Mendelova univerzita v Brně
Provozně ekonomická fakulta

Problematika sociálního inženýrství v souvislosti s elektronickými platebními systémy

Bakalářská práce

Vedoucí práce:

Ing. Stratos Zerdaloglu **Veronika Chrástová**

Brno 2015

Děkuji svému vedoucímu bakalářské práce Ing. Stratosi Zerdaloglu za cenné rady, připomínky a metodické vedení práce. Děkuji také své rodině za poskytovanou podporu během celého studia.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Problematika sociálního inženýrství v souvislosti s elektronickými platebními systémy**
vypracoval/a samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědom/a, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 22. května 2015 _____

Abstract

Chrástová, V. The issue of social engineering in connection with electronic payment systems. Bachelor thesis. Brno: Mendel University, 2015.
This bachelor`s thesis focuses on the issue of social engineering in connection with electronic payment systems. It analyzes the currently used electronic payment systems in the Czech Republic and introduces the problems of sociotechnics. Based on information gathered suggests measures to reduce the risk of abuse of sensitive data.

Keywords

Social engineering, phishing, pharming, hoax, electronic payment systems, payment cards, internet banking, PayPal, safety.

Abstrakt

Chrástová, V. Problematika sociálního inženýrství v souvislosti s elektronickými platebními systémy. Bakalářská práce. Brno: Mendelova univerzita v Brně, 2015.
Bakalářská práce se zaměřuje na problematiku sociálního inženýrství v souvislosti s elektronickými platebními systémy. Analyzuje aktuálně používané elektronické platební systémy v České republice a seznamuje s problematikou sociotechniky. Na základě získaných informací navrhuje opatření vedoucí ke snížení míry rizika zneužití citlivých údajů.

Klíčová slova

Sociální inženýrství, phishing, pharming, hoax, elektronické platební systémy, platební karty, internetové bankovnictví, PayPal, bezpečnost.

Obsah

1 Úvod a cíl práce 13
1.1 Úvod 13
1.2 Cíl práce 13
2 Elektronické platební systémy (EPS) 14
2.1 Hlavní charakteristiky EPS 14
2.2 Bezpečnost EPS 14
2.2.1 Technologie zabezpečení 15
2.3 Základní rozdělení EPS 16
2.4 Autentizace uživatelů 16
2.5 Platební karty 16
2.5.1 Rozdělení platebních karet podle použité technologie 17
2.5.2 Rozdělení platební karet podle způsobu zaúčtování 17
2.5.3 Rozdělení platebních karet podle provedení 17
2.5.4 Rozdělení platebních karet podle vydávající asociace 18
2.5.5 Průběh platby na Internetu prostřednictvím platební karty 18
2.6 Elektronické bankovnictví 18
2.6.1 Formy elektronického bankovnictví 18
2.7 Příkaz k úhradě 21
2.8 Skrill 21
2.8.1 Bezpečnost 21
2.8.2 Poplatky 21
2.9 PayPal 22
2.9.1 Bezpečnost 22
2.9.2 Poplatky 22
2.10 PayU 22
2.10.1 Bezpečnost 23
2.10.2 Poplatky 23
2.11 PaySec 23

2.11.1 Bezpečnost ... 24
2.11.2 Poplatky ... 24

3 Sociální inženýrství 25
3.1 Sociotechnik ... 25
3.2 Kevin Mitnick ... 26
3.3 Metody sociálního inženýrství ... 26
3.3.1 Phishing ... 26
3.3.2 Vhishing ... 28
3.3.3 Pharming ... 28
3.3.4 Baiting ... 29
3.3.5 Hoax ... 29

4 Metodika 30

5 Vlastní práce 31
5.1 Metodika dotazníku ... 31
5.2 Cíle a předpoklady dotazníku ... 31
5.3 Vyhodnocení dotazníku a jeho grafické zpracování ... 33
5.4 Zhodnocení předpokladů dotazníku ... 50
5.5 Návrh souboru opatření ... 51
5.5.1 Opatření pro každého uživatele ... 51
5.5.2 Opatření pro univerzity ... 52
5.5.3 Opatření pro firmy ... 52

6 Závěr 54

7 Literatura 55

8 Seznam obrázků 58

9 Seznam tabulek 59

10 Seznam grafů 60

A Dotazníkové šetření 62

1 Úvod a cíl práce

1.1 Úvod

Hotovostní platební styk, pro jehož realizaci je nezbytnou podmínkou existence fyzických peněz, má v celosvětovém měřítku spíše tendenci k celkovému poklesu. To je způsobeno zejména tím, že informační a komunikační technologie zažívají nevídaný rozmach a pronikají do všech oblastí lidského života. Internet patří bezesporu k hlavním globalizačním faktorům, který dnes společnosti umožňuje nakupovat zboží a služby elektronickou cestou, říká se tomu tzv. e-komerce. Jeho obrovskou výhodou je rychlý a efektivní přenos informací. Proto není překvapením, že finanční instituce zavádějí a masově podporují vývoj elektronických platebních systémů. Tyto systémy zajišťují přenos určité částky mezi různé účastníky. Obchodníci přijímají elektronické platby v reálném čase a obdrží bezhotovostní peněžní zdroje, což podstatně urychluje samotnou transakci nákupu či prodeje. Dnes už lidé nemusí se složenkou utíkat na poštu. Stačí se přihlásit do svého elektronického bankovnictví a pomocí příkazu k úhradě zaplatit dlužnou částku z pohodlí domova. V zásadě všechny nástroje, které mají takovouto transakci urychlit, zabezpečit a zpříjemnit, řadíme do elektronických platebních systémů.

Je třeba si uvědomit, že na správném fungování elektronických platebních systémů je závislá celá ekonomika. Byť jen sebemenší výpadek by vedl k nešťastným následkům. A právě z tohoto důvodu jsou elektronické platební systémy nejčastějším terčem hackerů a podvodníků, kteří se snaží pomocí různých metod získat peníze od uživatelů. Mezi takové se řadí metody sociálního inženýrství. Jedná se o způsob manipulace lidmi s cílem získat od nich neoprávněně informace důvěrného charakteru za účelem jejich zneužití. K choulostivým informacím patří přístupové kódy, hesla, čísla platebních karet a další.

1.2 Cíl práce

Cílem praktické části této bakalářské práce je na základě analýzy mezi studenty Mendelovy univerzity snížit míru rizika zneužití citlivých údajů v souvislosti se sociálním inženýrstvím v oblasti elektronických platebních systémů. Navrhnu komplexní a dostatečně obecný soubor opatření, použitelných v praxi, jejímž jádrem bude minimalizovat rizika sociálního inženýrství.
V teoretické části představím nejpoužívanější elektronické platební systémy v České republice jakožto moderní způsob komunikace v bankovnictví a uvedu teoretická východiska k problematice sociálního inženýrství.

2 Elektronické platební systémy (EPS)

Schlossberger (2005) definuje elektronické platební systémy jako systémy, které slouží k provádění, zúčtování nebo vypořádání platebních transakcí prostřednictvím informačních technologií. Obecně se dá říci, že elektronickou platbou je jakákoliv platba, která není v hotovosti a probíhá přes Internet. Pomocí těchto virtuálních plateb můžeme penězi nejen platit, ale také platby přijímat. S EPS se můžeme střetnout při nákupu zboží a služeb na Internetu.

2.1 Hlavní charakteristiky EPS

V publikaci, která pojednává o klasických a elektronických systémech, Máče (2006) uvádí několik důležitých charakteristik:

- rychlost vyřízení transakce,
- zabezpečení citlivých informací proti krádežím a jiným podvodům,
- nízké náklady za transakci,
- jednoduchost použití pro plátce i příjemce,
- ověřitelnost a dohledatelnost.

Hlavní výhodou elektronických plateb je jejich rychlost. Doba mezi odesláním platby a připsáním na účet příjemce se pohybuje řádově v hodinách, maximálně v několika dnech. EPS fungují jako prostředník mezi odesílatelem a příjemcem peněz. Příjemce obdrží pouze peníze a identifikační údaje k platbě, nikoliv citlivé údaje odesílatele, např. číslo platební karty. Cena za transakci se liší podle použitého elektronického systému. Vždy platí, že plátce i příjemce chtějí minimalizovat své náklady. EPS musí být snadno uživatelsky obsluhovatelný.

2.2 Bezpečnost EPS

Každý systém má své slabé stránky. Zejména u EPS, které pracují s identifikačními údaji uživatelů, je nutné mít zajištěnou co nejvyšší míru zabezpečení. Hackeři usilují o získání přístupových údajů k účtům, o napadnutí prováděných plateb, o nabytí cizích finančních prostředků. Proto je zabezpečení EPS základní podmínkou pro jejich rozvoj a rozšíření mezi internetové uživatele.

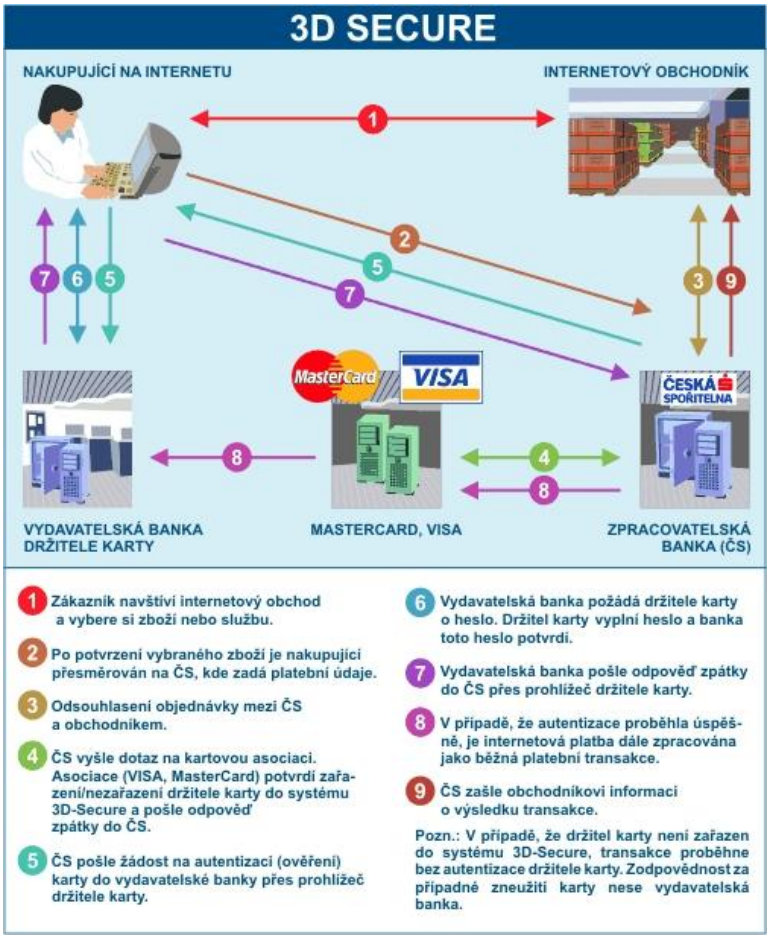
Mezi standardní mechanismy, jak se proti takovým útokům bránit, patří:

- šifrování přenášených zpráv,
- ochrana elektronickým podpisem,
- kvalitní antivirový software,
- využívání bezpečnostních protokolů. (Schlossberger, 2005)

2.2.1 Technologie zabezpečení

- SSL/HTTPS,
- 3D-Secure.

Protokol Secure Sockets Layer (SSL) zajišťuje bezpečnou komunikaci mezi dvěma komunikujícími uzly v prostředí Internetu. (Odvárka, 2002) Princip funkce SSL certifikátů je založen na asymetrickém šifrování. Každá z komunikujících stran má dva šifrovací klíče - veřejný a soukromý. Veřejný klíč je možné zveřejnit a za předpokladu, že pomocí tohoto klíče je zašifrována zpráva, může jí rozšifrovat jen majitel soukromého klíče. (Co je to SSL, 2009) Veřejné klíče jsou sdělovány pomocí certifikátů, které přiděluje Certifikační autorita. Klient pošle požadavek na SSL spojení, jako odpověď od serveru obdrží certifikát. Na jeho základě je vygenerován šifrovací klíč, kterým je zpráva zašifrována a odeslána od klienta na server. Ten použije svůj soukromí šifrovací klíč k rozšifrování zprávy. Mezi klientem a serverem je nyní ustanoveno SSL spojení, jsou dohodnuty kryptografické algoritmy, které se budou používat. Z pohledu běžného uživatele je SSL spojení možné ověřit tak, že URL serveru začíná s https://.



Obr. 1: Zabezpečení plateb pomocí 3D-Secure (Osobní finance, 2015)

3D-Secure je protokol, který zajišťuje bezpečnost tím, že údaje o své kartě nakupující neposkytuje obchodníkovi, ale přímo bance. (Protokoly pro elektronické platební systémy, 2007) Byl vyvinut společností VISA jako celosvětově uznávaný standart pro zabezpečení internetových plateb pomocí platebních karet. Je založený na jazyce XML – používá XML zprávy posílané přes SSL připojení. 3D-Secure umožňuje kromě ověření samotné karty i ověření identity držitele karty (většinou prostřednictvím SMS kódu zaslaného během platby), což výrazně zvyšuje úroveň zabezpečení transakce a snižuje riziko zneužití karty.

2.3 Základní rozdělení EPS

- on-line platby,
- off-line platby.

Před poskytnutím služby ověřuje obchodník s bankou platby od zákazníka (ověřování probíhá obvykle přes autorizační server na straně vydavatele či nabyvatele). On-line systémy zahrnují více komunikace a jsou považovány za více bezpečné než offline platby. Nepotřebují kontakt se třetí stranou během transakce. Většina off-line plateb k tomu používá nějaké hardwarové zařízení, které brání podvodům například smart karty či softwarové prostředky.

2.4 Autentizace uživatelů

Každý uživatel, který chce použít nějaký elektronický platební systém, musí projít autentizací. Autentizace uživatele je proces ověřování identity uživatele. (Matyáš, 2008) Uživatel obvykle udá svojí identitu, např. přihlašovací jméno, a bezprostředně umožní její ověření. Můžeme ověřovat nejen identitu uživatelů, ale i původ dat, tomu se říká autentizace dat. V tomto případě ověřujeme, že známe autora či odesílatele daných dat. Po autentizaci obvykle následuje proces autorizace uživatele, který přiřadí oprávnění pro práci v systému a specifikuje, co daný uživatel může a nemůže. Typickým příkladem autentizace je přihlášení do elektronického bankovnictví.

Základní metody autentizace:

- něco, co daný uživatel zná (heslo, PIN, přístupová fráze),
- něco, co daný uživatel vlastní (platební karta, elektronický klíč),
- něco, čím uživatel je (biometrický informace – otisk prstu). (Matyáš, 2008)

2.5 Platební karty

Platební karty, nejčastější autentizační token, jsou nástroje určené k bezhotovostním platbám. Placení pomocí karet je dnes nejrozšířenějším způsobem platby u obchodníka, protože je nejpohodlnější a jsou akceptovány po celém světě.

2.5.1 Rozdělení platebních karet podle použité technologie

Juřík (2006) rozděluje platební karty podle použité technologie:

- karty s magnetickým proužkem,
- čipové karty,
- hybridní karty.

