ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

Katedra informačních technologií

Obor: Informatika

BAKALÁŘSKÁ PRÁCE

Krádež identity

Autor:
František Chorvát

Vedoucí bakalářské práce:
RNDr. Dagmar Brechlerová, Ph.D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Chorvát František

Informatika

Název práce
Krádež identity

Anglický název
Identity theft

Cíle práce
Cíl: Seznámení s praktikami krádeží osobních informací a způsoby předcházení těmto krádežím
a/ čím je pro zloděje krádež identity zajímavá, co tím sledují
b/ praktiky získávání
1/ phishing
2/ pharming
3/ sociální inženýrství
c/ typy podvodu s těmito identitami; jejich prodej
d/předcházení krádeži
e/ zhodnocení

Metodika
Řešení bakalářské práce je založeno na studiu, analýze a čerpání informací z odborných zdrojů týkajících se této problematiky.

Harmonogram zpracování
1/Příprava a studium odborných informačních zdrojů, upřesnění dílčích cílů práce a volba postupu řešení: 6/2011
2/Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2011 - 8/2011
3/Vypracování vlastního řešení, diskuze a zhodnocení výsledků: 9/2011 - 10/2011
4/Tvorba finálního dokumentu bakalářské práce 11/2011 - 2/2012
5/Odevzdání bakalářské práce a teze 3/2012

Rozsah textové části
30 - 40 stran

Klíčová slova
identity theft, krádež identity, phishing, pharming, sociální inženýrství, osobní údaje

Doporučené zdroje informací

Sandra K. Hoffman and Tracy G. McGinley. Identity Theft - A reference Handbook. ABC-CLIO LLC,2010, 263 s.ISBN 978-1-59884-144-2

Michael J. Arata Jr. Identity Theft for Dummies. Wiley Publishing, Inc., 2010, 261s.,ISBN 978 -0-470-56521-6

Martin T. Biegelman. Identity Theft Handbook - Detection, Prevention, and Security. John Wiley and Sons, Inc., 2009, 339s., ISBN 978-0-470-17999

Joseph T. Wells. Internet Fraud Casebook - The World Wide Web of Deceit. Johny Wiley and Sons, Inc., 2010, 383s., ISBN 978-0-470-64353-1

Vedoucí práce
Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání
březen 2012

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 21.11.2011

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci Krádež identity jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.02.2012

…….

Chorvát František

PODĚKOVÁNÍ

Rád bych zde poděkoval své vedoucí bakalářské práce RNDr. Dagmar Brechlerové, Ph.D. za odborné vedení a možnost výběru tohoto tématu. Rád bych také poděkoval mé sestře Monice za její velkou podporu. A také všem ostatním, kteří mne různým způsobem podporovali.

„Život je neustálý podvod, ve velkém i malém.“

Johnatan Swift

Krádež identity

Identity theft

Souhrn: Bakalářská práce seznamuje její čtenáře s pojmem krádež identity a popisuje typy útoků, díky nimž útočníci získávají nelegálně osobní údaje a jiné citlivé obchodní informace.

Summary: This bachelor thesis introduces to readers a term “identity theft” and describes what kind of attacks potential thieves use for illegal collection of various personal data and other sensitive bussines information.

Klíčová slova: krádež identity, osobní údaje, phishing, pharming, sociální inženýrství, internetový podvod.

Keywords: identity theft, personal data, phishing, pharming, social engineering, internet fraud.

OBSAH

1 ÚVOD

Téma bakalářské práce „Krádež identity“ bylo zvoleno záměrně, protože většina z nás denně využívá služeb internetových bankovnictví, nákupů online či komunikace. Přestože jsou osobní údaje vnímány jako to nejdůležitější, co každý z nás má, tak jejich ochraně při práci s internetem není mnohdy věnována dostatečná pozornost. A to může v nejhorším případě vést až k zneužití těchto údajů a citelné finanční ztrátě.

S krádežemi identity se lidstvo setkává již delší dobu. Riziko představují zejména ztracené nebo odcizené osobní doklady (nejčastěji občanské průkazy a různé karty, které jsou nošeny v peněženkách). Na ukradené doklady pak může být podvodníky získána půjčka, vypůjčeno vozidlo, které pak není vráceno, uzavřena smlouva apod. Okradená osoba tak může být i po letech nemile překvapena.

S rozmachem internetu však tento zločin nabývá nových rozměrů a riziko zneužití osobních údajů prudce stoupá. Zde se však již nekradou „pouze“ peněženky, ale jsou používány důmyslné podvodné metody, díky nimž může útočník získat např. uživatelovy přístupové údaje k účtům, hesla, čísla kreditních karet s daty jejich expirace aj. Krádež identity je považována za to nejhorší, co se může na internetu stát, a mezi lidmi povědomí o těchto podvodných technikách není bohužel stále moc rozšířeno.

2 CÍL PRÁCE A METODIKA

2.1 CÍL PRÁCE

Cílem práce je seznámit s problematikou podvodného získávání osobních informací na internetu, což se dnes při masivním využívání počítačové sítě internet dotýká téměř každého člověka, který s ní pracuje.

2.2 METODIKA

Teoretická část je rozdělena do pěti kapitol a je realizována studiem odborných textů týkajících se této problematiky. První kapitola seznamuje s pojmem identita a je úvodem pro kapitoly následující. Druhá kapitola se zaměřuje na manipulační metodu nazývanou sociální inženýrství, která je při podvodech uplatňována. Ve třetí kapitole se čtenář seznámí s podvodnou metodou Phishing, jejím historickým vývojem a znaky, podle kterých lze identifikovat podvodný e-mail. Následující kapitoly se věnují dalším podvodným metodám jako je Vishing a Pharming.

Vlastní část je rozdělena do dvou kapitol. V první kapitole je popsán teoretický útok na internetové bankovnictví České spořitelny, který slouží pro demonstraci toho, jak takový phishingový útok může vypadat a jak probíhají jeho přípravy. V druhé kapitole je vyhodnocen autorův dotazník, který vznikl pro zjištění informovanosti lidí o tématech, kterými se zaobírá tato bakalářská práce.

3 TEORETICKÁ ČÁST

3.1 IDENTITA

Krádež identity není žádnou novinkou několika posledních let, jedná se o již dlouho známý podvod. Jen se nyní převážně přesídlil ze „skutečného“ světa do světa počítačů, kde je mnohdy jednodušší získat potřebné údaje než ve světě skutečném, a to i s menším rizikem odhalení, dopadení a následky. Níže uvedená tabulka porovnává klasický trestný čin (ozbrojené přepadení) s trestným činem způsobeným pomocí počítače (tzv. kybernetický útok).

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn nebo zabit	Bez rizika fyzického zranění
Zisk	Průměrně 3 až 5 tisíc USD	od 50 až do 500 tisíc USD
Pravděpodobnost dopadení	Dopadeno 50 až 60 % útočníků	Dopadeno cca 10 % útočníků
Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených útočníků	Z dopadených útočníků dojde k soudnímu projednávání u 15 % útočníků a z nich je skutečně odsouzeno jenom 50 %
Trest	Průměrně 5 až 6 let, pokud pachatel nikoho nezranil	Průměrně 2 až 4 roky

Tabulka 1- Porovnání následků klasického a internetového trestného činu. Zdroj (1) str. 30

V roce 2007 byly FTC[1] zveřejněny výsledky výzkumu, ze kterých vyplynulo, že v roce 2005 se stalo obětí krádeže identity 8,4 milionu Američanů; krádež identity byla označena jako nejrychleji rostoucí trestný čin; ve 25 % případů oběť „znala“ svého zloděje; v 50 % případů oběť dodnes vůbec neví, jak jí byly osobní údaje ukradeny (2). Je třeba však uvést, že tyto údaje se z větší části netýkají krádeže identity na internetu, ale krádeže identity v běžném životě (krádeže šekových knížek, krádeže kreditních karet; získávání privátních informací z dopisů v poštovních schránkách, vydávání se za jiného atd.)

[1] Federal Trade Commission – americký úřad pro ochranu spotřebitelů před využíváním dominantního postavení na trhu velkými společnostmi

Pod pojmem identita se rozumí souhrn několika osobních údajů, tj. údajů, díky kterým můžeme ať již přímo, či nepřímo identifikovat konkrétního člověka (fyzickou osobu) nebo firmu (právnickou osobu). U osob to může být jméno, příjmení, adresa bydliště, rodné číslo, číslo bankovního účtu, čísla kreditních karet, datum narození, číslo občanského průkazu, číslo řidičského průkazu, přístupové údaje k bankovním účtům atd. V případě firem a organizací se nejčastěji jedná o informace, jako jsou např. název firmy, adresa sídla, telefonní čísla, údaje o zaměstnancích, logo, e-mailové adresy, obchodní značka, údaje o firemních kreditních kartách, šeky atd. (3).

„Krádež identity jsou všechny druhy trestné činnosti spočívající v podvodném získání a zneužití cizích osobních údajů obvykle ze zištných důvodů“ (4). Mezi nejčastější motivace útočníků patří:

- finanční zisk (např. získání přístupu k bankovnímu účtu oběti; úvěry na falešné doklady);
- pomsta (např. spáchání činů pod identitou jiné osoby, což může vést ke ztrátě zaměstnání příp. ostudě);
- využití údajů k dosáhnutí vlastních cílů (využít získané údaje a dle nich přizpůsobovat své chování, např. firemní konkurence).

3.2 SOCIÁLNÍ INŽENÝRSTVÍ

„Soukromé osoby se mohou držet všech nejlepších zásad doporučovaných odborníky, mohou otrocky nainstalovat všechny nejnovější produkty vylepšující zabezpečení a odpovídajícím způsobem pozorně zkonfigurovat systém, mohou použít všechna jeho vylepšení či opravy, a přece jsou tyto osoby stále nechráněné“ (5).

