Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra systémové analýzy

Študijný program: Aplikovaná informatika

Obor: Informatika

Phishing a vhodná ochrana proti nemu

BAKALÁRSKA PRÁCA

Študent : Miloš Olejár

Vedúci : Ing. Ladislav Luc

Oponent : Ing. Jakub Novotný, Ph.D.

2018

Prehlásenie:

Čestne prehlasujem, že som bakalársku prácu spracoval samostatne a že som uviedol všetky použité pramene a literatúru, z ktorej som čerpal.

V Prahe 20. apríla 2018 . . . . . .

Miloš Olejár

Poďakovanie

Veľmi rád by som sa poďakoval Ing. Ladislavovi Lucovi za ochotu, užitočné rady a pripomienky, ktoré mi poskytol pri spracovaní tejto bakalárskej práce.

Abstrakt

Táto bakalárska práca sa zaoberá phishingom ako takým a vhodnou ochranou proti nemu. Na začiatku práce sa čitateľ najskôr oboznámi tým čo je to phishing, aké typy možných phishingových útokov existujú a aký je za takéto útoky trestnoprávny postih v Českej republike. Taktiež sú popísané najčastejšie profily možných útočníkov. V ďalšej časti je predstavená história phishingu od jeho úplných začiatkov, jeho postupný vývoj a samozrejme nechýbajú ani súčasné štatistiky. Následne je popísaný priebeh typického phishingového útoku od jeho naplánovania, vytvorenia jednoduchej phishingovej stránky až po profit z úspešného útoku. V závere teoretickej časti tejto bakalárskej práce sú popísané príklady reálnych phishingových útokov. V praktickej časti práce sú na konkrétnom vzorku aktívnych phishingových stránok otestované najčastejšie používané internetové prehliadače ako prvotná ochrana pri odhalení phishingovej stránky. Zároveň sú popísané aj odporúčania ako je možné phishingovú stránku čo najjednoduchšie odhaliť.

Kľúčové slová

phishing, phishingové emaily, sociálne inžinierstvo, IDN, anti-phishing, webové prehliadače

Abstract

This Bachelor Thesis deals with phishing as such and with proper protection against it. At the beginning of this work, reader first gets acquainted with what phishing is, what are the possible types of phishing attacks and what is the criminal sanction for such attacks in the Czech Republic. Accordingly, the most frequently used profiles of attackers are described. The next section is devoted to the introduction to history of phishing from its early beginnings, through its successive evolution and, of course, the current statistics are not missing. Subsequently, the story of typical phishing attack is described, from early planning, through the creation of a simple phishing web page to the profit from the successful attack. At the end of the theoretical section of this work, examples of real phishing attacks are described. In the practical section, the most commonly used internet browsers are tested on a specific example of an active phishing web page as the primary protection when a phishing attack is detected. At the same time, recommendations are made on how to phishing web page can be detected as easily as possible.

Keywords

phishing, phishing e-mails, social engineering, IDN, anti-phishing, web browsers

Obsah

1 Úvod

1.1 Cieľ práce

V dnešnej dobe ešte stále len veľmi nízky počet užívateľov internetu pozná pojem phishing a zároveň aj jeho riziká. Práve z toho dôvodu je cieľom tejto bakalárskej práce predovšetkým oboznámiť čitateľa čo tento pojem vlastne znamená, aké rôzne typy phishingových útokov existujú a ako sa proti nim čo najúčinnejšie brániť. Taktiež otestujem najbežnejšie webové prehliadače na konkrétnej vzorke reálnych phishingových strán ok. Následne podľa výsledkov testu vyhodnotím, ktoré webové prehliadače sú pri odhaľovaní phishingových stránok najspoľahlivejšie, v prípade zanedbania či úplnej absencie bezpečnostného softwaru, ktorý je aj napriek všetkým možným hrozbám stále často podceňovaný.

1.2 Štruktúra práce

V úvode bakalárskej práce je bližšie popísaný pojem phishing, jeho druhy, možný postih za vykonávanie phishingu a typy najčastejších útočníkov. Následne je čitateľovi priblížená história, kompletný podrobný priebeh emailového phishingového útoku, ale aj príklady útokov, ktoré sa odohrali v blízkej minulosti.

Testovanie jednotlivých prehliadačov prebiehalo na predom vybranej vzorke sto aktívnych phishingových stránok, ktoré boli zoradené v tabuľke. Tieto stránky sú z oblastí s rôznym zameraním ako napríklad finančný sektor, sociálne siete, cloudové služby a pod. Zistené výsledky boli ďalej vyhodnotené podľa predom stanovených kritérií. Následne na základe hodnotenia je odporúčané najbezpečnejšie riešenie pre užívateľské využitie.

1.3 Rešerš

Autor pri písaní tejto bakalárskej práce čerpal z rôznych zdrojov či už išlo o internetové články alebo knihy s danou tematikou. Pri písaní o phishingu všeobecne, jeho rôznych formách a postupe pri útokoch autor používal najmä zdroje „CyberCrime“ od Jána Koloucha a „Phishing bez záhad“ od autora Lance Jamesa.

V praktickej časti autor použil vzorky phishingových stránok z webu *„https://www.phishtank.com“*, ktorá sa zameriava na odhaľovanie podvodných stránok, ich následný popis a evidenciu. Táto časť, ktorá je zameraná na prvotnú ochranu voči

phishingovým stránkam bez použitia špeciálneho softwaru by mala nepriamo nadviazať na bakalársku prácu od autora Eduarda Beneša s názvom „Phishing a vhodná ochrana proti němu“, ktorý sa zameral práve na rôzny špecializovaný anti-phishingový software.

2 Phishing

Phishing predstavuje modernú formu sociálneho inžinierstva, ktorá využíva technické ale aj netechnické prostriedky s cieľom dostať sa k citlivý informáciám ako napríklad užívateľské mená, heslá, čísla kreditných kariet, PIN kódy a pod. Phishing môžeme chápať v užšom a širšom slova zmysle, ktoré sa líšia v akej miere je potrebná interakcia užívateľa. Avšak v oboch prípadoch je cieľ identický, a to oklamať užívateľa. [1] [5] [11]

V užšom slova zmysle sa jedná o činnosť kedy sa od užívateľa vyžaduje navštívenie určitej webovej stránky, vo väčšine prípadoch ide o stránky internetového bankovníctva, online obchodov a pod., ktorá je svojou adresou a vzhľadom takmer na nerozpoznanie od skutočnej stránky konkrétnej bankovej či nebankovej inštitúcie. Na takejto stránke je následne užívateľ vyzvaný, aby vyplnil svoje prihlasovacie údaje pre pokračovanie. [1]

V širšom slova zmysle je možné phishing chápať ako akékoľvek podvodné jednanie, pomocou ktorého si útočník najprv získa užívateľovu dôveru čím následne zníži jeho ostražitosť a tým prinúti užívateľa postupovať podľa predom pripraveného scenára. V danom prípade už nie je potrebné, aby užívateľ na stránkach zadával svoje údaje, ale na jeho emailovú adresu mu je doručený email s infikovanou prílohou alebo je jednoducho presmerovaný na stránku obsahujúcu malware, ktorý si potrebné údaje časom zozbiera aj sám bez toho, aby užívateľ mal nejaké podozrenie. [1]

2.1 Typy phishingových útokov

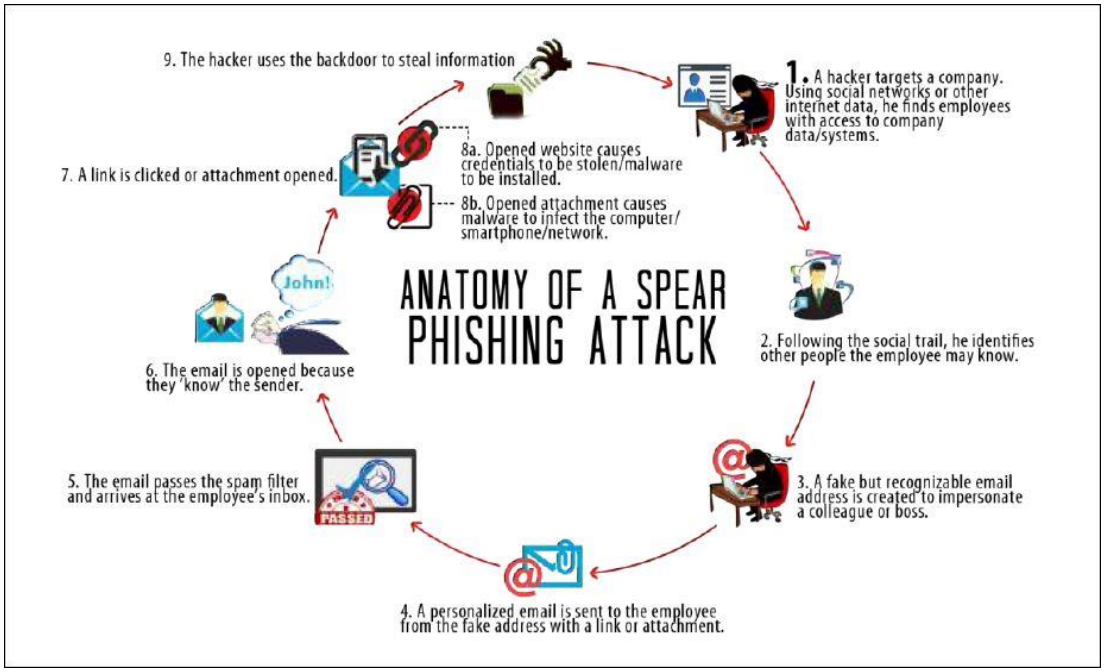
2.1.1 Pharming

Pharming patrí medzi nebezpečnejšiu a viac prepracovanú formu útoku. V tomto prípade ide o útok priamo na DNS server, ktorý slúži na preklad doménového mena webovej stránky na IP adresu. Celý útok začína až v momente keď užívateľ v prehliadači potvrdí danú adresu stránky. Za normálnych okolností by došlo k prepojeniu na danú IP adresu a užívateľovi by sa zobrazila konkrétna stránka, na ktorú sa chcel dostať. Avšak v tomto prípade dôjde k prepojeniu na inú IP adresu práve podvodnej stránky. Táto stránka je samozrejme vzhľadovo takmer na nerozpoznanie od tej originálnej a teda užívateľ má skoro nulovú šancu zistiť, že sa jedná o podvod. [1]

"Falošné webové stránky môžu slúžiť k inštalácii vírusov alebo trójskych koní do užívateľovho počítača alebo sa pomocou nich môžu útočníci pokúsiť získať osobné či finančné údaje, ktoré môžu byť následne zneužité ku krádeži identity. Pharming je zvlášť nebezpečná forma kyberkriminality, pretože v prípade nakazeného serveru DNS sa môže užívateľ stať obeťou i v prípade, že v jeho počítači nie je nainštalovaný vôbec žiadny malware. Dokonca ani keď používate preventívne opatrenia, napríklad zadávate internetové adresy ručne alebo používate výhradne dôveryhodné záložky, nie ste pred útokom tohoto druhu chránení, pretože k nechcenému presmerovaniu dochádza až potom, čo počítač odošle žiadosť o spojenie." [1]

2.1.2 Spear Phishing

Spear phishing sa od klasického phishingu líši predovšetkým tým, že tento útok sa nesústredí na náhodné ciele, ale je práve zameraný na konkrétnu organizáciu alebo spoločnosť, presnejšie na ich dáta a informácie ako napr. duševné vlastníctvo, osobné a finančné údaje, obchodná stratégia, tajné informácie a pod. Ďalším podstatným rozdielom je aj odosielateľ phishingových správ. Na úplnom začiatku je to práve útočník, ktorý si najprv z voľne dostupných zdrojov zistí čo najviac informácií o danej organizácii, jej štruktúru a pod. Následne vytvorí dôveryhodne vyzerajúcu emailovú správu a začne komunikovať s osobou, ktorá pracuje v danej spoločnosti. Útočník s touto osobou komunikuje ako by sa jednalo o jeho kolegu a využije ju k šíreniu danej správy. Táto správa obsahuje buď odkaz na určitú webovú stránku obsahujúcu malware alebo prílohu, ktorá po otvorení nainštaluje do počítača obete škodlivý software. Keďže užívatelia považujú odosielateľa správy za dôveryhodného, tak ich ostražitosť sa zníži na minimum a bez najmenšieho podozrenia otvoria obsah daného emailu. [1]



Obrázok 1 Spear phishing
Zdroj: [1]

2.1.3 Vishing

Tento pojem kombinuje slová voice (hlas) a phishing, teda sa jedná o phishing po telefóne. V tomto prípade sa útočník predstaví ako zástupca nejakej banky prípadne inej inštitúcie a za pomoci využitia sociálneho inžinierstva sa snaží od obete získať citlivé údaje v podobe čísla účtu, prihlasovacieho mena a hesla do internetového bankovníctva a pod. Využíva sa predovšetkým vo VoIP (Voice over Internet Protocol) komunikácii. Týmto spôsobom sa taktiež útočníci snažia získať aj informácie o firmách. Vo väčšine prípadoch jednoducho zavolajú na helpdesk danej spoločnosti a začnú komunikovať so zamestnancom. Do tejto ich nenápadnej konverzácie vložia útočníci správne načasované otázky, na ktoré chcú odpovede. V tomto prípade je útočník skúsený sociotechnik, ktorý presne vie ako danú konverzáciu usmerniť správnym smerom, aby nevzbudil podozrenie a zároveň sa dozvedel všetko čo potrebuje. K tomu naviac prispieva fakt, že častokrát zamestnanci helpdesku nie sú dostatočne vyškolení v oblasti bezpečnosti a tým pádom neriešia prečo sa ich niekto pýta dané otázky, ale snažia sa len automaticky a čo najrýchlejšie všetko zodpovedať a venovať sa ďalšiemu volajúcemu. [1] [2]

2.1.4 Smishing

Smishing je ďalší typ phishingu, ktorý využíva SMS správy na to, aby od užívateľa vylákal citlivé údaje. Takáto správa obyčajne obsahuje nejakú URL adresu a po jej otvorení je často

potrebné vyplniť nejaké osobné údaje. Taktiež ale obsahom SMS môže byť aj obyčajné telefónne číslo, na ktoré má daná osoba zavolať, pretože došlo napríklad k zablokovaniu kreditnej karty. Hovor na takéto číslo je samozrejme spoplatnený veľmi vysokou čiastkou. [1] [4]

2.2 Trestnoprávny postih

Phishing v Českej Republike je klasifikovaný ako istý druh podvodného jednania, ktorý je dokonaný obohatením sa a je ho možné postihnúť podľa §209 (Podvod) Trestného zákonníka. Taktiež podľa §209 Trestného zákonníka sa postihuje aj vytvorenie podvodnej stránky a následné získanie prihlasovacích údajov. Táto činnosť sa kvalifikuje ako príprava alebo pokus z trestného činu, ale následné získanie prístupových hesiel či PIN kódov od kreditných kariet bez ich ďalšieho zneužitia už trestné nie je. [1]

Ak sa jedná o phishingové útoky, ktoré využívajú aj rôzne druhy malware k tomu, aby infikovali počítač, tak takúto činnosť útočníka je možné postihnúť taktiež podľa §230 (Neoprávnený prístup k počítačovému systému a nosiču informácií) Trestného zákonníka. Ustanovenie §230 odst.3 Trestného zákonníka je možné uplatniť v prípade, ak je cieľom útoku získať sebe alebo niekomu inému neoprávnený prospech. [1]

Za určitých okolností je ešte možné použiť aj ustanovenie §234 (Neoprávnené opatrenie, falšovanie a pozmenenie platobného prostriedku) Trestného zákonníka. [1]

V prípade pharmingu, spear phishingu, vishingu a smishingu je trestnoprávny postih identický ako u klasického phishingu. Avšak typ útoku spear phishing môže vykonať aj teroristická organizácia, a preto podľa okolností to je možné ohodnotiť aj ako teroristický čin podľa §311 Trestného zákonníka. [1]

2.3 Profil útočníkov

Zistiť kto sa reálne skrýva za všetkými tými phishingovými útokmi nie je vždy jednoduché. Ale všeobecne platí, že je dobré poznať svojho nepriateľa. V tomto prípade jednoducho kto sú tí ľudia čo chcú ukradnúť práve naše dáta a z akého dôvodu. Môže sa jednať len o znudených teenagerov čo sa práve hrajú s phishingovými nástrojmi, ale môže ísť aj o mafiu. [15]

Existujú rôzne phishingové komunity a diskusné fóra kde si útočníci vymieňajú nové informácie a všelijaké tipy a triky. Predovšetkým to aké metódy fungujú najlepšie alebo ako to ešte vylepšiť, kto je ľahký cieľ a kto zase náročný. Taktiež mnoho z daných užívateľov sa snaží svoje útoky obhajovať predovšetkým argumentom, že okrádajú len veľké a bohaté organizácie. Avšak v tomto by im určite mohla oponovať osoba, ktorá sa stala napríklad obeťou krádeže identity. [15]

2.3.1 Script kiddies

Tieto tzv. *„skriptovacie deti"* používajú vírusové nástroje na šírenie malwaru a podvádzajú v počítačových hrách, aby vyhrávali. Práve phishing AOL ich zlákal na vlnu phishingu, pretože to bolo jednoduché a dokázal to ktokoľvek. Potrebné nástroje k tomu získavajú z rôznych voľne dostupných stránok na internete. Peniaze, ktoré získali buď predajom získaných údajov alebo priamo ukradli svojej obeti využívajú na kúpu nových počítačov, hier, telefónov a pod. [15]

2.3.2 Hackeri

Skutoční hackeri vo väčšine prípadoch využívajú omnoho sofistikovanejšie metódy útokov. Dokážu vyvinúť vlastný malware, spúšťať skripty cez email a webové stránky. Takýto hacker môže mať k dispozícii aj botnet, pomocou ktorého využije veľké množstvo napadnutých počítačov na posielanie spamu prípadne aj na iné útoky. Prenajatie jedného takéhoto počítača na jeden mesiac stojí približne jeden dolár. [15]

2.3.3 Organizovaný zločin

Organizované kriminálne skupiny sú zodpovedné za tie najviac dôkladné a do detailov prepracované útoky. Na technickú činnosť si najímajú hackerov a zakladajú webové stránky, ktoré im slúžia na najímanie ľudí, ktorých následne zneužívajú na pranie peňazí. Pomocou získaných informácií vo veľkom falšujú kreditné karty. [15]

Toto je asi tá najhoršia možná varianta kde môžu skončiť naše osobné informácie. Tieto organizované skupiny majú rozsiahle skúsenosti a rôzne nástroje na to, ako maximálne zneužiť našu identitu. Vyprázdnia nám bankový účet, založia nové kreditné karty, vyrobia falošné vodičské preukazy a pasy s našimi údajmi a pod. [15]

2.3.4 Teroristické organizácie

Teroristické siete vo väčšine prípadoch nevyužívajú phishing na kradnutie peňazí, ale profitujú predovšetkým z ukradnutia identity. Napríklad španielska bunka teroristickej organizácie Al-Káida využívala ukradnuté kreditné karty v podvodných obchodoch a pre veľké množstvo rôznych nákladov. [15]

3 História phishingu

3.1 America Online

Už v roku 1987 bola podrobne popísaná technika útoku neskôr známa práve ako phishing, no tento pojem bol po prvýkrát spomenutý až v roku 1996. Avšak k vôbec prvým zaznamenaným phishingovým útokom došlo v roku 1995 na službu AOL (America Online).[7]

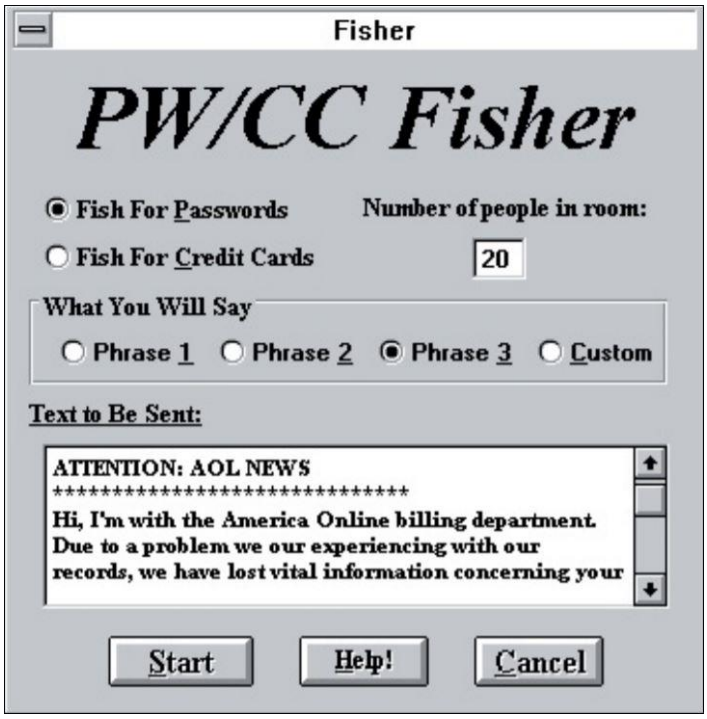
Práve táto služba bola v 90. rokoch minulého storočia pre obyvateľov v USA prvou dostupnou možnosťou ako nahliadnuť do sveta počítačových sietí a neskôr aj internetu. Všetko čo k tomu potrebovali bola iba kreditná karta, resp. len jej číslo. Veľmi vynaliezaví užívatelia však časom zistili, že k prístupu im stačí falošné číslo kreditnej karty, ktoré vyzerá aspoň trochu hodnoverne. Dokonca vyvinuli rôzne generátory, ktoré boli schopné vypočítať dôveryhodne vyzerajúce platobné údaje. Tieto vymyslené údaje síce nefungovali večne, ale aspoň po určitú dobu im to umožnilo prístup k daným službám. Avšak keď v AOL prišli na túto chybu v systémoch, tak netrvalo dlho a oprava bola na svete. Tým pádom si už podvodníci nevystačili s falošnými údajmi, ale potrebovali pravé čísla kreditných kariet, ktoré sa snažili získať práve prostredníctvom phishingu. [3] [6] [7] [8] [9]

Útočníci využívali prevažne chat AOL IM (America Online Instant Messenger) kde sa vydávali za administrátorov a oznamovali užívateľom, že sa vyskytol určitý problém napr. s vyúčtovaním alebo platbou a žiadali od nich obnovenie prihlasovacích údajov a údajov o kreditnej karte. Takýmto spôsobom sa postupne vyvinuli tradičné phishingové frázy, ktoré sa často používajú ešte aj dnes ako napríklad:

- overte svoj účet,
- potvrďte svoje platobné údaje,
- vaše heslo môže byť prezradené, zmeňte si ho.