V magnetickém proužku je uložena neměnná informace, která je zapsaná ve 2 až 3 řádcích. Magnetický proužek je umístěný na zadní straně karty. V čipových kartách se nachází čip, který se skládá z programovatelného mikroprocesoru s pamětí. (Juřík, 2006) Karty dokážou komunikovat i bezkontaktně pomocí bezkontaktního čipu a silného elektromagnetického pole. Bezkontaktní platby umožňují zaplatit malé nákupy do výše 500,- Kč bez nutnosti zadání PINu pouze přiložením karty k terminálu. Hybridní platební karty mají jak magnetický proužek, tak i čip pro záznam dat a komunikaci s terminály.

2.5.2 Rozdělení platební karet podle způsobu zaúčtování

- debetní,
- kreditní,
- charge,
- nákupní úvěrové. (Juřík, 2006)

Debetní karty jsou svázány s běžným bankovním účtem. Jejich použitím se čerpají peníze uložené na bankovním účtu držitele karty. Úvěr lze čerpat pouze tehdy, je-li k účtu sjednán kontokorent. Kreditní karty nejsou napojeny na běžný účet, ale na účet úvěrový. Každá transakce s kartou znamená čerpání poskytnutých financí od banky. Vrácení peněz lze rozložit na splátky v delším časovém období. Charge karty fungují obdobně jako karty kreditní s tím rozdílem, že dohodnutý dluh musí držitel jednorázově splatit v dohodnutém termínu. Nákupní úvěrové karty tvoří podmnožinu kreditních karet. Vydávají je nebankovní instituce. Od klasických kreditních karet se liší především cenou, výší úročení a omezenou použitelností.

2.5.3 Rozdělení platebních karet podle provedení

- embosované,
- elektronické.

Na embosovaných platebních kartách jsou identifikační údaje vyznačeny reliéfním písmem (vystupují z plochy). (Platební karty a jejich druhy, 2015) S takovou kartou je možné platit i v obchodech nevybavených elektronickým platebním terminálem, kde se ještě používá mechanické snímací zařízení nazývané imprinter - tzv. „žehlička“. Ten při placení embosované informace z karty otiskne na účtenku, kterou následně zákazník podepíše. Elektronické platební karty jsou použitelné pouze pro transakce, které jsou on-line ověřeny v kartovém centru, tedy pro výbě-

ry z bankomatů a platby u obchodníků disponujících elektronickým platebním terminálem. Výhodou tohoto typu karet jsou zhruba poloviční náklady na vedení oproti embosovaným kartám.

2.5.4 Rozdělení platebních karet podle vydávající asociace

- VISA,
- MasterCard,
- Maestro,
- Dinners Club,
- American Expres,
- Japan Credit Bureau,
- Discover Financial a další.

Většina vydaných platebních karet v České republice nese logo mezinárodní asociace VISA nebo MasterCard. VISA je největší kartový systém na světě, její karty vydává více než 21 000 bank. MasterCard je jejím konkurentem. Zbylé kartové asociace jsou populární zejména v zahraničí.

2.5.5 Průběh platby na Internetu prostřednictvím platební karty

Proces placení na Internetu prostřednictvím platební karty je snadný. Držitel vyplní do speciálního formuláře identifikační údaje o kartě – číslo karty, dobu platnosti karty (MM/RR) a bezpečnostní kód CSC/CVV/CVC. Požadavek je zabezpečeným přenosem šifrován a poslán zpracovateli ke zpracování. Velké nebezpečí tkví v tom, kdy se citlivé údaje dozví cizí osoba a kartou bude moci platit na Internetu.

2.6 Elektronické bankovnictví

Elektronické bankovnictví je jedna z nejoblíbenějších metod obsluhy bankovních účtů. Tato metoda přímého bankovnictví je založena na principu kontaktu klienta s bankou přes elektronické komunikační kanály, jíž cílem je nabídnout pro klienta pohodlný způsob obsluhy účtu a snížit náklady na přepážkový provoz. (Máče, 2006)

2.6.1 Formy elektronického bankovnictví

- Internet banking,
- Home banking,
- Phone banking,
- GSM banking,
- WAP banking,
- TV banking.

Internet banking, nebo-li internetové bankovnictví, je služba, díky níž lze obsluhovat bankovní účet prostřednictvím webového rozhraní bez nutnosti speciálního nainstalovaného softwaru. (Co je internetové bankovnictví, 2015) Stačí pouze počítač připojený na Internet a internetový prohlížeč.

Ochranu a bezpečnost přenášených dat podporují banky a družstevní záložny těmito prvky zabezpečení:

- autentizační kalkulátor,
- autentizací SMS zaslaná jako běžná SMS,
- autentizací SMS zaslaná jako šifrovaná SMS,
- podpisový certifikát,
- podpisový certifikát uložený na čipové nebo optické kartě,
- podpisový certifikát uložený na USB tokenu,
- TAN kódy,
- uživatelské jméno a heslo. (Počátky internetového bankovnictví, 2015)

Autentizační kalkulátor je založen na hardwarové variantě ověření uživatelovy identity. Přístup do kalkulátoru je chráněn PINem, po jeho zadání se automaticky vygeneruje heslo, které má omezenou platnost a které je nutné pro potvrzení provedení finanční operace na bankovním účtu. Po potvrzení bankovní operace banka zašle na registrovaný mobilní telefon autentizační kód prostřednictvím SMS, který je nutné následně přepsat do vyznačeného pole, Tímto krokem potvrdíme prováděnou operaci. U šifrovaných SMS je nutné mít SIM kartu podporující bankovní aplikace, SIM karta vyžaduje zadání tzv. BPINu.

Bankovní podpisový certifikát je heslem chráněný šifrovaný soubor, který je uložen na disku v počítači. (Počátky internetového bankovnictví, 2015) K potvrzení bankovní operace pomocí podpisového certifikátu na čipové nebo optické kartě je třeba speciální čipová karta a dále čtečka čipových karet. Podpisový certifikát může být uložen i na speciálním USB tokenu. Avšak vydání takového tokenu je zpoplatněno.

TAN kód tvoří unikátní, zpravidla 6místné číslo, kterým se potvrdí bankovní operace. Seznam TAN kódů zasílá banka. Po potvrzení je TAN kód neplatný a je potřeba příště použít jiný. (Počátky internetového bankovnictví, 2015)

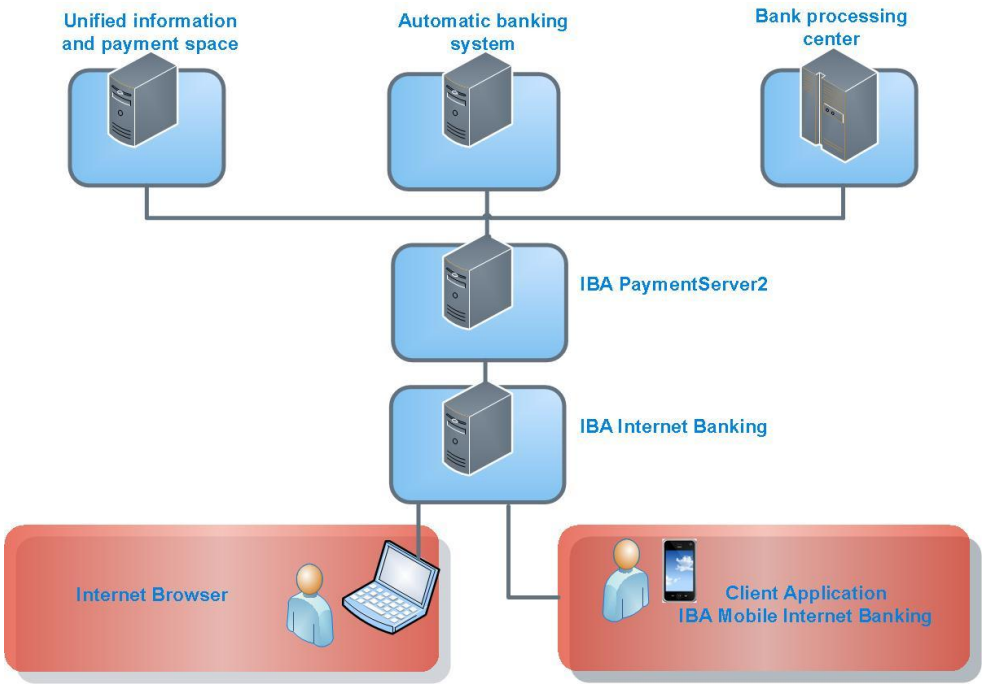
U některých bank či družstevních záložen není třeba potvrzovat bankovní operaci. Stačí se pouze přihlásit do internetového bankovnictví a zadat požadavek. Takový postup uplatňuje například ING Bank.

K užívání Home bankingu je potřeba mít v počítači nainstalovanou speciální aplikaci, která komunikuje s bankovním systémem. Home banking byl oblíbený zejména na konci 90. let, kdy Internet nebyl ještě tak rozšířený. Dnes ho využívají zejména firemní klienti a klienti, kteří nechtějí používat přístup do banky přes Internet. Home banking je zároveň řešení pro banky, které nemají vlastní internetové bankovnictví a vzhledem k počtu jejich klientů se jim jeho vývoj a údržba nevyplatí. Nevýhodou Home bankingu je to, že takový program je licenčně vázaný na jeden konkrétní počítač, a tak přihlášení z jiného počítače není možné. Programy

používají pro zabezpečení a potvrzení bankovních operací podpisový certifikát a data jsou přenášena buď využitím Internetu přes šifrované SSL spojení, anebo přímým spojením na modem banky.

Phone banking využívá ke komunikaci mezi klientem a bankou klasické telefonní linky či mobilní telefony. Uživatel provádí bankovní operace zavoláním na speciální telefonní číslo banky a komunikuje s telefonním bankéřem nebo automatem. (Matyáš, 2008) Ověření uživatele probíhá nahlášením nebo zadáním uživatelského jména a hesla. Součástí autentizaci může být i ověření znalosti identifikačních údajů vlastníka účtu, např. čísla smluv.

GSM bankovnictví je pokročilejší forma než telefonické bankovnictví. Bankovní operace jsou prováděné prostřednictvím mobilního telefonu. Základním prvkem je bankovní aplikace uložená na SIM kartě. (Matyáš, 2008) GSM banking lze provozovat k jednomu účtu pouze z jedné SIM karty. Přístup je zabezpečen přístupovým bankovním PINem a komunikace mezi bankou a telefonem je šifrovaná.



Obr. 2: Schéma elektronického bankovnictví (IBA Internet Banking Systém, 2015)

2.7 Příkaz k úhradě

Příkaz k úhradě je nejsnazší způsob bezhotovostního převodu peněžních prostředků. Předpokladem pro jeho provedení je vedení vlastního bankovního účtu u některé z bank na území České republiky. (Příkaz k úhradě, 2007) Příkaz k úhradě lze podávat pouze v té bance, která vede náš účet, ze kterého chci platit. Poté už jen stačí vyplnit formulář příkazu k úhradě. Správné vyplnění je podmínkou pro jeho hladké vyřízení. Mezi takové údaje patří:

- bankovní spojení plátce,
- bankovní spojení příjemce,
- konstantní, variabilní a specifický symbol,
- částka a měna převodu,
- datum splatnosti. (Příkaz k úhradě, 2007)

2.8 Skrill

Digitální peněženka Skrill (dříve MoneyBookers) patří k populárním platebním systémům na internetu, který je velké míře využíván zejména sázkovými kanceláři. Skrill dovoluje komukoliv s emailovou adresou bezpečně posílat a přijímat peníze prostřednictvím internetu. Nejedná se o klasický bankovní účet, protože peníze vložené na Skrill účet nejsou nijak úročené. (Proč Skrill, 2011) Mezi hlavní výhody digitální peněženky Skrill patří, že vše co potřebujete k vykonávání plateb je emailová adresa a heslo. Při posílání peněž prostřednictvím Skrillu není potřeba poskytovat citlivé informace ohledně platební karty.

Pro využívání Skrillu je nutné se na jejich webových stránkách nejdříve registrovat a otevřít si účet. Po jeho otevření a ověření si na něj můžeme převést peníze prostřednictvím bankovního převodu. Jakmile se peníze připíší na účet, můžeme nakupovat, posílat peníze dalším uživatelům této peněženky, anebo si peníze jednoduše vybrat. Všechny transakce jde jednoduše dohledat na Skrill účtě.

2.8.1 Bezpečnost

Skrill splňuje klasické zabezpečovací standardy pro bezpečnost dat v odvětví platebních karet. Údaje o kartě a bankovních údajích se nikde nezveřejňují. Pokud se někdo pokusí citlivé informace zachytit, šifrování a zabezpečení dat zajistí jejich nečitelnost. (Důvěryhodné zabezpečení, 2011)

2.8.2 Poplatky

Dle informací z oficiální české stránky společnosti je registrace účtu Skrill zdarma. Vkládání peněžních prostředků na účet je zdarma, ale v některých případech můžou účtovat malý poplatek. Příjem peněz je zdarma. Za odeslání peněz účtují 1 % z odeslané částky, maximální poplatek však činí 10 EUR. Platba v obchodě nebo převod peněžních prostředků u všech obchodníků je zdarma.

2.9 PayPal

PayPal je nejbezpečnější, nejpohodlnější a nejspíš nejrozšířenější způsob, jak platit po internetu služby i zboží z celého světa. Jedná se o elektronický platební prostředek, na který se dá přímo napojit na miliony internetových obchodů po celém světě a přesun peněz z účtu na účet probíhá v podstatě okamžitě. (Jak systém funguje, 2008)

Účet u platebního systému PayPal si lze představit jako běžný bankovní účet, který je ideální pro nákupy a prodej zboží na internetu. Uživatelům umožňuje přesuny peněžních prostředků mezi sebou. Každý účet je zde identifikovatelný pomocí registrované emailové adresy. Účet lze využívat ihned po registraci. Uživatel je nucen si nejprve dobít účet, aby mohl platit na internetu. V případě nedostatku zůstatku na PayPal účtu se strhne požadovaná částka z platební karty nebo připojeného bankovního účtu. Před tím než připíše obchodníkovi platbu, strhne si marži.

2.9.1 Bezpečnost

Z hlediska bezpečnosti je PayPal spolehlivý. K zabezpečení účtů používá SSL/HTTPS spojení a šifrování. (Sellers Protection, 2015) Bezpečnostní úroveň uživatelského hesla hraje velmi důležitou roli. V minulosti čelil PayPal několika hackerským útokům, které měly za cíl zneužít uživatelské informace. PayPal zakázal reagovat na emaily, které vyzývají k zaslání hesla účtu.

2.9.2 Poplatky

Založení účtu je zdarma. Zpoplatněny jsou příchozí transakce, které se pro každého obchodníka liší a společnost PayPal s nimi vše konzultuje individuálně. Cena za příjem plateb se pohybuje podle obratu za daný měsíc. Odchozí transakce jsou zdarma. Vklad je zpoplatněn přes platební kartu na PayPal ve výši 1,9 % z částky. Při převodu peněz z PayPal účtu na bankovní účet klienta při chybném uvedení čísla účtu jsou náklady na opravu transakce 200 Kč.