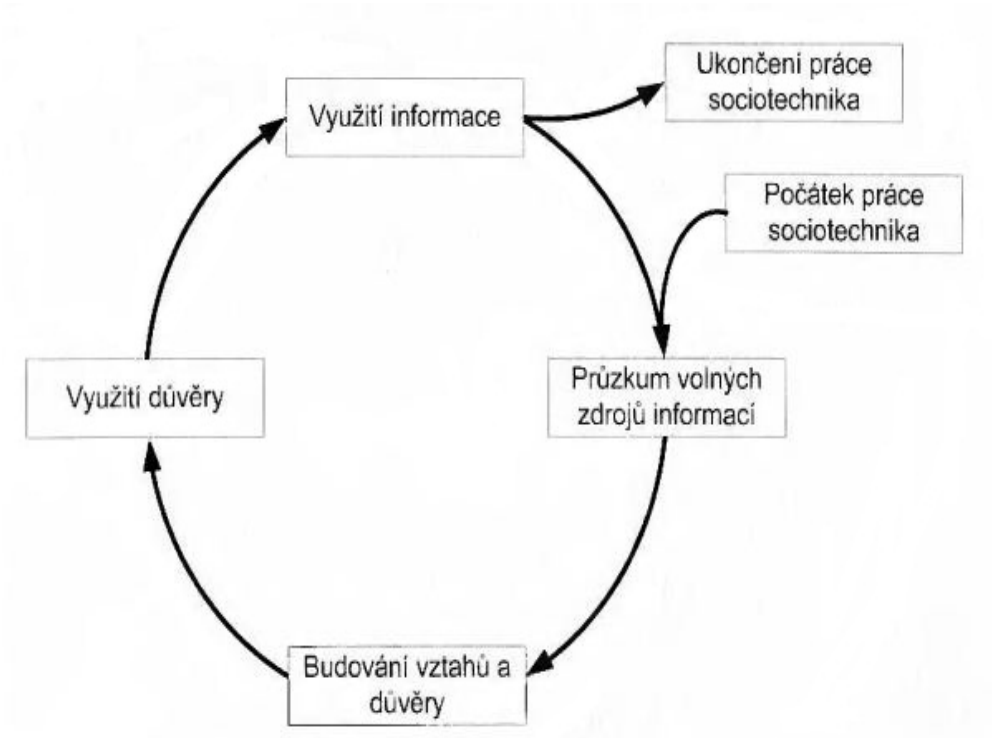
Za sociální inženýrství je označován způsob manipulace založený na ovlivňování za účelem provedení určité akce, případně sdělení informace. Podvodník, který využívá tento druh manipulace, je označován jako sociotechnik. Sociotechnik se snaží, aby jeho oběť uvěřila, že je osobou, za kterou se vydává pro potřeby manipulace a dosažení svých cílů.

Tato kapitola je rozdělena na dvě části. První část se věnuje útokům s cílem získat, resp. vylákat interní informace z firem. V této části jsou popsány jednotlivé fáze práce sociotechnika a slabiny obětí, na které se útočník zaměřuje. Druhá část se věnuje odlišnostem podvodných technik při útoku na soukromé osoby, kde je nejčastějším cílem přístup k počítači, bankovním účtům či ke kreditním kartám obětí.

3.2.1 *ÚTOK NA SPOLEČNOSTI*

Tato část se zaměřuje na získání interních informací z firmy. Těmito informacemi můžou být účetní výkazy, osobní informace zaměstnanců, přístupové údaje do systémů, informace o kreditních kartách, telefonní čísla, know-how a jiné privátní informace.

Činnost sociotechnika při získávání informací je možné rozdělit do několika fází, jak je znázorněno na Obrázek 1.



Obrázek 1 - Sociotechnický cyklus. Zdroj (1)

Fáze 1. Průzkum volných zdrojů informací

V této fázi sociotechnik shromažďuje informace z veřejně dostupných zdrojů, jako jsou internetové vyhledávače (např. články na internetu, internetová fóra), stránky firmy aj. Mezi nejčastěji získané informace z těchto zdrojů patří e-mailové adresy, telefonní čísla, historie firmy, jména některých zaměstnanců firmy. Z těchto informací si sociotechnik sestavuje profil své budoucí oběti, mapuje slabá místa oběti a hledá vhodnou taktiku pro útok (1).

Fáze 2. Budování vztahů a důvěry

Tato fáze je časově náročná, neboť vybudování vztahu mezi obětí a sociotechnikem, zejména získání důvěry oběti není jednoduchou záležitostí. Na začátku vzájemné komunikace se probírají sociotechnikem předem vybraná témata týkající se každodenních záležitostí. Po získání určité důvěry nastává období, kdy sociotechnik do obyčejných rozhovorů vkládá menší dotazy, které postupným skládáním vedou k získání jím požadované informace. Oběť častokrát ani netuší, že se stala obětí sociotechnického útoku (1).

Fáze 3. Využití informace

V této fázi sociotechnik už jen pouze nakládá se získanou informací, kterou můžou být v případě firem například přístupové údaje do firemních systémů apod., a jeho práce sociotechnika zde končí.

3.2.1.1 Psychické slabiny obětí

Mezi nejslabší místa, na které sociotechnici v komunikaci cílí, jsou:

- **zbavení se odpovědnosti** – útočníkovi hodně pomáhá, když u oběti vyvolá pocit, že v případě, že se stane něco špatného, neleží celá zodpovědnosti jen na ní, ale také na některých dalších kolezích, případně na nadřízeném (typickou frází je „*operace již byla schválena nadřízeným*“);

- **společenský souhlas -** oběť je ochotnější vyhovět útočníkově žádosti, pokud tento zmíní, že jiné osoby jeho prosbě již vyhověli („*vyplňte to, prosím, Petr a Pavel ze čtvrtého patra to již udělali*“)
- **důvěra;**
- **morální povinnost** – vyvolání pocitu dějícího se bezpráví, kdy jen oběť může útočníkovi v dané situaci pomoci;
- **odměna** – oběť uvěří, že po splnění získá nějakou odměnu (dobrý pocit, potěšení nadřízeného, finanční odměna, lepší postavení ve firmě);
- **altruismus[2] oběti;**
- **pocit viny**
    - vytvoření psychického tlaku, že pokud oběť nesplní požadavek, bude se cítit provinile („*výpomoc kolegovi v nouzi*“);
    - vytvoření situace, kdy se již oběť cítí provinile, ta pak udělá vše, co je v jejích silách, aby se tohoto pocitu zbavila;
- **sympatie** – oběť o to více vyhoví, pokud zjistí, že sociotechnik je osobou, co má podobné názory a zájmy jako oběť (1) (5).

3.2.1.2 Varovné příznaky útoku

Níže uvedený seznam obsahuje varovné signály, které mohou indikovat pokus o sociotechnický útok:

- *„odmítnutí sdělit zpáteční číslo;*
- *neobvyklá žádost;*
- *ohánění se autoritou;*

[2] Jednání ve prospěch druhé osoby. Opak egoismus

- *zdůraznění naléhavosti záležitosti;*
- *hrozba důsledky nevyhovění žádosti;*
- *neochota volajícího odpovídat na dotazy;*
- *zmiňování mnoha jmen;*
- *komplimenty […]"* (5).

Je třeba si však uvědomit, že ne ve všech případech, kdy se s varovným signálem potkáme, půjde o akci sociotechnika, nicméně v těchto případech je vhodné zbystřit.

3.2.2 ÚTOK NA SAMOSTATNÉ OSOBY

Útok na jednotlivé osoby se příliš neliší od útoku na větší čí menší společnosti, proto lze techniky uvedené v podkapitole Útok na společnosti ve většině případů použít i pří útoku na jednotlivce, a naopak, útoky směřující primárně na jednotlivce, jako jsou phishing a pharming (více v samostatných kapitolách), lze použít při útoku na společnosti. Cyklus fází činnosti sociotechnika je taktéž stejný, jen s tím rozdílem, že ve fázi průzkumu volných zdrojů informací toho sociotechnik o jednotlivci často nenalezne tolik jako o firmě, zvláště pak pokud osoba nežije internetovým společenským životem, tj. nezúčastňuje se diskusních fór, nebo nevlastní profily na sociálních sítích (Facebook, Myspace, Hi5 atp.).

3.2.3 REVERZNÍ SOCIÁLNÍ INŽENÝRSTVÍ

Někdy se můžeme setkat také s tzv. reverzním sociálním inženýrstvím. Při tomto typu manipulace je přímo útočeno na konkrétní vybranou oběť. Příkladem může být pokus sociotechnika o získání přístupu k firemnímu počítači oběti. Nejdříve útočník zkontaktuje oběť a představí se jako správce počítačové sítě ve firmě. Provede konverzaci ve stylu, že jsou nově přeinstalovávány podnikové systémy například z důvodu virové nákazy sítě, a že je možné, že se vyskytnou nějaké problémy. Nechá oběti kontaktní informace, pro případ, že by se u oběti tyto problémy vyskytly. Tím se snaží u oběti navodit pocit důvěry. Nyní

přichází nejtěžší část práce sociotechnika, a to vyvolat problém na počítači oběti. Pokud se mu to povede, oběť ho s největší pravděpodobností sama kontaktuje a v následné konverzaci mu v domnění, že mluví s firemním technickým pracovníkem, sdělí přístupové údaje do svého počítače, případně ještě další informace, k nimž bude sociotechnik konverzaci nenápadně směřovat (6).

3.3 PHISHING

3.3.1 CO TO JE

Phishing je jedna z nejvíce používaných technik k podvodnému získaná osobních údajů, která využívá metody sociálního inženýrství. Převážná část podvodných e-mailů se tváří, že přichází z bankovních institucí, spořitelen, aukčních serverů nebo sociálních sítí. V přijaté zprávě je na oběť vyvíjen tlak, v případě bank například, že došlo k podezřelé transakci z účtu oběti a je třeba tuto transakci zkontrolovat. Součástí zprávy je také odkaz směřující na útočníkovy stránky, které jsou téměř identické s pravými stránkami banky. Oběť zadá své osobní údaje, v daném případě tedy přístupové údaje k účtu internetového bankovnictví. Tyto údaje se uloží na útočníkovu stránku, čímž tento získá přístup k účtu oběti a jejím financím.

Na odborné stránce www.hoax.cz zabývající se počítačovou bezpečností je phishing definován takto:

„PHISHING je druh internetového podvodu, kterým se podvodníci snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro svoje obohacení. K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vypadají, že jsou odeslány přímo z banky a snaží se přesvědčit uživatele, aby kliknul na odkaz. Jestliže neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde jsou po něm požadovány přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Pokud je uživatel naivně vyplní, získají tato data podvodníci, kteří je následně využijí pro svůj prospěch“ (7).

