

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky



Diplomová práce

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Phishing a lidský faktor

Vypracovala: Bc. Diana Kalinová

Vedúci práce: Mgr. Ing. Tomáš Sigmund, Ph.D.

Rok vypracovania: 2014

Čestné vyhlásenie:

Vyhlasujem, že som diplomovú prácu napísala samostatne. Všetky zdroje, ktoré som pri písaní práce použila sú uvedené v zozname zdrojov a v súlade s normou ČSN ISO 690.

V Prahe dňa 30. 11. 2014

Podpis:

Pod'akovanie:

Ďakujem predovšetkým Mgr. Ing. Tomášovi Sigmundovi, Ph.D., vedúcemu mojej diplomovej práce, za podnety, pripomienky, cenné rady a usmerňovanie pri písaní práce. Ďalej by som sa chcela poďakovať za podporu a pomoc Alexandrovi Molnárovi, Márii Slovákovej a mojej rodine.

Abstrakt

Hlavným cieľom diplomovej práce je vyzdvihnúť dôležitosť ľudského faktora pre úspešnosť phishingových útokov a zistiť dôvody, prečo sú českí a slovenskí používatelia náchylní na phishing. Práca sa zameriava na používateľa ako na najslabší článok systému, ktorý phisher zneužívajú. Prvá kapitola je venovaná phishingu a jeho zločkám. Popisuje phisherom ich ciele a dôvody ich konania. Sociálne a technické triky, ktoré slúžia k podvádzaniu používateľov sa nachádzajú v druhej kapitole. Tretia kapitola sa zameriava na sociálne inžinierstvo a metódy sociologického útoku. Štvrtá kapitola sa venuje spôsobom doručenia phishingu používateľovi a piata rôznym typom phishingových útokov. V šiestej kapitole sú uvedené dôvody fungovania phishingu, aspekty dôveryhodnosti a pravosti e-mailov i webových stránok sledované používateľmi. Nachádzajú sa tu aj dôsledky použitia kontextu vo phishingu. Obete phishingu sa vyznačujú špecifickými reakciami, ktoré sú spomenuté v siedmej kapitole. Ôsma kapitola sa venuje rôznym opatreniam proti phishingu, a nielen technologickým. Spomínaných osem kapitol predstavuje teoretické východisko pre nasledujúce kapitoly diplomovej práce.

V deviatej kapitole je uskutočnená analýza globálnej situácie v oblasti phishingu. Na základe ktorej sú zistené súčasné i historické trendy vo phishingu. Na záver kapitoly sú uvedené dopady na používateľa, ktoré z analýzy vyplývajú. Desiata kapitola sa venuje phishingovým útokom v Českej a Slovenskej republike, zaujímavým z hľadiska dôležitosti ľudského faktora. Analýzou útokov sa zisťuje, či sa používatelia dokážu ubrániť útokom len obozretnosťou, všímavosťou a znalosťami o phishingu. V rámci poslednej kapitoly je uskutočnený empirický výskum prostredníctvom dotazníkového šetrenia. Výskum overuje povedomie o phishingu a osobné skúsenosti českých a slovenských používateľov, bezpečnostné návyky používateľov a aspekty dôveryhodnosti a pravosti, ktoré používatelia posudzujú u e-mailov a webových stránok. Na základe všetkých zistení sú vyvedené závery a odporúčania.

Kľúčové slová: phishing, ľudský faktor, používateľ, phisher

Abstract

The main objective of the diploma thesis is to underline the importance of human factor for the success of phishing attacks and to identify the reasons, why the Czech and Slovak users are vulnerable to phishing. The thesis focuses on the user as the weakest part in the system which phishers exploit. Social and technical tricks that are cheating users are in the second chapter. The third chapter focuses on social engineering and sociological methods of attack. The fourth chapter is devoted to the delivery of phishing and fifth chapter explores the various types of phishing attacks. The sixth chapter presents the reasons for the operation of phishing, the aspects of credibility and authenticity of e-mails and web sites, that users follow and the implications of using the context in phishing. The victims of phishing have specific reactions which are mentioned in the seventh chapter. The eighth chapter explores the various measures against phishing, not just technology. Mentioned eight chapters present a theoretical basis for the following chapters of the diploma thesis.

In the ninth chapter is performed analysis of the global situation of phishing. Through analysis are identified current and historical trends in phishing. Finally, the chapter shows the implications for the user. The tenth chapter is devoted to the phishing attacks in the Czech and Slovak Republic which are interesting in terms of the importance of human factor. We determine whether users are able to defend attacks only with their carefulness, mindfulness and awareness of phishing. Within the last chapter is taken empirical research through the questionnaire survey. The research verifies the awareness of the Czech and Slovak users about phishing, their personal experiences with phishing, their security habits and the aspects of credibility and authenticity that they consider in emails and websites. Based on all findings are drawn conclusions and recommendations.

Keywords: phishing, human factor, user, phisher

Obsah

Úvod	9
1 Phishing.....	12
1.1 Úlohy, ciele a dôvody konania phisherov	13
1.2 Základné zložky phishingu.....	15
2 Typy trikov používané na oklamanie používateľov.....	16
3 Sociálne inžinierstvo	18
3.1 Metódy sociologického útoku	18
4 Spôsoby doručenia phishingu používateľovi	21
4.1 Phishingové e-maily	21
4.2 Phishingové webové stránky	21
4.3 Konferenčné systémy a rýchle správy	22
4.4 Hostitelia trójskych koní	22
5 Typy phishingových útokov.....	23
5.1 Typy útokov v závislosti od počtu zberných miest	26
5.1.1 Distribuovaný phishingový útok	27
6 Dôvody fungovania phishingu	28
6.1 Aspekty dôveryhodnosti e-mailov a webových stránok posudzované používateľmi.....	28
6.2 Stratégie phisherov na oklamanie používateľov	30
6.3 Stratégie používateľov pri posudzovaní pravosti webových stránok	31
6.4 Kontext vo phishingu	33
6.4.1 Sociálny phishing	33
6.4.2 Spear phishing.....	34
7 Reakcie obetí phishingu	35
8 Opatrenia proti phishingu.....	37
8.1 Obranné mechanizmy	37
8.1.1 Opatrenia proti phishingu na strane klienta	37
8.1.2 Opatrenia na strane serveru.....	39
8.1.3 Podniková úroveň	41
8.1.4 Antispamové filtre.....	42
8.2 Bezpečnostné zásady pre používateľov.....	43
8.3 Vzdelávanie používateľov, antiphishingové skupiny a legislatíva	44
8.3.1 Vzdelávanie používateľov.....	44

8.3.2	Antiphishingové skupiny	45
8.3.3	Legislatíva	46
8.3.4	Zhodnotenie.....	46
9	Analýza globálnej situácie v oblasti phishingu.....	48
9.1	Phishingové gangy	48
9.2	Čínski phisher.....	49
9.3	Počet phishingových útokov	49
9.4	Ciele phishingových útokov	51
9.5	Názov značky v doménovom mene.....	52
9.6	Doba životnosti phishingových útokov	52
9.7	Používanie doménových mien k phishingu	53
9.8	Subdoménové služby.....	54
9.9	Skrátené URL adresy.....	55
9.10	Útoky na zdieľané virtuálne servery	55
9.11	IP adresy používané k phishingu.....	56
9.12	Internacionalizované doménové mená v phishingu	56
9.13	Spear phishing	57
9.14	Zhrnutie situácie a dopady na používateľov.....	57
9.15	Domény .SK, .CZ a .EU vo phishingu	58
10	Zaujímavé phishingové útoky z hľadiska dôležitosti ľudského faktora	62
10.1	E-mail od Daňového úradu SR.....	62
10.2	Phishing prostredníctvom sociálnej siete	64
10.3	Phishingový e-mail upozorňujúci na dlh.....	65
10.4	Veľká phishingová kampaň.....	66
10.5	Zhodnotenie prípadov	67
11	Výskum	69
11.1	Metodika výskumu	69
11.2	Dotazník a priebeh šetrenia	69
11.3	Súbor respondentov	71
11.4	Výskumné hypotézy	74
11.5	Reflexia možných skreslení.....	75
11.6	Spracovanie a interpretácia dát.....	75
11.7	Konfrontácia výsledkov	94

11.7.1	Hypotéza 1	94
11.7.2	Hypotéza 2	95
11.7.3	Hypoteza 3	96
11.7.4	Hypotéza 4	97
Záver		99
Zoznam skratiek		105
Zoznam obrázkov		106
Zoznam grafov		107
Zoznam tabuliek		109
Zoznam zdrojov		110
Zoznam príloh		115

Úvod

Témou tejto diplomovej práce je phishing a ľudský faktor. V rámci práce skúmame dôležitosť ľudského faktora, v podobe používateľa, pre úspešnosť phishingu a dôvody náchylnosti českých a slovenských používateľov na phishing. Často sa totiž zabúda, že phishing sa sústreďuje nielen na zneužívanie technických zraniteľností, ale najmä na človeka ako najslabší článok bezpečnostného systému. Práca sa snaží poukázať na fakt, že používateľ, ktorý sa stane obeťou phishingu, sám dopomôže k úspešnosti útoku svojím správaním, neopatrnosťou, nevšímavosťou a nevedomosťou. Spomínaný fakt sa snažíme dokázať aj v ČR a SR. Výber témy je prejavom záujmu o oblasť počítačovej kriminality. Diplomová práca voľne nadväzuje na bakalársku prácu, ktorá sa týkala počítačovej kriminality na Slovensku. Práve jedným z piatich druhov kriminality, ktorými sa zaoberala bol phishing. K výberu témy prispelo i množstvo novinových článkov a reportáží o phishingu za posledný rok a zamýšľanie sa nad prípadmi, ktoré sa v SR a ČR vyskytli.

Hlavným cieľom diplomovej práce je vyzdvihnúť dôležitosť ľudského faktora pre úspešnosť phishingových útokov a zistiť dôvody, prečo sú českí a slovenskí používatelia náchylní na phishing. Hlavný cieľ sa pokúsime naplniť prostredníctvom štyroch čiastkových cieľov. **Prvým čiastkovým cieľom** práce je zistiť zložky phishingu a používané triky, preskúmať typy phishingových útokov, zistiť prečo phishingu funguje a aké aspekty používateľa sledujú, aký je dopad zavedenia kontextu do phishingu a aké opatrenia proti phishingu sú k dispozícii. **Druhým cieľom** je prevedenie analýzy situácie v oblasti phishingu a zistenie možných dopadov na používateľa. **Tretí cieľ** je zameraný na zistenie dôležitosti povedomia o phishingu, opatrnosti a všímavosti používateľov pri odhaľovaní phishingu v rámci ČR a SR. Dokážu vďaka nim používatelia odhaliť útok? **Štvrtým cieľom** je uskutočnenie výskumu, ktorý má zistiť úroveň povedomia o phishingu u českých a slovenských používateľov, ich osobné skúsenosti, bezpečnostné návyky a aspekty, ktoré berú do úvahy pri posudzovaní pravosti e-mailov a web stránok.

Posledné tri z vyššie uvedených cieľov sme vyjadrili prostredníctvom nasledovných otázok, ktoré zodpovieme v závere práce:

- Aká je súčasná situácia v oblasti phishingu a akým spôsobom vplýva na bežného používateľa?
- Aké dôležité sú opatrnosť, všímavosť a základné znalosti o phishingu u českých a slovenských používateľov pri odhaľovaní phishingových útokov v rámci ČR a SR? Dokážu opatrní a všímaví používatelia útok odhaliť?
- Aké je povedomie o phishingu u českých a slovenských používateľov? Majú osobné skúsenosti s phishingom?
- Odlišuje sa vnímanie reálnosti hrozby phishingu v závislosti od pobytu v Českej a Slovenskej republike?
- Majú slovenskí a českí používatelia nejaké bezpečnostné návyky, ktoré im môžu pomôcť vyhnúť sa phishingu?
- Ktoré aspekty dôveryhodnosti a pravosti českí a slovenskí používatelia berú v úvahu pri e-mailoch a webových stránkach?

Zo stanovených cieľov a otázok zistíme, na čo by si používatelia mali dávať väčší pozor, aby sa nestali obeťou phishingu, a na ktoré slabé stránky používateľov by sme mali pôsobiť prostredníctvom vzdelávania alebo vytvárania opatrení proti phishingu.

Štruktúru práce tvorí jedenásť kapitol. Na začiatku je vysvetlený pojem sociálne inžinierstvo a popísaný sociotechnický cyklus, pretože sociálne inžinierstvo je používané pri zavádzaní používateľov. Druhá kapitola obsahuje definíciu phishingu a zložky, z ktorých pozostávajú najbežnejšie phishingové útoky. Následne sa práca zameriava na typy trikov používané na oklamanie používateľov. Phishing je používateľom doručovaný rôznymi spôsobmi, ktoré sú uvedené v štvrtej kapitole. Jedeným z najčastejšie využívaných je e-mail. Piata kapitola popisuje niekoľko členení typov phishingových útokov. Aby sme mohli proti phishingu bojovať, musíme spoznať typy útokov, inak nemôžeme zaviesť správne protiopatrenia. Významné sú i zistenia, prečo vôbec phishing funguje a aké stratégie phisherov vytvorili na klamanie používateľov, aspekty pravosti a dôveryhodnosti webových stránok a e-mailov ako aj vplyv zneužitia kontextu na úspešnosť phishingu. Sú popísané v šiestej kapitole. S reakciami obetí phishingu sa môžeme oboznámiť v siedmej kapitole. Celá ôsma kapitola popisuje opatrenia proti phishingu na rôznych úrovniach a zaoberá sa výberom

vhodných, nielen technologických opatrení. Témou deviatej kapitoly je analýza súčasnej globálnej situácie v oblasti phishingu a posúdenie dopadov na používateľa. Do desiatej kapitoly boli vybrané a popísané štyri útoky zaujímavé z hľadiska ľudského faktoru. Posledná kapitola popisuje výskum zameraný na používateľov z Českej a Slovenskej republiky. Na základe analýzy súčasnej globálnej situácie vo phishingu, analýzy prípadov útokov a výsledkov šetrenia sú následne vyvodené závery a odporúčania pre používateľov.

1 Phishing

Pojem phishing sa prvýkrát objavil v Spojených štátoch amerických v roku 1995 (James, 2007), kedy došlo ku krádeži údajov o platobných kartách a používateľských účtoch viacerých klientov *America online (AOL)*. Útočníci sa vydávali za administrátora AOL, ktorý požadoval obnovenie údajov. Phishing vznikol ako reakcia na opatrenia AOL. Organizácia chcela zamedziť vytváraniu falošných účtov, a tak zaviedla overovanie čísla platobnej karty pri registrácii nového účtu. Hackeri už nemohli vytvárať falošné účty a tak sa snažili zneužiť existujúce (Jakobsson a Myers, 2006). Neskôr sa tento pojem rozšíril a dodnes zahŕňa krádež akéhokoľvek používateľského účtu, osobných či finančných údajov používateľa (James, 2007).

Phishing môžeme nazvať aj brand spoofing (James, 2007), čiže falšovanie názvu firmy. Útočníci využívajú sociálne inžinierstvo a stelesňujú dôveryhodný zdroj – napr. helpdesk banky alebo podporu obľúbeného internetového obchodu. K dôveryhodnosti útokov prispieva aj používanie firemnej grafiky (Ollmann, 2004). Oklamáný používateľ sám pomôže útočníkovi svojou neopatrnosťou.

Pojem phishing vychádza z techniky, akou sú získavané údaje (James, 2007), pretože sa podobá rybárčeniu (v anglickom jazyku fishing). Útočník nahadzuje háčiky v podobe podvodných e-mailov a webových stránok a čaká, kým sa obeť chytia na jeho návnadu. Ph na začiatku slova značí sofistikovanosť celého tohoto procesu (James, 2007) alebo je prejavom hackerského dialektu, v ktorom sa namiesto F používa Ph (Jakobsson a Myers, 2006).

Phishing je zväzkom sociálneho inžinierstva a technológie (Jakobsson a Young, 2005). Predstavuje komplexnú sadu nástrojov a je technologickým prejavom ľudskej túžby klamať. Útočník sa snaží podvodným konaním získať prístup k prostriedkom používateľa prostredníctvom odcudzenia dôverných informácií a citlivých poverení v napodobnenej elektronickej komunikácii (Jakobsson a Myers, 2006).

Ekonomika phishingu je zaujímavá. Náklady phisherov na útoky sú veľmi nízke v porovnaní so vzniknutými výnosmi, preto sú ochotní sa phishingu dopúšťať. Pre spoločnosť je však phishing veľmi nákladný. **Priame náklady**, ktoré sú cenou za odcudzené tovary a služby, rátajú dotknuté organizácie na milióny dolárov ročne (Jakobsson a Myers, 2006). **Nepriame náklady** sa spájajú so servisom a pomocou

zákazníkom a používateľom pri vyrovnaní sa s phishingom. Predstavujú stovky tisíc dolárov ročne (Jakobsson a Myers, 2006). V neposlednom rade vznikajú i **náklady obetovaných príležitostí**, pretože zákazníci prestávajú veriť a nakupovať produkty a služby dotknutých spoločností. Páchateľov je ťažké odhaliť. Dôkazy veľmi rýchlo miznú. Phishing spôsobuje obrovské škody ale jeho dôsledky sú ťažko vymáhateľné (James, 2007). Môže byť páchaný z ktorejkoľvek krajiny.

Phishing prešiel od svojho vzniku obrovským prerodom. Jednoduché e-maily, ktoré na začiatku získavali údaje používateľov len prostredníctvom odpovede, sú dnes nahradené prepracovanými útokmi, so správnou gramatikou, bezchybným vzhľadom a presvedčivým obsahom. Spôsoby doručenia sa postupne menia a phisher sa snažia dostať čoraz bližšie k svojim potenciálnym obetiam. Neštítia sa vydávať za najbližšiu osobu, len aby dosiahli svoj zisk. V súčasnosti sa stáva phishing čoraz organizovanejším, inteligentnejším, zložitejším a prepracovanejším z hľadiska psychologického i technologického, pretože prebieha neustále súperenie medzi útočníkmi, kriminalistami a organizáciami vytvárajúcimi protiopatrenia (Jakobsson a Young, 2005). Všetci sa snažia byť o krok napred. Útoky sa prispôbujú novým technickým i sociálnym situáciám (Jakobsson a Myers, 2006). Staré typy útokov sú nahradzované novými a mení sa celé prostredie. Phishing sa však stane ešte horším, agresívnejším a opatrnejším. Začne zneužívať všetky dostupné informácie, ktoré používatelia zverejnia.

Phishing je tak nebezpečný, organizovaný a prepracovaný i z dôvodu, že ho vo väčšine prípadov uskutočňuje dobre zorganizovaná skupina osôb. Úlohy jednotlivých členov v rámci skupiny, ako aj ciele a dôvody vykonávania phishingu sú bližšie popísané v nasledujúcej kapitole.

1.1 Úlohy, ciele a dôvody konania phisherov

Phisher sú taktiež predstaviteľmi ľudského faktora vo phishingu, avšak ľudského faktora, ktorý phishing zapríčiňuje a spôsobuje škody. Dôležitosť phisherov spočíva v originalite, prepracovanosti, škodlivosti a účinnosti nimi vytvorených útokov. Čím je phisher lepší, tým sú jeho útoky nebezpečnejšie a zapríčia väčšie škody.

Phisherov môžeme rozdeliť vzhľadom na prepracovanosť útokov, ktoré prevádzajú. Amatéri nevytvárajú vlastné scenáre útokov, ale útoky uskutočňujú iba

prostredníctvom zakúpených phishingových sád, ktoré obsahujú vopred vytvorené šablóny útokov zamerané na veľké ciele. Zatiaľ čo profesionáli sú veľmi skúsení, inteligentní, konajú racionálne, vytvárajú originálne a prepracované phishingové útoky.

Phishing vo väčšine prípadov nevykonáva jedna osoba, ale skupina osôb, ktoré sa snažia optimalizovať útoky. Útočníci hrajú tri dôležité úlohy (Jakobsson a Myers, 2006). **Odosielateľ** distribuuje veľké množstvo podvodných e-mailov, najčastejšie pomocou botnetov (siete infikovaných domácich počítačov). **Zberateľ** zabezpečuje zber informácií, či už prostredníctvom webových stránok, e-mailov alebo formulárov. Často je klientom odosielateľa. **Pokladník** zaplatí zberateľovi za získané informácie v závislosti od ich kvality a speňaží ich. Buď prostredníctvom použitia informácií, výmenou informácií s inými útočníkmi alebo predajom na čiernom trhu.

Hlavným cieľom phisherov je oklamať používateľa a získať jeho dôverné informácie alebo citlivé poverenia (Jakobsson a Myers, 2006). Zároveň však chcú docieľať maximalizáciu zisku z phishingových útokov, minimalizáciu nákladov na útoky a obmedzenie rizika, že budú odhalení.

Phisherí potrebujú získať informácie a poverenia používateľov z troch **dôvodov** (Jakobsson a Young, 2005):

- aby používateľom ukradli finančné prostriedky,
- aby prostredníctvom získaných dôverných informácií a citlivých poverení mohli páchať ďalšie trestné činy (napr. krádeže identity),
- a aby zakryli skutočný finančný tok svojej zločineckej skupiny.

Ďalším dôvodom môže byť získanie finančných prostriedkov predajom prihlasovacích údajov na čiernom trhu.

Sú stimulovaní útoky uskutočňovať najmä kvôli získaným finančným prostriedkom. Podľa Lance Jamesa (2007) je phishing ľahkým spôsobom, ako môže útočník nadobudnúť peniaze. Výnosy z phishingu sú vysoké, zatiaľ čo náklady na phishingové útoky sú nízke. Spoznať ďalšie motívy phisherov je veľmi zložitá, pretože ich poznajú iba samotní phisherí, prípadne osoby, ktoré preniknú do phishingovej skupiny.

Či už phishing uskutočňuje amatér alebo profesionál, jednotlivec alebo organizované skupiny, prevažná väčšina útokov sa skladá z určitých základných zložiek, ktoré by v úspešnom útoku mali byť obsiahnuté.

1.2 Základné zložky phishingu

Najbežnejšie phishingové útoky pozostávajú z troch základných zložiek (Jakobsson a Mayers, 2007), pomocou ktorých je útok uskutočnený:

1. **Návnada** je správa s presvedčivým príbehom, ktorá nabáda používateľa k nasledovaniu URL (Uniform Resource Locator - jednotná adresa zdroja) odkazu a následnému odovzdaniu informácií na podvodných webových stránkach. Poskytuje používateľovi presvedčivý argument pre vyplnenie informácií.
2. **Háčik** predstavuje podvodné webové stránky vizuálne nerozoznatelné od legitímnych stránok zvolenej organizácie. Presviedča používateľa o legitímnosti útoku, podporuje ho v konaní a snaží sa nevzbudiť ani najmenšie podozrenie. Účelom stránok je zachytiť poverenia a údaje používateľa.
3. **Úlovok** reprezentuje využitie získaných informácií k nelegálnemu účelu napr. pre krádež identity, či podvod.

Z hľadiska dôležitosti ľudského faktora a zároveň úspešnosti útoku sú najdôležitejšími zložkami phishingu návnada a háčik, pretože presviedčajú používateľa a získavajú si jeho dôveru. Vďaka návnadám a háčikom dokážu phisherí používateľa podviesť. Do značnej miery však úspešnosť útoku závisí aj na používateľovi, jeho správaní, vedomostiach a všímavosti. Čím kvalitnejšie návnady a háčiky útočníci pripraví, tým väčšiu škodu spôsobia. Z pohľadu phishera má najväčšiu cenu úlovok, ktorý je výsledkom úspešne uskutočneného útoku.

Pre úspešnosť útoku sú dôležité nielen spomínané zložky phishingu. Phisherí musia pripraviť vhodnú kombináciu dvoch typov trikov, ktoré sa navzájom dopĺňajú tak, aby používateľov presvedčili, ale zároveň nevzbudili pozornosť.

2 Typy trikov používané na oklamanie používateľov

Phishing nezneužíva len technické zraniteľnosti ale najmä zraniteľnosť a omylnosť bežného používateľa. Útočníci sa snažia pôsobiť najmä na človeka, pretože predstavuje najslabší článok systému (Mitnick a Simon, 2003). V niektorých prípadoch je jednoduchšie zneužiť používateľa, než prekonať technologické opatrenia, ktoré sú čoraz lepšie a dôkladnejšie. Práve k prekonaniu a oklamaniu používateľa slúžia sociálne i technické typy trikov. Aby phishing pôsobil na používateľov legitímne a zároveň lákavo, musí obsahovať oba typy trikov (Jakobsson a Myers, 2006):

1. Sociálne triky majú podobu príbehu, scenára a metódy na presvedčenie používateľa. Je ich neobmedzené množstvo a zabezpečia dôveryhodnosť kontextu. Poskytujú potenciálnej obeti vierohodný stimul pre uskutočnenie akcií požadovaných útočníkom. Medzi najčastejšie sociálne triky (Jakobsson a Myers, 2006) patria:

- a. bezpečnostná aktualizácia – výzva k aktivácii novej bezpečnostnej služby prostredníctvom prihlásenia do účtu a zadania údajov,
- b. neúplné informácie o účte – žiadosť o prihlásenie a aktualizáciu uvedených údajov pre zachovanie služby,
- c. finančné stimuly – poskytnutie zľavy, kupónu, výhry alebo hotovosti po prihlásení k účtu,
- d. a falošná obnova účtu – žiadosť o aktualizáciu informácií o účte.

Scenáre musia byť prispôbené kontextu, ktorý potenciálna obeť očakáva. Jedným z najlepších spôsobov obrany a odhalenia útoku je zlý kontext. Napr. používateľ nie je klientom banky, za ktorú sa útočník vydáva.

2. Technické triky (Jakobsson a Myers, 2006) pomáhajú vytvoriť umelý sociálny kontext. Najbežnejšími sú:

- a. použitie prvkov chránených ochrannou známkou – začlenenie loga, obrázkov a iných prvkov, ktoré umocňujú pocit bezpečia a autenticitu,
- b. spoofing e-mailu – identita odosielateľa je útočníkom zmenená na dôveryhodnú inštitúciu,
- c. zamaskovanie, zakódovanie a prispôbenie URL – odkaz musí zdanlivo súvisieť s cieľovou inštitúciou a zároveň odkazovať na útočníkov server, preto ho útočník zamaskuje, zakóduje alebo prispôsobí,

- d. a botnety – siete pozostávajúce z napadnutých počítačov, ktoré slúžia na rozosielanie veľkého množstva e-mailov, hostovanie podvodných stránok a ďalšie nelegálne činnosti.

Zatiaľ čo sociálne triky uvádzajú používateľov do kontextu a poskytujú im prvotný dôvod k dôvere v nelegitímny obsah, technické triky vizuálne podporujú manipuláciu ľudského faktora a pomáhajú útok uskutočniť.

Používanie sociálnych trikov v rámci phishingu predstavuje aplikáciu praktík sociálneho inžinierstva. Zo spomínaného dôvodu je dôležité vysvetliť bližšie pojem sociálne inžinierstvo a taktiež metódy sociotechnického útoku.

3 Sociálne inžinierstvo

Sociálne inžinierstvo je súčasťou phishingu, pretože phishing je kombináciou technického podvodu a sociotechnických praktík (Ollmann, 2004). Dokonca, môžeme phishing považovať za formu sociálneho inžinierstva (Jagatic a kol., 2005). Počas celej histórie ľudstva zneužíva sociálne inžinierstvo ľudskú hlúposť a slabiny ľudského vnímania (Jirovský, 2007). Prostredníctvom jeho aplikácie sa snaží útočník potenciálnu obeť presvedčiť k vykonaniu súboru akcií a získať tak prístup k dôverným informáciám.

Pojem sociálne inžinierstvo alebo sociotechnika môžeme definovať aj ako ovplyvňovanie a presvedčanie ľudí s cieľom oklamať ich, že sociotechnik je osobou s predstieranou totožnosťou. Vďaka manipulácii dokáže využiť ľudí, s ktorými komunikuje a nadobudnúť potrebné informácie. Existuje základný rozdiel (Mitnick a Simon, 2003) medzi sociotechnikom a podvodníkom. Osoba, ktorá sa snaží získať informácie, kvôli svojej zvedavosti a túžbe po poznaní technológií, je sociotechnikom, zatiaľ čo osoba získavajúca spomínaným spôsobom peniaze je podvodníkom. Sociotechnik zväčša oplýva sklonmi k manipulácii a schopnosťou presvedčať ľudí (Mitnick a Simon, 2003). Pôsobí na človeka veľmi príjemne a dokáže si získavať porozumenie a dôveru, tak aby nevzbudil podozrenie. Ne je vtieravý a nevytvára na používateľa nátlak. Naopak vystupuje priateľsky a obeť nadobúda pocit, že všetko robí z vlastnej vôle (Jirovský, 2007). Pre dobrého sociotechnika je iba otázkou času, úsilia, osobnosti a trpezlivosti (Mitnick a Simon, 2003), kedy potrebnú informáciu získa. Sociotechnici zväčša začínajú útok obstaraním zdanlivo bezvýznamnej informácie (Mitnick a Simon, 2003), preto nevzbudzujú pozornosť. Získané informácie ale môžu byť významné pri predstieraní identity a skladaní celku z jednotlivých informácií. Kladú bežné otázky a pritom začlenia aj otázky na informácie, ktoré potrebujú zistiť. Náhľad na postup sociotechnika pri získavaní informácií nám poskytuje sociotechnický cyklus, ktorý je vysvetlený v nasledujúcej kapitole o metódach sociologického útoku.

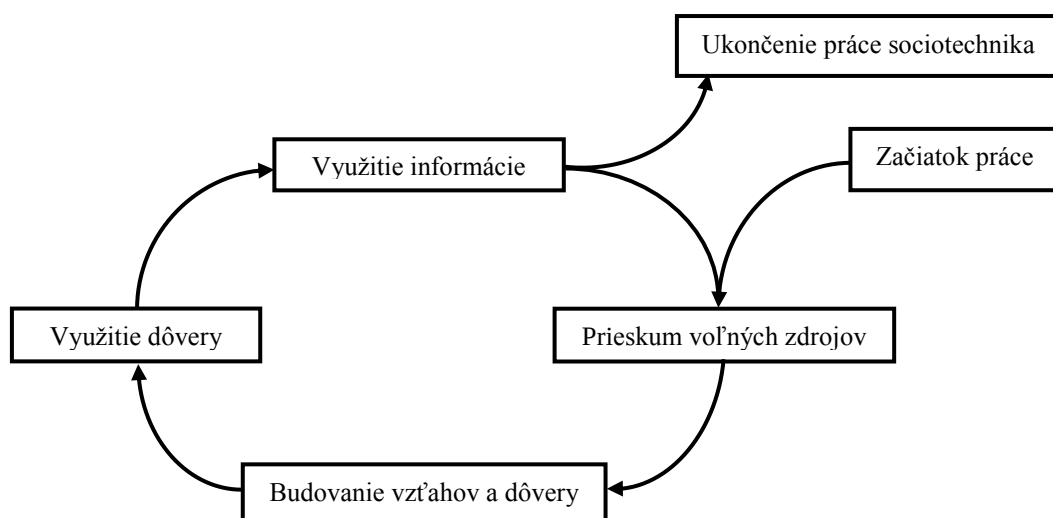
3.1 Metódy sociologického útoku

Základom sociotechnických metód sú podvedomé zvyky a vlastnosti jedinca, schopnosť manipulácie a tvorby pripravených situácií. Zneužívajú slabé miesta

bezpečnostnej politiky firmy. Jednou z metód sociologického útoku je krádež informácií. (Jirovský, 2007)

Na obrázku 1.1 je zobrazený cyklus (Jirovský, 2007), v rámci ktorého sociotechnik začína prácu prieskumom voľných a dostupných zdrojov, ktoré obsahujú zdanlivo neužitočné a neškodné informácie. Voľné zdroje informácií (Jirovský, 2007) predstavujú všetky informácie dostupné verejnosti zákonným spôsobom. Sú nimi webové stránky firmy, reklamné brožúry a mnohé iné tlačené alebo elektronické materiály. V ďalších prípadoch obstarávajú sociotechnici informácie i vytvorením podvodných stránok, e-mailov a problémových situácií, ktoré pomáhajú riešiť. Následne si útočník vytipuje osoby, s ktorými si vytvára vzťah a získava si ich dôveru. Zameriava sa predovšetkým na ľudí neuvedomujúcich si dôležitosť informácií. Vždy je pripravený na určitý odpor, podozrievavosť a snaží sa predvídať reakcie osôb.

Budovanie vzťahu a dôvery je veľmi časovo náročnou činnosťou, ak obeť nemá mať ani najmenší dôvod k podozreniu. Úspešným prevedením získava útočník možnosť ťaženia informácie z obeť zdanlivo nevinnými otázkami. Kľúčovými faktormi úspechu sú znalosť žargónu, sebaistota vystupovania útočníka a vhodná komunikačná stratégia (Jirovský, 2007). Pri oficiálnej komunikačnej stratégii nemusí sociotechnik poznať osobné údaje, ale musí pôsobiť profesionálne. Familiárna komunikačná stratégia vyžaduje znalosť osobných údajov a rysov cieľovej osoby. Najzložitejšia úzko osobná komunikačná stratégia vyžaduje mnoho podrobných informácií, vyvoláva pocit dôverného priateľstva a tak môže zlyhať i na neznalosti nepatrného detailu. Vybudovanú dôveru sociotechnik zneužíva pre získanie potrebných informácií. Využitím informácií pri útoku môže sociotechnický cyklus skončiť alebo sa zopakovať.



Obrázok 1.1 – Sociotechnický cyklus (zdroj: autorka, podľa Václava Jirovského, 2007)

4 Spôsoby doručenia phishingu používateľovi

Existuje viacero spôsobov ako phishing doručiť používateľovi a ich voľba záleží na pripravených sociálnych a technických trikoch aj na preferenciách určitého typu útoku phisherom. Všetko musí do seba perfektne zapadať, aby útok pôsobil legitímne. Pretože phishing nemožno úplne zastaviť, ale možno zmierniť jeho dopady (James, 2007) a je dôležité identifikovať spôsoby doručenia phishing pre vytvorenie správnych opatrení. Ollmann rozlišuje štyri spôsoby doručenia používateľovi (2004) a to: e-maily, webové stránky, konferenčné systémy, rýchle správy a hostiteľov trójskych koní.

4.1 Phishingové e-maily

Začiatky i súčasnosť phishingu sú spojené s e-mailom. Na počiatku boli informácie získavané prostredníctvom odpovedí používateľov na podvodné správy (Ollmann, 2004). Dnes sú stále jedným z najčastejších spôsobov doručenia. Phishingové e-maily sú podskupinou scamu (James, 2007), ktorý sa zameriava na získavanie finančných prostriedkov od používateľov, ale nevymáha zálohové platby. Úspešnosť e-mailu závisí na tvorivosti útočníka, grafickej úprave, originalite, štýle a dôveryhodnosti správy (James, 2007). Dôležité je tiež vyjadrenie obáv o bezpečnosť používateľa, miesto a akcia, ktorú má vykonať i nátlak kliknúť na zaslaný odkaz.

Pre distribúciu e-mailov používajú útočníci nástroje pre hromadné rozosielanie pošty. Zoznamy e-mailových adries získavajú s pomocou služieb hackerov, špecifických nástrojov pre zber adries alebo internistov (James, 2007), ktorí kradnú dáta zamestnávateľovi. Adresu odosielateľa upravujú pomocou spoofingu (Jakobsson a Myers, 2006), napriek tomu je však možné overiť si e-mailový server odosielateľa. Z dôvodu uchovávania anonymity a zakrytia stôp útočníci používajú k odosielaniu e-mailov open relay a open proxy servery, otvorené bezdrôtové siete a zamedzujú analýze prevádzky siete (James, 2007).

4.2 Phishingové webové stránky

Phishingový útok môže byť uskutočnený vložением škodlivého obsahu do webových stránok (Ollmann, 2004), ktoré prevádzkujú phisher alebo tretia strana. Napríklad použitím techniky falošnej internetovej reklamy (Ollmann, 2004). Útočníci skopírujú banner organizácie, pozmenia URL adresu a objednávajú si reklamný priestor.

Ak používateľ klikne na reklamu, je presmerovaný na podvodné webové stránky, kde phisher môže získať dôverné informácie. Útočníci ohrozujú používateľov aj z dôveryhodných domén, pretože dokážu odhaliť slabiny serverov, ktoré využijú napríklad s pomocou útokov svojvoľného presmerovania, Cross-site scripting (XSS), či injektovania nedôveryhodného kódu do dôveryhodného obsahu (James, 2007).