2.10 PayU

Platební systém PayU funguje v Evropě od roku 2005. PayU nabízí komplexní platební řešení pro online platby, které zaručuje zákazníkům inovativní technologie, nejvyšší bezpečností opatření a kontinuální vývoj služeb pro všechny typy e-komerce platforem. (Fungování online plateb u PayU, 2015) Nejznámějším internetovým obchodníkem, který využívá služeb PayU, je e-komerce aukční síň – Aukro.cz, kde původně PayU fungoval jako prostředek k platbě za poplatky, ale postupem času je již využíván jako platební metoda. Hlavním cílem systému je zajistit rychlé, jednoduché a především bezpečné platby na Internetu, které pomáhají e-shopům růst a nakupujícím přinášejí pohodlí, jistotu bezpečných nákupů a plateb za ně.

Výhoda tohoto platebního systému spočívá v tom, že jako klient internetového obchodu se nemusí registrovat a může rovnou zaplatit. Samotná online platba probíhá velmi jednoduše. Zákazník se rozhodne zakoupit zboží či službu a zvolí způsob, jakým jej chce uhradit. V případě, že upřednostňuje rychlý online převod, vybere banku, ve které chce provést platbu (banka, ve které má účet). Následně jej systém přesměruje přímo na stránku jeho internetového bankovnictví, kde se přihlásí tak, jak je zvyklý. Po přihlášení do jeho internetového bankovnictví je pro něho již platební příkaz předvyplněný (vyplněné číslo účtu prodejce, variabilní symbol, částka za zboží) a zákazník ho jen potvrdí. Potvrzená platba od zákazníka je následně převedena prostřednictvím platebního kanálu na účet určený pro službu PayU u této banky. Transakce je autorizována v internetovém bankovnictví – například SMS zprávou. Transakce probíhají v reálném čase a jsou rychlejší než klasický bankovní převod. Zákazníci mohou také zvolit možnost úhrady za vybrané zboží či službu platební kartou, popřípadě jiné platební metody.

2.10.1 Bezpečnost

Platební brána PayU je provozována na základě licence pro poskytování platebních služeb, udělené Českou národní bankou a podléhá tedy stanovené kontrole České národní banky. (Zabezpečení online plateb u PayU, 2015) Veškerý přenos dat mezi internetovým obchodem nebo e-shopovou platformou a jednotlivými platebními kanály je zabezpečen SSL certifikátem. Zprostředkovávají kódování informací při přenosu mezi e-shopem a zákazníky. V roce 2012 firma PayU obdržela bezpečnostní standart PCI-DSS level 1, který garantuje nejvyšší bezpečnost platebních karet, která je na úrovni bank. Obrovskou výhodou je také to, že transakce rychlým bankovním převodem probíhají přímo v prostředí webové aplikace na internetovém bankovnictví uvnitř banky a jsou tedy zabezpečeny bankovními prostředky. Naopak platba kartou je zabezpečena technologií 3D-Secure.

2.10.2 Poplatky

Na svých oficiálních stránkách společnost uvádí, že výše poplatků za procesování online plateb prostřednictvím platební brány PayU je určována individuálně pro každého uživatele, s ohledem na jeho průměrný obrat, průměrnou výši transakce (online platby) a typu obchodní činnosti.

2.11 PaySec

Platební systém PaySec působí na českém trhu od roku 2008 a je provozovaný Československou obchodní bankou, a. s. ve spolupráci s Poštovní spořitelnou s. p. Jedná se o ryze českou společnost, která vznikla, aby zaplnila mezeru na trhu s elektronickými platebními systémy, jelikož se PayPal neuchytil tak, jak se očekávalo. Velkou výhodou je, že PaySec se řídí tuzemskou legislativou a je lokalizován do češtiny (na rozdíl například od Skrillu).

PaySec funguje velmi podobně jako výše zmíněné platební systémy, ovšem na rozdíl od PayPalu nepodporuje párování platební karty, funguje na předplaceném principu. Uživatel si nejdříve musí založit účet. Ten si musí nabít svou platební kartou nebo přes běžný účet, a až poté může systém používat. Není přitom nutné mít u ČSOB nebo Poštovní spořitelny běžný účet.

Platba probíhá v následujících krocích - klient si v internetovém obchodě přidá do košíku zboží a vybere si jako platební metodu PaySec. Internetový obchod klienta vzápětí přesměruje na platební bránu a předvyplní platební informace. Klient transakci potvrdí pomocí uživatelského jména a hesla a peníze jsou převedeny do peněženky internetového obchodu. Klient je přesměrován zpátky do internetového obchodu, kde je vidět identifikace platby. V případě, že bylo vráceno číslo provedené platby, internetový obchod si pomocí mechanismu VerifyTransactionPaid ověří, jestli byla skutečně provedena. Klientovi se posléze zobrazí informace o úspěšném/neúspěšném pokusu o zaplacení

2.11.1 Bezpečnost

Bezpečnost je během celého pobytu na stránkách systému zajištěna technologií SSL. Veškerá komunikace s uživatelským účtem je šifrována. Výhodou pro klienta je přihlášení na svůj účet pomocí uživatelského jména a hesla, kdy je při platbě vyzván, aby zadal kód autorizační SMS zprávy, která mu přišla na mobilní telefon. Tento krok je nutný pro dokončení požadované platby. (Co je PaySec, 2007)

2.11.2 Poplatky

Registrace peněženky je zdarma včetně provozu. Vklad na PaySec účet přes bankovní účet je zdarma. Vklad pomocí platební karty je zpoplatněn 2 % z vkládané částky. Vyplácení na účet vedený u provozovatele PaySecu je zdarma, na ostatní bankovní účty vedené u jiné banky v ČR je poplatek 2 Kč. V případě obchodního konta se stanovují individuální poplatky za transakce a pohybují se v rozmezí 0.8 % - 2 % za transakci + 1 Kč.

3 Sociální inženýrství

O důležitosti bezpečnosti EPS jsem se zmiňovala v kapitole 2.2. Je nutné si však uvědomit, že kromě nebezpečí hackerského útoku hrozí také selhání lidského faktoru.

Termín sociální inženýrství se běžně používá ve významu podvodu. Jedná se o jeden z možných způsobů získávání uživatelských dat. Sociotechnika, nebo-li sociální inženýrství, je ovlivňování a přesvědčování lidí s cílem oklamat je, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá. Takový člověk následně vhodně využije technologické prostředky tak, aby získal požadované informace. (Mitnick, 2003) Pro termín sociální inženýrství existuje mnoho dalších definic, avšak ze všech vyplývá, že pokud jde o bezpečnost systémů, nejslabším článkem je vždy člověk.
Hlavní myšlenka sociotechniky tkví v distancování se použití hrubé síly k prolamování počítačové bezpečnostní bráně, když lze chytře a jednoduše citlivé informace získat od člověka, který je zná. (Šimek, 2003) Při dobře vedeném útoku si oběť v drtivé většině vůbec neuvědomí, že něco vyzradila nepovolané osobě, což je právě nejnebezpečnější rys problematiky sociálního inženýrství.

3.1 Sociotechnik

Sociální inženýr, nazývaný také jako sociotechnik, je osoba, která za účelem získání důvěrných dat předstírá cizí identitu a využívá k tomu technické prostředky. (Mitnick, 2003) Schopný sociotechnik využívá pro efektivní útok vlastností lidské povahy (Sociální inženýrství, 2004):

- autorita,
- sympatie,
- vzájemnost,
- důslednost,
- společenský souhlas,
- poukázání na vzácnou příležitost.

Lidé mají obecně tendenci podřídit se osobě s větší mocí (vyšší funkce, vedoucí pozice ve firmě či škole apod.). Vydává-li se sociotechnik například za asistenta ředitele či samotného ředitele, jeho slova mají vzhledem k běžnému zaměstnanci vyšší váhu. Záměrem sociotechnika je získat větší důvěru a přimět tak oběť k činu, který útočník požaduje. Sympatii si lze získat různými způsoby – stejné názory na problém s obětí, společné zájmy s obětí apod. Je velmi pravděpodobné, že potenciální oběť bude se sociálním inženýrem snadněji spolupracovat, pokud se bude cítit vůči útočníkovi za něco zavázána. Tedy například sociotechnik pro oběť něco udělá – potřebná rada, vyřešení technického problému, drobná pomoc s instalací softwaru, atp. Mimoděk útočník oběti řekne, ať si nainstaluje daný program, který ji zajistí bezpečnost na počítači. Daným programem může být buď spyware (štěnice),

nebo jednoduše program pro přístup ke vzdálené ploše uživatele (RealVNC apod.). Často se také stává, že technický problém, který oběť řeší, sám sociotechnik přivodí a posléze ho pomáhá řešit.

Součástí lidského charakteru je tendence podřídit se, pokud předtím veřejně vyhlásili svou podporu a angažovanost v určité záležitosti. Například veřejný slib, veřejná sázka apod. (Nebezpečné komunikační praktiky a sociální inženýrsví, 2008)

Společenský souhlas funguje tak, že sociotechnik oznámí oběti, že potřebuje něco vyplnit s tím, že všichni ostatní už to vyplnili. Obvykle se jedná o nejrůznější dotazníky a průzkumy. Tato vlastnost je spojena s nenápadným nátlakem na postiženou oběť.

Šikovný sociotechnik může například operovat s tím, že prvních 100 registrovaných uživatelů dostane nějaký dárek. Registraci odkáže na uměle vytvořenou stránku, která získá od uživatelů hesla a osobní údaje. Nebo se jedná o e-maily obsahující vidinu vysoké výhry, nebo velkého majetku.

3.2 Kevin Mitnick

Američan, který poprvé definoval pojem sociotechnika a superhacker, to je Kevin Mitnick. Jeho kariéra hackera začala už v mládí. Na školní síti našel bezpečnostní díru v operačním systému a získal veškerá práva na počítačích IBM. V dalších letech například nezákonně vniknul do počítačového systému kalifornského registru vozidel, na jiný server poslal software firem Nokia, Novell, Motorola, Fujitsu nebo NEC.

Byl jednou z nejhledanějších osob v historii FBI. Po zatčení mu hrozil trest několika set let odnětí svobody. Mitnick vždy tvrdil, že veškeré jeho konání pocházelo čistě ze zvědavosti, nikdy nezničil data na jediném počítači, do kterého pronikl, ani ze svých akcí neměl nikdy finanční prospěch. (Mitnick, 2003) Nicméně o protizákonné kroky šlo, jakkoli neměly zlé úmysly. Soudním výrokem mu byl zakázán jakýkoliv přístup k počítači. Po propuštění z vězení v roce 2000 Mitnick zcela změnil svůj život. Stal se profesionálním počítačovým konzultantem a je z něj dodnes uznávaný expert na bezpečnost počítačových systémů. Uplatňuje své znalosti o bezpečnosti informací a osobní zkušenosti se sociálním inženýrstvím k tomu, aby pomáhal institucím i soukromým osobám odhalovat ohrožení bezpečnosti informací. Založil firmu Mitnick Security Consulting, LLC a doposud vydal spolu s Williamem Simonem dvě knihy - Umění klamu, rok vydání 2002 a The Art of Intrusion, rok vydání 2005.

3.3 Metody sociálního inženýrství

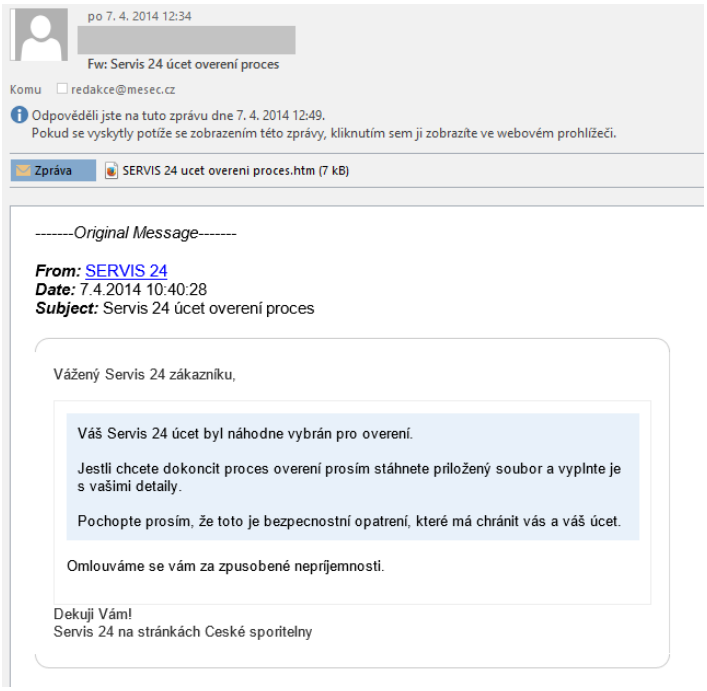
3.3.1 Phishing

Phishing je druh internetového podvodu, kterým se podvodníci snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro svo-

je obohacení. (Phishing, 2015) Princip phishingu spočívá v rozesílání falešných emailových zpráv, které zdánlivě vypadají jako zprávy od banky či podobné legální instituce, v nichž vyzývá adresáta k zadání cenných údajů. (James, 2007) Metody rhybaření pro získání potřebných informací mohou být různé, zpravidla očekávají přímo odpověď na zaslaný e-mail či spuštění přílohy e-mailu. Dále existují i sofistikovanější postupy, kdy na základě e-mailu přimějí navštívit podvrženou kopii stránky, kterou běžně uživatel navštěvuje. Daná webová stránka napodobuje přihlašovací okno například do internetového bankovnictví, zejména design a některé bezpečností prvky. (James, 2007) Pokud do něj uživatel zadá své přihlašovací údaje, předá tím údaje útočníkům, kteří potom mohou účet snadno vykrást.

Phishing čerpá zejména z nepozornosti, důvěřivosti a neznalosti. Pro většinu uživatelů internetu bývá neznalost problematiky zásadním handicapem. Tuto vadu částečně napravují média i samotné poškozené instituce informativními zprávami uvnitř online systému. Například banky samy informují uživatele o aktuálních hrozbách a radí, jak jim čelit. Existuje řada příznaků podvodných emailů, při jejich spatření je nutné zvýšit pozornost (James, 2007):

- Je vyžadováno okamžité sdělení citlivých údajů nebo jinak bude něco omezeno/zrušeno/nevydáno.
- Hypertextové odkazy vedou na úplně jinou adresu, než je specifikováno v textu e-mailu.
- Neočekávaný jazyk zprávy, špatná gramatika, stylistické chyby.
- Přítomna spustitelná příloha (samostatně nebo v archivu), nebo na ní vede odkaz.



Obr. 3: Phishingový útok na klienty České spořitelny, a.s. v roce 2014 (Chvátal, 2014)

3.3.2 Vhishing

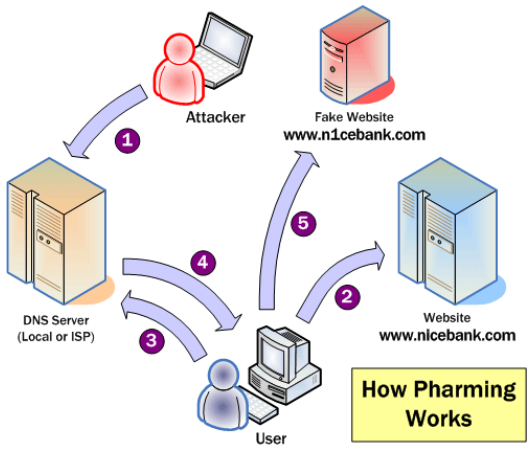
Termín vhishing vznikl kombinací dvou termínů - phishing a voice (v překladu hlas). Jedná se o metodu, která má za úkol vylákat z uživatelů důvěrné informace pomocí telefonního hovoru.