Je možné se setkat také s tzv. spear phishingem, kdy se jedná o phishing zaměřený na určitou konkrétní osobu a je dělán tzv. „na míru“. Podvodný e-mail je sestaven tak, aby oběť opravdu zaujal a tím se zvýšila pravděpodobnost, že na něj zareaguje. E-mail z banky se například může vztahovat k poslední známé transakci oběti. Nebo v případě sociálních sítí je možné se setkat s tím, že oběti byla poslána časově omezená pozvánka k přidání se ke skupině se slevami na bílé zboží (ví-li útočník, že oběť má v plánu si v nejbližší době pořídit třeba ledničku).

3.3.2 VZNIK NÁZVU

Anglický název phishing vznikl z anglického slova fishing (česky rybaření). Tento typ útoku je totiž přirovnáván k rybaření, kdy jsou pomocí spamu[3] rozeslány velkému počtu lidí podvodné e-maily a pak se jen čeká, až se někdo „chytí“, tedy až adresát útoku klikne a vyplní požadované údaje, čímž je uloven. V názvu pak už jen došlo k záměně písmene „f“ za znaky „ph“.

3.3.3 HISTORIE

První zmínky o phishingu, takovém, jak ho známe dnes, jsou z přelomu roku 1995 a 1996, kdy byly provedeny první phishingové útoky na uživatele služeb firmy AOL[4]. Jednalo se o zprávy skrze uživatelské rozhraní AOL, kdy se phisher[5] vydával za technického pracovníka AOL a tvrdil, že je nutné zadat uživatelské jméno a heslo k AOL účtu. V této době mezi běžnými uživateli nebyly známy a používány téměř žádné, alespoň základní, bezpečnostní návyky, tak jak je tomu dnes, a proto uživatele ani nenapadlo, že by ten, komu své uživatelské jméno a heslo sdělují, mohl být někdo jiný než administrátor AOL.

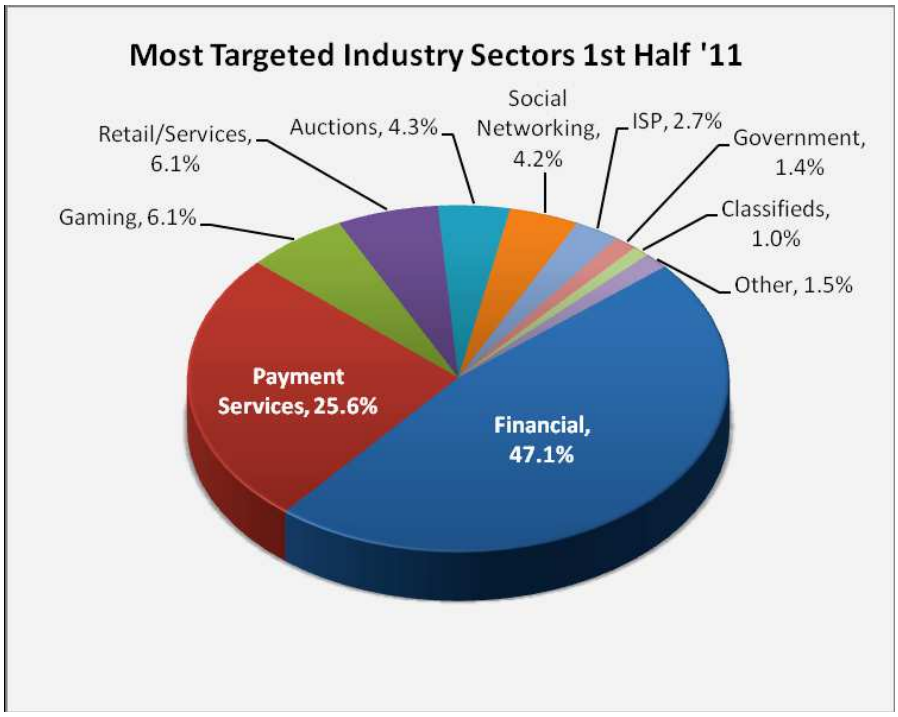
[3] Nevyžádané zpráva, nejčastěji komerčního rázu
[4] AOL – America Online. V té době jeden z největších poskytovatelů internetového připojení a služeb v USA.
[5] Tvůrce phishingového útoku

Určitým mezníkem v historii phishingových útoků se stal rok 2001, kdy došlo k prvnímu útoku se zaměřením na finanční instituci, a to konkrétně E-gold[6]. Dalším mezníkem byl rok 2003, kdy již došlo k útokům na bankovní instituce Citibank a Wells Fargo (8). S rokem 2003 dochází k masivnímu šíření podvodných e-mailových zpráv až do dnešních rozměrů. Dle zprávy sdružení The Anti-Phishing Working Group (APWG) došlo k nejvyššímu počtu odhalených phishingových stránek za první polovinu roku 2011 v březnu, kdy bylo odhaleno 38173 stránek (9) (Obrázek 2). Rekord stále drží měsíc srpen z roku 2009, kdy došlo k odhalení 56362 phishingových stránek (10).

Obrázek 2 - Počet odhalených phishingových stránek za první polovinu roku 2011. Zdroj: www.antiphishing.org

Na Obrázek 3 jsou znázorněna graficky jednotlivá odvětví napadaná phishingem. Nejčastěji napadaným odvětvím se v první polovině roku 2011 stalo odvětví finanční s 47,1 %, na druhém místě skončily platební systémy s 25,6 %.

[6] E-gold - elektronický platební systém



Obrázek 3 – Odvětví napadaná phishingovými útoky nejčastěji v 1. polovině 2011. Zdroj: www.antiphishing.org

3.3.3.1 AOHell

Svým způsobem se stal revolučním program AOHell, který byl napsán uživatelem Da Chronic. AOHell obsahoval vymoženosti, které využívaly chyb v softwaru AOL např.:

- phishing (v AOHell pojmenováno jako CC/PW Fisher, kdy CC znamená „Credit Card“ a PW „password“);
- psaní do chatu pod přezdívkou jiného;
- odpojení momentálně připojeného uživatele;
- zahlcení e-mailové schránky velkým množstvím zpráv;
- vytvoření falešného, ale přesto funkčního AOL účtu atd. (11) (12)

Důvodem ke vzniku tohoto programu byla nenávist jeho tvůrce vůči AOL kvůli tomu, že AOL tvrdě zasahovala proti hackerské scéně, ale proti pedofilům nic nečinila (viz níže uvedené prohlášení Da Chronica v manuálu k AOHell).

„Důvodem proč jsem vytvořil tento program, je, že prostě nesnáším všechny na AOL. (ano, to znamená pravděpodobně i TEBE). Je mi zle ze všech těch teploušů, a na zvracení ze všech těch zpropadených pedofilů. Všechny místnosti jsou pojmenovány nějak takhle "Tátova holčička", "fotky mladých chlapců", "Chlap pro Chlapa", […] Dokonce jsem viděl místnost pojmenovanou "Kluk pro chlapa ke znásilnění". Jednoho dne jsem se rozhodl, že už je toho dost.

AOL neustále uzavírá "hackerské" místnosti, ale odmítá něco dělat s těmi pedofilními. Jednou jsem napsal dohledovému pracovníkovi AOL a zeptal jsem se ho, proč zavírají hackerské místnosti a ty s dětským pornem ne. Neodpověděl, místo toho mi zrušil účet. Hádám, že z tohoto tedy vidíme, kde leží priority AOL. Pokud AOL nic nebude dělat s tímto zvráceným chováním, tak udělám vše, co můžu, abych zničil AOL. Myslím, že dvacet tisíc idiotů používajících AOHell k vykopávání lidí z místností, kradení hesel a informací o kreditních kartách, a v podstatě k obtěžování všech ostatních, je dobrý začátek. Da Chronic“. (12)

Tento program AOHell tedy stál při zrodu phishingu.

3.3.3.2 První český phishingový útok

Až do roku 2006 byli čeští uživatelé před phishingovými útoky chráněni díky českému jazyku, který byl pro většinu zahraničních útočníků nepřekonatelný. Nepočítaje amatérské pokusy o phishingové útoky na majitele účtů na webových fórech nebo malých stránkách, se tak první český phishingový útok odehrál „až“ v pátek 3. března 2006. Tento den byly v ranních hodinách obětem odeslány e-maily s žádostí o přihlášení se k internetovému bankovnictví z důvodu nutnosti potvrdit převod zahraniční platby na účet oběti pod pohrůžkou její ztráty (13). Text tohoto phishingového útoku je uveden na Obrázek 4.

Od: Citibank Online [alerts@citibank.cz]
Komu: Petr Nadenicek
Kopie:
Předmět: Important notice: Confirm Payment

citibank

Serial EM202-16

Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.

Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

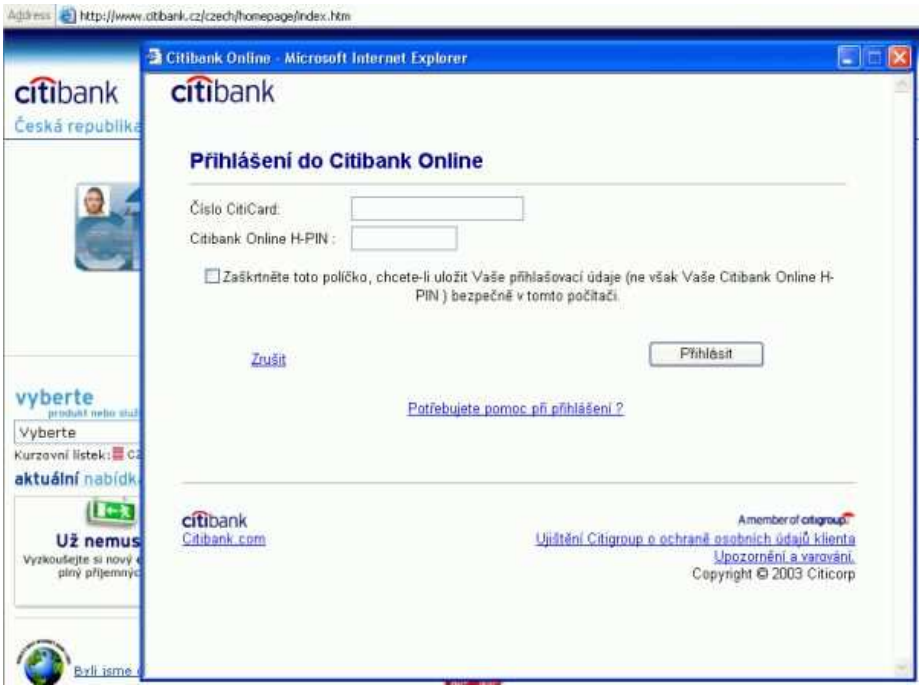
Pro vstup do programu CitiBank® online, **klikněte sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Obrázek 4 – Text phishingového e-mailu z března 2006. Zdroj: www.mesec.cz

Po kliknutí na odkaz „klikněte sem“, který byl ve výše uvedeném e-mailu, se otevřela stránka na adrese http://citi-online.czechrepublic-online.com/. Na ní došlo k okamžitému otevření pop-up[7] okna a přesměrování na oficiální stránku Citibank (13). Kombinace pravé stránky Citibank a vyskakovacího okna se skrytým adresním řádkem, působila pro člověka, který nebyl o možnostech phishingových útoků nikterak informován, poměrně věrohodně. Vyskakovací okno je možno vidět na Obrázek 5. Tato forma útoku by v dnešní době neobstála, jelikož většina dnešních prohlížečů již automaticky v základní verzi obsahuje alespoň základní blokování vyskakovacích oken, a pro starší prohlížeče existují volně dostupné doplňky k tomuto blokování.

