Bezpečnostní rizika při využívání smart technologií

Štěpán Rožek

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Štěpán Rožek**
Osobní číslo:	**A17698**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní rizika při využívání smart technologií**
Téma práce anglicky:	**Security Risks When Using Smart Technologies**

Zásady pro vypracování

1. Zpracujte rešerši literatury a pramenů k danému tématu.
2. Vymezte zkoumanou oblast (fenomenologie, etiologie) včetně právních aspektů.
3. Analyzujte aktuální rizika při využívání smart technologií.
4. Pro tvůrčí část bakalářské práce aplikujte syntézní postupy, výstupy analytické části využijte pro vlastní návrhy a opatření.
5. Výsledky zpracujte do grafů a tabulek.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary (online). AFCEA Praha, 2013, ISBN 978-80-7251-397-0.* Dostupné z: http://afcea.cajthaml.pfld.cz/wp-content/uploads/2015/03/Slovnik Final screen v2 0.pd.
2. STERLING, Bruce. *The hacker crackdown: law and disorder on the electronic frontier*. New York: Bantam Books, 1992. ISBN 05-530-8058-X.
3. *Measuring the Information Society Report Volume 1 2018 [online]*. Place des Nations CH-1211 Geneva 20 Switzerland: International Telecommunication Union, 2018 [cit. 2019-09-28]. ISBN 978-92-61-27231-9. Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf
4. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.
5. ČR, NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Důvodová zpráva k zákonu o kybernetické bezpečnosti (online)*. 1. Praha, 2013. Dostupné z: https://www.nbu.cz/downoload/nodeid-806/.

Vedoucí bakalářské práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **7. prosince 2019**
Termín odevzdání bakalářské práce: **25. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Ve Zlíně dne 7. prosince 2019

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne

Štěpán Rožek v. r
podpis diplomanta

ABSTRAKT

Bakalářská práce je věnována problematice rizik spojených s využíváním smart technologií. Teoretická část seznamuje širší veřejnost s aspekty kybernetické kriminality a souvisejícími bezpečnostními riziky. Zároveň informuje o rizikových způsobech chování v kyberprostoru, především na sociálních sítích a zásadách bezpečnosti při užívání smart technologií. Praktická část práce se zabývá phishingovým útokem mobilní přihlašovací stránky a osobního účtu Facebook a následnou analýzou získaných dat a informací, které Facebook za dobu mého používání této aplikace získal a mohly by v případě zneužití představovat bezpečnostní riziko. Dále poskytuje praktická doporučení, jak odhalit kybernetické hrozby pomocí online nástroje a postupy k zvýšení bezpečnosti a soukromí při používání aplikace Facebook.

Klíčová slova: smartphone, kyberkriminalita, kyberprostor, phishing, botnet, sociální sítě

ABSTRACT

The bachelor thesis is devoted to the issue of risks associated with the use of smart technologies. The theoretical part acquaints the wider public with aspects of cybercrime and related security risks. At the same time it informs about risky behavior in cyberspace, especially on social networks and principles of security when using smart technologies. The practical part of the thesis deals with the phishing attack of mobile login page and personal Facebook account and subsequent analysis of the data and information that Facebook acquired during my use of this application and could in case of misuse be a security risk. It also provides practical recommendations on how to detect cyber threats using an online tool and procedures to increase security and privacy when using Facebook application.

Keywords: smartphone, cybercrime, cyberspace, phishing, botnet, social networks

Mé poděkování patří především PhDr. Mgr. Stanislavu Zelinkovi za věcné rady a připomínky, které mi během psaní této bakalářské práce poskytoval. Dále bych chtěl poděkovat svým služebním nadřízeným a kolegům, kteří mě ve studiu podporovali i v této nelehké době. V neposlední řadě patří velký dík za podporu také mé snoubence Monice a rodině.

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

OBSAH

ÚVOD

Dnešní vyspělá doba internetu a různých smart (chytrých) zařízení připojených do internetu nám nabízí spoustu možností jejich využití a bezesporu nám tyto technologie usnadňují život. Můžeme rychle a efektivně komunikovat s člověkem na opačné straně zeměkoule i včetně přenosu videa v reálném čase, seznamovat se s novými lidmi, sdílet společné zážitky a fotografie na sociálních sítích, ale i využívat tyto chytré technologie k provádění plateb a ovládání dalších smart zařízení, které se například starají o naši domácnost, a mít tak přehled o všem, co se u nás doma děje pomocí chytrého telefonu, který se stal neoddělitelnou součástí života většiny mladých, ale i starších lidí a dětí. Mohlo by se zdát, že žijeme v takřka ideální době a smart technologie poskytují samé výhody, ale opak je pravdou. Jelikož tato zařízení mají přístup k internetu, existují zde hrozby v podobě kybernetických útoků a útočníků, které pro uživatele představují různá bezpečnostní rizika. Motivace původců těchto útoků se mění v závislosti na druhu vykonávané kybernetické kriminality. Z velké části jde útočníkům o finanční zisk na základě získaných dat uživatele a zneužití jeho neznalosti či důvěry. V jiných případech, je jejich cílem například vyřadit z provozu systémy organizací či firem hromadnými útoky, skrze zneužitá chytrá zařízení anebo vyvolat určitým způsobem nátlak na lehce zmanipulovatelnou osobu, např. nezletilé dítě, které se stalo terčem útočníka na sociálních sítích a přimět ji k provedení činnosti, jako je v častých případech zaslání obnažených fotografií, díky níž útočník získává sexuální uspokojení a určitou moc nad obětí, kdy tyto materiály později může používat jako prostředky k vydírání a tzv. „kyberšikany“.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE (ICT)

K tomu, aby vůbec k páchání kybernetických útoků a s tím souvisejícím bezpečnostním rizikům docházelo, je za potřebí využití nehmotného, virtuálního prostředí, které zprostředkovávají zařízení s přístupem do sítě internet. [1] Toto prostředí dává pachatelům široké pole působnosti a za určitých okolností i dostatek anonymity, což je pro kyberzločince velkou výhodou oproti konání trestné činnosti v reálném světě, kde je riziko odhalení totožnosti bezesporu vyšší. [2]

1.1 Internet

„*Internet je decentralizovaná celosvětová síť spojující počítače různých vlastníků, která je odolná proti výpadku jedné nebo několika částí. Umožňuje sdílení dat, používání e-mailu a mnoho dalších služeb. Internet nekontroluje žádná autorita a celý systém je vybudován tak, aby se řídil sám.*“ [3]

Jednotlivá zařízení v této síti mezi sebou komunikují pomocí protokolů TCP/IP. Mezi desítkami služeb, které internet poskytuje je nutno zmínit službu WWW (World Wide Web), která je kombinací textů a grafiky vzájemně propojenými hypertextovými odkazy a služba elektronické pošty známé jako email. Cílem této sítě je zajištění rychlé a bezchybné výměny dat mezi uživateli (komunikace). [4]

1.1.1 **Historie a současnost**

První zmínky o internetu sahají na přelom 50. a 60. let, kdy Ministerstvo obrany Spojených států zadalo požadavek na vytvoření datové sítě, která nebude závislá na centrálním prvku v případě zničení některých částí a bude nadále funkční díky svému nezávislému propojení. V roce 1969 začíná vývoj sítě s názvem ARPANET, která se rychle rozšířila už v roce 1973 až za hranice, přesněji do Velké Británie a Norska. Díky finančním dotacím se vývoj zrychluje a rodí se protokol TCP/IP (používaný dodnes), který je veřejně dostupný a připojují se další počítače a sítě. Následkem tohoto vývoje vznikla globální síť, kterou dnes známe pod pojmem internet. [3]

Za oficiální připojení České republiky (Československa) k internetu se považuje rok 1992, kdy došlo k připojení sálového počítače IBM 4341, pomocí pronajatého pevného telefonního okruhu vedoucího z ČVUT na Univerzitu Jana Keplera v rakouském Linci a Československo se tímto krokem stalo 39. zemí připojenou do globální sítě internet. [5]

V současné době, dle údajů, které zveřejnil Český statistický úřad, bylo v roce 2018 připojeno do sítě internet 4/5 českých domácností. [6] Mezinárodní telekomunikační unie (ITU) ve své výroční zprávě uvádí informaci, že k síti internet bylo v témže roce připojeno více než polovina světové populace (51,2 %). [7]

1.2 Kyberprostor

Jelikož prozatím neexistuje jedna konkrétní definice kyberprostoru, považujme ho tedy za jakýsi virtuální (nehmotný) svět plný informací tvořen vzájemným propojením informačních a komunikačních systémů, který nám umožňuje vzájemně komunikovat, vytvářet, využívat a ukládat informace. Zahrnuje tak všechny vzájemně propojené počítače, zařízení a databáze připojené do celosvětové sítě internet. [1], [8]

Zákon o Kybernetické bezpečnosti č. 181/2014 Sb. vykládá tento pojem následovně:

„*Kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“ [9]

Další definicí kyberprostoru dle knihy CyberSecurity je:

„*Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.*“ [10]

Představit si kyberprostor lze také na příkladu podle britského spisovatele Bruce Sterlinga z roku 1982. Definuje jej jako místo, kde se nachází telefonní konverzace. Není to ani v telefonu, ze kterého voláme, ani v telefonu příjemce hovoru, ale někde mezi nimi. [11]

1.3 Smart zařízení a Internet věcí (IoT)

Za smart zařízení, v překladu do češtiny „chytrá zařízení“, jsou považována všechna zařízení, která jsou schopna se připojit do sítí či komunikovat s dalšími zařízeními pomocí bezdrátových technologií. Díky své interaktivitě mají uživateli pomáhat a ulehčovat běžné denní činnosti včetně možnosti vzdálené komunikace a ovládání. Většina těchto chytrých zařízení jsou v podobě osobní spotřební elektroniky, jako jsou chytré mobilní telefony (smartphony), tablety, chytré hodinky, chytré brýle, chytré televize apod. [12]

Nicméně patří sem i méně známá chytrá zařízení, která se však v dnešní době velice rychle vyvíjí. Jedná se například o chytré lednice, žárovky, zásuvky, chytré termostaty, ale i chytré zvonky či zámky, dětské chůvičky, vysavače apod. [13]

Všechna tato zařízení a mnoho dalších, která jsou schopna sbírat a odesílat data například do aplikace v našem chytrém telefonu a vzájemně komunikovat pomocí bezdrátových sítí, spolu tvoří síť, kterou nazýváme Internet věcí, v překladu Internet of Things – IoT. [14]

Obr. 1. Internet věcí – IoT [15]

Statistiky z roku 2019 uvádí, že k této rychle rostoucí síti bylo připojeno více než 26 miliard zařízení a podle odhadů bude jejich počet v roce 2025 skoro trojnásobný. [16]

Na každé takové zařízení, které je připojené a schopné komunikovat po síti internet, mohou působit hrozby v podobě kybernetických útoků, jejichž cílem je získat nad daným zařízením plnou kontrolu či získat přístup k citlivým datům. [14]

1.3.1 **Chytrá domácnost (Smart home)**

Kniha Inside the Smart Home definuje chytrou domácnost jako:

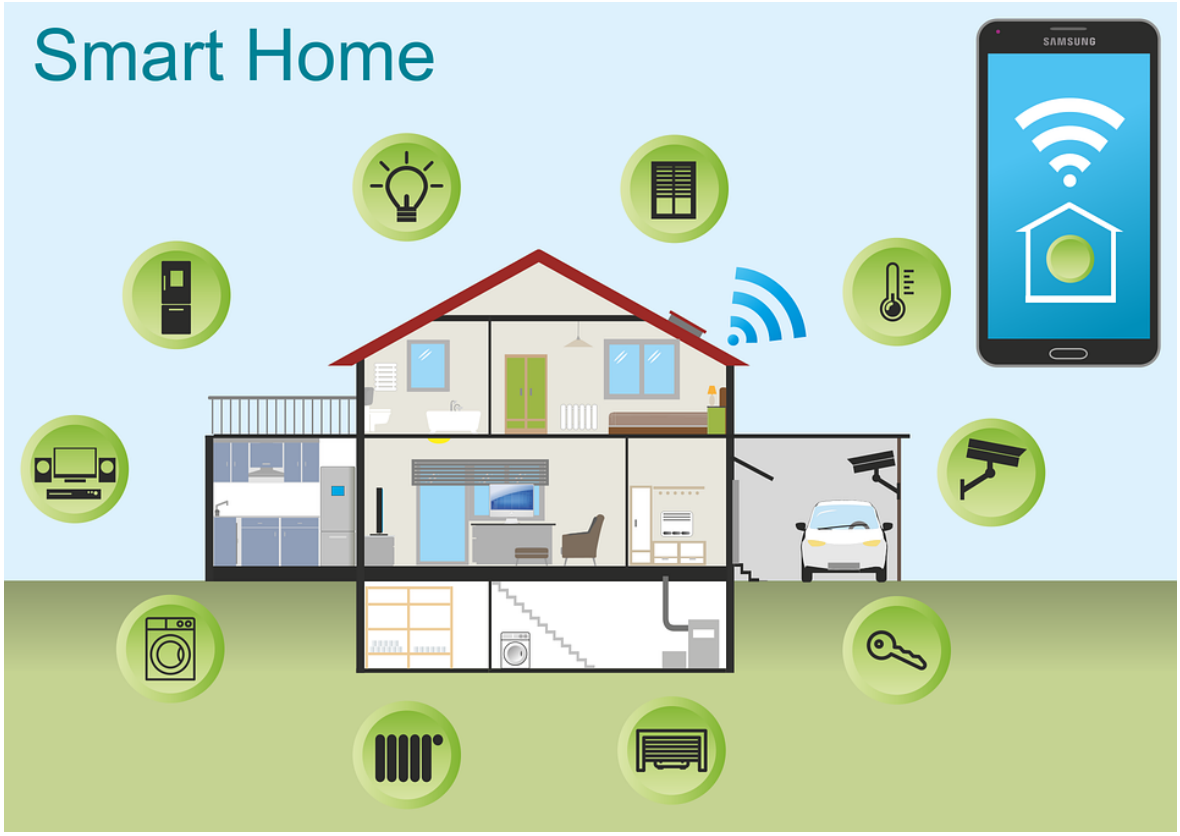
„*Domácnost, která je vybavena výpočetními a informačními technologiemi, které předvídají a odpovídají potřebám obyvatelům domácnosti, zajišťují komfort, zábavu a bezpečí prostřednictvím správy technologií v domácnosti a propojení s okolním světem.*“ [17]

Jak již bylo zmíněno, chytrá zařízení mají uživatelům pomáhat v denních aktivitách a šetřit čas a případně i peníze. Přes aplikaci v našem smartphonu si nastavíme požadovanou teplotu na našem chytrém termostatu a po příjezdu domů máme dům vyhřátý či vychlazený. Připojíme se k bezpečnostním zařízením a systémům, které monitorují prostory domácnosti, máme možnost živého sledování kamer a jejich ovládání, zhasínání či rozsvěcování světel, zatahování rolet, informace o zásobách v lednici, až po sledování našich ratolestí pomocí dětských chůviček. Množství výhod a funkcí chytrých zařízení je opravdu široká škála, ale měli bychom mít i povědomí o druhé, temné straně těchto zařízení, kterou je možnost zneužití těchto smart technologií. [14] Jsou známy případy, kdy útočníci získali přístup k zařízením v chytrých domácnostech a převzali kontrolu nad kamerami, termostaty či audio systémem apod. Útočníci tak například v domácnosti pomocí napadených chytrých zařízení nastavovali vysoké teploty a pouštěli hlasitou hudbu s vulgárním kontextem. [18] Scénářů, které se tedy mohou díky zneužití těchto chytrých zařízení odehrát si můžeme představit několik:

- kamerový systému – sledování – odhalení soukromí
- dveřní zámkové systémy – odemčení – krádeže
- chytrý vysavač – sledování prostoru domácnosti
- lednice – vypnutí – zkažení potravin
- termostat – nastavení vysokých teplot – možnost vzniku požáru

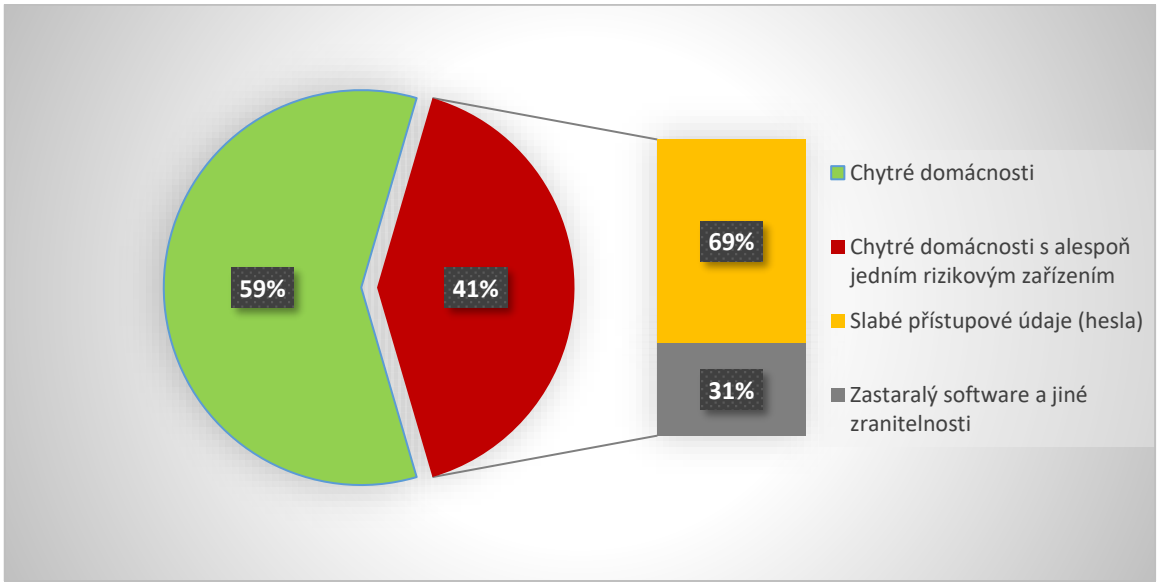
  a další…

Avšak zneužití například zmíněného chytrého termostatu v sobě neskrývá jen riziko přetopené domácnosti, či v extrémním případě vznik požáru. Vzhledem ke skutečnosti, že toto zařízení lze uživatelem naprogramovat tak, aby udržovalo teplotu na určité úrovni, když je majitel či rodina v domě, může být nastaven i režim, kdy není třeba domácnost udržovat „v teple“. Příkladem může být odjezd rodiny na zimní dovolenou. Tento údaj o teplotě může představovat bezpečnostní riziko, jelikož útočník se pomocí této informace dozvídá, zda je dům prázdný či nikoliv a zvyšuje se tedy riziko vykradení domácnosti. [19]



Obr. 2. Smart home – chytrá domácnost [20]

Společnost Avast, která je jedním z největších poskytovatelů kybernetického zabezpečení, prováděla analýzu více než 16 milionů „chytrých domácností“, při které zjistila, že dvě z pěti chytrých domácností má připojeno alespoň jedno chytré zařízení, které není dostatečně zabezpečené proti kybernetickým útokům a představuje tak bezpečnostní riziko pro všechna zařízení v síti dané chytré domácnosti. Ze statistik taktéž vyplývá, že největší bezpečnostní rizika představovaly pro chytré domácnosti slabé a snadno uhodnutelné přístupové údaje k jednotlivým zařízením a hned poté následoval neaktuální software zařízení. [21], [22]



Obr. 3. Bezpečnostní rizika chytrých domácností [22]

1.3.2 **Router – dveře do chytré domácnosti**

Router, česky „směrovač“, je síťové zařízení, které slouží k propojení dvou anebo více počítačových sítí a následnému předávání (směrování) datových paketů. [23] V případě chytré domácnosti tedy komunikuje mezi internetem a jednotlivými zařízeními, která jsou do této sítě připojeny. [24] Lze jej tedy považovat za pomyslnou „bránu k internetu“. V případě, že je toto zařízení nedostatečně zabezpečeno, je tedy zranitelné vůči kybernetickým útokům a představuje riziko pro všechna zařízení, která jsou v dané chytré domácnosti připojena. Dle statistiky společnosti Avast bylo zjištěno, že bezmála 60 % routerů má slabé přihlašovací údaje, především heslo anebo jinou zranitelnost, jako je například zastaralý software. Alarmující je taktéž fakt, že stejné procento uživatelů se nikdy nepřihlásilo do administračního prostředí routeru pro změnu hesla či aktualizaci softwaru zařízení. [22] Není tedy těžké si představit, že v případě prolomení ochrany tohoto prvku chytré domácnosti může dojít k neoprávněnému přístupu třetí osoby k naší síťové komunikaci, osobním informacím a datům, který může vést ke krádeži identity a následným podvodům, instalací škodlivých kódů (malware) či napadání a zneužívání dalších zařízení apod. [25]

1.3.3 Chytrý telefon (smartphone)

Nejčastější smart zařízení, které denně využívá většina z nás. Chytrý telefon neboli „smartphone“, je mobilní telefon především s dotykovým displejem, který používá operační systém, a kromě telefonování či zasílání textových SMS zpráv poskytuje uživateli mnoho dalších funkcí. Patří mezi ně například pořizování fotografií či videí pomocí vestavěného fotoaparátu, surfování na internetu, hraní her, používání sociálních sítí, čtení a odesílání mailů, navigování pomocí GPS či využívání spousty různých aplikací třetích stran včetně mobilního bankovnictví a provádění plateb. Mezi dva nejvíce využívané operační systémy patří Android a iOS. [26]

Android – operační systém, který je veden společností Google, ale zdrojový kód je poskytován jako tzv. open source, což znamená, že je veřejně přístupný a lze jej tedy upravovat a vytvářet vlastní varianty pro různá zařízení. [27] Dle statistik využívá tento operační systém celosvětově bezmála 76 % smartphonů. [28] Pro instalaci aplikací je vyhrazená aplikace Google Play Store, avšak instalovat je lze i mimo tento prostředek, což však zvyšuje riziko zneužití takového zařízení.