Vishingový útok může mít velmi mnoho scénářů. Jedním z nich je, když hacker informuje uživatele o „problémech“ s účtem pomocí e-mailové zprávy nebo telefonního vzkazu. Příjemci jsou požádáni, aby problém vyřešili zavoláním na bezplatné telefonní číslo. Po zavolání oběť uslyší zprávu, která je k nerozeznání od zprávy pravého automatického telefonního systému. Osoba je vyzvána, aby uvedla číslo platební karty a heslo, popřípadě jinou citlivou informaci jako datum vypršení platnosti platební karty, číslo bankovního účtu, datum narození aj. Pokud tak důvěřivá osoba učiní, předává informace útočníkovi. Tyto údaje jsou poté prodávány na internetu a používány k podvodům se získanou identitou.

3.3.3 Pharming

Pharming, do češtiny překládáno jako farmaření, je další z podvodných technik sociálního inženýrství. Tato metoda je někdy v literatuře přiřazována k phishingu, někdy však stojí samostatně.

Princip pharmingu je založen na tom, že útočník neoslovuje přímo jednotlivé uživatele služby, ale napadne vybraný DNS server. Všichni uživatelé, kteří jsou napojeni na tento DNS server a zadají do adresního řádku prohlížeče správnou adresu kupříkladu internetového bankovnictví, ale jsou přesměrováni na stránky, které pouze vypadají jako stránky jejich banky, ovšem ve skutečnosti se jedná o podvrh. (Phishing a pharming, 2015) Pokud je podvodná stránka dobře vypracovaná, pak je šance, že by uživatel na tento podvod přišel, téměř minimální. Musel by totiž kontrolovat certifikát, kterým je podepsána, a kterým se šifruje přenos dat. Tento certifikát se všemi náležitostmi není podvodník schopen padělat, nicméně může navodit stav, kdy je z pohledu uživatele, který netrvá na velmi podrobném průzkumu, vše v pořádku.



Obr. 4: Schéma pharmingu (Chaudhari, 2006)

Obrázek popisuje schéma principu pharmingu. Znázorňuje napadení DNS serveru a následné přesměrování uživatele na podvodnou stránku banky. Nebezpečí spočívá zejména ve stejné adrese webu. Čísly jsou označeny jednotlivé komunikace mezi účastníky.

1. Napadení DNS serveru útočníkem.
2. Připojení uživatele k oficiálním stránkám banky.
3. Komunikace uživatele s DNS serverem.
4. Napadený DNS server pošle podvrženou informaci o IP adrese stránky.
5. Komunikace uživatele s podvodnou stránkou banky. (Phishing a pharming, 2015)

Podezřelé stránky se pod útokem pharmingu chovají nestandardně. Můžou požadovat po svých klientech údaje, které běžně k přihlášení nepotřebují. V tu chvíli je nutné, aby se uživatel odhlásil z aplikace a operaci ihned ukončil. Následně by měl kontaktovat klientské centrum své banky. Na možné zneužití může upozorňovat také adresní řádek. (Phishing a pharming, 2015)
Faktem je, že pharming je mnohem nebezpečnější než phishing, protože jím lze oklamat i zkušenějšího uživatele. Nemusí jej odhalit dokonce ani ochrana před podvodnými weby, jež je součástí posledních verzí webových prohlížečů.

3.3.4 Baiting

Baiting jedna z metod sociálního inženýrství, která bývá přirovnávána k útoku trojského koně, modifikovaného pro reálné prostředí. Scénář útoku je analogický s použitím Trojského koně jako lsti k dobytí města Tróje. (Kuneš, 2012) Pouze namísto dřevěného koně, který měl v útrobách řecké vojáky, je použito médium (CD, USB disk) s programem k „dobytí“ počítače oběti.

Útočník nechá paměťové médium s lákavým nápisem či dokumentem – například „platy zaměstnanců“ na místě, kde jej oběť s velkou pravděpodobností nalezne. Poté již nechá pracovat zvědavost. (Kuneš, 2012)Po otevření složky na CD se do počítače automaticky nainstaluje malware v podobě trojského koně nebo viru. Tento vir bude napadený počítač sledovat, čerpat informace a odesílat je útočníkovi.

3.3.5 Hoax

Hoax patří k další podvodné technice, kterou lze zařadit do problematiky sociálního inženýrství. V počítačovém světě slovem HOAX nejčastěji označují jako poplašnou a nevyžádanou zprávu, která chce příjemce vystrašit, pobavit nebo jinak nepravdivě informovat. (Co je to hoax, 2015) Hoax obvykle obsahuje žádost o další rozeslání pokud možno co největšímu počtu příjemců, proto je dost často nazýván jako řetězový email. Nejčastěji se v hoaxových e-mailech vyskytují tyto základní prvky:

- popis nebezpečí,
- ničivé účinky viru,
- výzva k dalšímu šíření zprávy. (Co je to hoax, 2015)

4 Metodika

Bakalářská práce se skládá ze dvou částí, a to konkrétně z teoretické části a praktické části.

V literární části jsou představena základní teoretická východiska pro elektronické platební systémy s důrazem na bezpečnost. Jsou zde uvedené nejpoužívanější elektronické platební systémy v České republice jako platební karty, elektronické bankovnictví, příkaz k úhradě, Skrill, PayPal, PayU a PaySec. V posledním bloku teorie vykresluji sociální inženýrství jako jeden ze způsobů získávání uživatelských dat. Definuji, kdo je sociotechnik a co je phishing, vhishing, pharming, baiting a hoax.

Vlastní práci zaměřuji na analýzu povědomí studentů o problematice sociálního inženýrství a jejich chování na Internetu. K analýze jsem využila dotazníkové šetření, které se skládalo celkem z 15 uzavřených otázek. Cílem ankety bylo zjistit, zda pojmy úzce spjaté s počítačovou kriminalitou v podobě sociálního inženýrství zná především mladá počítačová generace.

Prostřednictvím získaných informací z dotazníkového šetření vytyčím vhodná opatření, která povedou k minimalizaci rizika sociálního inženýrství jak pro běžného uživatele, tak pro univerzitu a firmu.

V závěru svou práci zhodnotím.

5 Vlastní práce

5.1 Metodika dotazníku

Dotazník jsem vytvořila prostřednictvím formuláře Mendelovy univerzity a on-line byl vystaven pro všechny studenty školy po dobu jednoho měsíce v informačním systému. Studenti byli o vyvěšení dotazníku informováni a požádáni o jeho vyplnění. Celkem se ho zúčastnilo 210 respondentů z řad studentů celé univerzity. Dotazník se skládal ze dvou částí. První část (7 otázek) se týkala tématu sociálního inženýrství, druhá část (8 otázek) se zabývala chováním na Internetu. Otázky byly uzavřené, anonymní a sestaveny pouze za účelem určité klasifikace znalostí z oblasti sociálního inženýrství a bezpečnosti na Internetu.

Celý dotazník je uveden v příloze, byl vyhodnocen pomocí koláčových grafů a tabulek

5.2 Cíle a předpoklady dotazníku

Cíl č. 1
Zjistit, zda studenti Mendelovy univerzity vědí, co je sociální inženýrství.

Cíl č. 2
Zjistit, zda studenti Mendelovy univerzity znají metody sociálního inženýrství, zda se s nějakou z nich již osobně setkali a analyzovat, jak by na danou metodu reagovali.

Cíl č. 3
Zjistit, jakou platební metodou studenti Mendelovy univerzity nejraději platí na Internetu.

Cíl č. 4
Zjistit, zda se studenti Mendelovy univerzity chovají na Internetu bezpečně.

Předpoklad č. 1
Domnívám se, že více jak 80 % studentů vědí, co si pod pojmem sociální inženýrství představit.

Předpoklad č. 2
Předpokládám, že více jak 65 % studentů vědí, co je to Phishing.

Předpoklad č. 3
Odhaduji, že více jak 80 % respondentů by hoaxovou zprávu nikomu nepřeposlalo a smazalo ji.

Předpoklad č. 4
Domnívám se, že stále minimálně 10 % studentů platí na Internetu nejraději pomocí dobírky.

Předpoklad č. 5
Předpokládám, že minimálně 50 % studentů si při přihlašování do svého internetového bankovnictví ověřuje stránky certifikátem.

Předpoklad č. 6
Domnívám se, že více jak 65 % studentů používá při přihlašování na různé stránky různá hesla.

5.3 Vyhodnocení dotazníku a jeho grafické zpracování

Otázka č. 1 - Co je sociální inženýrství?

Odpověď	*Počet respondentů*	*Procenta*
a. Společenská věda zkoumající sociální život jednotlivců, skupin a společností.	32	15 %
b. Disciplína, která vytváří flexibilní a komplexní řešení pro dlouhodobé zvyšování výkonností firem bez rozdílu odvětví a velikostí.	20	10 %
c. Ovlivňování a přesvědčování lidí s cílem získat požadované informace.	107	51 %
d. Činnost zahrnující inženýrství, informatiku a management, jejímž cílem je návrh, tvorba a údržba počítačových programů.	51	24 %
Celkem	210	100 %

Tab. 1: Co je sociální inženýrství

Graf 1: Co je sociální inženýrství

Získané odpovědi mi umožňují vyhodnotit hypotézu č. 1. Správná odpověď je c. Z tabulky i grafu je zřejmé, že pouze 51 % studentů opravdu vědí, co znamená sociální inženýrství. Zbytek studentů odpověděl nesprávně. Průzkumy zaměřené na vědomosti o sociálním inženýrství vykazovaly v minulých letech mnohem větší

neznalost. Tato skutečnost souvisí zejména s tím, že jsou hackerské útoky spojené se sociotechnickou v posledních měsících stále častější a tudíž o nich média častěji informují. Zloději prahnou po citlivých údajích a jsou každým dnem vynalézavější. Přibývá okradených uživatelů a média nás informují o stále nových a nových fintách. Bohužel se velmi často stává, že člověk takovým informacím nevěnuje dostatečnou pozornost, dokud sám nenaletí. A právě velká zbraň sociotechniky tkví především v neznalosti jejích základních praktik.

Za základní problém považuji nedostatečnou osvětu sociotechniky a obrany proti ní. Polovina studentů vysoké školy netuší, co si pod pojmem sociální inženýrství představit. Co teprve až se setkají s jednou z metod? Nechají se napálit? A co osoby s nižší úrovní dosaženého vzdělání? Nebo naopak ti, co nevyrostli v moderní době s tabletem v ruce? Metody sociálního inženýrství jsou velmi zákeřné. Je třeba o nich trvale mluvit, upozorňovat na ně a zejména se jim bránit.

Otázka č. 2 - Setkali jste se osobně s nějakou z metod sociálního inženýrství?

Odpověď	*Počet respondentů*	*Procenta*
a. Ne	132	63 %
b. Ano, ve škole	21	10 %
c. Ano, v zaměstnání	6	3 %
d. Jinde	51	24 %
Celkem	210	100 %

Tab. 2: Setkání s metody sociálního inženýrství

Graf 2: Setkání s metody sociálního inženýrství

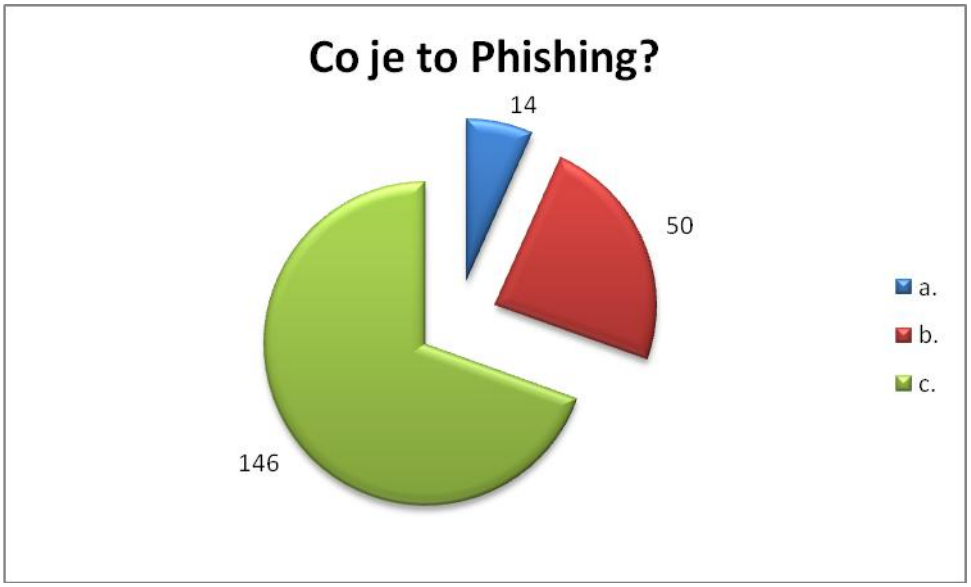
Pro mě překvapivě docela vysoké číslo - 63 % respondentů si nemyslí, že se osobně setkalo s jakoukoliv metodou sociálního inženýrství. Naopak 37 % se s touto problema-

tikou osobně seznámilo ať už při studiu, v práci či jinde. Jsem si vědoma, že čísla jsou mírně zavádějící a nepravdivá, protože je na místě vzít v potaz možnou nevědomost studentů o jednotlivých metodách sociálního inženýrství. Respondent nemusí tušit, že se stal obětí sociálního inženýrství. Klidně se mohlo stát, že mu do e-mailové schránky přišla hoaxová zpráva, která žádala například o příspěvek na operaci srdíčka malého dítěte a rozeslání největšímu počtu kontaktů za účelem získání co nejvyšší vybrané částky. Obětí se nemusí stát jen osoba s tučným kontem, ale i student, který sice nedisponuje žádným majetkem, ale má pro útočníka i jiné cenné informace. Opět narážíme na potřebnou medializaci sociotechniky, jejích metod a obrany proti nim. Otázka se vztahovala k hypotéze č. 2.

Otázka č. 3: Co je to phishing?