[7] Vyskakovací okno



Obrázek 5 – Falešné vyskakovací okno, v pozadí oficiální stránky Citibank. Zdroj: www.mesec.cz

Dle vyjádření paní Markéty Dvořáčkové z tiskového odboru Citibank byla podvodná stránka vyřazena do několika hodin a žádný z klientů banky neutrpěl finanční ztrátu v důsledku zneužitých údajů.

"*Citibank se podařilo vyřadit stránku z provozu pár hodin poté, co se objevily první falešné emaily. Bezprostředně po zjištění podezření na phishing, byli naši klienti informováni o podvodných emailech prostřednictvím SMS zpráv a emailu. Žádný z klientů Citibank neutrpěl finanční ztrát*“" (13).

Avšak dle informace uvedené na serveru Lupa.cz ze dne 11.04.2006, došlo k zatčení jednoho ze spolupachatelů tohoto útoku, konkrétně osoby najaté na vybrání hotovosti z konta jednoho klienta, který tomuto podvodu naletěl (14).

V tomto případě tak lze vystopovat několik charakteristických znaků pro phishing

- Prvním byl e-mail, který se tvářil, že přišel z adresy patřící společnosti Citibank – alerts@citibank.cz, a to včetně grafického zaobalení e-mailu ve stylu Citibank. Jedná se o poměrně jednoduchý trik používaný k navození důvěry.

- Druhým znakem bylo využití sociálního inženýrství, a to nátlaku a postrašení uživatele, že pokud do 48 hodin nepotvrdí přijatou transakci, bude mu přijatá částka odečtena z účtu a navrácena odesílateli.

- Třetím znakem bylo využití falešného odkazu v těle e-mailu, který vedl na podvodný web, kde bylo otevřeno vyskakovací okno a zároveň došlo k okamžitému přesměrování původní stránky na pravou domovskou stránku společnosti Citibank. V tomto případě se tedy mohlo zdát, že vyskakovací okno patří Citibank a přihlášení je tedy bezpečné.

Bylo tedy použito:

- **použití falešného odesílatele e-mailu;**
- **nátlaku, vyvolání strachu;**
- **podvodného odkazu;**
- **podvodné stránky s vyskakovacím oknem.**

3.3.4 JAK POZNAT PHISHING

Téměř většina phishingových útoků má velmi podobné znaky, díky kterým lze tyto útoky poměrně jednoduše identifikovat. Mezi ty základní patří:

1) Žádost o přihlášení k účtu již v e-mailu – bankovní ani finanční instituce nikdy přes e-mail nežádají přihlášení klienta, případně uvedení přihlašovacích údajů svých klientů.

2) Po kliknutí na odkaz se oběť dostane na úplně jinou stránku, než na kterou se chtěla dostat (v adresním řádku je možné vidět jinou adresu). Adresa může být dlouhá a na první pohled divná (jako v případě dříve uvedeného prvního českého phishingového útoku - http://citi-online.czechrepublic-online.com/.) anebo je možné, že útočník má zaregistrovanou doménu s jinou koncovkou než má pravá stránka –např. .com, .eu, .net. Dále může útočník využít méně

nápadné záměny písmen, které jsou v psaném textu sobě podobná. Jako typický například lze uvést dvojice:

- l x I, tedy malé písmeno L a velké písmeno I,
- O x 0, tedy písmeno O a číslice nula atd.

3) Některé pokusy o útok obsahují gramatické chyby. Lze očekávat, že velké společnosti jako banky, pojišťovny atd. své zprávy nechávají projít jazykovou korekcí. I toto tak může být pro oběť varovným signálem.

4) Velká většina zpráv je psána bez diakritiky, díky složitému kódování českých znaků. Jedná se o jeden z **typických znaků českých phishingových zpráv**.

5) Zpráva se snaží oběť vyděsit případně na ni vytvořit nátlak (*„pokud se nepřihlásíte do XX hodin, Váš účet bude zrušen/zablokován“*).

6) Podvodné stránky tvářící se jako internetová bankovnictví na rozdíl od těch skutečných nepoužívají zabezpečený protokol HTTPS[8], a komunikace tedy probíhá přes obyčejný protokol HTTP[9].

3.3.5 TYPOSQUATTING

Typosquatting je taktéž jeden z phishingových útoků. Zde však nedochází k hromadnému rozesílání e-mailů s podvodným odkazem, ale využívá se zde překlepů při psaní názvu internetových adres.

Pro demonstraci si představme, že existuje banka s názvem Ultra Banka a.s., která má zaregistrovanou doménu www.ultrabanka.cz. Na začátku si útočník zaregistruje doménu[10], která zní velmi podobně. Klient se tak jednoduše při překlepu lapí do útočníkovy pasti, neboť při letmém přelétnutí očima přes adresní řádek si s velkou pravděpodobností této chyby nevšimne. Pro generování překlepů se dá využít veřejně

[8] Šifrovaná varianta protokolu HTTP
[9] Protokol pro přenos obrázků, textu atd. mezi webových serverem a prohlížečem
[10] Adresa, pod kterou vystupuje webová stránka na internetu (např. www.seznam.cz)

dostupné služby na adrese www.nastroje.webtrh.cz/preklepy. V našem příkladu si tedy útočník může zaregistrovat doménu www.ulrabanka.cz, www.ulrtabanka.cz, www.utrabanka.cz, www.ultrabamka.cz , www.ultrbanka.cz a další.

3.3.6 VISHING A SMSHING

Vishing je obdoba phishingu, ale namísto internetových stránek je využito telefonu nebo VoIP (např. Skype)[11]. Stejně tak SMShing, kde je využíváno textových zpráv.

Útok ale jinak probíhá velmi podobně. Útočníkem je připraven automatizovaný systém pro posílání SMS nebo vytáčení telefonních čísel. Po zvednutí sluchátka je oběti sděleno, že se vyskytl nějaký problém s jeho bankovnictvím nebo kreditní kartou a je odkázán na jisté telefonní číslo. Po zavolání na něj je vyžadováno, aby zadal informace o své kreditní kartě nebo přístupové údaje k internetovému bankovnictví (15).

3.4 PHARMING

Snadná odhalitelnost a postupem času i informovanost obyčejných uživatelů o možnostech phishingových útoků zapříčinila vznik novější zdokonalené verze phishingu. Tato varianta dostala jméno Pharming a je, dá se říci, mnohem nebezpečnější než phishingové útoky.

Aby uživatel nalezl určitou webovou stránku, musí znát její doménové jméno (seznam.cz, google.cz). Tato doménová jména ale vznikla pouze pro ulehčení práce lidem. Počítače pro komunikaci a vyhledání stránky používají IP adresy, což je pouze souhrn čísel. Aby mohla být nalezena webová stránka, kterou uživatel požaduje, musí být doménové jméno pomocí DNS serveru převedeno na IP adresu. Pomocí ní pak probíhá komunikace mezi počítači. Pro lepší pochopení je zde uveden příklad.

Uživatel zadá do prohlížeče internetovou adresu www.seznam.cz. Počítač nejdříve zkontroluje svůj *hosts* soubor (viz kapitola Soubor hosts), zdali se v něm nenachází IP

[11] VoIP je technologie umožňující telefonování prostřednictvím počítačové sítě

adresa nastavená pro uživatelem zvolenou doménu. Pokud zde nenajde žádný záznam, kontaktuje patřičný DNS server, který počítači vrátí IP adresu 77.75.76.3. S touto adresou začne počítač pracovat a připojí se na požadovanou stránku. Celá problematika DNS serverů je mnohem složitější, ale pro pochopení provádění pharmingových útoků uvedený popis postačí.

Při pharmingových útocích je buď útočeno na počítač uživatele, konkrétněji na soubor *hosts*, nebo přímo na DNS server.

3.4.1 ÚTOK NA DNS SERVER – CACHE POISONING

Cílem tohoto útoku je podvržení falešné adresy ke stránce do cache paměti DNS serveru internetového providera (dále označován jako „A“). DNS cache server si dočasně uchovává informace o předchozích dotazech na překlad doménových jmen ve své paměti, aby nemusel neustále při každém dotazu posílat žádosti na další DNS servery. Dochází tedy k urychlení komunikace mezi klientem a DNS serverem. (16)

Této dočasné paměti využívá útočník, který se dotáže na překlad adresy serveru A, ten nezná IP adresu a proto posílá svůj dotaz dalšímu DNS serveru (dále označován jako server „B“) a čeká na odpověď. V tomto momentu útočník serveru A odesílá velké množství falešných odpovědí tvářících se, že jsou od serveru B. Velké množství odpovědí útočník posílá z důvodu, že každý dotaz serveru A na B má své originální číslo (transaction ID). Toto 16bitové číslo identifikuje samotný dotaz, proto je nutné na dotaz odpovědět se stejným číslem. Více o problematice transaction ID lze nalézt v překladu zprávy o DNS cache poisoningu na serveru českého správce domén nic.cz:

„[…]Specifikace DNS protokolu obsahuje i pole transaction ID o délce 16 bitů. Pokud je specifikace implementována správně a transaction ID je náhodně vybráno robustním generátorem náhodných čísel, bude útočník potřebovat v průměru 32 768 pokusů, aby ID mohl předpovědět. Některé nekvalitní implementace mohou pro toto pole používat menší počet bitů, takže útočníci potřebují méně pokusů. Existují také známé nedostatky generování náhodných čísel v poli transaction ID.[…]“ (17).