4.3 Konferenčné systémy a rýchle správy

Komunikačné kanály ako konferenčné systémy (Internet Relay Chat) a rýchle správy (Instant messaging) sú medzi používateľmi obľúbené a majú zabudovaných veľa funkcií ako napr. zasielanie dynamického obsahu používateľmi, URL odkazov, multimédií atď.. Ide o spôsob doručenia, pri ktorom môžu phisher prostredníctvom botnetov odpočúvať, zúčastňovať sa komunikácie a odosielať odkazy i falošné informácie (Ollman, 2004) potenciálnym obetiam.

4.4 Hostitelia trójskych koní

Zdrojom phishingových útokov sú často infikované domáce počítače, ktoré sú zoskupené do botnetov a rozosielaajú podvodné e-maily alebo hostujú podvodné weby. Útočníci majú k dispozícii i špecifické trójske kone v podobe keyloggerov a screengrabber (Ollmann, 2004), ktoré dokážu sledovať a zbierať vybrané dáta konkrétnych používateľov. Medzi útokom prostredníctvom e-mailu a malwaru, i v podobe trójskych koní, existujú značné rozdiely (James, 2007). Phishingový malwaru je účinnejší, ale útok pomocou e-mailu vyžaduje nižšie náklady. Údaje získané pomocou e-mailov majú okamžitú hodnotu, zatiaľ čo dáta nadobudnuté pomocou malwaru sú ťažšie spracovateľné a je potrebné vytvoriť malware, ktorý získané dáta aj spracuje. Vďaka modifikácii je možné útok prostredníctvom rovnakého e-mailu uskutočňovať dlhšiu dobu, zatiaľ čo proti malwaru sú v krátkej dobe pripravené antivírové programy.

Používatelia by mali byť obozretní voči všetkým spomínaným spôsobom doručenia. Phishing sa k nim môže dostať akokoľvek, aj keď si to neuvedomujú. Poznajú obmedzený počet spôsobov doručenia phishingových útokov a tým sa snažia vyhýbať. Phisher sa vyznačujú obrovskou kreativitou a spôsoby doručenia sú čoraz originálnejšie a menej nápadne. Aby sme mohli zmierniť dopady phishingu, je potrebné okrem spôsobov doručenia poznať aj typy phishingových útokov.

5 Typy phishingových útokov

Od vzniku phishingu sa vytvorilo veľké množstvo typov phishingových útokov. Existujúce útoky sa vyvíjajú, prispôbujú vzniknutým opatreniam a situáciám alebo zanikajú. Neustále však vznikajú nové, pre používateľov neznáme útoky. V rámci tejto kapitoly sa zaoberáme vybranými typmi phishingových útokov.

Takmer každý z autorov zaoberajúci sa tematikou phishingu rozdeľuje typy phishingových útokov odlišne. V kapitole 5 sa nachádzajú štyri rôzne členenia, ktoré sa však prostredníctvom niektorých základných typov prelínajú. Prvé uvedené rozdelenie phishingových útokov vytvoril Lance James. Rozlišuje a popisuje tri základné typy (2007) phishingových útokov:

1. **Útok prostredníctvom falošnej identity (MITM – Man in the middle)** – používateľ je nalákaný a presmerovaný z legitímnych webových stránok na podvodné. Phisher je prostredníkom medzi používateľom a skutočnými serverom, zachytáva prenos dát a na záver prihlási používateľa na skutočné stránky, aby si nič nevšimol. Grafický materiál je získaný zrkadlením stránok cieľovej inštitúcie, upravený a prepojený so skutočným webom. K útoku prostredníctvom falošnej identity môžu byť použité nasledovné techniky (James, 2007):
 - a. Oklamanie ARP (Address Resolution Protocol) – útočník sa vydáva za hlavný smerovač, cez ktorý klient komunikuje so skutočným cieľom. Sleduje a modifikuje dáta.
 - b. Oklamanie DNS (Domain Name System) – Pharming – útočník prinúti DNS server, aby používateľovi odpovedal inú IP adresu, akú by mu mal odpovedať.
 - c. Útok vychýlením – zámenou URL a HTML (HyperText Markup Language) – pre pripojenie používateľa na nepriateľský server a krádež identifikačných údajov.
 - d. Trojský kôň – keylogger – škodlivý softvér pre získavanie údajov.
2. **Útok presmerovaním** – pre útok presmerovaním nie je vytvorená falošná webová stránka, ktorá zbiera dáta. V útoku je použitý presmerovací skript, ktorý zbiera dáta. Používateľ zadáva údaje priamo do e-mailu a tie sú odosielané do anonymnej schránky phishera. Po zadaní údajov je používateľ

prostredníctvom skriptu presmerovaný na pravé webové stránky cieľovej inštitúcie.

- 3. Útok pomocou vyskakovacích okien** – dnes je vďaka blokovaniu prehliadačov a ignorácii používateľov takmer neúčinný. Okná sú prispôsobené vzhľadu cieľových webových stránok a otvárajú sa v ich popredí. Na získavanie údajov slúži obsiahnutý formulár. Po zadaní sa zobrazí zväčša poďakovanie, ale používateľ nie je prihlásený na cieľové stránky.

Uvedené členenie je jednoduché a prehľadné. Nevýhodou je, že nezahŕňa niektoré novšie typy útokov. Jeden z troch hlavných typov je iba veľmi zriedkavo používaný a je považovaný za takmer neúčinný.

Ollmannove členenie typov phishingových útokov (2004) je oproti predošlému veľmi podrobné. Vytvoril rozdelenie obsahujúce sedem hlavných typov, ktoré zahŕňajú ďalšie podrobné členenia jednotlivých typov na techniky. Z dôvodu rozsiahlosti sú spomenuté a popísané najmä hlavné typy i z nich je však možné vidieť, aká rozsiahla a rozmanitá je oblasť phishingu a voči akým útokom sa musia používatelia brániť. Hlavnými typmi phishingových útokov sú:

- 1. MITM útoky** – útočník sa nachádza medzi používateľom a skutočnou webovou aplikáciou a sprostredkováva celú komunikáciu v reálnom čase. Môže byť uskutočnený pomocou niekoľkých techník (Ollmann, 2004). Prostredníctvom použitia transparentného proxy, otravou DNS Cache, zamaskovaním URL a proxy konfiguráciou používateľovho prehliadača.
- 2. Zamaskovanie URL** – nabádanie používateľa k nasledovaniu hyperodkazu (URL), ktorý ho bez povšimnutia presmeruje na server útočníka. Na zamaskovanie URL môže útočník využiť viacero techník (Ollmann, 2004) ako: registráciu nesprávneho doménového mena, techniku zahrnutia údajov do URL, skrátené URL, zamaskovanie mena hostiteľa a zakódovanie URL prostredníctvom jednej alebo viacerých schém kódovania.
- 3. Cross-site Scripting útoky (XSS)** – útoky ktoré využívajú vlastné URL odkazy a injekť kódu do platnej URL adresy alebo dátového poľa. Sú výsledkom zlého procesu vývoja webových aplikácií. Klient napríklad dostane phishingový e-mail obsahujúci URL adresu. Po kliknutí na odkaz je smerovaný na skutočnú webovú aplikáciu banky, ktorá používateľovi namiesto overenia poskytne

stránky z externého serveru, na ktoré útočník odkazoval. Väčšinu XSS útokov nemá používateľ možnosť odhaliť.

4. **Útoky prednastavenými reláciami** – webové aplikácie môžu používať vlastné metódy sledovania používateľov a spravovania prístupu k zdrojom požadujúcim overenie používateľa. Implementáciou zlého systému riadenia stavov, môže dôjsť k zneužitiu pomocou prednastavených relácií.
5. **Skryté útoky** – útočník používa HTML (HyperText Markup Language) alebo iný skriptovací kód, aby zmanipuloval zobrazenie poskytovaných informácií. Zakrýva falošný obsah, aby pôsobil dôveryhodne a legitímne. Skryté útoky sú uskutočňované pomocou techník (Ollmann, 2004) skrytých rámov, prepísania obsahu stránok a grafickej substitúcie.
6. **Zaznamenávanie zákazníckych dát** – vkladanie do webových aplikácií prostredníctvom malwaru. Dáta sú rôznymi spôsobmi lokálne zhromažďované a zasielané útočníkovi alebo vyzdvihnuté pomocou škodlivého softvéru backdoor. Na sledovanie a zaznamenávanie dát sú používané dva druhy programov (Ollmann, 2004). Keylogger pozoruje a zaznamenáva stlačenia kláves na prihlasovacích stránkach webových aplikácií. Screengrabber získava dáta snímaním časti obrazovky prihlasovacích stránok a slúži na prekonanie viacfaktorového zabezpečenia.
7. **Využitie zraniteľnosti na strane klienta** – väčší počet funkcií prehliadača a možnosť inštalácie doplnkov, prinášajú väčšiu pravdepodobnosť zraniteľnosti a zneužitia. Dodávateľia síce často prichádzajú s aktualizáciami, ale niektorí používatelia ich neaplikujú a vystavujú sa nebezpečenstvu.

Ollmanovo členenie a rozdelenie typov phishingových útokov sa v niektorých bodoch prelína s ďalším členením, preto nie sú vyššie uvedené typy znovu popisované. Jakobsson a Myers rozlišujú šesť hlavných typov phishingových útokov (2006):

1. **Klamlivý phishing** – má podobu e-mailu a vyznieva ako upozornenie, vyzýva k rýchlej reakcii a snaží sa používateľa ovplyvniť, aby klikol na zaslaný odkaz a odovzdal svoje údaje.
2. **Phishing založený na malwari** – útok spustením škodlivého softvéru na používateľovom zariadení. Malware môže byť prílohou e-mailu, stiahnutý ako infikovaný súbor z webu alebo zneužije bezpečnostnú chybu. Phishing

založený na malwari môže byť uskutočnený pomocou nasledovných techník (Jakobsson, Myers, 2007):

- a. Keylogger a screengrabber
 - b. Session Hijacking – malware, ktorý kontroluje aktivity používateľa, preberie kontrolu nad zariadením a vykonáva nepovolené akcie.
 - c. Webové trójske kone – útočník prostredníctvom neviditeľných pop-up trójskych koňov získava prihlasovacie údaje.
 - d. Infikovanie súboru hostiteľov – operačný systém Microsoft Windows, pri preklade doménového mena na IP (Internet Protokol) adresu najprv prezerá svoj súbor hostiteľov. Útočník infikuje súbor a používateľ nevedomky navštívi podvodnú webovú stránku.
 - e. Útok rekonfiguráciou systému – útok zmení nastavenia zariadenia v prospech útočníka, napr. nastavenia internetového prehliadača.
 - f. Krádež dát – často používaná k obchodnej špionáži. Útočník získava dôvernú komunikáciu, projektovú dokumentáciu a rôzne iné záznamy napadnutej spoločnosti, následne ich predá konkurencii alebo spôsobí finančné škody a ťažkosti napadnutej firme.
- 3. Pharming** – útočníci manipulujú so súborom hostiteľov alebo DNS tak, aby na žiadosti o URL adresy alebo názvy služieb boli vrátené adresy falošných webových stránok. Používateľ si pritom neuvedomuje, že sa nachádza na podvodných stránkach.
- 4. Injektáž škodlivého obsahu do legitímneho obsahu** – útok, pri ktorom nahradia phisher čať obsahu legitímnych stránok škodlivým obsahom.
- 5. MITM**
- 6. Phishing prostredníctvom vyhľadávača** – útočníci vytvoria atraktívne webové stránky, ktoré nechajú indexovať vyhľadávačmi. Keď používateľ vyhľadá produkt alebo služby, sú mu ponúknuté podvodné stránky. Pokiaľ používateľ vyplní požadované informácie, stane sa obeťou podvodu.

5.1 Typy útokov v závislosti od počtu zberných miest

Phisher už pri útokoch nespoliehajú len na jedno skryté koordinačné centrum. Zo spomínaného dôvodu môžeme phishingové útoky na základe počtu používaných zberných miest na:

- **útok s jedným koordinačným centrom**
- a **distribovaný phishingový útok** (Jakobsson a Young, 2005).

5.1.1 Distribovaný phishingový útok

Distribované phishingové útoky dokážu obísť mechanizmus detekcie, ktorý na základe reverzného inžinierstva odhalí a zneškodní koordinačné centrum phisherov. DPA – Distributed Phishing Attack (Jakobsson a Young, 2005) funguje na základe personalizácie umiestnenia zberných miest a skrytého prenášania získaných údajov. Phisherí pre každú obeť alebo malú skupinu používateľov vytvoria jedinečnú webovú stránku. Pre hostovanie zberných miest využívajú bežných používateľov prostredníctvom škodlivého softvéru, ktorý odosiela údaje útočníkovi. Ide o šifrovacieho trójskeho koňa (Jakobsson a Young, 2005), ktorý s pomocou steganografie verejného kľúča vytvorí asymetricky zašifrovaný text a odosiela ho v multimediálnych súboroch na verejné vývesky alebo nástenky.

Odhaliteľ DPA by mal identifikátor kostry e-mailu (Jakobsson a Young, 2005), ktorý skenuje e-maily a porovnáva s nahlásenými. Pre používateľov by útoky mali byť rozlíšiteľné vzhľadom na charakteristický vysoký stupeň podobnosti obsahu, vzhľadu i odkazov bez vzájomného vzťahu.

Žiadne členenie nie je schopné popísať všetky typy útokov, pretože neustále vznikajú nové, ktoré ešte nie sú popísané. Ukazujú nám však rozmanitosť, zložitosť, prepracovanosť sveta phishingu, jeho vývoj a to, aké opatrenia musíme vytvárať. Zo spomínaných typov útokov a ich fungovania vyplýva, ktoré znaky by si používatelia mali všímať u e-mailov a webových stránok. V nasledujúcej kapitole sa budeme venovať aspektom, ktoré si skutočne používatelia všímajú a utvrdzujú ich v pravosti e-mailov a webových stránok ale aj slabostiam používateľov, ktoré phisherí zneužívajú.

6 Dôvody fungovania phishingu

6.1 Aspekty dôveryhodnosti e-mailov a webových stránok posudzované používateľmi

Pre pochopenie úspešnosti phishingu je nevyhnutné sledovať aspekty pravosti (Jakobsson, 2007) v phishingu a zamerať sa na sociálnu zložku. Často sa zabúda, že phishing nezneužíva len technickú zraniteľnosť a nemožno ho riešiť iba technickými opatreniami. Musíme zvažovať ako používatelia reagujú na obsah, či už je legitímny alebo podvodný. Nezáleží len na pravosti informácie. Malé rozdiely v prezentovaní informácií môžu mať veľký vplyv na vnímanie pravosti informácií používateľmi.

Významné zistenia v oblasti phishingu priniesol kontroverzný experiment (Jakobsson, 2007) zisťujúci aspekty, ktoré robia phishingové e-maily a podvodné webové stránky autentickými a legitímny obsah pochybným. Experiment sa snažil otestovať schopnosť používateľov rozpoznať znaky phishingu. Subjektmi boli vysokoškolskí študenti a zamestnanci univerzít. Vylúčené boli osoby s väčšími znalosťami v oblasti informatiky. Počas experimentu boli subjektom ukazované podnety v podobe e-mailov i webových stránok, ktoré boli skutočné i podvodné. Subjekty mali obmedzenú možnosť interakcie. Hodnotili pravosť podnetov na základe päť bodovej Likertovej škály a pri posudzovaní jednotlivých podnetov boli žiadaní o zdôvodnenie rozhodnutia (Jakobsson, 2007). Výskumníci zistili, že sa niekedy subjekty rozhodli skôr, než si dôkladne prezreli e-maily a webové stránky.

Poradie aspektov odzrkadľuje ich vplyv na dôveryhodnosť a prvoradý kontext bezpečnosti. Experiment priniesol nasledovných desať zistení (Jakobsson, 2007), ktoré sú významné pre predchádzanie phishingu:

- 1. Používatelia zvažujú pravopis a dizajn.** Subjekty nedôverovali e-mailom s pravopisnými chybami a e-mailom podpísaným názvom pozície, nie konkrétnou osobou. Niekoľko phishingových správ odhalili iba kvôli pravopisu. Keď si všimli hrubú gramatickú chybu, nezmenil ich názor ani bezpečnostný certifikát. Podozrivé pre účastníkov boli i e-maily, na ktoré nemali odpovedať a legitímne webové stránky s neprofesionálnym prevedením.

2. **Príliš veľký dôraz na bezpečnosť môže byť kontraproduktívny.** Podnety, ktoré boli síce autentické, ale zdôrazňovali svoju pravosť a ochranu proti phishingu boli pre účastníkov podozrivé.
3. **Používatelia sa pozerajú na URL adresy.** Subjekty si počas experimentu pozorne prezerali URL adresy webových stránok. Boli podozrievaví voči IP adresám a syntakticky neobvyklým adresám, s ktorými zaobchádzali rovnako ako s pravopisnou chybou.
4. **Dôveryhodnosť certifikátu záleží na rozpoznaní certifikačnej authority.** Podnety, ktoré obsahovali certifikát od dobre známych certifikačných autorít ako napr. Verisign boli vnímané veľmi pozitívne a dôveryhodne. Použitie menej známych ale autentických autorít nemalo rovnaký efekt, dokonca boli považované za podozrivé a niektorými subjektmi označené za podvodné.
5. **Používatelia posudzovali relevantnosť obsahu skôr než autenticitu.** Účastníci sa často rozhodli, či je podnet legitímny, na základe obsahu na rozdiel od známk pravosti. Podnety ponúkajúce finančnú odmenu alebo vyžadujúce heslo boli považované za phishingové, nezávisle od toho, či boli pravdivé alebo nie. Subjekty pokladajú za bezpečné informačné e-maily. To je problém, pretože môžu byť použité pre prilákanie používateľov na podvodné webové stránky.
6. **Vysoká miera personalizácie zvyšuje dôveryhodnosť e-mailov a webových stránok.** Čím viac osobných informácií je v podnete prítomných, tým je pravdepodobnejšie, že ho používateľ pokladá za autentický. Útočníci môžu pre podvod získať osobné údaje z verejne dostupných databáz. V budúcnosti môže byť pri phishingu využívaný data mining. Príkladom personalizácie môže byť phishingový e-mail, ktorý sa pokúša overovať klientov finančných služieb prostredníctvom počiatočných štyroch číslic účtu. Žiaden poskytovateľ finančných služieb neoveruje svojich klientov týmto spôsobom, pretože prvé štyri číslice sú spoločné pre veľké množstvo klientov. Účastníci experimentu však tento e-mail nepovažovali za podvodný a neuvedomovali si, že útočník môže tieto číslice odhadnúť.
7. **E-maily sú pokladané za viac nedôveryhodné než webové stránky, zatiaľ čo telefonáty podľa účastníkov dôveryhodné.** Mnoho subjektov sa vyhlo navštíveniu odkazu z e-mailu. Pravdepodobne preto, že boli len čiastočne vystavení podvodným webovým stránkam, považovali e-maily

za nedôveryhodnejšie. Pokúšali by sa overiť pravosť e-mailu prostredníctvom telefonátu, ale neuvedomili si, že môžu zavolať na podvodnú zákaznícku linku a tak odovzdať osobné údaje útočníkovi.

- 8. Ikona visiaceho zámku má obmedzený efekt.** Sama o sebe ikona zámku nezlepšuje u subjektov dôveru. Dôveryhodne na väčšinu účastníkov pôsobila ikona SSL zámku, iba dva subjekty dôveru stratili, keď videli neznámu certifikačnú autoritu.
- 9. Nezávislý kanál vytvára dôveru.** Existencia možnosti overiť si pravosť e-mailu alebo webovej stránky telefonátom, posilnila dôveru účastníkov. Väčšina z nich by ale pravosť telefonátom neoverovala.

Vzhľadom na existenciu technologických opatrení bude pravdepodobne ďalšia vlna útokov viesť k zlepšeniu podvodnej zložky. Ako sme už uvádzali, je ľahšie zneužiť používateľa než obísť prepracované technologické riešenia. Zo spomínaného dôvodu je potrebné sledovať aspekty, ktoré vzbudzujú v používateľoch dôveryhodnosť a zameriavať sa na ne vo vzdelávaní o phishingu. Phisherí dokonca vytvárajú vlastné stratégie, ktoré slúžia na zmätenie a oklamanie používateľov, bližšie sú popísané v nasledujúcej kapitole.

6.2 Stratégie phisherov na oklamanie používateľov

Používatelia sa často stávajú obeťami phishingu z dôvodu nedostatku pozornosti pri prezeraní e-mailov a webových stránok, ako aj z dôvodu neporozumenia a neznalosti práce informačných systémov (Jakobsson, 2007). Ľahšie sa bránia známym, než novým podvodom. Niektorí z nich dokážu ignorovať adresný riadok, bezpečnostné ukazovatele a varovania aj kontrolu zabezpečeného pripojenia. Spomínané nedostatky využívajú útočníci pri uskutočňovaní útoku v podobe stratégií, ktoré môžeme rozdeliť do troch dimenzií (Dhamija, Tygar a Hearst, 2006):

- 1. Nedostatok znalostí** – stratégia využíva neznalosť a nevedomosť používateľov a zahŕňa (Dhamija, Tygar a Hearst, 2006):
 - a. Nedostatok znalostí o počítačových systémoch – používatelia majú nedostatok znalostí a vedomostí o operačných systémoch, aplikáciách, e-mailoch, weboch, o ich rozdieloch a fungovaní.

- b. Nedostatok znalostí o bezpečnosti a bezpečnostných ukazovateľoch – zneužívajú phisherí prostredníctvom webových stránok. Niektorí používatelia nerozumejú overovaciemu procesu cez SSL (Secure Sockets Layer) certifikáty. Nechajú sa zmiasť falošnou ikonou visiaceho zámku ako signálom bezpečia.

2. Vizuálny podvod – pomáha pri napodobňovaní legitímnych stránok a e-mailov a môže ísť o (Dhamija, Tygar a Hearst, 2006):

- a. Vizuálne klamlivý text – využitie zmätku pomocou syntaxe doménového mena napr. nejednoznačnosť medzi malým l a veľkým I.
- b. Obrázky maskujúce pôvodný text – napríklad obrázok slúži ako hypertextový odkaz na iné miesto než pôvodne.
- c. Okná maskujúce pôvodné okná – útočníci umiestnenia podvodné okná v popredí alebo vedľa legitímnych a používatelia sa mylne domnievajú, že sú z rovnakého zdroja.
- d. Klamlivý vzhľad a dojem – ak weby a e-maily skopírované perfektne, len niektoré zanechané stopy, ako napr. pravopisné chyby alebo žiadanie údajov, naznačujú známky manipulácie.

3. Nedostatok pozornosti – zneužitie nevšímavosti používateľov môže mať dve podoby (Dhamija, Tygar a Hearst, 2006):

- a. Nedostatok pozornosti venovaný bezpečnostným ukazovateľom – niekedy sú používatelia tak zameraní na prvoradú úlohu, že si nevšímajú varovné správy a bezpečnostné ukazovatele.
- b. Nedostatok pozornosti venovaný absencii bezpečnostných ukazovateľov – mnoho používateľov si ani nevšimne absenciu bezpečnostné ukazovateľa ak je nahradený falošným obrázkom alebo indikátorom.

6.3 Stratégie používateľov pri posudzovaní pravosti webových stránok

Používatelia, rovnako ako phisherí, majú svoje stratégie. Na ich základe sa rozhodujú, či webové stránky budú považovať za skutočné alebo phishingové. Nasledovné stratégie sú rozdelené v závislosti od počtu použitých faktorov pri rozhodovaní o phishingových stránkach (Dhamija, Tygar a Hearst, 2006):

- 1. Bezpečnostné ukazovatele v obsahu webových stránok** – v rámci stratégie používateľa určujú legitimitu na základe obsahu webových

stránok, vrátane loga, usporiadania stránok, grafického dizajnu, prítomnosti funkčných odkazov a obrázkov, typu prezentovaných informácií, jazyka a presnosti informácií. Mnoho z používateľov používajúcich stratégiu hľadá pri overovaní legitimacy určitý typ obsahu ako napr. informácie o autorských právach, ikonu zámku v obsahu, či kontaktné informácie. Nevšímajú si ďalšie časti prehliadača ako napr. adresný riadok. Zväčša dosiahnu najnižšiu úspešnosť pri rozlišovaní phishingu.

2. **Bezpečnostné ukazovatele v obsahu a názve domény** – takmer 40 % používateľov (Dhamija, Tygar a Hearst, 2006) používa na posúdenie pravosti obsah i adresný riadok. Sú si vedomí zmenou v adresnom riadku pri pohybe z jednej stránky na druhú. Dokážu rozoznať IP adresu a doménové meno v adresnom riadku, i keď mnohí nevedia vysvetliť pojem IP adresa. Zvyšuje sa u nich podozrenie, ak vidia namiesto názvu domény IP adresu. Nevšímajú si zabezpečené spojenie.
3. **Bezpečnostné ukazovatele v obsahu, názve domény a HTTPS** (Hypertext Transfer Protocol Secure) – skupina používateľov si overuje i HTTPS v adresnom riadku. Pre mnohých z tejto skupiny je informácia o HTTPS rozhodujúcim faktorom pre určenie legitímnosti webu. Nevšímajú si však ikonu visiaceho zámku.
4. **Bezpečnostné ukazovatele v obsahu, názve domény, HTTPS a ikone zámku** – 23 % používateľov (Dhamija, Tygar a Hearst, 2006) si všima ikonu visiaceho zámku predstavujúcu zabezpečené spojenie cez SSL certifikát. Niektorí však viac než ikone v adresnom alebo stavovom riadku, dôverujú ikone v obsahu stránky.
5. **Bezpečnostné ukazovatele v obsahu, názve domény, HTTPS, ikone zámku a certifikátoch** – iba 9 % používateľov (Dhamija, Tygar a Hearst, 2006) kontroluje certifikáty. Ak stránke nedôverujú a potrebujú si overiť identitu serveru, použijú certifikát. Taktiež reagujú na bezpečnostné varovanie.

Najlepším spôsobom overenia pravostí a zároveň najjednoduchším obranným opatrením proti phishingu je zlý kontext. Ak si používatelia všimnú, že dostali správu, ktorú nemali, ľahšie posúdia jej pravosť. Čo sa stane v prípade, ak je kontext správne zvolený? Phishingové útoky sa stávajú ešte nebezpečnejšími a účinnejšími.

6.4 Kontext vo phishingu

Útočníci v niektorých prípadoch nevedia takmer nič o príjemcovi, čoraz častejšie sa však objavuje phishing obsahujúci kontext. Tieto útoky sú efektívne a veľmi nebezpečné, pretože pôsobia dôveryhodnejšie (Jagatic a kol., 2005). Príkladom kontextového phishingu môže byť nasledovný útok. Phisher vyvolá nedostupnosť služby a následne obeti oznámi bezpečnostnú hrozbu. Keďže obeť očakáva správu, ľahšie odovzdá svoje údaje útočníkovi. V kontextovom phishingu útočníci využívajú informácie získané z histórie nákupných preferencií, webového prehliadača, verejne dostupných databáz ale aj zo sociálnych sietí (Jagatic a kol., 2005).

6.4.1 Sociálny phishing

Novou formou phishingu, ktorá obsahuje kontext je sociálny phishing. Pojem sociálny phishing (Jagatic a kol., 2005) sa prvý krát objavil v roku 2005. Odvtedy útočníci zvyšujú výnosy z phishingu a silu útokov vďaka zneužívaniu sociálnych kontaktov príjemcu a informácií nájdených na sociálnych sieťach. Vytvárajú si falošné účty, cez ktoré získajú informácie o okruhu priateľov, vzťahoch, spoločných záujmoch, komunitách a mnohé iné. Sledujú aj rôzne blogy a komunitné weby. Sociálny phishing má 4,5 krát vyššiu úspešnosť (Jagatic a kol., 2005) ako klasický. Väčšina príjemcov sa s väčšou pravdepodobnosťou stane obeťou phishingu, ak sa útočník vydáva za niekoho známeho.

Pojem vznikol v rámci štúdie (Jagatic a kol., 2005), ktorá prebehla na *Univerzite v Indiane* v roku 2005. Tvorcovia štúdie získavali voľne dostupné informácie zo sociálnych sietí a vytvorili databázu vzťahov. Obeťami útoku boli študenti univerzity, vybraní na základe množstva zverejnených informácií. Štúdia overovala vplyv sociálneho kontextu na úspešnosť phishingu. Príjemcovia dostali dva e-maily nabádajúce k návšteve podvodných webových stránok a zadaniu univerzitných prihlasovacích údajov. Prvý z podvodných e-mailov bol odoslaný v mene jedného vybraného priateľa a druhý fiktívnou osobou. Úspešnosť prvého emailu bola 72 % zatiaľ čo druhého 16 % (Jagatic a kol., 2005). Vysokú úspešnosť spôsobilo univerzitné prostredie, ale i tak vznikol predpoklad vyššej úspešnosti sociálneho phishingu. Z výsledkov štúdie vyplynulo, že sociálny kontext viedol príjemcov k prehliadaniu dôležitých stránok, znižovaniu ostražitosťi a väčšej zraniteľnosti. Zároveň preukázal, že sa

častejšie obeťami sociálneho phishingu stávajú ženy a mladšie osoby a vyššiu úspešnosť majú e-maily od opačného pohlavia. Odolnejšími voči klasickému útoku boli študenti technologických oborov avšak sociálnemu phishingu podľahli rovnako ako ostatní. Zisťoval sa taktiež počet návštev jednotlivých používateľov, pretože sa im po zadaní údajov zobrazila správa o zaneprázdnenosti serveru. Niektorí tak urobili opakovane až 80 krát (Jagatic a kol., 2005) a vôbec si neuvedomili, že sa jedná o podvod.

6.4.2 Spear phishing

Ďalšou z nových a nebezpečnejších foriem phishingu je spear phishing, ktorý využíva dôverné vzťahy k navodeniu pocitu bezpečia (FBI, 2009). Dôvernosťou presvedčujú phisherí obeť o svojej legitímnosti. Poznajú meno, e-mailovú adresu a predovšetkým niečo o obeti vedia (FBI, 2009). Používatelia v snahe pomôcť známej osobe, skôr konajú ako premýšľajú a navyše im phisher podsunie dobrý dôvod, prečo potrebuje ich pomoc. Pred útokom musia phisherí získať dostatočné množstvo informácií, aby pôsobili presvedčivo a neprezradili sa. Zneužívajú interakciu s obeťou, verejne dostupné informácie napr. na sociálnych sieťach, webových stránkach, blogoch alebo napádanie databáz. Používatelia si myslia, že zverejňujú neškodné informácie, ale nie je to tak.

Spear phishing je sofistikovanejším a automatizovaným útokom, zameriava sa na menšiu skupinu používateľov a organizácií (Jakobsson a Myers, 2006) – študentov vybranej školy či klientov jednej banky atď.. Zdroj ani obsah e-mailu sa nezdá byť vzhľadom k príslušenstvu do určitej skupiny podozrivý. Je lukratívnejší, účinnejší a ťažšie detekovateľný. Keď sa používateľ stane obeťou, phisherí sa snažia maximalizovať zisk a niekedy získajú prístup k viacerým účtom naraz. Často totiž majú používatelia pre viacero účtov rovnaké heslo alebo variáciu hesla. Na rozdiel od klasického phishingu nie je rozosielaný naslepo (FBI, 2009) na všetky získané emailové adresy. Útoky sa vzhľadom na povahu spear phishingu veľmi ťažko odhaľujú a nie sú nahlasované. Spear phishing je najnebezpečnejšou formou phishingu, pretože zneužíva kontext, ktorý používateľ očakáva a tým mu dáva falošný pocit bezpečia.

Pri spear phishingu niekedy používatelia ani nezistia, že boli oklamaní, až keď je príliš neskoro. Reakciami používateľov, ktorí zistili, že sa stali obeťou phishingu sa zaoberá kapitola 7.

7 Reakcie obetí phishingu

V spomínanom experimente na *Univerzite v Indiane* boli zisťované aj reakcie obetí po uskutočnení útoku prostredníctvom vytvorených webových stránok s verejným diskusným fórom. Bolo pozorovaných niekoľko reakcií obetí phishingu (Jagatic a kol., 2005):

- **Hnev** – niektorí účastníci považovali experiment za neetický, nevhodný, nezákonný, neprofesionálny a chceli zakročiť proti výskumníkom. Reakcia ukazuje výrazné psychické dopady na obeť. Účastníkom experimentu neboli ukradnuté údaje, ale pociťovali narušenie svojho súkromia.
- **Popieranie** – žiaden z komentárov neobsahoval priznanie o podľahnutí útoku. Práve naopak diskutujúci uvádzali, že obeťou sa stal ich kamarát. Popierali, že by sa niekedy stali obeťami. Reakcia naznačuje, aké ťažké je pripustiť si vlastnú zraniteľnosť.
- **Nepochopenie** – mnoho účastníkov si myslelo, že výskumníci napadli ich emailový účet a odoslali podvodnú správu. Ďalší účastníci sa domnievali, že ich počítače boli infikované vírusom. Zmenili si heslo a preinštalovali antivírusový softvér. Reakcie dokazujú, že mnoho ľudí nechápe phishing, jednoduchosť tvorby podvodnej správy, preceňujú bezpečnosť a súkromie e-mailu.
- **Podcenenie nebezpečenstva zverejňovania osobných informácií** – účastníci experimentu nechápali ako a odkiaľ výskumníci získali ich osobné informácie. Iní zasa namietali porušením ich súkromia získaním informácií zo sociálnych sietí. Používatelia si neuvedomujú dôsledky zverejňovania informácií na sociálnych sieťach. Útočníci dokážu beztrešne zbierať informácie pre phishingový útok.

Phishing má na svoje obeť psychické dopady. Zanecháva pocit narušenia súkromia. Pre používateľov je ťažké pripustiť si zraniteľnosť. Podceňujú hrozbu phishingu a nebezpečenstvo zverejňovania informácií. Nechápajú fungovanie phishingu a technológií. Spomínané zistenia zdôrazňujú potrebu vzdelávania o bezpečnostných hrozbách vrátane phishingových útokov. Používatelia musia očakávať, že útok môže prísť dokonca aj od priateľov.

Phishing má aj ďalšie dopady. U niektorých používateľov spôsobuje nedôveru v informačné a komunikačné technológie, dokonca až odpor voči ich používaniu. Obete phishingu zväčša odmietajú využívať služby ako internetové bankovníctvo alebo nakupovať v on-line obchodoch. Sú oveľa podozrievavejšie než bežní používatelia. Keď používatelia zistia, že sa stali obeťou phishingu, zmenia si heslo k napadnutému účtu, ale vtedy je už neskoro. U klientov zneužitých spoločností vzniká nedôvera a spoločnosti opustia, pretože ich vinia z toho, že sa stali obeťou phishingu. Neuvedomujú si, že ich organizácie nemôžu pred phishingom úplne ochrániť, a že iba oni sú zodpovední za svoje konanie. Ak používajú antivírusový softvér, tak ho po útoku preinštalujú na iný. Myslia si, že je softvér nekvalitný, ak ich neochránil. Môžeme povedať, že sa používatelia snažia obviniť všetkých okrem seba.

Nielen phishing má však negatívne dopady. Snaha vzdelávať používateľov o phishingu môže mať tiež negatívne dôsledky. Niektorí používatelia sa môžu stať podozriví napr. voči všetkým e-mailom, ktoré obsahujú odkaz alebo prílohu. Uvedomujú si, že je phishingu reálnou hrozbou, a pretože nevedia phishing odlíšiť, preventívne upodozrievajú všetky e-maily a webové stránky.

Phishing je veľmi nebezpečný. Zneužíva zraniteľnosť používateľov, ich omylnosť, nevedomosť, neopatrnosť a nevšímavosť. Používa technické i sociálne triky aby používateľov uviedol do omylu. Okrem krádeže dôverných informácií, poverení používateľa, či finančných prostriedkov má phishing aj dopady na psychiku obetí. Používatelia nemôžu byť ponechaní napospas phishingu, a preto boli a sú vytvárané rôzne opatrenia proti phishingu.

8 Opatrenia proti phishingu

Aby mohli byť vytvorené vhodné opatrenia proti phishingu, musíme poznať typy útokov a fungovanie jednotlivých typov útokov. Musíme poznať útoky, aby sme mohli používateľov pred nimi varovať a vzdelávať, ako ich môžu rozpoznať. Taktiež musíme vedieť, podľa ktorých aspektov a akým spôsobom používatelia posudzujú pravosť správ a webových stránok, aby sme ich mohli upozorniť, ktoré zo znakov si majú všímať naďalej a ktoré naopak vôbec nevypovedajú o legitímnosti správ a web stránok.