Odpověď	***Počet respondentů***	***Procenta***
a. Jedná se o typickou hoaxovou zprávu, která se hromadnou poštou šíří mezi uživateli a jejím cílem je příjemce vystrašit, pobavit, nebo jinak nepravdivě informovat.	14	7 %
b. V prostředí internetu se jedná zejména o různé podvodné nabídky výher, výhodné aukce, velké slevy na zboží. Kliknutím a stažením nabízeného softwaru se do počítače oběti nainstaluje škodlivý software.	50	24 %
c. Metoda sociálního inženýrství, při které je odeslán falšovaný e-mail napodobující legální instituci s úmyslem získat od příjemce důvěrné informace.	146	69 %
Celkem	210	100 %

Tab. 3: Znalost phishingu



Graf 3: Znalost phishingu

V otázce č. 3 jsem se studentů ptala, co je to Phishing. 69 % odpovědělo správně. Jedná se o metodu sociálního inženýrství, při které je odeslán e-mail napodobující finanční instituci s úmyslem získat od příjemce citlivé údaje, v ideálním případě přístupové jména a hesla do internetového bankovnictví. Rhybaření je jedna z nejrozšířenějších metod sociálního inženýrství. Pro většinu uživatelů internetu bývá neznalost problematiky zásadním handicapem, protože tady se potvrzuje, že sociotechnika čerpá z nepozornosti, přílišné důvěřivosti a taky neznalosti. O největší medializování této praktiky ze světa sociotechniky se postaraly především samotné finanční domy. Každá banka dnes vydává informační zprávy zveřejňované například v online systému, ve kterých upozorňují své klienty, aby si dávali pozor na falešné a jinak situované e-maily. Radí svým chlebodárcům, jak se bezpečně chovat na internetu a jak zacházet se službou kvůli které phishing vznikl. Tyto odpovědi mi pomůžou vyhodnotit hypotézu č. 3.

Základním pravidlem je – nikdy nikomu nesvěřovat své důvěrné informace. Banka nesmí požadovat po svých klientech přihlašování k účtům prostřednictvím emailu. Rovněž nepřecházet na odkazy jiných webových stránek, které jsou uveřejněné v emailech. Pokud tak učiníme, stačí bedlivě sledovat, kam jsme falešnou zprávou přesměrováni. Ačkoliv se podvodné stránky obvykle podobají originálu, je dobré zkontrolovat název domény, na které se právě nacházíme. I nepatrná změna v adrese stránek je varovným signálem, že není vše v pořádku.

Veřejná databáze Phishtank sdružuje na portálu Phishtank.com veřejně přístupné informace o phishingových stránkách. Na této doméně lze ověřit, zda jsou dané stránky nahlášeny jako phishingové. Webová stránka funguje jako komunitní, tudíž každý může nahlásit a sdílet objevené podezřelé webové stránky

Otázka č. 4: O jakou metodu sociálního inženýrství se jedná, pokud obdržíte zprávu, která má za cíl příjemce vystrašit, pobavit, nebo jinak nepravdivě informovat, a obsahuje žádost o další rozeslání pokud možno co největšímu množství adres?

Odpověď	*Počet respondentů*	*Procenta*
a. Hoax	153	73 %
b. Pretexting	22	10 %
c. Phishing	25	12 %
d. SCAM419	10	5 %
Celkem	210	100 %

Tab. 4: O jakou metodu se jedná

Graf 4: O jakou metodu se jedná

Správnou odpovědí je a. Hoax. Dobře odpovědělo 73 % studentů. Hoax se může zdánlivě jevit jako ne zas tak nebezpečná metoda sociálního inženýrství, ale opak je pravdou. Hoax škodí. Krom toho, že obtěžuje samotné příjemce, šířením hoaxové zprávy může dojít k vyzrazení důvěrných informací. Dává se k dispozici obrovský seznam e-mailových adres náhodným příjemcům. Seznam adres je rájem pro spamery, kteří pak mohou na získané adresy posílat nevyžádané e-maily. Nepříjemná situace může nastat, kdyby se seznam adres klientů a obchodních partnerů dostal ke konkurenci. V případě falešných petic nebo smyšlených podpisových akcí se požaduje vyplnění různých osobních údajů včetně adresy a rodného čísla. Opět nikdy není jasné, kdo si vyplněné informace přečte a jakým způsobem je zneužije. Zde opět platí – nikomu nesvěřovat své důvěrné údaje.

Otázka č. 5: Setkali jste se někdy s podobnou zprávou?

Odpověď	*Počet respondentů*	*Procenta*
a. Ano	180	86 %
b. Ne	30	14 %
Celkem	210	100 %

Tab. 5: Setkání s hoaxem

Graf 5: Setkání s hoaxem

14 % respondentů se s hoaxem nikdy nesetkalo. 86 % uvedlo, že ano, což jasně dokazuje, jak je tato metoda mezi uživateli na Internetu rozšířená. Jak jednoduše rozeznat planou a lživou informaci od důležité? Platí zde zlaté pravidlo – jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, jedná se s největší pravděpodobností o hoax. Pokud i tak nevíme, zda by se mohlo jednat o poplašnou zprávu, přichází na řadu server Hoax.cz. Ten obsahuje pravidelně aktualizovanou databázi nejrozšířenějších podvodných e-mailů. U mnoha hoaxů nalezneme vyjádření poškozených subjektů a organizací, ale i komentáře návštěvníků webů, kteří se dělí o své zkušenosti s vybraným poplašným e-mailem.

Pro zajímavost mezi tři nejznámější internetové hoaxy v České republice patří popálené, nebo smrtelně nemocné, zraněné nebo umírající děti, které může zachránit jen přeposílání jejich fotky. Velmi populární hoaxy o údajných výhodách, které mají Romové vůči zbytku národa. Nejznámější je složenka s třicetitisícovými sociálními dávkami či zpráva o tom, že Romové, jakožto sociálně slabí, nemusí platit v lékárně, protože léky za ně platí stát. A u posledního hoaxu se jedná se o škemrající zprávu, abyste se ujali štěňat rozličných ras, nejčastěji retrívra.

Otázka č. 6: Co uděláte, když obdržíte podobnou zprávu?

TUTO INFORMACI VYSILALI NA EUROPE 1. PREDEJTE JI DAL !!! V PRISTICH DNECH MUSITE DAVAT VELKY POZOR A NEOTEVRIT ZADNY E-MAIL S POZVANKA (INVITATION) NEZAVISLE NA TOM, OD KOHO JE. JEDNA SE O VIRUS, KTERÝ " OTEVIRA OLYMPIJSKOU POCHODEN" A KTERÝ SPALI HARD TENTO VIRUS BUDE ODESLAN OSOBOU, KTERA VAS MA VE SVYCH KONTAKTECH.MUSITE PROTO TUTO ZPRAVU ROZESLAT ! JE LEPSI ZPRAVU OBDRZET 25 X NEZ OBDRZET VIRUS A OTEVRIT HO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! TAKZE POKUD OBDRZITE E-MAIL S NAZVEM INVITATION - NEOTVIREJTE HO A VYPNETE OKAMZITE VAS POCITAC !!!!!!!!!!!!!!!!!!!!!!!!!!!! JE TO NEJHORSI VIRUS OHLASENY CNN A KLASIFIKOVANY SPOLECNOSTI MICROSOFT JAKO NEJDESTRUKTIVNEJSI VIRUS, KTERY KDY EXISTOVAL !!!!!!! BYL OBJEVEN VČERA ODPOLEDNE MCAFEE A IL ZATÍM NENASLA JEHO LOZISKO, ABY MOHLA ZNICIT "ZONU " NA HARD DISKU, KDE JSOU SCHOVANE VSECHNY "ZIVOTNI" (NEJDULEZITEJSI) NFORMACE. POSLETE TENTO E-MAIL VSEM, KOHO ZNATE, VASIM PRATELUM, VSEM VASIM KONTAKTUM CIM VICE OSOB UPOZORNITE PREDEM, TIM HURE SE BUDE VIRUS SIRIT !!!

Odpověď	*Počet respondentů*	*Procenta*
a. Automaticky přepošlu všem známým, aby se virus nešířil.	6	3 %
b. Zprávu nikomu nepřeposílám a smažu ji.	201	96 %
c. Nevím.	3	1 %
Celkem	210	100 %

Tab. 6: Co uděláte při obdržení podobné zprávy

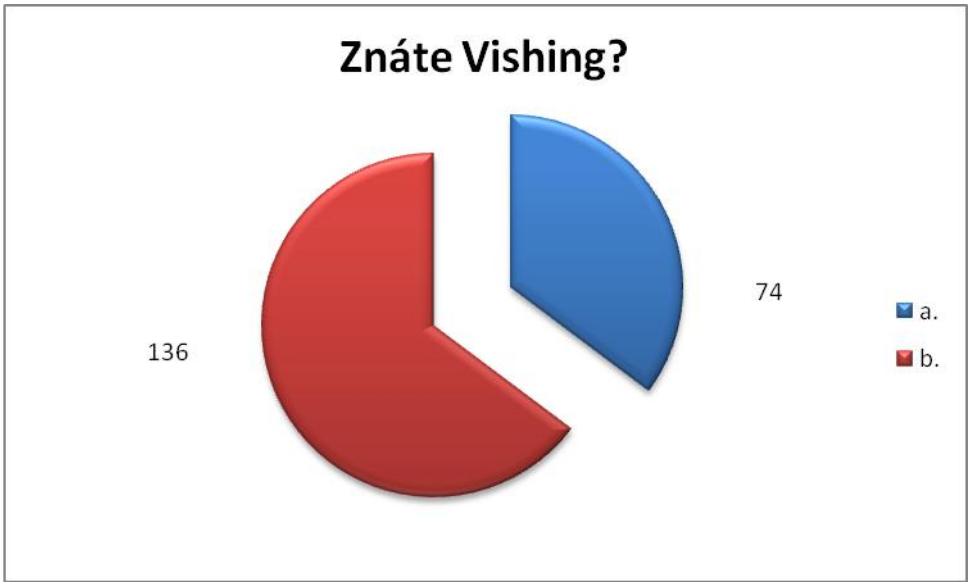
Graf 6: Co uděláte při obdržení podobné zprávy

Uvedená zpráva je klasickým příkladem metody sociálního inženýrství hoaxu. Řekla bych spíše nepovedeným příkladem kvůli gramatickým a stylistickým chybám v textu. Už takové hrubky, nesmyslná slova a věty by nás měly zalarmovat, že není něco v pořádku a zprávu raději smazat. Bohužel ani to některé jedince neodradí od přeposlání e-mailu svým známým, což věrně dokládá výsledek dotazníkové otázky, ve které 3 % dotázaných by přeposlala zprávu dál a 1 % by nevědělo, co udělat. Opatřené odpovědi mi pomůžou vyhodnotit hypotézu č. 4.

Otázka č. 7: Znáte Vishing?

Odpověď	*Počet respondentů*	*Procenta*
a. Ano	74	35 %
b. Ne.	136	65 %
Celkem	210	100 %

Tab. 7: Znalost Vishingu



Graf 7: Znalost Vishingu

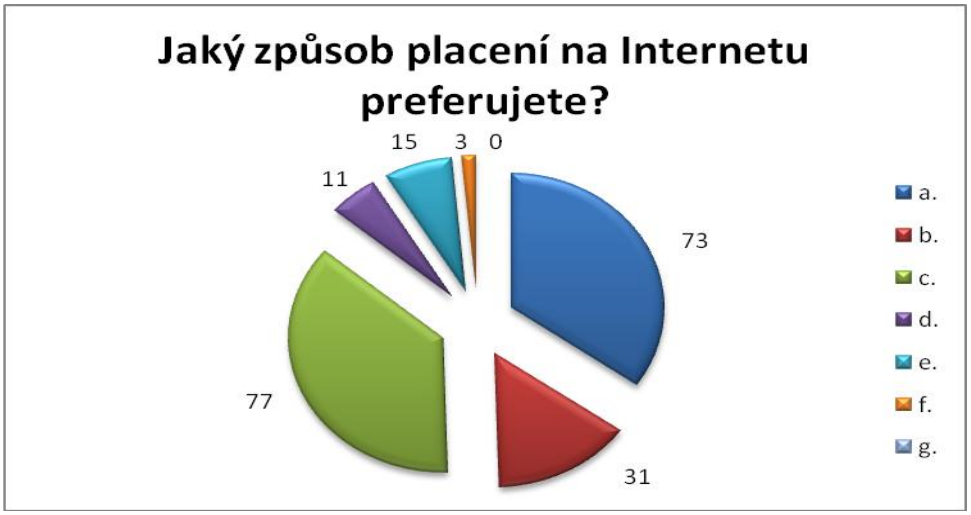
Více jak polovina studentů, konkrétně 65 %, uvedlo, že neznají vishing a dá se předpokládat, že si myslí, že se s ním nesetkali. Tato metoda sociálního inženýrství je relativně novější, ovšem její útoky se v poslední době množí. Často nám takto telefonují banky, pojišťovací agentury, mobilní operátoři, kteří po nás chtějí, abychom po telefonu odpovídali na otázky zasahující do našeho soukromí. Jak víme, že naše odpovědi nezneužijí?

Vhishingový styl útoku je velmi nebezpečný, protože lidé věří telefonům mnohem více než Internetu. Pocit toho, že uživatel s někým opravdu mluví, v něm vzbudí větší důvěru. Útočníci tuto metodu navíc zdokonalili natolik, že je prakticky nemožné rozeznat telefonát s falešným operátorem od pravého. Při zahlcení sítě a nedostatku operátorů používají stejné melodie jako finanční instituce. Zde platí jediné pravidlo – volat pouze na taková telefonní čísla, která jsou oficiálně zveřejňovaná danou institucí. Pokud však přesto uživatel zavolá a má tedy podezření, že se jedná o podvod, měl by nejdříve ověřit identitu osoby, která je na druhé straně linky - například pomocí dotazu na námi posledně provedenou finanční transakci – pokud nebudou odpovědi správné, je na místě ukončit hovor.

Otázka č. 8: Jaký způsob placení na internetu preferujete?

Odpověď	*Počet respondentů*	*Procenta*
a. Hotově na pobočce	73	35 %
b. Dobírka	31	15 %
c. Platební karta	77	37 %
d. Příkaz k úhradě	11	5%
e. Paypal	15	7 %
f. Paysec	3	1 %
g. Jiný	0	0 %
Celkem	210	100 %

Tab. 8: Způsob placení na internetu



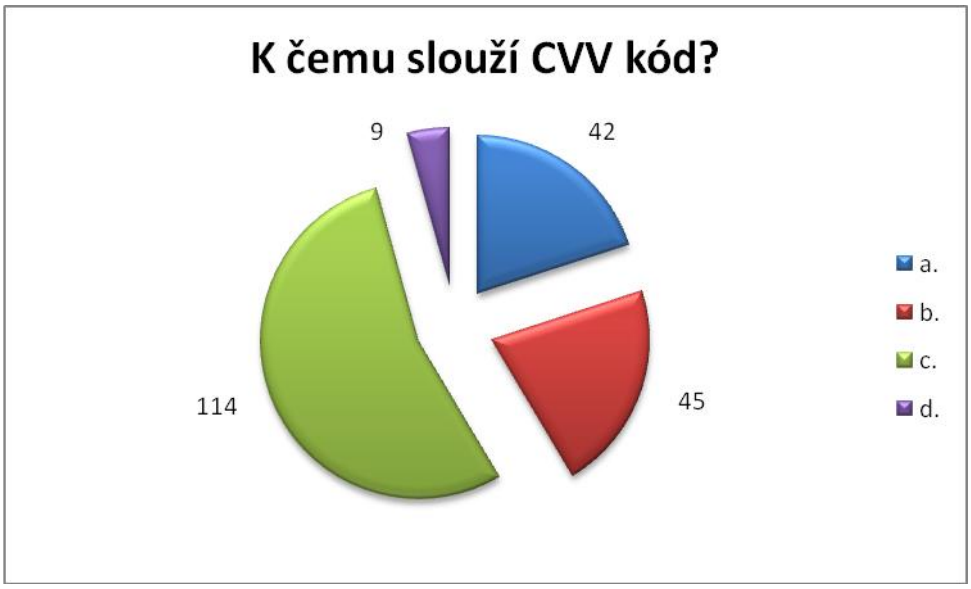
Graf 8: Způsob placení na internetu

Na odpovědi této otázky jsem byla sama moc zvědavá. Podle průzkumů, které pravidelně zveřejňuje Asociace pro elektronickou komerci (APEK), stále více zákazníků využívá při on-line nákupu zboží a služeb platební kartu. Jedním z nejdůležitějších faktorů při volbě způsobu platby je důvěra v bezpečnost. Navzdory obavám je platba kartou jedním z nejjistějších a nejbezpečnějších způsobů platby v prostředí Internetu. Zpracované výsledky dotazníkové otázky tyto průzkumy jasně potvrzují. 37 % studentů preferuje platbu platební kartou, 35 % upřednostňuje platit hotově při vyzvednutí zásilky na pobočce a 15 % využívá služeb dobírky. Na čtvrtém místě se umístilo placení přes bankovní příkaz z internetového bankovnictví a 7 % respondentů využívá služeb platebních systémů jako PayPal a PaySec. Otázka se vztahuje k hypotéce č. 5.