Jelikož útočník toto číslo nezná, posílá tedy velké množství odpovědí, u kterých toto číslo mění, a doufá, že se trefí, případně využije nějaké programové chyby na serveru A. V případě, že k tomu dojde, zapíše se podvržená adresa do tabulky na serveru A, a každý, kdo se serveru bude dotazovat na stránku, kterou na server A uložil útočník, bude přesměrován na falešnou adresu. To vše se bude dít do té doby, než vyprší TTL[12] u tohoto záznamu.

3.4.1.1 Obrana

Obrana proti cache poisoningu spočívá v používání rozšíření DNS na straně DNS serverů, a to DNSSEC. U tohoto rozšíření je při přenosu využíváno asymetrické kryptografie tj. dvou klíčů. Držitel domény si vygeneruje dva klíče – soukromý a veřejný. Pomocí soukromého klíče veškeré údaje, které o své doméně vkládá do DNS, podepíše. Veškerá komunikace mezi DNS servery kontroluje platnost dat pomocí veřejného klíče. Tím je tedy zajištěna důvěryhodnost dat a není možné provést cache poisoning. Nutno říci, že tohle vše probíhá v režii správců domén a DNS serverů. (18) (19)

3.4.2 SOUBOR HOSTS

Jak již bylo lehce nastíněno v úvodu, při zadání adresy dochází prvně k prohledání souboru *hosts* ještě před samotným kontaktováním DNS serveru. Ve své podstatě tento soubor slouží k přenastavení DNS záznamů. Na každé řádce tohoto souboru je uvedena IP adresa, mezera a pak doména.

Umístění souboru závisí na tom, na jakém operačním systému se pracuje. U Unixových operačních systému se nachází v */etc/hosts.* U Windows XP, Windows Vista, Windows 7 je umístění *%SystemDrive%\WINDOWS\SYSTEM32\DRIVERS\etc*.

[12] Time to Live – čas, po jehož uplynutí dojde k vymazání záznamu z paměti DNS serveru, a při dalším dotazování dojde k novému získání cílové IP adresy a opětovnému uložení do paměti

Obsah souboru hosts může vypadat následovně:

127.0.0.1 localhost

77.75.76.3 www.seznam.cz

Toto znamená, že při použití adresy *localhost* dojde k přesměrování na 127.0.0.1, a to je domácí počítač. Při použiti www.seznam.cz bude kontaktována IP adresa 77.7.5.76.3.

Některé antispywarové programy (např. Spybot – Search & Destroy) tento soubor používají k blokování známých škodlivých stránek, takže uživatelé těchto programů mají ve valné většině v tomto souboru více domén a IP adres. Blokování spočívá v přesměrování známé škodlivé adresy na IP adresu lokálního počítače, takže k načtení podvodné stránky, příp. stránky, která by nějak mohla ohrozit počítač v podobě nebezpečných skriptů nebo virů, vůbec nedojde.

Útočník tedy např. nějakým programem může u uživatele způsobit přidání jednoho řádku, který bude upravovat IP adresu určité stránky, a jelikož je nejdříve prohledáván tento soubor *hosts*, tak pokud se v něm zadaná stránka nachází, nedojde ke kontaktu DNS serveru a uživatel bude automaticky připojen na útočníkem zadanou IP adresu. Pokud se tedy útočníkovi podaří do souboru *hosts* propašovat řádek ve formátu „x.x.x.x www.banka.cz“, kde „x.x.x.x“ je IP adresa útočníkova stroje, a uživatel používá internetové bankovnictví na adrese www.banka.cz, je zaděláno na průšvih. Při zadání uvedené adresy uživatelem do prohlížeče dojde k načtení stránky nacházející se na IP adrese x.x.x.x, a v prohlížeči v adresním řádku je normálně uvedeno www.banka.cz. Oběť tedy kontrolou adresního řádku útok neodhalí.

Útočníkovi tedy stačí na stroji s touto IP adresou nasadit stránky totožné se stránkami pravé banky, kde dojde k zachytávání zadaných přístupových údajů. Totéž lze provést nejen pro internetová bankovnictví, ale pro jakékoliv internetové stránky typu sociálních sítí, platebních systémů, herních stránek, e-mailových účtů, aukčních serverů aj. Záleží jen na útočníkovi, jaké informace po oběti požaduje.

3.4.3 OBRANA

Obrana proti přepsání souboru *hosts*, spočívá v používání antivirového a antispywarového programu. Valná většina antivirových programů hlídá přepisování tohoto souboru programy, stejně tak některé antispywarové nástroje.

Další možností ochrany je nebýt v operačním systému přihlášen na uživatelském účtu s právy administrátora; případně nespouštět v administrátorském režimu programy, u nichž si nejsme jisti, že pocházejí z důvěryhodného zdroje (programy, které nejsou spuštěny administrátorským účtem nebo spuštěny s administrátorskými právy, nemohou modifikovat a přistupovat k systémovým souborům).

4 VLASTNÍ ČÁST

Mým plánem pro vlastní bakalářskou práci je popis phishingového útoku od fáze příprav a plánování, přes provedení vlastního útoku až po následnou „práci“ se získanými údaji. Cílem je ukázat, jak takový útok vůbec probíhá a co takový „lepší“ útočník provádí. Není v úmyslu popsat obyčejný útok, kdy útočník sežene nebo koupí nějakou velkou databázi e-mailových adres, a na ni pošle své e-maily s odkazem na stránku, a bude doufat, že nějaká osoba z této databáze bude klientem resp. uživatelem služby, na kterou se zaměřil.

Celý útok je prováděn v rovině teoretické a pouze pro studijní účely. Je třeba si uvědomit, že dle novelizovaného trestního zákoníku (zákon č. 40/2009 Sb.), který vstoupil v platnost dne 01.01.2010, by v případě jeho provedení došlo ke spáchání trestného činu podvodu dle § 209 (*„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou[…]*). Dále je možné, že by došlo k naplnění skutkové podstaty dle § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací) a dle § 231 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat). Z toho tedy plyne, že phishingové útoky nejsou legální, a z tohoto důvodu tedy útok není proveden a v práci popsaný postup slouží pouze ke studijním účelům a není návodem k jeho provedení.

V závěru vlastní části je vyhodnocen dotazník, který byl vytvořen k získání informací, zda lidé mají ponětí o tom, co to phishing, sociální inženýrství a pharming je.

4.1 PHISHINGOVÝ ÚTOK

4.1.1 FÁZE: PLÁNOVÁNÍ

V této fázi je třeba si uvědomit, co je cílem útoku. Pro demonstraci teoretického phishingového útoku bylo vybráno internetové bankovnictví České spořitelny a.s. (dále

také jen „ČS“). Protože česká internetová bankovnictví jsou relativně bezpečná pro odesílání peněz, a to jednak pomocí jednorázových potvrzovacích SMS, které jsou posílány na telefonní číslo uživatele, a pak také pomocí klientského certifikátu, který je umístěn na bezpečnostní kartě, což vyžaduje fyzické vlastnění této karty a znalosti PINu, bude útok zaměřen na získání klientského čísla a hesla ze stránek napodobujících internetové bankovnictví ČS nacházející se na adrese www.servis24.cz. Cílem útoku je u obětí pozměnit čísla účtů u šablon, které mají vytvořeny v internetovém bankovnictví, v případně konkurenčního boje pak zjistit čísla účtů a částky, kam jsou peníze odesílány.

4.1.1.1 Na koho bude útok zaměřen

Dalším krokem je výběr skupiny, na kterou bude útok zaměřen. Například je možné učinit toto rozdělení, kdy je vycházeno z vlastních zkušeností; dále z průzkumu z období únor – červenec roku 2005, kdy byl ve spolupráci tehdejšího Ministerstva informatiky a společnosti STEM/MARK proveden průzkum informační gramotnosti v České republice; a dalších dodatečných průzkumů dostupných na internetu.

Osoby ve věku 15-17 let. Jedná se převážně o začínající mladé studenty nebo osoby s dokončeným základním vzděláním zařazujících se do pracovního procesu. U těchto osob je předpoklad poměrně nízké informovanosti o problematice phishingu a také ještě mladická nerozvážnost. Dále u nich existuje, přestože poměrně malá, šance, že v internetovém bankovnictví mají vytvořené šablony, čímž se rozumí předdefinovaná čísla účtů pravidelně se opakujících se plateb (např. platby do školy; měsíční členské příspěvky aj.).

Osoby ve věku 18-35 let. Na tyto osoby nejsou útoky většinou směřovány, jelikož je u nich velká šance, že vzhledem ke své potenciální znalosti internetových podvodů útok odhalí a nahlásí, což by mohlo vést k okamžité velké medializaci a odstavení útočníkových podvodných stránek. Jedná se ale také převážně o lidi z tzv. internetové generace, kde je

povědomí o bezpečném chování poměrně dobře rozšířené. Ale i zde se najdou samozřejmě výjimky, které by své údaje dobrovolně lehce vyplnily. Ale riziko odhalení útoku a jeho nahlášení je zde vysoké, proto se tato skupina pro výše uvedený typ útoku **nehodí**.

Osoby ve věku 36-49 let. Pro potřeby útoku už mnohem lepší než kategorie předcházející, přesto je v této skupině dostatečně velká informovanost o podvodech. Pro útok je vhodnější ale až níže uvedená věková skupina.

Osoby 50 let a starší. Primárně na tuto kategorii je útok cílen. V této skupině starší generace je předpokládaná informovanost o phishingu, pharmingu a podobných internetových podvodech poměrně malá. Dalším důvodem, proč je útok cílen na tuto skupinu, je to, že ve skupině 50+ se nachází poměrně dost tzv. malých živnostníků. V souvislosti se změnou poplatků, kterou provedla ČS, kdy téměř dvojnásobně zvedla cena příkazu vhazovaného osobně na přepážce (ze 7,- Kč na 15,- Kč) a jako alternativa byla klientům nabídnuta levnější varianta placení, a to varianta internetového bankovnictví, došlo pravděpodobně k většímu využívání internetového bankovnictví u těchto osob. V této skupině je navíc dán předpoklad ve využívání šablon v internetovém bankovnictví pro ulehčení své práce.