Súčasná opatrenia nezadržia dlhodobo phishingové útoky. Názory na najvhodnejšie opatrenia sa veľmi odlišujú. Zatiaľ čo jedny sa spoliehajú v boji proti phishingu na technológie, iní vidia jadro bezpečnosti v človeku – používateľovi (Mitnick a Simon, 2003) a ďalší v kombinácii opatrení (James, 2007; Jakobsson a Myers, 2006). V tejto kapitole sú bližšie popísané jednotlivé opatrenia, ktoré sú na ochranu proti phishingu aplikované.

8.1 Obranné mechanizmy

Útočníci disponujú mnohými typmi phishingových útokov a práve preto neexistuje jedno univerzálne opatrenie proti rôznym útokom. Využíva sa zmes techník a technológií. Podľa Ollmanna vytvárajú najlepšiu ochranu proti phishingu bezpečnostné opatrenia na troch logických vrstvách (2004):

- **na strane klienta,**
- **na strane serveru,**
- **a na firemnej úrovni.**

8.1.1 Opatrenia proti phishingu na strane klienta

Strana klienta má vystupovať v popredí antiphishingového zabezpečenia. Vo všeobecnosti platí, že je menej zabezpečená než strana serveru. Jednotliví používatelia sa totiž vyznačujú rôznou úrovňou počítačovej gramotnosti, zručností a znalostí. Ochranu na strane klienta možno podporiť nasledovnými opatreniami (Ollmann, 2004):

- **Technológie na ochranu domácich zariadení** – používatelia si už uvedomujú potrebu ochrany svojich zariadení a často siahajú po spoločnom bezpečnostnom riešení v podobe antivírusového softvéru. Zvolený softvér by mal zahŕňať nasledovné služby (Ollmann, 2004):
 - lokálnu antivírusovú ochranu,
 - firewall,
 - systém pre odhalenie prieniku (Intrusion Detection System),
 - antispam,
 - a detekciu spywaru.
- **Zablokovanie niektorých funkcií e-mailového klienta** – e-mailoví klienti sú čoraz sofistikovanejší a poskytujú funkcie, ktoré nie sú každodenne používané a zároveň sú zneužívané k útoku. V prospech bezpečnosti by mali byť niektoré funkcie zablokované alebo vypnuté.
- **Zablokovanie niektorých funkcií prehliadača** – správne nakonfigurovaný prehliadač môže ochraňovať používateľa pred phishingom. Prehliadač obsahuje mnoho funkcií, ktoré môžu byť zneužitá a neúmyselne vytvárajú bezpečnostné chyby (napr. zablokovanie automatického sťahovania). Nové vlastnosti často riešia predošlé nedostatky, ale prinášajú aj nové možnosti útokov. Opatrením proti útoku je aj **využitie antiphishingového pluginu** alebo nástroja. Ide ochranný prvok, najčastejšie v podobe lišty do prehliadača, ktorý ponúka nástroje pre aktívny monitoring (napr. porovnáva navštevované weby so zoznamom podvodných). Zväčša funguje iba na široko distribuované útoky.
- **Digitálny podpis** – kryptografický systém s verejným kľúčom k digitálnemu podpísaniu emailu, ktorý slúži na overenie integrity obsahu správy. Podpis je sofistikovanou jednosmernou hash hodnotou, ktorá používa aspekty odosielateľovho súkromného kľúča, dĺžku správy, dátum a čas. Príjemca používa verejný kľúč na overenie hash hodnoty.
- **Všeobecné povedomie o bezpečnosti** – používatelia môžu urobiť niekoľko krokov aby sa nestali obeťou phishingu. Zásady, ktoré radia ako sa vyhnúť phishingu (APWG, © 2014b) znejú:
 - podozrieť e-maily urgentne žiadajúce o osobné údaje,
 - kontrolovať adresný riadok prehliadača, všímať si navštívené stránky,
 - nevypĺňať formulár vložený v e-maily, ktorý žiada o údaje,

- nenavštevovať stránky prostredníctvom odkazov zaslaných cez rýchle správy, chat, e-mail, od neznámej osoby alebo z nedôveryhodnej správy,
- zadať adresu stránok ručne, ak je účelom návštevy prihlásenie sa,
- vyhýbať sa odosielaniu osobných a finančných údajov prostredníctvom e-mailov a pred odoslaním cez webové stránky skontrolovať, či ide o zabezpečené spojenie v adresnom riadku prehliadača,
- skontrolovať certifikát a dôveryhodnosť certifikačnej authority vydávajúcej certifikát pri zabezpečenom spojení, kliknutím na ikonu visiaceho zámku,
- overiť digitálny podpis,
- kontaktovať spoločnosť odosielateľa v prípade podozrenia na nelegitímnosť e-mailu, nie však na telefónne číslo alebo adresu uvedenú v emaily.

Je potrebné, aby používatelia chápali, že musia byť obozretní, opatrní a dodržiavať určité opatrenia. Snaha o zachovanie bezpečnosti musí v prvom rade prichádzať zo strany používateľa. Ak sa správa nebezpečne a nechráni sám seba, ako ho má ochrániť niekto iný. Nevýhodou je pokrok v phishingu v podobe nových útokov a podvodných techník. Rozlišovanie phishingových útokov je čoraz ťažšie aj pre obozretných a opatrných používateľov.

8.1.2 Opatrenia na strane serveru

Organizácie by mali zaujímať aktívnu úlohu pri ochrane používateľov pred phishingovými útokmi. Implementovať antiphishingové technológie do webových stránok, rozvíjať interné procesy boja proti phishingu a vzdelávať svojich klientov. Uskutočnenie spomínaných krokov môže výrazne napomôcť v ochrane proti phishingu. Na strane serveru je možné urobiť nasledovné opatrenia (Ollmann, 2004):

- **Zlepšovanie povedomia používateľov a udržanie obozretnosti** spočíva v komunikácii s klientmi a používateľmi o hrozbe phishingu a možných preventívnych opatreniach. Je potrebné viditeľne zverejňovať informácie nápomocné pre používateľov a vykonať nasledovné kroky (Ollmann, 2004):

- Opakovane upozorňovať klientov prostredníctvom malých oznámení na prihlasovacích stránkach a hovoriť aj o spôsobe komunikácie spoločnosti s používateľmi.
- Vytvoriť jednoduchý spôsob nahlasovania phishingu, nápovedu pre nahlasovanie phishingu s názvom organizácie a spolupracovať s orgánmi činnými v trestnom konaní a poskytovateľmi.
- Poskytovať poradenstvo v prípade, že sa klienti stali obeťami útoku i ohľadne overenia pravosti e-mailov a webových stránok.
- Vytvoriť a uplatňovať jednotnú podnikovú komunikačnú politiku a prijímať kontrolné opatrenia na jej presadenie. Komunikačná politika má upravovať i obsah emailov tak, aby nevyzerali ako podvodné.
- Posielať používateľom jasné, stručné a konzistentné správy. Jedným chybným krokom môže organizácia narušiť dlhotrvajúce úsilie.
- Rýchlo a jasne reagovať na phishingové útoky a zdôrazniť reálnosť hrozby a prácu spoločnosti na ochrane pred útokom.
- Neposkytovať používateľom záplavu informácií.

Vyššie uvedené opatrenia sú dobrou investíciou. Pri používaní menej technologických riešení sú používatelia schopní väčšej dôvery (Ollmann, 2004) voči spoločnosti. Okrem spomínaných opatrení je dôležité, aby spoločnosť vytvorila plán (James, 2007), ktorý aplikuje v prípade phishingového útoku.

- **Poskytovanie prostriedkov a informácií pre overenie oficiálnej komunikácie** pomáha používateľom identifikovať potenciálne útoky. Organizácia musí prihliadnuť k vhodnosti prostriedkov vzhľadom k schopnostiam svojich klientov a môže vykonať nasledovné opatrenia (Ollmann, 2004):

- Personalizácia emailov prostredníctvom používania mien zákazníkov, častí jedinečných informácií a tiež uvádzaním mena, pozície a kontaktných informácií komunikujúcej osoby.
- Odkazovanie sa na predošlé správy, na predmet a dátum predošlých emailov. Opatrenie je zložité a nepohodlné.
- Používanie digitálneho podpisu pre podpisovanie správ.
- Vytvoriť webovú aplikáciu na overenie emailov a odkazov a umiestniť na firemných stránkach. Zákazníci si môžu overiť URL adresy alebo

texty prijatých správ pomocou interaktívneho formulára. Pokiaľ overenie zlyhá, mal by podnet preveriť pracovník spoločnosti.

- **Tvorba bezpečných webových aplikácií** – nepodceniť bezpečnosť pri vývoji webových aplikácií, aby nemohli byť ľahko zneužitú pre útok. Závažným problémom sú XSS zraniteľnosti, pretože môžu viesť k nezistiteľným a veľmi úspešným útokom.
 - Validovať obsah. Ak je zle implementovaná validácia obsahu alebo neexistuje proces validácie vstupov ide o pochybenie.
 - Používať spracovanie relácií, ktoré nie je náchylné na útoky.
 - Opatrne kvalifikovať URL. V rámci URL adresy by sa nemalo používať presmerovanie na inú adresu, IP adresa a odkazovať na alternatívnu cestu k súborom.
 - Skomplikovať overovacie procesy tak, aby útočník nemohol sledovať zadané údaje (napr. dvojfázové overenie a personalizácia obsahu).
 - Regulovať obrázky tak, aby bolo možné narušiť alebo identifikovať falošný web a zdroj útoku, s pomocou techník cyklenia obrázkov, obrázkov zviazaných so SessionID, neviditeľných vodoznakov alebo vkladania informácií o relácií do samotnej grafiky.
- **Overovanie založené na tokenoch** používa externý systém pre generovanie jednorázového hesla alebo časovo obmedzeného hesla. Môže byť založené buď na hardvéri napr. kľúčenka, karta, USB (Universal Serial Bus) kľúč alebo na softvéri.
- **Dodržiavať konvencie pomenovania hostiteľov a prepojení**. Organizácia by mala používať rovnaké koreňové domény, čo najjednoduchšie a výstižné názvy hostiteľov a URL adresy, automaticky presmerovať regionálne a iné registrované domény na hlavnú doménu organizácie, zabrániť použitiu číslovania hostiteľa, neuadržiavať informácie o relácii v URL.

8.1.3 Podniková úroveň

Podniky a poskytovatelia internetových služieb majú k dispozícii opatrenia (Ollmann, 2004) proti phishingu. Z Ollmannových zásahov na podnikovej úrovni boli vybrané tri opatrenia, ktorých aplikácia napomáha bežnému používateľovi – zákazníkovi podniku:

- **Automatické digitálne podpisovanie odchádzajúcich e-mailov** prostredníctvom konfigurácie e-mailových serverov organizácie.
- **Monitorovať podnikové domény a oznamovať podobné registrácie.** Organizácia by mala sama alebo pomocou zakúpenia služby sledovať registrácie súvisiacich a podobných pomenovaných domén, ktoré porušujú ochrannú známku spoločnosti a klamú, zavádzajú alebo metú zákazníkov. Tiež sledovať ukončenie platnosti a potrebu obnovy existujúcich domén.
- **Uskutočňovať aktívny web monitoring** s pomocou služieb pre sledovanie URL a webového obsahu stránok, ktorý monitoruje vyhľadávanie loga organizácie, ochrannú známku alebo unikátny webový obsah a nálezy porovnáva so zoznamov autorizovaných použití. V prípade neoprávneného použitia prijme sanačné opatrenia.

8.1.4 Antispamové filtre

Ochranný mechanizmus pred phishingovými e-mailami predstavujú aj antispamové filtre. Existujú dva typy filtrov (James, 2007), ktoré dokážu zachytiť spam a phishingové e-mail:

- **Automatický** pomáha používateľovi a zachytiť približne 95 – 99 % spamu a phishingových e-mailov.
- **Ľudský** má v sebe zabudovaný každý používateľ. E-mail musí vyzeráť dostatočne dôveryhodne a zaujímavo aby ho používateľ otvoril.

Kombinácia oboch filtrov znižuje úspešnosť prijatia spamu a phishingu na necelé 1% (James, 2007). Technické triky dokážu prekonať automatické antispamové filtre. Psychologická manipulácia vie oklamať ľudský antispamový filter. Filtre nezastavia šírenie phishingu, ale dokážu zabrániť prijatiu e-mailu vytriedením nevyžiadanej pošty. Zachytenú správu opatria varovaním pre používateľa. Každý e-mail je podrobený množstvu testov, ktoré overujú v správe znaky spamu a phishingu. Stále jestvuje riziko prijatia spamu alebo phishingu (James, 2007). E-mail môže byť priemerný a neupútať pozornosť. Nie je výnimkou, ak cez filter preklízne spam a phishing alebo je žiadaná pošta zaradená do spamu. Občas sa musíme prehrabávať nevyžiadanou poštou, ak nechceme prísť o zle zaradený email.

Úspešnosť prijatia phishingu je najvyššia prvých 48 hodín a následne klesá (James, 2007). S obsahom e-mailu sa oboznamuje čoraz viac používateľov, dochádza k osвете. Pre opätovné navýšenie úspešnosti musia phisherovia vytvoriť nový obsah emailu. Navyše prijatie phishingového e-mailu ešte neznamená, že používateľ prezradí svoje dôverné údaje. (James, 2007)

Nesmieme však zabudnúť, že phishing sa sústreďuje na oklamanie ľudského faktora a používateľ do značnej miery dokáže ovplyvniť úspešnosť útoku svojím konaním. Preto by sme prostredníctvom opatrení mali pôsobiť i na bežných používateľov a ich správanie. Musíme ich naučiť dodržiavať určité bezpečnostné zásady, ktoré im pomôžu zmierniť riziko ohrozenia phishingom.

8.2 Bezpečnostné zásady pre používateľov

Dodržiavanie nižšie uvedených všeobecných bezpečnostných zásad (Norton, ©1995 – 2014) používateľmi taktiež predstavuje jedno z opatrení proti phishingu. Síce nezamedzuje phishingu, ale môže používateľom pomôcť znížiť pravdepodobnosť, že sa stanú obeťou. Taktiež pomáhajú udržať určitú bezpečnostnú úroveň na strane používateľa. Rovnaké pravidlá uvádzajú v rámci bezpečnostných zásad i banky a ďalšie organizácie. Spomínané zásady a odporúčania znejú:

- **Udržať si súkromie** – je potrebné zamýšľať sa nad informáciami, ktoré zverejňujeme prostredníctvom internetu a nad dôsledkami ich zverejnenia. Vždy je nevyhnutné si premyslieť, či by sme chceli, aby informáciu získal útočník. Jednotlivé informácie sa zdajú byť neškodné, spolu ale môžu byť nápomocné k podvodu.
- **Používať rôzne heslá do jednotlivých účtov** – taktiež je dôležité premýšľať o výbere hesla a voliť si pre prihlasovanie do jednotlivých účtov odlišné prihlasovacie údaje. Z dôvodu ľahšej zapamätateľnosti niektorí používatelia siahajú po rovnakých prihlasovacích údajoch alebo ich variáciách. Spomínaný prístup uľahčuje útočníkom zneužitie viacerých účtov podvedeného používateľa. Správne heslo má byť silné a často menené.
- **Aplikovať aktualizácie a používať bezpečnostný softvér** – nesmiem ich nepovažovať za otravnú záležitosť ale vziať do úvahy ich potenciál z hľadiska bezpečnosti. Väčšina aktualizácií obsahuje bezpečnostné záplaty. Keď nám

softvér ponúkne možnosť aktualizácie, mal by sme ju aplikovať. Väčšina aktualizácií, totiž obsahuje bezpečnostné záplaty.

- **Premýšľať** – v prípade obdržania e-mailu, v ktorom sa na používateľa obracia priateľ, iná známa osoba alebo spoločnosť so žiadosťou o pomoc, by si mal najprv overiť, že nejde o podvod a kontaktovať známeho, priateľa alebo organizáciu. Na väčšine oficiálnych webových stránok spoločností sa nachádza kontakt v podobe emailu, na ktorý je možné zaslať podozrivé správy na overenie. V žiadnom prípade ale nesmie použiť kontakt organizácie, ktorý je uvedený v prijatej správe.
- **Antiphishingový filter** – v súčasnosti zahŕňa mnoho webových prehliadačov (FBI, 2009). Okrem antiphishingových filtrov sú na trhu dostupné aj pluginy na ochranu proti phishingu.

Ide o pravidlá, ktoré je potrebné rešpektovať a dodržiavať v kombinácii s opatreniami na strane klienta uvedenými v kapitole 8.1.1. Okrem spomínaných zásad existujú i ďalšie netechnologické opatrenia, ktoré zaujímajú dôležitú úlohu v boji proti phishingu a sú spomenuté v nasledujúcej kapitole.

8.3 Vzdelávanie používateľov, antiphishingové skupiny a legislatíva

Obranu proti phishingu môžeme vidieť aj v troch preventívnych netechnologických opatreniach, ktorými sú vzdelávanie používateľov, antiphishingové skupiny a legislatíva. (Shi a Saleem, 2012)

8.3.1 Vzdelávanie používateľov

Ľudský faktor je najzraniteľnejším článkom (Mitnick a Simon, 2003) akéhokoľvek bezpečnostného systému. I najlepší a najmodernejší bezpečnostný systém môže byť vďaka ľuďom nechránený. Hlúposť, naivita, ignorancia a ľahkovernosť sú ľudské vlastnosti, ktoré pomáhajú útočníkom a tvoria bezpečnostné trhliny.

Väčší počet účinených bezpečnostných opatrení a technológií vytvára u ľudí silnejší falošný pocit bezpečia (Mitnick a Simon, 2003) ale nevyrieši problém zraniteľného ľudského faktora. Môžeme používať riešenia ako firewall, šifrovací softvér, certifikáty, či dvojfaktorová autentizácia, ale ich schopnosť ochrany klesá, ak je pri zariadení neopatrná a nevšímavá osoba, ktorá si neuvedomuje nebezpečenstvo. Čím

sú bezpečnostné produkty lepšie a dokonalejšie, tým je pre útočníkov ťažšie nájsť chybu v systéme. Čoraz častejšie sa útoky zameriavajú na zlyhanie ľudí. Určitú dobu trvá i zapracovanie súčasných phishingových hrozieb do technologických riešení. V neposlednom rade podnecuje vývoj technologických riešení vývoj phishingu.

Východiskom z problému zraniteľnosti ľudského faktoru je naučiť používateľov využívať obmedzenú dôveru (Mitnick a Simon, 2003) v oblasti internetu. Predchádzať narušeniu súkromia, osobných údajov a informácií. Venovať pozornosť najväčšej bezpečnostnej hrozbe a to podvodom. Je ťažké žiť v neustálej pozornosti, a preto je nevyhnutné vytvoriť si návyky obozretnosti. Používatelia potrebujú byť preventívne vzdelávaní a oboznámení s následkami prezradenia údajov (Mitnick a Simon, 2003) a mať povedomie o význame informácií.

Vzdelávacie materiály o phishingu znížili návštevnosť podvodných stránok o 40% (Shi a Saleem, 2012). Problém však spočíva i v znížení návštevnosti legitímnych odkazov, pretože sa používatelia začali obávať útokov. Zo spomínaného dôvodu je dôležité nájsť správnu metódu vzdelávania veľkej časti populácie a spôsob ako upútať pozornosť používateľov. Niektorí používatelia už vyžadujú náležité bezpečnostné opatrenia, iní však stále uprednostňujú pohodlie pred bezpečnosťou vo forme nepríjemných ochranných mechanizmov.

8.3.2 Antiphishingové skupiny

V oblasti phishingu pôsobia zoskupenia, ktoré sa snažia pomáhať organizáciám aj bežným používateľom. Skúmajú a sledujú phishingové útoky, uskutočňujú prieskumy, vzdelávajú používateľov i organizácie, pomáhajú pri tvorbe legislatívy, vytvárajú bezpečnostné riešenia a vykonávajú ďalšie prospešné činnosti. Najznámejšími sú *Anti-phishing Working Group*, *FraudWatch International* a *PhisTank*.

Anti-Phishing Working Group (APWG) je medzinárodné konzorcium založené v USA. Združuje podniky vytvárajúce bezpečnostné produkty a služby, obchodníkov, finančné inštitúcie, orgány presadzovania práva, vládne agentúry, obchodné združenia, komunikačné spoločnosti a ďalšie inštitúcie. Konzorcium v súčasnosti pôsobí globálne a má európsku pobočku. Pravidelne zverejňuje prieskumy o phishingu, uskutočňuje rôzne projekty a vzdelávacie akcie.

Organizácia *FraudWatch International* ponúka celý rad bezpečnostných produktov a služieb i na ochranu pred phishingom. Odstraňuje podvodné webové stránky, malwarom infikované stránky, falošné profily na sociálnych sieťach i falošné mobilné aplikácie.

Komunita *PhisTank* sa zameriava na správu dát a informácií o phishingu na internete. Poskytuje prepracovaný systém nahlasovania phishingu a umožňuje používateľom aby hlasovali, či ide alebo nejde o phishing. Prevádzkuje stránky s archívom phishingových útokov a poskytuje možnosť overiť si prijatý e-mail alebo odkaz. Pre výskumníkov a vývojárov ponúka otvorené bezplatné API s integrovanými dátami na prevenciu proti phishingu.

8.3.3 Legislatíva

Legislatívna podoba opatrení proti phishingu nie je častá. Existuje málo zákonov, ktoré sa týkajú podvodov a zahŕňajú výslovne phishing alebo internetové podvody. Dôvodom môže byť nízke povedomie o phishingu na vládnej úrovni i u koncových používateľov (Shi a Saleem, 2012). Pre účel tvorby zákona je potrebná definícia pojem phishing a stanovenie jeho špecifik. Vzhľadom na neustále zmeny povahy phishingu a rozmanitosť phishingových útokov môže definícia phishingu a jeho charakteristík predstavovať značný problém. Phisher reagujú na opatrenia produkciou nových útokov. Navyše legislatívny proces je veľmi zdĺhavý a kým je zákon prijatý, sú už zahrnuté útoky zväčša prekonané novšími a nebezpečnejšími. V konečnom dôsledku existencia zákona nezaručuje obmedzenie phishingu. Vo väčšine prípadov je páchaný v zahraničí a o to ťažšie je páchateľa odhaliť a stíhať.

8.3.4 Zhodnotenie

V prípade phishingu neexistujú rýchle riešenia. Jestvuje mnoho typov útokov a stále vznikajú nové, avšak neexistuje jedno účinné opatrenie proti všetkým existujúcim typom útokov. Pred tvorbou opatrení musíme najskôr pochopiť útoky, vedieť na čo sa máme pripraviť, aby sme zistili, aké opatrenia vytvoriť. Preventívne opatrenia v podobe vzdelávania používateľov, antiphishingových skupín a legislatívy prinajmenšom podporujú technologické riešenia phishingu (Shi a Saleem, 2012). James (2007) vidí možné riešenie v kombinácii technologických, legislatívnych opatreniach a v aktívnej detekcii útokov. Podľa Mitnicka a Simon (2003) má zasa problém

najslabšieho článku – človeka vyriešiť vzdelávanie. Zvyšovania povedomia a vzdelávanie sú veľmi dôležité, ale problém phishingu podľa Jamesa (2007) nedokážu vyriešiť. Podľa ďalších (Jakobsoon a Myers, 2006) pomáhajú iba krátkodobo, pretože po zmene typov phishingových útokov nedokážu používatelia útok rozoznať. Vzdelávanie má aj svoje medze. Nemôžeme každého bežného používateľa naučiť všetko, čo vie odborník z oblasti IT. Ak sú určité útoky prevedené správne, nie je v moci používateľa odhaliť ich, ak nie je expertom.

Phishingové útoky ťažia z funkcií, ktorým bežní používatelia nerozumejú. Obmedzovanie funkcií nie je riešením, ale niekedy sa inak situácia riešiť nedá. Mali by sme používateľov nabádať k väčšej opatrnosti a nie k slepej viere v bezpečnosť internetu. Správne riešenie problému phishingu spočíva v nastavení vhodného pomeru medzi technologickými opatreniami a vzdelaním. Technológie musia zároveň začať rešpektovať ľudskú omylnosť. Softvér je len taký bezpečný, aký je bezpečný pri nesprávnom používaní (James, 2007), pretože môže byť väčšinou používaný nesprávne. V niektorých prípadoch je potrebná podniková zodpovednosť (James, 2007) za bezpečnosť. Významnú úlohu zastávajú aj antiphishingové zoskupenia, vďaka svojmu pôsobeniu na medzinárodnej úrovni. Zvyšujú povedomie o phishingu a pomáhajú nielen používateľom, aby si mohli phishingové správy a emaily overiť a nestali sa obeťami, ale aj organizáciám. Uskutočňujú osvetu medzi organizáciami. V niektorých prípadoch sú ich snahy neúčinné vďaka tzv. antiosвете. Nezodpovednému správaniu firiem, ktoré zlým spôsobom komunikujú so zákazníkmi.

Z predošlých kapitol vyplýva, že phishing je veľmi nebezpečný, organizovaný, prepracovaný a neustále sa vyvíja. Ľudský faktor je vo phishingu veľmi dôležitý a reprezentujú ho dve skupiny. Na jednej strane je stelesnený phisher, ktorí vytvárajú útoky a snažia prostredníctvom nich ukradnúť informácie a poverenia používateľov. Spôsobujú vývoj phishingu prostredníctvom nových útokov, scenárov, taktík, trikov a spôsobov doručenia a zároveň určujú trendy v oblasti phishingu. Na druhej strane ľudský faktor predstavujú bežní používatelia, ktorí sa musia útokom brániť. Phishing má na nich psychologické aj finančné dopady, avšak dokážu ovplyvňovať jeho úspešnosť svojím správaním. Aby sme zistili, ktoré taktiky phisherov najčastejšie používajú a taktiež, aké dopady má konanie phisherov na používateľov, rozhodli sme sa analyzovať celosvetovú situáciu v oblasti phishingu.

9 Analýza globálnej situácie v oblasti phishingu

Útočníci pracujú veľmi racionálne, aby ich útoky boli produktívne, prinášali peniaze a vyhýbali sa detekčným mechanizmom. Kvôli naplneniu spomínaných požiadaviek vznikajú neustále nové scenáre a taktiky. Ak chceme porozumieť situácii a trendom v oblasti phishingu, najkomplexnejšie informácie získame od skupiny APWG. Každý polrok zverejňuje prieskum – *Global Phishing Survey*, v ktorom sú zhromaždené dáta z organizácií APWG, *China Internet Network Information Center (CINIC)*, *Anti-Phishing Alliance of China (APAC)* a ďalších zdrojov. Prieskum je zameraný na používanie doménových mien ako hlavnú súčasť phishingu. Každá z nasledujúcich kapitol sa zameriava na jeden konkrétny znak, taktiku alebo trend, ktorý sa objavil v oblasti phishingu v minulosti alebo súčasnosti. V nich môžeme vidieť vplyv ľudského faktoru na phishing prostredníctvom phisherov a taktiež môžeme pozorovať, aké dôsledky majú tieto trendy a taktiky na bežného používateľa.

9.1 Phishingové gangy

Globálnu situáciu v oblasti phishingu dokáže výrazne ovplyvniť jeden subjekt. Dvomi najznámejšími zoskupeniami v phishingu boli *Rock Phish* a *Avalanche*. Gang *Rock Phish* bol na phishingovej scéne veľmi významným hráčom od začiatku roka 2006 do polovice roka 2008 (Rasmussen a Aaron, 2009a). Obohatil phishing o škodlivú registráciu doménových mien vo veľkom rozsahu a automatizáciu. Zameriaval sa najmä na zneužívanie registrátorov domén, ktorí reagovali veľmi pomaly a používali chabé overovanie platobných kariet.

Nástupcom *Rock Phish* sa stal v decembri 2008 phishingový gang *Avalanche* (Rasmussen a Aaron, 2009a). Využíval existujúcu infraštruktúru a metódy k napádaniu bankovníctva, finančných inštitúcií a veľkých on-line služieb. Zneužíval pomaly reagujúcich registrátorov doménových mien v malých krajinách. Menil zacielenie i objem útokov niekoľkokrát počas svojho pôsobenia. Zdokonalil masovo-produkčný systém nasadenia phishingových webov a crimewaru. Vyznačoval sa používaním menšieho počtu doménových mien, na ktorých bol umiestnený veľký počet rozmanitých útokov. Išlo o najsofistikovanejší a najškodlivejší subjekt pôsobiaci v oblasti phishingu.

V období svojej najväčšej slávy v 2. polroku 2009 *Avalanche* spôsobil 66 % všetkých phishingových útokov (Rasmussen a Aaron, 2010a) a globálny nárast

phishingu. Krátkodobé odstavenie botnetovej siete v roku 2009 a protiopatrenia začali značne pôsobiť na prácu gangu, preto v 1. polroku 2010 útočil menej a v polovici roka 2010 ukončil činnosť (Aaron, Rasmussen a Routt, 2011a). Gang prešiel k distribúcií trójskeho koňa, navrhnutého pre automatizáciu krádeží identity a uľahčenie neoprávnených transakcií v bankovníctve. Následne začali výrazne ovplyvňovať globálnu situáciu čínski phisher, ktorých pôsobenie sa výrazne odlišuje od činnosti gangu. Keď jeden subjekt zanikne je nahradený ďalším.

9.2 Čínski phisher

Rozmach phishingu v Číne pretrváva už niekoľko rokov. Čínski phisher uprednostňujú škodlivé registrácie lacných domén a subdomén a zriedka registrujú čínske domény .CN. Využívajú prevažne služby čínskych registrátorov, preto patria medzi najzneužívanějších registrátorov a niektorí sú zneužívaní dokonca opakovane. Útočia väčšinou na čínske ciele a veľké a známe organizácie ako napr.: *Taobao.com*, *Industrial and Commercial Bank of China*, *China Central Television*, *Zhejiang Satellite Television*, *Tencent*, *Facebook*, *PayPal* (Aaron, Rasmussen a Routt, 2014a). Útoky na čínske ciele sú pravdepodobne výnosné, pretože sa v Číne stále vyskytuje veľké množstvo začínajúcich používateľov. Dokonca sú pre napádanie čínskych inštitúcií vytvorené a predávané phisherské sady.

Čínski phisher sú zodpovední za 85 % všetkých phishingových doménových mien v 1. polroku 2014 (Aaron, Rasmussen a Routt, 2014b) a výrazne zvyšujú počet škodlivých registrácií. Deväť z desiatich najzneužívanějších registrátorov domén a subdomén sídli v Číne (Aaron, Rasmussen a Routt, 2014b). Trend ovládania globálnej situácie čínskymi phisher bol zaznamenaný po ukončení činnosti gangu *Avalanche* a v súčasnosti vrcholí.

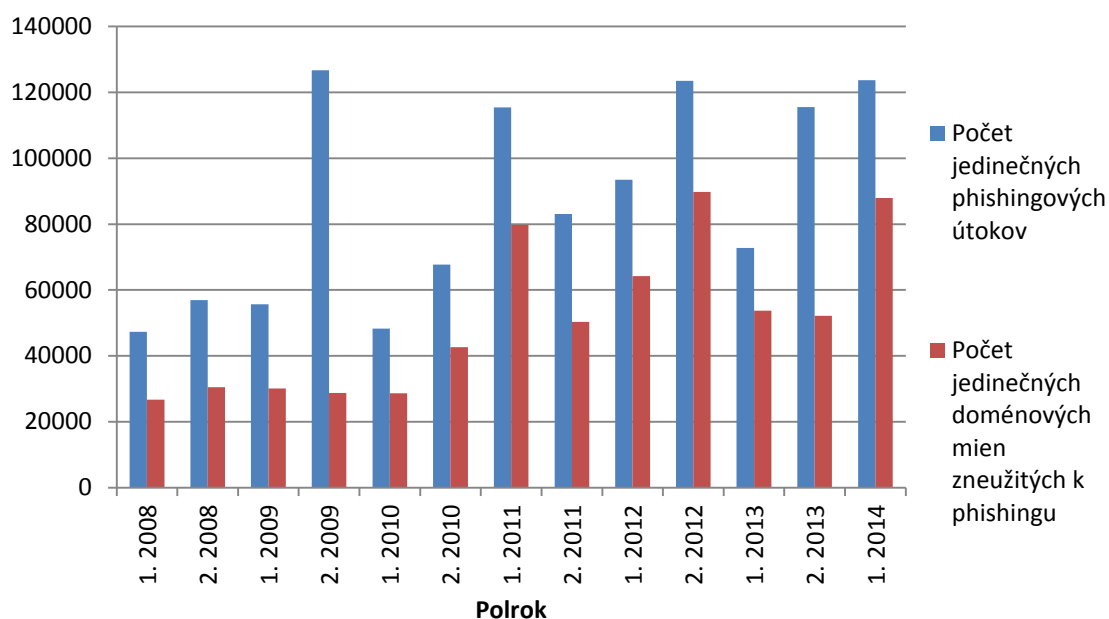
9.3 Počet phishingových útokov

Počet jedinečných phishingových útokov do značnej miery závisí od typu útoku preferovaného phisher v danom období. Štatistiky o phishingových útokoch vytvára skupina APWG na základe dát získaných z vlastných zdrojov (phishing nahlásený priamo skupine APWG, buď bežnými používateľmi, alebo organizáciami) ale aj z externých zdrojov (dáta poskytnuté spolupracujúcimi organizáciami CINIC a APAC ako aj členskými organizáciami, ktoré sledujú phishingové útoky).

Po kompletizácii dát, sú vylúčené duplicitné útoky (ak bol napr. ten istý útok nahlásený viackrát, prípadne sa s jedným útokom spájajú rôzne URL adresy a pod.), aby neboli štatistiky skreslené. **Za posledné dva roky je počet unikátnych phishingových útokov pomerne stabilný a vysoký, pohybuje sa tesne pod historickým maximom.** Počet phishingových útokov sa v 1. polroku 2014 mierne zvýšil a vyskytlo sa takmer 124 000 útokov (Aaron, Rasmussen a Routt, 2014b), čo je najviac od druhého polroka 2009 (Rasmussen a Aaron, 2010a). Vzrast zapríčinilo napádanie zdieľaných virtuálnych serverov a taktiež registrovanie doménových mien a subdomén čínskymi phisherami. V 1. polroku 20013 však počet útokov výrazne poklesol (Aaron, Rasmussen a Routt, 2013a) vďaka úbytku útokov na zdieľané virtuálne servery, zatiaľ čo o obdobie neskôr prišiel rapidný vzostup počtu phishingových útokov až od 60 % (Aaron, Rasmussen a Routt, 2014a) vďaka činnosti čínskych phisherov. Podobné výkyvy v počte jedinečných útokov, ktoré sú spôsobené preferenciou určitých typov phishingu, môžeme sledovať od začiatku roka 2009. Historické maximum počtu phishingových útokov, viac než 126 679 útokov (Rasmussen a Aaron, 2010a), bolo zaznamenané počas pôsobenia gangu Avalanche v 2. polovici roka 2009.

Polrok	Počet jedinečných phishing. útokov	Počet jedinečných doménových mien použitých k phishingu	Počet jedinečných IP adries použitých k phishingu	Počet škodlivo registrovaných doménových mien	Počet TLD	Počet IDN	Počet cieľov
1. 2014	>123 741	87 901	2 317	22 679	227	112	756
2. 2013	>115 565	82 163	837	22 831	210	82	681
1. 2013	>72 758	53 685	1 626	12 153	194	78	720
2. 2012	>123 486	89 748	1 841	5 835	207	147	611
1. 2012	>93 462	64 204	1 864	7 712	202	58	486
2. 2011	>83 083	50 298	1 720	12 895	200	36	487
1. 2011	>115 472	79 753	2 385	14 650	200	33	520
2. 2010	>67 677	42 624	2 318	11 769	183	10	587
1. 2010	>48 244	28 646	2 018	4 755	177	10	568
2. 2009	>126 697	28 775	2 031	6 372	173	12	
1. 2009	>55 698	30 131	3 563	4 382	171	13	
2. 2008	>56 969	30 454	2 809	5 591	170	10	
1. 2008	>47 342	26 678	3 389		155	52	
2. 2007		28 818	5 217		145	10	

Tabuľka 9.1 – Vývoj globálnej situácie v oblasti phishingu (zdroj: autorka, podľa: Rasmussen a Aaron, 2008a – 2010a; Aaron, Rasmussen a Routt, 2010b – 2014b)



Graf 9.1 – Vývoj počtu phishingových útokov a doménových mien (zdroj: autorka, podľa: Rasmussen a Aaron, 2008b – 2010a; Aaron, Rasmussen a Routt, 2010b – 2014b)

9.4 Ciele phishingových útokov

Útočníci neustále hľadajú nové a rozmanité ciele, aby maximalizovali výnosy z phishingu. Nové ciele sú menej rizikové a umožňujú používanie starých praktík. V ohrození je každá organizácia, ktorá je on-line. Roky sa útočníci najviac sústreďia na banky, elektronické obchody, transfery peňazí a sociálne siete. Rozmanitosť cieľov phishingu je skutočne obrovská. Napádané sú organizácie od vládnych a daňových úradov cez módné domy, realitné kancelárie, poštové a prepravné služby, poskytovateľov telekomunikačných služieb, spoločnosti obchodujúce s cennými papiermi až po firmy vytvárajúce antivírusové programy alebo on-line hry.