Otázka č. 9: K čemu slouží CVV kód?

Odpověď	*Počet respondentů*	*Procenta*
a. Identifikuje platební kartu.	42	20 %
b. Je speciálním identifikačním číslem držitelem karty.	45	22 %
c. Užívá se pro zvýšení ochrany elektronických transakcí.	114	54 %
d. Identifikuje prodejce při platbě platební kartou.	9	4 %
Celkem	210	100 %

Tab. 9: CVV kód



Graf 9: CVV kód

Při provádění bezhotovostních plateb na Internetu je třeba zadat platební číslo karty, dobu platnosti a také ochranné číslo karty – trojčíslí, označované jako CSC (Card Security Code), CVV (Card Verification Value), CVC (Card Verification Code), které je v podstatě obdobou PINu. Nachází se na zadní straně platební karty v podpisovém proužku a užívá se pro zvýšení ochrany elektronických transakcí. Při platbou karty na Internetu se potom ověřuje, či zadaný CVV kód patří k zadanému číslu karty a k zadané exspiraci. Pokud je autentizace úspěšná, následuje ověření velikosti disponibilního zůstatku a je-li dostatečný, platba proběhne. Správná odpověď je tedy c. a dobře odpovědělo 54 % studentů.

Otázka č. 10: Používáte antivirový program?

Odpověď	*Počet respondentů*	*Procenta*
a. Ano	203	97 %
b. Ne.	7	3 %
Celkem	210	100 %

Tab. 10: Používání antivirového programu

Graf 10: Používání antivirového programu

Ochrana pomocí antivirového programu, antispywarového SW a firewalu je velmi důležitá, a to nejen v otázkách problematiky sociálního inženýrství. Pro řadu lidí připojených k internetu se jedná o naprostou samozřejmost. Z grafu je jasné, že i v dnešní době plné počítačové kriminality a virů se najdou jedinci, kteří takové programy nepoužívají. Představují celé 3 % z dotázaných, zbylých 97 % je používají. Nejde jen o to nainstalovat si antivir, ale je třeba ho pravidelně aktualizovat a starat se o něj. Většina programů funguje na automatických aktualizacích a samostatných plánovaných kontrolách, což je výborná prevence před internetovým nebezpečím. Každá společnost nabízející bezpečnostní aktualizace denně sleduje síť a upozorňuje své uživatele před případnými problémy. Vypnutí aktualizací a jejich ignorování je velmi nebezpečné. Programy se zastaralým systémem nemohou pružně reagovat na viry a jinou havěť ze sítě.

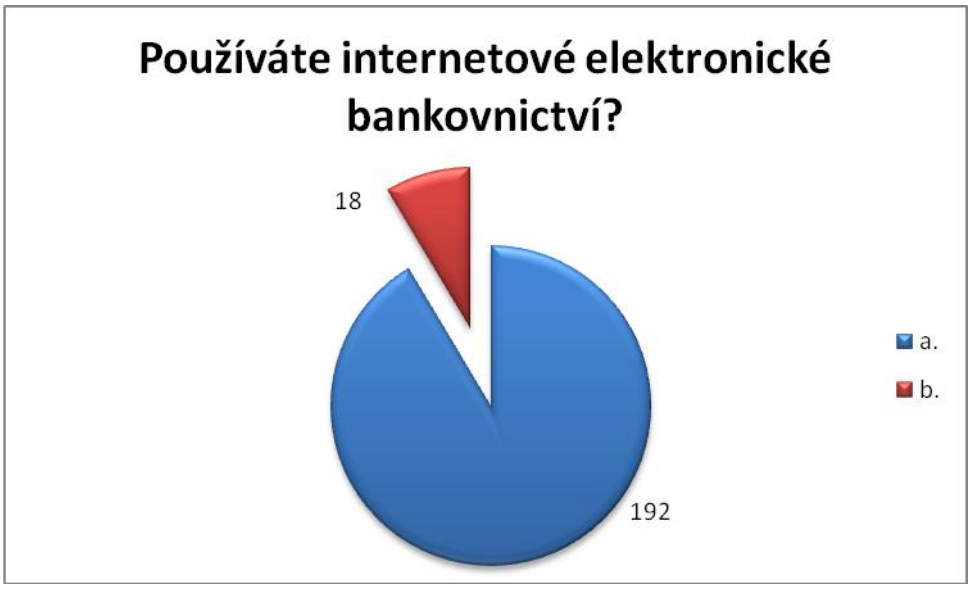
Ochranné programy se dnes netýkají pouze počítačů, ale také tabletů a zejména mobilních telefonů. S tím jak jde technologie kupředu, má dotykové telefony a tablety snad každý. Prostřednictvím telefonů stahujeme nejrůznější soubory a aplikace. Snadno se může stát, že si v nestřeženém okamžiku do mobilu nainstalujeme vir nebo jiný spyware. Od té chvíle je naše činnost na mobilním telefonu či jiném zařízení monitorována, což může být problém například při přihlášení do

internetového bankovnictví. Nutnost antivirových či jiných programů zajišťující bezpečnost našich citlivých údajů, bych tedy nijak nezlehčovala.

Otázka č. 11: Používáte internetové elektronické bankovnictví?

Odpověď	*Počet respondentů*	*Procenta*
a. Ano	192	91 %
b. Ne.	18	9 %
Celkem	210	100 %

Tab. 11: Používání elektronického bankovnictví



Graf 11: Používání elektronického bankovnictví

91 % respondentů používá internetové bankovnictví. Internet banking je dobrý sluha, ale může být i zlý pán. Ušetří náš čas a kilometry, které bychom jinak museli absolvovat při cestě do kamenné pobočky. Na druhou stranu ztracené peníze, o které můžeme přijít díky praktikám sociálního inženýrství, nám nikdo nevrátí. Moderní doba využívá moderní nástroje, nejdříve je ale nutné se s nimi naučit správně pracovat. Proto každá dobrá finanční instituce vydává a aktualizuje zásady správného používání internetového bankovnictví.

Otázka č. 12: Jak se zachováte?

Představte si situaci: Na e-mail Vám přišla zpráva od Vaší banky, ve které Vás vyzývá k aktualizaci Vašich osobních údajů v internetovém bankovnictví. Ve zprávě je také přiložen odkaz na internetové bankovnictví Vaší banky.

Odpověď	*Počet respondentů*	*Procenta*
a. Odkaz otevřu, přihlásím se a aktualizuji své údaje.	17	8 %
b. Zprávu smažu, aniž bych udělal/a, co se po mně vyžaduje.	60	29 %
c. Kontaktuji svou banku a ověřím zprávu.	120	57 %
d. Nevím.	13	6 %
Celkem	210	100 %

Tab. 12: Zpráva z banky

Graf 12: Zpráva z banky

Nejhorší možná odpověď je, že odkaz otevřu, nezkontroluji doménu a bezmyšlenkovitě „aktualizuji“ své údaje. Takto odpovědělo bohužel 8 % vysokoškolských studentů, což mi přijde jako relativně vysoké číslo. Jedná se samozřejmě o phishing, metodu sociotechniky, která z nás chce vymámit uživatelské jméno a heslo k našemu účtu, aby nás mohla následně okrást.

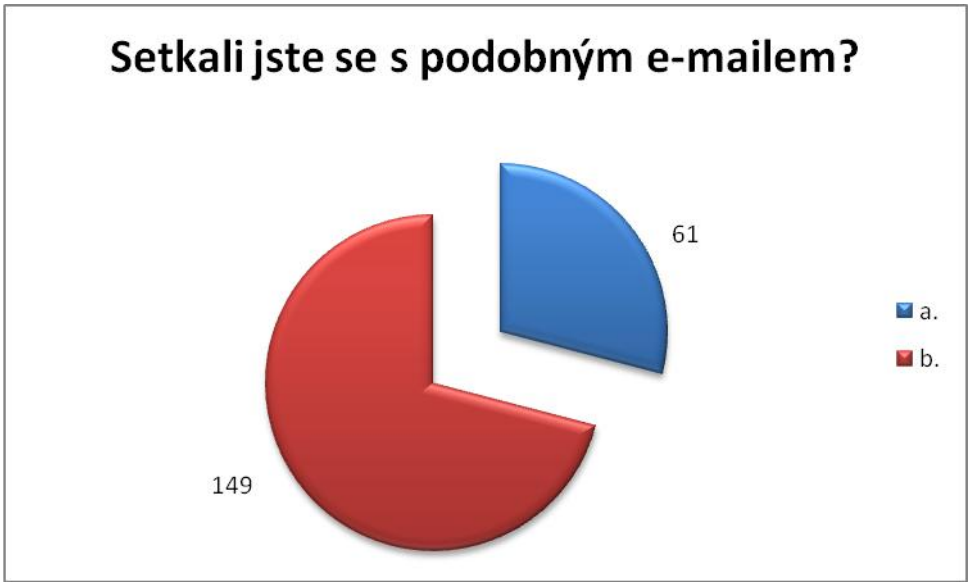
Správná odpověď je b. i c. Pokud takovou zprávu obdržíme, nikdy nesmíme zadávat svá osobní data, přístupové údaje, loginy, hesla, piny a telefonní čísla. Banka nikdy po klientovi tyto osobní údaje v elektronické komunikaci nežádá. V přípa-

dě, že takovýto e-mail obdržíme, je vhodné kontaktovat klientské centrum naší finanční instituce.

Otázka č. 13: Setkali jste se někdy s podobným e-mailem, který se vydával za finanční instituci a požadoval Vaše přihlášení v podobě uživatelského jména a hesla?

Odpověď	*Počet respondentů*	*Procenta*
a. Ano	61	29 %
b. Ne.	149	71 %
Celkem	210	100 %

Tab. 13: Setkání s podvodným e-mailem



Graf 13: Setkání s podvodným e-mailem

29 % studentů uvedlo, že se s podobnou zprávou zatím nesetkalo. Toto nízké číslo mě docela překvapilo, protože phishingové útoky jsou v poslední době čím dál hojnější a i já mám s nimi zkušenosti. Tento trend potvrzují i finanční instituce. Ochrana proti internetové kriminalitě je stojí stovky milionů korun ročně. Banky také nemají jednotný postup při odškodnění poškozených klientů a každý případ posuzují samostatně. Phishingové útoky nejsou cílené pouze na bankovní domy, ale zaměřují se i na jiné elektronické platební systémy. Konkrétně útoky na PayPal jsou velmi časté. Pokud totiž má klient ke svému účtu v této službě připojenu platební kartu, může útočník, po získání přihlašovacích údajů, získat také přístup k penězům na jeho bankovním účtu. Poslední útok zaznamenala společnost PayPal na začátku května tohoto roku. Zpráva oznamuje omezení účtu z důvodu změn v programu pro ochranu zákazníků. Odstranění tohoto omezení pak provede zákazník přihlášením do svého PayPal účtu prostřednictvím odkazů ve zprávě. Tyto

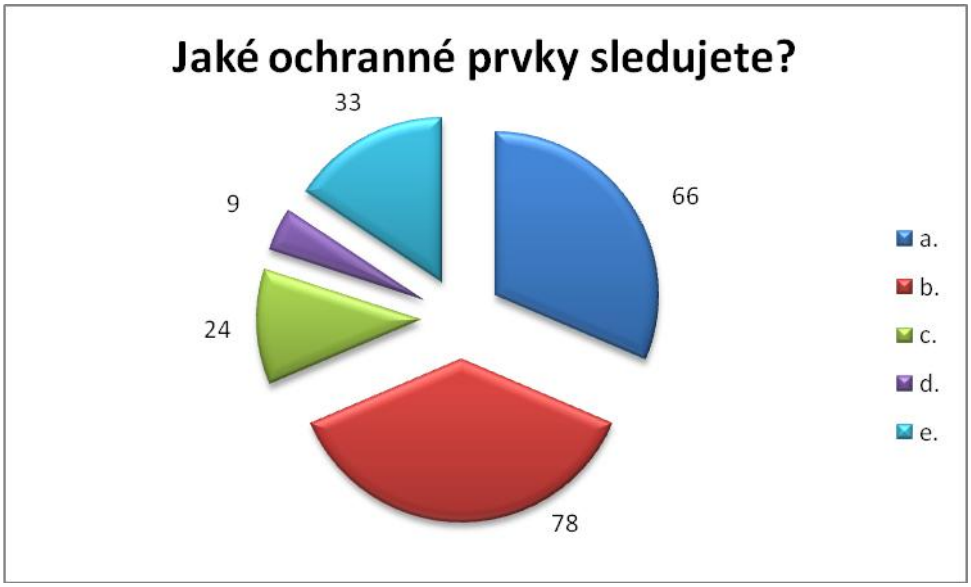
odkazy však vedou na falešnou stránku, která nemá se službou PayPal nic společného. Ze zprávy společnosti RSA z března roku 2014, RSA Online Fraud Report, vyplývá, že celkové finanční ztráty z důvodu phishingových útoků provedených v únoru 2014 dosáhly výše 491 miliónů dolarů. V meziročním srovnání se jejich počet zvýšil o 35 %.

Velmi zajímavou studii na začátku tohoto roku přinesla společnost Kaspersky Lab. Podle ní více než čtvrtina, konkrétně 28,8 %, phishingových útoků v roce 2014 byla zaměřena na krádež finančních dat od uživatelů. Oproti předchozímu roku je to sice o 2,7 procentního bodu méně, ale to je hlavně proto, že kybernetičtí zločinci přesměrovali svou pozornost z bank na platební systémy a internetové obchody. V kategorii platebních systémů útočili kybernetičtí zločinci na uživatele karet Visa (31 %), PayPal (30 %) a American Express (25 %). V kategorii internetových obchodů vede stále Amazon s 32 %, i když zaznamenal pokles o 29 procentních bodů. Analytici to připisují faktu, že se tyto firmy snaží s podobnými podvody ve velké míře bojovat. Útočníci proto hledají nové cíle – například v roce 2014 narostl počet phishingu cílícího na stránky prodávající letenky.