Tento operační systém obsahují i telefony značky Huawei a ZTE, kterých se týkala nedávná mediální kauza, díky které je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), označil za kybernetickou hrozbu a vydal varování před možnými bezpečnostními riziky plynoucími z využívání těchto chytrých zařízení. Zároveň doporučil tato zařízení nepoužívat. Především se varování týkalo možných odposlechů hovorů, přístup k datům či lokalizace uživatelů až krádeží identity. [29]

iOS – operační systém, který vytvořila společnost Apple a je určen pouze pro zařízení pod touto značkou. Chytré telefony s tímto operačním systémem známe pod názvem iPhone. [30] Celosvětově tento operační systém používá necelých 23% zařízení. [28] Místo, odkud je možné stahovat a instalovat aplikace pro tato zařízení se nazývá App Store.

Vzhledem k stále větší dostupnosti internetu a rychlosti růstu počtu chytrých zařízení lze předpokládat, že se stanou běžnou součástí, dá se říci, každého jednotlivce i domácnosti. Statistiky však stále dokazují, že poměrná část uživatelů těchto zařízení nedbá na jejich dostatečné zabezpečení a vystavují se tak riziku jejich zneužití.

2 KYBERNETICKÁ KRIMINALITA

Způsobů, jak zneužít chytrá zařízení a uživatele s přístupem do sítě internet je velké množství. Hrozby působí na uživatele, dá se říci, na každém „kroku“, který v rámci internetu provede. Ať už se jedná o čtení emailů, sledování videí, stahování a používání aplikací či využívání sociálních sítí. Definovat lze tedy kybernetickou kriminalitu jako „*jednání namířené proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu.*“ [10]

2.1 Sociální inženýrství

Je definováno jako „*Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.“* [31] Jedná se tedy o manipulační či přesvědčovací techniku, kterou používají hackeři nebo jen obyčejní podvodníci na uživatele, který se stal obětí jejich útoku, provedeného skrze chytré zařízení a internet. Cílem sociálního inženýrství v oblasti kyberkriminality je tedy *„v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je.*“ [2] Využívá se tedy neznalosti či důvěry největší slabiny všech bezpečnostních systémů – člověka (uživatele), který v případě vhodně zvolené techniky sociálního inženýrství dobrovolně vyzradí například hesla či jiné citlivé informace při provedení určité akce. [2]

2.2 Hackeři a jejich dělení

Slovo „hacker“ je veřejnosti poměrně známé, ale ne zcela všichni chápou plně jeho pravý význam. Většina z nás si tento pojem spojí s osobou, která pomocí informačních technologií provádí útoky na různé cíle a způsobuje škody. Definice tohoto slova dle Výkladového slovníku kybernetické bezpečnosti zní následovně:

„*Osoba, která se zabývá studiem a prozkoumáváním detailů programovatelných systémů nejčastěji pro intelektuální zvídavost a tuto schopnost si neustále zdokonaluje.*“ [31]

Je tedy zřejmé, že pojem „hacker“ nemusí být nutně označení pro útočníka, který se snaží využívat své znalosti k páchání škod, ale i pro užitečnou osobu, která se velmi dobře orientuje v oblasti informačních technologií a být tak v mnohých případech velice prospěšnou a žádanou. Hackery proto můžeme rozdělit do tří základních skupin dle jejich zaměření a způsobu vykonávání své činnosti. [2]

White Hat

Jedná se o tzv. etické „hodné“ hackery, kteří jsou často zaměstnáváni či najímáni společnostmi. Jejich činností je napadání a prolamování bezpečnostních opatření různých systémů s cílem vyhledávání bezpečnostních slabin. Jde tedy o hackery, kteří pomáhají subjektům odhalovat slabá místa v jejich systémech a navrhují řešení k odstranění nedostatků v bezpečnostních opatřeních. Činnost této skupiny hackerů tedy nemá žádný kriminální podtext. [32]

Black Hat

Tato skupina hackerů je pravým opakem etických hackerů (White Hat). Dle terminologie se označují i jako tzv. crackeři – odvozeno od anglického slova crack – prolomit. [31] Jsou to právě ti „zlí hackeři“, o kterých se mezi veřejností a v médiích hovoří v souvislosti s hackerskými útoky a kyberkriminalitou.

„Jejich motivací je snaha způsobit uživateli napadeného systému škodu či jinou újmu, resp. získat majetkový nebo jiný prospěch. Mimo vlastní realizaci prolomení napadeného systému je v jejich jednání patrný ještě další, kriminální prvek.“ [2]

Za tyto prvky můžeme označit například tvorbu a šíření škodlivých kódů, krádeže dat či finančních prostředků a následné vydírání atd. [2]

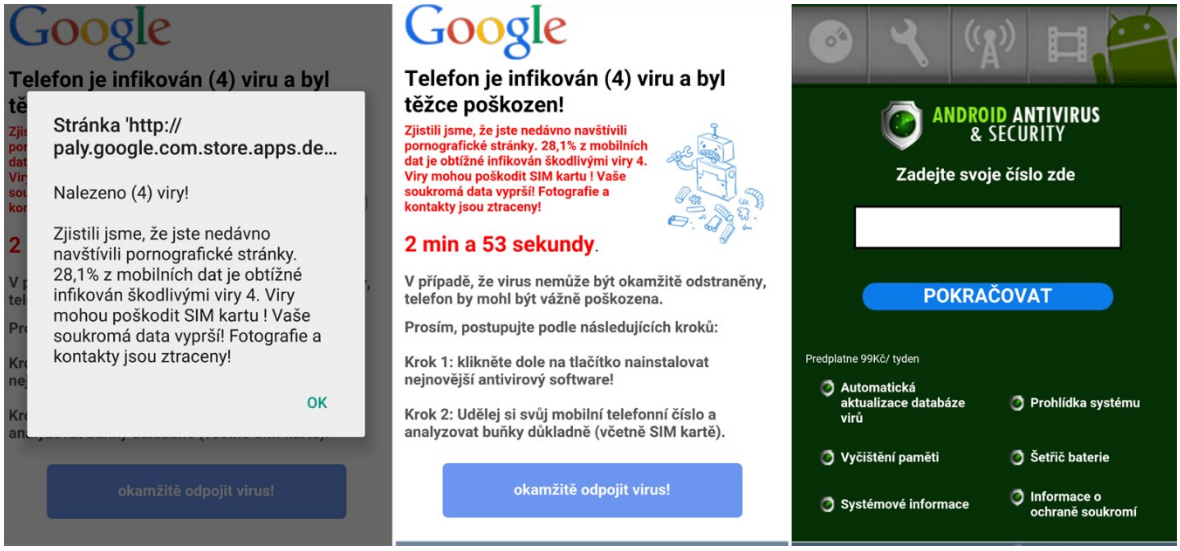
Gray Hat

Do této skupiny hackerů, která značí „šedou zónu“ patří osoby, které svými aktivitami působí na rozmezí předešlých dvou skupin. [2] Tito hackeři například provádějí útoky a zneužívají slabin v systému, avšak bez předchozího uvědomění či souhlasu napadeného subjektu. V případě, že se podaří najít způsob jakým prolomit bezpečnostní opatření systému, oznámí tuto skutečnost oprávněným osobám daného subjektu a za úplatu nabídnou řešení k ochraně před dalšími útoky. [33]

2.3 Malware

Malicious software, zkráceně malware, je obecný výraz pro jakýkoliv škodlivý program, kód či aplikaci. [31] Druhů malware existuje několik a liší se od sebe způsobem, jakým se chovají v napadeném zařízení a co je jejich cílem. Dle statistik společnosti Kaspersky, která se zabývá otázkou kyberbezpečnosti, bylo zjištěno, že v roce 2018 se s určitým druhem malware pro chytrá zařízení, především smartphonů, setkalo přibližně 10 milionů uživatelů.

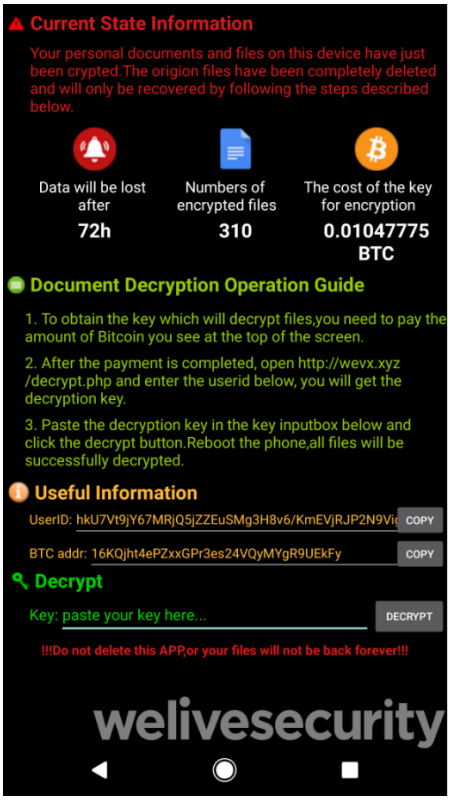
Největší nárust byl zaznamenán u tzv. Trojan dropperů, které do infikovaného zařízení instalují další škodlivé kódy, například Trojské koně určené k napadání mobilního bankovnictví či ransomware. [34]



Obr. 4. Falešná výzva k instalaci podvodné aplikace k odstranění malware [35]

Ransomware

Ransomware je typ malware, který je specifický v tom, že v napadeném zařízení zašifruje data, či uzamkne uživatelské prostředí a za rozšifrování či odemknutí požaduje po uživateli zaplatit „výkupné“. Často bývá tato výzva k zaplacení umocněna zobrazeným časovým limitem pro ještě větší nátlak na oběť tohoto útoku. V případě, že úhrada výkupného neproběhne, dojde ke nenávratnému zašifrování či smazání dat. [36] Příkladem může být ransomware s názvem Android/Filecoder.C, který se začal šířit začátkem července 2019 na různých internetových fórech za pomocí odkazu na aplikaci pro systém Android. Útočníci lákali uživatele na určitý pornografický materiál, který měl být dostupný po instalaci této aplikace. U uživatelů, kteří si na daném odkazu do zařízení stáhnuli a nainstalovali danou aplikaci, došlo k zašifrování souborů s výzvou k zaplacení určité částky. Mimo tuto skutečnost docházelo k šíření tohoto typu malware pomocí SMS zprávy, kterou napadené chytré zařízení rozeslalo všem kontaktům. [37]



Obr. 5. Ukázka ransomware – Android/Filecoder.C [38]

Spyware

Jedná se o malware, který má za úkol sledovat činnost, kterou na daném zařízení uživatel provádí s cílem získávat různá data. [39] Dochází například ke sledování nejčastěji navštěvovaných webových stránek, spouštěných aplikacích, ale i informací osobního charakteru. Tato data jsou následně odesílána původci tohoto malware. [2] Sesbíraná data poté mohou posloužit k lepšímu cílení reklamy na uživatele. Větší bezpečnostní riziko však může představovat ten typ spyware, který je schopný získat přístup ke kameře či mikrofonu chytrého zařízení, což může vést až ke krádeži identity uživatele či průmyslové špionáži. [40]

Viry

Virus je typ malware, který je schopný se sám šířit či mutovat a často bývá spuštěn spolu s jinou aplikací. [31] Na smartphonech se viry nejčastěji vyskytují pro operační systém Android. Oproti tomu na zařízeních s iOS je jejich výskyt poměrně vzácný. Cílem viru je z napadeného zařízení odcizit citlivá data, která útočníci mohou využít pro finanční zisk.

Viry dokáží například i nahrávat telefonní hovory a číst či odesílat zprávy. Bez vědomí uživatele tak dochází k odesílání SMS zpráv na prémiová telefonní čísla a tím k finanční ztrátě oběti takto napadeného chytrého zařízení, a naopak zisku na straně původce viru. [41]

Trojský kůň

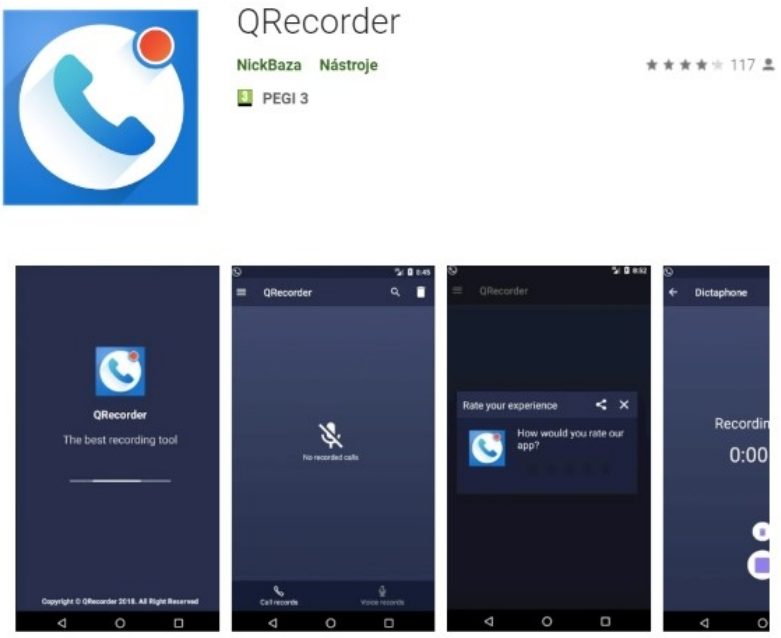
Definice Trojského koně dle výkladového slovníku kybernetické bezpečnosti zní následovně:

„*Program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelné užitné funkci, kterou poskytuje.*“ [31]

Trojský kůň tedy může vypadat jako obyčejná aplikace například v podobě antiviru (aplikace pro odstranění malware) či přílohy v emailu. Po spuštění dochází k instalaci malware do zařízení a následnému páchání škod podle toho, k čemu byl Trojský kůň vytvořen. Typů Trojských koní existuje velké množství, avšak za zmínku stojí například Trojský kůň zaměřený na bankovnictví, který se soustředí hlavně na krádeže údajů kreditních karet a dalších dat týkajících se oblasti financí a plateb. [42]

Známým případem byla aplikace CamScanner, která dle oficiálního obchodu Google Play dosáhla přes 100 milionů stažení do chytrého telefonu či jiného zařízení. Aplikace sloužila ke tvorbě PDF dokumentů pomocí fotoaparátu a funkce OCR neboli optického rozpoznávání znaků. První verze aplikace byly „čisté“, avšak v průběhu aktualizování a vylepšování aplikace došlo i k implementaci malware, který uživatelům v nabízel nežádoucí reklamy či nutil uživatele k jiným placeným službám. [43]

Další aplikací představující bezpečnostní riziko byla volně dostupná aplikace QRecorder, sloužící k nahrávání hovorů. Po aktualizaci se stala Trojským koněm a v telefonu zjišťovala, zda má uživatel nainstalované především bankovní aplikace. Jestliže byl výsledek hledání pozitivní, proběhlo stažení dalšího malware, který měl za úkol číst přihlašovací údaje a v neposlední řadě i číst SMS zprávy, což umožnilo plný přístup k internetovému bankovnictví, i přes existenci dvoufázové autentizace. [44]



Obr. 6. Riziková aplikace QRecorder [45]

Malware útoky, lze vzhledem k jejich společenské škodlivosti, postihovat podle ustanovení Trestního zákoníku č. 40/2009 Sb., na základě naplnění skutkové podstaty následujících trestných činů:

- Neoprávněný přístup k počítačovému systému a nosiči informací, dle § 230, zákona č. 40/2009 Sb.,
- Porušení tajemství dopravovaných zpráv, dle § 182, zákona č. 40/2009 Sb.,
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, dle § 231, zákona č. 40/2009 Sb.,
- Vydírání, podle § 175, zákona č. 40/2009 Sb.