4.1.1.2 Dotazník

Aby útočník získal potřebné údaje, jeví se tvorba fiktivního dotazníku jako dostatečná.

Ideální možností by bylo využití některé z dostupných služeb na internetu. Tyto služby ale nezpřístupňují tvůrcům dotazníků e-mailové adresy lidí, kteří chtějí po vyhodnocení dostat výsledky, protože výsledky jsou automaticky rozeslány systémem bez toho, aniž by si je útočník mohl prohlédnout. Proto je vhodnější vytvořit pomocí technologií HTML, CSS a PHP internetovou stránku a umístit ji na některém z *free*

webhostingů[13]. Příkladem může být webhosting webzdarma.cz, u kterého se pro registrace může využít koncovky jako *nazory.cz* nebo *kvalitne.cz*[14].

Aby stránka působila věrohodně, bude se na ní nacházet archiv již provedených dotazníků, které budou zcela fiktivní, a v archivu bude uveden jen název s možností „ZOBRAZIT VÝSLEDKY“. Po kliknutí na tento odkaz bude uživatel odkázán na stránku, kde je třeba vložit heslo, aby se k dotazníku dostal. V tomto případě se osoby, které na tento fiktivní web útočník pošle, nedostanou na výsledky dotazníků, tudíž je není třeba plnit falešnými údaji a útočník si tak nepřitěžuje práci. Stačí vymyslet jen několik názvů těchto „ již provedených“ anket. K navození důvěryhodnosti stránky je potřeba minimálně tak cca 40 „názvů aktivit“.

Dále na stránce bude umístěno počítadlo s velkým počtem přístupů. Velký počet přístupů proto, aby stránka vypadala velmi navštěvovaně a používaně.

Ke konci už jen stránce udělat slušivou grafiku, zpřístupnit několik fiktivně vytvořených koláčových grafů jako výsledek nějakého posledního dotazníku.

Nyní má tedy útočník připravenou důvěryhodně vypadající stránku např. na adrese www.dotazniky.kvalitne.cz a zbývá tedy ještě vytvořit dotazník, který bude sbírat potřebné informace.

Jelikož útočník potřebuje zjistit informace o tom, jaké uživatelé používají banky, je třeba tento dotazník umístit do peněžního sektoru. Název dotazníku může být třeba následující – „Jak jste spokojeni se službami své banky?“. Dotazníky tohoto rázu se na internetu vyskytují poměrně často, tudíž se dá předpokládat, že uživatel ho vyplní a nebude jej podezírat z možnosti nějakého zneužití informací.

Dotazník se může skládat třeba z otázek uvedených v Tabulka 2.

[13] Služba umožňující zdarma umístit svou stránku na internet. Např. www.webzdarma.cz, www.ic.cz
[14] Při využití tohoto webhostingu není třeba nic platit a ani není třeba registrace domény na své vlastní jméno. Důsledkem toho je v názvu stránky použita vybraná koncovka, kterou webhosting nabízí (u webzdarma.cz se jedná např. o koncovky - .kvalitne.cz, .prodejce.cz, .nazory.cz, chytrak.cz, unas.cz).

Otázka	Možnosti
Vaše pohlaví?	Muž, Žena
Váš věk?	15-17, 18-29, 30-36, 37-49, 50-60, 61+
Jakou banku používáte?	Komerční banka, Česká spořitelna, Poštovní spořitelna, Československá obchodní banka, GE Money Bank, ING Bank, UniCredit Bank, RaiffeisenBank
Jak hodnotíte služby své banky? (hodnoťte jako ve škole)	1,2,3,4,5
Jak hodnotíte přístup zaměstnanců k Vám jakožto klientovi? (hodnoťte jako ve škole)	1,2,3,4,5
Používáte internetové bankovnictví?	Ano, Ne
Používáte v internetovém bankovnictví šablony příjemců?	Ano, Ne
Jaký typ účtu používáte?	Osobní, Podnikatelský, Studentský
Používáte k přihlašování klientský certifikát (čtečka + přístupová karta)?	Ano, Ne
Vyhovuje Vám internetové bankovnictví Vaší banky? (hodnoťte jako ve škole)	1,2,3,4,5
Myslíte si, že by banky měli snížit, ne-li úplně zrušit poplatky za vedení účtu, příjem platby na účet a výběr z bankomatu jako tomu je v zahraničí?	Ano, Ne

Tabulka 2 - Možné otázky v dotazníku. Zdroj: vlastní tvorba autora

Pro sběr e-mailových adres je třeba na konci dotazníku ještě nějakým způsobem požádat uživatele, aby zadal svou e-mailovou adresu. Ať už ze zvědavosti nebo kvůli možné odměně, která mu bude ze zadání e-mailu plynout. Příkladným textem může být: „*Chcete-li obdržet vyhodnocení tohoto dotazníku a zjistit, jaký názor mají lidé používající stejnou banku jako Vy nebo banky jiné, vložte zde prosím Váš e-mail. Na e-mail Vám budou po vyhodnocení zaslány výsledky dotazníku společně s tipy jak ušetřit na poplatcích ve Vámi zvolené bance. Tipy jsou pro každou banku vytvářeny zvlášť, nejedná se tedy o*

obecné bezcenné tipy. Dotazník je zcela anonymní a vložená e-mailová adresa bude po zaslání vyhodnocení okamžitě smazána“. Zde tedy odměnu představují tipy, jak ušetřit peníze na bankovních poplatcích.

Dotazník je tedy již připraven a nyní stačí, aby si útočník obdržené odpovědi ukládal. Pro potřeby útoku pak může vyfiltrovat e-mailové adresy podle odpovědí. V daném případě budou útočníka zajímat odpovědi lidí starší generace, kteří využívají internetové bankovnictví České spořitelny a, kteří nepoužívají k přihlášení klientský certifikát. Nejlépe ještě lidé s podnikatelským účtem.

Rozšíření dotazníku mezi potenciální oběti. Možností, jak rozšířit dotazník je spousta. Nejlepší možností se jeví rozšíření dotazníku pomocí Facebooku koupením několika již vytvořených skupin/stránek s velkým množstvím členů. Vhodnými kandidáty na nákup mohou být skupiny tematicky blízké skupinám, na které je směrován útok (skupiny zaměřené na koníčky, finance, banky atd.). Jelikož na Facebooku se skupina, na kterou je primárně tento útok směřován (starší generace) nenachází, je potřeba tento dotazník rozšířit i mimo Facebook. Žádost o rychlé vyplnění krátkého dotazníku jako pomoc k tvorbě bakalářské či diplomové práce studenta na fórech, kde se scházejí starší generace, určitě nezůstane bez povšimnutí. Dále je možné použít veřejně dostupné seznamy firem na internetových katalozích a rozeslat e-mail, který bude přímo směrován konkrétní osobě s žádostí o vyplnění.

Řekněme, že útočník se šíření dotazníku aktivně věnuje určitou dobu a již sesbíral dostatečné množství údajů. V době, kdy bude čekat, než lidé na dotazník zapomenou (aby jim den po vyplnění dotazníku o bankách nepřišel útočníkův „podvodný“ e-mail z banky, to by bylo podezřelé), je nutné, aby si vytvořil falešnou přihlašovací stránku.

4.1.1.3 Falešná stránka

Dalším krokem je příprava falešné webové stránky napodobující originální přihlašovací stránku internetového bankovnictví zvolené banky. Typický postup při této části je navštívení originální stránky a uložení jejího zdrojového kódu. Zdrojový kód je poté upraven do podoby, kdy veškeré obrázky načítá z originálního serveru, stejně tak

všechny odkazy vedou na stránku pravé banky. Většinou jediný rozdíl mezi originální stránkou a stránkou falešnou je ten, že falešná obsahuje nejčastěji jednoduchý PHP skript, který slouží k ukládání zadaného klientského čísla a hesla. Po zadání požadovaných údajů dojde k jejich uložení a k okamžitému přesměrování na pravou stránku internetového bankovnictví, což by u oběti mělo vzbudit dojem, že pouze zadal klientské číslo nebo heslo špatně. Pro přístup do bankovnictví zadá své údaje znovu a tentokrát se již do opravdového internetového bankovnictví přihlásí.

Poslední věcí, kterou je potřeba před útokem provést, je registrace vhodné domény. Možností, jakou si zvolit doménu, je několik (samozřejmě za předpokladu, že tyto domény jsou volné a nejsou již registrovány).

1. Doména s jinou koncovkou – http://www.servis24.com, http://www.servis24.cc
2. Využití nastavení serveru a vytvoření adresy http://www.servis24.cz.utocnik.cz - požadavek se dostává na server www.utocnik.cz, protože „www.servis24.cz“ je jen subdoména na daném serveru.
3. Zaregistrovat jméno „wwwservis24“, výsledkem bude http://wwwservis24.cz.
4. Registrace domény „www-servis24“ (místo tečky pomlčka).
5. Využít nějakou z překlepových domén, které na první letmé přelétnutí pohledem nejsou moc odhalitelné - www.servsi24.cz www.sevris24.cz, www.srvis24.cz atp.
6. Použití písmen, která si jsou vzájemně podobná (malé L a velké I – „l x I“ nebo velké O a nula – „O x 0“) – v případě útoku na bankovnictví ČS nepoužitelné.

Nyní již má útočník vytvořenou internetovou stránku s připravenými skripty na zachytávání hesla a klientského čísla, stejně tak má databázi budoucích obětí. Nyní postupuje do fáze útoku.

4.1.2 FÁZE: ÚTOK

Útok spočívá ve vytvoření e-mailu a jeho odeslání na e-mailové adresy, které útočník získal z dotazníku. Při tvorbě e-mailu je použito metod sociálního inženýrství, aby bylo zajištěno, že oběť e-mailu uvěří, klikne na odkaz v ní obsažený a směřující na útočníkovu stránku a zadá své přihlašovací údaje.