Otázka č. 14: Jaké ochranné prvky stránky nejčastěji sledujete, když se přihlašujete do svého internetového bankovnictví?

Odpověď	*Počet respondentů*	*Procenta*
a. Ověření stránky certifikátem	66	32 %
b. Kontrola šifrovaného spojení (HTTPS)	78	37 %
c. Kontrola webové adresy	24	11 %
d. Kontrola vzhledu webové stránky	9	4 %
e. Žádné z uvedených	33	16 %
Celkem	210	100 %

Tab. 14: Sledování ochranných prvků



Graf 14: Sledování ochranných prvků

U této otázky nelze jednoznačně posoudit správnou a špatnou odpověď. Zde totiž platí, čím vyšší opatrnost, tím lépe. To nejmenší co můžeme udělat, je to, že zkontrolujeme pouze vzhled stránky. Stránku s podobou našeho internetového bankovnictví napodobí každý šikovnější útočník za pár minut.

V ideálním případě je vhodné postupovat následovně. Po spuštění prohlížeče zapsat přímou adresu na stránky našeho internetového bankovnictví do adresního řádku nikoliv do vyhledávacího okénka prohlížeče. Většina internetových bankovnictví využívá protokolu HTTPS. HTTPS používá protokol HTTP, přičemž přenášená data jsou šifrována pomocí SSL. Právě tento prvek zabezpečuje spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany. Z pohledu běžného uživatele je takové spojení možné ověřit tak, že URL serveru začíná s https://. V dalším kroku si zkontrolujte v adresním řádku po kliknutí na zámeček, že se zobrazí informace o certifikovaném zabezpečení dané služby. Pokud je vše v pořádku, můžeme se přihlásit. Po skončení práce v internetové bankovnictví je nutné se vždy odhlásit a zavřít prohlížeč. Bohužel ani tento postup nám nezajistí, že se naše citlivé informace nedostanou k třetím osobám. Pharming totiž skýtá mnohem větší nebezpečí, které nemusí rozpoznat ani zkušenější uživatel. I zde dochází k podvržení falešné stránky, která vypadá, jakoby pocházela z bankovního domu, ale navíc se na ni můžeme dostat i při správném zadání regulérní internetové adresy banky v prohlížeči. Získané odpovědi mi pomůžou vyhodnotit hypotézu č. 6.

Otázka č. 15: Používáte pro přihlášení na různé stránky stejná hesla?

Odpověď	*Počet respondentů*	*Procenta*
a. Ano	69	33 %
b. Ne.	141	67 %
Celkem	210	100 %

Tab. 15: Používání stejných hesel

Graf 15: Používání stejných hesel

Otázka č. 15 se vztahovala k hypotéze č. 7. Zjistila jsem, že 33 % respondentů používá pro přihlášení na různé stránky stejná hesla, zbylých 67 % je prozíravých a hesla má různá. A tak je to správně, protože užívat jedno heslo k přihlášení na všechny služby, které používáme, není bezpečné. Pokud totiž někdo toto heslo získá, může ihned „ukrást naší identitu“, bavit se s našimi kolegy/kamarády, prohlížet si e-maily, stahovat osobní data, nakupovat v e-shopech, a to všechno naším jménem. Aplikování hesel by mělo vycházet z určité pyramidy důležitosti přístupu. Základnu by tak mohly tvořit registrace na nejméně důležitých webových serverech a špici by měly představovat e-maily, platební systémy, internetové obchody. V žádném případě se nedoporučují jednoduchá hesla jako jména členů rodiny, domácího mazlíčka, datum narození, 12345 atp. Mnohem vhodnější jsou na první pohled nepochopitelné shluky písmen – například Ko1Le2Di3Pe4Ok5. Jedná se o počáteční písmena dětské písničky (Kočka Leze Dírou Pes Oknem) doplněné pouze o čísla. Toto heslo je prolomitelné takzvaným útokem hrubou silou, při použití průměrného počítače však trvá jeho odhalení několik milionů let. A to už je nějaká doba, kterou útočník nebude mít zájem absolvovat. Při vytváření hesla je dobré se vyhnout použití písmen s háčky nebo čárkami (diakritikou). Při návštěvě některých cizích zemí bychom se pak třeba nemohli přihlásit na svůj účet, neboť tamní počítače nemusí umožňovat zvolit znaky s českou diakritikou. Experti také doporučují jednou za čas hesla pravidelně měnit.

5.4 Zhodnocení předpokladů dotazníku

Předpoklad č. 1
Domnívám se, že více jak 80 % studentů vědí, co si pod pojmem sociální inženýrství představit.
Předpoklad č. 1 se nepotvrdil.
Odhad jsem ověřovala pomocí otázky č. 1. Celkem 51 % respondentů odpovědělo správně. Toto nízké číslo mě velmi překvapilo, očekávala bych u studentů vysoké školy lepší výsledek.

Předpoklad č. 2
Předpokládám, že více jak 65 % studentů vědí, co je to Phishing.
Předpoklad č. 2 se potvrdil.
Hypotézu jsem testovala pomocí otázky č. 3. Počet studentů, kteří odpověděli správně, je 69 %. Tento počet studentů považuji za uspokojivý a předpoklad se mi potvrdil.

Předpoklad č. 3
Odhaduji, že více jak 80 % respondentů by hoaxovou zprávu nikomu nepřeposlalo a smazalo ji.
Předpoklad č. 3 se potvrdil.
Otázku jsem ověřovala prostřednictvím otázky č. 6. Dohromady 96 % studentů odpovědělo, že by hoaxovou zprávu nikomu nepřeposlalo a raději ji smazalo. 3 % by zprávu automaticky přeposlalo svým známým a 1 % nevědělo. Výsledek je více než potěšující a koresponduje s mým odhadem.

Předpoklad č. 4
Domnívám se, že stále minimálně 10 % studentů platí na Internetu nejraději pomocí dobírky.
Předpoklad č. 4 se potvrdil.
Z dotazníku vyplynulo, že nejvíce studentů preferuje platbu platební kartou, 35 % upřednostňuje hotovost a na třetím místě se umístila dobírka s 15 %. Výsledek dokonce předčil moji domněnku. Předpoklad jsem si ověřila pomocí dotazníkové otázky č. 8.

Předpoklad č. 5
Předpokládám, že minimálně 50 % studentů si při přihlašování do svého internetového bankovnictví ověřuje stránky certifikátem.
Předpoklad č. 5 se nepotvrdil.
Pouze 32 % respondentů ověřuje stránky do internetového bankovnictví prostřednictvím certifikátu. Výsledné číslo se mi zdá značně neuspokojivé a nepotvrzuje můj odhad. Předpoklad jsem testovala pomocí otázky č. 14.

Předpoklad č. 6
Domnívám se, že více jak 65 % studentů používá při přihlašování na různé stránky různá hesla.
Předpoklad č. 6 se potvrdil.
Ze 100 % uvedlo 67 % studentů, že používá při přihlašování na různé stránky rozdílná hesla. Dosažené skóre potvrzuje mojí hypotézu a ověřovala jsem jí pomocí otázky č. 15.

5.5 Návrh souboru opatření

Na základě zjištěných informací z teoretické části a dotazníkového šetření se v následujících odstavcích pokusím navrhnout komplexní soubor opatření, které sníží míru rizika zneužití citlivých údajů v souvislosti s problematikou sociálního inženýrství.

5.5.1 Opatření pro každého uživatele

V souvislosti s tím, jak se rozšiřuje nabídka služeb elektronických platebních systémů, zvyšuje se i počet sociotechnických útoků na jejich uživatele. Bezpečnost každého vzdáleně ovládaného účtu však nezávisí pouze na zabezpečení informačních systémů jednotlivých bank, ale také na péči a pozornosti, kterou věnuje bezpečnosti samotný klient. Nyní uvedu několik doporučení, kterými by se měl uživatel řídit.

- Veřejně přístupný počítač s připojením na Internet přiměřenou bezpečnost nezaručuje, proto bychom měli používat zejména zařízení důvěryhodná, nám známá a řádně zabezpečená. Zařízení by mělo být vybaveno aktualizovaným operačním systémem, aktualizovaným internetovým prohlížečem, trvale zapnutým a aktualizovaným antivirovým programem. Na takové zařízení bychom měli instalovat pouze programy z důvěryhodných zdrojů a věnovat pozornost oprávněním požadovaným instalovanou aplikací. Tyto opatření se však netýkají pouze našeho počítače, ale také tabletu a mobilního telefonu.
- Nikdy bychom neměli sdělovat naše autentizační údaje. Stejně tak bychom neměli povolovat v nastavení našeho zařízení automatické za-pamatování hesel systémem.
- Nikdy bychom neměli reagovat na e-mailové zprávy s podezřelým názvem a obsahem. Banka nikdy po klientovi tyto osobní údaje v elektronické komunikaci nežádá.
- Pokud obdržíme podezřelou zprávu, nereagujme na ni, neotvírejme přílohy, neklikejme na odkazy a kontaktujme naši svou banku.
- Používejme složitá hesla, nikoliv hesla prostá a která jdou odvodit z informací o naší osobě.
- Ujistěme se, že vstupujeme na správné webové stránky. Zkontrolujme, zda funguje šifrované spojení (HTTPS) a ověřme stránku pomocí certifikátu.

5.5.2 Opatření pro univerzity

Sociální inženýrství do vzdělávacích osnov
Z mého pohledu vidím největší problém v tom, že plno lidí, a to nejen studentů, nevědí, co je sociální inženýrství. Tuto skutečnost mohu potvrdit ze zkušeností z mého okolí – kdokoli se mě zeptal, o čem píši svou práci, nevěděl, co si pod pojmem představit. Nevědí, že existují různé metody útoků sociotechniky, že se můžou nechat snadno napálit, když nebudou mít dobře chráněný počítač a budou příliš důvěřiví. Ostatně to potvrzuje i výsledek otázky č. 1 v dotazníku. Přitom se jedná o tak zajímavé a hlavně důležité téma ve vztahu k uživatelské bezpečnosti na Internetu.

V rámci opatření, které povede k minimalizaci rizika zneužití důvěrných informací, navrhuji přidat problematiku sociálního inženýrství jakožto osvětu o bezpečnosti do vzdělávacích osnov na univerzitách. Podle mého názoru by stačily dvě až tři přednášky k tématu v jakémkoliv IT předmětu pro vytvoření základní představy o co se jedná a jak se bránit. Dokonce si dokážu představit volitelný předmět Sociální inženýrství, který by obsahoval studium problematiky do detailu včetně seminární práce, ve které by si studenti sami mohli vyzkoušet jednu z metod sociotechniky formou experimentu na svých známých.

Soukromé údaje na jiný server
Kybernetické útoky nemusí mít nutně za cíl získat přihlašovací údaje k platebním účtům. Mohou útočit i s cílem získat například rodná čísla uživatelů, adresy a další. Obětí se tak snadno mohou stát univerzity, které takové citlivé informace o studentech shromažďují. Pokud tak už činí, měly by mít tyto citlivá data uloženy na samostatném serveru odděleném od veřejnosti i od školní sítě. Infrastruktura datové sítě spojující tento server s veřejností by měla být zabezpečena firewally a systémy IDS a IPSI (Intrusion Detection Systems a Intrusion Prevention Systems), zaznamenávajícími "vniknutí" či nějaký "pohyb" na této síti. Univerzity by také měly mít specializované zaměstnance, kteří budou dohlížet, monitorovat a analyzovat výsledky systémů IDS, IPS a firewallů, aby bylo možno případný útok či zneužití odhalit a lokalizovat. Všechny výstupní informace hlídacích systémů by měly být dlouhodobě logovány a uschovány.

5.5.3 Opatření pro firmy

Z pohledu sociotechnika je nejzranitelnějším objektem v organizaci její zaměstnanec. Z průzkumů o stavu informační bezpečnosti v organizacích, které pravidelně pořádá společnost Eset, vyplývá, že velkou část bezpečnostních rizik identifikovaných v rámci organizace reprezentuje lidské chování jako chyba, nepozornost, nedbalost a nevědomost. Přes 60 % organizací označuje za příčiny výskytu bezpečnostních incidentů právě chování zaměstnanců, proto jsem v následujícím odstavci pokusila navrhnout několik řešení, které by pomohly eliminovat nebezpečí spojená s chováním zaměstnanců a případnými útoky sociotechniky.

Nejprve si musí organizace vytvořit jednotné interní pravidla bezpečnosti. Všichni zaměstnanci by měly být s těmito pravidly seznámeni a minimálně jednou ročně by mělo proběhnout pravidelné školení v oblasti informační bezpečnosti. Zaměstnavatel musí vyžadovat po personálu jejich dodržování. Jako nejúčinnější způsob ověření se mi zdá simulace potenciálního útoku sociotechnikou.

Testování pomocí sociálního inženýrství se může vykonat s různými znalostmi interního prostředí dané organizace. V závislosti na určitých požadavcích firmy může toto testování simulovat odlišné situace z reálného prostředí. Může to být útok skrytého útočníka, útok zaměstnance, který už ve společnosti dávno nepracuje nebo útok zaměstnance současného, který má veškerý přístup k důležitým datům.

Můj vlastní návrh testování může proběhnout pomocí následujících technik:

- phishingový test,
- test s přenosnými médii,
- pokus o fyzický průnik do prostoru organizace,
- telefonický test,
- prohledávání odpadků.

Nejdůležitější částí jsou výstupy tohoto simulačního testu. Na základě těchto výstupů by měla mít daná firma lepší představu o tom, jak je na tom po stránce bezpečnosti a co pro ni případná reálná hrozba představuje. Dopady pro společnosti by za předpokladu dodržení mého navrhovaného systému testů měly být minimální.

Musím však zdůraznit, že hlavním cílem realizovaných testů není zjištění selhání jednotlivých pracovníků, ale poukázání na případnou nefunkční část systému informační bezpečnosti. Zaměstnanci budou také obohaceni o informace týkajících se bezpečnosti před zneužitím elektronického platebního systému a celkové bezpečnosti celé firmy.

Všechna tato opatření z vykonaných testů dále budou implementována do systému řízení informační bezpečnosti systematicky a komplexně.
Doporučuji zahrnutí do následujících oblastí:

- Řízení rizik – sem patří identifikovaná rizika z předchozího testu
- Definování a revize interních bezpečnostních pravidel – např. Ve formě směrnic nebo interních předpisů
- Zvyšování povědomí o hrozbách – toto opatření jsem navrhla za účelem zvyšování povědomí o informační bezpečnosti a bude probíhat prostřednictvím pravidelných školení nebo za pomocí jiné interní komunikace se zaměstnanci

Testy na obranu před sociálním inženýrstvím mají velmi významnou úlohu. Tímto opatřením má určitá firma možnost vyzkoušení si tzn. „nanečisto“, jestli je určitou hrozbou zranitelná a jak je schopná s opatřeními, které už existují, této hrozbě odolat.

6 Závěr

Tato práce byla věnována problematice sociálního inženýrství v souvislosti s elektronickými platebními systémy. V první části byla rozebrána teoretická témata související s prací a tyto poznatky byly následně využity v části praktické. Dále byl popsán metodický postup, který vycházel ze zadání práce.

