]. [cit. 2019-09-09]. Dostupné z: https://www.jaknait.cz/co-je/slovnikovy-utok/

[71] Ukrást přihlašovací údaje je díky HTTP snadné. Magazín o SSL/TLS certifikátech a certifikačních autoritách [online]. [cit. 2019-11-28]. Dostupné z: https://blog.sslmarket.cz/inpage/ukrast-prihlasovaci-udaje-je-diky-http-snadne-obranou-je-https/

[72] Testování nezávislosti (Pearsonův chí-kvadrát test). Matematická biologie učebnice [online]. [cit. 2019-09-29]. Dostupné z: https://portal.matematickabiologie.cz/index.php?pg=aplikovana-analyza-klinickych-a-biologickych-dat--analyza-a-management-dat-pro-zdravotnicke-obory--testovani-hypotez-o-kvalitativnich-promennych--analyza-kontingencnich-tabulek--testovani-nezavislosti-pearsonuv-chi-kvadrat-test

[73] Se správcem hesel budete na internetu ve větším bezpečí. Blog Mall.cz [online]. 12. 6. 2018 [cit. 2019-11-29]. Dostupné z: https://blog.mall.cz/technologie/se-spravcem-hesel-budete-na-internetu-ve-vetsim-bezpeci-791.html

[74] LEE, Admond. P-values Explained By Data Scientist. Towards Data Science [online]. [cit. 2019-11-29]. Dostupné z: https://towardsdatascience.com/p-values-explained-by-data-scientist-f40a746cfc8

[75] Equa bank. Equa bank [online]. [cit. 2019-11-05]. Dostupné z: https://www.equabanking.cz/IBS/

[76] Zabezpečení a přihlašování. Facebook [online]. [cit. 2019-09-08]. Dostupné z: https://www.facebook.com/settings?tab=security

Seznam obrázků, grafů a tabulek

Obrázky

Grafy

Tabulky

Seznam příloh

Příloha 1 – Skript

```
import time
import re


count = 0
second = 0
ip = ""
ips = []
ipsUnique = []
ipUnique = 0
file = open('vstup.txt','r')
number = file.readlines()
for line in number:
  if "2019-10" in line:
    second = 0
  if "<td>" in line:
    second += 1
    if second == 2:
      for letter in line:
        address = re.sub('<td>|\s|</td>', '', line)
      ip = re.findall(r'[0-9]+(?:\.[0-9]+){3}', address)
      if ipsUnique == []:
        ipsUnique += ip
        if ip:
```

```
            count = 1
            ipUnique = 1
        else:
          count += 1
          if address not in ipsUnique:
            ipsUnique += ip
            ipUnique += 1
print("Unikátních adres je: ", ipUnique)
print("Celkový počet adres je: ", count)
time.sleep(15)
file.close()
```

Příloha 2 – Dotazník

1. Pohlaví (*)
    - Muž
    - Žena
2. Věk (*)
    - Do 30 let
    - Nad 30 let
3. Dokončené vzdělání (*)
    - Základní škola
    - Střední škola ukončena výučním listem
    - Střední škola ukončena maturitou
    - Vysokoškolské – bakalář
    - Vysokoškolské – magistr, inženýr
    - Jiné
4. Co Vás přimělo k otevření stránky? (*) #
    - Zaujal mě popis – text ve zprávě
    - Osoba odesílající odkaz
    - Otevírám vždy odkazy, které mi odešlou ‚přátelé'
    - Jiné
5. Kontrolujete na webových stránkách, zda je Vaše připojení zabezpečené? (*)
    - Ano
    - Ne
    - Nevím, co to znamená
6. Byla někdy Vaše osobní data ve virtuálním světě napadena nebo ukradena? (může se jednat o zneužití dat, profilů na sociálních sítích, dalších webových stránkách a účtech) (*)
    - Ano
    - Ne

Pokud respondent odpověděl Ano na 6. otázku

7. Kde Vám byla tato data odcizena? (*) #

- Facebook
- Instagram
- Twitter
- E-mail
- Jiné

8. Jak jste napadení řešil/a? (*)
9. Byly Vám následkem krádeže virtuální identity způsobeny nějaké problémy? Pokud ano, jaké? (např. pomluvy, poškození reputace...)

Pokračují všichni respondenti

10. Narazil/a jste někdy na podvodnou stránku? (*)
    - Ano
    - Ne
    - Nevím
11. Pokud ano, jak jste se zachoval/a?
12. Používáte pro různé účty různá hesla? (*)
    - Ano
    - Ne
    - Na některých účtech používám stejné heslo
13. Používáte správce hesel? (*)

V případě, že byl Váš účet napaden, prosím odpovídejte na níže položené otázky dle toho, jak byl nastaven Váš napadený účet. Pokud Váš účet nebyl napaden, vyberte si k zodpovězení otázek jeden z Vašich účtů - nejlépe účet na sociální síti.

14. Jak složité je Vaše heslo? Zvolte prosím všechny pravdivé možnosti. Obsahuje: (*) #
    - Malá písmena
    - Velká písmena
    - Čísla
    - Speciální znaky
15. Kolik znaků obsahuje Vaše heslo? Prosím napište číslici. (*)
16. Jak často měníte toto heslo? (*)

- Častěji než 1x za měsíc
- Nejpozději do 3 měsíců
- Nejpozději do půl roku
- Nejpozději do roka
- Měním heslo za dobu delší než 1 rok
- Nikdy

17. Používáte na tomto profilu vícefaktorovou autentizaci? (např. autorizační kód formou SMS, otisk prstu, osobní otázky apod.) (*)
    - Ano
    - Ne

(*) povinné pole

možnost zvolit více odpovědí

Další přílohy

Další přílohy – skript v pythonu, odpovědi z dotazníku, statistické zpracování dat z dotazníku pomocí aplikace Statistica – jsou přístupné jako přílohy této práce v databázi STAG provozované Jihočeskou univerzitou v Českých Budějovicích.