Do začiatku 2. polroka 2011 sa phisher zameriavali na všetky webové stránky, ktoré im mohli poskytnúť nejakú hodnotu. Na významné ciele dovedy útočili menej zdatní phisher, ktorí používali zakúpené nástroje a skúsení phisher, ktorí tvorili nové útoky. Od polovice roka 2011 sa útočníci začali zameriavať na väčšie a populárnejšie ciele (Aaron, Rasmussen a Routt, 2012a). Dôvodmi mohli byť stabilizácia neustále sa znižujúcich výnosov z phishingu, jednoduchšia predajnosť, výhodnejšia cena prístupových údajov k stránkam populárnych inštitúcií na čiernom trhu a efektívnejšie využitie pre rozosielanie spamu. Zároveň sa začali sústreďiť na novo populárne

a zraniteľné organizácie (Aaron, Rasmussen a Routt, 2012a), ktorých zákazníci sú proti phishingu bezbranný.

Počet napádaných organizácií sa takmer neustále zvyšuje. Dlhodobo je najčastejším terčom phishingu *PayPal*. Útoky sa nevyhnú ani veľkým firmám ako *Google*, *Apple*, *Facebook*, atď. Cieľom čínskych phisherov je najčastejšie *Taobao.com*. Webová stránka určená k on-line nakupovaniu a aukciám. Pozor by si mali dávať i hráči on-line hier napr. *World of Warcraft*. Cena prístupových údajov k on-line hrám je na čiernom trhu vysoká, najmä ak ide o pokročilého hráča.

9.5 Názov značky v doménovom mene

Útočníci sa vyhýbajú umiestňovaniu pôvodného alebo pozmeneného názvu značky do doménového mena. Skôr sa uchýľujú k nezmyselným reťazcom. Snažia sa obmedziť riziko odhalenia útoku pri aktívnom skenovaní, ktoré uskutočňujú majitelia značiek. Názvy značiek a ich variácie častejšie umiestňujú do podadresárov a subdomén. Používatelia potom názov značky v rámci URL vidia a tak môžu byť oklamaní.

Kedysi phisherí veľmi často používali taktiku uvádzania názvu značky alebo jej variácie v doménovom mene. Najextrémnejším bol rok 2007, kedy značku obsahovalo viac ako 42 % doménových mien (Rasmussen a Aaron, 2008a). Výrazný trend neuvádzania značiek v doménových menách môžeme vidieť od začiatku roka 2008 (Rasmussen a Aaron, 2008b). V 1. polroku 2014 bola značka zakomponovaná iba do 1,7 % zo všetkých doménových mien (Aaron, Rasmussen a Routt, 2014b) použitých k phishingu. Podiel doménových mien obsahujúcich značku kolíše medzi 1,4 – 9 % (Aaron, Rasmussen a Routt, 2014b), ale v poslednom roku môžeme vidieť mierny pokles. Zaujímavým faktom je, že niektoré doménové mená síce obsahovali značku, ale boli použité k útokom na úplne inú značku.

9.6 Doba životnosti phishingových útokov

Doba životnosti phishingových útokov je do značnej miery ovplyvnená preferovanými a uskutočňovanými útokmi. U domén s malým počtom phishingových útokov je doba životnosti zreteľne vyššia. S poklesom doby životnosti útokov stúpajú phisherom náklady. Čím viac phishingu je uskutočneného napádaním zdieľaných

virtuálnych serverov, tým je doba životnosti útokov kratšia. Sú veľmi rýchlo ohlásené a je zamedzené viacerým phishingovým stránkam súčasne. **Priemerná doba životnosti phishingových stránok sa znižuje a blíži sa k historickému minimu** (Aaron, Rasmussen a Routt, 2014).

Najvyššia priemerná doba životnosti bola nameraná v 2. polroku 2010 po ukončení činnosti gangu *Avalanche* (Aaron, Rasmussen a Routt, 2011a). Naopak jedny z historicky najnižších hodnôt priemernej doby životnosti boli zaznamenané za ich pôsobenia v roku 2009. Doba životnosti útokov *Avalanche* značne ovplyvňovala celkovú priemernú dobu životnosti phishingových útokov a dokonca bola o polovicu nižšia (Aaron, Rasmussen a Routt, 2010a). Historické minimá priemernej doby životnosti – 23 hodín a 10 minút a mediánu životnosti – 5 hodín 45 minút (Aaron, Rasmussen a Routt, 2010b) boli namerané v prvom polroku 2010 vďaka vzostupu útokov na zdieľané virtuálne servery. Polovica phishingových útokov v spomínanom období bola aktívna menej ako 5 hodina a 45 minút. Znižovanie doby životnosti je veľmi dobrým trendom. Čím dlhšie je phishing totiž aktívny, tým viac strát napácha a výnosy phisherov sú vyššie.

9.7 Používanie doménových mien k phishingu

V phishingu dlhodobo prevláda **používanie napadnutých a z hľadiska webhostingu zraniteľných doménových mien**, pretože útočníci nad nimi získajú priamu kontrolu. Naopak registrované doménové mená a subdomény sú citlivejšie na kontrolu. Na základe sťažností sú rýchlo blokované. Trend vyvrcholil v 2. polroku 2012, v ktorom bolo 93,5 % doménových mien použitých k phishingu získaných hackingom alebo zraniteľným webhostingom (Aaron, Rasmussen a Routt, 2013a).

K škodlivým registráciám je používaná široká škála domén najvyššej úrovne, ktorá sa takmer neustále rozširuje. Až na výnimky, ktorými sú domény so slabším zabezpečením, kopíruje zneužívanie domén ich podiel na trhu (Aaron, Rasmussen a Routt, 2014b). Prvoradým faktorom výberu registrátora je používanie opatrení proti zneužívaniu. Významné sú i jednoduchosť registrácie a existencia prekážok napr. v podobe čakacej doby, občianstva či pobytu. Cena je nepodstatná, avšak znižovanie cien určitej domény najvyššej úrovne (Top Level Domain – TLD)

spôsobí nárast používania aj phishingu. Dôležitý je kompromis medzi komfortom a bezpečnosťou.

Škodlivé registrácie sa dlhodobo koncentrujú do troch až piatich domén najvyššej úrovne. Napríklad v 1. polroku 2012 sa sústredilo 90 % škodlivých registrácií do troch TLD (Aaron, Rasmussen a Routt, 2013b). Ohľadne domén najvyššej úrovne, funguje vo phishingu „Teória rozbitého okna“ (Rasmussen a Aaron, 2008b). Ignorovanie malých problémov vytvára pocit úpadku a priťahuje zlé prvky nerešpektujúce zákon. Nedbalí a nepozorní registrátori a poskytovatelia pritiahli phisherov a vytvorili z phishingu globálny problém.

Dlhodobo je k phishingu zneužívaná doména Thajska .TH, kvôli napádaniu a zneužívaniu vládnych a univerzitných serverov. Tri roky po sebe sa držala na vrchole najzneužívanějších domén najvyššej úrovne (Aaron, Rasmussen a Routt, 2011b). Ako doméne pomôže zavedenie antiphishingového programu, vidieť na doméne Tokelau .TK. Výrazné a dlhodobé zneužívanie ukončilo zavedenie opatrení a prístupu partnerov do registra s možnosťou zablokovať škodlivé domény. Vďaka zásahom sa znižuje počet registrátorov využívaných k registrácií phishingových doménových mien. V 1. polroku 2014 sa klesol až o pätinu (Aaron, Rasmussen a Routt, 2014b).

9.8 Subdoménové služby

V rámci subdoménových služieb dostane zákazník hostingový účet pod názvom domény poskytovateľa. **Oblasť subdomén je obrovská a ich použitie v phishingu napomáha dlhšiemu prežitiu útokov, pretože sú ťažšie odhaliteľné.** Mnoho služieb je zadarmo. Ponúkajú jednoduchú, anonymnú a hromadnú registráciu. Ak poskytovateľ nie je schopný riešiť problém zneužívania, je služba predurčená k ohrozeniu. Obmedziť spomínaný problém môže len samotný poskytovateľ služieb. Zatiaľ však postrádajú spoľahlivú metódu na odstraňovanie škodlivých subdomén vo veľkom meradle. Hlavná doména nemôže byť zablokovaná, pretože by na zneužitie doplatili i nevinní. V krajnom prípade ale musí poskytovateľ pristúpiť k tomuto riešeniu. Rýchla reakcia na sťažnosti je nedostačujúca. Vzniká potreba zavádzať opatrenia proti zneužívaniu odrádzajúce útočníkov. Prijímanie opatrení spôsobuje presun phisherov k novým subdoménovým službám. Počet dlhodobo využívaných služieb k phishingu je preto veľmi nízky.

Trend používania veľkého počtu subdomén v phishingu sa objavuje v roku 2007, kedy tvorili približne 20 % zo všetkých doménových mien použitých k phishingu (Rasmussen a Aaron, 2007). Spomínaná situácia pretrvávala dlhodobo až na výrazný pokles (Rasmussen a Aaron, 2008b) podielu subdomén v roku 2008. Na začiatku roka 2011 sa objavil ďalší trend a používanie subdomén v phishingu mierne pokleslo (Aaron, Rasmussen a Routt, 2011b). V roku 2013 stúpala na zatiaľ najvyššiu zaznamenanú úroveň a druhej polovici roka subdomény predstavovali 27,8 % doménových mien (Aaron, Rasmussen a Routt, 2013b) použitých k phishingu. V poslednom roku počet registrovaných phishingových subdomén klesal, napriek tomu stále predstavujú 14 % zo všetkých phishingových útokov (APWG, 2014).

9.9 Skrátené URL adresy

Trend zneužívania služieb na skrátenie URL adres sa prvýkrát objavuje v 1. polroku 2009 (Aaron, Rasmussen a Routt, 2009b). **Phisher sa v súčasnosti vracajú k maskovaniu URL adres podvodných stránok prostredníctvom skrátených URL adres.** Skrátené URL adresy majú veľkú základňu používateľov, ktorí im veria i keď sú netransparentné. Počty útokov prostredníctvom skrátených URL adres sú malé, pretože veľa poskytovateľov používa skríningový mechanizmus pre odhaľovanie nebezpečných adres, nástroj pre určenie cieľovej URL adresy a funkciu jednoduchšieho a efektívnejšieho nahlásenia nebezpečných adres. V dôsledku spomínaných opatrení začali phisher vytvárať vlastné skracovače URL adres.

V druhom polroku 2013 bol zaznamenaný doteraz najvyšší počet phishingových útokov prostredníctvom skrátených URL adres, pretože phisher objavili nezodpovedného poskytovateľa *TinyURL.com* a vďaka nemu uskutočnili 50 % zo všetkých útokov (Aaron, Rasmussen a Routt, 2014a) so skrátenými URL adresami. V súčasnosti skrátené URL adresy tvoria 1,4 % phishingových útokov (Aaron, Rasmussen a Routt, 2014b) a medzi najviac zneužívané služby patria *TinyURL*, *Bit.ly* a *Owl.ly*.

9.10 Útoky na zdieľané virtuálne servery

Počas útokov na zdieľané virtuálne servery narušia phisher celkovú správu systému a sfaľujú konfiguračný súbor serveru. Dokážu pridať phishingový obsah na všetky webové stránky umiestnené na napadnutom serveri a zneužiť súčasne stovky

webových stránok. Používatelia webov vidia namiesto legitímneho obsahu phishingový. **Napadnuté servery sú ďaleko výkonnejšími prostriedkami pre phishing než infikované domáce počítače.**

Do začiatku roka 2013 bolo zaznamenaných menej než 200 útok na zdieľané virtuálne servery. Následne prišiel obrovský nárast. Len v 1. polroku 2014 phisherí uskutočnili 215 napadnutí, ktoré mali za následok 20 % zo všetkých phishingových útokov (Aaron, Rasmussen a Routt, 2014b). Nárast útokov je pravdepodobne spôsobený ich kratšou dobou životnosti a v konečnom dôsledku menšou účinnosťou. Náklady na phishing s kratšou dobou životnosti rastú ale v prípade zneužívania zdieľaných virtuálnych serverov sú vyvážené počtom napadnutých doménových mien.

9.11 IP adresy používané k phishingu

Phisherí k útokom používajú IP adresy už len veľmi málo. Od roku 2010 (Aaron, Rasmussen a Routt, 2010b) nebola žiadna z adries použitých k phishingu IPv6 (Internet Protocol version 6). Najmenej phishingových IP adries sa vyskytlo v 2. polroku 2013 a tvorili 0,7 % phishingových útokov (Aaron, Rasmussen a Routt, 2014a). Najvyššie využitie dosiahli v roku 2007, kedy tvorili až 18 % phishingových útokov (Rasmussen a Aaron, 2008a). Od začiatku roka 2009 sa IP adresy podieľajú na phishingových útokoch približne 2 %.

9.12 Internacionalizované doménové mená v phishingu

Phisherí zriedkavo zneužívajú internacionalizované doménové mená IDN (Internationalized Domain Names) môžu obsahovať písmená národných abecied (napr. písmená s diakritikou a taktiež písmená a znaky z abecied jazykov, ktoré nepoužívajú latinku – čínština, arabčina, hindčina atď.) V inom jazyku môže byť doménové meno na nerozoznanie od pôvodného a dokáže používateľa oklamať k návšteve phishingových stránok, avšak **homografické útoky phisherí takmer vôbec nevytvárajú.** Homografickému útoku dokážu zabrániť webové prehliadače, keď namiesto prirodzených znakov zobrazia verziu punycode. Od januára 2007 bolo zaznamenaných 9 homografických útokov a z toho jeden v prvom polroku 2014 (Aaron, Rasmussen a Routt, 2014b). Väčšina zneužitých internacionalizovaných doménových mien bola napadnutá.

9.13 Spear phishing

Spear phishing je nebezpečný, ale jeho sledovanie je problémové, keďže sa sústreďí na malé a špecializované ciele, ktoré zväčša útoky nenahlásia.

9.14 Zhrnutie situácie a dopady na používateľov

Analýzou prieskumov *Global Phishing Survey* od roku 2007 do konca 1. polroka 2014 sme zistili, že **protiopatrenia neznižujú počet phishingových útokov**. Spôsobia iba presun útočníkov k iným taktikám, prostriedkom a útokom. Pre používateľov je spomínaná situácia zložitou. Keď sa práve naučia chrániť pred určitými útokmi, phisheri musia v dôsledku protiopatrení prejsť na iné útoky, ktoré sú pre používateľov neznáme a ľahšie sa stanú ich obeťou.

Celkový počet útokov a priemerná doba životnosti phishingu sú významne ovplyvnené práve phisherami a nimi využívanými typmi útokov. Phishing má svoju ekonomiku a útočníci sa snažia maximalizovať zisk, preto sa vždy uchýľujú k výnosným útokom. V posledných dvoch rokoch sa počet jedinečných phishingových útokov približuje k historickému maximu.

Situáciu v oblasti phishingu dokáže ovládnuť jeden subjekt, ktorý môže spôsobovať nielen zmeny v počte útokov ale aj ich prevedení. Nikdy nevieme, kedy môže na phishingovú scénu vstúpiť gang, ktorý bude ohrozovať používateľov na celom svete. Už niekoľko rokov virtuálny svet sužujú útoky čínskych phisherov. Vyberajú si zväčša čínske inštitúcie, ale neváhajú útočiť aj na celosvetovo významné ciele ako *Facebook*, *Google*, *Paypal* atď.

Phishingový útok môže prísť odkiaľkoľvek. Phisher sa zameriavajú na širokú paletu cieľov a používatelia nemôžu podľahnúť falošnému pocitu bezpečia. Ak útočníci zatiaľ nejakú spoločnosť nezneužili, neznamená to, že sa tak v budúcnosti nestane. Kradnú používateľom prístupové údaje, ktoré sú práve cenné a požadované na čiernom trhu. **Phisher nezahŕňajú názvy značiek alebo ich variácie do doménových mien**, kvôli aktívnemu monitoringu vlastníkov značiek. Názov značky je prevažne vkladajú do podadresára alebo subdomény, kde je ťažšie odhaliteľný. Často sa stáva, že phisher útočia na určitú organizáciu napr. *Facebook*, ale pritom použijú názov inej značky napr. *Google*. Niekedy sa používateľom vyplatí všímavosť.

Doba životnosti phishingového útoku vplýva na jeho výnosnosť. Čím je útok kratšie aktívny, tým sú náklady na jeho uskutočnenie vyššie a výnos nižší. Pokiaľ používatelia nie sú ľahostajní a nahlásujú phishing, dokážu ovplyvňovať životnosť phishingu a výnosy z útoku. **Ak potrebujú útočníci predĺžiť dobu životnosti phishingových útokov zneužijú subdoménové služby.** Sú ťažšie odhaliteľné a niektoré služby umožňujú jednoduchú a bezplatnú registráciu, zatiaľ čo poskytovatelia nedisponujú účinnou metódou proti hromadnému zneužívaniu. Opakom sú útoky na zdieľané virtuálne servery, ktoré sa vyznačujú nízkou životnosťou a súčasne väčším počtom zneužitých doménových mien.

Väčšina doménových mien je získaná hackingom a s pomocou zraniteľného webhostingu. Útočníci sa uchýľujú k zraniteľným doménam najvyššej úrovne, ktorých registrátori ťažkopádne reagujú na útoky. Preto nie je žiadnou výnimkou, ak je pre útok na českých používateľov využitá napr. doména .NET (pôvodne doména založená pre sieťové technológie) namiesto .CZ. V malej miere sú v súčasnosti zužitkovávané IP adresy, skrátené URL a internacionalizované doménové mená. Homografických útokov sa zatiaľ používatelia obávať nemusia. Na základe prieskumov *Global Phishing Survey* môžeme analyzovať nielen taktiky phisherov a celosvetové trendy, ale aj zneužívanie českej, slovenskej a európskej domény. Podrobnejšie sa spomínaným doménam venujeme v nasledujúcej kapitole.

9.15 Domény .SK, .CZ a .EU vo phishingu

Na základe dát zhromaždených skupinov APWG môžeme sledovať zneužívanie domén v čase. Pre účel porovnávania domén .SK, .CZ a .EU bola vytvorená tabuľka 9.2. Pozostáva z dát týkajúcich sa spomínaných domén, ktoré boli publikované v prieskumoch *Global Phishing Survey* od začiatku roku 2008 až do konca roku 2014.

Na globálnej úrovni vidíme stále vysokú úroveň škodlivých registrácií doménových mien a subdomén pre phishingové útoky. U domén .SK, .CZ a .EU sa situácia značne odlišuje. Spomínané domény nie sú často používané k škodlivým registráciám. Najvyšším počtom škodlivých registrácií sa vyznačuje doména .EU. Jediným obdobím, kedy boli domény .EU a .CZ zneužívané k škodlivým registráciám, je obdobie pôsobenia phishingového gangu *Avalanche*. Z uvedeného vyplýva, že sú

domény používané k phishingu, získavané v prevažnej väčšine hackingom alebo prostredníctvom zraniteľného webhostingu.

Do prvého polroka 2010 sa spomínané domény pomerne často pohybovali medzi najzneužívanejšími na svete najmä podľa ukazovateľa – počet phishingových útokov na 10 000 domén v registri. Dosiahli nasledovné pozície:

- V roku 2007 získala doména .CZ 10. miesto so skóre 8.2 a doména .SK 13. miesto so skóre 7.1. Naopak doména .EU bola druhou najmenej zneužívanou doménou so skóre 0.7. (Rasmussen a Aaron, 2008a)
- V prvom polroku 2008 skončila doména .SK 14. v poradí so skóre 3.1. Zároveň subdoménová služba host.sk stala 20. najvyužívanejšou na svete, pretože obsahovala 40 phishingových stránok. (Rasmussen a Aaron, 2008b)
- Ku koncu roka 2008 obsadila doména .SK 15. miesto so skóre 5.0. (Rasmussen a Aaron, 2009a)
- V 1. polroku 2009 sa umiestnila doména .SK so skóre 7.1 na 15. mieste a doména .EU na 7. mieste so skóre 12.7. V uvedenom období bola .EU doménou s 2. najvyšším skóre ukazovateľa – počet škodlivých registrácií na 10 000 domén. (Rasmussen a Aaron, 2009b)
- Zatiaľ posledným umiestnením bolo 10. miesto domény .CZ so skóre 7.0 v prvom polroku 2010. (Aaron, Rasmussen a Routt, 2010b)

Po roku 2010 sa už žiadna zo spomínaných domén neumiestnila medzi najzneužívanejšími. Až na dve výnimky, sú všetky hodnoty ukazovateľa počet phishingových útokov na 10 000 domén nižšie ako 10. Pre domény .SK, .CZ a .EU teda pripadá na 10 000 doménových mien v registri, menej ako 10 phishingových útokov. Podrobné údaje o spomínaných doménach sa nachádzajú v tabuľke 9.2 a 9.3.

Polrok	TLD	Lokácia TLD	Počet unikátnych phishingových útokov	Unikátne doménové mená použité pre phishing	Celkový počet domén (vedených v registri)	Počet phishingových domén na 10 000 domén	Počet útokov na 10 000 domén	Doba životnosti	Medián životnosti	Počet škodlivých registrácií domén	Počet škodlivých registrácií na 10000 domén v registri
1. 2014	.SK	SR	111	72	312,160	2.3	3.6	51:41	05:53	-	-
	.EU	EÚ	547	444	3,800,500	1.2	1.4	48:43	10:01	99	0.3
	.CZ	ČR	272	168	1,132,206	1.5	2.4	41:25	12:28	1	0.0
2. 2013	.SK	SR	89	60	3,091,189	0.2	0.3	43:54	09:35	3	0.0
	.EU	EÚ	456	386	3,700,750	1.0	1.2	30:49	09:00	29	0.1
	.CZ	ČR	295	201	1,0991,320	1.8	2.7	37:45	10:08	-	-
1. 2013	.SK	SR	67	41	292,572	1.4	2.3	86:23	14:35	-	-
	.EU	EÚ	325	275	3,723,077	0.7	0.9	35:49	12:08	53	0.1
	.CZ	ČR	111	73	1,048,161	0.7	1.1	67:08	12:33	-	-
2. 2012	.SK	SR	48	30	285,222	1.1	1.7	31:40	08:12	-	-
	.EU	EÚ	443	354	3,690,729	1.0	1.2	29:02	14:00	23	0.0
	.CZ	ČR	135	97	1,004,655	1.0	1.3	24:56	15:02	-	-
1. 2012	.SK	SR	66	34	274,360	1.2	2.4	17:47	09:42	0	0.0
	.EU	EÚ	347	276	3,592,000	0.8	1.0	20:22	07:30	7	0.0
	.CZ	ČR	170	107	948,871	1.1	1.8	39:41	13:54	0	0.0
2. 2011	.SK	SR	49	32	256,849	1.2	1.9	34:42	14:52	0	0.0
	.EU	EÚ	261	188	3,503,500	0.5	0.7	49:56	12:41	9	0.0
	.CZ	ČR	171	105	871,572	1.2	2.0	41:11	14:46	1	0.0
1. 2011	.SK	SR	81	65	246,461	2.6	3.3	82:23	49:26	0	0.0
	.EU	EÚ	320	250	3,346,401	0.7	1.0	45:21	11:42	9	0.0
	.CZ	ČR	198	128	805,281	1.6	2.5	61:45	15:30	0	0.0

Tabuľka 9.2 – Údaje o doménach .SK, .CZ a .EU 2011 – 2014 (zdroj: autorka, Aaron, Rasmussen a Routt, 2011b – 2014b)

Polrok	TLD	Lokácia TLD	Počet unikátnych phishingových útokov	Unikátne doménové mená použité pre phishing	Celkový počet domén (vedených v registri)	Počet phishingových domén na 10 000 domén	Počet útokov na 10 000 domén	Doba životnosti	Medián životnosti	Počet škodlivých registrácií domén	Počet škodlivých registrácií na 10000 domén v registri
3. 2010	.SK	SR	71	27	227,664	1.2	3.1	32:24	09:17	1	0.0
	.EU	EÚ	301	220	3,248,347	0.7	0.9	64:06	10:27	26	0.1
	.CZ	ČR	222	94	732,305	1.3	3.0	64:34	12:49	2	0.0
1. 2010	.SK	SR	57	35	213,045	1.6	2.7	56:51	17:18	-	-
	.EU	EÚ	378	242	3,201,948	0.8	1.2	24:31	09:55	75	0
	.CZ	ČR	480	207	689,813	3.0	7.0	31:27	08:57	100	1
2. 2009	.SK	SR	58	26	202,000	1.3	2.9	53:51	-	0	0.0
	.EU	EÚ	28,793	1,234	3,140,216	3.9	91.7	15:59	10:56	1,070	3.4
	.CZ	ČR	207	71	624,893	1.1	3.3	46:12	-	2	0.0
1. 2009	.SK	SR	132	46	184,943	2.5	7.1	49:05	-	0	0.0
	.EU	EÚ	3,869	864	3,043,070	2.8	12.7	23:31	13:16	662	2.2
	.CZ	ČR	195	99	550,328	1.8	3.5	31:26	-	3	0.1
2. 2008	.SK	SR	87	31	172,500	1.8	5.0	48:30	-	1	0.1
	.EU	EÚ	315	234	2,988,269	0.8	1.1	53:54	-	35	0.1
	.CZ	ČR	159	111	506,258	2.2	3.1	92:12	-	33	0.7
1. 2008	.SK	SR	63	50	159,758	3.1	3.9	10:59	-	-	-
	.EU	EÚ	213	134	273,047	0.5	0.8	11:23	-	-	-
	.CZ	ČR	116	74	432,246	1.7	2.7	11:37	-	-	-
1. a 2. 2007	.SK	SR		107	150,601	7.1					
	.EU	EÚ		197	2,671,846	0.7					
	.CZ	ČR		286	347,989	8.2					

Tabuľka 9.3 Údaje o doménach .SK, .CZ a .EU od začiatku roka 2007 – 2010 (zdroj: autorka, podľa: Rasmussen a Aaron, 2008a – 2011a)

10 Zaujímavé phishingové útoky z hľadiska dôležitosti ľudského faktora

V predošlých kapitolách sme sa dozvedeli, že si používatelia všímajú určité aspekty, na základe ktorých posudzujú pravosť a dôveryhodnosť e-mailov a webových stránok. Taktiež sme sa v kapitole o opatreniach proti phishingu na strane klienta dozvedeli o určitých odporúčaní ako sa vyhnúť phishingu od skupiny APWG pre používateľov (ako napr. všímať si URL adresu, certifikát, ikonu visiaceho zámku atď.). Rozhodli sme sa analyzovať niekoľko prípadov phishingu, ktoré sa uskutočnili na území Českej a Slovenskej republiky a zhodnotiť, či by používatelia útoky odhalili, ak by sledovali relevantné aspekty a riadili sa odporúčaniami skupiny APWG. Na prípadoch je možné vidieť, či by českým a slovenským používateľom pri odhaľovaní phishingových útokov pomohla všímavosť a opatrnosť, aby sa útoku vyvarovali.

V rámci ČR a SR sa útočníci už dlhšiu dobu nezameriavajú len na klientov bánk. Čoraz častejšie sa vydávajú za nenápadnejšie zdroje, akými sú stávkové kancelárie, daňové úrady, mobilní operátori a iné organizácie. Vybrané útoky sú zaujímavé nielen napadnutými organizáciami ale aj spôsobmi prevedenia.

10.1 E-mail od Daňového úradu SR

V marci roku 2013 prišli útočníci s veľmi zaujímavým scenárom útoku a vydávali sa za *Daňový úrad SR*. V spomínanej dobe sa už *Daňový úrad SR* nazýval *Finančným riaditeľstvom SR – Sekciou daňovou*. E-mailová adresa odosielateľa nezodpovedala e-mailovej adrese daňovej sekcie s koncovkou @drsr.sk. Patřila neznámej osobe, ktorá v skutočnosti e-mail neodoslala, ale bola do záhlavia e-mailu zadaná prostredníctvom spoofingu. Útok s podobným scenárom prebiehal vo viacerých krajinách. Správa bola celá napísaná v slovenskom jazyku viz. príloha 1.

E-mail bol určený všetkým registrovaným daňovým subjektom a dôrazne upozorňoval na závažné zmeny v platení daní. Najmä skutočnosť, že všetky daňové subjekty musia uhradiť daň na jedinečné číslo účtu, ktoré je určené pre konkrétneho daňového platcu. Od roku 2012 má skutočne každý daňový subjekt na Slovensku pridelené unikátne číslo účtu. Odoslanie správy bolo perfektne načasované na obdobie,

v ktorom daňové subjekty uhrádzali dane. Spomínané skutočnosti mohli uviesť do omylu viacerých príjemcov e-mailu.

Text správy navádzal príjemcu k stiahnutiu súboru prostredníctvom uvedeného odkazu. V súbore malo byť podrobnejšie popísané jedinečné číslo účtu. V prípade, že príjemca správy súbor stiahol, nainštaloval sa mu do systému trójsky kôň s názvom Win32/Sazoor.A. Išlo o keylogger, ktorý získaval prístupové údaje do rozličných webových služieb z internetových prehliadačov *Internet Explorer*, *Google Chrome* a *Mozilla Firefox*. Údaje spoločnosti *ESET* potvrdili, že phishingovému útoku, po odhalení hrozby, podľahlo niekoľko fyzických osôb i firiem. (ESET, 2013) Vďaka protipatreniu nebol do systému týchto osôb a organizácií nainštalovaný trójsky kôň. Nie je teda vylúčené, že si spomínaný phishingový útok vyžiadal obeť i pred odhalením.

Správa obsahovala dostatočné množstvo pravdivých skutočností, ktoré dokázali niektorých príjemcov zmiasť. Bola napísaná gramaticky správne a používala oficiálny spôsob komunikácie. Pre zvýšenie dôveryhodnosti bol pridaný názov *Ministerstva financií SR* a dokonca správne číslo vyhlášky, ktorá upravuje jedinečné číslo účtu k úhrade daní. Správa zneužívala rešpekt používateľov k *Finančnému riaditeľstvu SR*. Každý príjemca, ktorého správa uviedla do omylu, určite nechcel mať problémy so spomínaným úradom, a preto poslúchol inštrukcie uvedené v správe. Pozornejší používateľ si ale mohol všimnúť detaily a usúdiť, že nejde o skutočnú správu z *Finančného riaditeľstva SR*. Nesúhlasila adresa odosielateľa. Názov úradu bol nesprávny. U vyhlášky bol uvedený pozmenený dátum účinnosti tak, aby e-mail pôsobil dôveryhodne. Navyše skutočnosť o existencii jedinečného čísla účtu daňovníka už mala byť daňovníkom známa minimálne rok. Pozorný používateľ by sa obeťou nestal ale nepozorného by neochránilo ani najlepšie antivírusové riešenie, keď ešte útok nebol zistený.

Z prípadu je možné vidieť potrebu vzdelávania zamestnancov a potrebu vedenia k zodpovednému správaniu. Jedným z možných riešení podobných útokov je projekt *PhishMe.com* (Turek, 2008), ktorý je zameraný na vzdelávanie o phishingu prostredníctvom uskutočňovania útokov. Rieši problém nevedomosti používateľov a nevnímania nebezpečenstva. Akákoľvek osoba môže prostredníctvom editora vytvoriť podvodnú webovú stránku a odoslať ju na vybrané e-mailové adresy. Systém všetko

ostatné vykoná sám a prevedie útok. Prostredníctvom fingovaného útoku je možné overiť správanie používateľov v prípade reálneho phishingového útoku.

10.2 Phishing prostredníctvom sociálnej siete

Na začiatku júna 2014 bol zaznamenaný veľmi nebezpečný phishingový útok. Pre používateľov žijúcich v Českej republike bol pomerne nový a neznámy. Podvodné správy boli zaslané používateľom sociálnej siete *Facebook* a snažili sa získať údaje o platobných kartách. Útočník k phishingu využil kontakty príjemcov. Vydával sa jedného z priateľov príjemcu a žiadal o pomoc. Poprosil o dobytie svojho účtu v stávkovej spoločnosti *Fortuna*. Zväčša išlo o nenápadne nízke čiastky ako napríklad 50 Kč. Skutočná škoda spôsobená obetiam bola však ďaleko vyššia. Útočník zaslal príjemcovi odkaz a požiadal o vyplnenie údajov potrebných pre uskutočnenie transakcie prostredníctvom platobnej karty. Pokiaľ príjemca správe uveril a údaje vyplnil, boli ihneď útočníkom zneužitú pre odcudzenie finančných prostriedkov obete. Útok pôsobil autentickejšie, pretože konverzácia prebiehala v Českom jazyku.

Pokiaľ sa pri podobných útokoch phisher neprezradí neznalosťou konkrétneho detailu a vedie bežnú konverzáciu, používateľ nezistí, že sa za profilom priateľa skrýva podvodník. Avšak v spomínanom prípade mohol všímavejší príjemca podvod odhaliť. Mnoho organizácií varuje používateľov aby si všímali odkazy, ktoré dostanú a URL adresy, na ktorých sa nachádzajú. Zaslaný odkaz pôsobil už na prvý pohľad veľmi podozrivo. Nejednalo sa o URL adresu webu stávkovej kancelárie *Fortuna*. Ak si používateľ túto skutočnosť všimol v žiadnom prípade nemal vyplňovať požadované údaje. V prílohe 2 môžete vidieť nielen časť konverzácie medzi obeťou a útočníkom ale taktiež zaslaný odkaz na podvodné webové stránky. Ďalšia možnosť, ako sa príjemca mohol vyhnúť problémom, spočívala v kontaktovaní priateľa iným spôsobom než prostredníctvom sociálnej siete napríklad telefonickým hovorom.

Veľké nebezpečenstvo vyplýva zo spôsobu prevedenia útoku. Väčšina používateľov je totiž obozretná voči externým hrozbám a e-mailom zaslaným neznámou osobou. Organizácie totiž roky upozorňujú, aby používatelia podobným správam neverili, nenavštevovali odkazy a neotvárali prílohy e-mailov od neznámych osôb. Žiadna z nich pred spomínaným útokom nevarovala používateľov pred phishingom

prostredníctvom priateľov na sociálnej sieti. Viaceré inštitúcie zareagovali vytvorením vzdelávacích stránok pravdepodobne až potom, keď sa obeťami útoku stali ich klienti.

Útok prostredníctvom Facebooku nebol jediným scenárom. Ďalší sa zameral na zákazníkov stávkových spoločností. Bol uskutočnený prostredníctvom falošnej internetovej reklamy na weboch stávkových spoločností ako napríklad *Synotip*, či *Fortuna*. Reklama bola atraktívna a ponúkala zákazníkovi možnosť dostať finančný bonus. Pre získanie bonusu bolo potrebné navštíviť uverejnený odkaz na webové stránky a zaregistrovať svoju platobnú kartu. Keď používateľ vyplnil požadované údaje, nielenže nedostal žiaden bonus, ale jeho platobná karta bola zneužitá. Scenár útoku nie je žiadnou novinkou, skôr ide o typický sociálny trik používaný pre zmätenie obetí. V cudzojazyčnom prevedení sa objavuje už niekoľko rokov. Používatelia mali byť schopní spomínaný útok rozpoznať.

10.3 Phishingový e-mail upozorňujúci na dlh

Na konci apríla sa v ČR objavila veľká záplava phishingových e-mailov, ktoré sa snažili príjemcov presvedčiť o existencii dlhu. Dlžná čiastka mala podľa textu správy vzniknúť používaním produktu banky. Útočník uviedol presnú dlžnú čiastku, číslo účtu, na ktorom mala vzniknúť a taktiež dátum splatnosti. E-mail príjemcov nabádal k uhradeniu dlhu kvôli zachovaniu pozitívnej úverovej histórie. Taktiež preto, aby sa príjemcovia vyhli súdnym sporom, plateniu poplatkov a vzniku ďalších súdnych nákladov.