V praktické části jsem testovala povědomí studentů Mendelovy univerzity o problematice sociálního inženýrství a jejich chování na Internetu pomocí dotazníkového šetření. Dotazník se skládal z 15 testových otázek a před jeho aplikací jsem si stanovila 4 cíle, kterých jsem s jeho pomocí chtěla dostát. Mezi cíle patřily:

- zjištění, zda studenti vědí, co je sociální inženýrství,
- zjištění, zda se s nějakou z metod sociotechniky již setkali a jak by na ni reagovali,
- zjištění, jakou platební metodou používají na Internetu nejčastěji,
- zjištění, zda se chovají na Internetu bezpečně.

Získané odpovědi od respondentů mi pomohly nejen dostát cíle, ale vyhodnotit všechny otázky dotazníku jak slovně, tak i graficky. Na základě výsledků jsem se rozhodla stanovit soubor opatření, který by pomohl zvýšit povědomí o sociálním inženýrství. Nejprve jsem stanovila opatření pro běžné uživatele elektronických platebních systémů, které nezávisí pouze na zabezpečení informačních systémů jednotlivých bank, ale také hlavně na péči a bezpečnosti, kterou jim věnuje samotný klient. Dále jsem navrhla opatření pro univerzity ve smyslu zavedení sociálního inženýrství přímo do vyučovacích osnov ve formě přednášek, diskuzí a ostatních komunikačních metod, které si kladou za cíl zvýšit povědomí o tomto problému mezi samotnými studenty škol. Dalším návrhem opatření bylo ukládání soukromých informací na jiný server před kybernetickým útokem.

V neposlední řadě jsem navrhla systém simulačních testů pro firmy. Nastínila jsem nejprve podmínky před samotným testem a následně uvedla jednotlivé techniky celého testu. Výsledek těchto simulačních testů poukazuje na současné zabezpečení společností před neznámými útoky a hlavním cílem nebylo poukázat na chyby zaměstnanců, ale hlavně na chyby v nefunkčních částech systému firmy.

Věřím, že by mnou navržená opatření byly v praxi využitelná jak pro běžné uživatele, studenty nebo zaměstnance společnosti a pomohly by tak celkově zvýšit povědomí o sociálním inženýrství v elektronických platebních systémech.

7 Literatura

Co je internetové bankovnictví [online]. 2015. [cit. 2015-04-02]. Dokument ve formátu HTML. Dostupné z: http://www.penize.cz/80347-co-je-internetove-bankovnictvi.

Co je PaySec [online]. 2007 [cit. 2015-05-05]. Dokument ve formátu HTML. Dostupné z: https://www.paysec.cz/CmsPage.aspx?Id=whatIsPaysec.

Co je to hoax [on-line]. 2015. [cit. 2015-05-15]. Dokument ve formátu HTML. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax.

Co je to SSL [on-line]. 2009. [cit. 2015-03-19]. Dokument ve formátu HTML. Dostupné z: http://www.ssl-thawte.cz/ssl/co-je-to-ssl.

Důvěryhodné zabezpečení [on-line]. 2011. [cit. 2015-04-08]. Dokument ve formátu HTML. Dostupné z: https://www.skrill.com/cz/osobni/bezpecnost/.

Fungování online plateb u PayU [on-line]. 2015. [cit. 2015-04-30]. Dokument ve formátu HTML. Dostupné z: http://www.payu.cz/zabezpeceni-line-plateb-e-shopy.

CHVÁTAL, D. *Klienty Servisu 24 České spořitelny zkouší phishing* [online]. 2014. [cit. 2015-05-11]. Dokument ve formátu HTML. Dostupné z: http://www.mesec.cz/aktuality/klienty-servisu-24-ceske-sporitelny-zkousi-zlakat-phishing/.

IBA *Internet Banking System* [on-line]. 2015. [cit. 2015-04-03]. Dokument ve formátu HTML. Dostupné z: http://ibagroupit.com/en/products/information-and-payment-systems/internet-bank/.

Jak systém funguje [on-line]. 2008 [cit. 2015-04-08]. Dokument ve formátu HTML. Dostupné z: http://www.paypalcz.cz/jak-system-funguje.

James, L. *Phishing bez záhad*. Grada. 2007. 281 s. ISBN 80-2471-766-1.

JUŘÍK, P. *Platební karty*: 1870-2006 : velká encyklopedie. 1. vyd. Praha: Grada, 2006, 296 s. ISBN 80-247-1381-0.

KUNEŠ, J. *Co je to sociální inženýrství* [on-line]. 2012. [cit. 2015-05-15]. Dokument ve formátu HTML. Dostupné z: http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-2-dil-44372.

MÁČE, M. *Platební styk: klasický a elektronický*. 1. vyd. Praha: Grada, 2006, 220 s. Osobní a rodinné finance. ISBN 80-247-1725-5.

MATYÁŠ, V.,KRHOVJÁK, J. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. 1. vyd. Brno: Masarykova univerzita, 2008, 125 s. ISBN 978-80-210-4556-9.

MITNICK, Kevin D a William L SIMON. *Umění klamu*. Gliwice: Helion, 2003, 348 s. ISBN 83-7361-210-6.

Nebezpečné komunikační praktiky a sociální inženýrství [on-line]. 2008. [cit. 2015-05-11]. Dokument ve formátu HTML. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/18-20.

ODVÁRKA, P. *SSL protokol (1) - princip a přínosy* [online]. 2002 [cit. 2015-05-22]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=SSL-protokol-1-princip-a-prinosy-2542002.

Osobní finance [online]. 2015. [cit. 2015-04-02]. Dokument ve formátu HTML. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/sc_1585.xml.

Phishing [online]. 2015. [cit. 2015-05-11]. Dokument ve formátu HTML. Dostupné z: http://www.hoax.cz/phishing/.

Phishing a pharming [on-line]. 2015. [cit. 2015-05-11]. Dokument ve formátu HTML. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx.

Platební karty a jejich druhy [online]. 2015 [cit. 2015-04-02]. Dokument ve formátu HTML. Dostupné z: http://www.penize.cz/15744-platebni-karty-a-jejich-druhy.

Počátky internetového bankovnictví [online]. 2015. [cit. 2015-04-02]. Dokument ve formátu HTML. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce.

Proč Skrill [online]. 2011. [cit. 2015-04-08]. Dokument ve formátu HTML. Dostupné z: https://www.skrill.com/cz/osobni/.

Protokoly pro elektronické platební systémy [on-line]. 2007. [cit. 2015-03-19]. Dokument ve formátu HTML. Dostupné z: http://www.security-portal.cz/clanky/protokoly-pro-elektronicke-platebni-systemy.

Příkaz k úhradě [on-line]. 2007. [cit. 2015-04-07]. Dokument ve formátu HTML. Dostupné z: http://www.financnivzdelavani.cz/webmagazine/page.asp?idk=312.

Sellers Protection [on-line]. 2015. [cit. 2015-04-08]. Dokument ve formátu HTML. Dostupné z: https://www.paypal.com/cz/webapps/mpp/paypal-safety-and-security.

SCHLOSSBERGER, O.,HOZÁK, L. *Elektronické platební prostředky*. 1. vyd. Praha: Bankovní institut vysoká škola, 2005, 144 s. ISBN 80-7265-073-4.

Sociální inženýrství [on-line]. 2004. [cit. 2015-05-11]. Dokument ve formátu HTML. Dostupné z: http://www.security-portal.cz/clanky/socialni-inzenyrstvi.

ŠIMEK, R. *Sociotechnika* [on-line]. 2003. [cit. 2015-05-11]. Dokument ve formátu HTML. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm.

Zabezpečení online plateb u PayU [on-line]. 2015. [cit. 2015-04-30]. Dokument ve formátu HTML. Dostupné z: http://www.payu.cz/zabezpeceni-line-plateb-e-shopy.

8 Seznam obrázků

Obr. 1: Zabezpečení plateb pomocí 3D-Secure (Osobní finance, 2015).....15
Obr. 2: Schéma elektronického bankovnictví (IBA Internet Banking Systém, 2013) 20
Obr. 4: Phishingový útok na klienty České spořitelny, a.s. v roce 2014 (Chvátal, 2014).....27
Obr. 5: Schéma pharmingu (Chaudhari, 2006).....28

9 Seznam tabulek

Tab. 1: Co je sociální inženýrství 33
Tab. 2: Setkání s metody sociálního inženýrství 34
Tab. 3: Znalost phishingu 35
Tab. 4: O jakou metodu se jedná 37
Tab. 5: Setkání s hoaxem 38
Tab. 6: Co uděláte při obdržení podobné zprávy 39
Tab. 7: Znalost Vishingu 40
Tab. 8: Způsob placení na internetu 41
Tab. 9: CVV kód 42
Tab. 10: Používání antivirového programu 43
Tab. 11: Používání elektronického bankovnictví 44
Tab. 12: Zpráva z banky 45
Tab. 13: Setkání s podvodným e-mailem 46
Tab. 14: Sledování ochranných prvků 47
Tab. 15: Používání stejných hesel 49

10 Seznam grafů

Graf 1: Co je sociální inženýrství....33
Graf 2: Setkání s metody sociálního inženýrství....34
Graf 3: Znalost phishingu....36
Graf 4: O jakou metodu se jedná....37
Graf 5: Setkání s hoaxem....38
Graf 6: Co uděláte při obdržení podobné zprávy....39
Graf 7: Znalost Vishingu....40
Graf 8: Způsob placení na internetu....41
Graf 9: CVV kód....42
Graf 10: Používání antivirového programu....43
Graf 11: Používání elektronického bankovnictví....44
Graf 12: Zpráva z banky....45
Graf 13: Setkání s podvodným e-mailem....46
Graf 14: Sledování ochranných prvků....48
Graf 15: Používání stejných hesel....49

Přílohy

A Dotazníkové šetření

1. Co je sociální inženýrství?

a. Společenská věda zkoumající sociální život jednotlivců, skupin a společností.
b. Disciplína, která vytváří flexibilní a komplexní řešení pro dlouhodobé zvyšování výkonností firem bez rozdílu odvětví a velikostí.
c. Ovlivňování a přesvědčování lidí s cílem získat požadované informace.
d. Činnost zahrnující inženýrství, informatiku a management, jejímž cílem je návrh, tvorba a údržba počítačových programů.

2. Setkali jste se osobně s nějakou z metod sociálního inženýrství?

a. Ne
b. Ano, ve škole
c. Ano, v zaměstnání
d. Jinde

3. Co je to Phishing?

a. Jedná se o typickou hoaxovou zprávu, která se hromadnou poštou šíří mezi uživateli a jejím cílem je příjemce vystrašit, pobavit, nebo jinak nepravdivě informovat.
b. V prostředí internetu se jedná zejména o různé podvodné nabídky výher, výhodné aukce, velké slevy na zboží. Kliknutím a stažením nabízeného softwaru se do počítače oběti nainstaluje škodlivý software.
c. Metoda sociálního inženýrství, při které je odeslán falšovaný e-mail napodobující legální instituci s úmyslem získat od příjemce důvěrné informace.

4. O jakou metodu sociálního inženýrství se jedná, pokud obdržíte zprávu, která má za cíl příjemce vystrašit, pobavit, nebo jinak nepravdivě informovat, a obsahuje žádost o další rozeslání pokud možno co největšímu množství adres?

a. Hoax
b. Pretexting
c. Phishing
d. SCAM419

5. Setkali jste se někdy s podobnou zprávou?

a. Ano
b. Ne

6. Co uděláte, když obdržíte podobnou zprávu?

TUTO INFORMACI VYSILALI NA EUROPE 1. PREDEJTE JI DAL !!! V PRISTICH DNECH MUSITE DAVAT VELKY POZOR A NEOTEVRIT ZADNY E-MAIL S POZVANKA (INVITATION) NEZAVISLE NA TOM, OD KOHO JE. JEDNA SE O VIRUS, KTERÝ " OTEVIRA OLYMPIJSKOU POCHODEN" A KTERÝ SPALI HARD TENTO VIRUS BUDE ODESLAN OSOBOU, KTERA VAS MA VE SVYCH

KONTAKTECH.MUSITE PROTO TUTO ZPRAVU ROZESLAT ! JE LEPSI ZPRAVU OBDRZET 25 X NEZ OBDRZET VIRUS A OTEVRIT HO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! TAKZE POKUD OBDRZITE E-MAIL S NAZVEM INVITATION - NEOTVIREJTE HO A VYPNETE OKAMZITE VAS POCITAC !!!!!!!!!!!!!!!!!!!!!!!!!!!! JE TO NEJHORSI VIRUS OHLASENY CNN A KLASIFIKOVANY SPOLECNOSTI MICROSOFT JAKO NEJDESTRUKTIVNEJSI VIRUS, KTERY KDY EXISTOVAL !!!!!!! BYL OBJEVEN VČERA ODPOLEDNE MCAFEE A IL ZATÍM NENASLA JEHO LOZISKO, ABY MOHLA ZNICIT "ZONU " NA HARD DISKU, KDE JSOU SCHOVANE VSECHNY "ZIVOTNI" (NEJDULEZITEJSI) NFORMACE. POSLETE TENTO E-MAIL VSEM, KOHO ZNATE, VASIM PRATELUM, VSEM VASIM KONTAKTUM CIM VICE OSOB UPOZORNITE PREDEM, TIM HURE SE BUDE VIRUS SIRIT !!!

a. Automaticky přepošlu všem známým, aby se virus nešířil.
b. Zprávu nikomu nepřeposílám a smažu ji.
c. Nevím.

7. Znáte Vishing?

- Ano
- Ne

8. Jaký způsob placení na Internetu preferujete?

a. Hotově na pobočce
b. Dobírka
c. Platební karta
d. Příkaz k úhradě
e. PayPal
f. PaySec
g. Jiný

9. K čemu slouží CVV kód?

a. Identifikuje platební kartu.
b. Je speciálním identifikačním číslem držitelem karty.
c. Užívá se pro zvýšení ochrany elektronických transakcí.
d. Identifikuje prodejce při platbě platební kartou.

10. Používáte antivirový program?

a. Ano
b. Ne

11. Používáte internetové elektronické bankovnictví?

a. Ano
b. Ne

12. Představte si situaci: Na e-mail Vám přišla zpráva od Vaší banky, ve které Vás vyzývá k aktualizaci Vašich osobních údajů v internetovém bankovnictví. Ve zprávě je také přiložen odkaz na internetové bankovnictví Vaší banky. Jak se zachováte?

a. Odkaz otevřu, přihlásím se a aktualizuji své údaje.
b. Zprávu smažu, aniž bych udělal/a, co se po mně vyžaduje.

c. Kontaktuji svou banku a ověřím zprávu.
d. Nevím.

13. Setkali jste se někdy s podobným e-mailem, který se vydával za finanční instituci a požadoval Vaše přihlášení v podobě uživatelského jména a hesla?
a. Ano
b. Ne

14. Jaké ochranné prvky stránky sledujete, když se přihlašujete do svého internetového bankovnictví?
a. Ověření stránky certifikátem
b. Kontrola šifrovaného spojení (HTTPS)
c. Kontrola webové adresy
d. Kontrola vzhledu webové stránky
e. Žádné z uvedených

15. Používáte pro přihlášení na různé stránky stejná hesla?
a. Ano
b. Ne