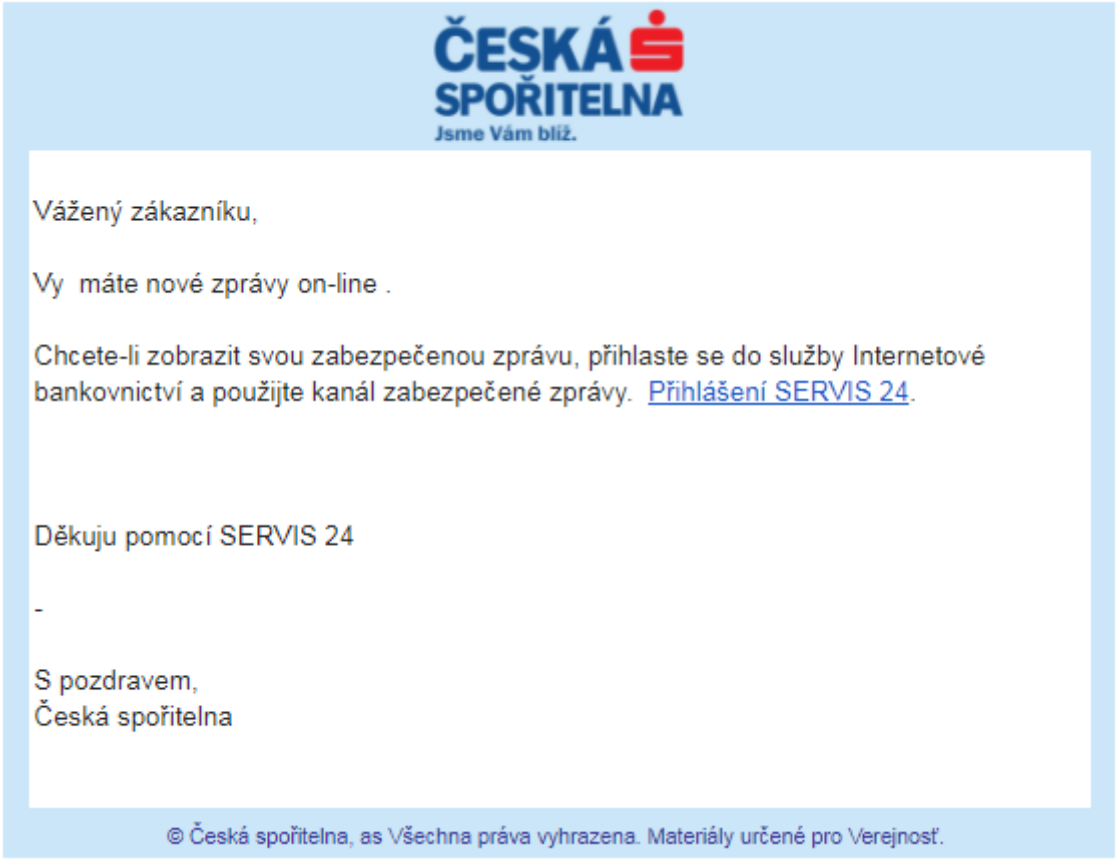
V závislosti na rozsahu, způsobených škodách a způsobu provedení, se trest v podobě odnětí svobody pohybuje od 6 měsíců do 8 let. [2], [46]

2.4 Phishing

Jedná se o velmi častý projev kyberkriminality, kdy se využívá technika sociálního inženýrství, kterou útočníci zneužívají k získání cenných informací oběti. Jelikož se skrze chytrá zařízení uživatelé přihlašují do různých aplikací a online služeb či provádí finanční transakce, představuje phishing poměrně velké bezpečnostní riziko v případě zmocnění se

důležitých údajů útočníkem. Mezi tyto údaje patří například údaje o kreditních kartách či přístupová hesla a jména k různým službám jako internetové bankovnictví, sociální sítě, email apod. Populární formou šíření phishingu je skrze mailovou komunikaci, kdy uživatel obdrží zprávu, která se například vydává za důležitou zprávu z banky, týkající se zabezpečení účtu a změny hesla. Mailová zpráva zpravidla obsahuje odkaz na podvodnou webovou stránku, která je identická s tou, kterou uživatel považuje za důvěryhodnou. V okamžiku, kdy dojde uživatelem k vyplnění požadovaných údajů na podvodné webové stránce, dochází k odeslání těchto citlivých informací k útočníkovi. [47]

Obr. 7. Phishing zaměřený na klienty Raiffeisenbank ČR - nenechte se nachytat, odkazy vedou na podvodné stránky. [48]



Obr. 8. Podvodný email vydávající se za Českou spořitelnu [49]

Jelikož v dnešní době, dá se říct, všechny banky poskytující internetové bankovnictví mají zavedený systém dvoufaktorové autentizace, který většinou spočívá v zadání hesla a následně potvrzení přihlášení skrze SMS kód zaslaný do mobilního telefonu, je k dokončení útoku a získání plného přístupu k bankovnímu účtu oběti získat právě i tento SMS kód. Poté, co tedy oběť vyplnila na podvodné webové stránce své přihlašovací údaje a došlo tedy k jejich odeslání k útočníkovi, následoval další krok v podobě přesvědčení uživatele ke stažení aplikace pod záminkou zvýšení bezpečnosti spojení. Tato aplikace však pro operační systém Android obsahovala malware, který byl určený právě ke čtení a skrytému přeposílání autentizačních SMS zpráv (aniž by oběť na SMS byla upozorněna). Útočník tak získal plný přístup k internetovému bankovnictví oběti a provádění finančních transakcí. [2]

Obr. 9. Výzva ke stažení aplikace ke čtení a přeposílání autentizačních SMS obsahující malware [2]

2.4.1 Osobní zkušenost s phishingem

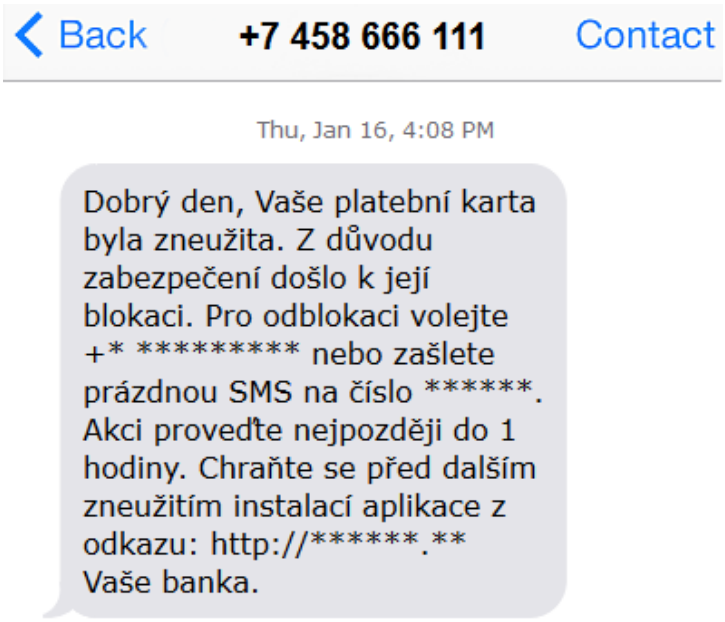
Bohužel i já osobně jsem se v roce 2015 stal obětí phishingu. Využíval jsem internetovou peněženku, na které jsem měl uložené určité finanční prostředky, které jsem využíval k bezhotovostním platbám na internetu. Jednoho večera jsem na svůj chytrý telefon obdržel mailovou zprávu, právě v podobném znění, jako uváděné příklady výše. Zpráva nabádala ke kliknutí na odkaz a změnu hesla, jelikož údajně došlo k neoprávněnému přístupu k mému účtu. Bohužel ve stresu a snaze, co nejrychleji ochránit své finance, jsem ani nezkontroloval odesílatele této zprávy, ani URL adresu, a na podvržené, totožně vypadající webové stránce peněženky, jsem zadal své přihlašovací údaje. Asi dvě minuty po této akci jsem obdržel zprávu, že došlo k převodu 1153 $, tedy v přepočtu cca 26 000 Kč na účet U7993376 vedený pod jménem Valeriy Green.

Created ↓	Action	Batch	From/To Account	Amount	Fees	Balance	Details
21:08 07.09.15	Transfer	[redacted]	U7993376 valeriygreen	-1153.62	5.73945	[redacted]	Sent Payment 1147.89 USD to account U7993376.

Obr. 10. Odcizené finanční prostředky [archiv autora]

SMiShing

Jak již může být z názvu patrné, jedná se o druh phishingu, který útočníci provádí skrze SMS zprávy. Příkladem SMiShingu může být opět zpráva, která se vydává za bankovní společnost a upozorňuje, že došlo k blokaci kreditní karty a pro její reaktivaci je třeba poslat SMS zprávu či zavolat na některé z uvedených čísel, které jsou však zpoplatněnou službou. Útočník tedy inkasuje určitý zisk z této zprávy či hovoru. Touto formou phishingu však lze šířit i URL odkazy, které vnucují instalaci malware. [2]



Obr. 11. Příklad SMiShingu [archiv autora]

Na příkladu této SMS lze pozorovat, že je vyvíjen nátlak na uživatele i pomocí časové lhůty, kterou je potřeba splnit. Ideální obětí pro původce tohoto útoku je tedy méně znalý uživatel, který po obdržení této textové zprávy ve snaze ochránit své finance splní všechny požadavky, ke kterým je vyzván. Po odeslání SMS či hovoru dochází ke stržení peněz z kreditu a případně i napadení zařízení malwarem z nainstalované aplikace.

Phishing tedy obecně můžeme z právního hlediska považovat za naplnění skutkové podstaty následujících trestných činů:

- Podvod, dle § 209, zákona č. 40/2009 Sb.,
- Neoprávněný přístup k počítačovému systému a nosiči informací, podle § 230 odst. 2, zákona č. 40/2009 Sb.,
- Neoprávněné opatření, padělání a pozměnění platebního prostředku, podle § 234, zákona č. 40/2009 Sb.

V případě uznání viny lze uložit tresty odnětí svobody dle rozsahu, způsobů páchání trestné činnosti a způsobených škod v rozmezí 6 měsíců až 12 let nebo trestem v podobě zákazu činnosti či propadnutí věci. [2], [46]

2.5 Sniffing

Jde o metodu, kterou využívají kybernetičtí útočníci k zachycování dat přenášených mezi chytrým zařízením a službou, ke které uživatel skrze toto zařízení přistupuje. Jinými slovy řečeno, jedná se o jakýsi odposlech komunikace, při kterém se útočník snaží bez souhlasu uživatele získat citlivé informace, nejčastěji v podobě přihlašovacích jmen a hesel či zpráv posílaných přes různé komunikační aplikace či služby. [2] Útočníci pro provádění tohoto druhu kybernetické kriminality často využívají veřejné a nezabezpečené Wi-Fi sítě, ke kterým se připojuje velké množství uživatelů a zařízení. Jedná se především o kavárny, letiště, hotely apod. Využívá se tedy neopatrnosti uživatelů, kteří na svých chytrých zařízeních připojených k internetu skrze tyto přístupové body využívají aplikace a služby, jejichž zneužití může mít závažné následky. [50]

Podle trestního práva lze takovéto nelegální zachycování přenášených dat považovat za naplnění skutkové podstaty trestného činu Porušení tajemství dopravovaných zpráv, dle § 182 trestního zákoníku č. 40/2009 Sb., za což pachateli hrozí zákaz činnosti či odnětí svobody až na dva roky. [46]

2.6 Botnet útoky

Každé chytré zařízení, které bylo infikováno tzv. botem neboli kódem, který umožňuje útočníkovi dané zařízení na dálku ovládat pomocí příkazů je součástí tzv. botnet sítě. Tato síť může být tvořena v některých případech až stovkami tisíc napadnutých chytrých zařízení, které se označují jako zombie. Znamená to tedy, že chytré telefony, televize, pračka,

termostaty i vysavač mohou být na povel zneužity ke hromadným útokům na různé cíle, od obyčejných webových stránek, až po sítě bank, nemocnic či státních organizací. Tyto útoky jsou nazývány jako DoS či DDoS. Zjednodušeně řečeno, každé takové zařízení v botnet síti začne přistupovat a vysílat velké množství požadavků například na určitou webovou stránku, což má za následek přetížení serveru a jeho nedostupnost. Během těchto útoků dochází často k šíření různých typů malware, především vyděračského ransomware.

Ukázkovým příkladem tak mohou být nedávné útoky na nemocnice, kdy došlo k vyřazení z provozu části či celé sítě. Nemocnice tak rázem řeší problém s nedostupností sítě, zároveň vydírání přes zašifrovaná citlivá data o pacientech. Tyto útoky je taktéž možné objednat na černém trhu i s možností zvolení délky trvání útoku. Cena DDoS útoku se pohybuje průměrně 1500 Kč za hodinu, což je v poměru s následky takového útoku pakatel. Identifikace pachatele, který tyto zařízení ovládal či dal k pokyn k útoku je v tomto případě velmi obtížná, jelikož na útocích se podílí často velké množství napadených zařízení, zpravidla bez vědomí jejich uživatele.

Z hlediska práva lze botnet útoky posuzovat jako trestný čin – Neoprávněný přístup k počítačovému systému a nosiči informací, zejména potlačení dat a jejich neupotřebitelnosti, podle § 230, zákona č. 40/2009 Sb. [2], [39], [51], [46]

2.7 Krádež identity

Za krádež identity je v kybernetické kriminalitě považován protiprávní čin, kdy je oběti odcizena identita a dochází k jejímu zneužívání. V podstatě jde o páchání trestných činů díky získaným osobním a citlivým informacím, jménem oběti. Útočník tedy může na základě odcizené identity například páchat podvody na další uživatele, kteří s ním komunikují a vyměňují si citlivá data či údaje v domněním, že se jedná o pravou osobu, kterou dobře znají. Získané citlivé údaje či data jako jsou jména, hesla, adresy, kreditní karty nebo v nejhorším případě vyfocené doklady uložené v chytrých zařízeních útočníci mohou zneužít i k čerpání finančních půjček jménem oběti, což může mít pro dotčenou osobu velmi vážné následky.

Z právního hlediska je toto protizákonné jednání posuzováno dle trestního zákoníku č. 40/2009 Sb. Krádež identity lze v případě, kdy útočník neoprávněně získá přístup k identitě oběti pomocí překonání bezpečnostního opatření či malware, posuzovat jako naplnění skutkové podstaty trestného činu – Neoprávněný přístupu k počítačovému systému a nosiči informací, dle § 230 odstavce 1 a 2, zákona č. 40/2009 Sb. Aplikovat lze i odstavec 3, v

případě, že způsobí svým jednáním oběti škodu, jinou újmu či získá neoprávněný prospěch. [2], [52], [46]

2.8 Kyberšikana

Jedná se o druh šikany, která je prováděna skrze elektronická zařízení a jejich služby. Nejvíce ohroženou skupinou jsou především děti a teenageři ve věku 12-18 let, kteří skrze své chytré telefony využívají různé sociálních sítě, hrají hry, posílají zprávy, videa nebo obrázky pomocí chatovacích aplikací, a právě skrze tyto prostředky k těmto útokům dochází. Častou formou kyberšikany je šíření pomluv, veřejné urážení, vydírání či přeposílání informací, které jsou pro oběť citlivé a dotýkají se jejich soukromí. Příkladem může být zveřejňování intimních fotografií a videí oběti, které se velmi rychle šíří.

Psychický nátlak na oběť může být tak velký, že situaci neustojí a v nejhorších případech dojde až ke spáchání sebevraždy. [53]

2.8.1 Cyberstalking

Patří mezi časté projevy kybernetické kriminality. Jde o nebezpečnou formu pronásledování či obtěžování prováděnou skrze síť internet a komunikační prostředky nebo aplikace. Útočník vytipované oběti opakovaně zasílá nevyžádané a obtěžující zprávy, které v oběti mohou vzbuzovat pocity ohrožení a vyvolat obavy o vlastní zdraví či život. Takovéto jednání je z právního hlediska naplnění skutkové podstaty trestného činu – Nebezpečné pronásledování, dle § 354, trestního zákoníku č. 40/2009 Sb., s trestní sazbou odnětí svobody šest měsíců až tří let. [54], [46]

2.8.2 Sexting a zneužívání dětí

Jak již z názvu můžeme odvodit, jedná se o „*elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem.*“ [55] V dnešní době zcela běžně dochází k zasílání intimních fotografií nebo videí mezi partnery či při chatování na sociálních sítích a na seznamovacích portálech. Sexting jako takový není v rozporu se zákonem mezi dospělými osobami, avšak jedná se o velmi rizikové chování v kyberprostoru, jelikož tyto materiály mohou být později použity jako prostředky k vydírání.

Velké bezpečnostní riziko však představuje sexting pro děti, kdy jsou přesvědčovány útočníkem k zaslání intimních materiálů či přímo živému přenosu videa skrze aplikace jako

je Skype, Messenger, Whatsapp a další, které má nainstalované v chytrém zařízení. [2]

Velkou osvětou v této oblasti je dokument Víta Klusáka a Barbory Chalupové s názvem „V síti“, který se pomocí reálného experimentu, zaměřeným na zneužívání dětí na internetu, snaží upozornit na hrozby kyberprostoru v podobě sexuálních predátorů, ale také na rizikové chování nezletilých na sociálních sítích. Za pomocí tří dospělých hereček s dětskými rysy a věrohodných prostor ve studiu, v podobě dětských pokojíčků, zakládají fiktivní profily 12letých dívek na sociálních sítích a komunikují s muži, kteří je na těchto sociálních sítích vyhledali. Celý tento experiment trval 10 dní, během kterých tyto tři herečky oslovilo neuvěřitelných 2458 mužů, z nichž převážná většina po „nezletilých“ dívkách žádali fotografie s intimním obsahem či před nimi masturbovali, a v některých případech došlo i na osobní setkání a vydírání. [56]

Obr. 12. Tereza Těžká – pořizuje fotografii pro jednoho z mužů [57]

2.8.3 **Cybergrooming**

Jedná se o další projev kyberkriminality, který cílí opět nejčastěji na nezletilé děti, avšak od klasického sextingu se odlišuje tím, že útočník má za cíl zneužít důvěry oběti a přimět ji k osobní schůzce za účelem následné konání trestné činnosti, např. pohlavního zneužívání či focení a natáčení pornografického materiálu. [2]

Obr. 13. Tereza Těžká – připravuje se na osobní setkání s predátorem [58]

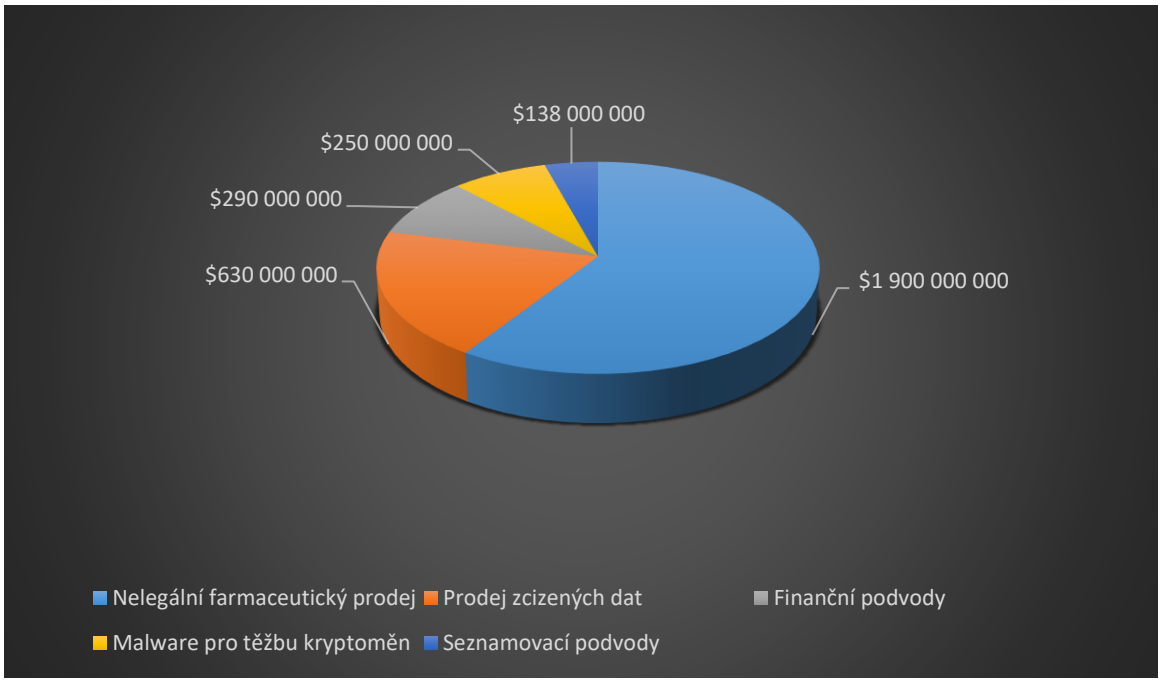
Z právního hlediska tyto způsoby jednání naplňují skutkové podstaty trestných činů:

- Vydírání, podle § 175, zákona č. 40/2009 Sb.; trestní sazba odnětí svobody činí 6 měsíců až 4 roky či peněžitý trest.
- Výroba a jiné nakládání s dětskou pornografií, podle § 192, zákona č. 40/2009 Sb.; trestní sazba odnětí svobody až na 2 roky.
- Zneužití dítěte k výrobě pornografie, dle § 193, zákona č. 40/2009 Sb.; trestní sazba odnětí svobody 1 až 5 let.
- Navazování nedovolených kontaktů s dítětem, podle § 193b, zákona č. 40/2009 Sb.; s trestní sazbou odnětí svobody až na 2 roky. [2], [54], [46]

3 SOCIÁLNÍ SÍTĚ

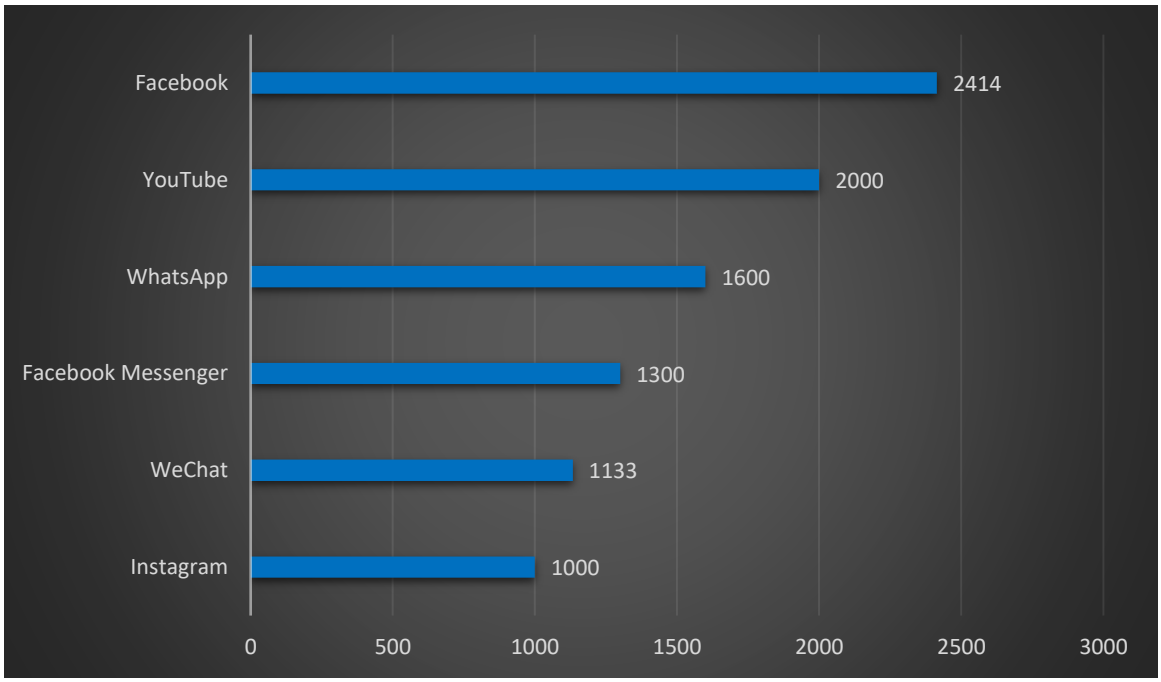
Používání chytrých zařízení, především telefonů jde ruku v ruce i s používáním sociálních sítí. Možnost rychlé a efektivní komunikace vedlo k jejich rozvoji a staly se velmi častým působištěm v mnoha oblastech kyberkriminality. Ačkoliv si to většina uživatelů neuvědomuje, používání sociálních sítí může představovat poměrně velká bezpečnostní rizika. Tato populární forma komunikace a sdílení informací skrze chytrá zařízení vede k v mnoha případech k naprostému odkrytí svého vlastního soukromí, jelikož nás určitou formou také nabádá k vyplnění velmi citlivých osobních údajů. Těchto informací (jméno, příjmení, datum narození, údaje o poloze, email, připojené kreditní karty, přátelé apod.) poté využívají útočníci. Výhodou pro ně je anonymita, kterou jim tyto sociální sítě poskytují, jelikož nepožadují žádné ověření totožnosti při zakládání profilů. V oblibě je tedy maskování se za profil známé osoby potencionální oběti a následné páchání různých deliktů od finančních podvodů, instalace malware do zařízení či kyberšikany atd. [59]

Podle výzkumu společnosti Bromium hodnota ukradených uživatelských dat ze sociálních sítí ročně přesahuje částku 630 milionů dolarů. [60]



Obr. 14. Roční výnos kriminálních činností souvisejícími se sociálními sítěmi [60]

Jelikož sociálních sítí dnes existuje poměrně velké množství, zaměříme se především na sociální síť s nejvíce aktivními uživateli – Facebook.