Kópia zmluvy a platobné údaje mali byť uvedené v prílohe. Správa mala v príjemcoch vzbudiť zvedavosť, aby následne otvorili priložený súbor. Prílohou správy bol spustiteľný súbor, ktorý bol vydávaný za súbor .ZIP (formát súboru). Išlo o trójskeho koňa. Ak používateľ prílohu otvoril, nainfikoval si počítač a trójsky kôň začal sťahovať do počítača ďalší malware. Na dôveryhodnosti mal správe pridať názov oddelenia, meno zodpovednej osoby a telefónny kontakt. Phisherí uviedli telefónne číslo skutočnej osoby, ktorá o zneužití svojho čísla najprv vôbec netušila.

Phishingové e-maily sa odlišovali e-mailovou adresou odosielateľa, číslom osobného účtu, číslom zmluvy, dlžnou čiastkou, dátum splatnosti, zodpovednou osobou a uvedeným telefónnym číslom. Príjemcovia e-mailu, ktorí nepochopili, že je e-mail podvodný, sa pokúšali uvedenú osobu kontaktovať prostredníctvom odpovede na e-mail

alebo pomocou telefónneho čísla. Text jednej zo spomínaných správ nájdete ako prílohu 3.

Útok bol menej prepracovaný, pretože správa nebola napísaná gramaticky a štylisticky správne. Používatelia si už zvykli na to, že väčšina phishingu sa vyznačuje gramatickými chybami, prípadne nezmyselným textom. Už len z toho dôvodu by príjemcovia mali vyhodnotiť e-mail ako podvodný. Nápadná bola aj adresa odosielateľa, ktorá nesúhlasila so žiadnou e-mailovou adresou banky. V texte nebola ani zmienka o názve banky. Správa na rozdiel od ostatných lepšie pripravených útokov neobsahovala ani žiadnu firemnú grafiku. Išlo o prostý text. E-mail nebol rozosielaný len v apríli a niektorí používatelia ho dokonca dostali opakovane. Po odhalení útoku začali určité antivírusové programy detekovať prílohu emailu ako vírus a príjemcovia nedokázali prílohu vôbec otvoriť.

10.4 Veľká phishingová kampaň

Veľká phishingová kampaň – i takto boli označované útoky, ktoré sa odohrali na Slovensku pred polovicou júla 2014 a boli zamerané najmä na používateľov elektronického bankovníctva. Veľkosť a rozsiahlosť útokov spočívala najmä v zameraní na klientov rozličných bánk pôsobiacich v SR a ČR. Phishing zaznamenala *Slovenská sporiteľňa*, *Prima banka*, či *Poštová banka*.

Účelom útokov bolo získanie prístupových údajov do elektronického bankovníctva. Správy vyzerali ako oficiálne e-maily bánk a v predmete mali napísané slovo Poplach. Za odosielateľa boli vydávané neexistujúce doménové mená veľmi podobné skutočným doménam jednotlivých bánk. Telo správy obsahovalo upozornenie na doručenie jednej novej správy od banky. Text bol strohý. E-mail obsahoval podvrhnutý odkaz na prihlásenie sa do elektronického bankovníctva, ktorý používateľov presmeroval na poľskú doménu drl.pl. Podvodné správy neboli účinné, pretože ich phisher odosielať na všetky získané adresy. Príjemcovia tak dostávali e-maily od bánk, v ktorých nemali zriadený účet. Niekoľko hodín po odoslaní e-mailov bola podvodná webová stránka a celá doména zablokovaná. Banky reagovali na útok upozornením na svojich webových stránkach. *Prima banka* dokonca rozosielať svojim klientom i informačné SMS.

V ČR phisherí zaútočili s podobným phishingovým e-mailom s takmer totožným strohým textom dokonca opakovane. Konkrétne sme si pre analýzu vybrali phishingový e-mail, ktorý mala odoslať ČSOB (*Československá obchodná banka*) banka. E-mail bol napísaný v českém jazyku a tiež upozorňoval na novú správu z bezpečnostného centra banky. Už samotný predmet správy vyzeral veľmi podozrivo a znel „Poplach centrum“. Išlo o nezmyselné slovné spojenie, ktoré mohlo príjemcovi naznačiť, že je email podvodný. Emailová adresa odosielateľa obsahovala názov banky, čo mohlo niektorých príjemcov zmiatať. Uvedená adresa, ale nezodpovedala skutočnej adrese ČSOB banky. Na začiatku správy sa, na rozdiel od slovenskej verzie, nachádzalo oslovenie „Vážený zákazník“.

E-mail upozorňoval príjemcov na správu z bezpečnostného centra banky a obsahoval hypertextový odkaz, ktorý mal príjemcom umožniť prístup k elektronickému bankovníctvu. URL adresa, na ktorú odkaz príjemcov správy presmeroval, sa jednotlivých e-mailov použitých v ČR odlišovala. Pokiaľ by sa bol používateľ nastavil kurzorom myši na odkaz, videl by, že URL adresa nezodpovedá adrese banky. Taktiež to príjemcovia mohli vidieť v prípade, ak na odkaz klikli a webovú stránku navštívili. Vzhľad webu bol na nerozoznanie od skutočného webu ČSOB. Z podvrhutej stránky a pohľadu do adresného riadka prehliadača bolo však jasné, že nejde o zabezpečené pripojenie. V adresnom riadku sa nezobrazovala ani ikona visiaceho zámku. Banky svojich klientov dlhodobo varujú, aby si všímali pri prihlasovaní do elektronického bankovníctva zabezpečené pripojenie prostredníctvom https v adresnom riadku, taktiež ikonu visiaceho zámku a platnosť certifikátu. Pokiaľ by príjemca dodržiaval spomínané pravidlá, všimol by si útok najneskôr pri návšteve webových stránok. Ukážky oboch uvedených správ i podvodnej webovej stránky sú súčasťou práce ako prílohy 4 – 6.

10.5 Zhodnotenie prípadov

Pri všetkých spomínaných útokoch sa mohol používateľ brániť. Phisherí nevytvorili natoľko prepracované útoky, že by sa nedali odhaliť. Obsahovali detaily i významnejšie znaky, z ktorých bolo možné vydedukovať, že ide o podvod. **Všímavosť, opatrnosť a znalosti o phishingu sú u českých a slovenských používateľov veľmi dôležité. Ak by venovali útokom dostatočnú pozornosť, dokázali by ich odhaliť. Zatiaľ čo phisherí ovplyvňujú úspešnosť phishingu**

kvalitou pripravených útokov, používatelia dokážu úspešnosť ovplyvniť svojou všímavosťou, opatrnosťou a správaním útok odhaliť a zmariť. Lenže z ľudskej povahy vyplýva omylnosť. Niektorí bežní používatelia trpia nevedomosťou, nepozornosťou a nevšímavosťou. Dokonca nevnímajú ani nebezpečenstvo vo virtuálnom svete. Preto nie je žiadnou výnimkou ak e-mail a webové stránky, ktoré vykazujú znaky podvodu, považujú za legitímne. Navyše phisher tvoria útok tak, aby obsahoval rôzne sociálne a technické triky zavádzajúce používateľa. Zakomponovávajú do útokov prvky, ktorými sa snažia otupiť všímavosť, pozornosť a spôsobiť u používateľa pocit bezpečia, strachu, rešpektu alebo hnevu. Phishing zostáva bojom medzi útočníkom snažiacim sa oklamať zmysly používateľa a vytvoriť dôveryhodný umelý kontext a medzi všímavosťou, pozornosťou a znalosťami bežného používateľa. V tomto boji rozhodne používateľovi nepomáha ani fakt, že v prípade niektorých útokov najprv koná a až následne, najmä keď je už neskoro, premýšľa. Skôr než zbrklo zareaguje, mal by zvážiť všetky okolnosti a dôsledky svojho konania. Inak sa stane obeťou útoku. Úloha uvedomelého a pozorného používateľa, nekončí pri odhalení phishingového útoku. Je dôležité, aby phishing nahlásil. Čím skôr je útok nahlásený, tým viac sa skrátí jeho životnosť a teda aj výnosy phisherov. Zároveň pomôže ďalším menej všímavým a nevedomým používateľom.

11 Výskum

Vybrané poznatky zistené v predošlých kapitolách práce sme sa rozhodli overiť empirickým výskumom. Zamerali sa najmä na overenie zistení o opatreniach proti phishingu a aspektoch dôveryhodnosti a pravosti e-mailov a webových stránok. Keďže sme sa dozvedeli, že jedným z opatrení proti phishingu je budovanie a zvyšovanie povedomia o phishingu a ochrane proti nemu, snažili sme sa u českých a slovenských používateľov overiť úroveň povedomia o phishingu. Taktiež sme zisťovali, či si používatelia všímajú snahy organizácií o zvyšovanie povedomia o phishingu, ktoré organizácie uskutočňujú prostredníctvom vzdelávacích kampaní, akcií, videí ale taktiež varovaní o phishingových útokoch. Overovali sme, či používatelia využívajú technologické opatrenia v podobe antivírusového programu a antiphishingového nástroja, ktoré sme spomenuli v rámci kapitoly o obranných mechanizmoch. Zisťovali sme, či sa používatelia správajú podľa odporúčaní od skupiny APWG, ako sa vyhnúť phishingu a či dodržiavajú bezpečnostné zásady, ktoré sme uviedli. V rámci kapitoly o dôvodoch fungovania phishingu sme sa dozvedeli, že používatelia sledujú určité vybrané aspekty u e-mailov a webových stránok a na základe nich určujú pravosť a dôveryhodnosť. Zistili sme však i to, že sa používatelia skôr sústredia na obsah a vizuálne prvky, než na bezpečnostné znaky a tak sme sa túto skutočnosť rozhodli overiť i na českých a slovenských používateľoch. Empirický výskum i všetky zistenia výskumu sú uvedené v rámci kapitoly 11.

11.1 Metodika výskumu

K empirickému výskumu bola v diplomovej práci použitá metóda dotazníkového šetrenia. Pre účel výskumu bol vytvorený a použitý elektronický dotazník. Bližší popis dotazníka, ako aj priebeh dotazníkového šetrenia sa nachádza v nasledujúcej kapitole.

11.2 Dotazník a priebeh šetrenia

Dotazník sme vytvorili prostredníctvom formulára v službe *Google Disk*. Do nového formulára boli postupne pridávané otázky a nakoniec grafická šablóna. Odpovede respondentov sa zaznamenávali do tabuľky v dokumente, ktorý bol automaticky vytvorený a umiestnený na *Google Disku*. Respondentom bol dotazník zaslaný prostredníctvom odkazu.

Cieľom dotazníka bolo zistiť, aké sú osobné skúsenosti a povedomie českých a slovenských používateľov o phishingu, aké sú bezpečnostné návyky českých a slovenských používateľov a ktoré aspekty dôveryhodnosti berú v úvahu pri posudzovaní phishingu aj legítimných e-mailov a webových stránok.

Otázky v dotazníku boli vytvorené na základe poznatkov obsiahnutých v teoretickej časti práce a získaných pri štúdiu problematiky phishingu. Štruktúra dotazníka pozostávala zo štyroch častí. **Prvá časť** bola zameraná na povedomie českých a slovenských používateľov o phishingu a ich osobné skúsenosti s phishingom. Snažila sa zistiť, či sa používatelia cítia pri vykonávaní bežných činností bezpečne, poznajú pojem phishing, opatrenia na ochranu pred phishingom aj spôsob ako phishing nahlásiť. **Druhá časť** dotazníka sa zaoberá dodržiavaním bezpečnostných opatrení používateľmi. Aplikácia opatrení síce celkom neodstráni hrozbu phishingu, ale môže používateľom do značnej miery pomôcť. Preto nás zaujímalo, či českí a slovenskí používatelia využívajú bezpečnostný softvér, antiphishingové riešenie a celkovo, či sa správajú bezpečne. **Tretia časť** preveruje aspekty dôveryhodnosti, ktoré berú používatelia v úvahu pri posudzovaní pravosti e-mailov a webových stránok. **Štvrtá časť** obsahuje demografické otázky, ktoré zisťujú pohlavie, vek, krajinu pobytu, študijné a pracovné zameranie respondentov.

Dotazník obsahoval **32 otázok** a všetky boli pre respondentov povinné. Z celkového počtu otázok boli 4 polouzavreté a 28 uzavretých. Len jedna podotázka bola otvorená a používatelia v nej boli vyzvaní, aby napísali aspoň jedno opatrenie proti phishingu, ktoré dodržiavajú. U každého respondenta bola zaznamenaná špecifická časová pečiatka, pomocou ktorej mohol byť identifikovaný.

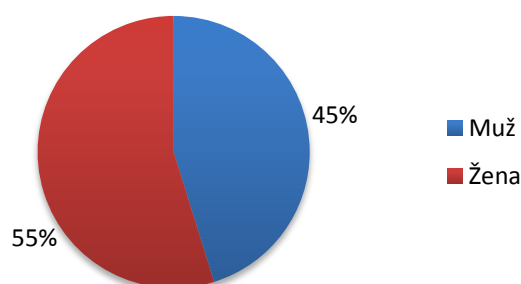
Dotazník sa stal prístupným dňa 31. októbra 2014 a šetrenie prebiehalo až do 23. novembra 2014. Celkovo bol elektronický dotazník aktívny počas 24 dní. Pred rozoslaním dotazníka sa najprv uskutočnila kontrola zrozumiteľnosti dotazníka na vzorke 15 respondentov. Respondenti boli oslovovaní osobne, prostredníctvom e-mailov a správ zaslaných na sociálnej sieti Facebook. Odpovede boli zaznamenávané a po ukončení dotazníka analyzované a vyhodnotené.

11.3 Súbor respondentov

Dotazník sa zameriaval na respondentov, ktorí sú používateľmi e-mailu a internetu a zároveň majú viac ako 18 rokov. S prosbou o vyplnenie bolo oslovených 548 respondentov. Dotazník vyplnilo 354 osôb, čo predstavuje 64,6 % zo všetkých oslovených. Z nižšie uvedenej tabuľky 11.1 a grafu 11.1 je možné vidieť, že ženy predstavovali 55 % respondentov, zatiaľ čo muži 45 %.

Pohlavie	Počet respondentov
Muž	160
Žena	194

Tabuľka 11.1 – Rozdelenie respondentov z hľadiska pohlavia (zdroj: autorka)

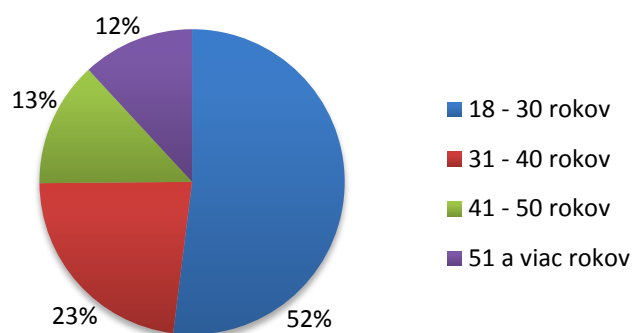


Graf 11.1 – Rozdelenie respondentov podľa pohlavia (zdroj: autorka)

Z hľadiska veku bolo dotazníkové šetrenie zamerané na osoby staršie ako 18 rokov. Najpočetnejšou vekovou skupinou bola skupina s vekom 18 – 30 rokov, ktorá tvorila 52 % všetkých respondentov. O niečo menšou bola skupina 31 – 40 rokov s 23 % opýtaných. Najmenší podiel predstavovali vyššie vekové kategórie.

Vek	Počet respondentov
18 – 30 rokov	184
31 – 40 rokov	81
41 – 50 rokov	47
51 a viac rokov	42

Tabuľka 11.2 – Rozdelenie respondentov z hľadiska veku (zdroj: autorka)

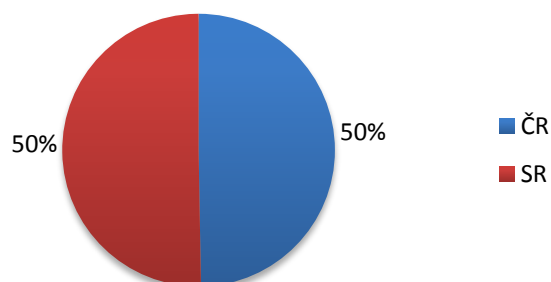


Graf 11.2 – Rozdelenie respondentov podľa veku (zdroj: autorka)

Dotazník vyplnilo 176 respondentov z Českej republiky a 178 respondentov zo Slovenskej republiky. Podiel respondentov z oboch krajín bol približne rovnaký 50 %.

Krajina pobytu	Počet
ČR	176
SR	178

Tabuľka 11.3 – Rozdelenie respondentov na základe krajiny pobytu (zdroj: autorka)

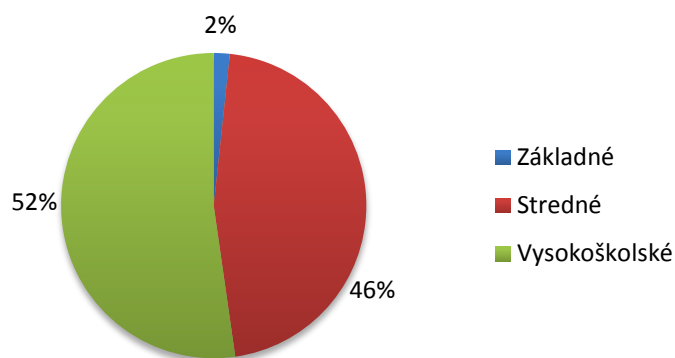


Graf 11.3 – Rozdelenie respondentov na základe krajiny pobytu

Otázky z dotazníka vyplnilo iba 2 % respondentov so základným vzdelaním. Osoby s vysokoškolským vzdelaním tvorili 52 % a so stredným vzdelaním 46 %.

Najvyššie dosiahnuté vzdelanie	Počet respondentov
Základné	6
Stredné	163
Vysokoškolské	185

Tabuľka 11.4 – Rozdelenie respondentov z hľadiska najvyššieho dosiahnutého vzdelania
(zdroj: autorka)

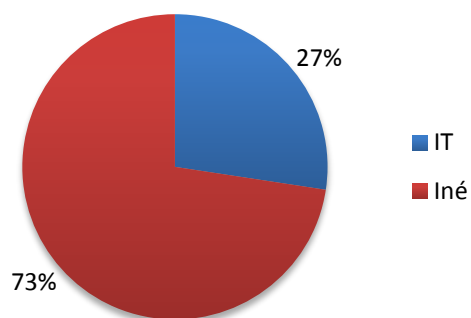


Graf 11.4 – Rozdelenie respondentov z hľadiska najvyššieho dosiahnutého vzdelania
(zdroj: autorka)

Z nasledujúcich tabuliek je možné vidieť, že otázky dotazníka zodpovedalo 27 % respondentov so študijným zameraním IT (Information technology) a 20 % osôb s pracovným zameraním IT.

Študijné zameranie	Počet respondentov
IT	97
Iné	257

Tabuľka 11.5 – Rozdelenie respondentov podľa študijného zamerania (zdroj: autorka)

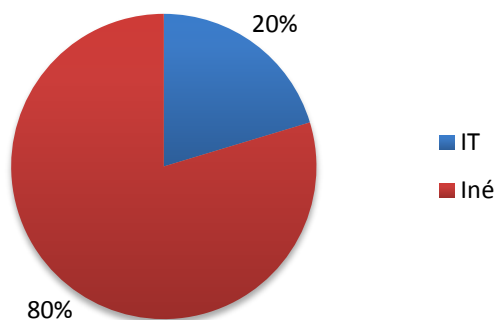


Graf 11.5 – Rozdelenie respondentov podľa študijného zamerania (zdroj: autorka)

Zo všetkých respondentov malo 66 osôb študijné a zároveň pracovné zameranie IT. Šesť respondentov vyštudovalo iný odbor, ale v súčasnosti pracuje v oblasti IT a 31 odpovedajúcich má iné pracovné zameranie, ale študovalo IT.

Pracovné zameranie	Počet respondentov
IT	72
Iné	282

Tabuľka 11.6 – Rozdelenie respondentov na základe pracovného zamerania (zdroj: autorka)



Graf 11.6 – Rozdelenie respondentov na základe pracovného zamerania (zdroj: autorka)

11.4 Výskumné hypotézy

V rámci výskumu sme stanovili štyri nasledovné hypotézy:

- **Hypotéza 1:** „Existuje závislosť medzi znalosťou opatrení proti phishingu a študijným a pracovným zameraním respondentov.“

- **Hypotéza 2:** „Jestvuje závislosť medzi znalosťou opatrení a pohlavím respondentov.“
- **Hypotéza 3:** „Existuje závislosť medzi krajinou pobytu respondentov a tým, či považujú phishing za reálnu hrozbu v Českej a Slovenskej republike.“
- **Hypotéza 4:** „Používatelia, ktorí majú aspoň jedno zo zameraní IT sledujú pri e-mailoch a webových stránkach viac relevantných znakov než bežný používatelia.“

Uvedené hypotézy sme overovali po ukončení a vyhodnotení dotazníkového šetrenia prostredníctvom štatistických metód.

11.5 Reflexia možných skreslení

Dotazník bol predložený menšej skupine respondentov ku kontrole zrozumiteľnosti, i tak je možné, že u niektorých respondentov došlo k nepochopeniu niektorých otázok a teda aj k zakresleniu výsledkov. Kontrolou zrozumiteľnosti otázok a jednotlivých odpovedí by malo byť možné skreslenie výrazne obmedzené. Nemôžeme ho ale úplne vylúčiť.

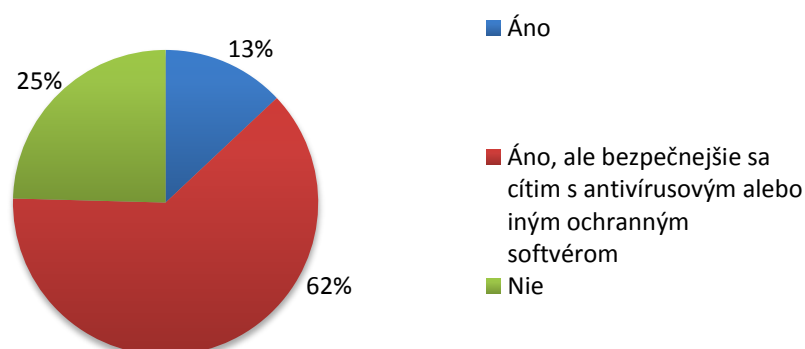
V úvode dotazníka bol vysvetlený základný pojem – phishing. Pri tvorbe dotazníka sme vzali v úvahu, že niektorí používatelia nemusia tento pojem poznať, čo by výrazne skreslilo výsledky.

Ďalším faktorom, ktorý mohol spôsobiť skreslenie, je okruh známych osôb a priateľov. Spomínaný faktor bolo zložité obmedziť, pretože známe osoby a priatelia boli oveľa ochotnejší zodpovedať otázky dotazníka než neznáme osoby.

11.6 Spracovanie a interpretácia dát

Ako už bolo spomínané dotazník je rozdelený do štyroch hlavných častí. Prvá časť otázok sa zameriava na povedomie o phishingu u českých a slovenských používateľov a zahŕňa otázky jedna až osem. Deviatou otázkou začína ďalšia časť dotazníka zameraná na dodržiavanie opatrení a bezpečnostné návyky používateľov. Otázky 21 až 26 zisťujú aspekty dôveryhodnosti a pravosti sledované používateľmi. Posledných šesť otázok je demografických.

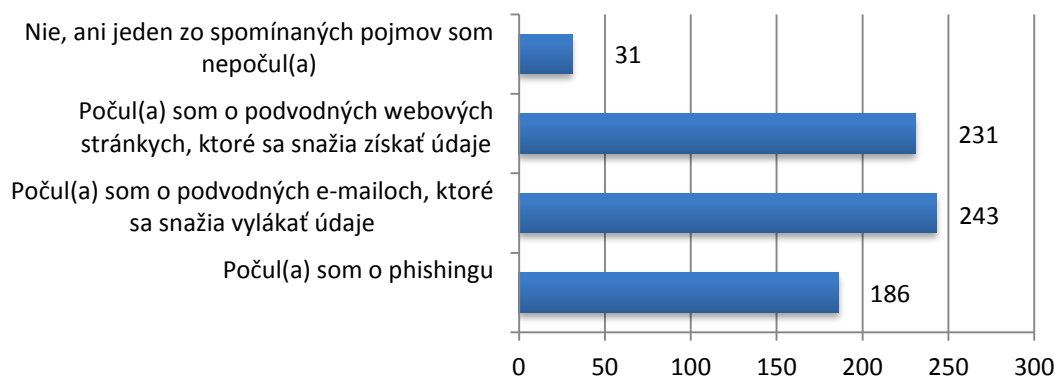
Prvá otázka zisťovala, či majú používatelia **pocit bezpečia pri vykonávaní bežných činností vo virtuálnom svete**. Pod bežnými činnosťami si môžeme predstaviť odosielanie a prijímanie e-mailov, nakupovanie prostredníctvom e-shopov, prehliadanie webových stránok, uskutočňovanie transakcií prostredníctvom elektronického bankovníctva atď.. Iba 13 % (46) respondentov sa cíti bezpečne, zatiaľ čo 25 % (87) opýtaných sa necíti bezpečne. Najväčší podiel respondentov – 62 % (221), sa síce cíti bezpečne, ale ich pocit bezpečia je silnejší v prípade použitia antivírusového alebo iného ochranného softvéru. Pocit bezpečia má výrazný vplyv na obozretnosť a opatrnosť používateľov. Čím sa cítia používatelia bezpečnejšie, tým menej sú obozretní voči všetkým nástrahám číhajúcim vo virtuálnom svete. Mitnick a Simon (2003) hovoria, že s využívaním antivírusu u používateľov vzniká falošný pocit bezpečia. Odpovede respondentov jeho názor potvrdzujú. Antivírus je nápomocný, vždy je dobré mať ho nainštalovaný, ale v niektorých prípadoch nemusí pomôcť a hrozbu odhaliť. Preto by mali byť používatelia obozretnejší a premyslieť si svoje konanie.



Graf 11.7 – Pocit bezpečia pri vykonávaní bežných činností vo virtuálnom svete (zdroj: autorka)

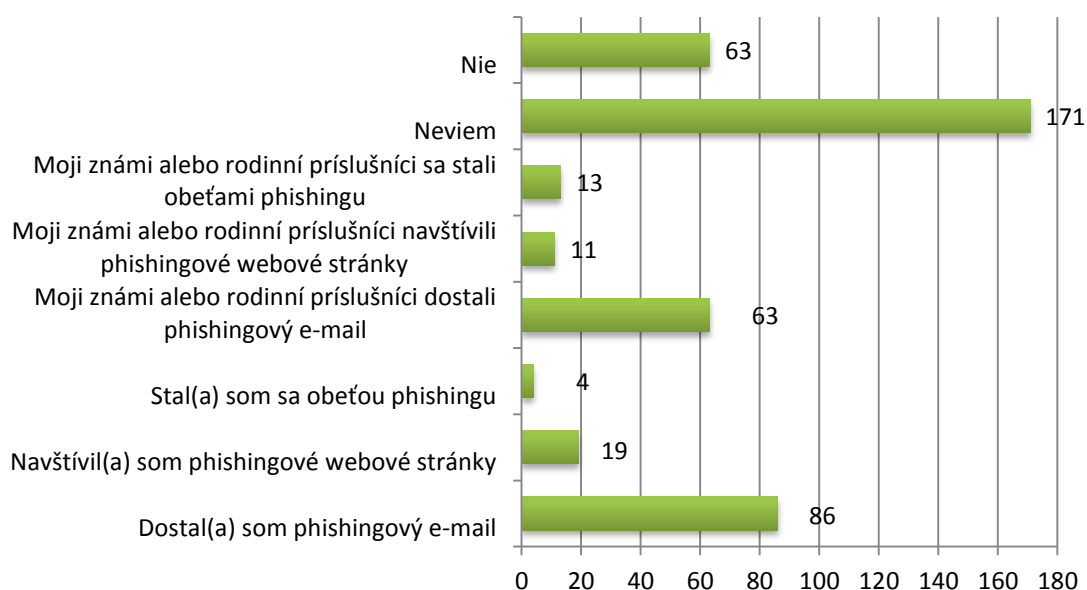
Prostredníctvom druhej otázky sme sa snažili zistiť, či **počuli používatelia v ČR a SR o phishingu, podvodných e-mailoch alebo podvodných webových stránkach, ktoré sa snažia získať osobné údaje**. Najviac 243 (69 % zo všetkých) opýtaných zaznamenalo pojem podvodný e-mail a 231 (65 % zo všetkých) respondentov počulo o podvodných webových stránkach. So slovom phishing sa stretlo 186 (53 % zo všetkých) opýtaných. Skôr než pôvodný pojem phishing teda obyvatelia ČR a SR poznajú podvodné e-maily a webové stránky. Ani jeden zo spomínaných pojmov nezaregistrovalo 31 (9 % zo všetkých opýtaných) respondentov. Veľmi zaujímavé je percento respondentov, ktorí používajú e-mail a internet, ale o podobných nástrahách

vôbec nepočuli. Najmä vzhľadom k súčasnej situácii a častému výskytu phishingu v ČR a SR.



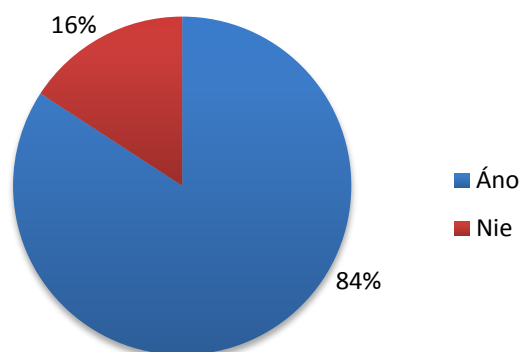
Graf 11.8 – Povedomie o phishingu, podvodných e-mailoch a webových stránkach (zdroj: autorka)

Tretia otázka bola položená s cieľom zistiť **osobné skúsenosti s phishingom u českých a slovenských používateľov**. Otázku nevedelo zodpovedať až 171 (48 % zo všetkých) respondentov. Osobnú skúsenosť s phishingom nemá 63 (18 % všetkých) opýtaných. Phishingový e-mail dostalo 86 respondentov, phishingové webové stránky navštívilo 19 respondentov a obeťou phishingu sa stali 4 respondenti. Phishingový e-mail prišiel známym a rodinným príslušníkom 63 opýtaných. Niekoľko zo známych a rodiny 11 respondentov navštívilo phishingové webové stránky. Presne 13 respondentov potvrdilo, že ich známy alebo rodinný príslušník sa stal obeťou phishingu. Štyria opýtaní uviedli, že sa stali obeťou phishingu, čo je vzhľadom na reakcie obetí uvedené v predchádzajúcej časti veľmi zaujímavé. Používatelia sa zväčša hanbia a ťažko si priznávajú svoju zraniteľnosť. Cítia sa nahnevaní, oklamaní a nechcú si priznať, že sa práve oni mohli stať obeťou, preto sú výsledky prekvapivé. Skôr sme očakávali, že všetky obeť označia odpoveď – áno, moji známi alebo rodinní príslušníci sa stali obeťami phishingu namiesto odpovede – áno, stal(a) som sa obeťou phishingu.



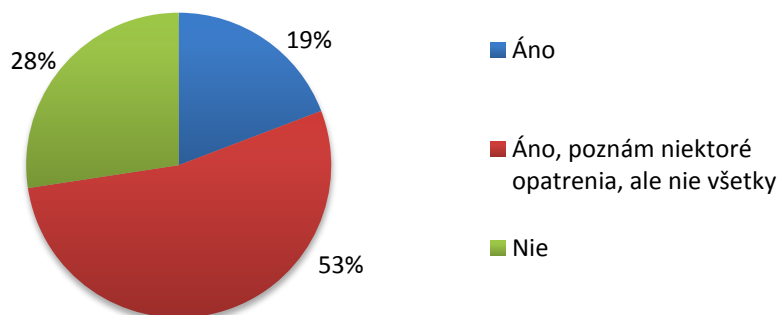
Graf 11.9 - Osobné skúsenosti používateľov s phishingom (zdroj: autorka)

Štvrtá otázka zisťovala, či **používatelia v Českej a Slovenskej republike považujú phishing za reálnu hrozbu**. Phishing je skutočnou hrozbou v Českej a Slovenskej republike podľa 84 % (298) respondentov. Naopak 16 % (56) opýtaných si nemyslí, že phishing predstavuje v ČR a SR nebezpečenstvo. Pravdepodobne ide o osoby, ktoré nemajú s phishingom vlastnú skúsenosť, o phishingu nepočuli alebo o osoby, ktoré používateľov považujú za odolných voči útokom. Phishing je na území ČR a SR skutočnou hrozbou. Niektoré útoky sú vytvorené v spisovnom jazyku, používajú nové taktiky, scenáre, triky a sú oveľa ťažšie rozpoznateľné. Každý mesiac prichádza niekoľko nových phishingových útokov a phishing sa stáva čoraz nebezpečnejším.



Graf 11.10 – Reálnosť hrozby phishingu v ČR a SR podľa používateľov (zdroj: autorka)

Piata otázka zisťovala **znalosť bezpečnostných opatrení proti phishingu používateľmi v ČR a SR**. Z opýtaných si 19 % (68) osôb myslí, že pozná opatrenia proti phishingu a naopak 28 % (97) opýtaných nevie, ako sa proti phishingu brániť. Najväčšia skupina respondentov, ktorá sa na celkovom počte podieľala 53 % (189), pozná niektoré bezpečnostné opatrenia. Zarážajúca je veľkosť podielu osôb, ktoré nepoznajú opatrenia proti phishingu. Často sú zdôrazňované v médiách a na webových stránkach bánk, spoločností vytvárajúcich antivírusový softvér alebo vo vzdelávacích kampaniach a materiáloch.



Graf 11.11 – Znalosť opatrení proti phishingu (zdroj: autorka)

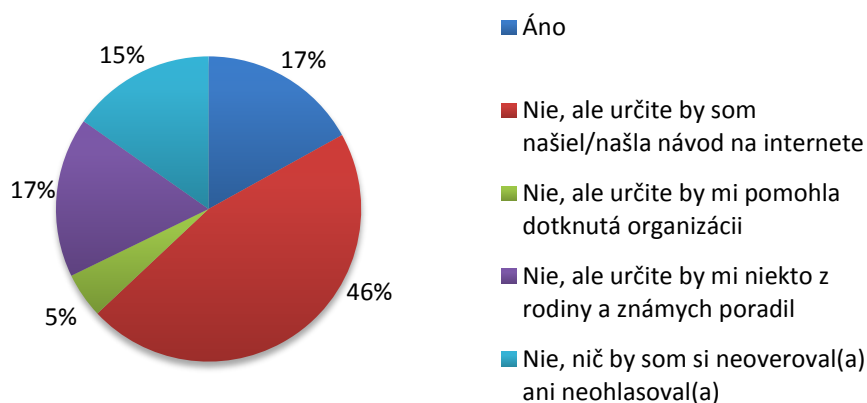
Respondenti so znalosťou opatrení a znalosťou niektorých opatrení proti phishingu boli následne požiadaní o napísanie aspoň jedného opatrenia, ktoré sami dodržiavajú. Na otázku odpovedalo 257 respondentov. Vyplnené opatrenia a počty respondentov, ktoré opatrenia napísali sú uvedené v tabuľke 11.7.

Odpoveď	Počet respondentov
Antivírus	92
Neposkytovať svoje údaje	35
Neodpovedať a nereagovať na podozrivé e-maily	30
Neotvárať e-maily od neznámych osôb	27
Kontrolovať zabezpečené pripojenie	25
Neklikovať na podozrivé a neznáme odkazy	24
Neotvárať podozrivé e-maily	21
Nenavštevovať podozrivé webové stránky	19
Kontrolovať certifikát	17
Navštevovať iba overené webové stránky	16
Antispamový filter	11
Skontrolovať URL adresu	11
Premýšľať	9
Antispyware	9
Opatrnosť	8
Aktualizácie	8
Ochrana proti phishingu	8
Nezverejňovanie údajov	8
Prihlasovanie do elektronického bankovníctva na vlastnom PC	8
Neotvárať prílohy podozrivých e-mailov	7
Nedôverovať všetkému	7
Neinštalovať neznámy softvér	7
Silné heslo	7
Firewall	6
Overiť si odosielateľa na internete	6
Zadávať názov stránok ručne	6
Nesťahovať neznáme súbory	5
Skontrolovať odosielateľa	4
Dvojfázové overenie	4
Kontrolovať ikonu visiaceho zámku v adresnom riadku	3
Kontrolovať hlavičku e-mailu	3
Nečítať Spam	2
Často si meniť heslo	2
Používať oficiálnu aplikáciu internetového bankovníctva	2
Elektronický osobný kľúč	1
Mazať históriu prehliadača	1
Používať inkognito karty	1
Skontrolovať presmerovanie	1

Tabuľka 11.7 – Opatrenia proti phishingu, ktoré respondenti dodržiavajú (zdroj: autorka)

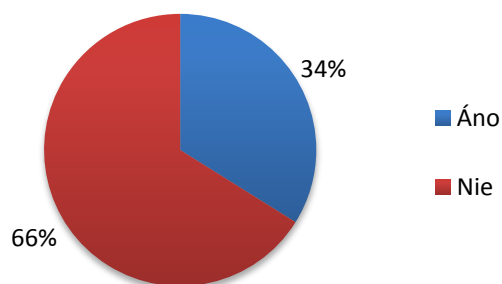
Najčastejšou odpoveďou bol antivírusový program, ktorý napísalo 92 respondentov. Väčšie skupiny respondentov (obsahujúce viac ako 20 respondentov) uviedli, že neposkytujú svoje údaje, neodpovedajú a nereagujú na podozrivé e-maily, neotvárajú e-maily od neznámych osôb, kontrolujú zabezpečené pripojenie, neklikajú na podozrivé a neznáme odkazy a neotvárajú podozrivé e-maily.

V šiestej otázke sme sa pýtali, **či si používatelia vedia overiť a nahlásiť phishingový e-mail alebo webové stránky**. Možnosť áno vybralo 17 % (60) respondentov. Najviac – 46 % (163) respondentov by hľadalo návod na internete. Iba 5 % (17) opýtaných by sa obrátilo so žiadosťou o pomoc na dotknutú organizáciu a 17 % (60) by si nechalo poradiť rodinným príslušníkom alebo známym. Veľmi nízky počet respondentov by kontaktoval dotknutú organizáciu, aj napriek tomu ako napr. banky zdôrazňujú klientom aby phishing nahlasovali a v prípade podozrenia banku kontaktovali. Dokonca ponúkajú aj návod, prípadne e-mailovú adresu pre nahlásenie útoku. Zvyšných 15 % (54) opýtaných by e-mail alebo webové stránky ani neoverovalo, ani neohlasovalo. Ako bolo spomínané v predošlej časti práce o dobe životnosti phishingu, nahlasovanie útokov je veľmi dôležité, dokáže značne ovplyvniť dobu životnosti útokov a výnosy z phishingu. Práve preto by ho používatelia nemali ignorovať. Pomáhajú prostredníctvom ohlásenia ďalším používateľom, ktorí môžu byť včas pred útokom varovaní alebo sú na základe nahlásenia útoku vytvorené opatrenia, ktoré zabránia ďalším obetiam. Ak napríklad nahlásia phishingový e-mail používatelia služby Gmail, správa sa už nezobrazí ďalším príjemcom.



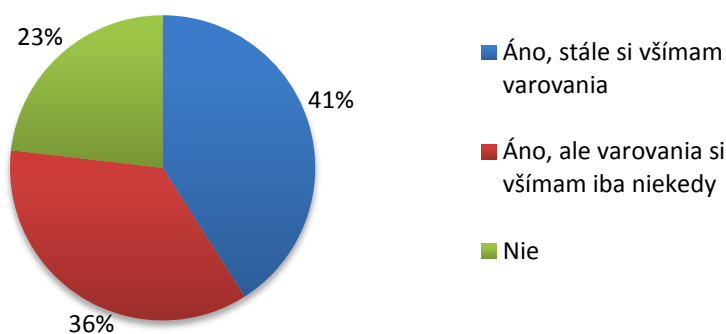
Graf 11.12 – Vedia používatelia overiť a nahlásiť phishing (zdroj: autorka)

Rôzne organizácie sa snažia svojich klientov ochrániť a predchádzať škodám z phishingu pomocou preventívnych opatrení v podobe vzdelávania. Všimli si však používatelia túto iniciatívu? V siedmej otázke sme sa preto pýtali, **či respondenti zaznamenali za posledných 12 mesiacov vzdelávaciu kampaň, materiál, video a webovú stránku o phishingu a obrane proti nemu**. Iba 34 % (120) respondentov, ktorí si všimli vzdelávaciu kampaň, materiál, video alebo web o phishingu. Väčšina respondentov až 66 % (234) nič podobného nezaznamenali.



Graf 11.13 – Pomer používateľov, ktorí zaznamenali a nezaznamenali v posledných 12 mesiacoch vzdelávaciu kampaň, materiál, video a webovú stránku o phishingu (zdroj: autorka)

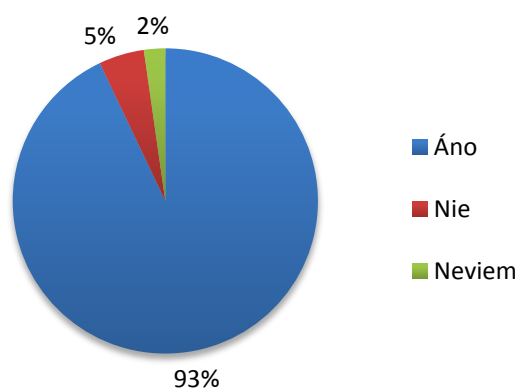
S každým uskutočneným phishingovým útokom sa objavujú varovania jednak v médiách, na stránkach bánk a organizácií, ktoré sa snažia upozorniť na konkrétny phishingový útok a jeho prevedenie. Podobné varovania sa zobrazujú na stránkach pre prihlasovanie do elektronického bankovníctva. Študenti môžu upozornenie na phishingové emaily vidieť v ISISe (Integrated Study Information System). **Prostredníctvom ôsmej otázky sme zisťovali, či používatelia upozornenie všímajú alebo nie.** Spomínané varovania si stále všíma 41 % (145) respondentov a 36 % (127) respondentov ich zachytí niekedy. Upozornenia ignoruje 23 % (82) opýtaných.



Graf 11.14 – Sledovanie varovaní používateľmi (zdroj: autorka)

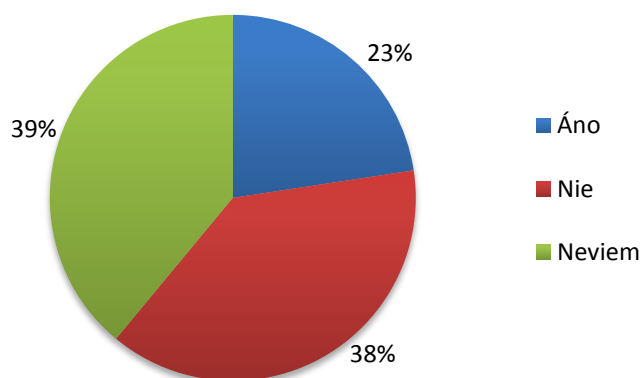
Deviata otázka preverovala, či majú používatelia na svojich zariadeniach nainštalovaný antivírusový softvér. Väčšina respondentov (329) používa antivírusový program. Môžeme konštatovať, že 93% používateľov v ČR a SR dodržiava jedno zo základných opatrení proti phishingu. Zo všetkých opýtaných nemá antivírus

nainštalovaný 5 % (17) používateľov. Ďalšie 2 % (8) respondentov nevedeli, či ho využívajú alebo nie.



Graf 11.15 – Používanie antivírusového softvéru (zdroj: autorka)

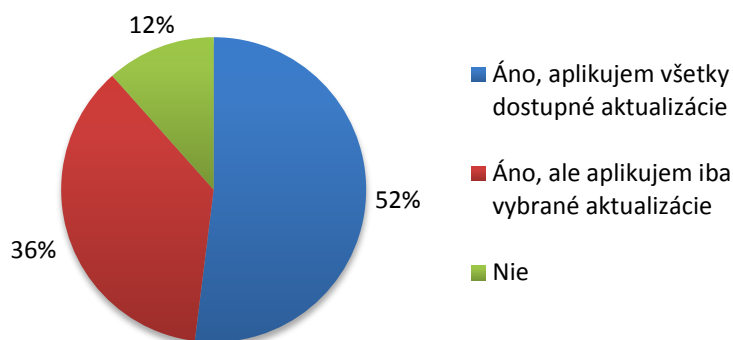
Ak si používateľ nezaobstará neplatenú verziu antivírusového softvéru, ale zakúpi si licenciu, dostane komplexné bezpečnostné riešenie, ktoré obsahuje aj nadstavbu v podobe antiphishingového nástroja, pluginu alebo filtra. Z tohoto dôvodu sme sa v desiatej otázke pýtali na **používanie antiphishingového filtra alebo nástroja**. Najviac respondentov nevie 138 (39 %), či používa antiphishingové riešenie. Ďalších 136 (38 %) opýtaných uviedlo, že ho nepoužíva a 80 (23 %) respondentov si antiphishingový filter alebo nástroj zaobstaralo. V súčasnosti už antiphishingový filter obsahujú aj webové prehliadače. Z odpovedí uvedených pri piatej otázke vyplýva, že si väčšina používateľov zakúpila antivírus spolu s antiphishingovým riešením.



Graf 11.16 – Používanie antiphishingového filtra alebo nástroja (zdroj: autorka)

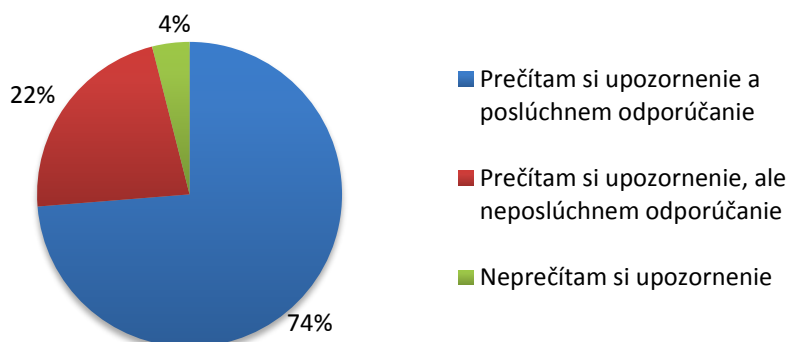
Jedno z často zdôrazňovaných opatrení proti phishingu zahŕňa inštaláciu dostupných aktualizácií operačného systému, antivírusu a ďalšieho softvéru.

Pre niektorých používateľov sú aktualizácie veľmi otravné a neuvedomujú si ich úlohu z hľadiska bezpečnosti. **Jedenásta otázka dotazníka sa zameriavala na pravidelnú aplikáciu aktualizácií nainštalovaného softvéru.** Z odpovedí vyplýva, že 12 % (41) respondentov vôbec neinštaluje aktualizácie. Ďalších 36 % (129) používateľov aplikuje vybrané aktualizácie. Najviac používateľov, až 184 (52 %) inštaluje všetky dostupné aktualizácie.



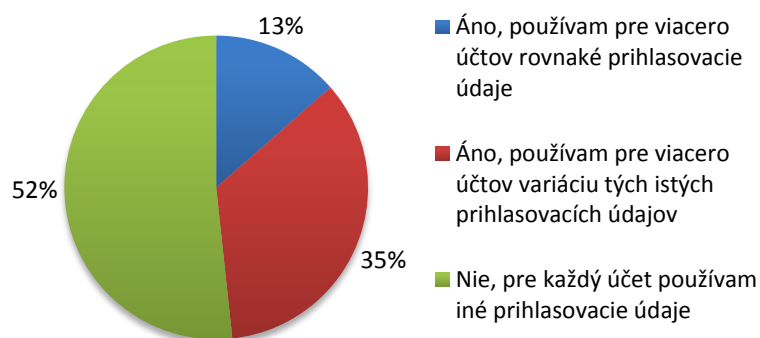
Graf 11.17 – Aplikácia aktualizácií nainštalovaného softvéru (zdroj: autorka)

K dvanástej otázke bol priložený obrázok s bezpečnostným upozornením. Informovalo používateľa, že prehliadač *Opera* nemôže overiť identitu servera kvôli problému s certifikátom. Varovalo používateľa, že sa ho stránka môže snažiť podviesť. Na obrázku je možné vidieť ako je zvýraznená ponúknutá možnosť zrušiť. **Opýtali sme sa respondentov na ich reakciu po zobrazení uvedeného upozornenia.** Skupina respondentov, ktorí by si upozornenie ani neprečítali predstavovala 4 % (14) z celkového počtu opýtaných osôb. Ďalšia skupina s podielom 22 % (79) respondentov by si síce upozornenie prečítala, ale neposlúchli by odporúčanie. Najviac respondentov až 74 % (261) by si upozornenie nielen prečítalo, ale aj poslúchlo.



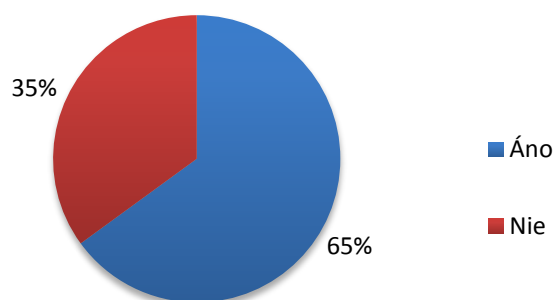
Graf 11.18 – Reakcie na bezpečnostné upozornenie (zdroj: autorka)

Používatelia často uľahčujú phisherom prácu, pretože používajú rovnaké alebo podobné heslá do rôznych účtov. Ak útočník získa spomínané prihlasovacie údaje dokáže naraz zneužiť a odcudziť niekoľko rôznych účtov používateľa. Používatelia sú dlhšiu dobu upozorňovaní, aby sa vyhýbali riziku a používali odlišné a silné heslá. **Zo spomínaného dôvodu sme v trinástej otázke zisťovali, či používatelia využívajú rovnaké alebo podobné prihlasovacie údaje.** Zatiaľ čo totožné prihlasovacie údaje do rôznych účtov používa 13 % (48) respondentov, 35 % (123) opýtaných sa do rôznych účtov prihlasuje prostredníctvom variácií prihlasovacích údajov. Počet respondentov, ktorí skutočne využívajú rôzne prihlasovacie údaje do rôznych účtov, je 183 (52 %).



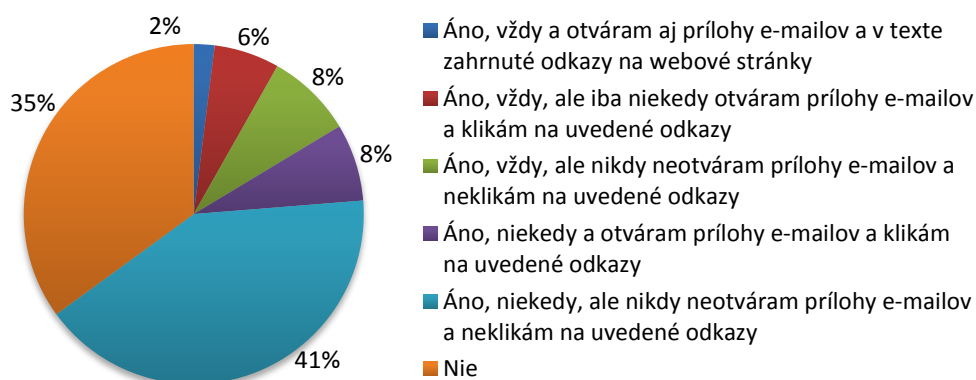
Graf 11.19 – Používanie rovnakých a podobných prihlasovacích údajov (zdroj: autorka)

Jedným zo spôsobov, ako sťažiť útočníkom zneužitie prihlasovacích údajov je dvojfázové overenie. **Cieľom štrnástej otázky bolo zistiť, či sa používatelia do niektorých účtov prihlasujú prostredníctvom dvojfázového overenia** napr. prostredníctvom SMS (Short message service) kódu a grid karty. Skupina respondentov tvoriaca podiel 65 % (230) používa dvojfázové overenie, zatiaľ čo zvyšných 35 % (124) nie.



Graf 11.20 – Používanie dvojfázového overenia (zdroj: autorka)

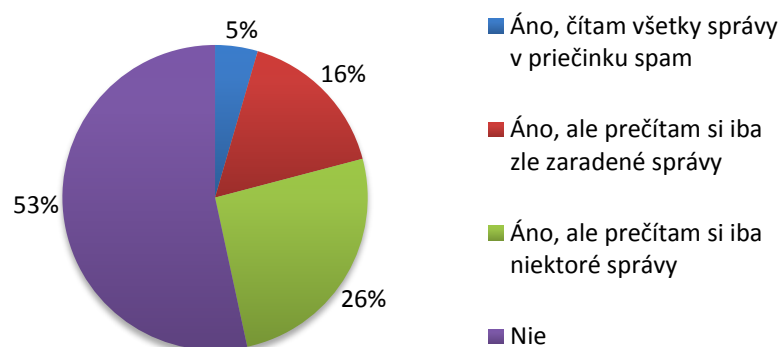
Jedným z najčastejšie spomínaných opatrení je nečítanie e-mailov od cudzích ľudí. **V pätnástej otázke sme sa respondentov pýtali, či čítajú emaily od neznámych osôb.** E-maily od cudzích osôb neprečíta 35 % opýtaných (124). Najpočetnejšia skupina 146 (41 %) osôb síce e-mail prečíta, ale v žiadnom prípade neotvára prílohy a nenavštevuje uvedené odkazy. Respondenti, ktorí niekedy otvoria e-mail od neznámej osoby, otvoria prílohy a klikajú na umiestnené odkazy predstavujú 8 % (26). Vždy si e-maily od neznámych osôb čítajú ale nikdy neklikajú na prílohy ani odkazy, 29 respondenti (8 %). Vždy si e-maily prečíta, ale len niekedy prílohu otvorí alebo odkaz navštívi 6 % (22) opýtaných. Najmenej respondentov 2% (7) vždy otvorí e-mail od neznámej osoby a navštívi uvedený odkaz. Skupiny, ktoré riskujú čítaním podobných emailov, otvárajú prílohy a klikajú na odkazy sú pomerne malé.



Graf 11.21 – Otváranie emailov od neznámych osôb (zdroj: autorka)

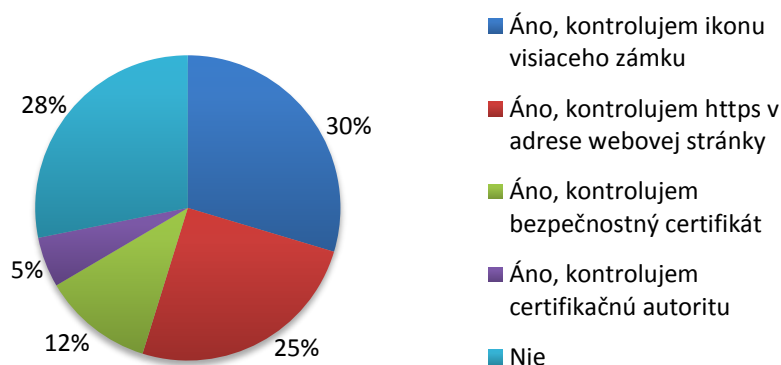
Niektoré phishingové e-mailly sú pomocou antispamového filtru odhalené a zaradené do spamu. Keď si však používateľ číta správy v priečinku spam, znovu sa

vystavuje nebezpečenstvu, že sa stane obeťou phishingu. Používateli sa zobrazuje varovanie, ktoré však môžu ignorovať. Šestnásta otázka znela: „**Čítate e-maily, ktoré boli umiestnené do priečinku spam?**“ Prevažná väčšina 189 (53 %) respondentov správy nečíta. Naopak 16 (5 %) odpovedajúcich číta všetok spam. Zle zaradené správy si prezrie 58 (16 %) respondentov a niektoré správy si prečíta 91 (26 %) opýtaných.



Graf 11.22 – Čítanie e-mailov v priečinku spam (zdroj: autorka)

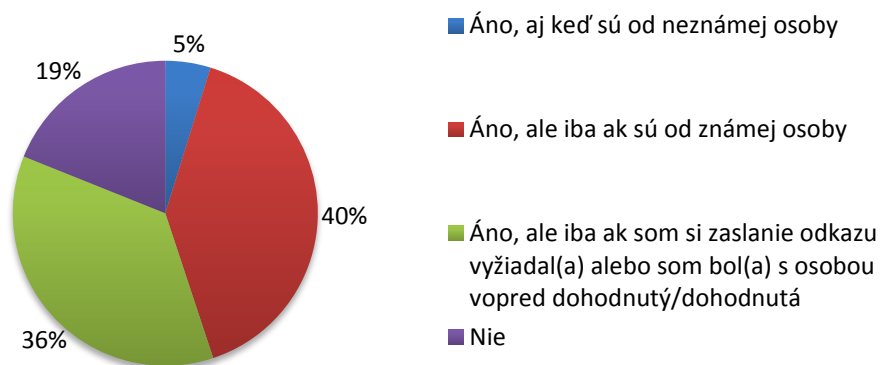
Sedemnásť otázka skúma, či používatelia pri prihlasovaní kontrolujú zabezpečené pripojenie a podľa čoho. Prekvapivo vysoký počet 132 (28 %) respondentov vôbec nekontroluje zabezpečené pripojenie. Najviac – 139 (30 %) opýtaných si pri prihlasovaní všima ikonu visiaceho zámku. HTTPS v adrese webovej stránky preveruje 118 respondentov a bezpečnostný certifikát si prehliada 55 respondentov. Iba 25 odpovedajúcich kontroluje certifikačnú autoritu.



Graf 11.23 – Kontrola zabezpečeného pripojenia pri prihlasovaní (zdroj: autorka)

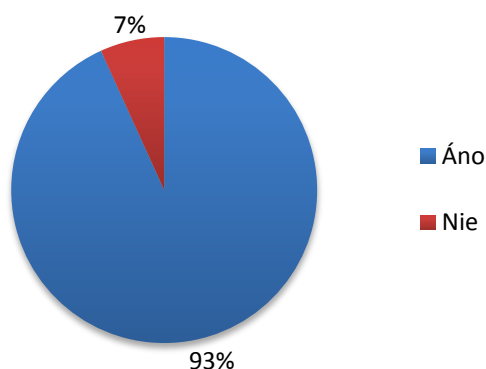
Osemnásť otázka znie: „Navštevujete odkazy, ktoré dostanete prostredníctvom e-mailu, chatu, sociálnej siete alebo rýchlych správ (Skype,

ICQ)?“ Zaslané odkazy vôbec nenavštíví 19 % (67) odpovedajúcich. Všetky odkazy, vrátane odkazov od neznámych osôb navštíví 5 % (17) respondentov. Najvyšší podiel 40 % (142) opýtaných klikne len na odkaz od známej osoby a 36 % (128) respondentov navštíví iba vyžiadaný odkaz alebo odkaz, o ktorom sa osobou vopred dohodli.



Graf 11.24 – Návštevnosť odkazov, ktoré používatelia dostanú (zdroj: autorka)

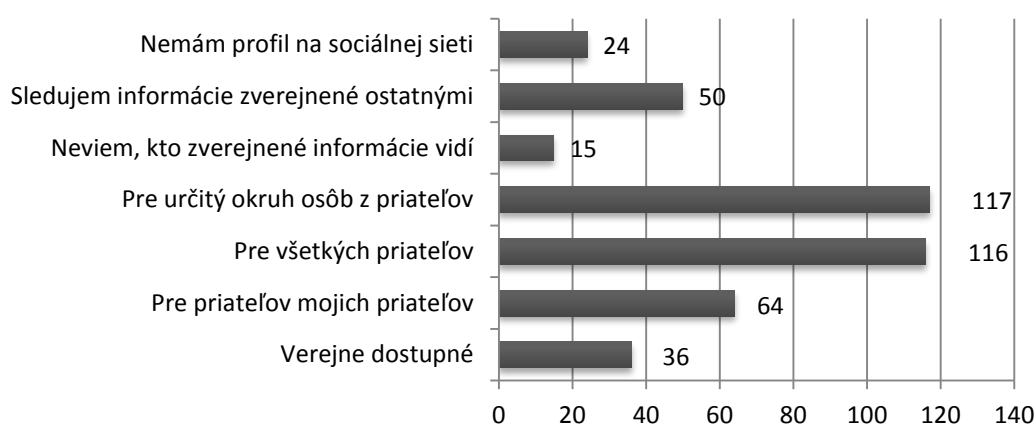
V osemnástej otázke nás zaujímalo, či používatelia prehodnocujú, ktoré informácie o sebe zverejnia na sociálnych sieťach, webových stránkach, blogoch atď. Podľa odpovedí zvažuje 93 % (330) respondentov informácie, ktoré o sebe zverejnia. Zvyšných 7 % (24) odpovedajúcich nepremýšľa nad zverejňovanými informáciami. Neopatrní používatelia, ktorí prostredníctvom internetu o sebe zverejňujú množstvo informácií a nepremýšľajú o možnosti zneužitia zverejnených informácií, sa môžu ľahko stať obeťou phisherov.



Graf 11.25 – Zvažovanie informácií, ktoré používatelia zverejňujú (zdroj: autorka)

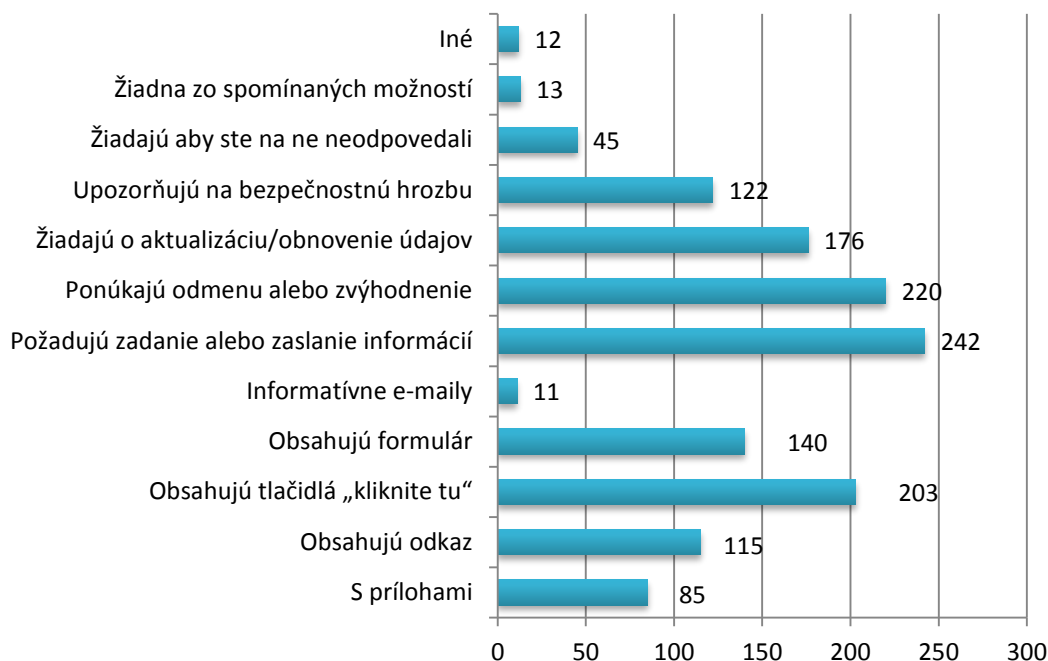
Informácie zverejnené prostredníctvom sociálnych sietí dokážu útočníci zužitkovať v phishingu. Čím viac informácií používateľ zverejňuje, tým je

pravdepodobnosť napadnutia väčšia. Z uvedeného dôvodu sme položili respondentom devätnástu otázku, ktorá znela: „**Zverejňujete o sebe informácie na sociálnych siet'ach? Kto môže tieto informácie vidieť?**“ Z grafu 11.26 môžeme vidieť, že najviac 117 odpovedajúcich zdieľa informácie s okruhom osôb z priateľov. Takmer rovnaký počet 116 respondentov zverejňuje informácie pre všetkých priateľov. Ďalších 64 opýtaných zverejňuje informácie pre priateľov svojich priateľov. Zatiaľ čo 24 respondentov nemá na sociálnej sieti účet, 50 respondentov iba sleduje informácie ostatných.



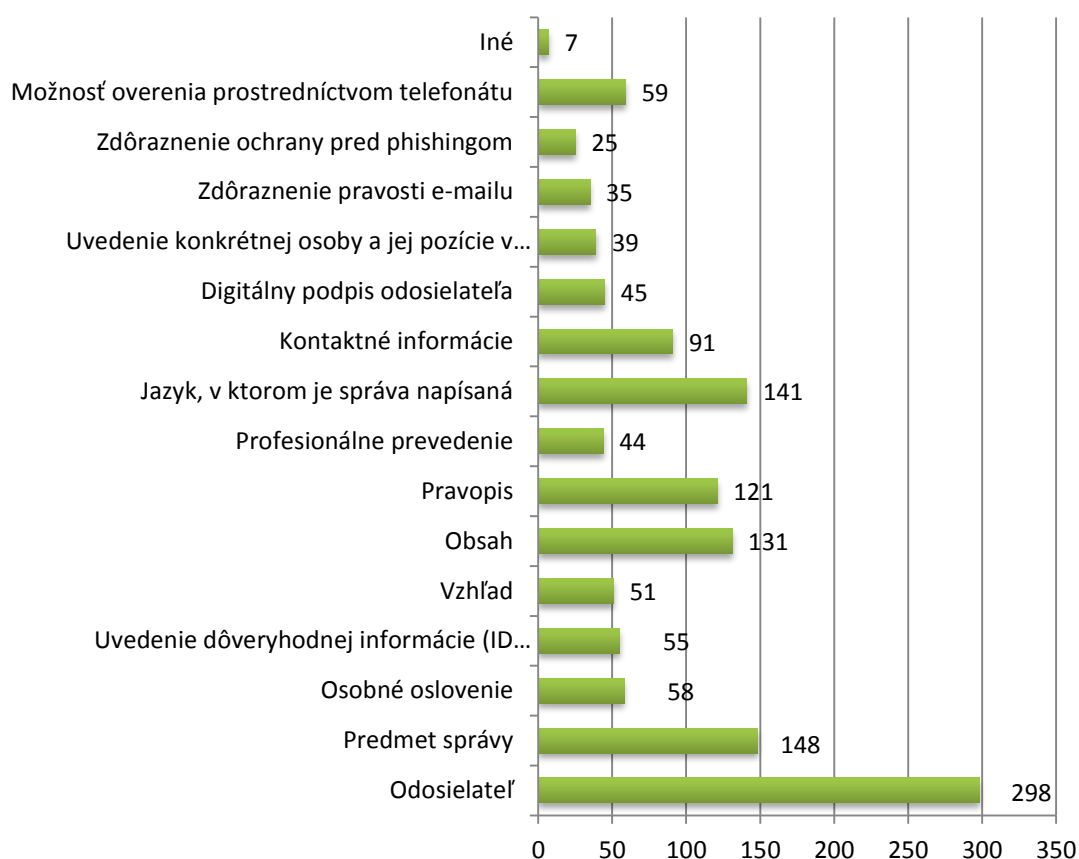
Graf 11.26 – Zverejňovanie informácií na sociálnych siet'ach (zdroj: autorka)

Dvadsať otázka zisťovala voči ktorým e-mailom sú používatelia podozrievaví. Najpochybnejšie sú e-maily urgentne požadujúce informácie, ktoré označilo 242 (68 %) opýtaných. Ide o jeden z najpoužívanějších sociálnych trikov. Druhé najpodozrivejšie sú pre 220 (62 %) respondentov e-maily ponúkajúce odmenu alebo zvýhodnenie. Phishingové útoky niekedy ponúkajú zvýhodnenie, často však spomínané e-maily zasielajú aj rôzne e-shopy (napr. e-maily so zľavovými kódmi). Na treťom mieste sú e-maily, ktoré obsahujú tlačidlá „kliknite tu“. Za nedôveryhodné ich považuje 203 (57 %) respondentov. Žiadny s uvedených emailov sa nezdal podozrivý 4 % odpovedajúcich. Touto otázkou sme taktiež chceli zistiť, či sa používatelia na základe rôznych vzdelávacích kampaní o phishingu nezačali obávať všetkých e-mailov s prílohami a odkazmi. Z výskumu vyplýva, že 115 (32 %) respondentov považuje za podozrivý e-maily s odkazmi a 85 (24 %) odpovedajúcich e-maily s prílohami. Uvedení respondenti pravdepodobne nedokážu odhaliť phishing od legitímneho e-mailu, a tak sa obávajú všetkých správ s prílohami a odkazmi.



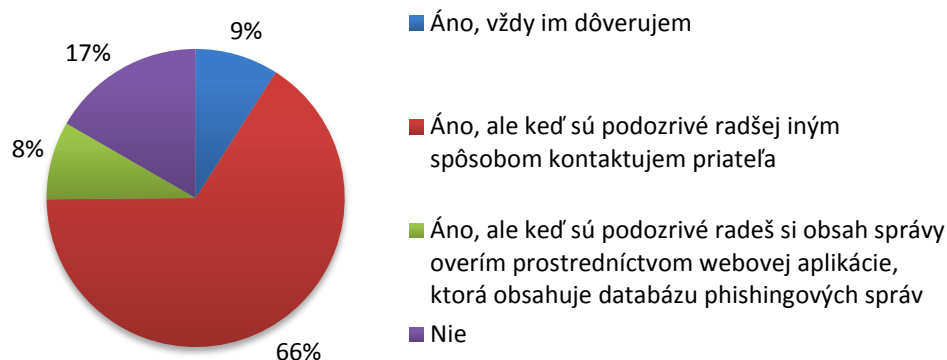
Graf 11.27 – Podozrivé e-maily (zdroj: autorka)

Dvadsať druhá otázka sa pýtala, podľa ktorých znakov e-mailu posudzujú jeho dôveryhodnosť a pravosť. Prevažná väčšina 298 (84 %) odpovedajúcich pri posudzovaní správy zvažuje odosielateľa správy. Na základe predmetu hodnotí pravosť a dôveryhodnosť e-mailu 148 (42 %) respondentov. Treťou, najpočetnejšou odpoveďou so 141 hlasmi (40 % odpovedajúcich) je jazyk, v ktorom je správa napísaná. Ďalšími zvažovanými znakmi sú obsah (131 respondentov), pravopis (121 respondentov) a kontaktné informácie (91 respondentov). Aby phisher vzbudili u používateľov pocit dôveryhodnosti v niektorých útokoch zdôrazňujú pravosť emailov a ochranu pred phishingom. Napriek tomu, by spomínaným dvom znakom uverilo 35 (10 %) a 25 (7 %) odpovedajúcich. Prekvapivé je i zistenie, že len 45 (13%) respondentov by dôveryhodnosť e-mailu posudzovalo na základe digitálneho podpisu.



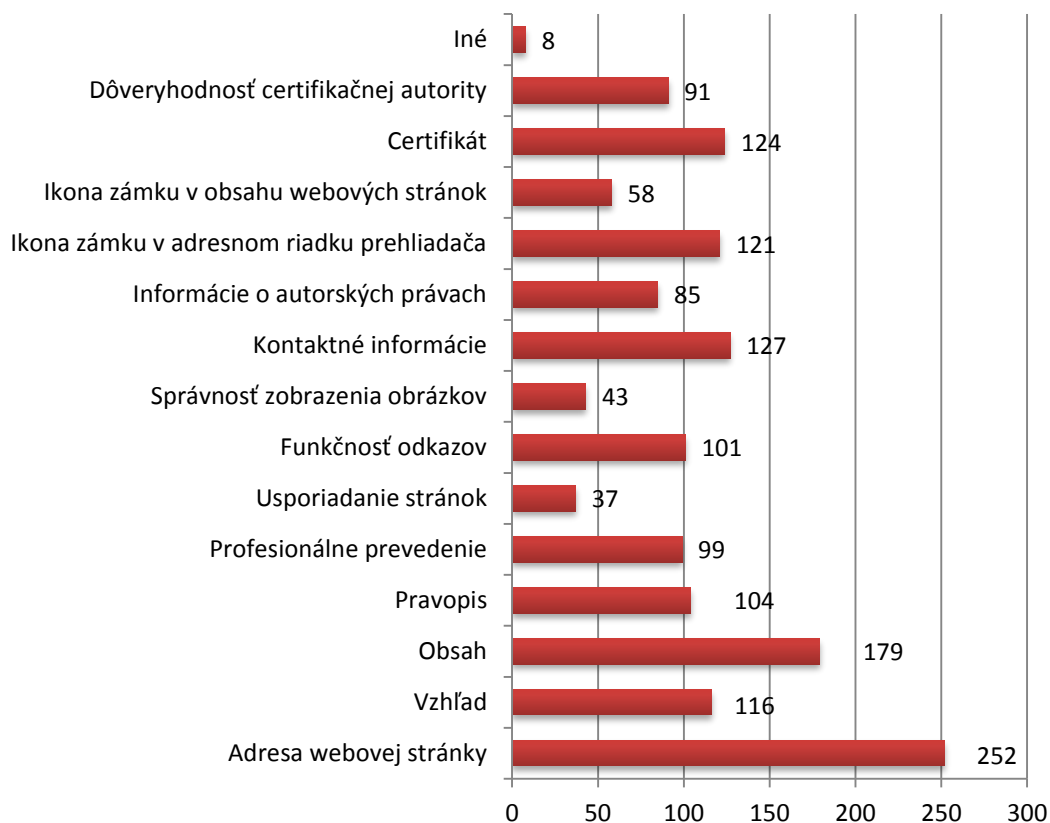
Graf 11.28 – Znaký dôveryhodnosti a pravosti e-mailu (zdroj: autorka)

V posledných mesiacoch bolo v ČR a SR uskutočnených niekoľko phishingových útokov, ktoré zneužívali kontakty potenciálnych obetí. **Na základe spomínaných skutočností sme sa v dvadsiatej tretej otázke používateľov pýtali, či dôverujú e-mailom a správam, ktoré dostanú z e-mailovej adresy alebo profilu priateľa.** Zatiaľ čo 9 % (32) respondentov správam vždy dôveruje, 17 % (59) opýtaných im nedôveruje. Ak je správa podozrivá 66 % (233) respondentov radšej iným spôsobom kontaktuje priateľa a zvyšných 8 % (30) respondentov si obsah správy preverí prostredníctvom webovej aplikácie s databázou phishingových správ.



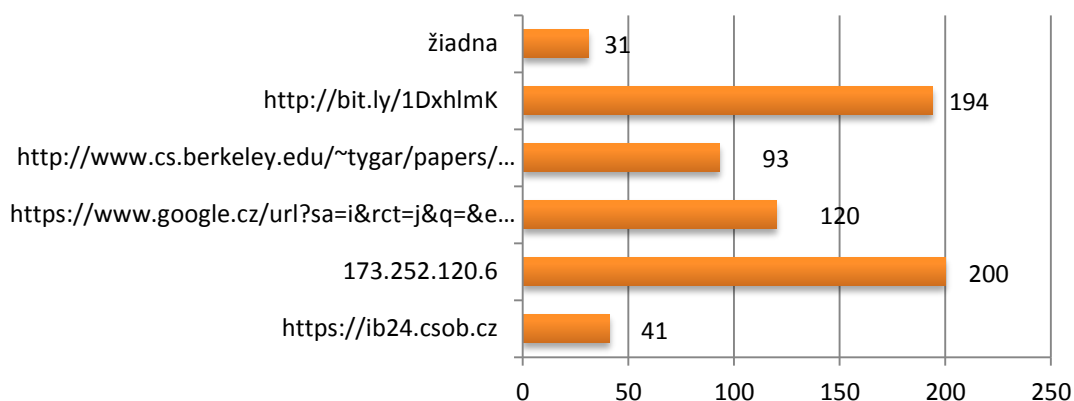
Graf 11.29 – Dôvera v správy z emailov a profilov priateľov (zdroj: autorka)

V dvadsiatej štvrtej otázke mali respondenti označiť, ktoré z vymenovaných možností zvažujú pri posudzovaní dôveryhodnosti a pravosti webových stránok. Možnosti obsahovali znaky, ktoré by si používatelia mali skutočne všímať ako napr. adresa webovej stránky, ikona zámku v adresnom riadku prehliadača, certifikát, dôveryhodnosť certifikačnej autority. Medzi možnosťami sa však nachádzali aj znaky, ktoré bežne používajú phisher aby vzbudili v používateľoch pocit dôveryhodnosti (napr. ikona zámku v obsahu webových stránok, informácie o autorských právach). Do možných odpovedí sme zahrnuli taktiež znaky, ktoré by mali hodnotiť bežný používatelia bez odbornejšieho vzdelania v oblasti Informačných technológií (napr. obsah, vzhľad, pravopis, usporiadanie webu). Z 354 respondentov až 252 (71 % respondentov) si prehliada adresu webovej stránky. Ďalších 179 (51 %) opýtaných zvažuje dôveryhodnosť a pravosť stránok na základe obsahu a 127 (36 %) odpovedajúcich hodnotí stránky na základe uvedených kontaktných informácií. Tesne za kontaktnými informáciami sa umiestnili s počtom hlasov 124 (35 %) certifikát a 121 (34 %) ikona zámku v adresnom riadku prehliadača. Kompletné výsledky môžete vidieť v grafe 11.30. Zaujímavosť je, že až 24 % (85) respondentov by do úvahy vzalo informácie o autorských právach a 16 % (58) odpovedajúcich ikonu zámku v obsahu stránok. Ikona zámku v obsahu je používaná pri tvorbe phishingových webových stránok a informácie o autorských právach už dnes bežne phisher používajú. Na základe spomínaných dvoch možností nemožno odlíšiť legitímne a podvodné stránky.



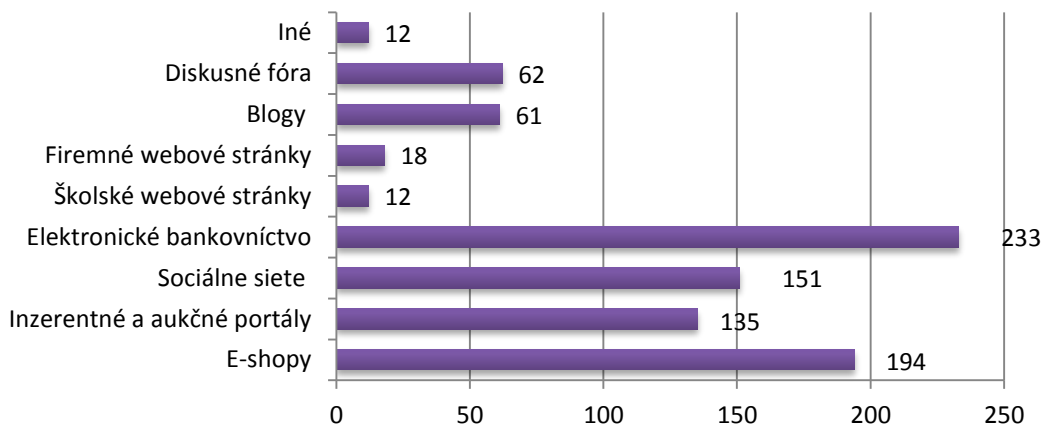
Graf 11.30 – Znaky dôveryhodnosti a pravosti web stránok (zdroj: autorka)

Prostredníctvom dvadsiatej piatej otázky, sme sa snažili zistiť, ktoré adresy web stránok pôsobia podozrivo. Respondenti boli požiadaní, aby na odkazy neklikali a iba si ich prezreli. Najpodozrivejšou bola IP adresa, ktorú označilo 200 opýtaných. Menší počet 194 respondentov podozrieval skrátenú URL adresu. Treťou najpodozrivejšou adresou, s počtom 120 hlasov, bola veľmi dlhá URL adresa. Za podozrivý považovalo 93 opýtaných odkaz na .PDF dokument na stránkach *Berkeley*, ktorý v rámci URL adresy obsahoval pojem Phishing. Najmenej podozrivo pôsobila adresa internetového bankovníctva *ČSOB*, i keď dostala 41 hlasov. Žiadna zo spomínaných adries sa nezdala podozrivou 31 respondentom.



Graf 11.31 – Podozrivosť adries webových stránok (zdroj: autorka)

Dvadsať šiesta otázka zisťovala, pri návšteve ktorých webových stránok sú používatelia obozretnejší. Najviac respondentov – 233 je obozretnejších pri používaní elektronického bankovníctva. Pri prezeraní e-shopov koná opatrnejšie 194 opýtaných. O niečo menší počet 151 respondentov sa správa obozretnejšie v prípade návštevy sociálnych sietí. Dvanásť odpovedajúcich je opatrnejších aj v prípade iných stránok, konkrétne pornografických stránok a portálov určených k sťahovaniu súborov.



Graf 11.32 – Zvýšená obozretnosť (zdroj: autorka)

11.7 Konfrontácia výsledkov

11.7.1 Hypotéza 1

Hypotéza 1 znie nasledovne „Existuje závislosť medzi krajinou pobytu respondentov a tým, či považujú phishing za reálnu hrozbu v Českej a Slovenskej republike.“ Hypotézu 1 sme overovali a závislosť premenných počítali použitím Chi-kvadrát testu nezávislosti s hladinou významnosti $\alpha = 0,05$. Chi-kvadrát test overuje, či

sú rozdiely v skutočných a očakávaných početnostiach náhodné alebo štatisticky významné. Premenné sú nezávislé, ak sú rozdiely v skutočných a očakávaných početnostiach náhodné.

Najprv sme si v programe *Microsoft Excel* vytvorili kontingenčnú tabuľku, ktorá obsahuje skutočné početnosti dvoch kvalitatívnych premenných. Následne sme vytvorili tabuľku očakávaných početností. Jednotlivé hodnoty sme vypočítali na základe nasledovného vzorca:

$$\text{očakávaná početnosť} = \text{riadková početnosť} \times \text{stĺpcová početnosť} / \text{celkový počet}.$$

	Krajina pobytu ČR	Krajina pobytu SR	Celkom
Reálna hrozba	157	141	298
Nereálna hrozba	19	37	56
Celkom	176	178	354

Tabuľka 11.8 – Kontingenčná tabuľka hypotézy 1 (zdroj: autorka)

	Krajina pobytu ČR	Krajina pobytu SR
Reálna hrozba	148,1581921	149,8418079
Nereálna hrozba	27,84180791	28,15819209

Tabuľka 11.9 – Tabuľka očakávaných početností hypotézy 1 (zdroj: autorka)

Výpočet Chi-kvadrát testu nezávislosti sme uskutočnili v programe *Microsoft Excel* s pomocou funkcie CHITEST. Výsledkom výpočtu bola p-hodnota, ktorá sa rovná 0,010006793. Na 5 % hladine významnosti bola nulová hypotéza, ktorá vyjadruje nezávislosť premenných, zamietnutá. Hypotézu 1 bola potvrdená. **Existuje slabá závislosť medzi krajinou pobytu respondentov a tým, či považujú phishing za reálnu hrozbu v ČR a SR.**

11.7.2 Hypotéza 2

Hypotéza 2 bola stanovená nasledovne: „**Jestvuje závislosť medzi znalosťou opatrení a pohlavím respondentov.**“ Ako aj v prvom prípade sme overovali hypotézu prostredníctvom Chi-kvadrát testu nezávislosti na 5 % hladine významnosti. Kvalitatívnymi premennými boli pohlavie a znalosť opatrení proti phishingu.

	Muži	Ženy	Celkom
Znalosť opatrení	120	137	257
Neznalosť opatrení	40	57	97
Celkom	160	194	354

Tabuľka 11.10 – Kontingenčná tabuľka hypotézy 2 (zdroj: autorka)

	Muži	Ženy
Znalosť opatrení	116,1581921	140,8418079
Neznalosť opatrení	43,84180791	53,15819209

Tabuľka 11.11 – Tabuľka očakávaných početností hypotézy 2 (zdroj: autorka)

S pomocou tabuľky očakávaných početností, kontingenčnej tabuľky a funkcie CHITEST sme vypočítali p-hodnotu, ktorá sa rovná 0,357639817. P-hodnota je vyššia než hladina významnosti $\alpha = 0,05$. Nulovú hypotézu o nezávislosti nemôže zamietnuť. Zistený rozdiel nie je štatisticky významný a môže byť iba dôsledkom náhodného výberu. **Medzi znalosťou opatrení proti phishingu a pohlavím nejestvuje vzťah.**

11.7.3 Hypotéza 3

Hypotéza 3 predpokladá: „Existuje závislosť medzi znalosťou opatrení proti phishingu a študijným a pracovným zameraním respondentov.“ Znovu sme hypotézu overovali Chi-kvadrát testom nezávislosti na hladine významnosti $\alpha = 0,05$.

	IT pracovné zameranie, IT študijné zameranie a obe zamerania IT	Iné študijné a pracovné zameranie	Celkom
Znalosť opatrení	87	170	257
Neznalosť opatrení	16	81	97
Celkom	103	251	354

Tabuľka 11.12 – Kontingenčná tabuľka hypotézy 3 (zdroj: autorka)

	IT pracovné zameranie, IT študijné zameranie a obe zamerania IT	Iné študijné a pracovné zameranie
Znalosť opatrení	74,77683616	182,2231638
Neznalosť opatrení	28,22316384	68,77683616

Tabuľka 11.13 – Tabuľka očakávaných početností hypotézy 3 (zdroj: autorka)

Na základe skutočných a očakávaných početností sme funkciou CHITEST vyrátali p-hodnotu, ktorá sa rovnala 0,001341901. Na základe p-hodnoty nižšej ako bola 5 % hladina významnosti, sme nulovú hypotézu zamietli. **Medzi znalosťou opatrení proti phishingu a študijným a pracovným zameraním respondentov existuje závislosť.**

11.7.4 Hypotéza 4

Hypotéza 4 znela: „**Používatelia, ktorí majú aspoň jedno zo zameraní IT sledujú pri e-mailoch a webových stránkach viac relevantných znakov než bežní používatelia.**“ Zo všetkých znakov uvedených v otázke 22. sme vybrali relevantné znaky, ktoré by si mali používatelia všimnúť: odosielateľa, predmet, uvedenie dôvernej informácie, digitálny podpis a inú možnosť (napr. e-mailový server odosielateľa). Respondentov sme rozdelili do troch skupín. Prvá skupina respondentov mala buď pracovné alebo študijné zameranie IT. Druhá skupina odpovedajúcich mala pracovné aj študijné zameranie IT a tretia skupina mala obe zamerania iné. Následne sme u respondentov zisťovali, koľko zo spomínaných znakov označili.

Ako môžeme vidieť v tabuľke 1.14 respondenti s IT pracovným alebo študijným zameraním a respondenti s pracovným aj študijným zameraním IT sledujú viac relevantných znakov než bežní používatelia. Obe skupiny označili minimálne jeden a maximálne štyri znaky. Žiaden z respondentov nesleduje 5 relevantných znakov. **Zatiaľ čo respondenti zo skupiny s aspoň jedným IT zameraním a s oboma IT zameraniami sledujú v priemere 2 relevantné znaky, bežní používatelia 1 jeden.** Prvá časť hypotézy sa teda potvrdila.

	Počet responden.	Relatívny počet responden.	Vážený aritmetický priemer	Medián	Minimálny počet označených znakov	Maximálny počet označených znakov
IT pracovné/študijné zameranie	37	10,45 %	2	2	1	4
IT pracovné aj študijné zameranie	66	18,65 %	2,12	2	1	4
Iné pracovné aj študijné zameranie	251	70,90 %	1,36	1	0	4

Tabuľka 11.14 – Počet relevantných znakov sledovaných pri e-mailoch (zdroj: autorka)

Podobne sme postupovali aj s otázkou 24. Ako relevantné znaky sme si vybrali: adresu webovej stránky, ikonu zámku v adresnom riadku, certifikát, dôveryhodnosť certifikačnej autority a inú možnosť. Výsledok bol podobný ako v prvom prípade. Odpovedajúci, ktorých pracovné a študijné zameranie je IT alebo majú pracovné alebo študijné zameranie IT označili priemerne dva relevantné znaky, zatiaľ čo bežní používatelia 1. Hypotéza 4 bola potvrdená.

	Počet responden.	Relatívny počet responden.	Vážený aritmetický priemer	Medián	Minimálny počet označených znakov	Maximálny počet označených znakov
IT pracovné/študijné zameranie	37	10,45 %	2,48	3	1	4
IT pracovné aj študijné zameranie	66	18,65 %	2,42	3	0	4
Iné pracovné aj študijné zameranie	251	70,90 %	1,34	1	0	4

Tabuľka 11.15 – Počet relevantných znakov sledovaných pri webových stránkach (zdroj: autorka)

Záver

Prvý z cieľov diplomovej práce bol naplnený v prvých ôsmych kapitolách práce, v ktorých sme sa zaoberali zistenými zložkami phishingu, trikmi, typmi phishingových útokov, dôvodmi fungovania phishingu, aspektami pravosti a dôveryhodnosti sledovanými používateľmi, dopadmi zavedenia kontextu do phishingu ako aj opatreniami, ktoré vznikli na ochranu proti phishingu. Zistili sme, že sa phishing skladá z návnady, háčika a úlovku. Používa na oklamanie používateľov sociálne aj technické triky. Vyznačuje sa množstvom rôznych typov útokov a neustále vznikajú ďalšie typy útokov. Dôvody fungovania phishingu spočívajú v stratégiách phisherov, ktoré zneužívajú nedostatok znalostí, pozornosti ale aj vizuálny podvod. Phishing funguje i preto, že väčšina používateľov sa pri posudzovaní legitímnosti a dôveryhodnosti správa a web stránok sústreďí viac na vizuálne prvky a obsah, než na bezpečnostné prvky. Najhoršou formou phishingu je phishing, ktorý obsahuje sociálny kontext a zneužíva sociálne kontakty potenciálnych obetí. Je približne 4,5 krát účinnejší (Jagatic a kol., 2005) než bežný phishing. Zistili sme, že phishing nezneužíva len technické nedostatky, ale sústreďí sa najmä na podvedenie používateľa, preto nemôžeme phishing riešiť len prostredníctvom technologických opatrení. Dôležité opatrenia proti phishingu predstavujú zlepšovanie povedomia o phishingu, vzdelávanie používateľov a pôsobenie antiphishingových skupín.

Aby sme preukázali splnenie ďalších troch cieľov, v krátkosti zodpovieme všetky otázky položené v úvode práce. **Druhým cieľom diplomovej práce** bolo prevedenie analýzy súčasnej situácie v oblasti phishingu a zistenie možných dopadov na používateľa a preto sme sa pýtali: „**Aká je súčasná situácia v oblasti phishingu a akým spôsobom vplýva na bežného používateľa?**“ Analýzou prieskumov Global Phishing Survey sme zistili, že počet phishingových útokov je v posledných rokoch veľmi vysoký a blíži sa k historickému maximu. Môžeme konštatovať, že dochádza k rozmachu phishingu. Útoky sú síce aktívne kratšiu dobu, čiže spôsobia menšiu škodu, ale ich agresivita sa stupňuje. Phisherí ohrozujú širokú škálu populárnych organizácií, ale nepoužívajú názvy napadnutých značiek v doménových menách. Celosvetovým trendom je získavanie doménových mien používaných k phishingu prostredníctvom hackingu a zraniteľného webhostingu.

Hlavným zistením analýzy globálnej situácie vo phishingu je, že súčasné protiopatrenia neznižujú počet phishingových útokov, iba spôsobujú presun phisherov k používaniu iných útokov a taktík, k obchádzaniu vytvorených opatrení. Situácia v oblasti phishingu sa vďaka súpereniu organizácií vytvárajúcich opatrenia a phisherov rýchlo mení. Dôsledkom je sťaženie života bežných používateľov, pretože u nich neustále vzniká potreba vzdelávania o nových útokoch, o ich odhaľovaní i o spôsobe obrany proti nim. Používateľ, ale tiež dokáže znepríjemňovať život phisherom vďaka nahlasovaniu phishingu.

Tretí cieľ je zameraný na zistenie dôležitosti povedomia o phishingu, opatrnosti a všímavosti používateľov pri odhaľovaní phishingu. V úvode práce sme si položili otázku: „**Aké dôležité sú opatrnosť, všímavosť a základné znalosti o phishingu u českých a slovenských používateľov pri odhaľovaní phishingových útokov v rámci ČR a SR? Dokážu opatrní a všímaví používatelia útok odhaliť?**“ Analýzou konkrétnych prípadov útokov sme zistili, že phishingové útoky v ČR a SR sú síce prepracované, avšak odhaliteľné. Používateľ môže podvod odhaliť ak je opatrný, všímavý a má základné znalosti o phishingu a opatreniach proti nemu. Musí si premyslieť svoje konanie a všímať si aspoň znaky ako odosielateľ a predmet správy, odkazy uvedené v e-mailoch, adresu webovej stránky, ikonu zámku v adresnom riadku, či certifikát. Podľa spomínaných znakov, dokáže odhaliť phishing v Českej a Slovenskej republike. Ak by boli všetci používatelia obozretní, všímaví a premýšľali by skôr než konali, phishing by bol odsúdený k zániku alebo obrovskej zmene formy. Dnešná uponáhľá doba môže spôsobovať, že používatelia nemôžu a nechcú venovať dostatok svojho času, pozornosti a všímavosti posudzovaniu pravosti e-mailov a webových stránok. Radšej sa spoliehajú na technologické riešenia v podobe antivírusového softvéru.

Štvrtým cieľom bolo uskutočnenie výskumu, ktorý mal zistiť úroveň povedomia o phishingu u českých a slovenských používateľov, ich osobné skúsenosti, bezpečnostné návyky a aspekty, ktoré berú do úvahy pri posudzovaní pravosti e-mailov a web stránok. Najprv sme sa snažili zistiť úroveň povedomia o phishingu a položili sme si otázku: „**Aké je povedomie o phishingu u českých a slovenských používateľov? Majú osobné skúsenosti s phishingom?**“ Pojem phishing pozná iba polovica respondentov, skôr sú používateľom známe podvodné e-maily a webové

stránky. Znepokojujúce je, že existuje skupina osôb (necelých 10 %), ktorá o spomínaných hrozbách vôbec nevie a skupina osôb (28 %), ktorá nevie ako sa proti phishingu brániť. Väčšina používateľov pozná aspoň niektoré opatrenia, avšak nevie ako phishing nahlásiť a nezaznamenala žiadnu vzdelávaciu kampaň, video, web stránku atď.. Takmer polovica používateľov pravdepodobne nedokáže rozpoznať phishing, pretože nevedeli, či majú s phishingom skúsenosti. Najviac skúseností majú českí a slovenskí používatelia s phishingovými e-mailami. Medzi respondentmi sa nachádzali aj osoby, ktoré phishingu podľahli. Na základe zistení môžeme konštatovať, v ČR a SR existuje povedomie o phishingu, je však na dosť nízkej úrovni a je potrebné ho zlepšovať. Problém však spočíva v spôsobe, pretože mnoho organizácií vytvára vzdelávacie kampane, materiály, stránky, videá o phishingu, ale používatelia ich na základe výskumu nezaznamenali v dostatočnej miere. Taktiež môžeme zhodnotiť, že českí a slovenskí používatelia majú osobnú skúsenosť s phishingom.

V rámci empirického výskumu sme nepreukázali závislosť medzi znalosťou opatrení a pohlavím respondentov, dokázali sme však existenciu závislosti medzi študijným a pracovným zameraním používateľov a znalosťou opatrení proti phishingu. Potvrdil sa i predpoklad, že ľudia ktorí pracujú v IT, študujú v obore IT alebo majú pracovné a študijné zameranie IT sú opatrnejší, než bežní používatelia. Posudzujú dôveryhodnosť a pravosť e-mailov aj web stránok na základe väčšieho počtu relevantných znakov.

Odlišuje sa vnímanie reálnosti hrozby phishingu v závislosti od pobytu v Českej a Slovenskej republike? Prevažná väčšina 84 % osôb si uvedomuje reálnosť hrozby phishingu. Potvrdila sa aj slabá závislosť medzi krajinou pobytu a vnímaním reálnosti hrozby phishingu používateľmi. O trochu viac si hrozbu phishingu uvedomujú obyvatelia Českej republiky.

Snažili sme sa zistiť, či sa používatelia správajú tak, aby sa vyhli phishingu a preto sme si položili otázku: **„Majú slovenskí a českí používatelia nejaké bezpečnostné návyky, ktoré im môžu pomôcť vyhnúť sa phishingu?“** Prevažná väčšina českých a slovenských používateľov má nainštalovaný antivírusový softvér a viac než 20 % používateľov si zakúpilo antivírusový softvér s antiphishingovou ochranou. Používatelia sú zodpovední a aplikujú aktualizácie. Všímajú si varovania a väčšinou poslúchajú odporúčania. Nadpolovičná väčšina používateľov má

do jednotlivých účtov rôzne prihlasovacie údaje a dokonca používa dvojfázové overenie. Tri štvrtiny používateľov neotvárajú e-maily od neznámych osôb alebo ak ich aj čítajú, v žiadnom prípade neotvárajú prílohy a neklikajú na uvedené odkazy. Spam nečíta polovica opýtaných. Nedisciplinovaní sú používatelia pri overovaní zabezpečeného spojenia. Problém spočíva taktiež v zistení, že veľká skupina používateľov kliká na všetky odkazy zaslané priateľmi. Používatelia zvažujú aké informácie o sebe zverejňujú a snažia sa ich zdieľať prevažne so svojimi priateľmi. Z popísaných skutočností môžeme zhodnotiť, že českí a slovenskí používatelia majú dobré bezpečnostné návyky, ktoré by sa však dali zlepšovať. Mali by si dávať väčší pozor pri prihlasovaní do svojich účtov a kontrolovať zabezpečené pripojenie a nedôverovať odkazom, ktoré im zaslali známe osoby.

Ktoré aspekty dôveryhodnosti a pravosti českí a slovenskí používatelia berú v úvahu pri e-mailoch a webových stránkach? Používatelia nedôverujú najmä e-mailom, ktoré od nich požadujú informácie, obsahujú tlačidlá „kliknite tu“, žiadajú obnovenie údajov ale aj e-maily, ktoré ponúkajú zvýhodnenie. Vzdelávacie kampane, materiály a web stránky majú pravdepodobne nielen pozitívny efekt. Výskumom sme zistili, že určitá skupina používateľov začala podozrievať všetky e-maily s prílohami ako aj e-maily obsahujúce odkazy. Niektoré phishinogové e-maily vytvorené pre ČR a SR sa dajú odhaliť už prostredníctvom odosielateľa a predmetu e-mailu. Spomínané znaky sú jedny z najviac všímavých relevantných znakov, avšak okrem toho sa používatelia sústredia najmä na aspekty ako jazyk, obsah, pravopis, kontaktné informácie, osobné oslovenie a možnosť overenia cez telefón. Sledujú teda skôr vizuálne prvky a obsah e-mailu než bezpečnostné aspekty. Tri štvrtiny opýtaných používateľov po nedávnych útokoch už nedôveruje e-mailom a správam od priateľov. Radšej si pravosť správ overujú kontaktovaním priateľa alebo prostredníctvom aplikácie. Ide o pozitívne zistenie, ktoré môže napovedať o znížení náchylnosti českých a slovenských používateľov na útoky s kontextom a sociálnymi kontaktmi. Vyšší počet českých a slovenských používateľov kontroluje relevantné znaky v podobe adresy webovej stránky, ikony zámku v adresnom riadku prehliadača, certifikátu a certifikačnej authority. Avšak podobne ako pri posudzovaní e-mailov, používatelia do značnej miery prihliadajú k znakom ako obsah, vzhľad, pravopis, kontaktné údaje, funkčnosť odkazov skôr než k bezpečnostným prvkom. Najviac používatelia upodozrievajú IP adresy,

skrátene URL adresy a príliš dlhé adresy. Obozretnejší sú pri návšteve elektronického bankovníctva, e-shopov a sociálnych sietí.

Na základe všetkých zistení a popísaných skutočností sme vytvorili niekoľko nasledovných odporúčaní:

- Používatelia by sa mali s novými phishingovými útokmi oboznamovať priebežne a vopred. Keď sa útoky začnú šíriť v ČR a SR je už na osvetu neskoro. Situáciu môžeme vidieť na phishingových útokoch prostredníctvom sociálnej siete, ktoré boli v zahraničí známe už dlhšiu dobu. V ČR a SR na nich nikto používateľa neupozornil, kým sa používatelia nestali obeťami útoku.
- Je potrebné používateľov pripraviť na skutočnosť, že phishingový útok môže prísť odkiaľkoľvek, nielen od finančnej inštitúcie a častokrát od spoločnosti, ktorej zneužitie by neočakávali.
- Okrem technologických je potrebné sa viac sústrediť na vzdelávanie používateľov. V spolupráci s používateľmi nájsť vhodnú metódu na vzdelávanie o phishingu. Zaujímavú kampaň vytvorila napr. *Česká spořitelna*, ktorá vzdeláva svojich klientov prostredníctvom videa o phishingu alebo varuje používateľov na phishing na obrazovke všetkých svojich bankomatov.
- Musíme používateľom vysvetliť, že antivírusový program ich vždy neochráni len v prípade, ak sa aj sami správajú zodpovedne, premýšľajú, sú všímvaví a v prvom rade ak už hrozba bola zistená. Neuvedomujú si, že určitú dobu trvá než je hrozba odhalená a je vytvorené opatrenie, ktoré ich chráni.
- V rámci vzdelávacích kampaní by sme mali viac zdôrazňovať potrebu nahlásenia phishingových útokov a taktiež vzdelávať používateľov ako a kam majú správu alebo stránku nahlásiť. Neuvedomujú si, že nahlásením predchádzajú ďalším obetiam a pomáhajú pri tvorbe opatrení.
- Naďalej musíme používateľov upozorňovať na podvodné správy od priateľov.
- Predovšetkým prostredníctvom vzdelávania používateľom zdôrazňovať, že na základe znakov ako napríklad pravopis, vzhľad, obsah, kontaktné údaje, funkčnosť obrázkov a podobne, nemôžu posudzovať pravosť a dôveryhodnosť e-mailov a web stránok. Prízvukovať im dôležitosť overovania zabezpečeného pripojenia, a to nielen prostredníctvom ikony zámku ale aj certifikátom a certifikačnou autoritou.

Všetky ciele práce boli splnené. Prostredníctvom práce sme vyzdvihli dôležitosť používateľa pre úspešnosť phishingu. Používateľ je najslabšou časťou bezpečnostného systému, ktorú sa snažia phisherí prekonať. Má podstatný vplyv na úspešnosť a odhalenie útoku. Dôležitým predstaviteľom ľudského faktora je však i phisher. Kvalitou vytvorených útokov ovplyvňuje nebezpečnosť a úspešnosť útoku. Vytváraním nových typov útokov, spôsobov doručenia a trikov spôsobuje vývoj phishingu.

Dôvodov náchylnosti českých a slovenských používateľov je niekoľko. Síce majú dobré bezpečnostné návyky avšak príliš spoliehajú na technologické opatrenia v podobe antivírusového softvéru a antiphishingového riešenia. Ich povedomie o phishingu je slabé a malo by sa zlepšovať. V niektorých prípadoch sú používatelia málo obozretní a všímaví. Sústredia sa na vizuálne znaky a obsah skôr než na bezpečnostné znaky e-mailov a webových stránok. Dôverujú odkazom zaslaným známymi osobami, aj keby nemali.

Phishing je nekonečným kolobehom. Phisherí stále vytvárajú nové útoky, proti ktorým sú pripravené opatrenia. Útočníci sa snažia opatreniam vyhýbať. Táto situácia sa nezmení pokiaľ sa nenájde účinné riešenie problému phishingu a to bude pravdepodobne trvať dlhšiu dobu. Riešením problému phishingu by mala byť kombinácia technologických opatrení a vzdelávania. Je veľmi zložitý najst' správny pomer medzi nimi. Ani vzdelávanie, a ani technologické opatrenie však nemôže byť samostatným riešením.

Zoznam skratiek

AOL	America Online
APAC	Anti-Phishing Alliance of China
APWG	Anti-Phishing Working Group
ARP	Address Resolution Protocol
CINIC	China Internet Network Information Center
.CN	Čínska doména najvyššej úrovne
ČR	Česká republika
ČSOB	Československá obchodná banka
.CZ	Česká doména najvyššej úrovne
DNS	Domain Name System
DPA	Distributed Phishing Attacks
.EU	Doména najvyššej úrovne Európskej únie
EÚ	Európska únia
FBI	Federal Bureau of Investigation
HTML	HyperText Markup Language
HTTPS	Hypertext Transfer Protocol Secure
ICQ	Komunikačný program
ID	Identification
IDS	Intrusion Detection System
IDN	Internationalized Domain Names
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISIS	Integrated Study Information System
IT	Information Technology
MITM	Man in the middle
.NET	Doména najvyššej úrovne pôvodne pre sieťové technológie
PDF	Portable Document Format
PIN	Personal Identification Number
.SK	Slovenská doména najvyššej úrovne
SMS	Short Message Service
SR	Slovenská republika
SSL	Secure Sockets Layer
.TH	Doména najvyššej úrovne Thajska
.TK	Doména najvyššej úrovne Tokelau
TLD	Top Level Domain
URL	Uniform Resource Locator
USB	Universal Serial Bus
ZIP	Archívny formát súboru
XSS	Cross-site scripting

Zoznam obrázkov

Obrázok 1.1 – Sociotechnický cyklus	20
---	----

Zoznam grafov

Graf 9.1 – Vývoj počtu phishingových útokov a doménových mien	51
Graf 11.1 – Rozdelenie respondentov podľa pohlavia	71
Graf 11.2 – Rozdelenie respondentov podľa veku	72
Graf 11.3 – Rozdelenie respondentov na základe krajiny pobytu	72
Graf 11.4 – Rozdelenie respondentov z hľadiska najvyššieho dosiahnutého vzdelania	73
Graf 11.5 – Rozdelenie respondentov podľa študijného zamerania	74
Graf 11.6 – Rozdelenie respondentov na základe pracovného zamerania	74
Graf 11.7 – Pocit bezpečia pri vykonávaní bežných činností vo virtuálnom svete	76
Graf 11.8 – Povedomie o phishingu, podvodných e-mailoch a webových stránkach ..	77
Graf 11.9 – Osobné skúsenosti používateľov s phishingom	78
Graf 11.10 – Reálnosť hrozby phishingu v ČR a SR podľa používateľov	79
Graf 11.11 – Znalosť opatrení proti phishingu	79
Graf 11.12 – Vedia používatelia overiť a nahlásiť phishing	81
Graf 11.13 – Pomer používateľov, ktorý zaznamenali a nezaznamenali v posledných 12 mesiacoch vzdelávaciu kampaň, materiál, video a webovú stránku o phishingu	82
Graf 11.14 – Sledovanie varovaní používateľmi	82
Graf 11.15 – Používanie antivírusového softvéru	83
Graf 11.16 – Používanie antiphishingového filtra alebo nástroja	83
Graf 11.17 – Aplikácia aktualizácií nainštalovaného softvéru	84
Graf 11.18 – Reakcie na bezpečnostné upozornenie	84
Graf 11.19 – Používanie rovnakých a podobných prihlasovacích údajov	85
Graf 11.20 – Používanie dvojfázového overenia	86
Graf 11.21 – Otváranie emailov od neznámych osôb	86
Graf 11.22 – Čítanie e-mailov v priečinku spam	87
Graf 11.23 – Kontrola zabezpečeného pripojenia pri prihlasovaní	87
Graf 11.24 – Návštevnosť odkazov, ktoré používatelia dostanú	88
Graf 11.25 – Zvažovanie informácií, ktoré používatelia zverejňujú	88
Graf 11.26 – Zverejňovanie informácií na sociálnych siet'ach	89
Graf 11.27 – Podozrivé e-maily	90
Graf 11.28 – Znaky dôveryhodnosti a pravosti e-mailu	91
Graf 11.29 – Dôvera v správy z e-mailov a profilov priateľov	92

Graf 11.30 – Znaký dôveryhodnosti a pravosti web stránok	93
Graf 11.31 – Podozrivosť adries webových stránok	94
Graf 11.32 – Zvýšená obozretnosť	94

Zoznam tabuliek

Tabuľka 9.1 – Vývoj globálnej situácie v oblasti phishingu	50
Tabuľka 9.2 – Údaje o doménach .SK, .CZ a .EU 2011 – 2014	60
Tabuľka 9.3 – Údaje o doménach .SK, .CZ a .EU od začiatku roka 2007 – 2010	61
Tabuľka 11.1 – Rozdelenie respondentov z hľadiska pohlavia	71
Tabuľka 11.2 – Rozdelenie respondentov z hľadiska veku	71
Tabuľka 11.3 – Rozdelenie respondentov na základe krajiny pobytu	72
Tabuľka 11.4 – Rozdelenie respondentov z hľadiska najvyššieho dosiahnutého vzdelania	73
Tabuľka 11.5 – Rozdelenie respondentov podľa študijného zamerania	73
Tabuľka 11.6 – Rozdelenie respondentov na základe pracovného zamerania	74
Tabuľka 11.7 – Opatrenia proti phishingu, ktoré respondenti dodržiavajú	80
Tabuľka 11.8 – Kontingenčná tabuľka hypotézy 1	95
Tabuľka 11.9 – Tabuľka očakávaných početností hypotézy 1	95
Tabuľka 11.10 – Kontingenčná tabuľka hypotézy 2	96
Tabuľka 11.11 – Tabuľka očakávaných početností hypotézy 2	96
Tabuľka 11.12 – Kontingenčná tabuľka hypotézy 3	96
Tabuľka 11.13 – Tabuľka očakávaných početností hypotézy 3	97
Tabuľka 11.14 – Počet relevantných znakov sledovaných pri e-mailoch	98
Tabuľka 11.15 – Počet relevantných znakov sledovaných pri webových stránkach	98

Zoznam zdrojov

- [1] About Fraudwatch. FRAUDWATCH INTERNATIONAL. *Fraudwatchinternational.com* [online]. © 2003 - 2014 [cit. 2014-11-02]. Dostupné z: <<http://www.fraudwatchinternational.com/about>>.
- [2] About the APWG. *APWG.org* [online]. © 2014a [cit. 2014-11-02]. Dostupné z: <<https://www.apwg.org/resources/overview/avoid-phishing-scams>>.
- [3] Aktuality: Upozornění na phishing - ČSOB. *ZCU.cz* [online]. 02.06.2014 [cit. 2014-11-20]. Dostupné z: <http://support.zcu.cz/index.php/Aktuality:Upozorn%C4%9Bn%C3%AD_na_phishing_-_%C4%8CSOB>.
- [4] Aktuality: Upozornění před možným zneužitím platební karty přes Facebook. *CSAS.cz* [online]. 04.06.2014 [cit. 2014-11-21]. Dostupné z: <http://www.csas.cz/banka/content/inet/internet/cs/news_ie_2152.xml?archivePage=news_archive_subportal03&navid=>>.
- [5] ČÍŽEK, Jakub. Na Česko opět útočí phishing. Oběti si za to mohou samy. *Zive.cz* [online]. 29.04.2014 [cit. 2014-11-20]. Dostupné z: <<http://www.zive.cz/clanky/na-cesko-opet-utoci-phishing-obeti-si-za-to-mohou-samy/sc-3-a-173472/default.aspx>>.
- [6] DHAMIJA, Rachna; TYGAR, J. D.; HEARST, Marti. Why Phishing Works. [online]. To appear in Proceeding of CHI-2006: Conference on Human Factors in Computing Systems, 2006 [cit. 2014-07-05]. Dostupné z: <http://www.cs.berkeley.edu/~tygar/papers/Phishing/why_phishing_works.pdf>.
- [7] ESET: Slovenské firmy ohrozuje trójsky kôň, ktorý zneužíva obdobie úhrady daní. *ESET.com* [online]. 14.03.2013 [cit. 2014-11-30]. Dostupné z: <<http://www.eset.com/sk/o-nas/press-centrum/tlacove-spravy/article/eset-slovenske-firmy-ohrozuje-trojsky-kon-ktory-zneuziva-obdobie-uhrady-dani/>>.
- [8] How to Avoid Phishing Scams. *APWG.org* [online]. © 2014b [cit. 2014-08-15]. Dostupné z: <<https://www.apwg.org/resources/overview/avoid-phishing-scams>>.
- [9] JAGATIC, Tom; JOHNSON, Nathaniel; JAKOBSSON, Markus; MENEZER, Filippo. Social Phishing. [online]. Bloomington, IN: Indiana University, 2005 [2014-07-23]. Dostupné z: <<http://markus-jakobsson.com/papers/jakobsson-commacm07.pdf>>.
- [10] JAKOBSSON, Markus; YOUNG, Adam. Distributed Phishing Attacks. [online]. Bloomington, IN: Indiana University, 2005 [cit. 2014-07-30]. Dostupné z: <<https://eprint.iacr.org/2005/091.pdf>>.
- [11] JAKOBSSON, Markus; TSOW, Alex; SHAH, Ankur; BLEVIS, Eli; LIM, Youn-Kyung. What Instills Trust?: A Qualitative Study of Phishing. [online]. Bloomington, IN: Indiana University, 2007 [cit. 2014-07-28]. Dostupné z: <<http://markus-jakobsson.com/papers/jakobsson-usec07-trust.pdf>> .