Hacker známy ako „Da Chronic“ naprogramoval jednoduchý program s názvom AOHell. Tento program obsahoval viacero funkcií ako napríklad emailové bomby, jednoduché a rýchle založenie falošného AOL účtu a samozrejme slúžil aj na získavanie hesiel a čísiel kreditných kariet ostatných užívateľov služieb AOL. Nástroj s názvom „Fisher“ umožňoval

užívateľovi založiť chatovaciu miestnosť kde sa vydával za administrátora a následne automaticky zisťoval údaje od užívateľov v danej miestnosti podľa nastavení útočníka. [12]



Obrázok 2 Fisher
Zdroj: [12]

Problémom bolo aj to, že prístup k danému chatu nemali len užívatelia AOL, ktorí by sa následne dali dohľadať, ale aj užívatelia iných poskytovateľov a to útočníkom poskytovalo anonymitu. Nakoniec to dospelo až do takého štádia, že pri každom prihlásení do AOL IM sa zobrazilo upozornenie s textom, že žiaden zamestnanec AOL sa nikdy nebude pýtať užívateľov na heslo alebo akékoľvek osobné údaje. [6]

3.2 E-Gold

Ako sa postupne vyvíjal svet internetu, tak bolo čoraz jednoduchšie a aj cenovo lacnejšie sa pripojiť k internetu a práve preto sa ciele hackerov taktiež v istom zmysle zmenili. Svojimi útokmi sa síce stále snažili získať údaje od kreditných kariet, no už sa nezameriavali na služby poskytujúce internetové pripojenie, ale svoju pozornosť upriamili na služby umožňujúce online platby. [6] [8]

Prvou takouto obeťou sa stal v roku 2001 systém známy pod názvom E-Gold, ktorý svojim užívateľom umožňoval vykonávať online platby. Tieto online prevody boli denominované v gramoch zlata alebo prípadne aj v iných cenných kovoch. Práve to zlákalo hackerov pochádzajúcich prevažne z Ruska a Ukrajiny, ktorí k oklamaniu užívateľov používali nie len

klasické emailové správy, ale aj bezpečnostné slabiny vo Windowse a Internete Explorer. K tomu všetkému ešte prispieval aj fakt, že tak ako všetci používatelia daného systému boli voči sebe anonymní, tak aj samotné platby prebiehali v úplnej anonymite. A aj napriek tomu, že vôbec prvý takýto útok, ktorý sa odohral v Júni 2001 bol vyhodnotený ako neúspešný, tak spustil lavínu podobných útokov aj na iné online služby ako napríklad PayPal alebo eBay. [6] [8]

Dôležitý zlom nastal až po útokoch 11. septembra, kedy v USA došlo k zmene legislatívy a ministerstvo financií určilo celkom nové pravidlá pre prevod peňazí. Tieto rapídne zmeny spôsobili mimo iné aj to, že v decembri 2011 služba E-Gold definitívne ukončila svoju činnosť. No na druhej strane to taktiež otvorilo dvere podvodníkom, ktorí začali rozosielať hromadné emaily kvôli kontrole dokladov po 11. septembri. [6]

Keď bolo v USA internetové bankovníctvo ešte len vo svojich začiatkoch, tak jeho zabezpečenie bolo na veľmi mizernej úrovni čo hralo do karát útočníkom. V tých časoch boli takéto služby v Európe ďaleko lepšie zabezpečené voči rôznym typom napadnutia. Postupne sa ale zabezpečenie takýchto služieb na celom svete výrazne zvýšilo, ale ani to stále nezabránilo hackerom k úspešným útokom. [6]

3.3 Sociálne siete

Postupne ako začali vznikať rôzne sociálne siete, ktoré boli stále viac a viac populárnejšie, tak sa útočníci zamerali aj na túto oblasť internetu. Zo sociálnych sietí sa snažia získať predovšetkým mená, adresy, dátumy narodenia, telefónne čísla, ale aj ďalšie osobné informácie. Takto získané údaje sa často objavujú aj na odvrátenej strane internetu Darknete, kde sú buď voľne dostupné alebo za určitú finančnú sumu. Prvý takýto masívny útok sa odohral v roku 2006, ktorý bol zameraný na sociálnu sieť MySpace. [6]

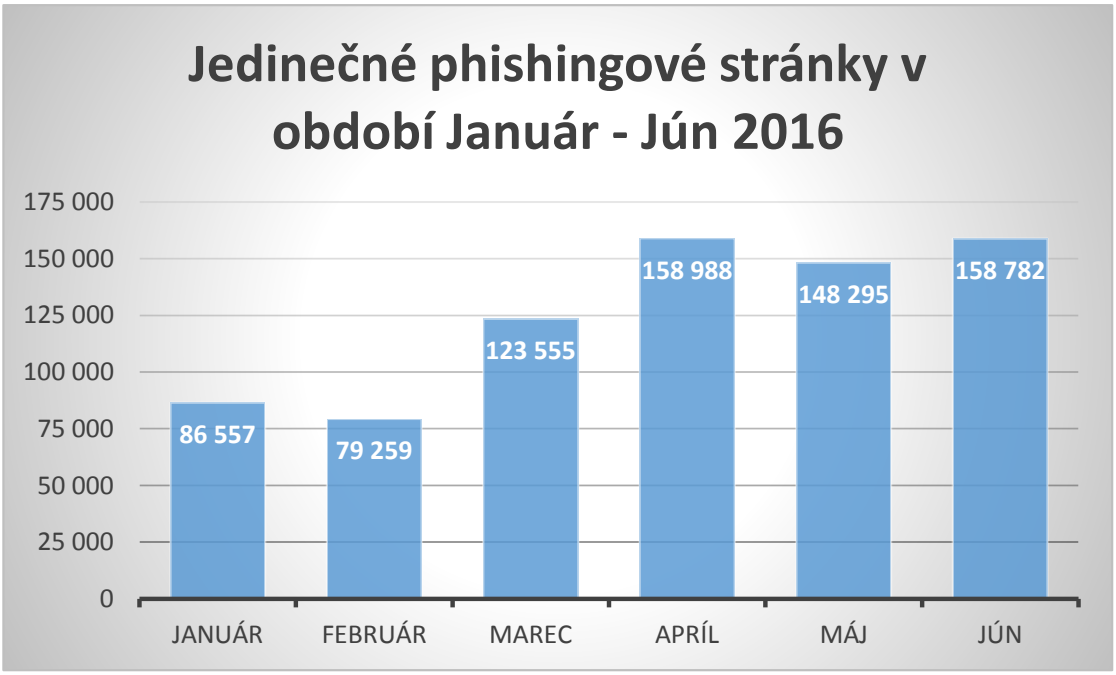
3.4 Súčasnosť

3.4.1 2016

V prvej polovici roku 2016 sa počet phishingových stránok odhalených asociáciou Anti-Phishing Working Group (APWG) zvýšil o 250% oproti poslednému štvrťroku 2015. V tomto období boli najviac napádaní poskytovatelia služieb, ktoré tvorili takmer polovicu všetkých

útokov. Za nimi nasledovali finančné organizácie a platobné služby. Vyše 75% týchto stránok malo webhosting práve v Spojených štátoch amerických. [23] [24]

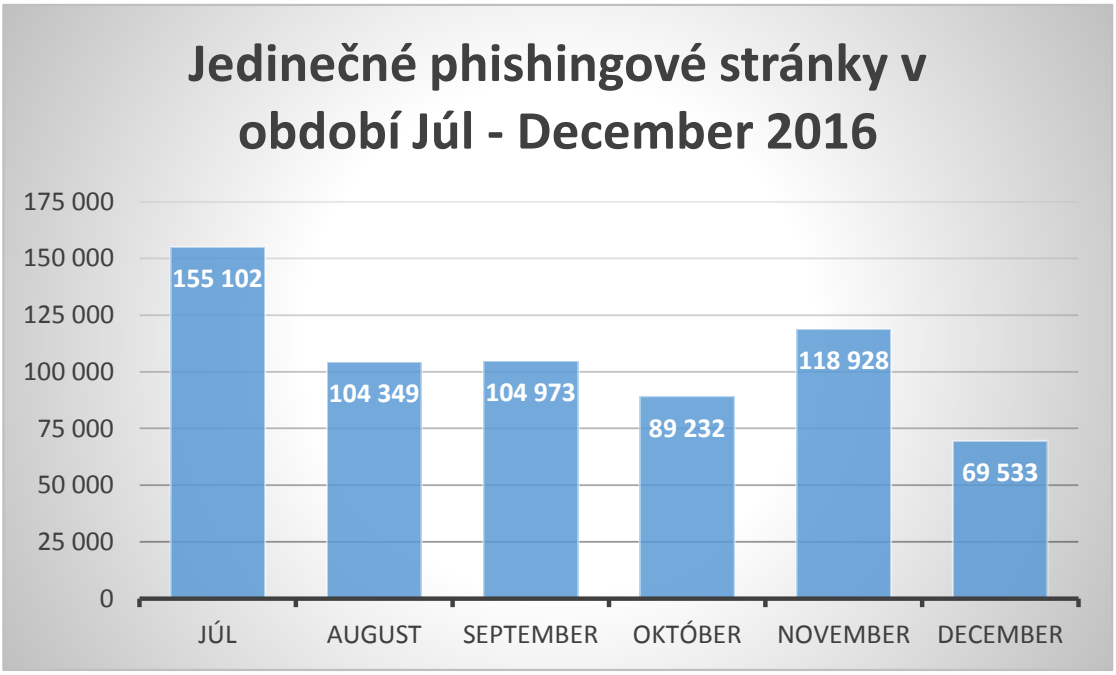
Na nasledujúcom grafe je viditeľné, že začiatok roka sa niesol ešte v relatívne pokojnom tempe kde počet phishingových stránok nedosiahol hranicu ani 90 000. Zlom nastal v mesiaci marec kedy tento počet presiahol hranicu 100 000 a v období od apríla do júna siahal na hranicu 160 000 jedinečných phishingových stránok.



Graf 1 Jedinečné phishingové stránky v období Január - Jún 2016
Zdroj: [23] [24] (spracovanie autora)

V druhej polovici roku 2016 bol stále najviac napádaný sektor poskytovateľov služieb s vyše 40%, nasledovaný na druhom mieste finančnými organizáciami. Zmena nastala akurát na mieste treťom kde platobné služby predbehol Internet Service Provider. [25] [26]

Na druhom grafe je možné vidieť, že ešte v júli sa držal počet podvodných stránok pri hranici 160 000. No v nasledujúcich mesiacoch tento počet klesol na rozmedzie približne 90 000 – 120 000 stránok. Najväčší prepad v roku 2016 nastal práve v úplne poslednom mesiaci kedy počet jedinečných phishingových stránok klesol na najnižšiu hranicu za celý rok a to len niečo vyše 69 000 stránok.



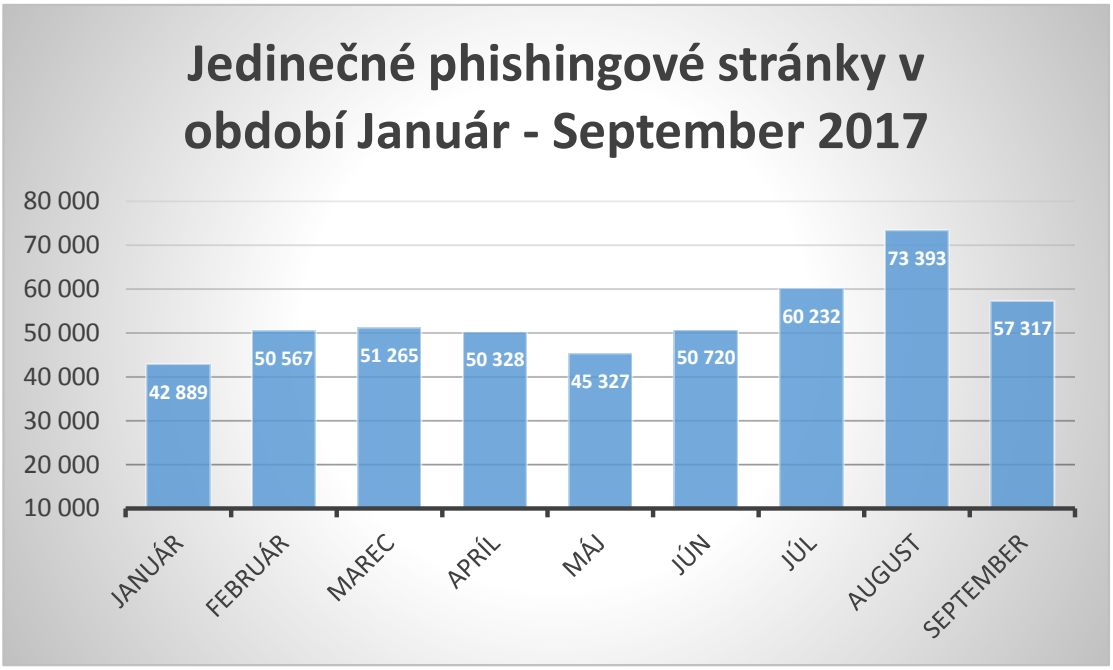
Graf 2 Jedinečné phishingové stránky v období Júl - December 2016
Zdroj: [25] [26] (spracovanie autora)

Za celý rok 2016 APWG odhalila 1 220 523 phishingových útokov čo znamená 65% nárast oproti roku 2015. Priemerný počet útokov za posledný štvrťrok 2016 činil 92 564 zatiaľ čo napríklad v poslednom štvrťroku 2004 bol takýto mesačný priemer iba 1 609 útokov. [26]

3.4.2 2017

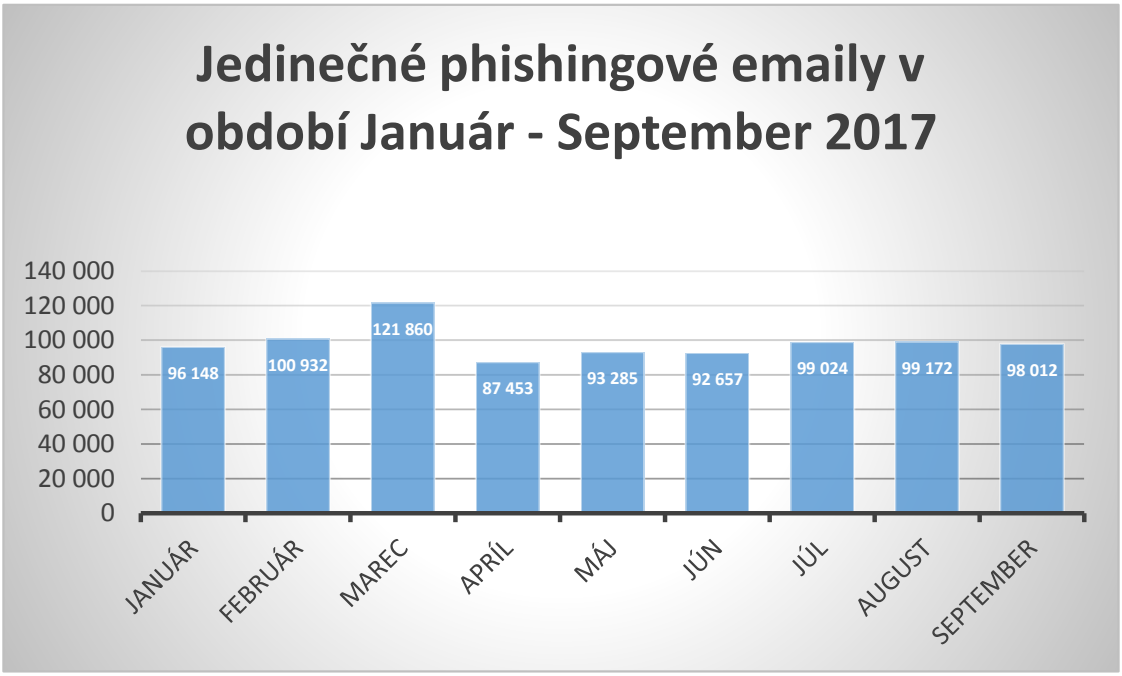
V roku 2017 sa útoky zamerali prevažne na platobné služby, finančné organizácie a Webmail. Bol zaznamenaný nárast počtu phishingových útokov, ktoré využívajú bezplatný webhosting. Taktiež útočníci začali vo väčšom množstve využívať HTTPS protokol, aby zvýšili šance na oklamanie užívateľov a navštívené stránky vyzerali ako bezpečné. V južnej Amerike sa v tomto období phishingové kampane zamerali prevažne na kryptomeny. [27] [28]

Na nasledujúcom grafe je možné vidieť, že počet phishingových stránok zaznamenaných spoločnosťou APWG za obdobie január až september 2017 klesol oproti roku 2016. Držia sa približne pri hranici 50 000 s výnimkou letných mesiacov júl a august kedy tento počet stúpol až takmer na 75 000.