Obr. 15. Sociální sítě dle počtu aktivních uživatelů (v milionech) [61]

3.1 Facebook

Sociální síť, kterou založil v roce 2004 mladý americký programátor jménem Mark Zuckerberg. Původně sloužila pouze jako prostředek ke komunikaci mezi studenty Harvardské univerzity na doméně thefacebook.com, avšak kvůli své popularitě byla během jednoho roku zpřístupněna všem uživatelům internetu starších 13 let již na doméně facebook.com. [39] Zpřístupnění této platformy celému světu vedlo k masivnímu nárustu uživatelů a v současné době tuto sociální síť využívá v průměru přes 2 miliardy uživatelů. [62] Facebook slouží uživatelům nejen ke sdílení fotografií a videí, posílání zpráv pomocí aplikace Messenger, ale nově i k prodeji movitých i nemovitých věcí na tzv. marketplace. [63] Platforma Facebooku je dostupná jak ve webové verzi, tak i ve verzích pro nejpoužívanější operační systémy smart zařízení ve formě aplikace.

3.1.1 Profil a informace

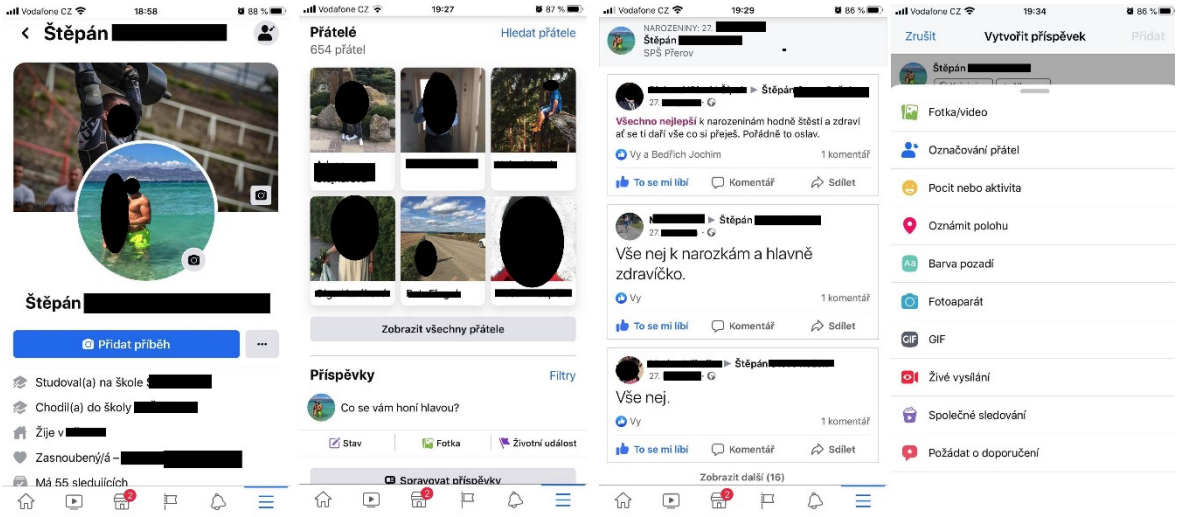
Vytvořený profil na Facebooku je v podstatě taková „internetová vizitka“ osoby, která obsahuje vyplněné osobní údaje a případně fotografie. Údajů, které tato sociální síť o osobě umožňuje v profilu vyplnit je celá řada.

- **Kontaktní a základní údaje** – jméno, příjmení, pohlaví, datum narození, přesná adresa pobytu, mobilní čísla, emailové adresy, náboženské vyznání, politické přesvědčení
- **Rodina a vztahy** – informace o vztazích osoby, rodinném stavu a trvání včetně odkazů na profily rodinných příslušníků či partnerů
- **Zaměstnání** – všechna aktuální, či v minulosti vykonávaná zaměstnání, včetně detailního popisu vykonávané činnosti, pozice, místo, období od – do
- **Vzdělání a odborné znalosti** – údaje o školách, které osoba studovala nebo studuje a odborných znalostech
- **Místa, kde osoba žila** – přehled míst, kde se osoba v minulosti žila, či aktuálně žije
- **Životní události** – přehled důležitých momentů ze života dané osoby, nové zaměstnání, vzdělání, zájmy a aktivity, milníky a úspěchy, vzpomínky, cestování apod.

Dalším viditelným prvkem na profilu je seznam přátel, kteří na této sociální síti mají profil a provedli s daným profilem osoby interakci v podobě „přidání do přátel“ a prvek, který se nazývá Timeline. [64]

3.1.2 **Timeline a příběhy (stories)**

Timeline, známý také pod pojmem „facebooková zeď“. Je to prvek, kam uživatelé přidávají příspěvky, tzv. statusy, ve formě fotografií, videí či textových zpráv. Těmito příspěvky například mohou sdělovat své pocity, aktivity, oznamovat svou polohu anebo zahájit živá vysílání pomocí kamery v telefonu. Ostatní uživatelé na ně mohou reagovat pomocí tlačítka „to se mi líbí“ a přidružených emotikon, díky kterým vyjadřují svůj postoj k danému statusu či zanechat komentář. Velmi oblíbené je v dnešní době sdílení příběhů neboli slangově „storýček“, což jsou krátké úryvky v podobě natočených videí, obrázků a textů, na kterých uživatelé sdílí své zážitky z dne a zůstávají viditelné po dobu 24 hodin od sdílení. [65]

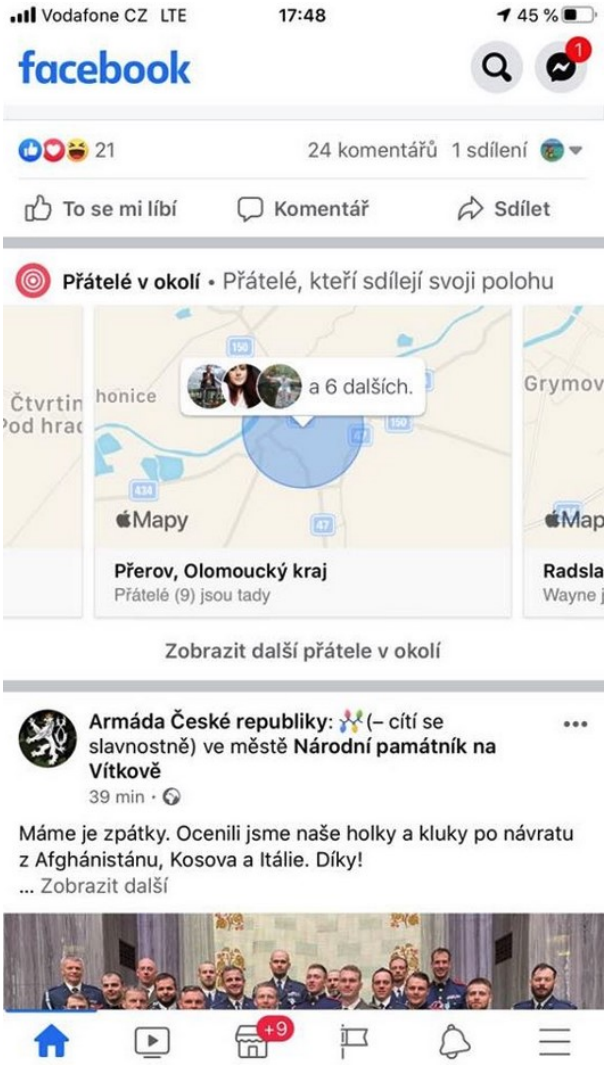


Obr. 16. profil, timeline, tvorba příspěvku v mobilní aplikaci [archiv autora]

3.1.3 Rizikové chování a sdílené informace

Za bezpečnostní riziko při používání jakékoli sociální sítě skrze chytrá zařízení, můžeme označit především povahu sdílených informací. Převážně se jedná o informace, které by měly zůstat soukromé. Jedná se o především o osobní údaje, informace o poloze, fotografie dětí, domácnosti, cenného majetku atd. I pouhý příspěvek o tom, že se chystáte na dovolenou nebo sdílíte příspěvek i včetně přesné aktuální polohy, může představovat potenciální riziko.

Může se totiž stát, že během vaší nepřítomnosti se vám po obydlí pohybuje zloděj a krade majetek, který právě tuto informaci využil ke svému prospěchu. Stejně tak se můžete stát obětí krádeže či poškození vašeho vozidla, které se objevilo i včetně registrační značky v některém z příspěvků. Často se na Facebooku lze také setkat s tím, že uživatelé sdílí fotografie dětí (v některých případech i obnažené a necenzurované), což může vést ke zneužití těchto fotografií pedofily, kteří tyto materiály aktivně vyhledávají. [66]



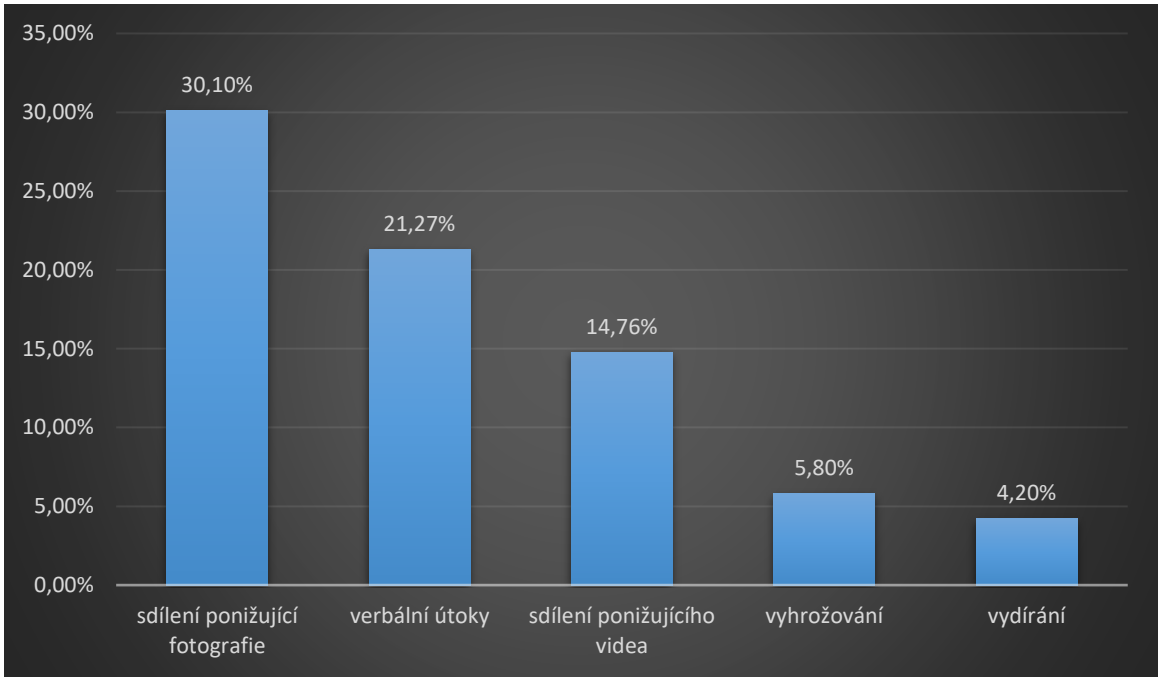
Obr. 17. Přátelé sdílející svou aktuální polohu v mobilní aplikaci Facebook [archiv autora]

Využívání Facebooku je také velmi oblíbená činnost „dětských uživatelů“ smart technologií, kteří častokrát nerespektují pravidla jeho užívání a minimální věkové hranice 13 let. V České republice však existuje poměrně nová legislativa v podobě Zákona o zpracování osobních údajů č. 110/2019 Sb., §7, který určuje minimální věkovou hranici 15 let, kdy je dítě způsobilé pro souhlas se zpracováním osobních údajů, a tím tedy i využívání této sociální sítě. [67]

V případě těchto uživatelů, kteří jsou na Facebooku velice aktivní, se jedná především o rizika vyplývající z různých druhů kyberšikany (sexting, cyberstalking, vydírání apod.), která je hrozbou při navazování přátelství a komunikací s osobami, jejichž pravou identitu neznají. Avšak může být i v podobě blízkých osob, například spolužáků, kteří oběť verbálně

napadají v komentářích, zprávách anebo disponují jakýmkoliv ponižujícím materiálem, který je následně nekontrolovatelně sdílen mezi další osoby a tím tak oběť může významně ohrozit.

Dle výzkumu Univerzity Palackého v Olomouci, který se týkal Facebooku a 1 122 českých dětí ve věku 8-17 let, aktivně využívajících tuto sociální síť, bylo zjištěno, že velká část z nich se již stala obětí jakéhokoliv kyberútoku či kyberšikany. [68]



Obr. 18. Projevy kyberšikany na Facebooku [68]

3.1.4 Šíření dezinformací (hoax)

Při používání této sociální sítě se také lze setkat s masivně sdílenými příspěvky či zprávami, které se svou povahou snaží působit na uživatele důležitě a věrohodně, avšak jedná se o poplašnou zprávu, která varuje například před neexistující hrozbou. Jejich společným znakem je ve většině případů výzva k jejich dalšímu sdílení či přeposlání a tím vzniká tzv. lavinový efekt. [69]

Je tedy zřejmé, že v případě celkového používání této sociální sítě skrze chytré zařízení, lze o osobě zjistit dostatek informací k tomu, aby sdílené informace mohly být zneužity k aktivitám, které pro danou osobu představují bezpečnostní rizika od krádeže identity, po nebezpečné vyhrožování či vydírání aj.

4 PREVENCE A OPATŘENÍ

K tomu, abychom se úspěšně bránili hrozbám v kyberprostoru a minimalizovali bezpečnostní rizika, je důležité se řídit několika základními pravidly, která nám pomohou zvýšit bezpečnost při celkovém používání smart zařízení.

4.1 Silná hesla

Pro přístup k různým účtům a službám je zapotřebí volit dostatečně silná hesla, která obsahují alespoň deset znaků. Dle společnosti Avast je však doporučeno minimálně 15 znaků, malá i velká písmena a ideálně i numerické a speciální znaky. [70] Nedoporučuje se volit jako heslo datum narození, jméno apod. Důležité je ovšem i provádět pravidelně změnu hesel a nikdy nepoužívat stejné heslo k více účtům. Především heslo k emailové schránce, která většinou slouží k obnově hesel u více služeb. [71]

Taktéž je výrazně doporučeno měnit v administraci původní hesla k zařízením jako jsou především routery a další IoT zařízení. Jak již bylo zmíněno, dle statistik 60 % uživatelů přesto původní hesla používá. [22]

4.2 Používání antivirové aplikace

Antivirová aplikace by měla být instalována na každém chytrém zařízení. Chrání před hrozbami v podobě malware, phishingovými stránkami, ale zároveň dokáží chránit soukromí a data, upozorňovat na nezabezpečené Wi-Fi sítě či nedostatky v bezpečnostních opatřeních. Příkladem může být instalace antivirové aplikace od společnosti Avast, kterou lze stáhnout zdarma z oficiálních obchodů Google Play Store či App Store. [72]

4.3 Ochrana soukromí

Jak již bylo zmíněno v předchozí kapitole, je třeba chránit své soukromí, a to především při využívání sociálních sítí. Doporučuje se tedy nezveřejňovat a neposílat citlivé údaje jako informace o vaší poloze, osobní údaje, hesla či fotografie soukromé povahy. Stejně tak nepřijímat žádosti o přátelství a sledování od osob, které neznáte. [2] Dále je doporučeno nastavit svůj profil jako neveřejný.

4.4 Všímání si detailů

V případě, že obdržíte email, SMS či se dostanete na podezřelou webovou stránku, všímejte si detailů. Častokrát lze např. phishing odhalit pouhým detailním přečtením zprávy, jelikož v mnoha případech obsahují gramatické chyby nebo přeházený slovosled. V žádném případě v takových zprávách neklikejte na odkazy či nestahujte přílohy. [2]

Stejně tak je důležité všímat si, zda je spojení se serverem, např. webovou stránkou, zabezpečené a je ověřené pomocí certifikátu. Všímat si tedy, že doména začíná zabezpečeným protokolem HTTPS, zobrazený ikonou zeleného zámečku, namísto nezabezpečeného protokolu HTTP. Ani to však zcela nezaručuje, že se nemůže jednat například o phishingový web. [10]

4.5 Uzamykání zařízení

Pokud zařízení nepoužíváte, zajistěte jeho automatické uzamknutí po určité době. Zařízení lze zabezpečit proti neoprávněnému užití pomocí PIN kódu, hesla či gestem. Standartní funkcí dnes již bývá i zabezpečení biometrickými prvky, jako jsou otisky prstů či rozpoznání obličeje. [73]

4.6 Ochrana dat

Jako ochrana před neoprávněným přístupem slouží funkce šifrování či vymazání dat v případech, kdy dojde ke ztrátě či krádeži zařízení. Většina chytrých zařízení v dnešní době disponuje funkcí vzdáleného vymazání dat či blokaci zařízení. [73]

4.7 Aktualizace

Instalace aktualizací operačního systému a aplikací patří k základním zásadám bezpečnosti při využívání chytrých technologií. Kromě různých vylepšení, ale především slouží jako opravy bezpečnostních slabin, kterých mohou využít hrozby. [73]

4.8 Aplikace z důvěryhodných zdrojů a oprávnění

Aplikace stahujte a instalujte pouze z oficiálních obchodů jako je Google Play Store či App Store. Snížíte tak riziko napadení chytrého zařízení malwarem, oproti stahování aplikací z

neověřených webových stránek. Měli bychom však mít na paměti, že i na oficiálních zdrojích stále existuje riziko výskytu aplikace, která v sobě skrývá škodlivý kód.