- [12] JAKOBSSON, Markus; MYERS, Steven. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. 1. vyd. Hoboken, N.J.: Wiley-Interscience, 2006. ISBN 978-047-1782-452.
- [13] JAKOBSSON, Markus. The Human Factor in Phishing. [online]. Bloomington, IN: Indiana University, 2007 [cit. 2014-07-29]. Dostupné z: <<http://markus-jakobsson.com/papers/jakobsson-psci07.pdf>>.
- [14] JAMES, Lance. *Phishing bez záhad*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1766-1.
- [15] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
- [16] LACHENBRUCH, P. A. Analýza kategoriálních dat. *EUROMISE.org* [online]. 05.01.1999 [cit. 2014-11-30]. Dostupné z: <<http://new.euromise.org/czech/tajne/ucebnice/html/html/node12.html>>.
- [17] MITNICK, Kevin a William SIMON. *Umění klamu: Nejslavnější hacker na světě*. 1. vyd. Gliwice: Helion, 2003. ISBN 83-736-1210-6.
- [18] Na klientov slovenských bánk útočila v stredu veľká phishingová kampaň - aktualizácia 1. *DSL.sk* [online]. 10.07.2014 [cit. 2014-11-08]. Dostupné z: <<http://www.dsl.sk/article.php?article=15816>>.
- [19] Novinky: Pozor - nový phishing cílí na klienty České spořitelny. *Csirt.cz* [online]. 20.06.2013 [cit. 2014-11-08]. Dostupné z: <<http://csirt.cz/page/1461/pozor----novy-phishing-cili-na-klienty-ceske-sporitelny/>>.
- [20] OLLMANN, Gunter. The Phishing Guide: Understanding & Preventing Phishing Attacks. *Textfiles.com* [online]. Next Generation Security Software Ltd., 2004 [cit. 2014-07-20]. Dostupné z: <<http://pdf.textfiles.com/security/nisrphishing.pdf>>.
- [21] Pokusy o phishing v České republice narůstají. *MBank.cz* [online]. 20.11.2014 [cit. 2014-11-04]. Dostupné z: <<http://www.mbank.cz/blog/post,529,pokusy-o-phishing-v-ceske-republice-narustaji.html>>.
- [22] Pozor na phishing a podvodné e-maily. *MBank.cz* [online]. 03.06.2014 [cit. 2014-11-04]. Dostupné z: <<http://www.mbank.cz/blog/post,505,pozor-na-phishing-a-podvodne-e-maily.html>>.
- [23] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 1H2014: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2014b [cit. 2014-09-10]. Dostupné z: <http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf>.
- [24] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 2H2013: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2014a [cit. 2014-09-13]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf>.
- [25] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 1H2013: Unifying the Global Response To Cybercrime. *APWG.org*

- [online]. Lexington, MA: An APWG Industry Advisory, 2013b [cit. 2014-09-15]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf>.
- [26] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 2H2012: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2013a [cit. 2014-09-18]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf>.
- [27] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 1H2012: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2012b [cit. 2014-09-20]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf>.
- [28] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 2H2011: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2012a [cit. 2014-09-23]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf>.
- [29] RASMUSSEN, Rod; AARON, Greg; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 1H2011: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2011b [cit. 2014-09-25]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2011.pdf>.
- [30] RASMUSSEN, Rod; AARON, Greg ; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 2H2010: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2011a [cit. 2014-09-27]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf>.
- [31] RASMUSSEN, Rod; AARON, Greg ; ROUTH, Aaron. Global Phishing Survey:Trends and Domain Name Use in 1H2010: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2010b [cit. 2014-09-29]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf>.
- [32] RASMUSSEN, Rod; AARON, Greg. Global Phishing Survey:Trends and Domain Name Use in 2H2009: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2010a [cit. 2014-10-03]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf>.
- [33] RASMUSSEN, Rod ; AARON, Greg. Global Phishing Survey:Trends and Domain Name Use in 1H2009: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2009b [cit. 2014-10-05]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf>.
- [34] RASMUSSEN, Rod; AARON, Greg. Global Phishing Survey:Trends and Domain Name Use in 2H2008: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2009a [cit. 2014-10-06]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf>.
- [35] RASMUSSEN, Rod; AARON, Greg. Global Phishing Survey:Trends and Domain Name Use in 1H2008: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA:

- An APWG Industry Advisory, 2008b [cit. 2014-10-09]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf>.
- [36] RASMUSSEN, Rod; AARON, Greg. Global Phishing Survey:Trends and Domain Name Use in 2007: Unifying the Global Response To Cybercrime. *APWG.org* [online]. Lexington, MA: An APWG Industry Advisory, 2008a [cit. 2014-10-11]. Dostupné z: <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey2007.pdf>.
- [37] RIMARČÍK, Marián. Dvojjrozmerná indukčná štatistika - nominálne premenné - nezávislé vzorky: Chi-kvadrát test nezávislosti. *RIMARCÍK.com* [online]. [cit. 2014-11-30]. Dostupné z: <<http://rimarcik.com/navigator/chi2.html>>.
- [38] ŘEZANKOVÁ, Hana. *Analýza dat z dotazníkových šetření*. 3. aktualiz. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-062-1.
- [39] SHI, Junxiao a Sara SALEEM. Phishing. *Arizona.edu* [online]. Tucson, AZ: The University of Arizona, 2012 [cit. 2014-07-10]. Dostupné z: <<http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic5-final/report.pdf>>.
- [40] Slovenské firmy ohrozuje trójsky kôň, ktorý zneužíva obdobie úhrady daní. *Inet.sk* [online]. 14.03.2013 [cit. 2014-11-22]. Dostupné z: <<http://blog.inet.sk/clanok/eset-slovenske-firmy-ohrozuje-trojsky-kon-ktory-zneuziva-obdobie-uhrady-dani/>>.
- [41] Spear Phishers: Angling to Steal Your Financial Info. *FBI.gov* [online]. 04.01.2009 [cit. 2014-07-27]. Dostupné z: <http://www.fbi.gov/news/stories/2009/april/spearphishing_040109>.
- [42] Spear Phishing: Scam, Not Sport. *Norton.com* [online]. ©1995 – 2014 [cit. 2014-07-26]. Dostupné z: <<http://us.norton.com/spear-phishing-scam-not-sport/article>>.
- [43] The PhishTank Story. *Phishtank.com* [online]. [cit. 2014-08-14]. Dostupné z: <<http://www.phishtank.com/about.php>>.
- [44] TUREK, Rastislav. PhishMe.com, phishing na dobré účely. *ITNEWS.sk* [online]. 09.05.2008 [cit. 2014-11-21]. Dostupné z: <<http://www.itnews.sk/spravy/bezpecnost/2008-05-09/c85975-phishme.com-phishing-na-dobre-ucely>>.
- [45] What is Spear Phishing?: Security definition. *Kaspersky.com* [online]. © 1997-2014 [cit. 2014-07-26]. Dostupné z: <http://usa.kaspersky.com/internet-security-center/definitions/spear-phishing?typnews=Social_media#.U9tccON_tik>.

Prílohy

Zoznam príloh

Príloha 1 – Phishing od Daňového úradu SR

Príloha 2 – Phishingová správa na sociálnej sieti

Príloha 3 – Phishingový e-mail s dlžnou čiastkou

Príloha 4 – Ďalší phishingový e-mail s dlžnou čiastkou

Príloha 5 – Veľká phishingová kampaň

Príloha 6 – Správa z bezpečnostného centra ČSOB

Príloha 7 – Phishingová webová stránka ČSOB

Príloha 8 – Dotazník

Príloha 1 – Phishing od Daňového úradu SR (zdroj: blog.inet.sk)

Subject: Notifikácia o zmene dane z nehnuteľnosti



Dobrý deň!

Daňové riaditeľstvo SR v súčinnosti s Ministerstvom financií SR v týchto dňoch informuje všetky registrované daňové subjekty o závažných zmenách v platení daní.

V týchto dňoch sú daňovým subjektom doručované (doporučne do vlastných rúk prostredníctvom Slovenskej pošty) oznámenia, v ktorých príslušný Daňový úrad oznamuje základné číslo účtu pre platenie dane, ktoré je jedinečné pre každý daňový subjekt.

Číslo účtu pre úhradu príslušnej dane sa skladá z predčísčia označujúceho druh dane, zo základného čísla účtu označujúceho daňový subjekt a z identifikačného kódu Štátnej pokladnice.

V prílohe Vám zasialame podrobný opis.

[Pre viac informácií stiahnite subor v prílohe](#)

Daňový úrad
Notifikácia o zmene dane z nehnuteľnosti

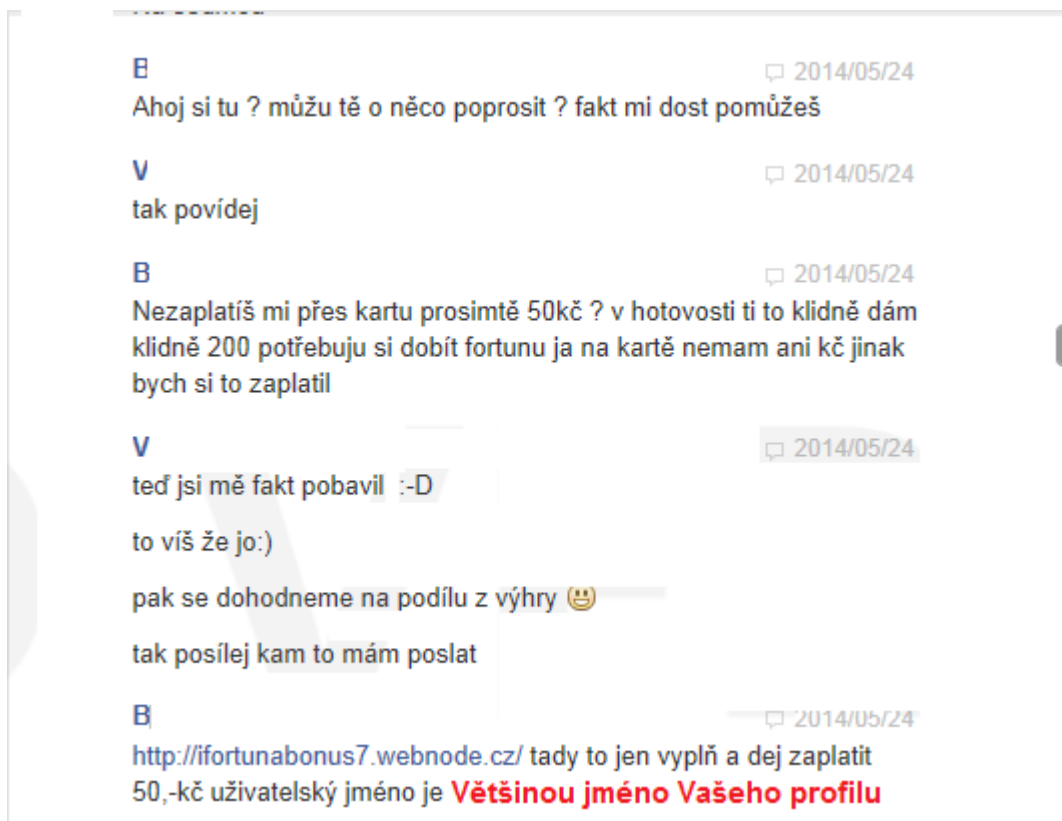
Zmenách v platení daní.

S účinnosťou od 1.1.2013 je daňový subjekt povinný platbu dane poukazovanú daňovému úradu označiť v zmysle Vyhlášky č. 378/2011 Z. z. o spôsobe označovania platby dane na nové číslo účtu.

Notifikácia

Každému daňovému subjektu je pridelené jeho vlastné číslo účtu – tzv. základné číslo účtu.

Príloha 2 – Phishingová správa na sociálnej sieti (zdroj: csas.cz)



Príloha 3 – Phishingový e-mail s dlžnou čiastkou (zdroj: img.cz.prg.cmestatic.com)

Vážený zákazník,

Jsme velmi rádi, že jste využívali produktu z naší banky.

Dovolujeme si Vás upozornit na dlužnou částku ve výši 7725.77 Kč, ke dni 26.05.2014 na osobním účtě #2768167054947897. Nabízíme Vám uhradit pohledávku v plné výši do 19.07.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #854080299E1280CB umožňujeme Vám:

- 1) Dodržet pozitivní úvěrovou historii
- 2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 7725.77 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

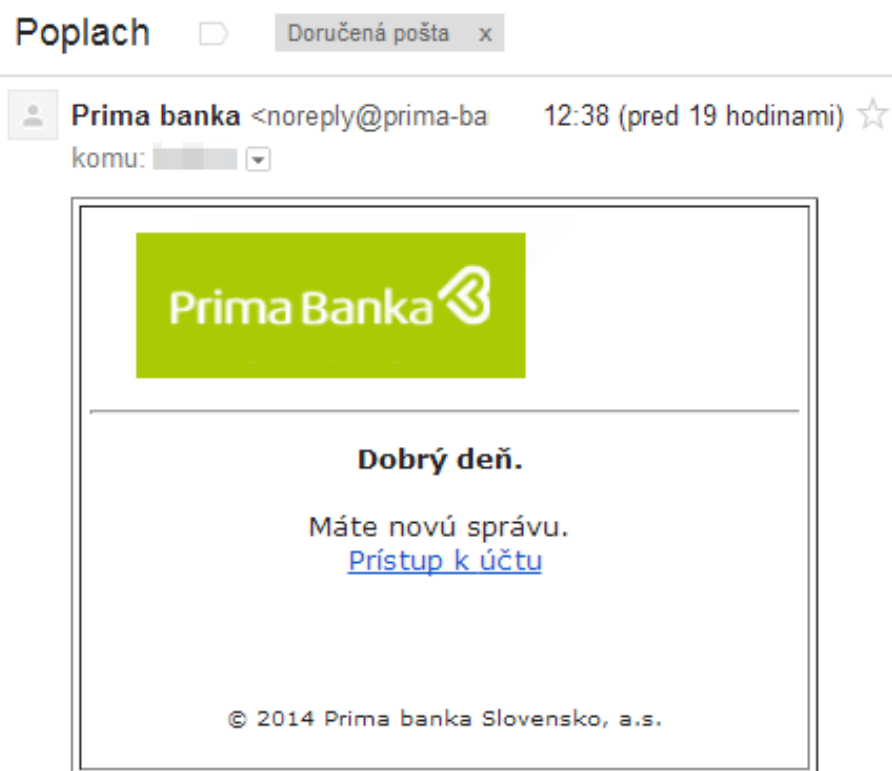
Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_854080299E1280CB.zip"

S pozdravem,
Vedoucí odboru vymáhání pohledávek
Bedřich Vlach
+420 607 799 835

Přílohy

 smlouva_854080299E1280CB.zip (50 kB) [Zobrazit](#) | [Stáhnout](#)

Príloha 4 – Veľká phishingová kampaň (zdroj: dsl.sk)



Príloha 5 – Správa z bezpečnostného centra ČSOB (zdroj: zcu.cz)

Předmět: Poplach centrum
Datum: Mon, 2 Jun 2014 08:59:18 +0000
Od: CSOB <security.alert@csobalert.cz>
Komu: <uzivatel>@<pracoviste>.zcu.cz

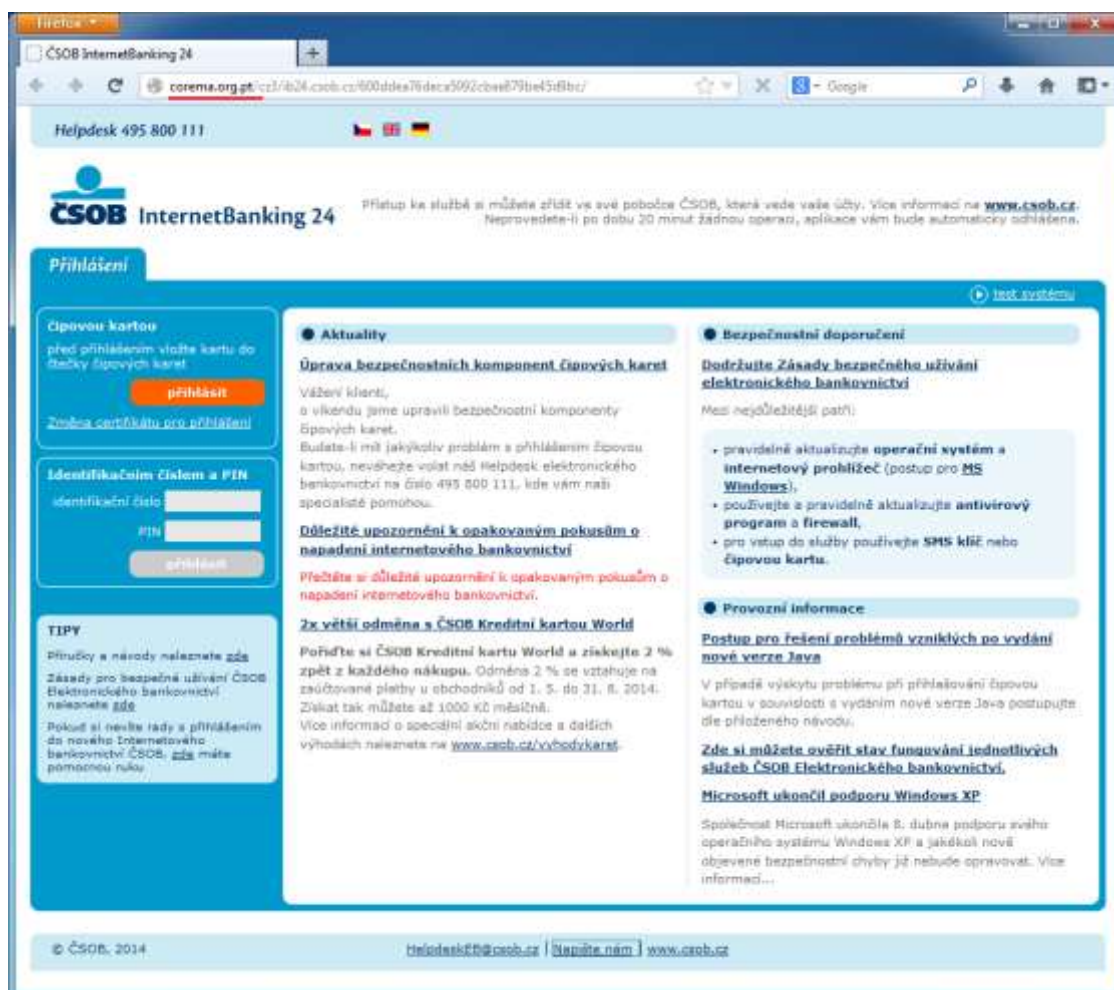
Untitled Document

*Vážený zákazníku, *

Obdrželi jste nový záznam z našeho bezpečnostního centra.

Přístup k účtu <<http://fisyrec.com/templates/cz/>>

Príloha 6 – Phishingová webová stránka ČSOB (zdroj: hoax.cz)



Príloha 7 – Dotazník (zdroj: autorka)

Dotazník k diplomovej práci

Dobrý deň,

volám sa Diana Kalinová a obraciam sa na Vás s prosbou o vyplnenie dotazníka. Je určený používateľom e-mailu a internetu, ktorí žijú na území Českej a Slovenskej republiky a majú viac ako 18 rokov. Dotazník je anonymný a jeho vyplnením mi pomôžete získať potrebné informácie pre diplomovú prácu zameranú na phishing a ľudský faktor. Phishing je počítačovým trestným činom, pri ktorom sa útočník vydáva za dôverný zdroj (napr. banku) a snaží sa podvodným konaním získať prístup k prostriedkom používateľa (napr. údajom o platobnej karte). Najčastejšie je uskutočňovaný prostredníctvom podvodných e-mailov a webových stránok.

Vyplnenie dotazníka Vám zaberie približne 10 – 15 min. O možnosti výberu jednej alebo viacerých odpovedí budete informovaný pri jednotlivých otázkach. V prípade doplnenia vlastnej možnosti odpovedajte prosím stručne a jasne. Dotazník je rozdelený na niekoľko častí. Pre zobrazenie ďalšej časti kliknite na “Continue (Pokračovať)” a po dokončení kliknite na “Submit (Odoslať)”. Vopred Vám ďakujem za ochotu a čas, ktorý venujete vyplneniu tohoto dotazníku.

- 1. Cítite sa pri vykonávaní bežných činností vo virtuálnom svete bezpečne (napr. pri odosielaní a prijímaní e-mailov, pri nakupovaní cez internet, pri prehliadaní webových stránok, pri uskutočňovaní transakcií prostredníctvom elektronického bankovníctva atď.)?**

(vyberte jednu odpoveď)

- a. áno
- b. áno, ale bezpečnejšie sa cítim s antivírusovým a iným ochranným softvérom
- c. nie

- 2. Stretli ste sa s pojmami phishing, podvodné emaily a podvodné webové stránky? (môžete vybrať viac odpovedí)**

- a. áno, počul(a) o phishingu
- b. áno, počul(a) som o podvodných e-mailoch, ktoré sa snažia vylákať údaje
- c. áno, počul(a) som o podvodných webových stránkach, ktoré sa snažia získať údaje
- d. nie, ani jeden zo spomínaných pojmov som nepočul(a)

- 3. Máte Vy alebo Vaši známi s phishingom osobnú skúsenosť?**

(môžete vybrať viac odpovedí)

- a. áno, dostal(a) som phishingový e-mail
- b. áno, navštívil(a) som phishingové webové stránky
- c. áno, stal(a) som sa obeťou phishingu
- d. áno, moji známi alebo rodinní príslušníci dostali phishingový e-mail
- e. áno, moji známi alebo rodinní príslušníci navštívili phishingové webové stránky
- f. áno, moji známa alebo rodinní príslušníci sa stali obeťou phishingu
- g. nie
- h. neviem

4. **Považuje phishing za reálnu hrozbu v Českej a Slovenskej republike?**
(vyberte jednu odpoveď)
- a. áno
 - b. nie
5. **Viete, aké bezpečnostné opatrenia by ste mali dodržiavať, aby ste sa nestali obeťou phishingu?**
(vyberte jednu odpoveď)
- a. áno
 - b. áno, poznám niektoré opatrenia, ale nie všetky
 - c. nie

Napište aspoň jedno bezpečnostné opatrenie, ktoré doržiate aby ste sa nestali obeťou phishingu:

6. **Viete, ako si overiť a nahlásiť phishingový e-mail alebo webové stránky?**
(vyberte jednu odpoveď)
- a. áno
 - b. nie, ale určite by som našiel návod na internete
 - c. nie, ale určite by mi pomohla dotknutá organizácia
 - d. nie, ale určite by mi niekto z rodiny a známych poradil
 - e. nie, nič by som si neoveroval(a) ani neohlasoval(a)
7. **Zaznamenali ste za posledných 12 mesiacov vzdelávaciu kampaň, materiál, akciu, video alebo webovú stránku o phishingu a ochrane pred phishingom?**
(vyberte jednu odpoveď)
- a. áno
 - b. nie
8. **Všímate si varovania pred phishingovým útokom v médiách, na webových stránkach Vašej banky, obľúbeného obchodu alebo iných organizácií?**
(vyberte jednu odpoveď)
- a. áno, stále si všímam varovania
 - b. áno, ale varovania si všímam iba niekedy
 - c. nie
9. **Máte nainštalovaný na svojich zariadenia antivírusový softvér?**
(vyberte jednu odpoveď)
- a. áno
 - b. nie
 - c. neviem

10. Používate antiphishingový filter alebo nástroj?

(vyberte jednu odpoveď)

- a. áno
- b. nie
- c. neviem

11. Aktualizujete pravidelne softvér, ktorý máte nainštalovaný?

(vyberte jednu odpoveď)

- a. áno, aplikujem všetky dostupné aktualizácie
- b. áno, ale aplikujem iba vybrané aktualizácie
- c. nie

12. Ak sa vám zobrazí bezpečnostné upozornenie (zobrazené na obrázku pod otázkou), ako zareagujete?

(vyberte jednu odpoveď)

- a. prečítam si upozornenie a poslúchnem odporúčanie
- b. prečítam si upozornenie, ale neposlúchnem odporúčanie
- c. neprečítam si upozornenie



13. Používate k prihláseniu do rôznych účtov rovnaké alebo podobné prihlasovacie údaje (prihlasovacie meno a heslo)?

(vyberte jednu odpoveď)

- a. áno, používam k prihláseniu do rôznych účtov rovnaké prihlasovacie údaje
- b. áno, používam k prihláseniu do rôznych účtov variáciu tých istých prihlasovacích údajov
- c. nie, do každého účtu používam iné prihlasovacie údaje

14. Používate k prihláseniu do určitých účtov dvojfázové overovanie (napr. zadanie SMS kódu alebo kódu z grid karty po zadaní prihlasovacích údajov)?

(vyberte jednu odpoveď)

- a. áno
- b. nie

15. Čítate e-mailové správy od cudzích osôb?

(vyberte jednu odpoveď)

- a. áno, vždy a otváram aj prílohy e-mailov alebo v texte zahrnuté odkazy na webové stránky
- b. áno, vždy, ale iba niekedy otváram prílohy e-mailov a klikám na uvedené odkazy
- c. áno, vždy, ale nikdy neotváram prílohy e-mailov a neklikám na uvedené odkazy
- d. áno, niekedy a otváram prílohy e-mailov a klikám na uvedené odkazy
- e. áno, niekedy, ale nikdy neotváram prílohy emailu a neklikám na uvedené odkazy
- f. nie

16. Čítate e-mail, ktoré boli umiestnené do priečinku spam?

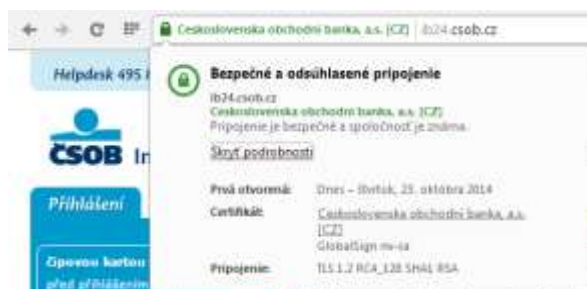
(vyberte jednu odpoveď)

- a. áno, čítam si všetky správy v priečinku spam
- b. áno, ale prečítam si iba zle zaradené správy
- c. áno, ale prečítam si iba niektoré správy
- d. nie

17. Keď sa prihlasujete do svojho účtu, kontrolujete, či ide o zabezpečené pripojenie (zabezpečené pripojenie môžete vidieť na obrázku pod otázkou)? Ak áno, podľa čoho kontrolujete zabezpečené pripojenie?

(môžete vybrať viac odpovedí)

- a. áno, skontrolujem ikonu visiaceho zámku
- b. áno, skontrolujem https v adrese webovej stránky
- c. áno, skontrolujem bezpečnostný certifikát
- d. áno, skontrolujem certifikačnú autoritu
- e. nie



18. Navštevujete odkazy, ktoré dostanete prostredníctvom e-mailu, chatu, sociálnej siete alebo rýchlych správ (Skype, ICQ)?

(vyberte jednu odpoveď)

- a. áno, aj keď sú od neznámej osoby
- b. áno, ale iba ak sú od známej osoby
- c. áno, ale iba ak som si zaslanie odkazu vyžiadal(a) alebo som bol(a) vopred s osobou dohodnutý/dohodnutá
- d. nie

19. Zvažujete, ktoré informácie o sebe zverejníte na sociálnych sieťach, webových stránkach, blogoch atď.?

(vyberte jednu odpoveď)

- a. áno
- b. nie

20. Zverejňujete o sebe informácie na sociálnych sieťach? Kto môže tieto informácie vidieť?

(môžete označiť viac odpovedí)

- a. áno zverejňujem, mnou zverejnené informácie sú verejne dostupné
- b. áno, zverejňujem informácie pre priateľov mojich priateľov
- c. áno, zverejňujem informácie pre všetkých priateľov
- d. áno, zverejňujem informácie pre určitý okruh osôb z priateľov
- e. áno, ale neviem, kto môže zverejnené informácie vidieť
- f. nie, sledujem iba informácie zverejnené priateľmi a inými osobami
- g. nie, nemám profil na sociálnej sieti

21. Ktoré z vymenovaných e-mailov sa Vám zdajú podozrivé?

(môžete označiť viac odpovedí)

- a. e-maily s prílohami
- b. e-maily, ktoré obsahujú odkazy
- c. e-maily, ktoré obsahujú tlačidlá „kliknite tu“
- d. e-maily obsahujúce formulár, do ktorého je možné vyplniť údaje
- e. informatívne e-maily
- f. e-maily, ktoré urgentne požadujú zadanie alebo zaslanie informácií
- g. e-maily, ktoré ponúkajú odmenu alebo zvýhodnenie
- h. e-maily, ktoré žiadajú o aktualizáciu alebo obnovenie údajov
- i. e-maily, ktoré upozorňujú na bezpečnostnú hrozbu
- j. e-maily, ktoré žiadajú aby ste na ne neodpovedali
- k. žiadna zo spomínaných možností
- l. iné

22. Na základe ktorých možností posudzujete dôveryhodnosť a pravosť e-mailu?

(môžete označiť viac odpovedí)

- a. odosielateľ
- b. predmet správy
- c. osobné oslovenie
- d. uvedenie dôvernej informácie (ID používateľa, posledné číslice platobnej karty,...)
- e. vzhľad
- f. obsah
- g. pravopis
- h. profesionálne prevedenie
- i. jazyk, v ktorom je správa napísaná
- j. kontaktné informácie
- k. digitálny podpis odosielateľa
- l. uvedenie konkrétnej osoby a jej pozície v organizácii

- m. zdôraznenie pravosti e-mailu
- n. zdôraznenie ochrany pred phishingom
- o. možnosť overenia e-mailu prostredníctvom telefonátu
- p. iné

23. Dôverujete e-mailom a správam, ktoré boli odoslané z e-mailovej adresy alebo prostredníctvom profilu priateľa?

(vyberte jednu odpoveď)

- a. áno, vždy im dôverujem
- b. áno, ale keď sú podozrivé, radšej iným spôsobom kontaktujem priateľa
- c. áno, ale keď sú podozrivé, radšej si obsah správy overím prostredníctvom webovej aplikácie, ktorá obsahuje databázu phishingových správ
- d. nie

24. Na základe ktorých z nasledovných možností posudzujete dôveryhodnosť a pravosť webových stránok?

(môžete označiť viacero odpovedí)

- a. adresa webovej stránky
- b. vzhľad
- c. obsah
- d. pravopis
- e. profesionálne prevedenie
- f. usporiadanie stránok
- g. funkčnosť odkazov
- h. správnosť zobrazenia obrázkov
- i. kontaktné informácie
- j. informácie o autorských právach
- k. ikona zámku v adresnom riadku prehliadača
- l. ikona zámku v obsahu webových stránok
- m. certifikát
- n. dôveryhodnosť certifikačnej authority
- o. iné

25. Ktorá z nasledovných adries webových stránok na Vás pôsobí podozrivo?

Rozhodnite sa len na základe uvedených adries. Webové stránky nenavštevujte.

(môžete označiť viacero odpovedí)

- a. <https://ib24.csob.cz>
- b. 173.252.120.6
- c. <https://www.google.cz/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0CAcQjRw&url=http%3A%2F%2Fwww.limorshiponi.com%2F2007%2F07%2F&ei=OUpJVMrMI4HvO53kgeAC&bvm=bv.77880786,d.bGQ&psig=AFQjCNE6ivLtiZpe29pRB6vbP085O3NB8Q&ust=1414175660265998>
- d. <http://www.cs.berkeley.edu/~tygar/papers/Phishing/DSS.book.pdf>
- e. <http://bit.ly/1DxhlmK>
- f. žiadna

26. Pri návšteve ktorých webových stránok ste obozretnejší?

(môžete označiť viacero odpovedí)

- a. e-shopy
- b. inzerentné a aukčné portály
- c. sociálne siete
- d. elektronické bankovníctvo
- e. školské webové stránky
- f. firemné webové stránky
- g. blogy
- h. diskusné fóra
- i. iné

27. Pohlavie:

- a. muž
- b. žena

28. Vek:

- a. 18 – 30 rokov
- b. 30 – 40 rokov
- c. 40 – 50 rokov
- d. 50 a viac rokov

29. Krajina pobytu:

- a. Česká republika
- b. Slovenská republika

30. Najvyššie dosiahnuté vzdelanie:

- a. základné
- b. stredné
- c. vysokoškolské

31. Študijné zameranie:

- a. IT
- b. iné

32. Pracovné zameranie:

- a. IT
- b. iné