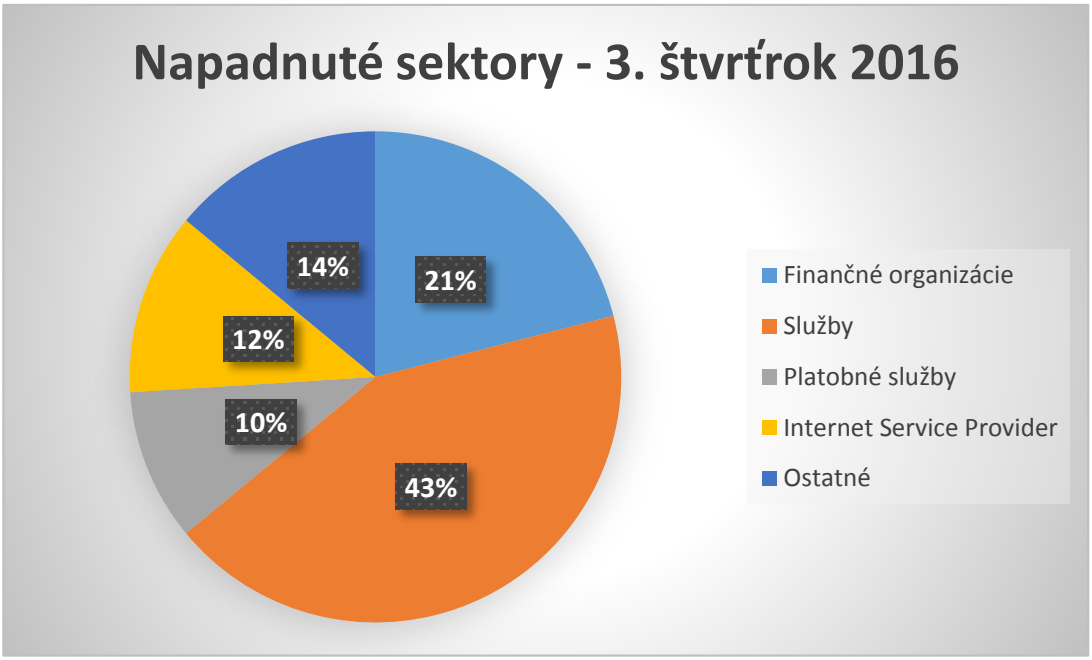


Graf 3 Jedinečné phishingové stránky v období Január - September 2017
Zdroj: [27] [28] (spracovanie autora)

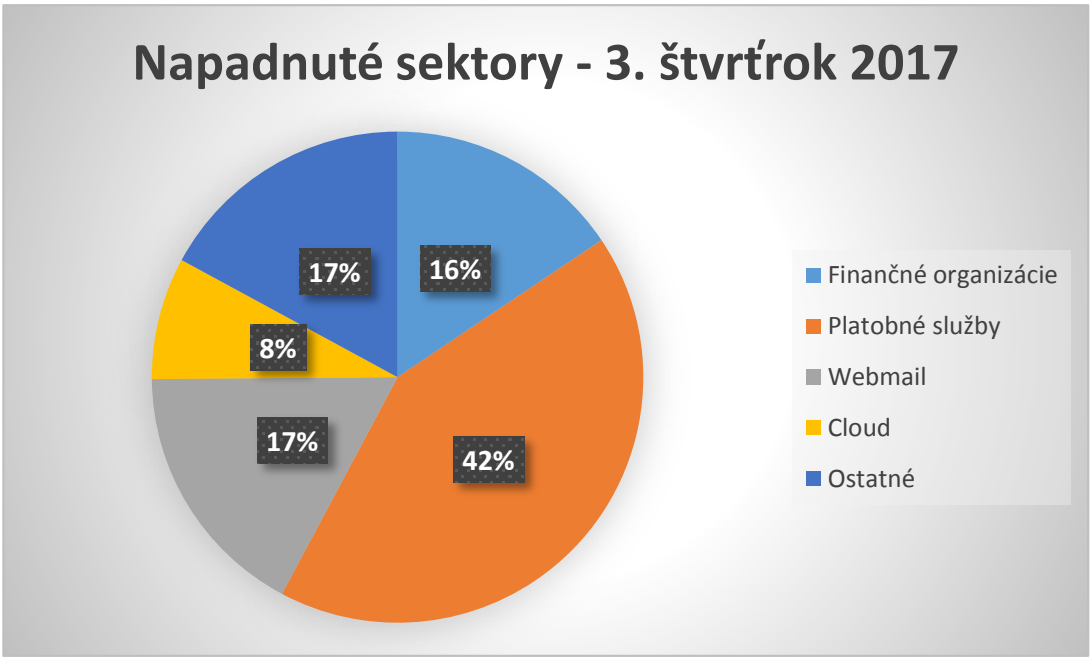
Graf 4 znázorňuje počet jedinečných phishingových emailov za rovnaké obdobie roku 2017. Počet podvodných emailov odhalených asociáciou APWG sa pohybuje väčšinou pri hranici 100 000. Výnimku tvorí marec kedy tento počet stúpol mierne nad 121 000 a taktiež apríl kedy zase počet odhalených phishingových emailov klesol pod hranicu 88 000.



Graf 4 Jedinečné phishingové emaily v období Január - September 2017
Zdroj: [27] [28] (spracovanie autora)



Graf 5 Napadnuté sektory - 3. štvrťrok 2016
Zdroj: [25] (spracovanie autora)



Graf 6 Napadnuté sektory - 3. štvrťrok 2017
Zdroj: [28] (spracovanie autora)

Na posledných dvoch grafoch sú pre porovnanie zobrazené najviac napádané sektory za 3. štvrťrok roku 2016 a 2017. Zatiaľ čo platobné služby v roku 2016 tvorili len 10%, tak v roku 2017 zaznamenali značný nárast a to až na 42%. Finančné organizácie zaznamenali mierny pokles o 5%. Do kategórie „ostatné“ patria napríklad sociálne média, telekomunikácie, online zoznamky, náučné stránky, cestovateľské stránky a pod.

4 Priebeh phishingového útoku

V tejto kapitole je bližšie popísaná príprava a aj samotný priebeh klasického phishingového útoku a taktiež je pomocou jednoduchej schémy zobrazený priebeh phishingového útoku, pri ktorom sa využíva aj malware.

4.1 Phishingové emaily

Vôbec najbežnejšia forma phishingu je založená práve na posielaní tzv. phishingových emailov, ktoré na prvý pohľad nepôsobia nijak podozrivo a ich súčasťou je aj odkaz, na ktorý má užívateľ kliknúť. Po otvorení daného odkazu sa užívateľovi zobrazí kópia určitej webovej stránky, ktorá je takmer na nerozpoznanie od tej pôvodnej. Z takto upravenej stránky sa však všetky vyplnené dáta automatický odosielajú útočníkovi bez toho, aby bežný užívateľ čokoľvek spozoroval. Takýto útok, ale aj všetky ostatné si musí útočník dopredu presne naplánovať a pripraviť sa naň čo najlepšie, ak chce dosiahnuť požadované výsledky, teda ukradnúť užívateľské mená, heslá, údaje o kreditných kartách a pod. V tejto kapitole si trochu priblížime v akých približných krokoch takýto útok prebieha a čo k nemu útočník všetko potrebuje. [1]

4.1.1 Plánovanie phishingového útoku

V tejto úplne prvej fáze prípravy na útok je potrebné dôkladne vybrať cieľ. Môže sa jednať o jednotlivcov, veľké skupiny užívateľov alebo rôzne národné, ale aj medzinárodné organizácie. Taktiež je nutné zvoliť správnu metódu, ktorá bude použitá na útok, či už pôjde o klasické phishingové emaily, vishing, spear phishing alebo iné spôsoby. Veľmi dôležité je aj vyhodnotiť všetky možné riziká ako napríklad stupeň technického zabezpečenia cieľu a v prípade zlyhania, tak pravdepodobnosť odhalenia identity útočníka. [1]

4.1.2 Vytváranie podmienok pre phishingový útok

Druhý krok pozostáva z technického riešenia phishingového útoku. V prípade, že si útočník zvolí ako najlepšiu metódu phishingové emaily, tak si musí zaobstarať čo najväčší počet emailových adries, vytvoriť falošnú emailovú adresu, z ktorej bude dané správy odosielať a samozrejme aj pripraviť dátovú schránku kam mu budú prichádzať získané údaje. Taktiež si pripraví text danej správy, ktorý musí znieť dôveryhodne a nevzbudiť žiadne pochybnosti,

že by sa mohlo jednať o podvod. No a samozrejme vytvorí aj čo najpresnejšiu kópiu stránky, z ktorej chce získať údaje užívateľov. [1]

4.1.2.1 Vytvorenie phishingovej stránky pre Facebook

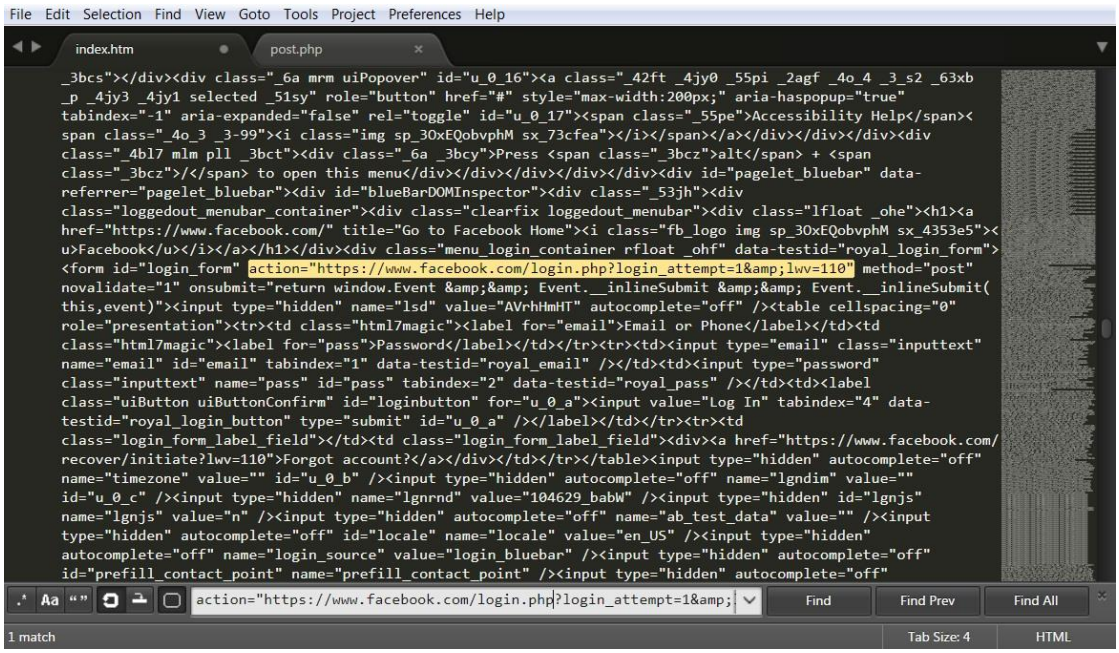
Nezainteresovaným sa často môže zdať, že phishing sa ich netýka, pretože si myslia, že príprava takejto stránky je určite veľmi zložitý proces, ktorý zvládnu len skutoční hackeri. Avšak práve opak je pravdou. V dnešnej dobe každú minútu pribudne na internete obrovské množstvo rôznych dát. Práve z toho dôvodu je snáď nemožné, aby tam niečo nešlo dohľadať. Či už ide o najnovšie filmy a seriály, hry, elektronické knihy, aktuálne správy zo sveta, rôzne články, programy alebo čokoľvek iné. A práve to nahráva hackerom alebo aj znudenému študentovi, ktorý chce zažiť pocit aké to je byť hackerom alebo sa len pobaviť na účet niekoho iného.

Nie je potrebné ani príliš dlho hľadať a hneď je možné naraziť na rôzne diskusné fóra a články o rôznych druhoch hackovania, mimo iné aj o phishingu. Je možné nájsť priamo návod, ktorý popisuje krok po kroku ako si vytvoriť vlastnú phishingovú stránku. V nasledujúcich jednoduchých krokoch je popísané ako je možné vytvoriť takú stránku na odchytávanie prihlasovacích údajov na Facebook. Cieľom samozrejme nie je, aby to slúžilo ako návod a následne vykonávanie akejkoľvek nelegálnej činnosti, ale aby aj menej zainteresovaní videli aké to je jednoduché, a že je skutočne dôležité byť ostražitý pri zadávaní akýchkoľvek osobných údajov na webe.

Po zadaní hľadaného výrazu do Googlu sa zobrazí hneď niekoľko rôznych výsledkov ako vytvoriť facebookovú phishingovú stránku. Medzi výsledkami boli zložitejšie aj menej zložité návody alebo prípadne aj celkom hotové zdrojové kódy pripravené na stiahnutie a okamžité použitie bez akýchkoľvek úprav.

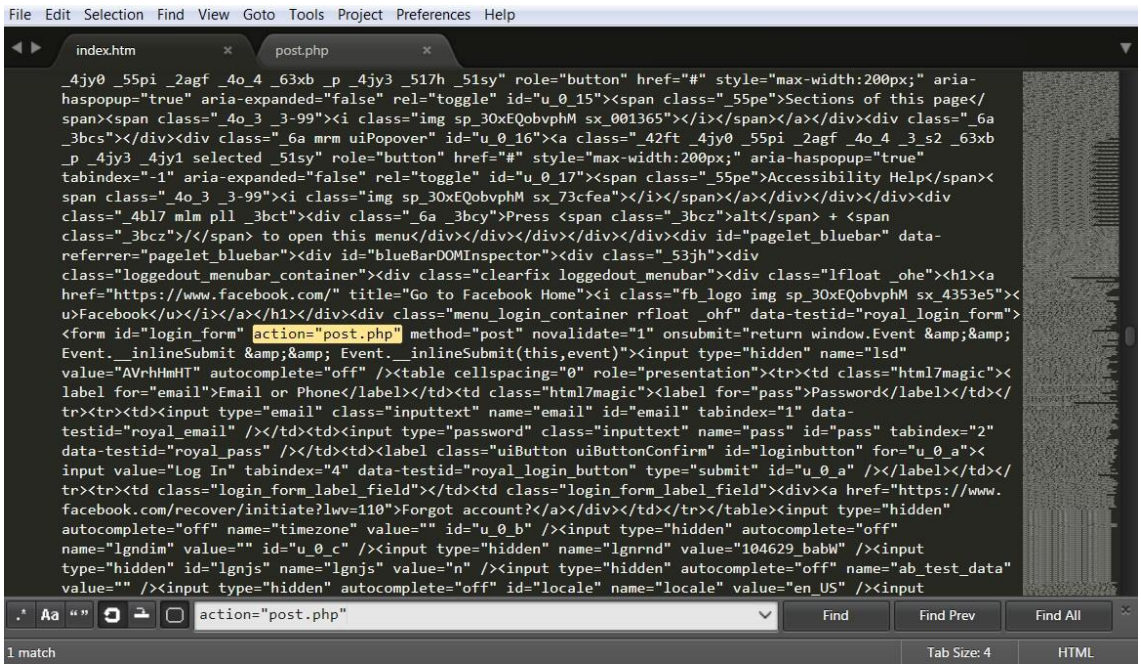
Ako prvé je potrebné v prehliadači otvoriť oficiálnu stránku facebook.com. Následne kliknutím pravého tlačidla myši na stránke je nutné zobraziť zdrojový kód stránky. Potom celý tento kód stačí označiť a nakopírovať do textového editora v počítači. [10]

Použitím skratky CTRL+F sa zobrazí okno pre vyhľadávanie kde treba zadať hľadaný reťazec v tvare *„action="https://www.facebook.com/login.php?login_attempt=1&lwv=110"“*. Je to zvýraznená časť textu na Obrázku 3 nižšie. [10]



Obrázok 3 Vyhľadanie potrebného reťazca v index.htm
Zdroj: Autor

Daný výraz je nutné zmazať a nahradiť ho napríklad *„"post.php"“*, ale názov reťazca môže byť ľubovoľný. Dôležité je, aby to bolo s koncovkou *„*.php“*. Takže teraz tam je *„action="post.php"“*, ako na Obrázku 4. Tento súbor, ktorý bude slúžiť ako hlavná phishingová stránka je potrebné uložiť ako *„index.htm“*. [10]

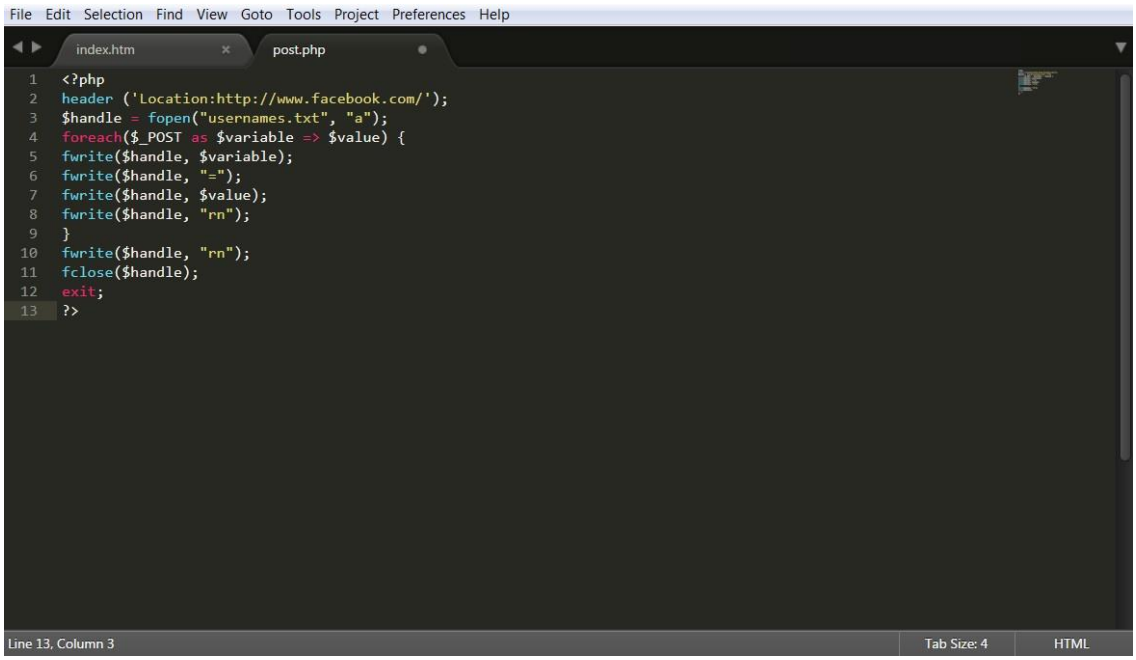


Obrázok 4 Zmena daného výrazu v index.htm
Zdroj: Autor

V ďalšom kroku je nutné vložiť php kód do úplne nového textového dokumentu, ktorý má zhodný názov *„post.php“* ako prepísaný reťazec v zdrojovom kóde:

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

Takže obsah daného súboru následne vyzerá ako na Obrázku 5. [10]

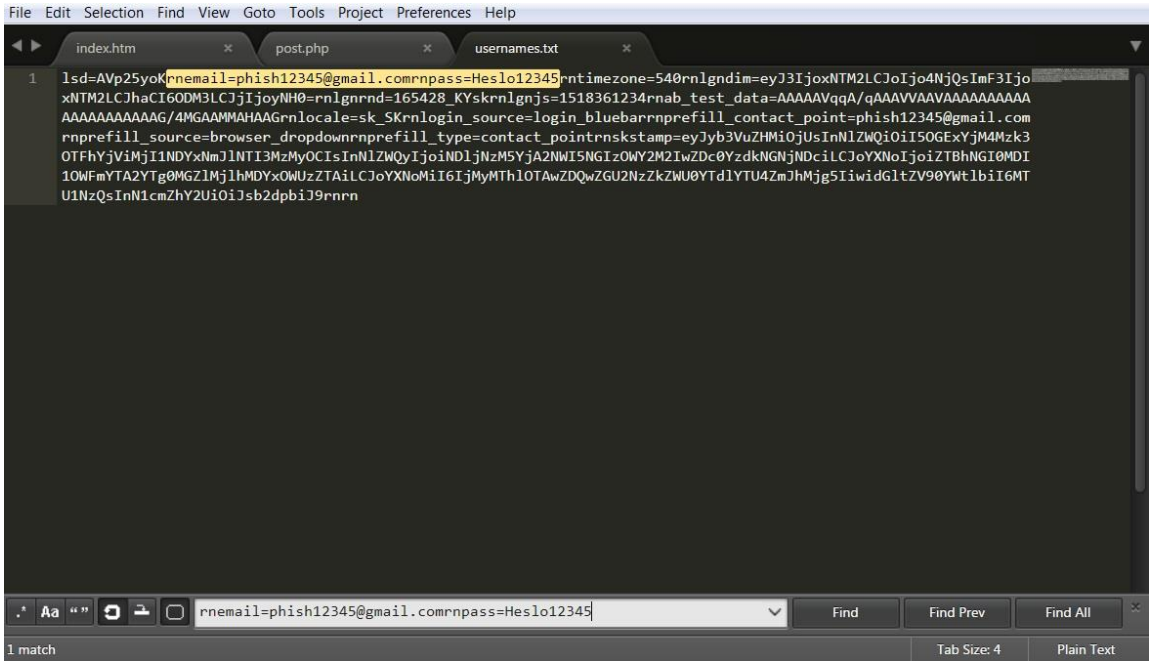


Obrázok 5 Post.php
Zdroj: Autor

Nachádza sa tam napríklad *„usernames.txt“* čo označuje názov súboru kde sa budú získané údaje ukladať. V tomto kroku je ešte nutné deaktivovať akúkoľvek antivírovú ochranu počítača, pretože inak daný php súbor vyhodnotí ako hrozbu, viď. Obrázok 6.

Obrázok 6 Eset smart security 8
Zdroj: Autor

Úplne posledným krokom je nahrať dané súbory na nejaký web hosting a tým vlastne vypustiť stránku do sveta. Ale vzhľadom na nelegálnosť tohto kroku je možné funkčnosť daného postupu overiť za pomoci vlastného lokálneho Apache servera. Po otvorení *„index.htm“* a následnom zadaní prihlasovacích údajov sa presne tieto údaje objavili v súbore *„usernames.txt“*, viď. Obrázok 7.



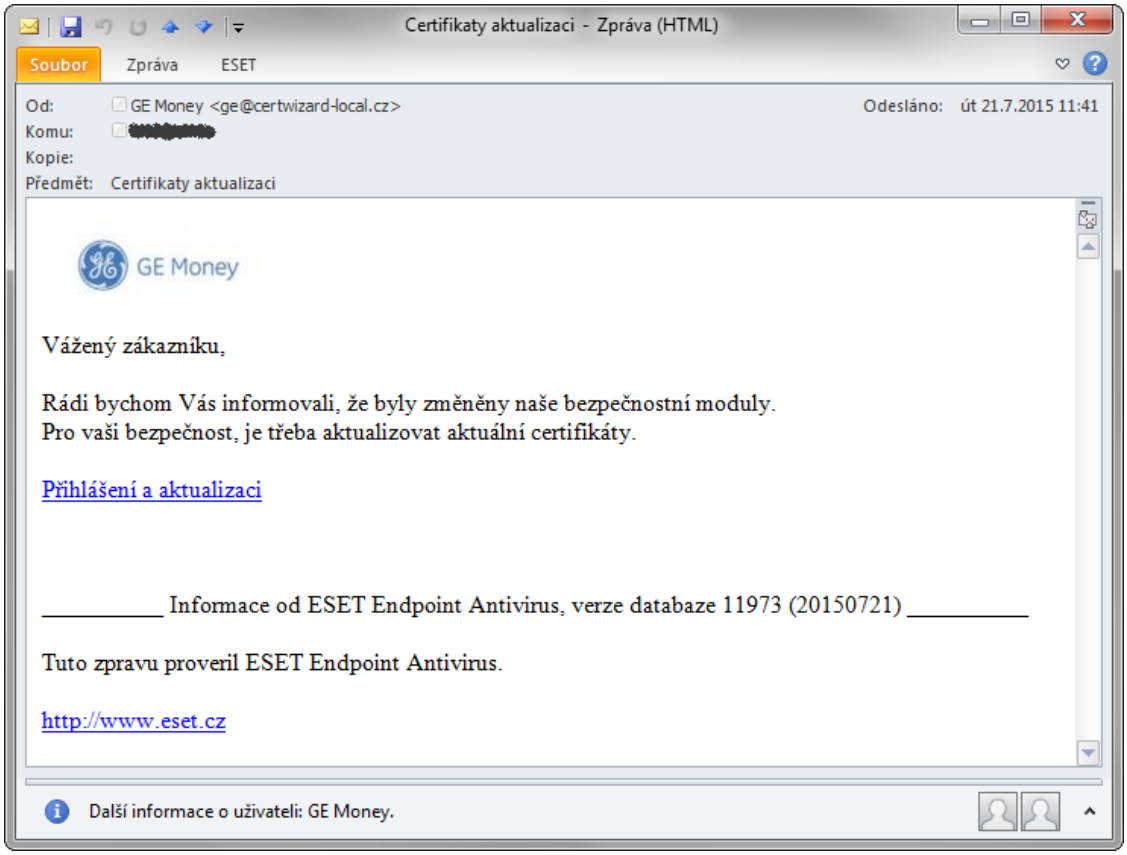
Obrázok 7 Usernames.txt
Zdroj: Autor

Ako je možné vidieť v týchto jednoduchých krokoch, tak nájsť potrebné informácie a následne vytvoriť všetko potrebné pre phishingovú stránku nie je vôbec zložité a ani časovo náročné. Voľne na internete je dostupné ohromné množstvo rôznych návodov zameraných nie len na Facebook, ale aj na rôzne iné stránky. Avšak pri takomto pátraní netreba strácať ostražitosť, aby sa hľadajúci nestal sám obeťou, pretože taktiež veľa takýchto stránok v mnohých prípadoch môže obsahovať rôzne druhy vírusov, ktoré by

mohli narobiť škody v počítači. A samozrejme netreba zabúdať aj na fakt, že zneužívanie takýchto návodov a následne aj samotných stránok nie je v súlade s platným zákonom.

4.1.3 Vlastný phishingový útok

V tejto fáze útočník začne rozosielať predom pripravené emailové správy s potrebnou textáciou a odkazom na phishingovú stránku. Dáta sú mu následne odosielané do jeho dátovej schránky. Avšak túto časť už útočník nemôže ovplyvniť a závisí to už len od kvality spracovania daného emailu, stránky a v neposlednom rade od faktorov ako znalosti užívateľa, jeho skúsenosti s phishingom, antiphishingové programy a pod. V tomto kroku celého útoku sa užívateľ po prvýkrát stretáva s phishingovým emailom. [1]



Obrázok 8 Phishingový email GE Money
Zdroj: [13]

4.1.4 Zber dát

Tento predposledný krok je asi najjednoduchší zo všetkých. Pozostáva len z prostého získavania dát, ktoré jednotliví užívatelia zadali na podvodnej webovej stránke.

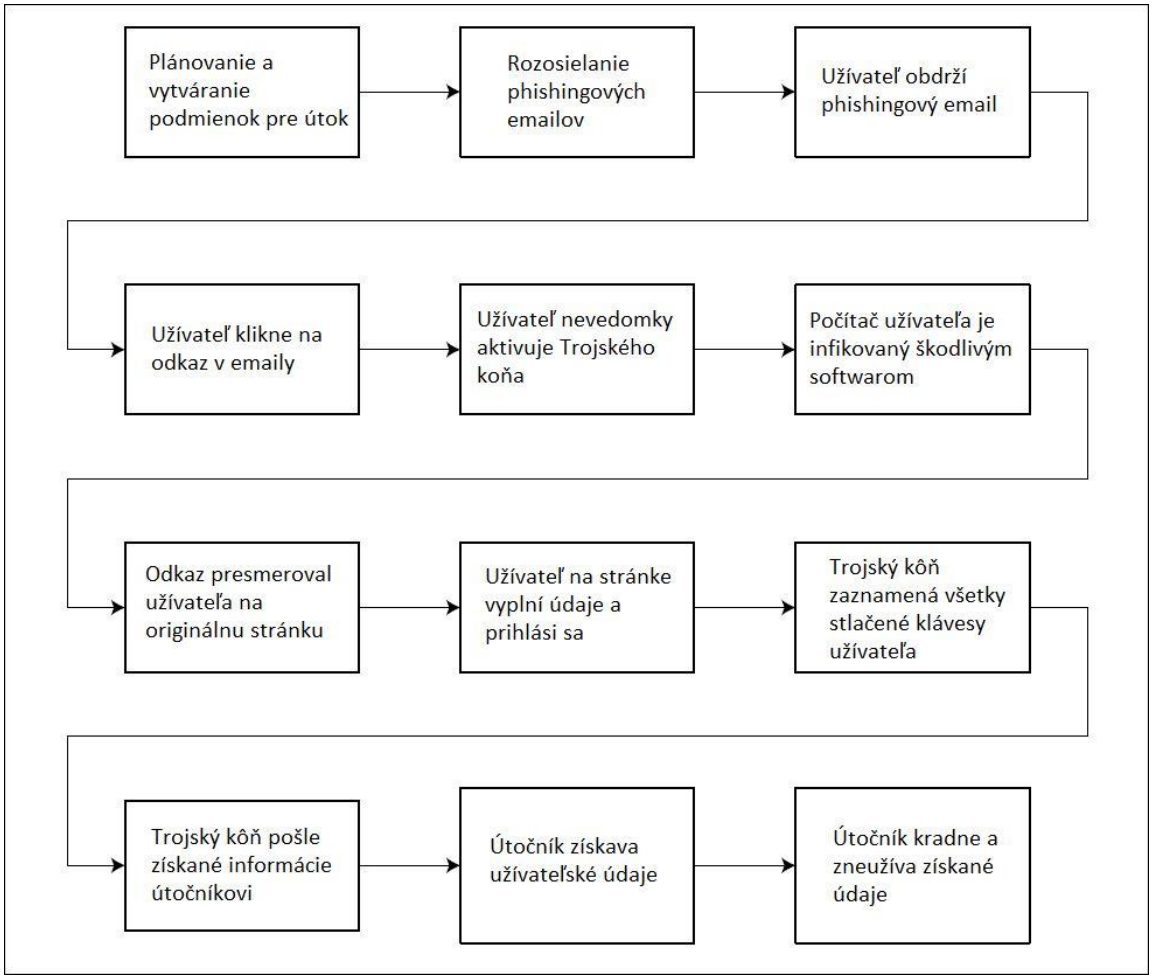
4.1.5 Profit z phishingového útoku

Úplne poslednou fázou celého procesu phishingového útoku je profit pre útočníka. Vo väčšine prípadoch ide o získanie peňažných prostriedkov z odcudzených kreditných kariet. Peniaze z účtov sú následne prevedené na rôzne zahraničné bankové účty, a preto je ich dohľadanie veľmi náročné a v niektorých prípadoch úplne nemožné. Finančnú odmenu môže útočník získať aj za predaj osobných informácii, ktoré sú žiadané predovšetkým na Darknete. Tieto údaje následne kupujúci ďalej zneužíva vo svoj prospech. Vzhľadom na to, že všetky transakcie prebiehajú výhradne vo virtuálnych kryptomenách, tak aj v tomto prípade je pravdepodobnosť odhalenia identity dotyčných osôb takmer nulová. [1]

4.2 Phishing a malware

O niečo pokročilejší útočníci k svojim phishingovým útokom často využívajú aj malware. Pojem malware vznikol z anglického výrazu *„malicious software“*, ktorý popisuje určitý škodlivý software, pomocou ktorého útočník získa prístup k počítaču užívateľa. Existujú rôzne typy malwaru ako napríklad spyware, adware, trojské kone, rootkity, ransomware a pod. Tento škodlivý software sa najčastejšie šíri cez internet a emailové správy a do počítača sa dostane najčastejšie pri zanedbaní antivírovej ochrany. [14]

Priebeh takého útoku je stručne vyobrazený na nasledujúcom Obrázku 9.



Obrázok 9 Phishing a malware
Zdroj: [15] (spracovanie autora)

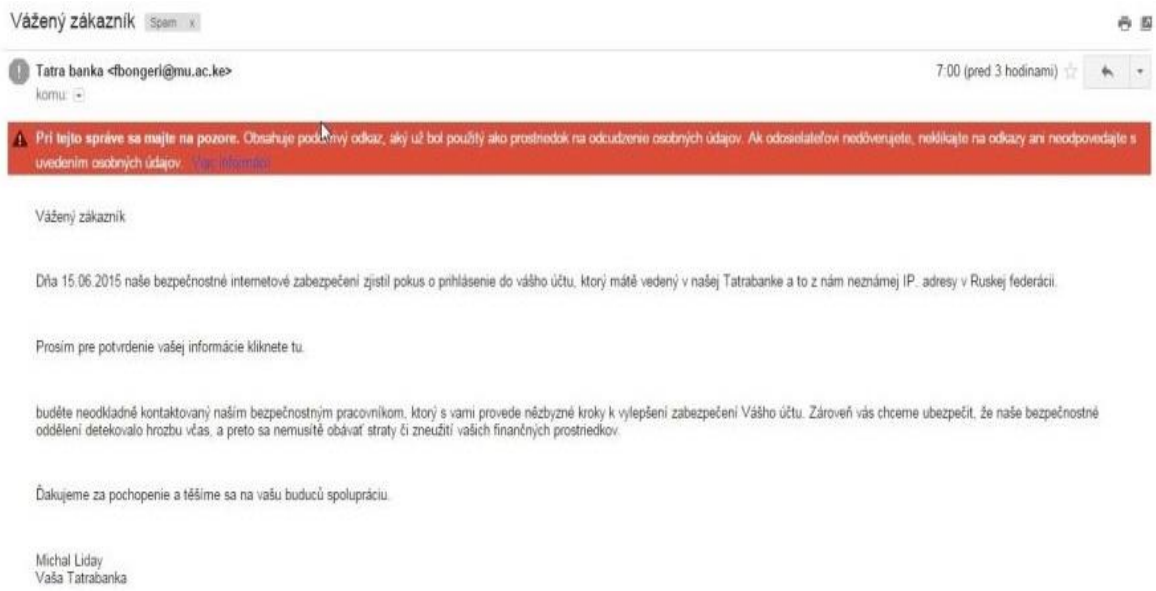
5 Reálne hrozby phishingu

V tejto kapitole je popísaných niekoľko reálnych phishingových útokov, ktoré sa odohrali v posledných rokoch na území Slovenska, ale aj inde vo svete. Posledný príklad so stránkou od Apple nebol zneužitý v praxi.

5.1 Finančné inštitúcie

Internetové bankovníctvo stále patrí medzi jeden z najčastejších cieľov phishingových útokov. V roku 2015 došlo k viacerým takýmto útokom hneď na niekoľko slovenských bánk ako napríklad Slovenská sporiteľňa, UniCredit Bank a Tatra banka. [16]

V tomto prípade išlo o podvodné emaily, ktoré boli rozosielané zákazníkom danej banky. Keďže banku klient vníma ako určitú autoritu, ktorá sa stará o jeho peniaze, tak sa logicky zľakne, že niečo nie je v poriadku a takto môže ľahko naletieť podvodníkom. Na obrázku nižšie je konkrétny príklad emailu, ktorý posielali klientom Tatrabanky. [16]


Vážený zákazník Spam x

Tatra banka <fbongeri@mu.ac.ke> 7:00 (pred 3 hodinami)

komu:

Pri tejto správe sa majte na pozore. Obsahuje podozrivý odkaz, ktorý už bol použitý ako prostriedok na odcudzenie osobných údajov. Ak odosielateľovi nedôverujete, neklikajte na odkazy ani neodpovedajte s uvedením osobných údajov. Viac informácií

Vážený zákazník

Dňa 15.06.2015 naše bezpečnostné internetové zabezpečení zjistil pokus o prihlásenie do vášho účtu, ktorý máte vedený v našej Tatrabanke a to z nám neznámej IP. adresy v Ruskej federácii.

Prosím pre potvrdenie vašej informácie kliknete tu.

buděte neodkladně kontaktovaný naším bezpečnostným pracovníkom, ktorý s vami provede nězbyzné kroky k vylepšení zabezpečení Vášho účtu. Zároveň vás chceme ubezpečit, že naše bezpečnostné oddělení detekovalo hrozbu včas, a preto sa nemusíte obávať straty či zneužití vašich finančných prostriedkov.

Ďakujeme za pochopenie a těšíme sa na vašu buducú spolupráciu.

Michal Liday
Vaša Tatrabanka

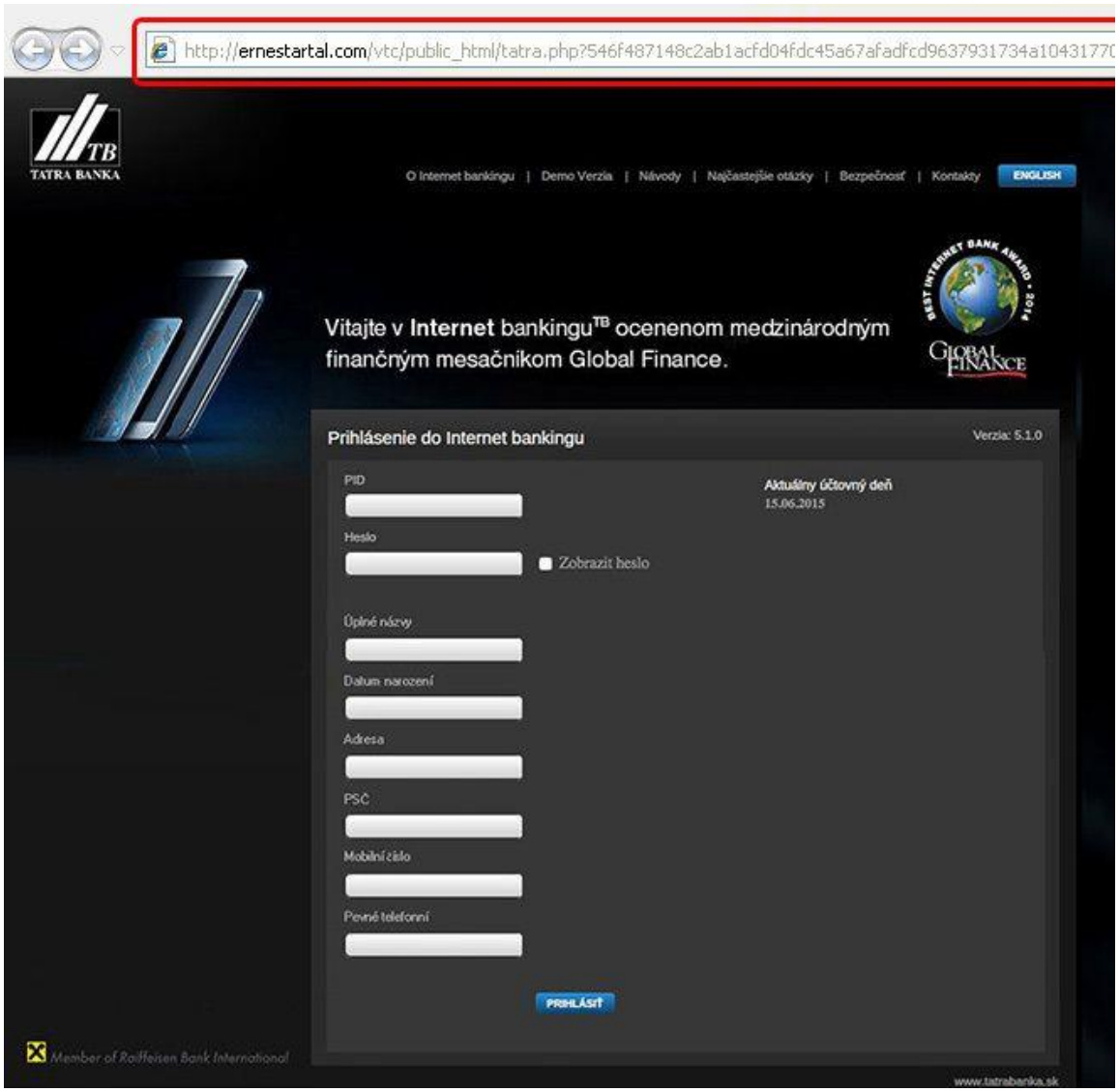
Obrázok 10 Plné znenie phishingového emailu zameraného na klientov Tatrabanky
Zdroj: [16]

Na tomto emaile je možné si všimnúť hneď niekoľko vecí. Ako prvé čo by malo vyvolať pochybnosti o pravosti emailu je to, že už samotný Gmail hlási, že táto správa obsahuje podozrivý odkaz, ktorý už bol použitý na odcudzenie osobných údajov.

Ďalšou nedokonalosťou tohto emailu, ktorá by mala udrieť užívateľovi do očí je páve text správy. V tomto prípade sa jedná o akúsi zvláštnu kombináciu češtiny a slovenčiny.

No a posledným zreteľným znakom, že sa jedná o falošný email je odosielateľ správy. Síce meno je nastavené ako *„Tatrabanka“,* ale emailová adresa *„fbongeri@mu.ac.ke“* určite nepatrí žiadnemu zamestnancovi Tatrabanky.

Po kliknutí na odkaz v danom emaily boli užívatelia presmerovaní na podvodnú stránku, viď. Obrázok 11.



Obrázok 11 Phishingová stránka zameraná na klientov Tatrabanky
Zdroj: [16]

Ak užívateľ v tomto prípade klikol na odkaz, ktorý sa nachádzal v správe, tak bol presmerovaný na presnú kópiu stránky pre prihlásenie do internet bankingu Tatrabanky.

Už na prvý pohľad je zrejmé, že celá webová adresa s istotou nepatrí Tatrabanke. Taktiež je viditeľná absencia overených bezpečnostných certifikátov danej banky.

V prípade, že klienti narazia na emaily, o ktorých pravosti majú značné pochybnosti, tak by to mali ihneď nahlásiť danej banke, aby to mohli bezpečnostní analytici čo najskôr preveriť a prípadne varovať ostatných klientov.

5.2 Univerzita MacEwan

Táto kanadská univerzita, ktorá sa v polovici minulého roka stala terčom podvodníkov sa nachádza v meste Edmonton. Títo podvodníci opäť využili sociálne inžinierstvo v praxi, keď sa vydávali za jednu z dodávateľských firiem. Pomocou emailovej komunikácie sa im podarilo presvedčiť zamestnancov univerzity, aby zmenili platobné údaje. Následne im škola poslala na účet 11,8 milióna kanadských dolárov. [17]

Po odhalení, že šlo o phishingový útok začala univerzita ihneď pracovať na tom, aby získala zaplatenú čiastku naspäť. Našťastie sa väčšiu časť tejto sumy (11,4 milióna kanadských dolárov) podarilo pomerne rýchlo vystopovať. Táto čiastka, ktorú vyšetrovatelia nechali ihneď zmraziť sa objavila na bankových účtoch v Kanade a Hongkongu. [17]

Aká celková škoda vznikla týmto neopatrným jednaním zatiaľ nie je úplne jasné. Takisto nie je isté či sa nakoniec podarí vypátrať úplne celú sumu. No univerzita sa zaviazala, že zavedie nové bezpečnostné postupy, aby sa podobné situácie už neopakovali. [17]

5.3 Kryptomena Ethereum

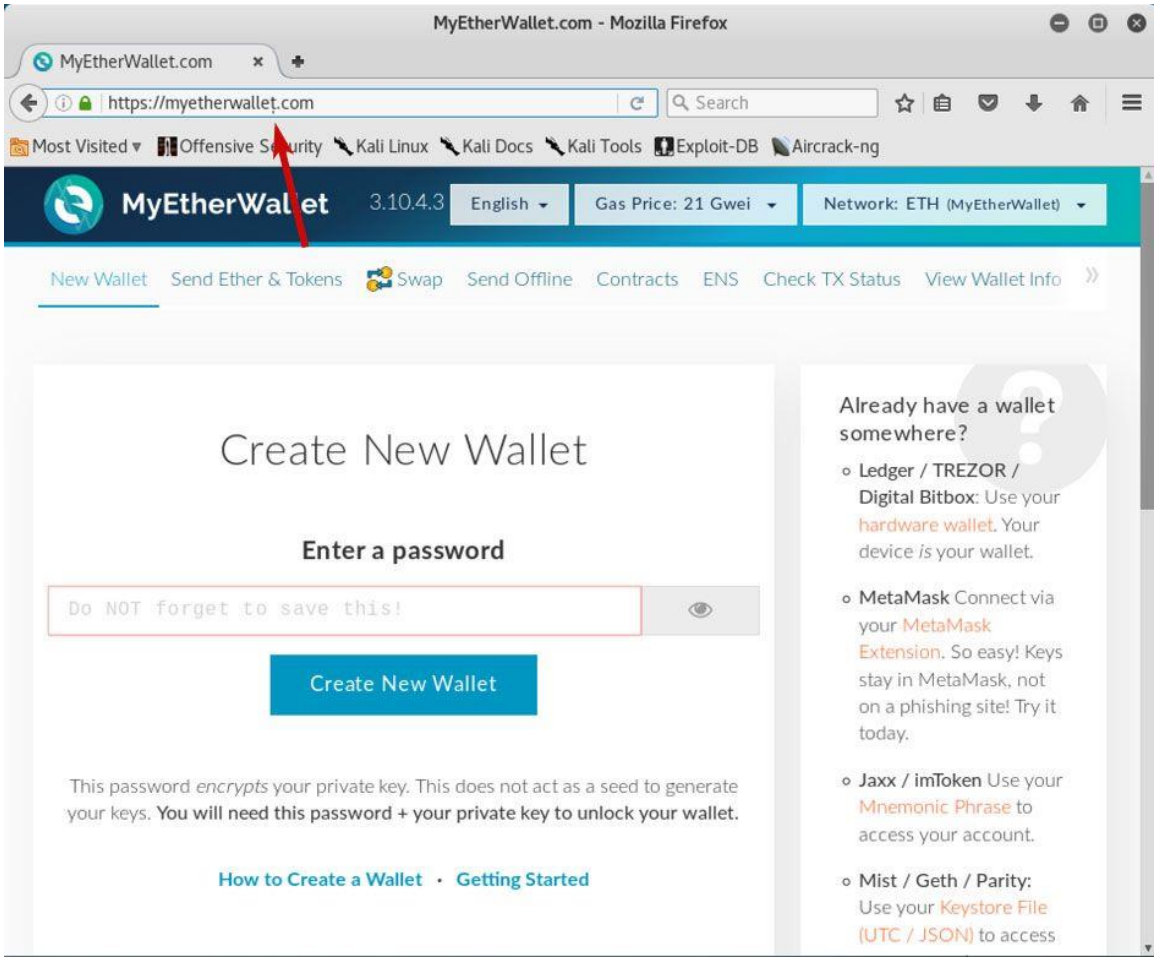
V posledných mesiacoch stále čoraz viac narastá popularita rôznych virtuálnych mien. A práve aj to je dôvod prečo sa podvodníci zameriavajú stále viac týmto smerom.

Koncom minulého roka sa stali terčom útokov vlastníci virtuálnej meny Ethereum, ktorí využívali open-source peňaženku MyEtherWallet. Tieto útoky boli o niečo sofistikovanejšie a mohli oklamať aj skúsenejších používateľov. [18]

Útočníci opäť využili phishingové emaily, ktorých obsah nabádal užívateľov, aby pod zámienkou aktualizácie klikli na priložený odkaz, synchronizovali peňaženku a skontrolovali bilanciu Etherea. [18]

Samotný email vyzeral pomerne vierohodne, angličtina bola tiež na vysokej úrovni a aj odkaz na stránku nepôsobil podozrivo. Avšak teraz prichádza ta zaujímavá časť, pretože po kliknutí na daný odkaz sa zobrazila presná kópia originálnej stránky. Aj webová adresa sa

zhodovala s originálom, a preto veľa užívateľov nemalo najmenšie tušenie, že aj napriek tomu sa jedná o podvod a už za niekoľko minút prídu o celý obsah svojej virtuálnej peňaženky.



Obrázok 12 Ukážka phishingovej stránky pre MyEtherWallet
Zdroj: [18]

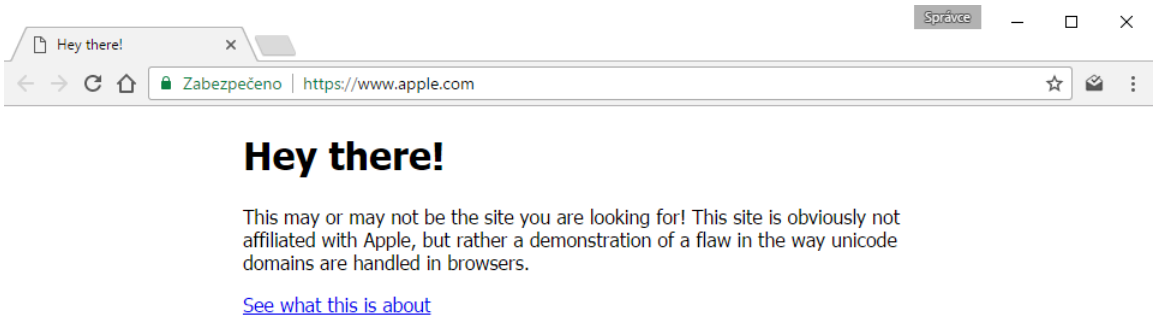
Avšak háčik bol práve v tom, že posledné písmeno nebol obyčajný ASCII znak *„t“,* ale šlo o Unicode znak, ktorý mal v spodnej časti ešte akúsi krátku čiarku. Takýto detail je takmer nemožné si všimnúť a mnoho užívateľov ho mohlo považovať len za prachovú časticu na monitore. Útočníci za približne dve hodiny takto odcudzili približne 52,56 Etherea, čo malo v tom čase hodnotu vyše 300 000 Kč. [18]

5.4 Apple.com

Nasledujúci útok na stránku *„apple.com“* našťastie nevyužili útočníci, ale bol použitý len ako príklad pri experimente čínskeho bezpečnostného odborníka Xudong Zheng. Tento čínsky špecialista sa zameral na hrozbu tzv. IDN phishingu, ktorý využíva chybu

v implementácii ochrany proti tzv. homograph attack a bol využitý aj pri útoku na virtuálnu peňaženku MyEtherWallet. [19]

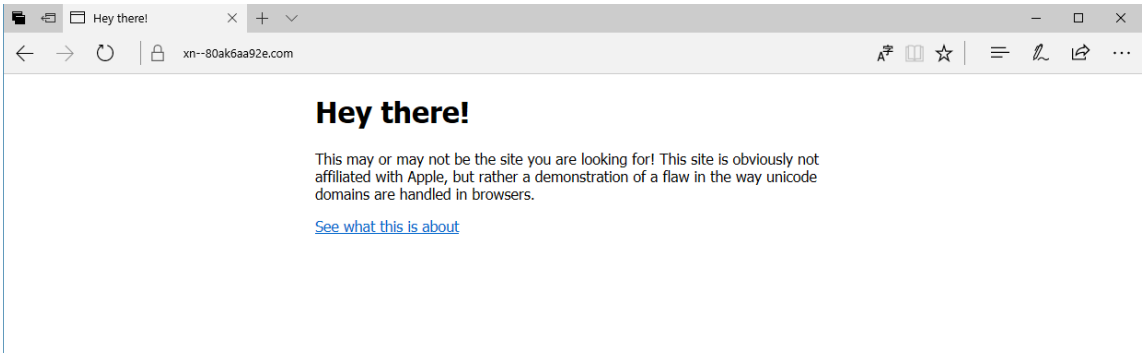
Pri tomto phishingu útočníci využívajú možnosť zaregistrovať si domény s národnými znakmi. Teda môžu využívať akékoľvek znaky zo sady Unicode. Je to problém hlavne z hľadiska, že mnoho Unicode znakov je veľmi náročné rozlíšiť od klasických ASCII znakov. Ak doménové meno stránky obsahuje znaky iba z jedného jazyka, tak niektoré internetové prehliadače jednoducho nedokážu odhaliť, že sa jedná o úplne inú stránku. Napríklad doména *„apple.com“* je registrovaná ako *„xn–80ak6aa92e.com“* kde sú využité len znaky z Cyriliky. Po zadaní tejto stránky do prehliadača, ktorý nemá mechanizmus na odhalenie takýchto útokov, tak zobrazí stránku ako na Obrázku 13. [20] [21]



Obrázok 13 Phishingový útok využívajúci IDN v prehliadači bez dostatočnej ochrany
Zdroj: [19]

V tomto prípade nie je dôležité všímať si obsah stránky, ktorá slúži len na demonštratívne účely, ale oveľa dôležitejšie je pole obsahujúce webovú adresu. Adresa vyzerá úplne identicky ako pre oficiálnu stránku Apple. Dokonca má vystavený aj vlastný certifikát a teda bez podrobnejšieho preskúmania certifikátu a pri doladení obsahu stránky by nebolo najmenších pochýb, že sa jedná o oficiálnu stránku. [22]

Na nasledujúcom obrázku je príklad ako sa takáto adresa zobrazí v prehliadači, ktorý má dostatočný bezpečnostný mechanizmus na odhalenie podobných útokov.



Obrázok 14 Phishingový útok využívajúci IDN v prehliadači s dostatočnou ochranou
Zdroj: [19]

V tomto prípade sa už nezobrazila adresa ako *„apple.com“*, ale ako skutočná adresa *„xn–80ak6aa92e.com“* a teda je možné odhaliť prípadný pokus o phishing veľmi jednoducho.

Takúto bezpečnostnú dieru mal donedávna aj prehliadač Google Chrome, avšak momentálne už túto chybu opravili. Taktiež ako Google Chrome to dokáže odhaliť aj často zavrhovaný prehliadač Microsoft Explorer, zatiaľ čo Mozilla Firefox ešte stále nie. Vo Firefoxe Xudong Zheng doporučuje zmeniť v *„about:config“* nastavenie *„network.IDN_show_punycode“* na hodnotu true. [21]

6 Anti-phishingový test

6.1 Kritéria testu

Zo stránky *„https://www.phishtank.com“* bola vybraná konkrétna vzorka sto potvrdených, aktívnych phishingových stránok. Tieto jednotlivé stránky sú z piatich rôznych oblastí internetu a to konkrétne:

- sociálne siete,
- finančné inštitúcie,
- streamovacie služby,
- internetové obchody,
- cloudové služby.

Následne každá vybraná webová stránka bola v rámci testu otvorená v piatich najpoužívanejších internetových prehliadačoch. Medzi tieto prehliadače patria:

- Google Chrome 64.0.3282.186,
- Mozilla Firefox Quantum 57.0,
- Opera 51.0.2830.40,
- Internet Explorer 11.0.9600.18920,
- Safari 5.1.7.

Testovanie prebiehalo výhradne bez použitia akýchkoľvek špecializovaných programov slúžiacich na ochranu pred nebezpečnými stránkami. Prehliadače Google Chrome, Mozilla Firefox Quantum a Safari majú v sebe zabudovanú funkciu na odhaľovanie potenciálne nebezpečných stránok. Preto tieto prehliadače boli otestované bez ich vstavanej ochrany proti podvodným stránkam, ale aj s ňou.

Test acid3 overuje správnu implementáciu webových štandardov internetových prehliadačov ako napríklad Document Object Model (DOM), JavaScript a ďalšie. Tento test bol spustený na stránke *„http://acid3.acidtests.org/“*.

Každý prehliadač je hodnotený celkovo v piatich hlavných kategóriách a ich podkategóriách pričom každá z nich je ohodnotená určitým počtom bodov:

- odhalenie phishingovej stránky – 50 bodov
- možnosť dodatočného nastavenia anti-phishingovej ochrany – 10 bodov

- možnosť externých doplnkov – 15 bodov
    - akékoľvek externé doplnky – 5 bodov
    - počet možných anti-phishingových doplnkov:
        - aspoň 1 doplnok – 2 body
        - aspoň 2 doplnky – 4 body
        - aspoň 3 doplnky – 6 bodov
        - aspoň 4 doplnky – 8 bodov
        - 5 a viac doplnkov – 10 bodov
- užívateľské prostredie – 15 bodov
    - možnosť vlastnej témy – 5 bodov
    - automatický import záložiek – 3 body
    - možnosť otvárania stránok v jednotlivých kartách – 2 body
    - rýchle vyhľadávanie pomocou klávese TAB pri písaní URL – 2 body
    - acid3:
        - 100-90 – 3 body
        - 89-75 – 2 body
        - 74-50 – 1 bod
        - 49-0 – 0 bodov
- ostatné (spotreba pamäte RAM, aktualizácie, rýchlosť) – 10 bodov
    - vyťaženie RAM (v MB):
        - 0-200 – 4 body
        - 201 – 400 – 2 body
        - 401 a viac – 0 bodov
    - priemerná doba spustenia:
        - 0-1 sekunda – 4 body
        - 1-3 sekundy – 2 body
        - viac ako 3 sekundy – 0 bodov
    - pravidelné aktualizácie – 2 body

Celkové body pridelené za odhalenie phishingovej stránky sú vypočítané pomocou jednoduchého vzorca $\frac{počet\ získaných\ bodov * 50}{100}$.

Maximum dosiahnutých bodov je teda presne 100. Súčtom jednotlivých bodov z každej vybranej kategórie bola následne vybraná konečná známka. Výsledné známky sú konkrétne:

- výborný – 100-90 bodov,
- veľmi dobrý – 89-75 bodov,
- dobrý – 74-50 bodov,
- nevyhovujúci – 49-0 bodov.

Celý proces testovania prebiehal na notebooku autora práce. Konfigurácia notebooku:

- Model: ASUS N53S
- Operačný systém: Windows 7 Home Premium
- Typ systému: 64-bitový
- Procesor: Intel® Core™ i7-2670QM, 2.2 GHz
- Pamäť RAM: 6 GB
- Grafická karta: NVIDIA GeForce® GT540M, 2 GB
- HDD: 750 GB

6.2 Testovaná vzorka

V nasledujúcej tabuľke sú konkrétne vybrané phishingové stránky z daných oblastí, ktoré boli postupne testovacím vstupom pre všetky spomínané prehliadače. V tabuľke sa nachádza poradové číslo stránky, popísaná oblasť a konkrétny odkaz na stránku.

Číslo	Oblasť internetu	URL odkaz
1	sociálne siete	http://vnrepots.heliohost.org/index.htm
2	sociálne siete	https://facebook.ba.org.ua/
3	sociálne siete	http://akunsecurity-com4.webnode.com/about/
4	sociálne siete	https://pages-central-recovery.ml/
5	sociálne siete	http://flymojo.com.ng/fgroup/?id=facebook
6	sociálne siete	http://privasi-acc.esy.es/
7	sociálne siete	https://vnnnmxzzxscvn.yolasite.com/
8	sociálne siete	http://listen.sitey.me/
9	sociálne siete	https://page-2018.yolasite.com/
10	sociálne siete	https://deloresmguay1.typeform.com/to/RykEmc
11	sociálne siete	http://akunsecurity-com4.webnode.com/about/
12	sociálne siete	https://peringatan-facebook19.webnode.com/about-us/
13	sociálne siete	https://central-page-recovery.gq/?Facebook.com=Recovery
14	sociálne siete	http://landing-page-display.ensarkizkurankursu.com/?Flow=9415118573539377&uid=b7d34bb847ae029c0ed96504d0edc367&toke=HPfAw0r=9&pagecode=1512928407.2586&actken===CDUtKkjuy1otoHTCCCY8V-a-lDWt9pUuyxo5LHQASbE7

		pGc=CLYs6xWs12V5o=WBhCE3ayZNmEI4dFgrVug8H=RBC6T925w-yzZra0lsitUtFyf
15	sociálne siete	http://hackear-fb.net/login.php
16	sociálne siete	http://0s.or3ws5dumvzc4y3pnu.drgo.ru/signup
17	sociálne siete	http://0s.or3ws5dumvzc4y3pnu.mbway.ru/signup
18	sociálne siete	http://0s.or3ws5dumvzc4y3pnu.xwerty.ru/signup
19	sociálne siete	http://finshome.com/
20	sociálne siete	http://sol.fm.br/index222.htm
21	finančné inštitúcie	http://standard.cba.pl/phone.php
22	finančné inštitúcie	http://52.70.129.120/js/.wp.php/rf/webapps/21f5f/websrc
23	finančné inštitúcie	http://warumrauchen.com/www.bb.com/
24	finančné inštitúcie	http://178.159.36.242/~hmornyf/Verify/bofa/
25	finančné inštitúcie	http://www.sabzcam.ir/cpen.scbs/sc.php
26	finančné inštitúcie	https://www.devapolline.fr/mbc.rses/sc.php
27	finančné inštitúcie	http://www.tornlundbygg.se/cpen.scbs/sc.php
28	finančné inštitúcie	http://www.viettaichi.q4.pl/prettyphoto/css/.@/acesso@seguro_banco_do_brasil/index1.php
29	finančné inštitúcie	http://bankofamericabusinessbanking.tk
30	finančné inštitúcie	https://acessocontaempresarial.com/pf.php
31	finančné inštitúcie	http://www.acessocontaempresarial.com
32	finančné inštitúcie	http://avecgestaoempresa.com
33	finančné inštitúcie	http://universitylanguageschool.com/wp-admin/images/index.php
34	finančné inštitúcie	https://citibwebs.com/update/
35	finančné inštitúcie	https://myvisioninteriordesign.com/
36	finančné inštitúcie	http://www.boucherierenerichard.com/te/
37	finančné inštitúcie	http://friendesign.com/financeiro/rjhjhgghghdhjhgDHJghjhsaGHJHJHGAJhjHGJAhjkhgjKDHGJagjhgGJHGHJHGHJFhgGHJGHhgjfgGHJGhgajghjghjHGJhgjHGJsa/FHFJHKDHJKsahjsfgjJHKAHAHJKhghjgjhjhahgjajkhlhgjASJKLahgjsdakjlSHGJsajklAHGJDSjlksAHGJSAJHasdsdadsasdadsasdarsfasaf.php
38	finančné inštitúcie	http://gsvvdesign.co/ametro
39	finančné inštitúcie	http://fraudinformationcenter14es.000webhostapp.com/HOMEPNc2017/HOMEPNc2017/auth/
40	finančné inštitúcie	http://jc00pnc0home0.000webhostapp.com/HOMEPNc2017%20_1/HOMEPNc2017/auth/

41	streamovacie služby	http://vdu.la-ligne-web.com
42	streamovacie služby	http://jeetkunedo31.com/6a3ce2f81c159ddb72546a526fce3f61a186a2806c6cc717b45bfbf1a92487c8bb26b063b0ffb2323c163edf441b576b1765f4a2de94af70c2cc9ac851efd0ee/session/page/login/
43	streamovacie služby	http://jeetkunedo31.com/66089ea9ca12d97527b4a82227e65cb1f9cb20c20f9cdd64b6eb656c48b3f5cc556dfe1f96bdfbe00957a3b2216966c5d72addac10c31e8b3cf5b53f84ea67b2/session/page/login/
44	streamovacie služby	http://br876.teste.website/~labor152/www.netflix.com/desktop/conta/index.php
45	streamovacie služby	https://hrp.ro/wp.php
46	streamovacie služby	http://promoteyourbrands.com/netflix-account-auth/indexa.html
47	streamovacie služby	http://fashionsky.com.cn/uploads/nexi.htm
48	streamovacie služby	https://netflix-account-auth.promoteyourbrands.com
49	streamovacie služby	https://netflix-account-auth.promoteyourbrands.com/indexa.html
50	streamovacie služby	http://blogp7.com.br/wp-includes/js/tinymce/plugins/colorpicker/rdr/d3/index.php?cliente=abuse@matadecagar.com.br
51	streamovacie služby	http://www.ruthconnell.org/
52	streamovacie služby	http://www.amchambd.org/Secured-Update-your-information/Secured-Update-your-information/Net/Rat6qAx/log/Login/
53	streamovacie služby	http://tiny.cc/2cu4qy
54	streamovacie služby	http://maitebijux.msnd1.com/tracking/lc/2217669b-9d01-4f9b-be9e-ad1f7f199383/c30995e1-a29f-4a92-8300-39ec4a89d67f/1d58ad18-550d-4c26-b0e0-9bfa033c9aae/
55	streamovacie služby	http://www.megustanetflix.com/us/registro1.php
56	streamovacie služby	http://www.megustanetflix.com/us/index.php
57	streamovacie služby	http://www.cinemanetflix.com/br/
58	streamovacie služby	http://svr.pamer.edu.pe/~pamered/DIR/info/net-flix/logging.php?country.x=en&locale.x=br_BR
59	streamovacie služby	http://svr.pamer.edu.pe/~pamered/DIR/info/net-flix/logging.php
60	streamovacie služby	http://pijal.club/
61	internetový obchod	https://www.allegro.pl.showitme.pl/apple-iphone-7-plus-gold-128gb-rezerwacja-i7091599813.html
62	internetový obchod	https://www.allegro.pl.showitme.pl/macbook-pro-retina-20162015-mid-rezerwacja-i7091599811.html#shippingInfo
63	internetový obchod	https://www.allegro.pl.showitme.pl/samsung-galaxy-s8-sm-g950f-64gb-nowy--i7091599807.html

64	internetový obchod	http://acessocontaempresarial.com
65	internetový obchod	https://www.antminers-bitmain.com/
66	internetový obchod	http://mojewnetrza.pl/logg.php
67	internetový obchod	http://www.ghousiasports.com/system/lib/cache/Alibaba.com/redirect.php
68	internetový obchod	http://https.signin.ebay.de.ebayisapidllocssignindeptnedeapppro.tsv-dauelsen.de/login.php?webscr&cmd=_login-run&SESSION=renpu6h70jIo539k3bo0zkEgCau0axtGgtIch1kB8gmdaYGiloAdiFD4vnq&dispatch=5e1b18c4c6a6d31695acbae3fd70ecc686c51678350f656dcc7f490a43946ee5cd758e8f59dfdf06a852adad277986ca
69	internetový obchod	http://upajmeter.com/css/bjqs/
70	internetový obchod	http://careertransitionworkshop.org/vega/
71	internetový obchod	https://theviralscene.com/wp-adm/133f7429ab5b1931321eefb20424964a/
72	internetové obchod	http://skinshut.com/kB2RO9f7UI/0n63p4uggy/ezm0lw7izn?q=kB2RO9f7UI&s=b98aec5c8324cc3696ea3bb8245f2035
73	internetové obchod	http://www.ghousiasports.com/system/cached/login.alibaba.com/
74	internetové obchod	https://steaRNcommuniFy.ml/tradeoffer/new/logon/&partner=324719633&token=S6WYNZv8
75	internetový obchod	https://csgolden.com/login/
76	internetový obchod	http://supportsteam.pe.hu/
77	internetový obchod	http://store.steampowered.com.ism.codes/
78	internetový obchod	https://theviralscene.com/wp-adm/99fe4dc8396c71d5c8350b1060585caf/
79	internetový obchod	http://csgotradecentral.weebly.com/
80	internetový obchod	http://www.ghousiasports.com/system/cached/Alibaba.com/redirect.php
81	cloudové služby	https://opmed.com.br/freshupdatenows/
82	cloudové služby	http://revsherri.com/drbfiles/drob/7feba8fe/x-mail/mxtool/actions/smallgif.html
83	cloudové služby	http://www.prismphotoimaging.com/dropfile.php
84	cloudové služby	https://purporabooks.com/redior/
85	cloudové služby	http://ywbcaf.org/wp-admin/images/dropfile.php
86	cloudové služby	http://fixleaks.com/dist/dxmbox/xmlprdot/
87	cloudové služby	https://hostmacau.com/~!@%23$%25^&*()_+~!@%23$%25^&*()_+/strdropbox-final/
88	cloudové služby	http://beta-technologies.net/docs/office-project/
89	cloudové služby	http://zecotilss.bid/rgulrul/dr2bf5o17on81w/ddfw/
90	cloudové služby	http://horchner.net/mines/happy/
91	cloudové služby	http://palabrasdevida.com.br/secureddocument/
92	cloudové služby	http://dropbox.com.jaifasteners.com/ll-ll/index.php

93	cloudové služby	http://ambasada.us/db222/db222/
94	cloudové služby	http://forums.goninja.de/data/WeTransfer/WeTransfer/new.php?cmd=login_submit&id=6c8d40df5b6f632e283e35f6103bc6c16c8d40df5b6f632e283e35f6103bc6c1&session=6c8d40df5b6f632e283e35f6103bc6c16c8d40df5b6f632e283e35f6103bc6c1
95	cloudové služby	http://forums.goninja.de/data/WeTransfer/WeTransfer/index.php
96	cloudové služby	http://laraoshoncolor.com/olo/nsw/data/office365.htm
97	cloudové služby	http://lambamsworld.com/transfer/rfm/4086930a9ce88a312c9bff067f11cddf/
98	cloudové služby	http://lambamsworld.com/transfer/rfm/
99	cloudové služby	http://zecotilss.bid/rgulrul/dr2bf5o17on81w/ddfw/74119851b5d20151e198cf77deffa3c7/
100	cloudové služby	https://www.staraskola.mk/mek/nme/nme/nme/rdc/index.php

Tabuľka 1 Vzorka phishingových stránok
Zdroj: [29] (spracovanie autora)

6.3 Testované prehliadače

V tejto podkapitole sú stručne predstavené jednotlivé testované prehliadače.

6.3.1 Google Chrome

Google Chrome, ako napovedá už samotný názov, je voľne dostupný webový prehliadač od spoločnosti Google, ktorý je najpoužívanejším prehliadačom vo svete. Tento prehliadač je vyvíjaný v jazyku C++ a prvá verzia bola vypustená do sveta koncom roka 2008. V súčasnosti je kompatibilný s operačným systémom Microsoft Windows, Android, iOS, macOS a Linux. Jednou z najväčších nevýhod tohto prehliadača je ale príliš veľká spotreba pamäte RAM. [30]

Obrázok 15 Google Chrome logo
Zdroj: [30]

6.3.2 Mozilla Firefox

Mozilla Firefox je bezplatný webový prehliadač, ktorý je vyvíjaný za pomoci stoviek dobrovoľníkov Mozilla Corporation. Prvá verzia bola vydaná už koncom roku 2004 a stala sa najviac používaným programom s otvoreným kódom. Prehliadač je dostupný pre Microsoft Windows, Android, Linux, macOS, ale aj pre ďalšie menej známe operačné systémy ako FreeBSD, SkyOS či BeOS. [31]

Obrázok 16 Mozilla Firefox logo
Zdroj: [31]

6.3.3 Opera

Tento internetový prehliadač je vyvíjaný nórskou firmou Opera Software. Prvé verzie Opery boli najskôr spoplatnené, ale od verzie 8.5 je taktiež zdarma. Opera je rovnako ako predchádzajúce prehliadače kompatibilná s väčšinou najpoužívanejších operačných systémov pre počítače a telefóny. [32]

Obrázok 17 Opera logo
Zdroj: [32]

6.3.4 Internet Explorer

Internet Explorer je webový prehliadač od spoločnosti Microsoft, ktorý je súčasťou všetkých operačných systémov od Microsoftu. Prvá verzia bola vydaná už v polovici roku 1995. Tento prehliadač je často kritizovaný práve kvôli jeho bezpečnostnej politike, ktorá vďaka veľkým bezpečnostným chybám umožňovala veľmi jednoduché šírenie rôznych vírusov, spyware a pod. Avšak nové verzie už v tejto oblasti spravili mierny pokrok. [33]

Obrázok 18 Internet Explorer logo
Zdroj: [33]

6.3.5 Safari

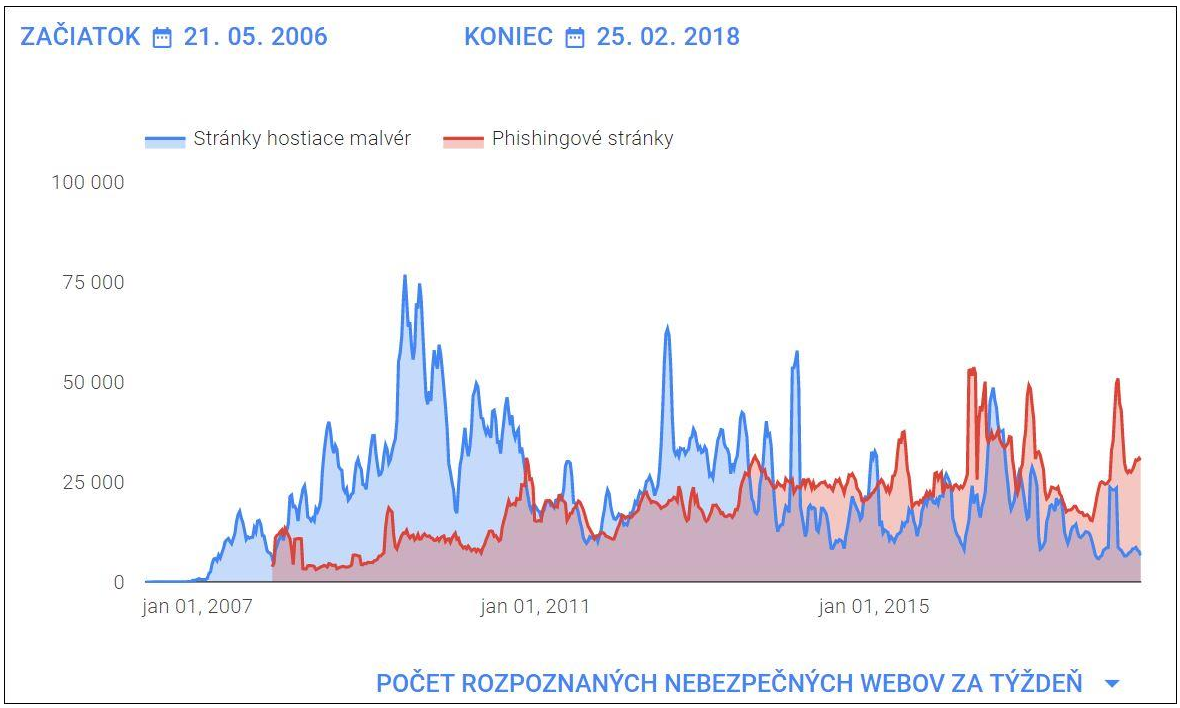
Webový prehliadač Safari, ktorý vyvíja spoločnosť Apple Inc. je súčasťou operačných systémov iOS a macOS. Prvá verejná verzia bola vydaná na začiatku roku 2003. V roku 2007 bola predstavená aj oficiálna verzia pre operačné systémy Windows, ale časom bol jej vývoj

kvôli malému tržnému podielu zrušený. Poslednou oficiálnou verziou pre Windows je Safari 5.1.7. [34]

Obrázok 19 Safari logo
Zdroj: [34]

6.4 Anti-phishingová ochrana v prehliadačoch

Odhalenie phishingovej stránky webovým prehliadačom vo veľkej miere závisí od toho, aké databázy používajú a ako často sú schopné svoje vlastné databázy aktualizovať. Takúto funkčnosť by mal mať v dnešnej dobe už každý moderný prehliadač. Google Chrome, Mozilla Firefox a Safari majú vo svojich nastaveniach možnosť zapnúť anti-phishingovú ochranu. Zapnutím tohto nastavenia sa zmení frekvencia aktualizácie zoznamov stránok s podozrivým obsahom (Mozilla Firefox uvádza frekvenciu každých 30 minút), takže novšie phishingové stránky môžu byť oveľa rýchlejšie rozpoznané. Google Chrome okrem upozornenia užívateľa, ktorý na stránku pristupuje, taktiež informuje aj správcu daného webu, pretože v niektorých prípadoch sa jedná o legitímne weby, ktoré boli napadnuté a následne zneužité hackermi. [35] [36]



Graf 7 Počet rozpoznaných nebezpečných webov Google Chrome za týždeň
Zdroj: [36]

Na grafe vyššie je zobrazený počet odhalených nebezpečných webov prehliadačom Google Chrome od roku 2006 až po rok 2018. Tento počet odhalených phishingových stránok v roku 2007 bol ďaleko pod úrovňou 25 000 avšak od roku 2011 sa tento počet začal postupne zvyšovať aj keď sa tam nachádzajú aj občasné výchylky. Každopádne to nemení nič na veci, že technológie prehliadačov, ktoré dokážu odhaliť nebezpečné stránky sa postupom času zlepšujú, no taktiež sa aj počet takýchto stránok každým rokom stále zvyšuje.

7 Vlastný anti-phishingový test

Pred úplným začiatkom anti-phishingového testu boli nainštalované najnovšie oficiálne dostupné verzie všetkých testovaných webových prehliadačov. Proces inštalácie prebehol so základnými nastaveniami, ktoré automaticky nastavil sprievodca inštaláciou. Taktiež neboli dodatočne inštalované žiadne externé doplnky, ktoré by mohli ovplyvniť výsledky testov.

7.1 Priebeh testu

Do nasledujúcej tabuľky boli postupne zaznamenané jednotlivé výsledky testu. V prvom stĺpci sa nachádza poradové číslo stránky, ktoré je uvedené rovnako aj v predchádzajúcej tabuľke s konkrétnymi vzorkami stránok. Zvyšné stĺpce tvoria jednotlivé prehliadače. Následné čísla 0 a 1 znamenajú bodové ohodnotenie za odhalenie phishingovej stránky, kedy 0 znamená, že phishingovú stránku webový prehliadač nedokázal odhaliť a 1 znamená, že došlo k úspešnému upozorneniu, že sa na stránke nachádza klamlivý alebo nebezpečný obsah. Posledný záznam v tabuľke je tvorený súčtom všetkých získaných bodov, na základe ktorých sa bude odvíjať bodové ohodnotenie v danej kategórii.

Poradové číslo	Google Chrome	Google Chrome (s aktívnou ochranou)	Mozilla Firefox	Mozilla Firefox (s aktívnou ochranou)	Opera	Internet Explorer	Safari	Safari (s aktívnou ochranou)
1	0	1	0	0	1	1	0	1
2	0	0	0	0	1	0	0	0
3	0	0	0	0	1	1	0	0
4	0	1	0	1	1	1	0	1
5	0	1	0	1	1	1	0	0
6	0	1	0	0	1	1	0	0
7	0	0	0	0	1	0	0	0
8	0	1	0	1	1	1	0	0
9	0	1	0	1	1	1	0	0
10	0	0	0	0	1	0	0	0
11	0	0	0	0	1	1	0	0
12	0	1	0	1	1	1	0	1
13	0	1	0	1	1	1	0	1
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	1	0	0	0
17	0	0	0	0	1	0	0	0
18	0	0	0	0	1	0	0	0

19	0	1	0	1	1	1	0	0
20	0	1	0	1	1	1	0	1
21	0	0	0	0	1	0	0	0
22	0	1	0	1	1	1	0	0
23	0	1	0	1	1	1	0	0
24	0	1	0	0	1	1	0	1
25	0	1	0	1	1	0	0	1
26	0	1	0	1	1	0	0	1
27	0	1	0	1	1	0	0	1
28	0	0	0	0	1	0	0	0
29	0	0	0	0	1	0	0	0
30	1	1	1	1	1	1	1	1
31	0	1	0	0	1	1	0	1
32	0	0	0	0	1	0	0	0
33	1	1	1	1	1	1	1	1
34	0	1	0	1	1	0	0	1
35	0	0	0	0	1	0	0	0
36	0	1	0	0	1	0	0	0
37	0	1	0	1	0	1	0	0
38	0	0	0	0	1	0	0	0
39	0	1	0	1	1	1	0	1
40	0	0	0	0	1	1	0	0
41	0	0	0	0	1	0	0	0
42	0	1	0	1	1	1	0	1
43	0	1	0	1	1	1	0	1
44	1	1	1	1	1	1	1	1
45	0	0	0	0	0	0	1	1
46	0	1	0	0	1	1	0	1
47	0	1	0	1	1	0	0	1
48	0	1	0	1	1	0	0	1
49	0	1	0	0	1	1	0	1
50	0	1	0	1	0	1	0	1
51	0	0	0	0	1	1	0	0
52	0	0	0	0	1	0	0	0
53	0	0	0	0	0	0	0	0
54	1	1	1	1	1	1	1	1
55	1	1	1	1	1	1	1	1
56	1	1	1	1	1	1	1	1
57	0	0	0	0	1	0	0	0
58	1	1	1	1	1	1	1	1
59	1	1	1	1	1	1	1	1
60	1	1	1	1	1	1	1	1
61	0	1	0	1	1	0	0	1
62	0	1	0	1	1	0	0	1
63	0	1	0	1	1	0	0	1
64	0	1	0	0	1	1	0	1

65	0	0	0	0	1	0	0	0
66	0	0	0	0	1	0	0	0
67	0	1	0	1	0	1	0	1
68	0	1	0	1	1	1	0	1
69	0	1	0	1	1	0	0	1
70	0	1	0	0	1	1	0	1
71	0	1	0	0	1	1	0	1
72	0	1	0	1	1	1	0	1
73	0	1	0	0	1	1	0	1
74	0	1	0	1	1	1	0	1
75	0	1	0	0	1	1	0	0
76	0	0	0	0	1	0	0	0
77	0	0	0	0	1	0	0	0
78	0	1	0	0	1	1	0	1
79	0	0	0	0	1	0	0	0
80	0	1	0	1	0	1	0	1
81	0	1	0	1	1	1	1	1
82	0	0	0	0	1	1	0	0
83	0	1	0	1	1	1	0	1
84	0	1	0	0	1	1	1	1
85	0	1	0	1	0	1	0	1
86	0	1	0	1	1	1	0	0
87	0	0	0	0	0	0	0	0
88	0	1	0	1	1	1	0	0
89	0	1	0	1	1	1	0	0
90	0	1	0	0	1	1	0	0
91	0	1	0	1	1	1	0	0
92	0	1	0	1	1	1	0	0
93	0	1	0	0	1	1	0	0
94	0	1	0	1	1	1	0	0
95	0	1	0	1	1	1	0	0
96	0	1	0	0	1	1	0	0
97	0	1	0	0	1	1	0	0
98	0	1	0	1	1	1	0	0
99	0	1	0	0	1	1	0	0
100	0	1	0	1	1	1	1	1
Súčet	9	70	9	51	90	64	13	48

Tabuľka 2 Výsledky testu
Zdroj: Autor

7.2 Výsledky testu

Výsledky tohto anti-phishingového testu sú vcelku rozmanité a pre niekoho možno až prekvapujúce. Na nasledujúcom grafe je zobrazená úspešnosť jednotlivých prehliadačov aký počet phishingových stránok dokázali počas testu odhaliť z celového počtu sto stránok.

Graf 8 Počet odhalených phishingových stránok
Zdroj: Autor

Nekompromisným lídrom s obrovským náskokom je jednoznačne prehliadač Opera, ktorý dokázal odhaliť takmer všetky testované stránky a to v počte až 90 stránok. Na druhom mieste skončil Google Chrome so zapnutou aktívnou ochranou v nastaveniach a hneď v závese za ním často podceňovaný Internet Explorer od Microsoftu. Mozilla Firefox a Safari, oba so zapnutou aktívnou ochranou, dokázali odhaliť len približne polovicu podvodných stránok. Bez tejto aktívnej ochrany všetky tri prehliadače Google Chrome, Mozilla Firefox a Safari skončili s katastrofálnym výsledkom kedy nedokázali upozorniť používateľa na nebezpečnú stránku ani v 15% prípadov.

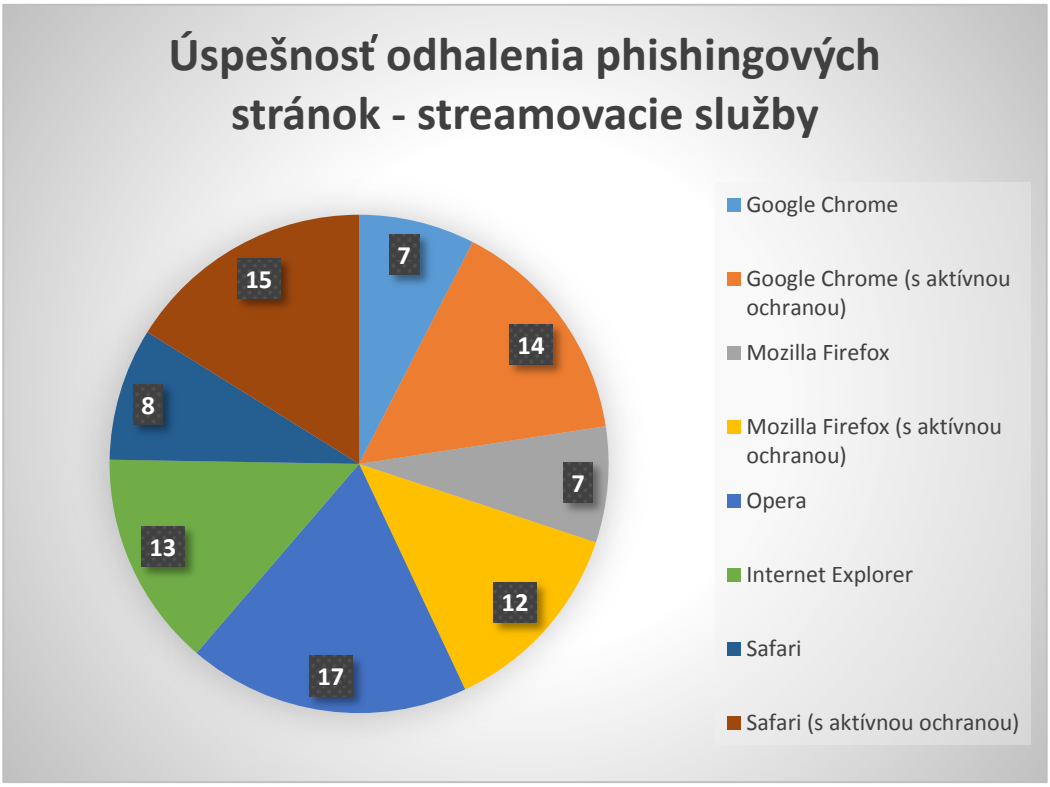
Keďže existuje určitý predpoklad, že stránky, ktoré sú zamerané na bankové inštitúcie, rôzne platené služby prípadne internetové obchody budú na vyššej technickej úrovni, ktorá by teoreticky mohla sťažiť odhalenie ako napríklad stránky so zameraním na sociálne siete. Je to hlavne kvôli tomu, že na takýchto stránkach sa celkovo kladie väčší dôraz na bezpečnosť ako pri obyčajnom prihlasovaní na Facebook. Takže na ďalšom grafe je možné vidieť celkovú percentuálnu úspešnosť odhalenia phishingovej stránky podľa toho, o ktorú testovanú oblasť sa jedná.

Graf 9 Celková úspešnosť odhalenia phishingovej stránky v závislosti na danej oblasti
Zdroj: Autor

Všetky testované prehliadače dokázali celkovo najúspešnejšie rozpoznať phishingové stránky zamerané na streamovacie služby typu Netflix. Avšak táto iba 26% úspešnosť je značne znížená práve kvôli neschopnosti Google Chrome, Mozille Firefox a Safari odhaliť podstatne väčšie množstvo týchto stránok. Nasledujú cloudové služby v tesnom závese s finančnými inštitúciami a internetovými obchodmi. Avšak najmenej úspešné boli prehliadače práve pri sociálnych sieťach s celkovou úspešnosťou len 15%.

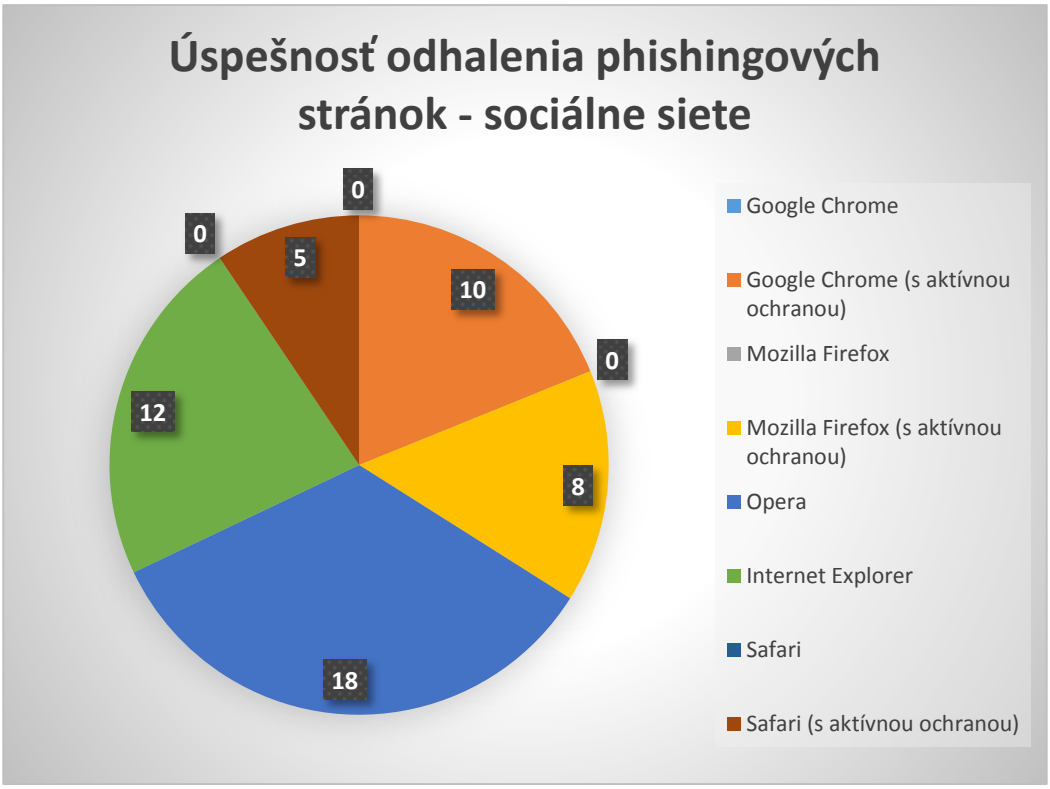
Streamovacím službám, ktoré skončili na prvom mieste a sociálnym sieťam, ktoré obsadili poslednú priečku sa budú venovať ešte nasledujúce dva grafy.

Na prvom z nich je zobrazená úspešnosť jednotlivých prehliadačov pri rozpoznávaní nebezpečných stránok obsahujúcich podvodný obsah na stránkach streamovacích služieb. Aj v tomto prípade je vo vedení prehliadač Opera so 17 odhalenými stránkami nasledovaný Safari a Google Chrome opäť oba s aktívnou ochranou proti podozrivým webom. V tomto prípade aj bez dodatočne zapnutej ochrany sa dokázali prehliadače Google Chrome, Mozilla Firefox a Safari priblížiť takmer polovičnej úspešnosti.



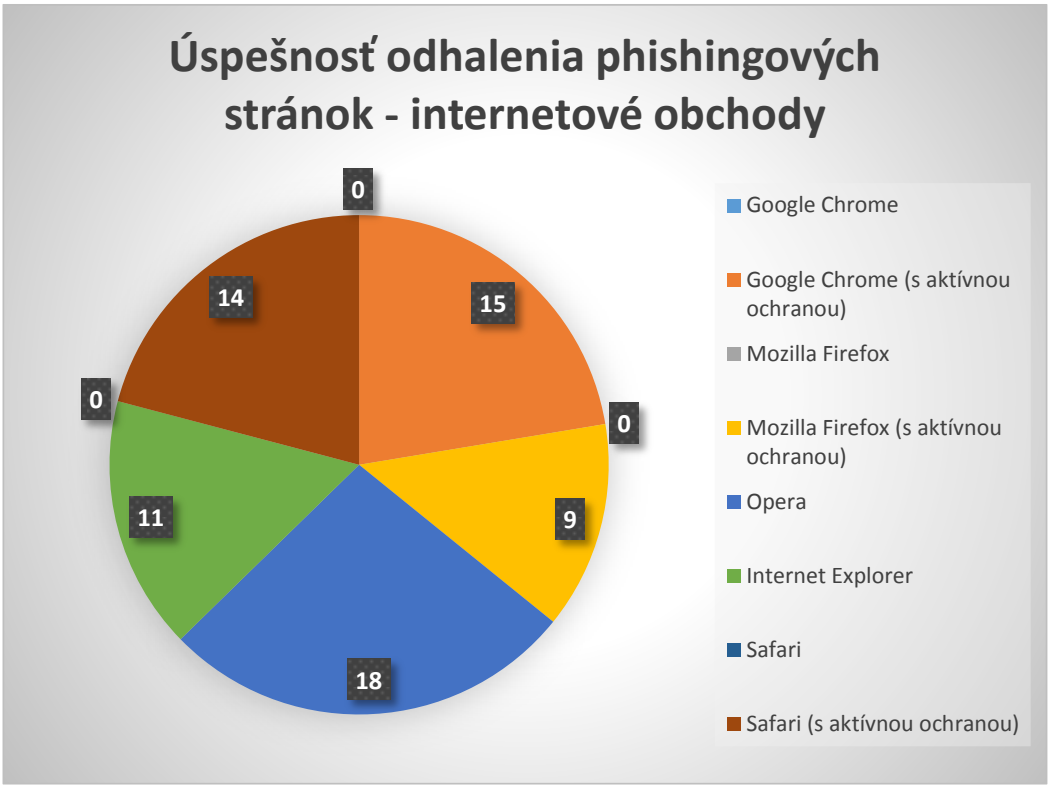
Graf 10 Úspešnosť odhalenia phishingových stránok - streamovacie služby
Zdroj: Autor

Na nasledujúcom grafe je možné vidieť úspešnosť odhalenia phishingových stránok z najmenej úspešnej oblasti, sociálne siete.



Graf 11 Úspešnosť odhalenia phishingových stránok - sociálne siete
Zdroj: Autor

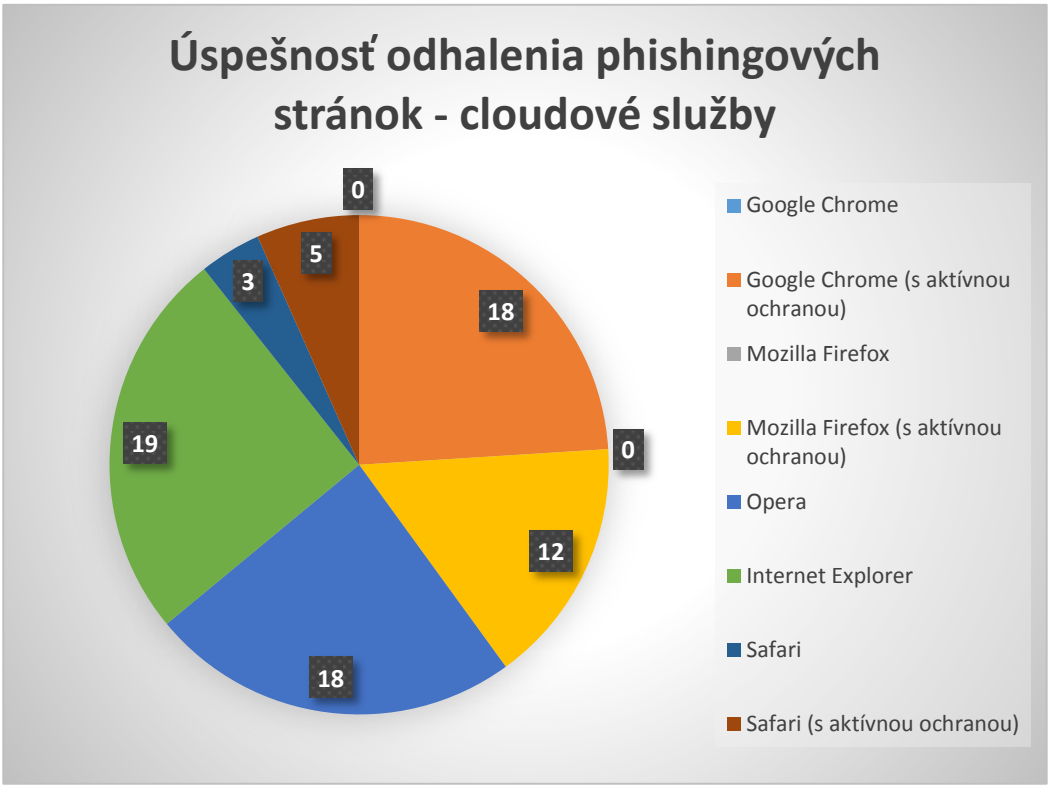
V tomto prípade doslova katastrofálny výsledok mala opäť trojica prehliadačov Google Chrome, Mozilla Firefox a Safari, ale bez zapnutej dodatočnej ochrany, kedy žiaden z nich nedokázal odhaliť čo len jedinú phishingovú stránku. No na druhej strane prehliadač Opera zasa exceloval s 18 upozorneniami užívateľa pred podvodným obsahom stránky.



Graf 12 Úspešnosť odhalenia phishingových stránok - internetové obchody
Zdroj: Autor

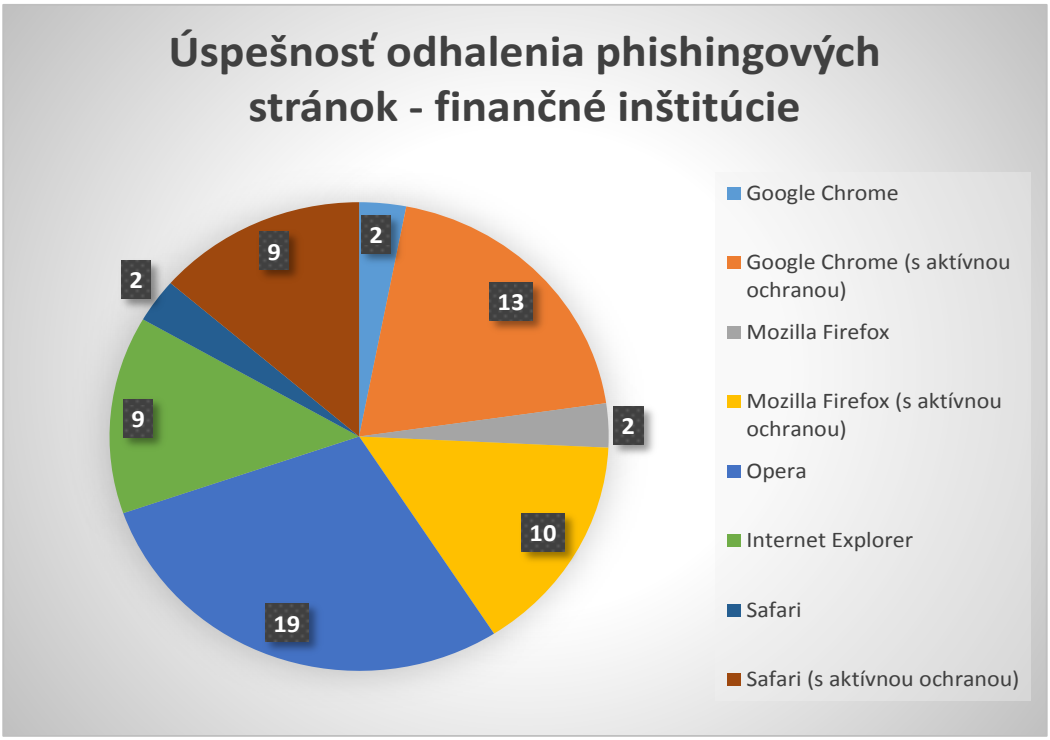
Na grafe vyššie je zobrazená úspešnosť odhalenia podvodných stránok z oblasti internetových obchodov. V tomto prípade opäť veľkým sklamaním boli prehliadače Chrome, Firefox a Safari v základnom nastavení. Opera aj v tomto prípade dosiahla takmer svoje maximum.

Na nasledujúcom grafe je vidieť, že dvojica prehliadačov Chrome a Firefox so základným nastavením zase nedokázali odhaliť čo i len jedinú podvodnú stránku ani v oblasti cloudových služieb, zatiaľ čo prehliadač Safari si trochu polepšil a dokázal upozorniť užívateľa aspoň na tri phishingové stránky. Avšak Internet Explorer dokázal odhaliť takmer úplne všetky stránky v tejto oblasti.



Graf 13 Úspešnosť odhalenia phishingových stránok - cloudové služby
Zdroj: Autor

Na poslednom grafe kde sú zobrazené výsledky úspešnosti odhalenia phishingových stránok z oblasti finančných inštitúcií je možné vidieť, že tentoraz webový prehliadač Opera dokázal odhaliť takmer všetky podvodné stránky až na jednu.



Graf 14 Úspešnosť odhalenia phishingových stránok - finančné inštitúcie
Zdroj: Autor

7.3 Hodnotenie jednotlivých prehliadačov

Celkové hodnotenie prehliadačov je závislé na počte získaných bodov v jednotlivých kategóriách.

7.3.1 Google Chrome

Google Chrome ako najpopulárnejší webový prehliadač príliš neoslnil čo sa týka anti-phishingového testu. Bez zapnutej aktívnej ochrany dokázal odhaliť len minimálne množstvo podvodných stránok, ale po aktivovaní tejto ochrany sa tento počet značne zvýšil. Avšak možnosť takto jednoduchej deaktivácie tohto nastavenia je značná nevýhoda keďže môže dôjsť k náhodnému vypnutiu a tým pádom vystaveniu sa väčšiemu nebezpečenstvu. Práve z tohto dôvodu bol v tomto prípade udelený len polovičný počet bodov v danej kategórii. Čo sa týka externých doplnkov, tak existuje obrovské množstvo rôznych rozšírení tohto prehliadača. Medzi nimi je možné nájsť aj anti-phishingové doplnky ako napríklad Anti-Phishing & Authenticity Checker alebo Netcraft Extension, ktoré by mali zvýšiť ochranu prehliadania. Užívateľské prostredie je taktiež príjemné, jednoduché a intuitívne. Nastavenia prehliadača sú veľmi prehľadné. Medzi nevýhodu patrí značná spotreba pamäte RAM, no na priemernom počítači pracuje rýchlo. Taktiež o neustále vylepšenia či už bezpečnosti alebo výkonu sa starajú aj pravidelné aktualizácie.

Bodové ohodnotenie:

- odhalenie phishingovej stránky – 35 bodov
- možnosť dodatočného nastavenia anti-phishingovej ochrany – 5 bodov
- možnosť externých doplnkov:
    - akékoľvek externé doplnky – 5 bodov
    - počet možných anti-phishingových doplnkov – 10 bodov
- užívateľské prostredie:
    - možnosť vlastnej témy – 5 bodov
    - automatický import záložiek – 3 body
    - možnosť otvárania stránok v jednotlivých kartách – 2 body
    - rýchle vyhľadávanie pomocou klávese TAB pri písaní URL – 2 body
    - acid3 – 3 body
- ostatné (spotreba pamäte RAM, aktualizácie, rýchlosť):

    - vyťaženie RAM – 2 body
    - priemerná doba spustenia – 4 body
    - pravidelné aktualizácie – 2 body
- **Celkom: 78 bodov**
- **Známka: veľmi dobrý**

7.3.2 Mozilla Firefox

Mozilla Firefox je na tom veľmi podobne ako prehliadač od Googlu čo sa týka upozornenia užívateľa na stránky s podvodným obsahom. Bez aktivovanej ochrany toho odhaliť nedokázal takmer nič, ale s aktivovanou ochranou sa to o niečo zlepšilo. Opäť je to považované za nevýhodu, že je vôbec možné toto nastavenie vypnúť jediným kliknutím bez akéhokoľvek upozornenia. Preto bol pridelený opäť len polovičný počet bodov. Taktiež má možnosť veľkého množstva rôznych externých doplnkov. Medzi tie anti-phishingové patria Netcraft Anti-Phishing Extension alebo Browser-Security a iné. Užívateľské prostredie je príjemné, rovnako aj nastavenia, ale menu je trochu menej prehľadné ako u Chrome. Pri jeho používaní spotrebúva pomerne dosť pamäte RAM, no opäť sa zdá byť vcelku rýchly s aktualizáciami na pravidelnej báze.

Bodové ohodnotenie:

- odhalenie phishingovej stránky – 25,5 bodov
- možnosť dodatočného nastavenia anti-phishingovej ochrany – 5 bodov
- možnosť externých doplnkov:
    - akékoľvek externé doplnky – 5 bodov
    - počet možných anti-phishingových doplnkov – 10 bodov
- užívateľské prostredie:
    - možnosť vlastnej témy – 5 bodov
    - automatický import záložiek – 3 body
    - možnosť otvárania stránok v jednotlivých kartách – 2 body
    - rýchle vyhľadávanie pomocou klávese TAB pri písaní URL – 0 bodov
    - acid3 – 3 body
- ostatné (spotreba pamäte RAM, aktualizácie, rýchlosť):
    - vyťaženie RAM – 0 bodov

    - priemerná doba spustenia – 2 body
    - pravidelné aktualizácie – 2 body
- **Celkom: 62,5 bodov**
- **Známka: dobrý**

7.3.3 Opera

V anti-phishingovom teste tento prehliadač jednoznačne dominoval a dokázal odhaliť takmer všetky testované stránky. Dokonca k tomu nepotreboval ani žiadne extra nastavenie. Takže v tomto smere celkovo prekvapil. Doplnky ako aj u predchádzajúcich sa dajú stiahnuť z oficiálnej stránky pre daný prehliadač. K anti-phishingovým patrí napríklad opäť Netcraft Extension alebo PunyCode Domain Detection. Druhé spomínané rozšírenie slúži práve na odhalenie unicode domén. Celkové užívateľské prostredie je veľmi príjemné na prvý pohľad, všetko je prehľadné a jednoduché. Pamäte RAM spotrebúva podstatne menej ako Firefox. Prehliadač taktiež dostáva pravidelne nové aktualizácie pre vylepšenie výkonu a bezpečnosti.

Bodové ohodnotenie:

- odhalenie phishingovej stránky – 45 bodov
- možnosť dodatočného nastavenia anti-phishingovej ochrany – 0 bodov
- možnosť externých doplnkov:
    - akékoľvek externé doplnky – 5 bodov
    - počet možných anti-phishingových doplnkov – 10 bodov
- užívateľské prostredie:
    - možnosť vlastnej témy – 5 bodov
    - automatický import záložiek – 3 body
    - možnosť otvárania stránok v jednotlivých kartách – 2 body
    - rýchle vyhľadávanie pomocou klávese TAB pri písaní URL – 0 bodov
    - acid3 – 3 body
- ostatné (spotreba pamäte RAM, aktualizácie, rýchlosť):
    - vyťaženie RAM – 4 body
    - priemerná doba spustenia – 4 body
    - pravidelné aktualizácie – 2 body

- **Celkom: 83 bodov**
- **Známka: veľmi dobrý**

7.3.4 Internet Explorer

Prehliadač od spoločnosti Microsoft dokázal upozorniť užívateľa na phishingovú stránku vo viac ako polovici prípadoch. Ako aj u Opery, tak aj v tomto prípade chýbala možnosť zapnúť extra ochranu. Ak by tam taká možnosť bola, tak výsledky by boli zrejme ešte o triedu lepšie. Nainštalovať externé doplnky do tohto prehliadača je podstatne náročnejšie ako u ostatných prehliadačov a aj ich výber je značne obmedzený. Užívateľské prostredie je viac menej neutrálne, ničím zvláštnym užívateľa neohúri. Rýchlosť prehliadača Internet Explorer nie je vždy najlepšia ako aj celková stabilita. Avšak pamäť RAM spotrebuje najmenej zo všetkých testovaných prehliadačov.

Bodové ohodnotenie:

- odhalenie phishingovej stránky – 32 bodov
- možnosť dodatočného nastavenia anti-phishingovej ochrany – 0 bodov
- možnosť externých doplnkov:
    - akékoľvek externé doplnky – 5 bodov
    - počet možných anti-phishingových doplnkov – 0 bodov
- užívateľské prostredie:
    - možnosť vlastnej témy – 0 bodov
    - automatický import záložiek – 0 bodov
    - možnosť otvárania stránok v jednotlivých kartách – 2 body
    - rýchle vyhľadávanie pomocou klávese TAB pri písaní URL – 0 bodov
    - acid3 – 3 body
- ostatné (spotreba pamäte RAM, aktualizácie, rýchlosť):
    - vyťaženie RAM – 4 body
    - priemerná doba spustenia – 2 body
    - pravidelné aktualizácie – 2 body
- **Celkom: 50 bodov**
- **Známka: dobrý**

7.3.5 Safari

Prehliadač určený predovšetkým pre zariadenia od Applu dokázal v poslednej oficiálnej verzii pre Windows odhaliť približne polovicu podvodných stránok. Aj napriek tomu, že táto verzia je niekoľko rokov stará, tak v nastaveniach sa objavilo tlačidlo pre aktivovanie anti-phishingovej ochrany. Doplnky pri tejto Windows verzii už nie sú podporované. Prostredie prehliadača má už trochu starší nádych. V spotrebe pamäte RAM patrí do prvej trojice najšetrnejších prehliadačov z pomedzi testovaných. Absencia ďalších aktualizácií značne obmedzuje lepšie a bezpečnejšie fungovanie tohto prehliadača.

Bodové ohodnotenie:

- odhalenie phishingovej stránky – 24 bodov
- možnosť dodatočného nastavenia anti-phishingovej ochrany – 5 bodov
- možnosť externých doplnkov:
    - akékoľvek externé doplnky – 0 bodov
    - počet možných anti-phishingových doplnkov – 0 bodov
- užívateľské prostredie:
    - možnosť vlastnej témy – 0 bodov
    - automatický import záložiek – 0 bodov
    - možnosť otvárania stránok v jednotlivých kartách – 2 body
    - rýchle vyhľadávanie pomocou klávese TAB pri písaní URL – 0 bodov
    - acid3 – 3 body
- ostatné (spotreba pamäte RAM, aktualizácie, rýchlosť):
    - vyťaženie RAM – 4 body
    - priemerná doba spustenia – 2 body
    - pravidelné aktualizácie – 0 bodov
- **Celkom: 40 bodov**
- **Známka: nevyhovujúci**

7.4 Celkové hodnotenie prehliadačov

V tomto teste najlepšie obstál prehliadač Opera s dohromady 83 bodmi a známkou *„veľmi dobrý“*. Na druhom mieste skončil s rovnakou známkou Google Chrome, ktorého celkové bodové ohodnotenie je 78. Prehliadač Mozilla Firefox sa umiestnil na tretej priečke

s o stupeň horšou známkou *„dobrý“* a celkovým počtom bodov 62,5. Veľmi tesne na hranici tejto známky ešte skončil Internet Explorer s presne 50 bodmi. Známku *„nevyhovujúci“* dosiahol webový prehliadač Safari, ktorý sa umiestnil na úplne poslednej priečke len so 40 bodmi. Toto poradie je zobrazené aj na nasledujúcom grafe.

Graf 15 Celkové poradie prehliadačov
Zdroj: Autor

8 Odporúčania pre obete phishingu

V prípade, že sa užívateľ stane obeťou phishingovej stránky, tak by nemal spanikáriť, ale si predovšetkým uvedomiť všetky potrebné kroky, ktoré je nutné spraviť, aby šanca na zneužitie získaných údajov útočníkom sa zminimalizovala. Jednotlivé kroky, ktoré by mali nasledovať sa líšia v závislosti na tom o aký prípad phishingu sa jedná. Záleží či došlo k získaniu údajov k účtu na sociálnej sieti alebo o prístup k údajom o kreditnej karte či internet bankingu.

8.1 Sociálne siete

Ak dôjde k prezradeniu prihlasovacích údajov k určitej sociálnej sieti, streamovacej službe či iným podobným stránkam, tak ako prvé je nutné okamžite zmeniť toto prístupové heslo. No nie na heslo podobné tomu odhalenému, ktoré by sa líšilo len v dvoch či troch znakoch, ale na úplne nové a predovšetkým bezpečné heslo. Ako ďalšie je nutné identický krok vykonať aj na emailovom účte, ktorý je nejakým spôsobom prepojený s daným kontom. Heslo by sa v tomto prípade nemalo zhodovať s prístupovým heslom k účtu v danej sociálnej sieti, no opäť by malo byť bezpečné. V prípade, ak odhalené alebo veľmi podobné heslo užívateľ používa aj na iných stránkach, tak aj tieto hesla by mal v čo najkratšom čase zmeniť na nové.

Vzhľadom na to, že počas návštevy takejto podvodnej stránky nemuselo dôjsť len k ukradnutiu údajov pomocou formulára, ktorý užívateľ vyplnil, ale taktiež mohlo dôjsť aj k stiahnutiu nebezpečného malwaru. Takže v druhej fáze bezpečnostných opatrení nasleduje kontrola počítača pomocou bezpečnostného softwaru. Boh užiaľ v prípade, že aktuálne používaný antivírus pri návšteve podvodnej stránky neupozornil užívateľa na nebezpečný obsah a nezablokoval spojenie, tak je veľká pravdepodobnosť, že nedokáže ani odhaliť potencionálny malware z tejto stránky. No to už je tak trochu aj o dôvere užívateľa k danému bezpečnostnému softwaru. Každopádne takáto plošná kontrola je nutná za každých okolností. Autorovi práce sa osvedčil aj software Malwarebytes, ktorý dokáže odhaliť v niektorých prípadoch viac než iný antivírusový program.

Ak po dokončení tejto kontroly antivírus upozornil užívateľa na podozrivé súbory, tak je nutné analyzovať či sa skutočne jedná o nebezpečný obsah alebo len planý poplach. Pre neskúseného užívateľa je asi najjednoduchšia voľba to hodiť do tzv. karantény. Samozrejme

následne by užívateľ mal opäť zmeniť všetky prístupové heslá, pretože mohlo dôjsť k ich odhaleniu aj pri prvej zmene. V prípade, ak antivírus neodhalil žiadne nebezpečné súbory, tak ostáva už len dúfať, že daný bezpečnostný software je skutočne kvalitný.

8.2 Internet banking

V druhom prípade, ak došlo k prezradeniu údajov o kreditnej karte, prípadne prístupu k internet bankingu, tak užívateľ musí najlepšie telefonicky čím skôr na tento fakt upozorniť svoju banku. Zamestnanci banky sa už následne postarajú o okamžité zablokovanie kreditnej karty alebo prístupu k internet bankingu. Následne je vhodné taktiež upozorniť danú inštitúciu, že došlo k takémuto útoku a čo najpresnejšie popísať ako sa poškodený užívateľ k takejto podvodnej stránke dostal a poskytnúť čo najviac informácií. Vďaka týmto informáciám bude môcť banka spustiť potrebné bezpečnostné opatrenia a upozorniť ostatných svojich zákazníkov, aby boli mimoriadne obozretní a nestali sa ďalšou obeťou útočníka.

Rovnako ako v predchádzajúcom prípade aj tu je potrebná kontrola počítača bezpečnostným softwarom. Takisto aj zmena hesiel ku všetkým rôznym účtom bude vhodným bezpečnostným opatrením pred možným zneužitím.

9 Záver

Útoky pomocou phishingových stránok sú stále viac rozšírené a ako napredujú bezpečnostné technológie, rovnako tak napredujú aj techniky útočníkov. Práve to je dôvod prečo je čoraz obťažnejšie odhaliť stránku s podvodným obsahom. Aj napriek tomu, že s takouto stránkou sa pravdepodobne stretol každý užívateľ internetu, tak len máloktorý dokáže definovať pojem phishing.

Cieľom tejto bakalárskej práce je oboznámiť čitateľa s problematikou phishingu, jeho rôznych foriem a ako sa proti takejto hrozbe čo najefektívnejšie brániť len s obyčajným prehliadačom.

Na začiatku práce sú popísané rôzne typy phishingových útokov, trestnoprávny postih za takéto konanie a taktiež aj profily najčastejších útočníkov. V ďalšej kapitole sú popísané začiatky phishingu, ale aj súčasné štatistiky takýchto útokov. Následne je čitateľ oboznámený s priebehom útoku od jeho počiatočnej prípravy cez vytvorenie phishingovej stránky až po možný profit z útoku. V závere teoretickej časti sa nachádza aj niekoľko reálnych príkladov phishingu.

V praktickej časti boli otestované prehliadače na vybranej vzorke phishingových stránok a podľa predom daných kritérií. Na základe výsledkov boli vyhodnotené prehliadače, ktorý z nich dokáže najspoľahlivejšie odhaliť phishingovú stránku. Z tohto testu vyšiel najlepšie prehliadač Opera a najhoršie Safari. Taktiež sú v poslednej časti práce popísané aj odporúčania ako sa zachovať v prípade, ak sa užívateľ stal obeťou phishingového útoku.

Po prečítaní tejto práce by čitateľ mal poznať čo to je phishing, jeho rôzne formy, možné profily útočníkov, priebeh takéhoto útoku, históriu a súčasné štatistiky, ako sa správne zachovať v prípade, že sa stane obeťou a vybrať si najvhodnejší internetový prehliadač, ktorý je nie len z hľadiska bezpečnosti najlepší, ale aj v kombinácii s príjemným užívateľským prostredím, výkonom a ďalšími možnými doplnkami.

Túto prácu by bolo možné ešte rozšíriť o test prehliadačov spolu s rôznymi doplnkami, ktoré by mali ešte viac zvýšiť ochranu pred podvodnými stránkami.

10 Zoznam použitej literatúry

[1] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[2] JIROVSKÝ, Václav. *Kybernetická kriminalita*. 1. Praha: Grada Publishing, a.s., 2007. ISBN 978-80-247-1561-2.

[3] JAMES, Lance. *Phishing bez záhad. [Phishing Exposed].* 1. Praha: Grada Publishing, a.s., 2007. ISBN 978-80-247-1766-1.

[4] SYMANTEC. *What Is Smishing?* [online]. [cit. 05.01.2018]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

[5] FBI. *Phishing/Spoofing* [online]. [cit. 05.01.2018]. Dostupné z: https://www.ic3.gov/crimeschemes.aspx#item-14

[6] ERBEN, Lukáš. *Příchod hackerů: rhybáři na AOL* [online]. 2014. [cit. 05.01.2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-rhybari-na-aol/

[7] ANTIMALWARE. Co je phishing [online]. [cit. 06.01.2018]. Dostupné z: https://www.antimalware.cz/blog/co-je-phishing

[8] PHISHING. *History of Phishing* [online]. [cit. 06.01.2018]. Dostupné z: http://www.phishing.org/history-of-phishing

[9] COFENSE. *History of phishing* [online]. [cit. 08.01.2018]. Dostupné z: https://cofense.com/history-of-phishing/

[10] HACKINGLOOPS. *How to Create a Facebook Phishing Page* [online]. [cit. 10.01.2018]. Dostupné z: https://www.hackingloops.com/how-to-create-a-facebook-phishing-page/

[11] UCEDAVELEZ, Tony. Phishing for Banks [online]. 2004. [cit. 10.01.2018]. Dostupné z: https://www.giac.org/paper/gsec/4323/phishing-banks-timely-analysis-identity-theft-fraud-financial-sector/107044

[12] RADER, Marc a Syed M. RAHMAN. *Exploring Historical And Emerging Phishing Techniques and Mitigating the Associated Security Risks* [online]. 2013. [cit. 10.01.2018]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1512/1512.00082.pdf

[13] ELSNEROVÁ, Ludmila. *Phishingový útok jménem GE Money* [online]. 2015. [cit. 10.01.2018]. Dostupné z: http://www.elsnerova.cz/blog/2015-07/phishingovy-utok-jmenem-ge-money.html

[14] AVAST. *Malware* [online]. [cit. 10.01.2018]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[15] LININGER, Rachel a Russell Dean VINES. *Phishing: Cutting the Identity Theft Line*. 1. Indianapolis: Wiley Publishing, Inc., 2005. ISBN 978-07645-8498-5.

[16] HODÁS, Martin. *Phishingové útoky na klientov slovenských bánk: Ako sa chrániť?* [online]. 2015. [cit. 10.01.2018]. Dostupné z: https://www.zive.sk/clanok/105906/phishingove-utoky-na-klientov-slovenskych-bank-ako-sa-chranit/

[17] HODÁS, Martin. *Univerzita naletela na phishing, podvodníkom poslala 8 mil. eur* [online]. 2017. [cit. 25.01.2018]. Dostupné z: https://www.zive.sk/clanok/127374/univerzita-naletela-na-phishing-podvodnikom-poslala-8-mil-eur/

[18] KOLIBA, Ján. *Pozor na sofistikovaný phishing. Útočníci kradnú virtuálnu menu Ethereum* [online]. 2017. [cit. 25.01.2018]. Dostupné z: https://www.zive.sk/clanok/128430/pozor-na-sofistikovany-phishing-utocnici-kradnu-virtualnu-menu-ethereum/

[19] ČÍŽEK, Jakub. *Nová forma phishingu: Keď Apple.com nie je Apple.com* [online]. 2017. [cit. 25.01.2018]. Dostupné z: https://www.zive.sk/clanok/124481/nie-je-apple-com-ako-apple-com-specialista-ukazal-ake-problemy-moze-sposobit-idn-phishing/

[20] KRČMÁŘ, Petr. *Phishingový útok výměnou IDN znaků v doméně znovu na scéně* [online]. 2017. [cit. 25.01.2018]. Dostupné z: https://www.root.cz/clanky/phishingovy-utok-vymenou-idn-znaku-v-domene-znovu-na-scene/

[21] ZHENG, Xudong. *Phishing with Unicode Domains* [online]. 2017. [cit. 25.01.2018]. Dostupné z: https://www.xudongz.com/blog/2017/idn-phishing/

[22] CSIRT. *Phishing s unicode doménami* [online]. 2017. [cit. 10.02.2018]. Dostupné z: https://www.csirt.cz/page/3527/phishing-s-unicode-domenami/

[23] AARON, Greg. *Phishing Activity Trends Report: 1st Quarter 2016* [online]. 2016. [cit. 15.03.2018]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[24] AARON, Greg. *Phishing Activity Trends Report: 2nd Quarter 2016* [online]. 2016. [cit. 15.03.2018]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

[25] AARON, Greg. *Phishing Activity Trends Report: 3rd Quarter 2016* [online]. 2016. [cit. 15.03.2018]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf

[26] AARON, Greg. *Phishing Activity Trends Report: 4th Quarter 2016* [online]. 2017. [cit. 15.03.2018]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

[27] AARON, Greg. *Phishing Activity Trends Report: 1st Half 2017* [online]. 2017. [cit. 15.03.2018]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf

[28] AARON, Greg. *Phishing Activity Trends Report: 3rd Quarter 2017* [online]. 2018. [cit. 15.03.2018]. Dostupné z: http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf

[29] [18.03.2018]. Dostupné z: https://www.phishtank.com/

[30] WIKIPEDIA. *Google Chrome* [online]. Posl. úpravy 18.03.2018. [cit. 20.03.2018]. Dostupné z: https://en.wikipedia.org/wiki/Google_Chrome

[31] WIKIPEDIA. *Firefox* [online]. Posl. úpravy 15.03.2018. [cit. 20.03.2018]. Dostupné z: https://en.wikipedia.org/wiki/Firefox

[32] WIKIPEDIA. *Opera (web browser)* [online]. Posl. úpravy 16.03.2018. [cit. 20.03.2018]. Dostupné z: https://en.wikipedia.org/wiki/Opera_(web_browser)

[33] WIKIPEDIA. *Internet Explorer* [online]. Posl. úpravy 15.03.2018. [cit. 20.03.2018]. Dostupné z: https://en.wikipedia.org/wiki/Internet_Explorer

[34] WIKIPEDIA. *Safari (web browser)* [online]. Posl. úpravy 29.02.2018. [cit. 20.03.2018]. Dostupné z: https://en.wikipedia.org/wiki/Safari_(web_browser)

[35] MOZILLA. *How does built-in Phishing and Malware Protection work?* [online]. [cit. 25.03.2018]. Dostupné z: https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work

[36] GOOGLE. *Bezpečné prehliadanie: malvér a phishing* [online]. [cit. 25.03.2018]. Dostupné z: https://transparencyreport.google.com/safe-browsing/overview?unsafe=dataset:0;series:malware,phishing;end:1519545600000;start:1148194800000&lu=unsafe

11 Zoznam obrázkov

12 Zoznam tabuliek

13 Zoznam grafov