Stejně tak je třeba zvýšit pozornost při instalaci samotné aplikace a oprávněním, ke kterým funkcím a informacím aplikace žádá přístup. [73]

4.9 Polohové služby

Využívání polohových služeb by mělo být aplikacím povoleno pouze v nezbytných případech, a hlavně dle jejich typu. Není třeba povolit přístup k vaší poloze aplikacím, které tyto informace zjevně nepotřebují. [73]

4.10 Veřejné Wi-Fi sítě

Využívání nezabezpečených veřejných Wi-Fi sítí může představovat bezpečnostní riziko z důvodu možného odposlechu nešifrované komunikace. Nedoporučuje se tedy tyto veřejné přístupové body využívat k používání aplikací typu mobilní bankovnictví či posílání a přijímání jiných citlivých údajů. [73]

4.11 Vypínání bluetooth

V případě, kdy bluetooth nevyužíváme, je doporučeno jeho vypínání. Vypínáním lze předejít šíření různých typů malware, ale také předejít krádežím zařízení například z automobilů na parkovištích apod. Existují totiž aplikace, které jsou schopny skenovat okolí a detekovat zařízení se zapnutým bluetooth, a to včetně typu zařízení a jeho polohy. [73], [74]

4.12 Ochrana dětí

Jelikož děti jsou považovány při využívání chytrých zařízení a sociálních sítí za rizikovou skupinu, je vhodné instalovat do jejich chytrých zařízení aplikace, které jsou schopny chránit před kyberšikanou či sextingem. Příkladem je aplikace s názvem SafeToNet, která je schopna v reálném čase analyzovat a filtrovat zprávy v telefonu dítěte. V případě, že aplikace zjistí nevhodný obsah jako např. intimní fotografie, provede se automaticky blokace telefonu a po několika pokusech o odeslání či přijmutí takového obsahu upozorní rodiče pomocí SMS zprávy. [75]

II. PRAKTICKÁ ČÁST

5 PHISHINGOVÝ ÚTOK A ANALÝZA DAT

Jak již bylo zmíněno v teoretické části, při phishingovém útoku se využívá sociálního inženýrství k získání cenných informací (přihlašovací údaje, údaje k platební kartě aj.), které původce útoku zneužívá k dalšímu páchání trestné činnosti.

Předmětem praktické části bude provedení simulovaného phishingového útoku zaměřeného na získání přístupu k Facebook účtu a následná analýza dat získaných ze zneužitého účtu uživatele. Dozvíme se tedy, jaká data o uživateli Facebook za dobu jeho používání v chytrém telefonu zjistil. První část je ukázkou samotného phishingového útoku, tvorba podvodné webové stránky a způsob, jakým se „sbírají“ přihlašovací údaje obětí. Druhá část je zaměřená na analýzu získaných dat, které mohou v případě zneužití představovat bezpečnostní riziko.

5.1 Postup tvorby podvodné webové stránky

V následujících krocích popíši, jak probíhá tvorba phishingové webové stránky včetně otestování její funkčnosti.

5.1.1 Výběr cíle

Určím si tedy službu, jejíž podobu budu duplikovat. Vzhledem k tomu, že předmětem je provádět útok na uživatelský účet služby Facebook, použiji tedy jako cíl mobilní verzi přihlašovací stránky Facebooku, dostupné na adrese https://m.facebook.com.

Obr. 19. mobilní verze přihlašovací stránky [archiv autora] [64]

5.1.2 Duplikace

K tomu, aby mohla být provedena duplikace webové stránky, je třeba znát její zdrojový HTML kód. Využívá se tedy funkce *„zobrazit zdrojový kód stránky“*, v jakémkoliv webovém prohlížeči. Celý zdrojový kód se následně zkopíruje a uloží do souboru *index.html*.

Obr. 20. Ukázka části zdrojového kódu mobilní přihlašovací stránky [archiv autora]

Nyní je kopie mobilní přihlašovací stránky Facebooku hotova, avšak je potřeba v tomto zdrojovém kódu provést úpravu, která zajistí, že v případě zadání přihlašovacích údajů dojde k jejich uložení do textového dokumentu.

Ve zdrojovém kódu je tak třeba vyhledat atribut, který určuje, jaká akce se má provést po stisknutí tlačítka „*Přihlásit se*“. V tomto případě se jedná o tuto část HTML kódu. [76]

```
<form method="post"
action="/login/device-based/regular/login/?refsrc=https%3A%2F%2Fm.facebook.com%2F&lwv=100&refid"
class="be bf" id="login_form" novalidate="1">
```

Obr. 21. HTML kód určující akci po stlačení přihlašovacího tlačítka [archiv autora]

Hodnotu atributu action je tedy třeba upravit, aby plnil funkci definovanou v souboru *post.php*, který budeme vytvářet následně a je zodpovědný za akci uložení přihlašovacích údajů do souboru. [76]

```
<form method="post" action="post.php" class="be bf" id="login_form" novalidate="1">
```

Obr. 22. Upravená hodnota atributu action [archiv autora]

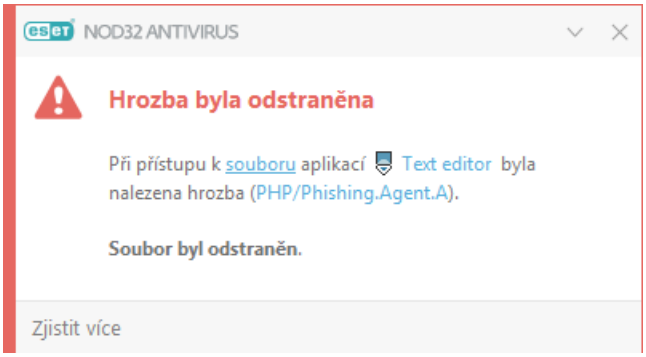
5.1.3 Script

V tomto kroku již dochází k vytvoření souboru s názvem *post.php*, do kterého se vloží samotný script (PHP kód), starající se o uložení přihlašovacích údajů oběti (uživatelské jméno a heslo) do textového souboru, a následné přesměrování na správnou, důvěryhodnou přihlašovací stránku https://m.facebook.com [76]

```
<?php
header ('Location: https://m.facebook.com');
$handle = fopen('prihlasovaciudaje.txt', 'a');
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, '=');
fwrite($handle, $value);
fwrite($handle, 'rn');
}
fwrite($handle, 'rn');
fclose($handle);
exit;
?>
```

Obr. 23. PHP script provádějící ukládání údajů [archiv autora]

Tento script je volně dostupný na několika webových stránkách, ale i v oficiálně vydané literatuře. To, že je script funkční a opravdu plní danou funkci potvrdil i antivirus, který tento soubor okamžitě rozpoznal jako hrozbu (PHP / Phishing.Agent.A.) a odstranil jej.

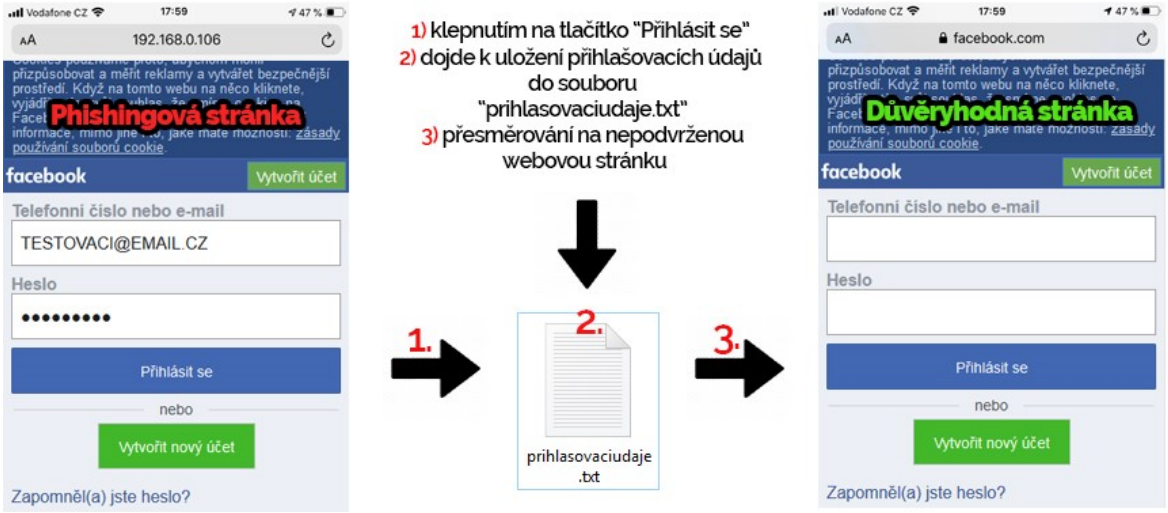


Obr. 24. Potvrzení phishingu [archiv autora]

Jelikož je tento soubor k funkčnosti nezbytný, přidám jej v antivirovém programu mezi výjimky, abych zamezil jeho další detekci.

5.1.4 Testování funkčnosti

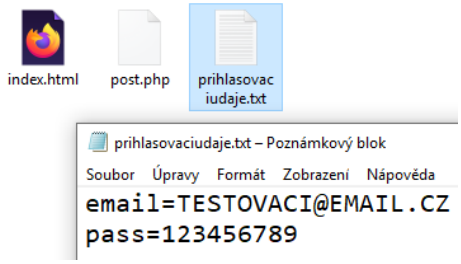
Na základě splněných kroků výše, adresář nyní obsahuje 2 soubory, *index.html* a *post.php*. Nyní tedy přichází část, kdy otestujeme, zda vytvořená phishingová webová stránka plní svou funkci a sbírá přihlašovací údaje. Funkčnost ověřím pouze na vytvořeném lokálním serveru pomocí software XAMPP, který se používá například při vývoji webových aplikací a je volně ke stažení. [77]



Obr. 25. Průběh útoku [archiv autora]

V prvním kroku tedy oběť vyplní své přihlašovací údaje a stiskne tlačítko „*Přihlásit se*“. V druhém kroku se údaje oběti uloží do souboru „*prihlasovaciudaje.txt*“ a následně v třetím

kroku proběhne přesměrování na oficiální přihlašovací stránku Facebooku, která je od naší podvržené k nerozeznání.



Obr.26. Získané přihlašovací údaje

[archiv autora]

Funkčnost scriptu byla tedy úspěšně ověřena díky uloženým přihlašovacím údajům oběti v souboru *„prihlasovaciudaje.txt“*.

5.1.5 Šíření phishingové webové stránky

Při reálném phishingovém útoku jsou tyto soubory samozřejmě nahrány na webhosting a šíří se nejčastěji pod vhodnou doménou, která působí na oběť důvěryhodně. Z minulosti např. útoky pod doménou alrbank.cz, což je snadno zaměnitelné s důvěryhodnou doménou airbank.cz. [10]

Jak již bylo popisováno v teoretické části, nejčastěji se tyto phishingové webové stránky šíří pomocí emailu s výzvou k přihlášení a změně hesla z důvodu napadení účtu, avšak k šíření lze využít jakýkoliv další způsob, např. zasláním SMS či smyšlené zprávy z falešného profilu přítele oběti.

Považujme tedy, že phishingový útok na Facebookový účet oběti byl úspěšný a útočník získal přihlašovací údaje v podobě uživatelského jména a hesla, což je dostačující k tomu, aby nad daným účtem získal kontrolu a mohl o oběti získávat další zajímavé informace. Následující část praktické části bude tedy věnována analýze dat, které Facebook sbírá při jeho používání.

6 ANALÝZA DAT SESBÍRANÝCH FACEBOOK APLIKACÍ

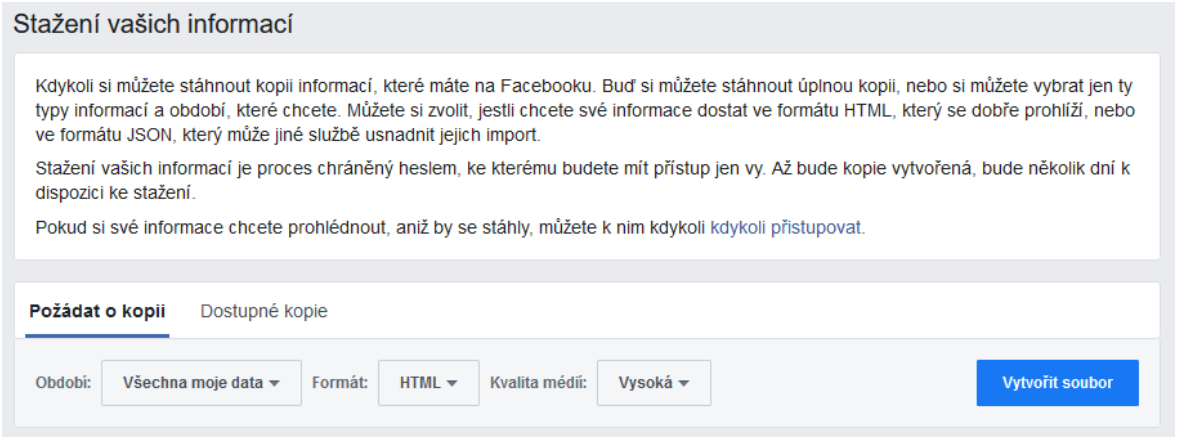
Jednou ze zajímavých funkcí, kterou Facebook nabízí v nastavení profilu je funkce stažení vašich informací, která je sice chráněna heslem, avšak došlo-li již k napadení účtu a neoprávněnému přístupu, je pravděpodobné, že heslo a uživatelské jméno je v rukou útočníka a nebrání tedy nic ve stažení všech informací z napadeného profilu.

V případech, kdy se uživatel přihlašoval na zařízení, ke kterému má přístup více osob a z nějakého důvodu nedošlo k odhlášení, se k této funkci všech informací o profilu dostane prakticky kdokoliv, jelikož lze tyto informace prohlížet (nikoliv však stahovat zmíněnou funkcí) i bez zadávání hesla. Informací, které lze tímto krokem získat je obrovské množství, protože Facebook ukládá veškerou aktivitu, kterou uživatel za dobu používání provede.

V této praktické části provedu analýzu dat stažených z mého osobního účtu Facebook, který používám od roku 2009.

6.1 Stažení informací

K informacím, které Facebook za celou dobu mého používání získal, se lze dostat přes aplikaci či webovou verzi Facebooku v záložce „*Vaše informace na Facebooku*“ a poté buďto procházet tyto informace online po zadání hesla anebo využít možnosti stažení informací do souboru. Pro rychlejší procházení dat využiji možnost stažení informací do souboru.

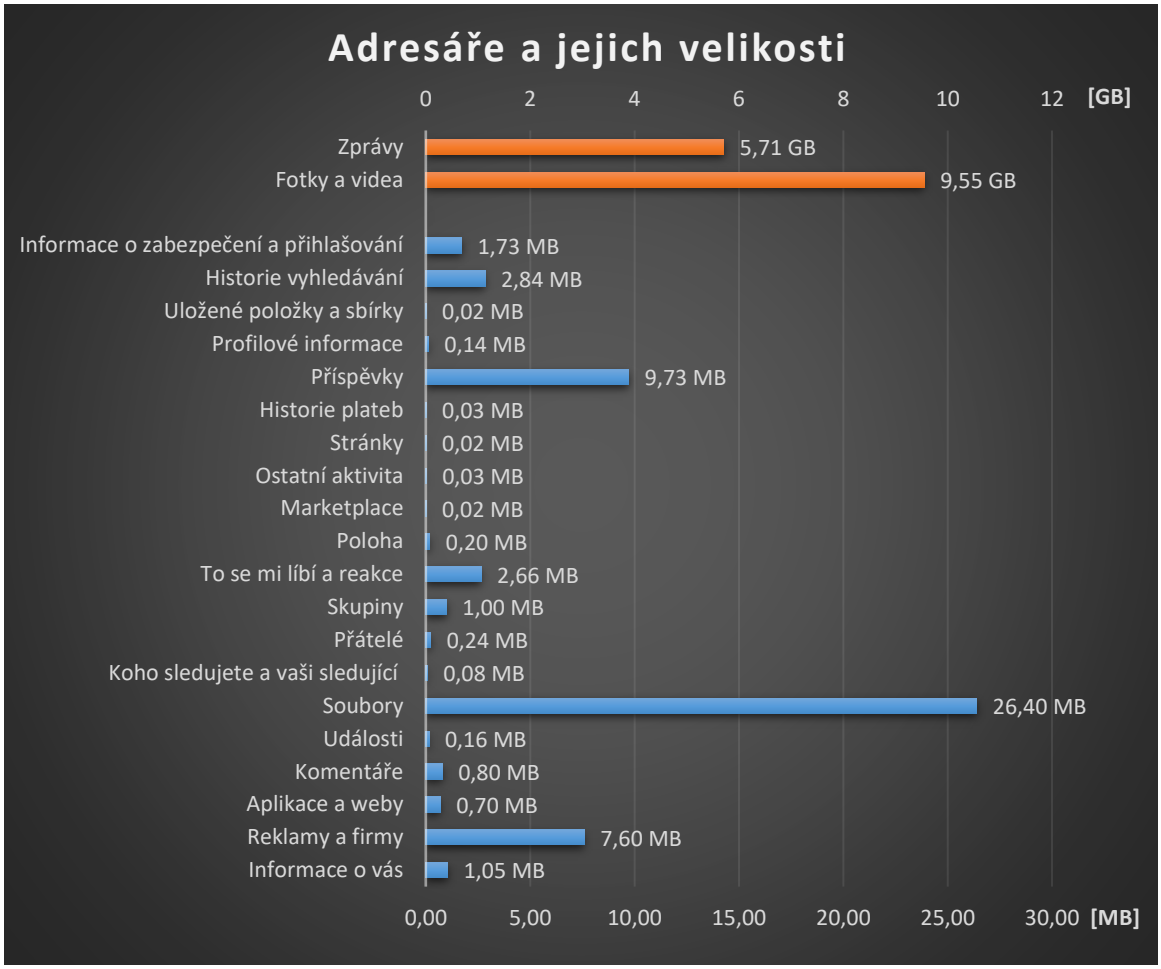


Obr. 27. Funkce stažení informací profilu [78]

Po kliknutí na tlačítko „*Vytvořit soubor*“ se objeví informační hláška o přijetí požadavku a vyčkání na kopii našich informací. V mém případě tato akce trvala cca 24 hodin.

6.2 Analýza stažených dat

Po obdržení informace o vytvořené kopii mých informací provedu tedy jejich stažení. Zde nastává první pocit „zděšení“, jelikož velikost stažených archivů byla neuvěřitelných 15,3 GB. Po extrahování a následném otevření adresářů zjišťuji, že součástí těchto stažených informací je prakticky vše od odeslaných zpráv, fotek, provedených platbách, telefonních kontaktů, používaných IP adres, až po polohové informace a mnoho dalšího.



Obr. 28. Velikosti sesbíraných dat Facebookem [archiv autora]

Jak lze z grafu pozorovat, adresáře, které obsahují nejvíce dat, jsou především odeslané zprávy, fotky a videa, v součtu 15,26 GB. Celkově se jedná o 28 694 souborů a 2938 složek.

Jednotlivé informace lze procházet buďto manuálně po složkách anebo pomocí souboru index.html, který data rozděluje do jednotlivých kategorií a umožňuje jejich procházení v uživatelsky přívětivém prostředí.

Obr. 29. Rozhraní souboru index.html [archiv autora]

Na obrázku výše jsou zobrazena ukázka tří kategorií informací z celkových čtyřiadvaceti, které lze procházet, avšak i na tomto malém příkladu si lze všimnout, že používáním aplikace Facebook zanecháváme velké množství různých dat, které je možné zneužít.

Všechny kategorie informací, které je možno prohlížet jsou uvedeny v tabulce č. 1 níže.