E-mail by mohl vypadat třeba následovně:

„Vážený kliente České spořitelny,

dovolujeme si Vás upozornit na 3 platby, které jsou připraveny k odeslání z Vašeho účtu. Jelikož příjemcem těchto plateb jsou zahraniční účty, na které jsou z velké části převáděny peníze z nelegální činnosti, žádáme Vás o součinnost. Rádi bychom Vás požádali o jejich kontrolu, a pokud se jedná o Vaše platby, prosíme o jejich potvrzení. Zároveň si Vás dovolujeme upozornit, že uvedené platby budou ještě blíže prozkoumány našim odborným týmem, a pokud dojde k zjištění, že se jedná o platby, které jste opravu nezadal vy, dojde k jejich stornování. Přesto bychom byli rádi, pokud byste je také sám prověřil. Přihlášení prověřte, prosím, co nejdříve na stránkách Internetového bankovnictví České spořitelny SERVIS24.cz.

S pozdravem a přáním krásného zbytku dne

Bezpečnostní tým České spořitelny

Česká spořitelna, a.s.
sídlo: Praha 4, Olbrachtova 1929/62, PSČ 140 00
IČ: 45244782
DIČ: CZ 699001261
Zapsána v obchodním rejstříku Městským soudem v Praze, oddíl B, vložka 1171.“

E-mail je formátován pomocí značkovacího jazyku HTML[15]. Při útoku může být e-mail vyzdoben grafickými prvky banky, jako jsou logo a jiné další pro banku typické prvky. Podtržená část e-mailu „*Internetového bankovnictví České spořitelny SERVIS24.cz*“ směřuje na útočníkovu podvodnou stránku.

[15] Jazyk používaný pro formátování internetových stránek. Umožnuje vkládat obrázky, odkazy atd.

Dále je pro větší věrohodnost u e-mailu podvržen odesílatel. Je tedy jen na útočníkovi jakého odesílatele e-mailu si zvolí, jestli to bude info@csas.cz[16], bezpecnostnitym@csas.cz, security@servis24.cz nebo nějaký jiný. K podvržení je možno použít PHP funkci mail().

Nyní již nic nebrání útočníkovi v odeslání zprávy na e-mailové adresy, které získal a vyfiltroval podle jím zvolených kritérií z dotazníku.

4.1.3 FÁZE: VÝSLEDKY

4.1.3.1 Přístup k účtům

V podstatě ihned po odeslání útočník vyčkává, jestli se někdo chytí a zadá své údaje. Dále je již jen na něm, jak naloží s přístupem do internetového bankovnictví a co měl v plánu. V případě, že by se jednalo o útok na konkurenční firmu za účelem získání informací o příchozích a odchozích platbách, jedinou věcí, kterou útočník udělá, je návštěva transakční historie. U účtů, ke kterým by získal přístup a jejichž uživatelé k posílání peněz používají možnosti šablon[17], má útočník možnost změnit u těchto šablon čísla účtů na útočníkovy.

4.1.3.2 Prodej

Další možností, co útočník se získanými přístupovými údaji může udělat, je to, že je nabídne na černém trhu (těchto trhů je na internetu a tzv. „deepwebu“[18] několik a získat k nim přístup zabere velmi mnoho úsilí, a zároveň je třeba mít známé, kteří útočníka doporučí). V tomto modelovém případě je prodej nevhodný, jelikož je zde poměrně velké riziko, že dojde k rychlému odhalení útoku a u obětí dojde ke změně přístupových údajů.

[16] Koncovka csac je používána u e-mailů České spořitelny.
[17] Používá se u účtů, na které uživatel často odesílá platby. Tedy, aby nemusel stále vyplňovat číslo účtu, vytvoří si šablonu, kde je již vše včetně čísla účtu předvyplněno.
[18] Část internetu, která není přístupná zadáním internetové adresy nebo ve vyhledávačích. Anonymní síť, kdy se k přístupu používá programu TOR. Právě zde se díky anonymnímu přístupu a dá narazit na spoustu ilegálních aktivit (prodej drog; prodej údajů o kreditních kartách; najmutí lidí na krádež, fyzickou likvidaci atd.)

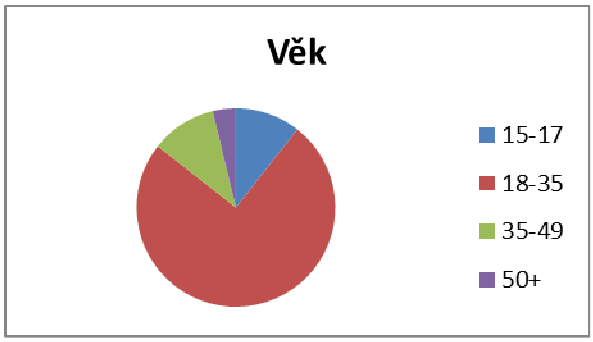
Proto musí útočník jednat ihned, jakmile se k němu přístupové údaje dostanou. Prodej údajů je nejčastěji prováděn při phishingových útocích na majitele kreditních karet, kde se cena pohybuje v rozmezí 20 -25 amerických dolarů za oběť, která má na účtu minimálně 1000 americký dolarů.

4.2 Dotazník

Průzkum o informovanosti širší veřejnosti proběhl formou dotazníku a zúčastnilo se jej 171 lidí. Jednalo se o jednoduchý dotazník zaměřený na znalosti pojmů phishing, pharming a sociální inženýrství. Dotazník byl vytvořen pomocí jednoho z volně dostupných hlasovacích systémů na internetu. Šíření dotazníku probíhalo pomocí sdílení na Facebooku mezi lidmi se středoškolským a vysokoškolským vzděláním, kteří jsou mladší 30 let. Dále pak rozesláním e-mailů s dotazníkem v jednom z českých pojišťovacích ústavů, kde byl vyplněn vysokoškolsky vzdělanými lidmi staršími 30 let.

První dvě otázky se týkaly věku a pohlaví. Z celkových 171 respondentů bylo 75 % mužů a 25 % žen. Věkové rozmezí bylo od 14 do 66 let. Níže na Obrázek 6 je uvedeno procentuální rozdělení dle věkových skupin (rozděleno do dle věku jako je uvedeno v kapitole Phishingový útok):

- 15-17 let – 10,61 %,
- 18-35 let – 74,99 %,
- 36-49 let – 10,64 %,
- 50 let a více – 3,76 %.



Obrázek 6 – Věkové složení respondentů
Zdroj: vlastní tvorba autora

Třetí otázka - „Víte, co se skrývá pod pojmem "Sociální inženýrství"?“

- 40,35 % ANO,
- 59,65 % NE.

Čtvrtá otázka - „Víte co je to "phishing", česky někdy označováno jako "rhybaření"?

- 57,56 % ANO,
- 42,44 % NE.

Pátá otázka – „Víte co je to "pharming"?“

- 28,65 % ANO,
- 71,5 % NE.

Šestá otázka – „Setkal(a) jste se někdy s phishingem? (Podvodná stránka vydávající se za pravou stránku, za účelem podvodného získání osobních informací, nejčastěji přístupového jména a hesla. Tyto zadané údaje jsou pak přístupné útočníkovi, který s nimi může jakkoliv nakládat.)

- 33,33 % ANO,
- 45,61 % NE,
- 25,15 % NEVÍM.

Sedmá otázka – „Pokud jste odpověděl(a), že jste se s phishingem setkal(a), zadal(a) jste požadované údaje? Pokud nesetkal(a), zadejte odpověď "nesetkal(a) jsem se s phishingem"“

(Obrázek 7)

- 7,02 % ANO,
- 29,82 % NE,
- 61,41 % Nesetkal(a) jsem se s phishingem.

Obrázek 7 - Úspěch phishingu Zdroj: vlastní tvorba autora

Pomocí výsledků u otázky šesté, kde respondenti zadávali, zda se s phishingem setkali, a výsledků u otázky sedmé, kde respondenti odpovídali, zda při setkání s phishingovou stránkou zadali své údaje, zjistíme, kolik procent lidí se na phishingový podvod nachytalo.

Z výsledků tedy vyplývá, že:

- 21 % své údaje zadalo,
- 79 % své údaje nezadalo.

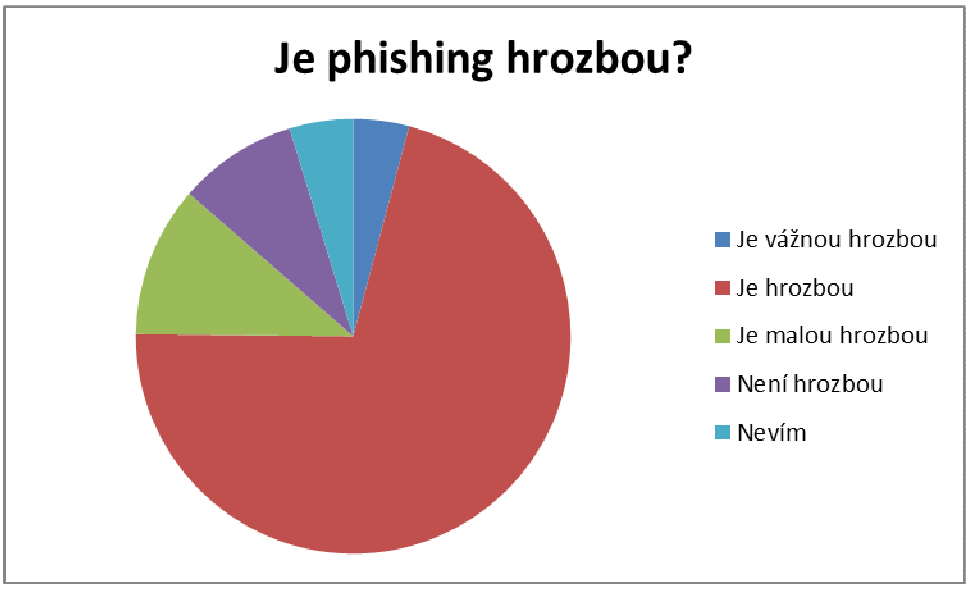
Tabulka 3 ukazuje procentuální zastoupení obětí útoku k celkovému počtu lidí, kteří se setkali s phishingem, dle věkových skupin (ze skupiny 50 let a více se s phishingem nikdo z účastníků nesetkal, nebo o tom neví, a tudíž ani nemohl vyplnit, že se stal obětí. Proto zde tato skupina není uvedena). Dle dotazníku se tedy s phishingem setkalo 57 lidí, z toho 12 zadalo požadované údaje.

Věková skupina	Setkalo se s phishingem	Zadalo požadované údaje	% lidí ve své skupině, kteří zadali údaje
15 – 17 let	7	2	29
18 – 35 let	42	8	19
36 – 49 let	8	2	25
Celkem	57	12	

Tabulka 3 - Oběti phishingu Zdroj: vlastní tvorba autora

Výše uvedená tabulka tedy potvrzuje, že rozdělení do věkových kategorií ve fázi Plánování v kapitole Phishingový útok bylo správné, a nejvíce ohroženou skupinou jsou mladiství ve věku 15 až 17 let a osoby starší 36 let. Nicméně 19% úspěch u skupiny 18 – 35 let je také poměrně vysoký. Důležitou poznámkou také je, zdali se osoby patřící do skupiny 50 let a více opravdu nestali obětmi, nebo to, díky poměrně nízké informovanosti v této oblasti, vůbec netuší.

Poslední otázkou, na které respondenti odpovídali textem, byla otázka – „Myslíte si, že phishingové útoky jsou v dnešní době hrozbou, nebo že nemají šanci na úspěch?“



Obrázek 8 - Je phishing pro uživatele hrozbou? Zdroj: vlastní tvorba autora

Pro vytvoření grafu byly jednotlivé odpovědi rozděleny do výše uvedených kategorií. Z grafu na Obrázek 8 vyplývá, že 4 % dotazovaných si myslí, že phishing je vážnou hrozbou; 71 %, že se jedná o hrozbu; 11 % dotazovaných jej považuje za malou hrozbu; 9 % dotazovaných se domnívá, že phishing není pro uživatele hrozbou; a 5 % dotazovaných neví.

Zde jsou sepsány některé zajímavé odpovědi, které se v dotazníku objevily:

„ "Dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoliv tím prvním si nejsem jistý" Albert Einstein. Podle mého phishing bude neustálá hrozba.“

„Mají šanci na úspěch u lidí, kteří o dané problematice nevědí, tj. nejlépe se obchoduje s lidskou hloupostí.“

„Určitě jsou hrozbou. Lidé jsou zdegenerovaní a věří kdečemu.“

„Nemají šanci u chytrých lidí, u hlupáků je možné vše“

„Ano, jsou hrozbou. Lidé nekontrolují, zda jsou na stránce, na které opravdu být chtějí a informace klidně zadají.“

„Jsou hrozbou pro naivní uživatele.“

Z výsledků dotazníku lze tedy zjistit, že povědomí o sociálním inženýrství a pharmingu je velmi malé. Naopak o tom, co je to phishing, věděla více jak polovina dotazovaných. Další zajímavostí, která z vyplněného dotazníku vyplynula, je, že téměř každý pátý respondent, který se setkal s phishingem, naletěl útočníkovi a zadal informace, které po něm na podvodné stránce byly žádány.

Dle výsledků dotazníku by tedy byl vhodný nějaký druh informační kampaně, která by se zaměřovala na zvýšení informovanosti osob o internetových podvodech, zejména pak v oblasti sociálního inženýrství a phishingu, na kterých je velká část podvodů stavěna. Každopádně osvěta v těchto oblastech by měla být velkou prioritou také u zaměstnavatelů, jehož zaměstnanci jsou denně v kontaktu s lidmi a mají přístup k internetu. Vyzrazení některých citlivých informací by pro firmu mohlo mít fatální následky.

V současné době by také své klienty měly dostatečně informovat banky. Přestože jsou na stránkách internetových bankovnictví zmínky o možnostech podvodů, je otázkou zdali tyto informace vůbec lidé čtou. Lepší variantou by mohla být informovanost o možnostech útoků již při samotném zakládání útoků a i občasné informační dopisy směřované přímo na klienty.

5 ZÁVĚR

Cílem práce bylo uvedení do problematiky krádeží identit na internetu. Toho bylo docíleno kapitolou číslo 3 s názvem Teoretická část. Zde byl čtenář seznámen se sociotechnickými útoky, phishingovými útoky a útoky, které se dají označit slovem pharming.

Kapitola čtvrtá seznamovala s jedním z mnoha typů phishingových útoků, a to od fáze plánování (tj. zaměřením se na určitou skupinu lidí, vytvořením falešného dotazníku a falešné stránky) přes fázi útoku kdy byl lidem odeslán e-mail s odkazem na falešnou stránku internetového bankovnictví, která sloužila k ukládání zadaných dat, až po fázi výsledků, kde byly popsány možnosti, jak může potenciální útočník se získanými informacemi nakládat. Útok byl proveden v rovině teoretické a žádné e-maily ani falešné stránky nebyly vytvořeny. Útok slouží pouze pro studijní ukázku, jak podobné typy útoků vypadají a není návodem, či nabádáním k provedení podobného útoku.

Dále v této čtvrté kapitole byly zveřejněny výsledky dotazníku, ze kterých vyplynulo, že by bylo vhodné zvýšit informovanost lidí v oblasti krádeže identity a internetových podvodech, zejména pak v oblasti sociálního inženýrství a phishingu, na kterých je velká část podvodů stavěna. Toho by šlo docílit mediálním zaměřením se na tuto problematiku.

Informovanost o možnostech útoků by také měla být v zájmu bank. Ty sice na svých stránkách mají odkazy vedoucí na články informující o těchto útocích, otázkou ale je, zda na ně lidé vůbec klikají a informují se nebo tomu nevěnují vůbec pozornost. Možností, jak zvýšit povědomí o těchto útocích, by bylo informování již při samotném zakládání účtu, a také pomocí občasných informačních dopisů na adresu klienta.

Každopádně osvěta v těchto oblastech by měla být velkou prioritou také u zaměstnavatelů, jejichž zaměstnanci jsou denně v kontaktu s lidmi a mají přístup k internetu. Vyzrazení některých citlivých informací by pro firmu mohlo mít fatální následky. V tomto ohledu lze doporučit rozšíření vstupních či jiných školení také o bezpečnost práce na internetu.

6 SEZNAMY

6.1 SEZNAM POUŽITÝCH ZDROJŮ

1. **Jirovský, Václav.** *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing a.s., 2007. 978-80-247-1561-2.

2. **Federal, Trade Commission.** Federal Trade Commission. *Identity Theft.* [Online] 27. 11 2007. [Citace: 28. 01 2012.] http://www.ftc.gov/opa/2007/11/idtheft.shtm.

3. **Hoffman, Sandra K. a McGinley, Tracy G.** *Identity theft - A reference handbook.* místo neznámé : ABC CLIO LLC., 2010. 978-1-59884-144-2.

4. **Evropská, Komise.** Evropská komise - Ochrana soukromí - slovníček. *Evropská komise - Ochrana soukromí.* [Online] [Citace: 30. 12 2011.] http://ec.europa.eu/information_society/eyouguide/fiches/glossary_privacy/index_cs.htm.

5. **Mitnick, Kevin.** *Umění klamu.* místo neznámé : Nakladatelství HELION S.A., 2003. 83-7361-210-6.

6. **Horníček, Jan.** *Sociální inženýrství.* Fakulta aplikované informatiky. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. str. 63, Vysokoškolská kvalifikační práce - bakalářská práce. Vedoucí bakalářské práce Ing.Jaroslava Gregušová. http://dspace.knihovna.utb.cz/bitstream/handle/10563/9113/horn%C3%AD%C4%8Dek_2009_bp.pdf?sequence=1 [PDF].

7. **Hoax.cz.** HOAX. *HOAX - PHISHING.* [Online] [Citace: 07. 01 2012.] http://www.hoax.cz/phishing/.

8. **James, Lance.** *Phishing bez záhad.* Praha : Grada Publishing, a.s., 2007. 978-80-247-1766-1.

9. **APWG.** The Anti-Phishing Working Group. *Phishing Activity Trends Report 1st Half 2011.* [Online] [Citace: 07. 01 2012.] http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf [PDF].

10. **ApWG.** The Anti-Phishing Working Group. *Phishing Activity Trends Report 3rd Quarter 2009.* [Online] [Citace: 07. 01 2012.] http://www.antiphishing.org/reports/apwg_report_Q3_2009.pdf [PDF].

11. **Wikipedia.** Wikipedia - internetová encyklopedie. *Wikipedia.* [Online] [Citace: 01. 12 2011.] http://en.wikipedia.org/wiki/AOHell.

12. **Chronic, Da.** AOL Watch. *AOL Watch - AOHell documentation.* [Online] [Citace: 01. 12 2011.] http://www.aolwatch.org/chronic2.htm.

13. **Pavel Nesejt.** Finance.cz. *Finance.cz.* [Online] 16. 03 2006. [Citace: 28. 12 2011.] http://www.finance.cz/zpravy/finance/63677-prvni-phishing-v-cesku-tercem-byla-citibank/.

14. **Macich, Jiří.** Lupa.cz. *Lupa.cz.* [Online] 11. 04 2006. [Citace: 28. 12 2011.] http://www.lupa.cz/zpravicky/prvni-ceske-zatceni-za-phishing/.

15. **FBI.** The Federal Bureau of Investigation. [Online] 24. 11 2010. [Citace: 29. 01 2012.] http://www.fbi.gov/news/stories/2010/november/cyber_112410.

16. **Šťastný, Petr.** Průvodce DNS - úvod, DNS záznamy a protokol. [Online] 29. 04 2007. [Citace: 11. 02 2012.] http://www.dns-info.cz/dns/index.html.

17. **Dougherty, Chad R.** CZ.NIC správce domény CZ. *CZ.NIC, z. s. p. o.* [Online] 14. 07 2008. [Citace: 11. 02 2012.] http://www.nic.cz/page/464/bezpecnostni-chyba-v-dns,-upgrade-doporucen/.

18. **The, European Registry of internet domain names.** The European Registry of internet domain names. [Online] [Citace: 11. 02 2012.] http://www.eurid.eu/cs/domenova-jmena-eu/dnssec-eu.

19. **CZ, CZ.NIC správce domény.** DNSSEC. [Online] [Citace: 11. 02 2012.] http://www.dnssec.cz/.

6.2 SEZNAM OBRÁZKŮ

6.3 SEZNAM TABULEK