Tab. 1. Všechny kategorie dostupných dat a jejich popis (upraveno, Rožek 2020) [78]

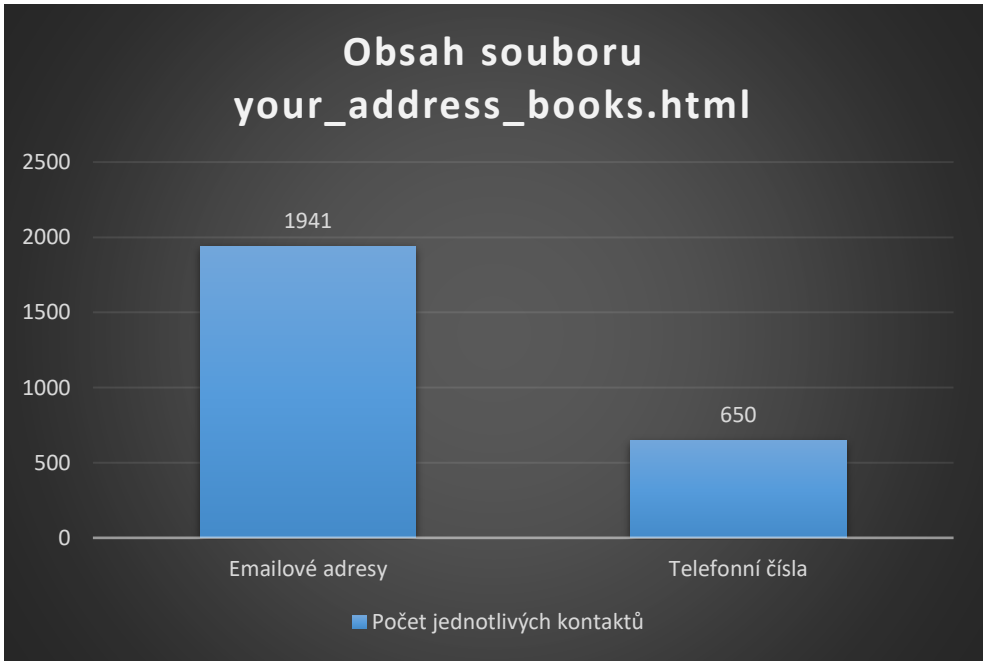
Kategorie	**Obsah**
Příspěvky	Vámi sdílené příspěvky na Facebooku, příspěvky skryté na vaší timeline a vámi vytvořené ankety
Fotky a videa	Vámi nahrané a sdílené fotky a videa
Komentáře	Komentáře, které jste přidal ke svým příspěvkům, příspěvkům jiných lidí nebo ve skupinách, ve kterých jste
To se mi líbí a reakce	Příspěvky, komentáře a stránky, kterým jste dal To se mi líbí nebo jste na ně zareagoval
Přátelé	Lidé, se kterými jste na Facebooku spojení
Příběhy	Fotky a videa sdílená ve vašem příběhu
Koho sledujete a vaši sledující	Lidé, organizace nebo firmy, u kterých jste určil, že od nich chcete vídat obsah, a lidé, kteří vás sledují
Zprávy	Zprávy, které jste si na Messengeru vyměnili s jinými lidmi
Skupiny	Skupiny, ve kterých jste, skupiny, které spravujete, a vaše příspěvky a komentáře ve skupinách, ve kterých jste
Události	Vaše reakce na události a seznam vámi vytvořených událostí
Profilové informace	Vaše kontaktní údaje, údaje z oddílu Informace na vašem profilu, vaše životní události, koníčky a hudba.
Stránky	Stránky, jichž jste správcem
Marketplace	Vaše aktivita na Marketplace
Historie plateb	Historie vámi provedených plateb přes Facebook
Uložené položky a sbírky	Seznam vámi uložených příspěvků a aktivita ve sbírkách
Vaše místa	Seznam vámi vytvořených míst
Aplikace a weby	Aplikace a weby, ke kterým se přihlašujete přes Facebook a vámi spravované aplikace
Další aktivita	Aktivita spojená s vaším účtem, například když někoho šťouchnete nebo někdo vás
Reklamy a firmy	Zájmy ohledně reklam Inzerenti, se kterými jste provedl nějakou interakci
Historie vyhledávání	Historie vašich vyhledávání na Facebooku
Poloha	Informace související s vaší polohou
Informace o vás	Informace spojené s vaším Facebook účtem • Váš adresář • Skupina podobných přátel
Informace o zabezpečení a přihlašování	Historie vašich přihlášení, odhlášení, dob, kdy jste byl na Facebooku aktivní, a zařízení, ze kterých na Facebook chodíte. • Použité IP adresy • Kde jste přihlášeni

6.2.1 Profilové informace, kontakty

Po otevření staženého souboru s profilovými informacemi jsem zjistil, že i když mám určité údaje na profilu označené jako skryté, tento soubor je i přesto obsahuje. Týká se to především následujících údajů:

- Emailové adresy
- Telefonní čísla
- Datum narození
- Bydliště
- Aktuální rodinný stav – včetně údajů o předchozích vztazích a jmen těchto osob
- Rodinné vazby – profily osob rodinných příslušníků se vztahem k mému profilu

Další zajímavý soubor s názvem „*your_address_books.html*“, který jsem při procházení jednotlivých adresářů nalezl mě svým obsahem zaskočil, jelikož si nejsem vědom, že bych někdy aplikaci udělil souhlas k přístupu ke kontaktům z emailové schránky či seznamu kontaktů v telefonu.



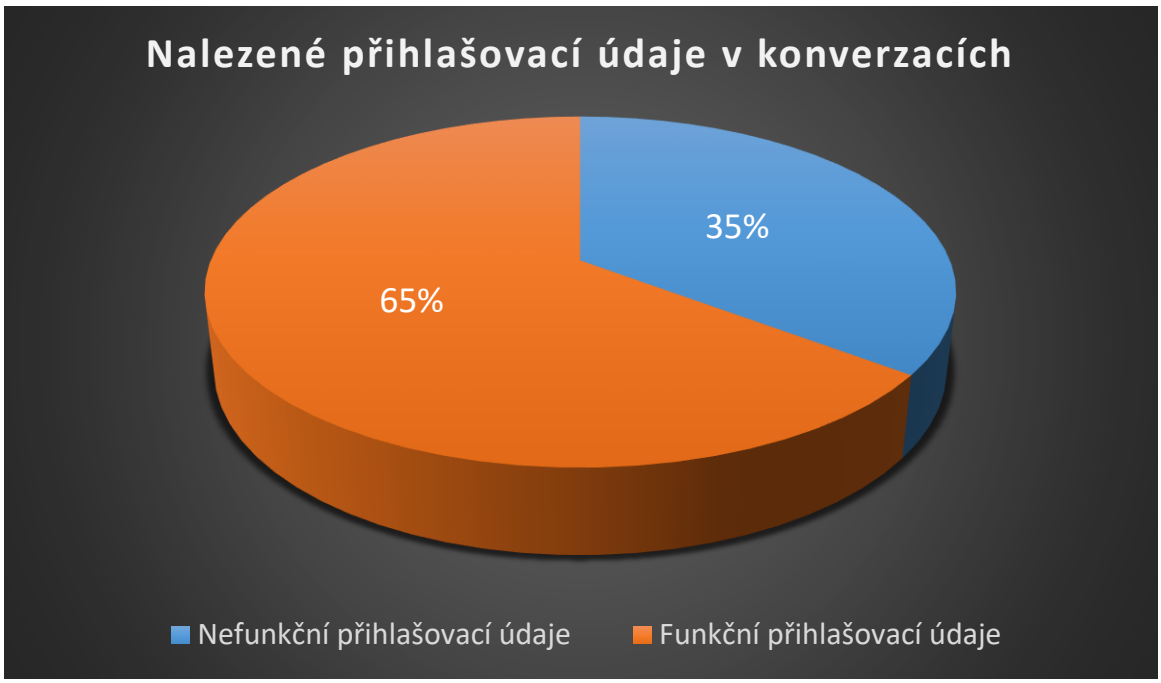
Obr. 30. Množství telefonních kontaktů a emailových adres [archiv autora]

Celkem se jednalo 2591 kontaktů, se kterými jsem někdy komunikoval buďto prostřednictvím emailu anebo telefonního hovoru. Zajímavé však je i zjištění, že některé kontakty už jsem z telefonu dávno smazal, ale zde jsou přesto dostupné.

6.2.2 Analýza konverzací

Co se týče konverzací (zpráv), tak ty jsou dostupné v souboru „*your_messages.html*“. Celkem se za 11 let používání Facebooku a Messengeru jedná o 1014 konverzací o velikosti 5,71 GB, viz. *Obr. 28*.

Co mě však překvapilo, bylo množství přihlašovacích údajů (uživatelských jmen a hesel), které mi buď byly v průběhu tohoto období zaslány nebo jsem sám zaslal k různým službám, z nejrůznějších důvodů. Většina údajů jsou dokonce stále aktuální a funkční.



Obr. 31. Nalezené přihlašovací údaje v konverzacích a jejich funkčnost [archiv autora]

Celkem jsem v konverzacích nalezl 34 přihlašovacích údajů z nichž neuvěřitelných 22 je stále aktuálních a funkčních. Jednalo se například o přístupové údaje k administraci webových stránek, Wi-Fi sítí či emailu. V konverzacích stačilo pouze vyhledat frázi „*heslo*“.

Troufnu si říci, že spousta uživatelů někdy skrze chatovací aplikaci Facebooku či jinou komunikační aplikaci poskytla nějaký přihlašovací údaj, k jakékoliv službě a vystavuje se tak riziku zneužití těchto údajů.

6.2.3 Přihlášená zařízení

Velmi zajímavá data obsahuje taktéž soubor s názvem „*where_you're_logged_in.html*“. Obsahuje informace o tom, na kterých zařízeních je můj Facebook účet přihlášený, včetně

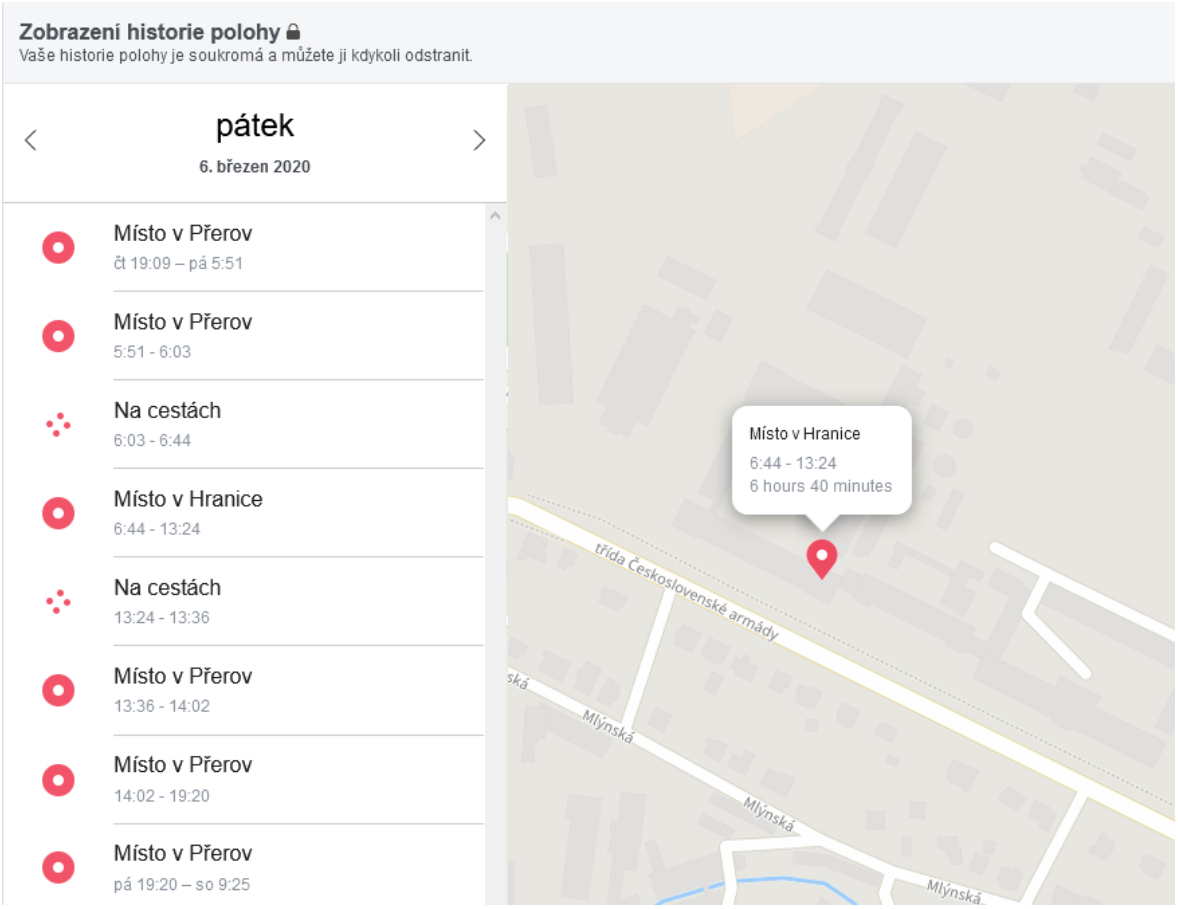
přesného data přihlášení, polohy a IP adresy či typu zařízení. Zjistil jsem, že svůj účet mám přihlášený na celkem sedmi zařízeních. V tabulce níže uvádím informace z jednoho z nich. Z údajů lze mimo jiné vyčíst i použitého mobilního operátora – Vodafone.

Tab. 2. Přihlášená zařízení a informace [archiv autora]

Zařízení	iPhone 7 Plus
Vytvořeno	18. 9. 2019 1:59
Aktualizováno	3. 2. 2020 14:32
Poloha	Brno, Czech Republic
IP adresa	46.135.93.123
Prohlížeč	Mozilla/5.0 (iPhone; CPU iPhone OS 13_3 like Mac OS X) Apple WebKit/605.1.15(KHTML, like Gecko) Mobile/15E148[FBAN/FBIOS;FBAV/255.0.0.34.118; FBBV/195456474;FBDV/iPhone9,4; FBMD/iPhone;FBSN/iOS; FBSV/13.3;FBSS/3;FBID/phone;FBLC/cs_CZ;FBOP/5; FBRV/196325838;FBCR/VF CZ]
Soubor cookie	826B**********

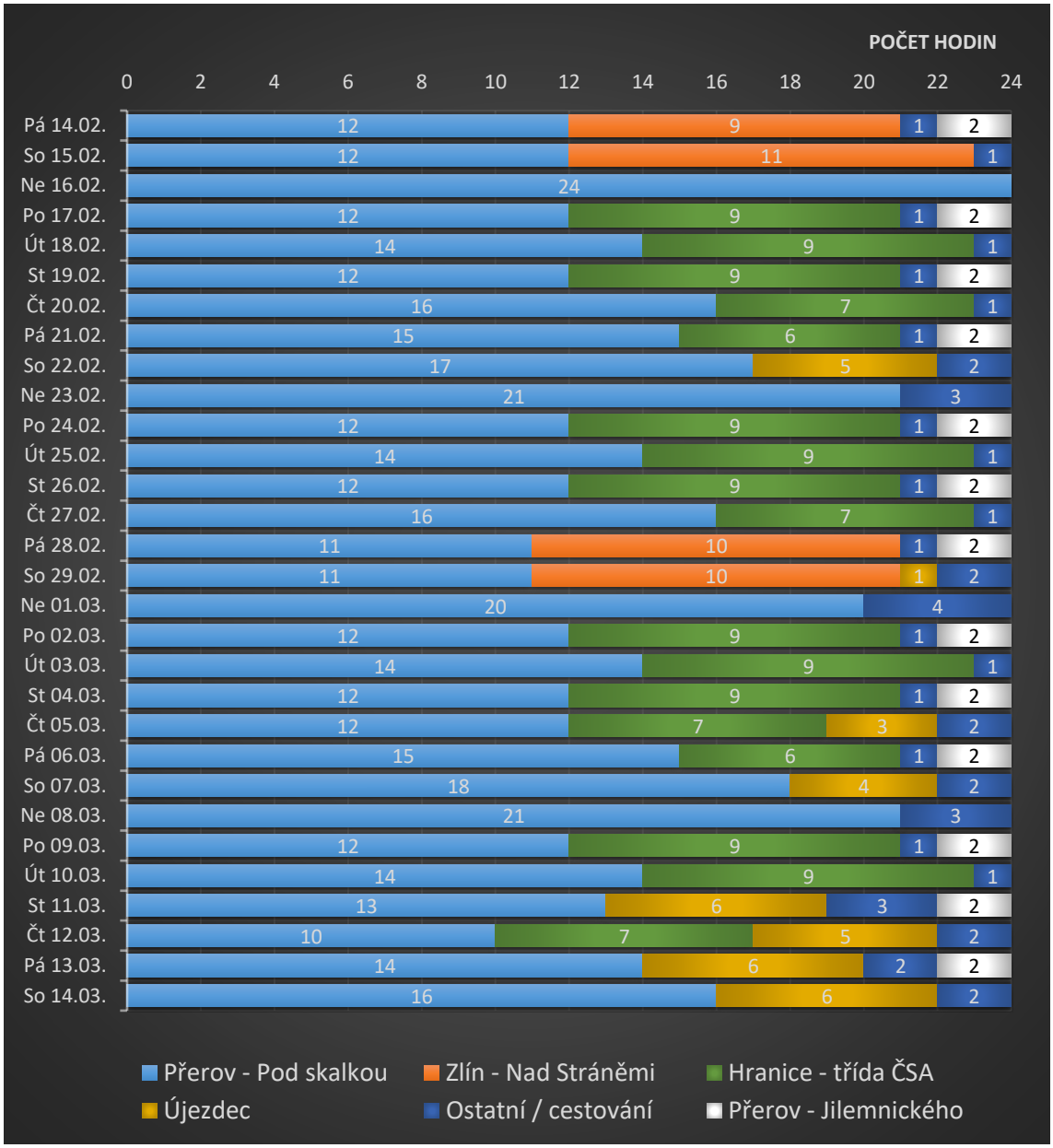
6.2.4 **Polohové údaje**

V této části se věnuji analýze polohových údajů, které aplikace Facebook v mém chytrém telefonu získala. K této analýze bylo potřeba udělit aplikaci oprávnění k přístupu k polohovým údajům. Data byla sbírána po dobu jednoho měsíce, přesněji od 14. února do 14. března 2020. Provedu ukázku toho, jak je možné ze získaných dat zjistit poměrně jednoduše například polohu bydliště, pracoviště či pravidelně navštěvovaných míst a zjistit tímto způsobem, v které dny a hodiny je daná osoba pravidelně mimo domov či na určitém místě.



Obr. 32. Zobrazení polohových údajů [archiv autora]

Při procházení zaznamenaných polohových údajů lze vyčíst i přesný čas strávený na určitém místě. Jako názornou ukázku jsem vybral pátek 6. března, kde lze tento časový údaj po rozkliknutí vidět. V levém menu lze sledovat všechny zaznamenané polohy za celý den.



Obr. 33. Analýza polohových dat – počet hodin strávených na určité poloze

[archiv autora]

Z těchto dat lze poměrně snadno odvodit, podle počtu strávených hodin na určitém místě a pravidelnosti výskytu, kde má dotyčná osoba bydliště, práci a další pravidelné aktivity.

Z mých dat za dané období lze tedy zjistit následující:

- Nejvíce času jsem strávil na poloze Přerov – Pod skalkou, což lze považovat za místo bydliště
- Druhá nejčastější zaznamenaná poloha – Hranice – třída ČSA, kde lze pozorovat pravidelnost ve dnech pondělí až pátek. Vzhledem k počtu strávených hodin lze logicky odvodit, že se jedná o místo pracoviště.
- Polohový údaj Přerov – Jilemnického, s pravidelným výskytem ve dnech pondělí, středa, pátek lze po prohlédnutí dat příspěvků na profilu, označit za adresu neoficiální posilovny.
- Další polohová data se vztahují k místu Zlín – Nad Stráněmi, opakující se každých 14 dní (mimo posledního týdne), lze odvodit, že se jedná o polohu FAI, kde strávím průměrně 10 hodin každý druhý pátek a sobotu.
- Pozorovat lze i určitou vazbu k poloze – Újezdec

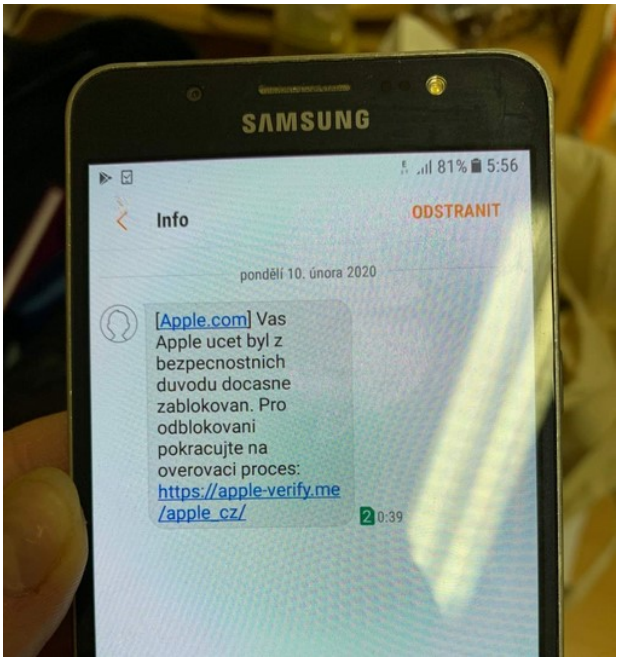
Z této krátké analýzy polohových dat si lze odvodit i související bezpečnostní rizika, která mohou představovat v případě, že by došlo k jejich zneužití (stalking, krádeže atd.). Stažená polohová data taktéž obsahují i přesné časové údaje, kdy se dotyčná osoba na určitém místě vyskytuje, avšak ty zde všechny z určitých důvodů uvádět nebudu. Viditelné jsou jako ukázka z jednoho dne na *Obr. 32*.

6.3 Opatření

Tato část navazuje na již vypsaná doporučení a opatření v teoretické části. Zaměřím se především na detekci samotného phishingu online nástrojem VirusTotal.com a dále doporučená nastavení aplikace Facebook a profilu, ke zvýšení soukromí a bezpečnosti při jejich používání.

6.3.1 **Detekce phishingu pomocí Virustotal.com**

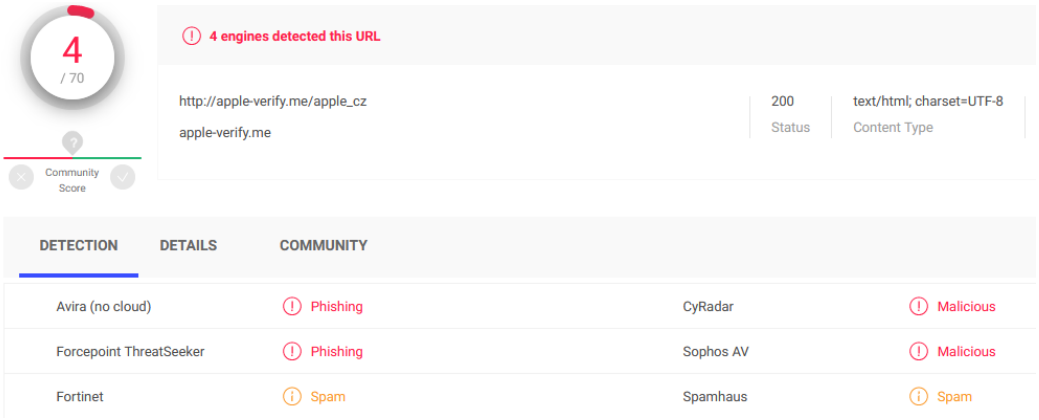
Během psaní teoretické části bakalářské práce jsem se shodou okolností setkal s phishingovým útokem skrze SMS zprávu, kterou obdržela má přítelkyně dne 10. února 2020. Zpráva upozorňovala na zablokování účtu u společnosti Apple a obsahovala také URL odkaz k jeho odblokaci viz. foto níže



Obr. 34. Phishingový útok ze dne 10.2.2020

[archiv autora]

K ověření, zda se jedná o phishingovou webovou stránku je možné využít online nástroj, dostupný na webové adrese VirusTotal.com, který zdarma analyzuje soubory i URL adresy a je schopný detekovat různé typy malware či phishing. Do pole pro analýzu URL adresy jsem tedy zadal odkaz, který obsahovala SMS zpráva. Výsledkem toho testu byl pozitivní nález phishingového či jinak škodlivého kódu ve čtyřech databázích antivirových společností.



Obr. 35. Výsledek testu nástrojem VirusTotal.com [79]

Stejným způsobem si lze otestovat jakoukoliv jinou URL adresu či soubor, u kterého si není uživatel jistý, zda neobsahuje malware, phishing či jiný prvek představující bezpečnostní

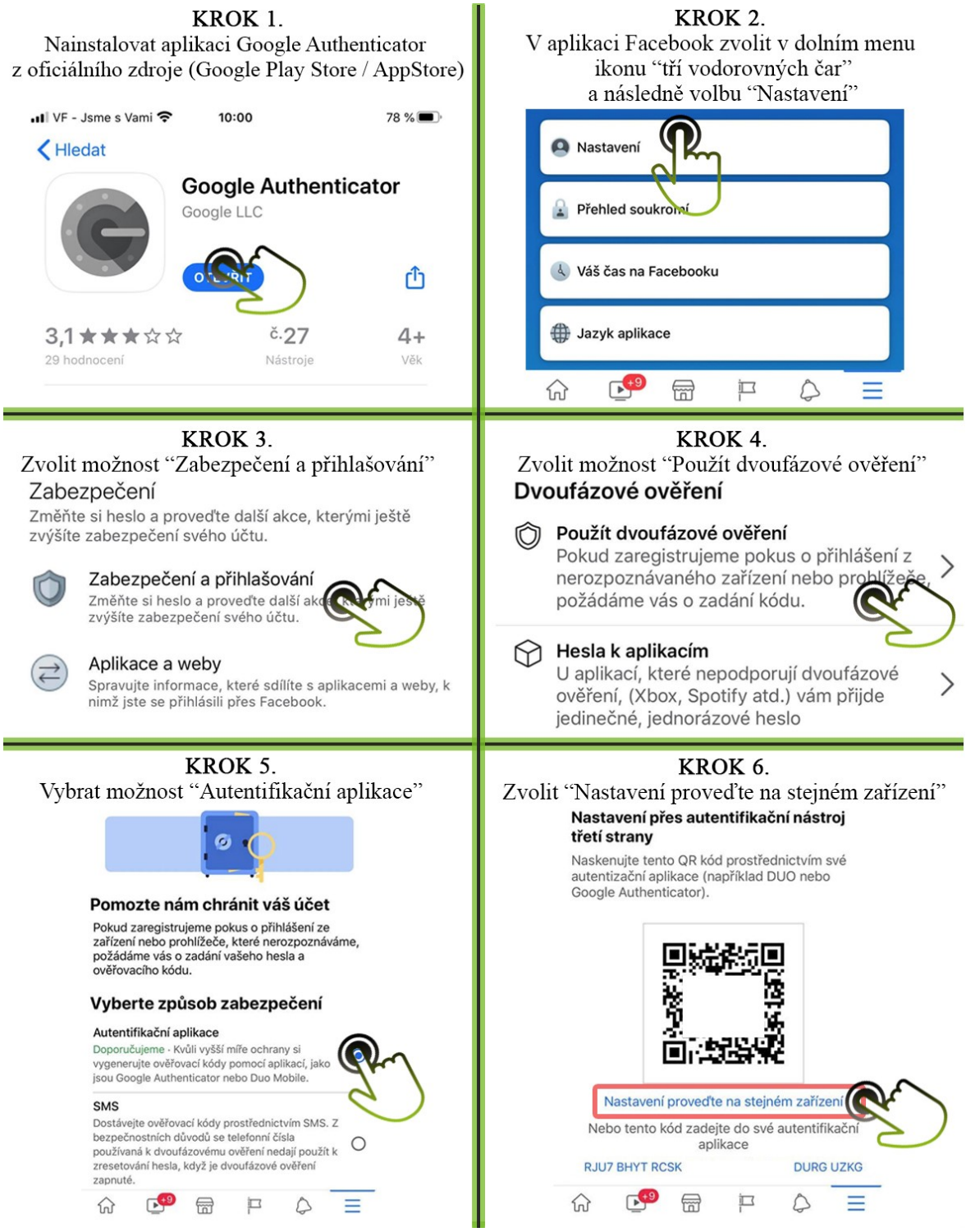
riziko. Je však nutno podotknout, že ne všechny hrozby jsou detekovány, kvůli množství, které jich denně vznikne.

6.3.2 Zvýšení bezpečnosti při využívání aplikace Facebook

Ke zvýšení bezpečnosti při využívání Facebook aplikace, doporučuji provést následující opatření.

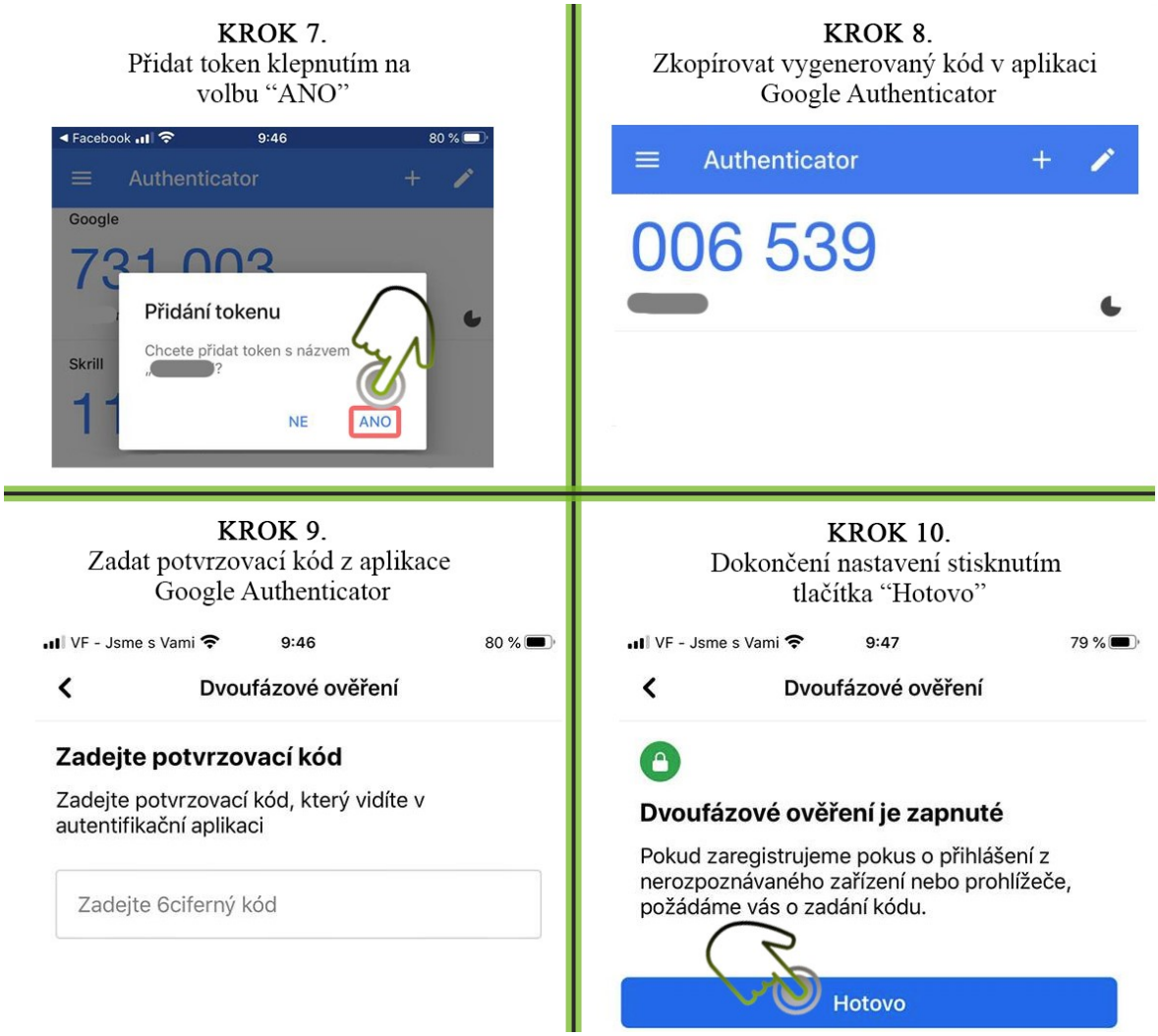
6.3.2.1 Dvoufázové ověření

Jedná se o nastavení, které zamezí přístupu k účtu uživatele z neznámého zařízení a vyzve jej k zadání ověřovacího kódu generovaného v aplikaci Google Authenticator. Tímto opatřením lze tedy výrazně snížit potenciální bezpečnostní rizika plynoucí z neoprávněného přístupu k účtu, osobním údajům a datům či jeho úplného odcizení.



Obr. 36. Kroky 1–6 k aktivaci dvoufázového ověření [archiv autora]

Po splnění těchto kroků dojde ke spuštění aplikace Google Authenticator, která je zodpovědná za generování potvrzovacích kódů.

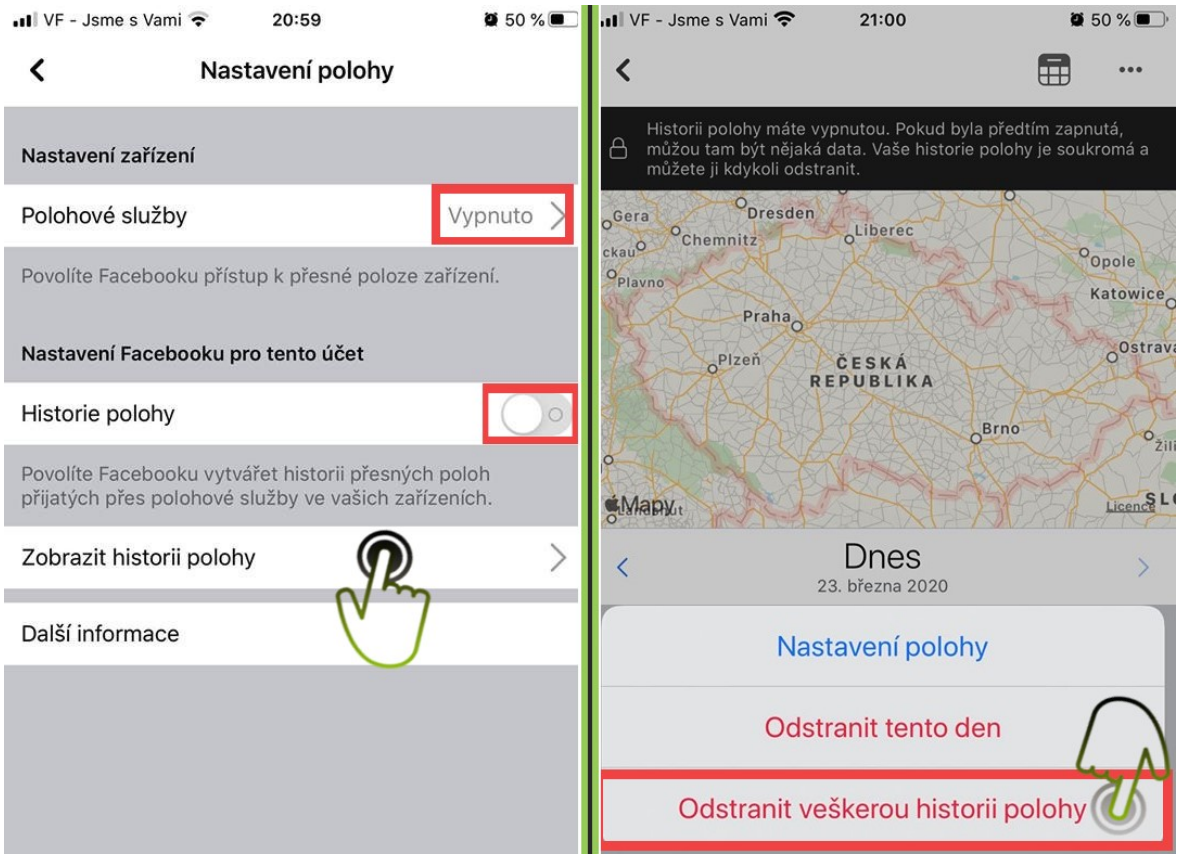


Obr. 37. Kroky 7–10 k aktivaci dvoufázového ověření [archiv autora]

Potvrzením nastavení, tlačítkem „Hotovo“, jsme úspěšně aktivovali ochranu našeho účtu v podobě dvoufázového ověření. V případě, že by se k účtu snažil přihlásit útočník, který nějakým způsobem získal přihlašovací údaje, aplikace tento přístup zablokuje a vyzve k zadání ověřovacího kódu z aplikace Google Authenticator.

6.3.2.2 Deaktivace využívání polohových údajů

Dalším bezpečnostním opatřením ke snížení rizika zneužití polohových údajů, je deaktivace využívání polohových služeb aplikací Facebook, včetně deaktivace vytváření historie přesných poloh a jejich smazání. K tomuto nastavení se opět, jako v předchozím případě, lze v aplikaci dostat přes možnost „Nastavení“ a příslušné položky s názvem „Poloha“.



Obr. 38. Deaktivace polohových služeb, vytváření historie polohy a její smazání [archiv autora]

Nastavením těchto hodnot lze zabránit snímání našich polohových údajů aplikací Facebook, které jsem analyzoval v předchozí kapitole. Odstraněním veškeré historie polohy eliminujeme riziko zneužití těchto údajů v případě zmocnění se zařízení či účtu neoprávněnou osobou.

ZÁVĚR

Teoretická část práce byla zaměřena především na různé druhy kriminality páchané v kyberprostoru a z ní vyplývající bezpečnostní rizika. Obsahem této části byla i má osobní zkušenost s kyberkriminalitou, přesněji phishingem a s následným odcizením financí. Poukazuje taktéž na rizika spojená s využíváním sociálních sítí prostřednictvím chytrých zařízení, a to především týkající se dětí, které se často stávají terčem kyberšikany či sextingu. Zároveň byly popsány základní pravidla či zásady, sloužící jako prevence a opatření.

V praktické části byla provedena ukázka toho, jakým způsobem vznikají phishingové webové stránky a jaká rizika phishing představuje v případě, že se útočník dostane k údajům a datům například Facebookového účtu. V mém případě se jednalo o data velikosti cca 15,3 GB, což se dá přirovnat k velikosti filmu v lepší kvalitě. Převážnou část, cca 9,55 GB tvořily fotky a videa. Mimo jiné tato data obsahovala spoustu osobních údajů typu: datum narození, bydliště, rodinné vazby, a dokonce i všechny emailové a telefonní kontakty (i včetně dávno smazaných).

Analýzou konverzací a hledané fráze „heslo“ jsem zjistil 22 stále platných přihlašovacích údajů k různým službám. Následnou analýzou polohových údajů jsem dospěl k závěru, že se z těchto údajů dá bez větších obtíží zjistit, kde má daná osoba bydliště, práci či jiná místa, které pravidelně navštěvuje, a to včetně časů, kdy se na těchto místech vyskytuje. Potvrdil jsem si tedy, že z pouhého měsíce snímání polohy aplikací Facebook lze z těchto dat kompletně zmapovat pohyb uživatele a využít tyto informace například k páchání další trestné činnosti. V návaznosti na tyto skutečnosti byly zpracovány postupy ke zjišťování kybernetických hrozeb pomocí online nástroje Virustotal.com a zabezpečení Facebook aplikace pomocí dvoufázového ověření, k minimalizaci rizika odcizení účtu a zneužití informací. V poslední řadě byl uveden postup k deaktivaci využívání polohových údajů a smazání veškeré historie polohy, kterou kdy aplikace Facebook získala.

SEZNAM POUŽITÉ LITERATURY

[1] ZELINKOVÁ, Věra. Kyberprostor – WikiKnihovna. *WikiKnihovna* [online]. [cit. 2020-02-09]. Dostupné z: http://wiki.knihovna.cz/index.php/Kyberprostor

[2] KOLOUCH, Jan. *CyberCrime* [online]. 1. Praha: CZ.NIC, z.s.p.o., 2016 [cit. 2019-12-12]. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[3] Internet. *Univerzitní informační systém MENDELU* [online]. Brno [cit. 2019-09-28]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=40844

[4] Internet – Wikipedie. *Wikipedie* [online]. [cit. 2019-09-28]. Dostupné z: https://cs.wikipedia.org/wiki/Internet

[5] Historie internetu v datech - 25 let v ČR. *ITPOINT.CZ* [online]. 2017 [cit. 2019-09-28]. Dostupné z: http://www.itpoint.cz/cesnet/clanky/?i=historie-internetu-25-let-cr-11512

[6] Počítače a internet v domácnostech. In: *Počítače a internet v domácnostech* [online]. 2018 [cit. 2019-09-28]. Dostupné z: https://www.czso.cz/documents/10180/61508128/06200818a.pdf/

[7] *Measuring the Information Society Report Volume 1 2018* [online]. Place des Nations CH-1211 Geneva 20 Switzerland: International Telecommunication Union, 2018 [cit. 2019-09-28]. ISBN 978-92-61-27231-9. Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

[8] H. WEIK, Martin. Computer Science and Communications Dictionary. *Springer* [online]. 2000 [cit. 2019-09-28]. Dostupné z: https://link.springer.com/referenceworkentry/10.1007%2F1-4020-0613-6_4119

[9] Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. [cit. 2020-02-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[10] KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. *CyberSecurity* [online]. Praha, 2019 [cit. 2020-02-14]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[11] STERLING, Bruce. *The hacker crackdown: law and disorder on the electronic frontier*. New York: Bantam Books, 1992. ISBN 05-530-8058-X.

[12] What is a Smart Device? - Definition from Techopedia. *Techopedia.com* [online]. [cit. 2019-12-11]. Dostupné z: https://www.techopedia.com/definition/31463/smart-device

[13] BROWN, Rich a Ry CRIST. The best smart home devices of 2019. *CNET: CNET is the world's leader in tech product reviews, news, prices, videos, forums, how-tos and more.* [online]. [cit. 2019-12-12]. Dostupné z: https://www.cnet.com/news/the-best-smart-home-devices-of-2019-amazon-alexa-google-assistant-apple-homekit-nest-hub-echo-show/

[14] KOVACS, Nadia. What is the Internet of Things? How the IoT works, and more. *Official Site | Norton™ - Antivirus; Anti-Malware Software* [online]. [cit. 2019-12-12]. Dostupné z: https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html

[15] The definition of Internet of Things: A simple explanation. In: *High-Speed, Secure & Anonymous VPN Service | ExpressVPN* [online]. [cit. 2019-12-12]. Dostupné z: https://www.expressvpn.com/blog/what-is-the-internet-of-things-iot/

[16] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). *Statista - The Statistics Portal for Market Data, Market Research and Market Studies* [online]. [cit. 2019-12-12]. Dostupné z: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[17] HARPER, Richard. *Inside the smart home* [online]. New York: Springer, 2003 [cit. 2019-12-16]. ISBN 18-523-3688-9. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.3611&rep=rep1&type=pdf

[18] ROBY, Karen. Why smart home devices may be an open invitation to hackers. *News, Tips, and Advice for Technology Professionals - TechRepublic* [online]. [cit. 2019-12-17]. Dostupné z: https://www.techrepublic.com/article/why-smart-home-devices-may-be-an-open-invitation-to-hackers/

[19] LOM, Ing. a Ph.D., PŘIBYL. Rizika chytrých zařízení a jejich zabezpečení. *Elektrotechnika - TZB-info* [online]. [cit. 2020-02-16]. Dostupné z: https://elektro.tzb-info.cz/inteligentni-budovy/15569-rizika-chytrych-zarizeni-a-jejich-zabezpeceni

[20] BENZL, Lukáš. Smart Home. In: *Elektřina.cz - vše co potřebujete vědět v oblasti energetiky a technologií* [online]. [cit. 2019-12-16]. Dostupné z: https://www.elektrina.cz/chytra-domacnost-setri-penize

[21] O nás | O AVAST Software. *Avast | Stáhněte si bezplatný antivirus a VPN | 100% zdarma a intuitivní* [online]. [cit. 2019-12-16]. Dostupné z: https://www.avast.com/cs-cz/about

[22] *Avast Smart Home Security Report 2019* [online]. In: . MOBILE WORLD CONGRESS, Barcelona, Španělsko, 2019 [cit. 2019-12-16]. Dostupné z: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf

[23] What is a Router? Webopedia Definition. *Webopedia: Online Tech Dictionary for IT Professionals* [online]. [cit. 2019-12-16]. Dostupné z: https://www.webopedia.com/TERM/R/router.html

[24] SCHUBERT, Christina. What is a router, and how does it work?. *Official Site | Norton™ - Antivirus; Anti-Malware Software* [online]. [cit. 2019-12-16]. Dostupné z: https://us.norton.com/internetsecurity-iot-smarter-home-what-is-router.html

[25] FOLTÝN, Tomáš. Most routers full of firmware flaws that leave users at risk. *WeLiveSecurity: WeLiveSecurity is an IT security site covering the latest news, research, cyberthreats and malware discoveries, with insights from ESET experts.* [online]. [cit.2019-12-16]. Dostupné z: https://www.welivesecurity.com/2018/10/08/routers-firmware-flaws-leave-users-risk/

[26] *Mobile and wireless technologies 2017* [online]. New York, NY: Springer Berlin Heidelberg, 2017 [cit. 2019-12-23]. ISBN 978-981-10-5280-4. Dostupné z: https://books.google.cz/books?id=Y1coDwAAQBAJ&printsec=front-cover&hl=cs&source=gbs_atb#v=onepage&q&f=false

[27] Android Open Source Project. *Android | The platform pushing what's possible* [online]. [cit. 2019-12-23]. Dostupné z: https://source.android.com/

[28] Mobile Operating System Market Share Worldwide | StatCounter Global Stats. *Web Analytics Made Easy - Statcounter* [online]. [cit. 2019-12-23]. Dostupné z: https://gs.statcounter.com/os-market-share/mobile/worldwide

[29] *METODIKA K VAROVÁNÍ ZE DNE 17. PROSINCE 2018* [online]. In: . 2018 [cit. 2020-02-16]. Dostupné z: https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

[30] *Apple* [online]. [cit. 2019-12-23]. Dostupné z: https://www.apple.com/

[31] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013 [cit. 2019-12-19]. ISBN 978-80-7251-397-0. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

[32] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství* [online]. Praha: Grada, 2007 [cit. 2020-01-10]. ISBN 978-80-247-1561-2. Dostupné z: https://books.google.cz/books?id=0TxDiektLJQC&lpg=PA91&ots=mHkpZafIKU&dq=Kybernetick%C3%A1%20kriminalita%20jirkovsk%C3%BD&hl=cs&pg=PA56#v=snippet&q=white&f=false

[33] What is the Difference Between Black, White and Grey Hat Hackers?. *Official Site | Norton™ - Antivirus & Anti-Malware Software* [online]. Mountain View, 2019 [cit. 2019-09-19]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

[34] The number of mobile malware attacks doubles in 2018, as cybercriminals sharpen their distribution strategies. *Expert Cyber Security Solutions for Home & Business |*

Kaspersky [online]. [cit. 2020-01-13]. Dostupné z: https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies

[35] Agresivní reklama nabízí falešný antivir. Nic nepotvrzujte. In: *IDNES.cz – s námi víte víc: Nejnovější zprávy z vašeho kraje, České republiky a celého světa.* [online]. [cit. 2020-01-17]. Dostupné z: https://www.idnes.cz/mobil/tech-trendy/foto/NYV61f6fa_malvertising.png

[36] CORRIGAN, Caroline. What is ransomware and how does it work?. *AVG 2020 | FREE Antivirus, VPN & TuneUp for All Your Devices* [online]. [cit. 2020-01-15]. Dostupné z: https://www.avg.com/en/signal/android-ransomware-guide

[37] STEFANKO, Lukas. Android ransomware is back. *WeLiveSecurity* [online]. [cit. 2020-01-15]. Dostupné z: https://www.welivesecurity.com/2019/07/29/android-ransomware-back/

[38] A ransom note displayed by Android/Filecoder.C. In: *WeLiveSecurity* [online]. [cit. 2020-01-16]. Dostupné z: https://www.welivesecurity.com/wp-content/uploads/2019/07/Figure-7-576x1024.png

[39] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015 [cit. 2019-12-15]. Průvodce (Grada). ISBN 978-80-247-5453-6.

[40] Avoiding Cell Phone Spyware Infestation. *Expert Cyber Security Solutions for Home & Business | Kaspersky* [online]. [cit. 2020-01-13]. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/cell-phone-spyware

[41] Can Your iPhone or Android Phone Get a Virus?. *Avast | Download Free Antivirus & VPN | 100% Free & Easy* [online]. [cit. 2020-01-16]. Dostupné z: https://www.avast.com/c-can-phones-get-viruses

[42] What is a Trojan? Is it a virus or is it malware?. *Official Site | Norton™ - Antivirus & Anti-Malware Software* [online]. [cit. 2020-01-16]. Dostupné z: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

[43] Malicious Android app had more than 100 million downloads in Google Play. *Expert Cyber Security Solutions for Home & Business | Kaspersky* [online]. [cit. 2020-02-01]. Dostupné z: https://www.kaspersky.com/blog/camscanner-malicious-android-app/28156/

[44] TRLICA, David. Pozor na nahrávač hovorů QRecorder: Aplikace vybírá bankovní účty českým klientům. *Homepage - Svět Androida* [online]. [cit. 2020-02-19]. Dostupné z: https://www.svetandroida.cz/nahravac-hovoru-qrecorder-malware/

[45] QRecorder trojan. In: *IT SECURITY NETWORK NEWS; Security, antivirus, malware* [online]. [cit. 2020-02-19]. Dostupné z: https://www.itsec-nn.com/wp-content/uploads/QRecorder-trojan.jpg

[46] Zákon č. 40/2009 Sb.: Zákon trestní zákoník. In: *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. [cit. 2020-02-05]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40/zneni-20191201

[47] DUNHAM, Ken. *Mobile malware attacks and defense* [online]. Burlington, MA: Elsevier, 2009 [cit. 2020-01-17]. ISBN 978-1-59749-298-0. Dostupné z: https://books.google.cz/books?id=Nd1RcGWMKnEC&pg

[48] Phishing zaměřený na klienty Raiffeisenbank ČR - nenechte se nachytat, odkazy vedou na podvodné stránky. In: *Projekt E-Bezpečí - Hlavní stránka* [online]. [cit. 2020-02-13]. Dostupné z: https://scontent.fprg2-1.fna.fbcdn.net/v/t1.0-9/85015022_10158363941506122_636642207717130240_o.jpg?_nc_cat=106&_nc_oc=AQnD1cQ3DzvS1-8ZCd_vgi3Zz8KDn78VTyYlvuGup250Dwm2DYygtKW14PGSw1BwnaQ&_nc_ht=scontent.fprg2-1.fna&oh=2f71428c5403f40155b4f301da81cd3f&oe=5EC0EF00

[49] Upozornění na nový phishingový útok. In: *Česká spořitelna* [online]. [cit. 2020-01-17]. Dostupné z: https://cdn0.erstegroup.com/content/sites/cz/csas/www_csas_cz/cs/zpravy-z-banky/2017/10/09/upozorneni-na-novy-phishingovy-utok/_jcr_content/mainParsys/textwithimage_1762737388/image.fitIn.w950.png/1507545629340150754557 4501.png

[50] The risks of public Wi-Fi. *Official Site | Norton™ - Antivirus & Anti-Malware Software* [online]. [cit. 2020-02-02]. Dostupné z: https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

[51] PANÁK, Martin. DDoS útok loni řešila třetina českých firem. Jak se bránit?. *Lupa.cz - server o českém Internetu: Svět IT, dění na trhu, bezpečnost na internetu, připojení k internetu, mobilní internet, online média a reklama, cloudové služby.* [online]. [cit. 2020-02-02]. Dostupné z: https://www.lupa.cz/market-voice/ddos-utok-loni-resila-tretina-ceskych-firem-jak-se-branit/

[52] *Computer forensics: Investigating Network Intrusions and Cybercrime (CHFI)* [online]. Second edition. Boston: Cengage Learning, 2017 [cit. 2020-02-02]. ISBN 978-1305883505. Dostupné z: https://books.google.cz/books?id=5QFVDAAAQBAJ&pg=PA53&dq=sniffing+cybercrime&hl=cs&sa=X&ved=0ahUKEwiWqv355bDnAhUHPFAKHXOlBhEQ6AEISzAD#v=onepage&q=identity%20theft&f=false

[53] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem* [online]. Praha: Grada, 2013 [cit. 2020-02-02]. Psyché (Grada). ISBN 978-80-247-4577-0. Dostupné z: https://books.google.cz/books?id=117XAgAAQBAJ&lpg=PA1&dq=kyber%C5%A1ikana&hl=cs&pg=PA4#v=onepage&q=kyber%C5%A1ikana&f=false

[54] JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. *Internetové právo* [online]. Brno: Computer Press, 2017 [cit. 2020-02-05]. ISBN 978-80-251-4884-6. Dostupné z: https://books.google.cz/books?id=Uhy2DwAAQBAJ&lpg=PA409&dq=cybergrooming&hl=cs&pg=PA1#v=onepage&q=cybergrooming&f=false

[55] Co je sexting. *Sexting.cz - vše, co chcete vědět o sextingu* [online]. [cit. 2020-02-02]. Dostupné z: http://www.sexting.cz/

[56] V síti (2020) | ČSFD.cz: 3 herečky, 3 pokojíčky, 10 dní a 2458 sexuálních predátorů. Radikální experiment otevírá tabuizované téma zneužívání dětí na internetu. Tři dospělé herečky s dětskými rysy se vydávají na sociální sítě, aby v přímém přenosu prožily zkušenost…. *Česko-Slovenská filmová databáze | ČSFD.cz* [online]. [cit. 2020-02-04]. Dostupné z: https://www.csfd.cz/film/720753-v-siti/prehled/

[57] Tereza Těžká. In: *Česko-Slovenská filmová databáze | ČSFD.cz* [online]. [cit. 2020-02-04]. Dostupné z: https://img.csfd.cz/files/images/film/photos/164/167/164167054_51a26c.jpg

[58] TOTALFILM.CZ, Kanál uživatele. V síti (2020) oficiální hlavní trailer. In: *YouTube* [online]. [cit. 2020-03-06]. Dostupné z: https://www.youtube.com/watch?time_continue=98&v=DEllhM2K_-s&feature=emb_logo

[59] Bezpečnostní hrozby - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. [cit. 2019-12-19]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D

[60] MCGUIRE, Dr. *SOCIAL MEDIA PLATFORMS ANDTHE CYBERCRIME ECONOMY* [online]. In: . 2019 [cit. 2019-12-06]. Dostupné z: https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

[61] Most popular social networks worldwide as of October 2019, ranked by number of active users (in millions). *Statista - The Statistics Portal for Market Data, Market Research and Market Studies* [online]. [cit. 2019-12-19]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[62] Company Info | Facebook Newsroom. *Facebook Newsroom* [online]. 2019 [cit. 2019-11-09]. Dostupné z: https://newsroom.fb.com/company-info/

[63] Facebook Marketplace: Nakupujte a prodávejte položky v místě, nebo si je nechte doručit. *Facebook* [online]. [cit. 2019-12-15]. Dostupné z: https://www.facebook.com/marketplace/

[64] *Facebook* [online]. [cit. 2019-12-06]. Dostupné z: https://www.facebook.com/

[65] Vytvořte a sdílejte svůj příběh | Centrum nápovědy na Facebooku. *Facebook* [online]. [cit. 2020-02-08]. Dostupné z: https://www.facebook.com/help/126560554619115

[66] Jak na Internet - Rizika sociálních sítí. *Jak na Internet - Jak na Internet* [online]. [cit. 2020-02-11]. Dostupné z: https://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/

[67] Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů. In: *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. [cit. 2020-02-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

[68] KOPECKÝ, Kamil. *České děti a Facebook 2015* [online]. Univerzita Palackého v Olomouci, Pedagogická fakulta, Centrum prevence rizikové virtuální komunikace, 2015 [cit. 2020-02-13]. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/76-ceske-deti-a-facebook-2015/file

[69] Co je to hoax. *HOAX | podvodné a řetězové e-maily, poplašné zprávy, phishing, scam* [online]. [cit. 2020-02-16]. Dostupné z: https://www.hoax.cz/hoax/co-je-to-hoax

[70] EMPEY, Charlotte. Jak si nastavit silné heslo. *Avast Blog* [online]. 2020 [cit. 2020-07-12]. Dostupné z: https://blog.avast.com/cs/jak-si-nastavit-silne-heslo

[71] POSPÍŠIL, Aleš. Češi podceňují kyberbezpečnost, mají slabá hesla. *E15.cz - Byznys, politika, ekonomika, finance, události* [online]. 2020 [cit. 2020-03-06]. Dostupné z: https://www.e15.cz/finexpert/setrime/cesi-podcenuji-kyberbezpecnost-maji-slaba-hesla-1339951

[72] Bezplatná antivirová aplikace pro Android | Avast Mobile Security. *Avast | Stáhněte si bezplatný antivirus a VPN | 100% zdarma a intuitivní* [online]. ©1988-2020 [cit. 2020-03-06]. Dostupné z: https://www.avast.com/cs-cz/free-mobile-security

[73] HO AU, Man a Raymond CHOO. *Mobile Security and Privacy: Advances, Challenges and Future Research Directions* [online]. Syngress, 2016 [cit. 2020-03-04]. ISBN 9780128046296. Dostupné z: https://books.google.cz/books?id=iANaCgAAQBAJ&lpg=PP1&dq=mobile%20security%20and%20privacy&hl=cs&pg=PP1#v=onepage&q=turn%20off%20location&f=false

[74] NEWMAN, Lily Hay. Burglars Really Do Use Bluetooth Scanners to Find Laptops and Phones. *WIRED* [online]. 2018 [cit. 2020-03-07]. Dostupné z: https://www.wired.com/story/bluetooth-scanner-car-thefts/

[75] HARISOVÁ, Sabrina. Konec loudění hanbatých fotek? Aplikace brání dětem v sextingu, má ale stále své mouchy. *Reflex.cz - Komentáře, zprávy, výrazné autorské fotografie* [online]. 2020 [cit. 2020-03-07]. Dostupné z: https://www.reflex.cz/clanek/zpravy/87112/konec-loudeni-hanbatych-fotek-aplikace-brani-detem-v-sextingu-ma-ale-stale-sve-mouchy.html

[76] SAPKALE, Yash. *Access Denied: Hacking For Beginners* [online]. 2015 [cit. 2020-02-20]. ISBN 9781329489646. Dostupné z: https://books.google.cz/books?id=02toCgAAQBAJ&lpg=PT31&ots=i6CpE2fznb&hl=cs&pg=PT31#v=onepage&q=php&f=false

[77] *XAMPP Installers and Downloads for Apache Friends* [online]. [cit. 2020-02-20]. Dostupné z: https://www.apachefriends.org

[78] Stažení vašich informací. *Facebook – přihlaste se, nebo se zaregistrujte* [online]. 2020 [cit. 2020-03-08]. Dostupné z: https://www.facebook.com/dyi/?x=AdkRCga5tjTHZ1HT&referrer=yfi_settings&tab=new_archive

[79] VirusTotal. *VirusTotal* [online]. [cit. 2020-03-18]. Dostupné z: https://www.virustotal.com/gui/url/48ffe18099d448dac832aea1c57c368e6a909c56a9736f6c7c5c5045e441cea7/detection

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT	(Information and Communications Technology) Informační a komunikační technologie
TCP/IP	Protokol pro síťovou komunikaci
WWW	World Wide Web
ČVUT	České vysoké učení technické v Praze
ITU	International Telecommunication Union (Mezinárodní telekomunikační unie)
IoT	Internet of Things (internet věcí)
SMS	Short Message Service (služba pro krátké textové zprávy)
GPS	Global Positioning Systém (globální poziční systém)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDF	Portable Document Format (formát pro dokumenty)
OCR	Optical Character Recognition (optické rozpoznávání znaků)
URL	Uniform Resource Locator – adresa informací v síti internet
Wi-Fi	Bezdrátová komunikace / síť
(D)DoS	(Distributed) Denial of Service – (distribuované) odepření služby
HTTP	Hypertext Transfer Protocol – protokol pro komunikaci webového prohlížeče a serveru
HTTPS	Hypertext Transfer Protocol Secure – protokol pro komunikaci webového prohlížeče a serveru (zabezpečený)
PIN kód	Číselný kód
HTML	Hypertext Markup Language – textový značkovací jazyk
PHP	Skriptovací jazyk webových stránek aplikací
GB	GigaByte – jednotka množství dat
IP adresa	Logická adresa zařízení v síti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK