Zabezpečení online platebních transakcí při nákupu v e - shopu

Security of Online Payment Transactions During E-shop Buying

Pavel Hubáček

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel HUBÁČEK**
Osobní číslo:	**A09292**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zabezpečení online platebních transakcí při nákupu v e-shopu**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury, která se vztahuje ke zvolenému tématu bakalářské práce.**
2. **V rámci východiskové hypotézy charakterizujte a analyzujte zkoumaný problém on-line platební systémy používané pro internetové platby (fenomenologie, etiologie).**
3. **Analyzujte aktuální bezpečnostní rizika a útoky v oblasti on-line platebních systémů, postupů a při využívání platebních karet, včetně ekonomických, sociálních a právních aspektů.**
4. **Analyzujte a specifikujte bezpečnostní opatření při využívání on-line platebních systémů a platebních karet.**
5. **V závěru bakalářské práce zhodnoťte současný stav v dané oblasti; v souladu s analytickými závěry a výstupy prezentujte vlastní návrhy, využitelné v praxi.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ČANDÍK, Marek. Základy informační bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-218-1.**
2. **LANCE, James. Phishing bez záhad. Praha: Grada, 2007. ISBN 80-247-1766-2.**
3. **MÁČE, Miroslav. Platební styk klasický a elektronický. Praha: Grada, 2006. ISBN 80-2471-725-5.**
4. **PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví: rady a tipy. Praha: Computer Press, 2000. ISBN ISBN 80-7226-328-5.**
5. **VAŠEK, Matyáš a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova Univerzita, 2008. ISBN 978-80-210-4556-9.**

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

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tématem bakalářské práce je bezpečnost platebních transakcí při platbách v internetových obchodech. V první části jsou popsány platební karty a systémy, jejichž prostřednictvím realizace transakce probíhá. V druhé části jsou specifikovány možné útoky a dotazníkový výzkum o povědomí uživatelů o možných hrozbách v této oblasti.

Klíčová slova:

Platební karta, internetové bankovnictví, platební systémy, bezpečnost, PIN

ABSTRACT

The theme of the Bachelor's thesis is Security of Online Payment Transactions during E-shopping. The first part describes various types of payment cards and systems through which the transactions take place. The second part of the thesis specifies possible attacks and questionnaire survey of users´ awareness of potential threats in this area.

Keywords:

Credit card, Internet banking, payment systems, security, PIN

Na tomto místě bych rád poděkoval vedoucímu bakalářské práce panu PhDr. Mgr. Stanislavu Zelinkovi za jeho ochotu, vstřícnost a věcné připomínky, které dopomohly k vypracování práce. V neposlední řadě patří můj dík rodině a osobám, které se účastnily dotazníkového průzkumu.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

…….
podpis bakaláře

OBSAH

ÚVOD

S rozvojem internetu v polovině 90. let minulého století nastal také prudký rozvoj služeb, které jsou poskytovány jeho prostřednictvím. Jednou z nich je možnost internetového prodeje, který je pro provozovatele nejlevnějším možným způsobem jak své výrobky a zboží nabídnout koncovým zákazníkům. Je zřejmé, že ruku v ruce s tímto trendem kráčel také rozvoj elektronických platebních systémů. Ty výrazně zrychlily a zjednodušily proces platby realizovaný v prostředí internetu tím, že jejich dostupnost je možná prakticky v kteroukoliv hodinu 7 dní v týdnu. Uživatelé by si však měli uvědomovat také možná rizika, které se mnohdy na úkor uživatelské přívětivosti pachatelům trestných činů nabízí.

Cílem bakalářské práce je popsat možnosti realizace a bezpečnosti platebního styku při nákupu v elektronickém obchodě. Práce je rozdělena na část teoretickou a praktickou. V části teoretické se nejprve věnuji historii a vysvětlení základních pojmů, které se vztahují k elektronickému obchodu a následně termínům z oblasti zabezpečení a šifrování dat. V následujících kapitolách jsou popsány možnosti úhrady za zboží prostřednictvím platebních karet, internetového bankovnictví a platebních systémů. Zvláštní pozornost věnuji platebním kartám, protože ty tvoří základní prostředek pro realizaci platby pomocí všech typů platebních systémů, neboť bývá vydávána zároveň se zřízením běžného účtu a internetového bankovnictví, z něhož je posléze možné přečerpávat finance na systémy elektronických peněženek. Dále je zmíněn výběr zákonů, které se vztahují k elektronickému obchodu a spotřebitelům.

V praktické části analyzuji možnosti zneužití platební karty jak možnými pachateli, tak ze strany nepoctivého majitele a nálezců. Dále jsou uvedeny potenciální hrozby z oblasti počítačové kriminality, jejich popis a projevy. Součástí je také dotazníkový průzkum, který napomohl analýze o informovanosti uživatelů vzhledem k elektronickým platbám a nákupu.

V závěru práce jsou prezentovány návrhy a postupy pro bezpečné používání platebních karet a uživatele, kteří realizují platební styk prostřednictvím svého osobního počítače.

I. - TEORETICKÁ ČÁST

1 HISTORIE A VÝVOJ ELEKTRONICKÉHO OBCHODOVÁNÍ

Za počátek elektronického obchodování můžeme považovat rok 1989, kdy Tim Berners-Lee přišel na nový způsob komunikace v prostředí internetu - hypertextové dokumenty neboli také WWW (Word Wide Web). Jsou to texty, které obsahují odkazy na další dokumenty, mohou být umístěny na jiném počítači, třeba na druhém konci světa. V důsledku jednoduchého ovládání se tento způsob komunikace (spolu s masivním rozmachem osobních počítačů) šířil mezi miliony nových uživatelů. Internet tak přinesl do světa nákupů zásadní průlom. Z pohodlí domova či kanceláře se ve Spojených Státech začalo, nakupovat již v roce 1992 a v letech 1994 a 1995 vznikat elektronické obchody dnešního typu. První prodejní komoditou se staly hudební nahrávky na CD, následovaly dárkové předměty a knížky, poté přišla na řadu elektronika, hračky a například nábytek. [11]

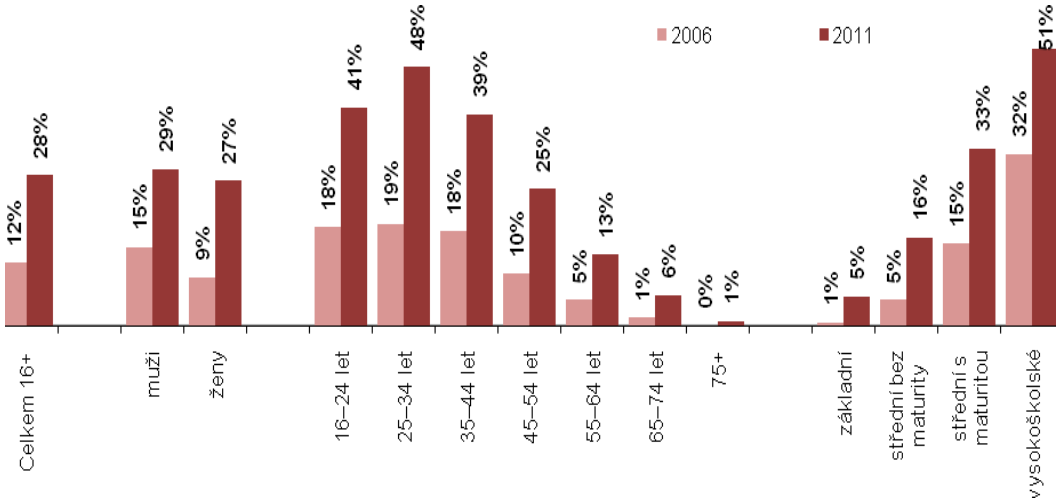
1.1 Vývoj

Elektronické obchodování v České republice má dnes již více než patnáctiletou historii, ale jeho vývoj je hodně odlišný. Elektronické obchody se totiž ubíraly různými směry nejen v Česku a v Americe, ale i jinde v Evropě. Zatímco na Starém kontinentu se projevovala nedůvěra zákazníků v on-line platby, ve Spojených Státech se internetový business rozvíjel. Rozdílný vývoj internetového obchodování na obou stranách Atlantického oceánu byl dán technologickým zaostáváním včetně rozšíření platebních karet. Teprve na začátku třetího tisíciletí začínají čeští zákazníci vnímat nákup prostřednictvím internetu jako relativně bezpečný. Důvodem je především mnohem více profesionální přístup některých on-line prodejců. Obecně se začíná zkracovat doba dodání zboží zákazníkům a silnější elektronické obchody začínají fungovat na smluvní bázi nad velkoobchody. Prakticky to má za následek, že mají již relativně přesné informace o stavu prodávaného zboží. Rozšiřuje se také využívání on-line plateb debetními i kreditními kartami. [12]

1.2 Současná situace v ČR

Pro prezentaci současné situace jsem využil dat Českého statistického úřadu. Ten uvádí, že ve 2. čtvrtletí roku 2011 nakoupilo prostřednictvím internetu 2,5 mil. osob, tedy 28 % z celkového počtu obyvatel ČR a 43 % z celkového počtu uživatelů internetu. Mezi nakupujícími prostřednictvím internetu nepatrně převažují ženy nad muži (pokud

hodnotíme podíl na uživatelích internetu) a nejčastěji nakupují prostřednictvím internetu vysokoškoláci a osoby ve věku 24 – 34 let. [13]



Obrázek 1 Jednotlivci nakupující v internetových obchodech [13]

2 VYMEZENÍ POJMŮ

2.1 Pojmy týkající se elektronického obchodu

2.1.1 E - business

E - business (elektronické podnikání) zahrnuje nejen prodej a poskytování služeb prostřednictvím internetu a procesy s tím spojené, ale znamená transformaci všech procesů uvnitř, ale také vně firmy, s využitím moderních technologií na bázi internetu či webu. Jinak řečeno, jde o způsob podnikání využívající technologie internetu jak v oblasti řízení podniku, tak v oblasti spolupráce s partnerskými podniky, v oblasti nákupu a prodeje, poskytování služeb zákazníkům atd. E - business tedy představuje využití moderních technologií pro zefektivnění všech firemních procesů.

2.1.2 E - commerce

Pod pojmem e - commerce (elektronický obchod) rozumíme především prodej či poskytování služeb skrze internet. Nejedná se však pouze o internetové obchody, ale řadíme sem také jakékoliv webové prezentace firem, které umožňují objednání nabízeného produktu či služby, například formou e - mailu. [14]

2.1.3 E - shop

Základem e - shopu (internetového obchodu) je běžný katalog výrobků, kterým podnikatelský subjekt specializuje na vymezený okruh svého působení. E - shop se tedy skládá z detailů jednotlivých výrobků a přehledů výrobků v daných kategoriích. Zpravidla informuje zákazníka pomocí náhledu fotografie, detailním popisem o daném výrobku, možností dopravy, způsobu úhrady či dokonce nechávají vyjádřit své názory v diskusi.

B2B

B2B (z angl. business to business) vyjadřuje vztah mezi dvěma podnikateli nebo firmami. Obchod se odehrává na úrovni, do které se nedostane klasický zákazník, typicky se jedná o vztah mezi dodavatelem a subdodavateli nebo velkoobchodem a jednotlivými maloobchody. Účelem tohoto obchodování není konečná spotřeba zboží či služby, ale další prodej, který nutně následuje. Před prvním nákupem je tedy třeba být zaregistrovaný v síti odběratelů. Často se stává, že dodavatelská firma založí e – shop až na žádost svých

odběratelů, kterým tato forma objednávání zboží vyhovuje mnohem lépe. Jedním z mnoha příkladů může být např. objednávání hardwarových komponentů u velkého dodavatele pro soukromou kamennou prodejnu.

B2C

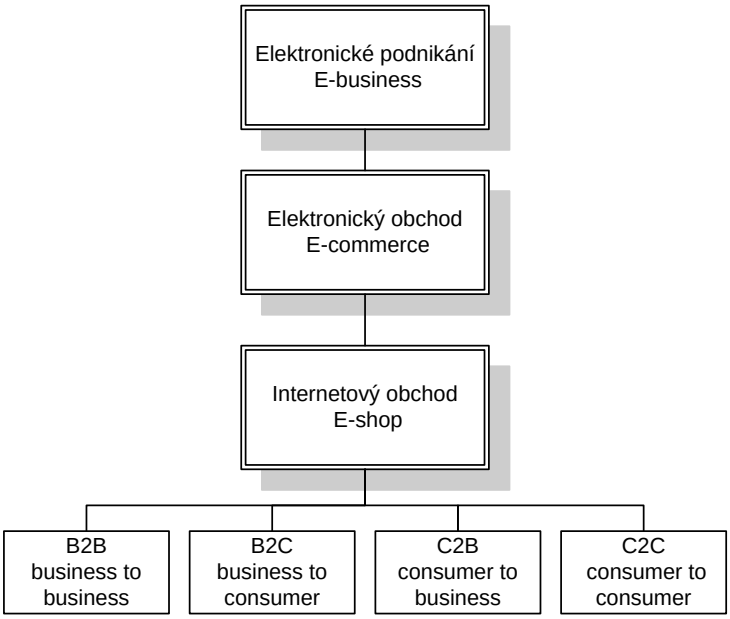
B2C (z angl. business to consumer) patří mezi nejčastější typ e-shopu, se kterým se běžně na internetu setkáváme. Zde vystupujete v roli zákazníka a vlastník e - shopu se snaží prodat zboží či služby. Prodej koncovým zákazníkům je vlastně internetová obdoba kamenného obchodu.

C2B

Model C2B (z angl. consumer to business) představuje vztah mezi spotřebitelem a podnikatelem. K tomuto vztahu dochází, pokud je pozice spotřebitele nějakým způsobem posílena, např. více spotřebitelů chce koupit zboží v takovém objemu, že společnými silami přimějí podnikatele k jednání o ceně. Tento způsob nabývá na oblíbenosti zejména v poslední době a vlivem sociálních sítí. Uživatelé se takto sdružují za účelem získat výhodnější ceny na konkrétní typ zboží, ale také hromadné výhody nebo slevy.

C2C

Kategorie C2C (z angl. consumer to consumer) je vztahem mezi spotřebiteli. Při těchto transakcích prodává jeden spotřebitel zboží druhému spotřebiteli. V dnešní době k tomuto obchodování dochází například prostřednictvím internetových aukcí nebo elektronických inzerátů. V České republice je čím dál více oblíbený aukční portál Aukro.cz a také české verze amerického aukčního portálu ebay.com. [15]



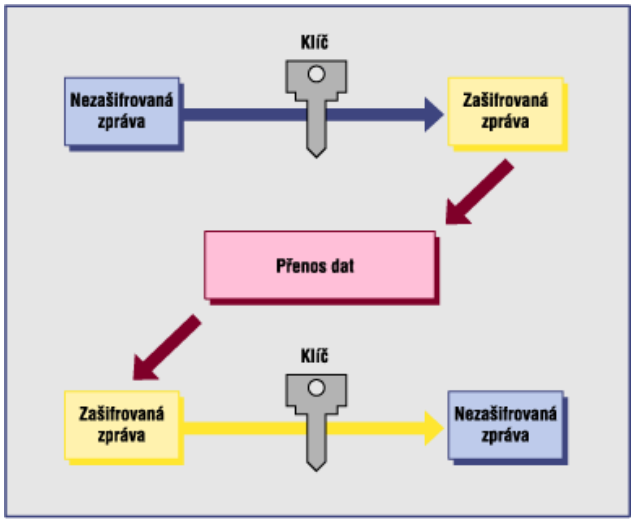
Obrázek 2 Dělení E – business [vlastní]

2.2 Pojmy z oblasti šifrování

Šifrování dat neboli také kryptografie tvoří základní kámen problematiky řešení internetové bezpečnosti. Jde o převedení zprávy určené příjemci pomocí šifrovacího algoritmu a její převod do srozumitelné podoby příjemci v případě, že příjemce zná algoritmus nutný k jeho dešifrování. K tomuto přenosu se využívají dva základní typy šifer a to symetrické a asymetrické.

2.2.1 Symetrické šifrování

Jde o šifry používající stejný šifrovací klíč jak pro zašifrování, tak pro dešifrování. Tato výhoda použití jediného klíče pro všechny úkony se zpracovávanými daty se projevuje i vyšší rychlostí práce počítače při šifrování. Výhoda na jedné straně je však nevýhodou na straně druhé, neboť v případě prolomení šifry jsou odkryta veškerá data. V praxi se tento způsob využívá při zálohování dat. Symetrické šifry dále dělíme na blokové a proudové. [4]



Obrázek 3 Symetrické šifrování [16]

Proudové šifry

Využívají se v případě, kdy je třeba šifrovat pouze několik bitů otevřeného textu a je třeba převedení v co nejkratším čase. Typickým představitelem je algoritmus RC4, který využívá 40 nebo 128 bitový klíč.

Blokové šifry

Blokové šifry zpracovávají nezašifrovanou zprávu po blocích stanovené bitové délky (např. 128 bitů) o stejné velikosti a poté je tento blok zašifrován pomocí algoritmu řízeného šifrovacím klíčem, přičemž proces dešifrování probíhá stejným postupem. Nejčastěji využívané blokové šifry jsou:

DES – základní bloková šifra o délce klíče 56 a 64 bitů

AES – délka klíče 128, 192 a 256 bitů

3DES – Triple - DES využívá DES jako stavební prvek a data jsou třikrát přešifrována. Délka klíče je v tomto případě 168 či 256 bitů.

2.2.2 Asymetrické šifrování

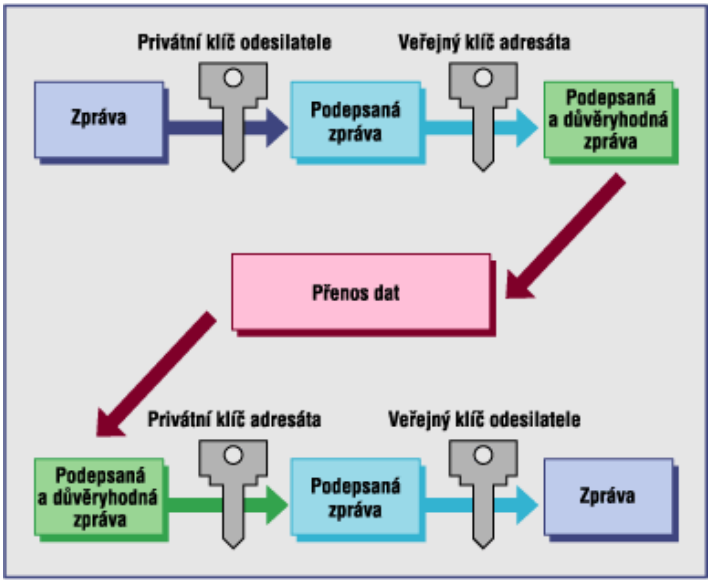
Oproti symetrické kryptografii se využívá dvojice klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných SW produktů (např. SSL), a stává se tak jejich jediným majitelem. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, tzv. privátní

klíč, je s maximální bezpečností ukrýván majitelem, zatímco druhý veřejný klíč je zveřejněn. Nejčastěji se používají algoritmy:

RSA – délka klíče 512 – 4096 bitů. Tento asymetrický kryptosystém se využívá u digitálního podpisu. Jeho bezpečnost je založena na faktorizaci velkých čísel, z nichž každé je součinem dvou velkých prvočísel (100 - 200 místných). Délka klíče se pak použije podle potřeby utajení. [4]

El Gamal – délka klíče 1024 bitů

Defie – Hellman – délka klíče 1024, 2048 3072 bitů



Obrázek 4 Asymetrické šifrování [16]

2.2.3 Hashovací funkce

Hash je algoritmus, který vytváří řetězec, obvykle 128 - bitové hodnoty, který je výsledkem jednosměrné matematické kalkulace (hash algoritmu), jež zabezpečí, že není možné se obráceným postupem dobrat k původní zprávě.

MD5

Velmi často používaná funkce se 128 bitovým výstupem. Generované kódy nejsou unikátní a je pouze malá pravděpodobnost, že dva dokumenty budou mít stejný hash. Výsledek MD5 má 32 znaků a možnost prolomení je tak 2^{32}. Využívá se především v programech, aby zajistila záruku neporušenosti dat. [18]

SHA-1

Je považována za nástupce MD5 a v současnosti je nejpoužívanější. Výsledkem je funkce o maximální délce 160 bitů a délkou 2^{64}. SHA-1 je používána v bezpečnostních aplikacích a protokolech (např. TLS, SSL, PGP). [18]

2.3 Protokoly pro bezpečnou komunikaci

Původní tvůrci protokolu HTTP vytvořili tento protokol jakožto prostředek pro přenos multimediálních dat - grafiky, videa, zvuku atd. Postupem času se však HTTP stal páteří neuvěřitelného množství komerčních aplikací. V oblasti bezpečného přenosu transakcí byl v roce 1994 navržen protokol S - HTTP. Dnes je již méně používán a v současné době je bezkonkurenčně nejrozšířenějším bezpečnostním protokolem SSL 3.0 a jeho následovník TLS. Oba protokoly používají architekturu klient/server. Klasický model protokolu TCP/IP v sobě nezahrnuje žádnou vrstvu, která by se zabývala problematikou bezpečnosti. Vrstva SSL (TLS) je tedy do modelu protokolů TCP/IP vložena mezi aplikační protokol a protokol TCP. Vrstva SSL nezkoumá data, která jsou zasílána aplikační vrstvou, prostě je zabezpečí a předá protokolu TCP. Vrstva SSL je schopna zajistit šifrování, integritu dat a autorizaci dat, nikoliv elektronický podpis. Autorizace dat se provádí na základě kontrolního součtu. Při navazování spojení SSL (TLS) vždy provádí autentizaci serveru. Autentizace klienta je volitelná. Komunikace mezi klientem a serverem je plně duplexní přičemž pro každý směr komunikace používá jiné symetrické šifrovací klíče a jiné „tajemství“ (MAC secret) pro výpočet kontrolního součtu. [2]

2.4 Autentizace

Je předem stanovený proces, při kterém uživatel pomocí stanovených prostředků prokazuje svoji identitu. V podstatě je možné provést tři základní způsoby identifikace přistupující osoby:

- autentizace pomocí znalosti, kterou disponuje daná osoba (PIN, heslo, login)
- autentizace za použití bezpečnostního předmětu (platební karta)
- autentizace pomocí fyzického znaku dané osoby (biometrie)

2.5 Certifikační autorita

Certifikát se používá jako záruka „pravosti zpráv“, které jsou posílány pres veřejnou nezabezpečenou sít. Uživatel, vlastník soukromého klíče, si vyžádá ke konkrétnímu veřejnému klíči od certifikační autority (dále jen CA) certifikát. Na jeho základě daná CA nese odpovědnost za ověření, že daný veřejný klíc patří určitému uživateli. Certifikát je proto platný pouze určitou dobu, přičemž certifikační autorita může jeho platnost zrušit. Aby mohl být certifikáty hromadně a celosvětově využívány, je jeho forma upravena dle celosvětově standardizované normy X. 509.

Digitální certifikáty vydávají veřejné CA (Česká pošta, První certifikační autorita, eIDENTITY, aj.). Organizace si mohou samy vytvářet své vlastní CA jako součást vnitrní struktury veřejného klíče (PKI – Public Key Infrastructure). Pomocí PKI systému lze prověřovat a ověřovat identifikační údaje ostatních organizací, které elektronicky s danou organizací komunikují.

Primární funkcí certifikátů je ověření pravosti jednotlivých uživatelů, kteří se snaží provést autentizaci na dané webové stránce. V našem případě jde o přihlášení do internetového bankovnictví nebo jiného typu platebního systému. [8]

2.6 EDI

EDI je elektronická výměna dat (zpráv) mezi nezávislými subjekty, splňující tyto charakteristiky:

Integritu

- změna zprávy během přenosu bude odhalena
- zpráva byla odeslána konkrétní osobou
- zpráva přišla ve správném pořadí

Autentičnost

- určení osoby, která zprávu odeslala
- neodmítnutí původu zprávy
- neodmítnutí příjmu zprávy

Důvěrnost zprávy

- zajištění obsahu zprávy před nepovolanými osobami

2.6.1 Zprávy

Výměna dat v EDI probíhá pomocí zpráv. Vlastní zprávy, které si subjekty vyměňují mezi sebou navzájem, jsou standardizovány. Mají definovány pravidla syntaxe. V rámci standardu jsou definovány základní prvky (formáty položek), číselníky a typové zprávy (zpráva - INVOIC, objednávka - ORDERS, faktura - PAYORD, platební příkaz apod.)

Při přenosu se zprávy jednoho druhu mohou sdružovat do funkčních skupin a funkční skupiny do tzv. výměny. Výměna je definována jako komunikace mezi partnery prostřednictvím strukturovaného souboru zpráv a služebních segmentů, který začíná záhlavím výměny a končí závěrem výměny. Výměna obsahuje nejméně jednu zprávu. Při jednom spojení se může uskutečnit jedna nebo více výměn. [19]

2.7 Elektronický podpis

Pro ověřování elektronických dat nelze použít ručně psaného podpisu, a proto se využívá jeho elektronická forma. Jde o číslo skládající se v binární podobě o délce 4096 bitů. Jeho prvotní funkcí je ověření pravosti dokumentu a jedná se především o zajištění těchto funkcí:

Autenticity – podpis přesvědčí adresáta, že odesílatel dokument skutečně podepsal. Jde o potvrzení původu dokumentu a totožnosti autora.

Integrity – nezfalšovatelnou zprávy. Vyjadřuje požadavek na zabránění neoprávněné modifikace dat.

Jednorázovosti – podpis lze aplikovat jen jednou a nelze přenést na jiný dokument.

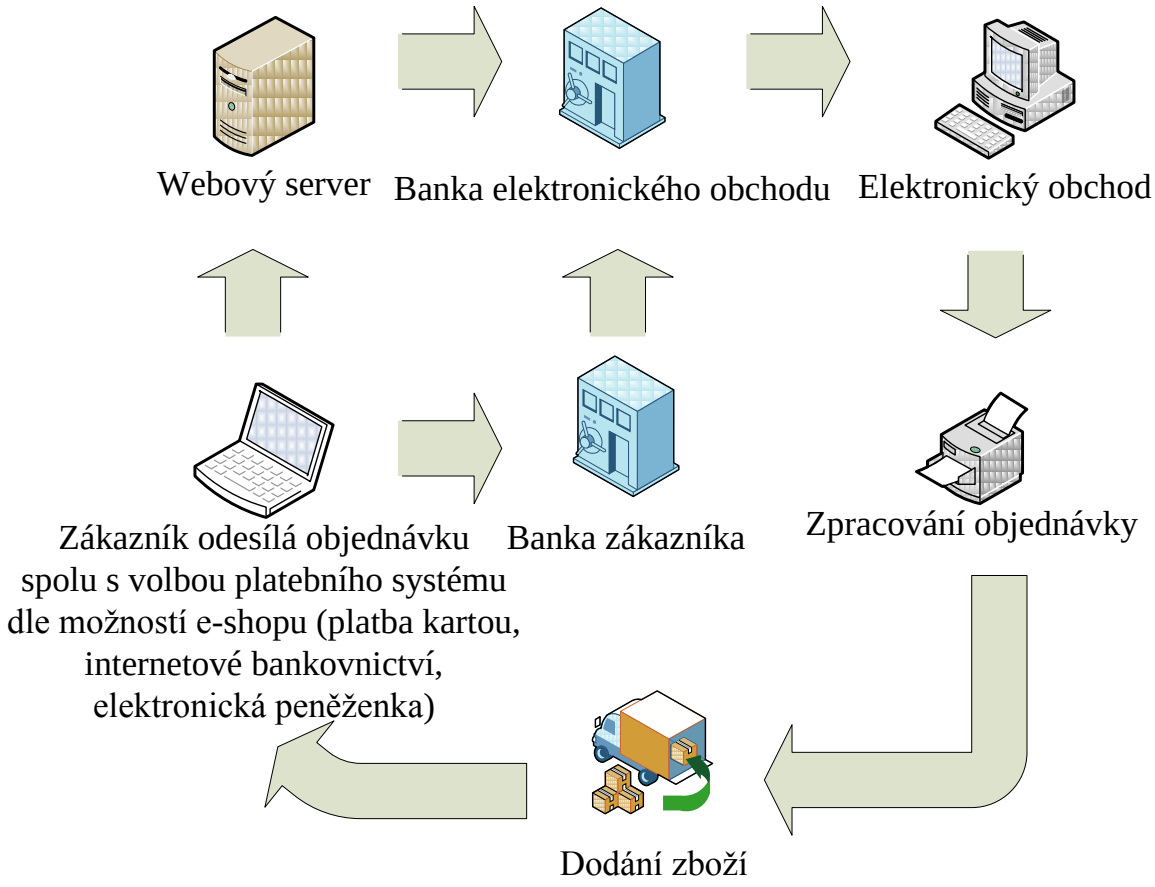
Nepopiratelnosti – odesílatel nemůže popřít, že daný dokument nepodepsal. To vyjadřuje důkaz v právním sporu, a tedy právní závaznost. [8]

Definice dle Zákona o elektronickém podpisu č. 227/2000 Sb. § 2 písmeno a) zní:

„Elektronický podpis jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k podepsané zprávě.“ [48]

3 MOŽNOSTI PLATEBNÍHO STYKU

V této kapitole jsou specifikované možnosti úhrady při platbě v elektronickém obchodu. Zvláštní pozornost je věnována platebním kartám, které figurují jako základní prostředek ke všem níže popsaným systémům. Na obrázku je znázorněn model nákupu v elektronickém obchodě.



Obrázek 5 Nákup v e-shopu [vlastní]

3.1 Platební karty

V současné době tvoří platební karty nepostradatelnou součást každodenního života většiny dospělé populace a jejich používání je naprosto běžné ve většině zemí světa. Nejrozvinutější síť bankomatů a obchodních míst akceptujících platební karty je zejména ve Spojených státech amerických, Kanadě, teprve poté na evropském kontinentě a následně ve velké části Asie, Austrálii a na Novém Zélandě. V České republice došlo k prudkému rozvoji vydávání platebních karet od počátku devadesátých let minulého století. Rychlý počátek vydávání platebních karet po roce 1989 přinesl eliminaci do té doby

nejpoužívanějších platebních prostředků mimo hotovostní peníze - šeků. Platební karty se vyznačují tím, že u nich odlišujeme majitele od držitele - majitelem je vždy vydávající banka a držitelem je osoba, která na smluvním základě využívá platební kartu poskytnutou bankou k přístupu k peněžním prostředkům na účtu. Platební karty můžeme dělit podle následujících hledisek. [5]

3.1.1 Dělení platebních karet

3.1.1.1 Dle způsobu zúčtování transakcí

Debetní karta

je karta pevně svázány s běžným účtem. Platby jsou účtovány neprodleně poté, co banka obdrží potvrzení o jejich provedení. Klient čerpá finanční prostředky uložené na jeho účtu. U nás se jedná o nejpoužívanější druh karet nejčastěji využívaných pro bezhotovostní platby u obchodníka či výběru hotovosti z bankomatu.

Kreditní karta

majitel disponuje určitým kreditním limitem umožňujícím čerpat finanční prostředky mimo peníze uložené na běžném účtu. Kreditní karta se totiž obvykle k žádnému účtu nevztahuje, a slouží tedy jako určitý druh úvěru, který můžeme z karty vyčerpat a následně jej splácet v předem určeném splátkovém kalendáři.

Charge karta

držiteli této karty nejsou peníze z účtu odečteny okamžitě, ale až s odstupem času. Klient provádí úhradu peněz např. dle měsíčního výpisu, který mu zašle vydavatel karty. Za vypůjčenou částku však na rozdíl od kreditní karty neplatí žádný úrok.

Nákupní úvěrová karta

je obdobou kreditní karty a je vydávána nebankovními institucemi. Od svých bankovních se liší hlavně v ceně karty, výši úročení a omezené použitelnosti. Do této skupiny patří např. OK karta, YES karta a Aura karta. [20]

3.1.1.2 Dle způsobu provedení

Elektronická karta

jedná se o platební kartu, díky které lze vybírat z účtu pomocí bankomatu a platit u obchodníků, kteří vlastní elektronický platební terminál. Tyto karty jsou nejčastěji vydávány k účtům zdarma. U nás je tento typ karet nejpoužívanější a do této skupiny řadíme karty VISA Elektron nebo Maestro.

Embosovaná karta

má na svém povrchu plasticky vytlačené údaje o majiteli, číslu karty atd. Proto mohou být použity pro platbu i tam, kde nejsou k dispozici elektronické snímače karet (sprinter). [21]

3.1.1.3 Dle vydavatele

VISA

(Visa International Servise Association) - je nadnárodní společností, která má největší síť elektronických plateb na světě. VISA nabízí širokou nabídku osobních i firemní karet např. VISA Electron, VISA Classic, VISA Gold atd.

MasterCard

(MasterCard Worldwide) – představuje nadnárodní společnost, která nabízí mnohé platební karty, mezi které patří Maestro, MasterCard Electronic, MaterCard Unembossed, MasterCard Gold, MasterCard Platinum, MasterCard Business Card atd.

Dále se můžeme setkat s vydavateli, kteří u nás na trhu platebních karet nezaujímají takové postavení jako společnosti výše uvedené. Patří sem Diners Club (Diners Club International, American Express Company (Amex), či japonská JCB (Japan Credit Bureau).

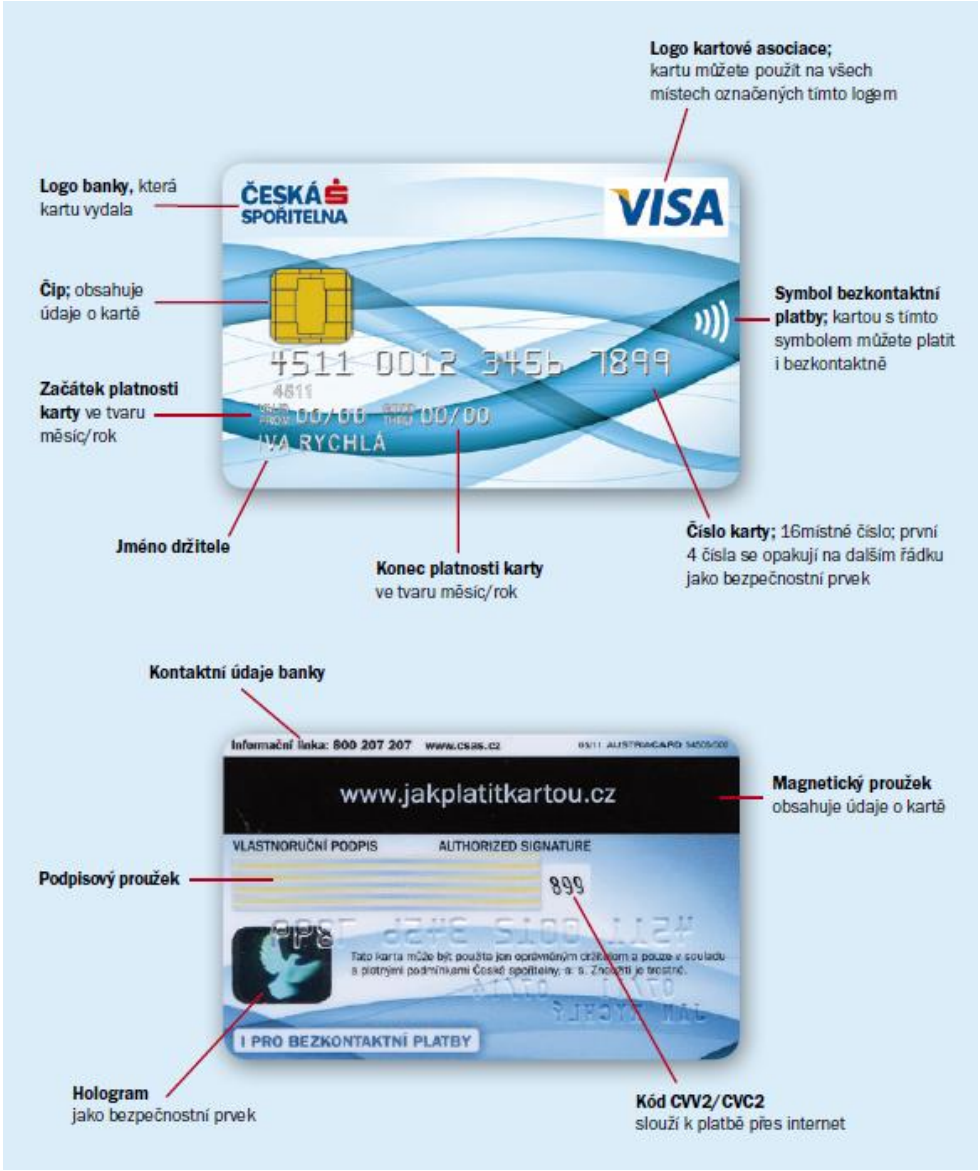
3.1.1.4 Dle použité technologie

Podle použité technologie můžeme platební karty rozdělit na karty s magnetickým pruhem, čipové, hybridní a s displejem. Tyto varianty jsou blíže specifikovány v následující kapitole.

Jednotlivé ochranné prvky platebních karet jsem se rozhodl rozdělit do dvou skupin. První tvoří technická ochrana karty, která zahrnuje rozměry platební karty a další prvky, které

jsou viditelnou součástí karty. Druhou část tvoří elektronická ochrana karty. Zde je znázorněn způsob uložení dat na magnetický proužek, čip nebo za použití RFID technologie.

3.1.2 Technická ochrana platební karty



Obrázek 6 Technická ochrana platební karty [22]

3.1.2.1 Rozměry platební karty

Patří také do skupiny ochranných prvků, protože karta odlišných rozměrů není příslušným snímacím zařízením akceptována. Základním standardem, který určuje rozměry platební karty, je ISO 7810, přičemž délka karty je stanovena na 85,595 mm, šířka na 53,93 mm

a její tloušťka na 0,76 mm. Povolené odchylky se pohybují řádově v setinách milimetrů. Stanoveny jsou i poloměry zakřivení rohů karty, dislokace magnetického proužku, dislokace případně použitého mikročipu a další.

3.1.2.2 PIN

Toto označení vychází z anglického personal identification number (osobní identifikační číslo). Zpravidla se jedná čtyřmístný číselný kód, který se vytváří kombinací čísla karty a generujícím klíčem banky metodou 3DES.

3.1.2.3 Embossing

Jedná se vystouplé písmo, kterým jsou na platební kartě vyraženy karetní informace a informace o jejím držiteli (číslo platební karty a jméno majitele). Pak probíhá platba pomocí tzv. žehličky – imprinteru obtiskujícím údaje z karty na účet. Její využitelnost je mnohem větší a je dokonce možné s ní platit prostřednictvím internetu. S tím také samozřejmě souvisí vyšší riziko zneužití, proto je dražší nejen vedení karty, ale také blokace.

3.1.2.4 Hologram

Hologram zapuštěný do karty je bezpečnostní znak, který je důvěrně známý všem uživatelům platebních karet. Bezpečnost hologramů je primárně založena na tom, že jsou vyráběny pouze několika málo společnostmi na světě, a že nejsou snadno dostupné. Hologramům používaným u čipových karet se také říká „embosované“ hologramy. Vzhledem k tomu, že jsou viditelné pomocí difuzního odrazu denního světla, tak jsou známé i jako „hologramy odrážející bílé světlo“. Oproti tomu běžný přenosový hologram musí být prohlížen za použití koherentního laserového světla. Hologram je nastálo vtmelený do těla karty, takže nemůže být odstraněn, aniž by byl zničen, nebo by byla zničena karta.

3.1.2.5 Číslo karty

Nejčastěji 16místné číslo karty, ve kterém je mj. označení typu karty (první číslice: 4 - VISA, 5 - MasterCard), kód vaší banky a samozřejmě číslo karty. Podrobnosti systému skladby čísla se však u jednotlivých karetních společností liší.

3.1.2.6 CVV/CVC kód

Používá se především při platbách po internetu jako další kontrola, zda ten, kdo platí, má opravdu v ruce kartu a ne jen kopii její přední strany. Nachází se na zadní straně karty v podpisovém proužku.

3.1.2.7 Podpis

Podpis provádí držitel karty při jejím převzetí na vyhrazené místo na zadní straně karty. Podpis slouží jako druhotná metoda ověření. Obchodník může porovnat, jestli se podpis na stvrzence shoduje s podpisem na kartě. V dnešní době se již příliš nepoužívá. [1]

3.1.3 Elektronická ochrana údajů

3.1.3.1 Magnetický proužek

Je umístěn na zadní straně karty. Jsou na něm uloženy údaje o kartě a jejím držiteli, které jsou nutné pro provedení dané platby či výběru z bankomatu. Magnetický proužek neumožňuje tak vysoké zabezpečení uložených dat jako čip, proto na něm není uložen PIN. Magnetický proužek má tři záznamové stopy, které mají specifický účel.

Obrázek 7 Karta s magnetickým pruhem [23]

Stopa 1 - má 79 znaků, které obsahují číslo karty (až 18 číslic) a jméno klienta (až 26 alfanumerických znaků).

Stopa 2 - obsahuje 40 numerických znaků včetně čísla karty (až 19 číslic) a v bankovnictví se používá nejvíce.

Stopa 3 - na rozdíl od 1. a 2. stopy, které jsou určeny pouze pro čtení, může být záznam na 3. stopě přepisován. Třetí stopa se používala u on - line bankomatů. Finanční limit klienta

se snižoval o vybírané částky a po uplynutí stanoveného času se opět navyšoval na původní úroveň. Na této stopě byl zaznamenán parametr, podle kterého bylo možné ověřit správnost kódu PIN. K záznamu potřebných informací sloužilo až 107 numerických znaků (PIN, kód země, měnová jednotka, finanční limit a další). [23]

Příklad záznamu:

1. stopa:

%B4406160384321844^NOVOTNY/ZDENEK.MR^021252116526000000000019100000?;

2. stopa:

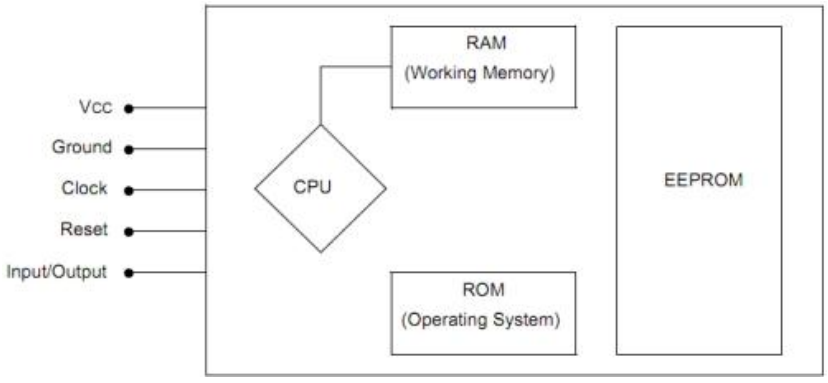
4406160384321844=02125211652619120?+

3. stopa:

014406160384321844=203000020000000030501200571310020000212 2=20316216181471803==1=70000000000000000000?

3.1.3.2 Čipové karty

Jejich součástí mikropočítač, který jednak přebírá funkci nosiče dat a také umožňuje řadu dalších funkcí, především nahrazuje při identifikaci držitele karty jeho podpis zadáním jeho osobního kódu PIN. Číselná kombinace PIN výrazně zvyšuje bezpečnost platby kartou.



Obrázek 8 Čip platební karty [24]

Význam jednotlivých pinů:

Vcc – napájení karty,

RST – reset karty,

CLK – vstup hodinového signálu,

GND – společná zem,

Vpp – vstup programovacího napětí,

I/0 – datový pin pro sériovou datovou komunikaci mezi čipovou kartou a čtecím zařízením,

RFU – vyhrazeny pro budoucí použití. V současnosti využívané pro USB rozhraní.

Ačkoliv norma ISO standart 7816 - 2, která specifikuje vlastnosti čipové karty, definuje osm pinů, v praxi se jich využívá jen šest. Mimo rozhraní, které slouží pro komunikaci se čtecím zařízením, obsahuje karta také řídící jednotku (CPU), která provádí kontrolu dat včetně kryptografických operací a paměti. Paměť RAM slouží pro uložení dočasných výsledků při výpočtech a po vyjmutí karty ze čtečky ztratí svůj obsah. Paměť ROM je nepřepisovatelná a obsahuje operační systém karty. Třetím typem paměti, kterým čipová karta disponuje, je paměť EEPROM, která je mazatelná a programovatelná a data na ní neztrácí ani po odpojení karty ze čtečky. Je nejdůležitější paměťovou oblastí čipové karty zejména proto, že obsahuje citlivé informace, a proto je strukturování těchto dat věnována velká pozornost. [24]

3.1.3.3 Hybridní karty

Obsahují jak magnetický proužek, tak i čip. Dnes již všechny banky vydávají pouze tento typ platebních karet, který odpovídá standardu EMV (vychází z normy ISO 7816). Tato zkratka je složena z počátečních názvů asociací Europay, MasterCard a Visa, které stály u zrodu myšlenky čipové platební karty a definovaly standardy toho, jak má taková platební karta fungovat.

3.1.3.4 Platební karty se zabudovaným displejem

Představuje novou generaci platebních karet a první interaktivní kartu na trhu. V podstatě funguje jako jakákoliv jiná platební karta, ovšem navíc je vybavena malým displejem a tlačítkem. Držitel karty si může na displeji prohlížet různé číselné a textové informace, jako například autentizační kód pro internetové platby, zůstatek na účtu a limit výběru. Karta může obsahovat i numerickou klávesnici. Tato karta je tedy opatřena dalším bezpečnostním prvkem, neboť před manipulací s kartou je třeba zadat PIN.

Obrázek 9 Platební karta se zabudovaným displejem a klávesnicí [25]

3.1.3.5 Bezkontaktní karty

Tento způsob realizace platby je u nás novinkou. Na konci loňského roku jej jako první banka u nás zavedla Česká spořitelna. Jedná se o metodu využívající vlastností rádiového přenosu na krátkou vzdálenost. Jedná se o tzv. NFC (Near Field Communication) bezdrátovou komunikaci, která je založena technologii RFID (Radio Frequency Identification). Čip, který je součástí karty využívá elektromagnetické pole vysílače. Pokud se karta objeví v tomto poli (max. do 10 cm), využije čip energii k nabití napájecího kondenzátoru a následně k výměně dat. Výhodou je rychlost platby, možnost úhrady částky bez použití PIN kódu (do 500 Kč) a tím, že držitel má kartu neustále u sebe. [25]

3.1.4 Prostředky k realizaci transakcí

3.1.4.1 Imprinter

Mechanické zařízení, které umožňuje akceptovat embosované platební karty a pracuje na principu otisku údajů karty a údajů na štítku obchodníka na speciální chemický papír. Využívá se v místech, kde z různých důvodů nelze mít platební terminál, nebo se využívá jako nouzová záloha při poruše platebního terminálu. V případě použití imprinteru není částka transakce odečtena z účtu zákazníka okamžitě (jako u elektronických platebních terminálů), ale její zúčtování trvá přibližně jeden týden. S imprinterem se často můžete setkat také pod ustáleným názvem „žehlička“. [26]

Obrázek 10 Imprinter upraveno dle [26]

3.1.4.2 Bankomat

Bankomat je samoobslužné výplatní zařízení, které vydává držitelům platebních karet bankovky. Obsluhuje se pomocí platební karty, zasouvané do speciální čtečky. Po zadání PIN (čtyřmístného číselného kódu) a požadované částky jsou bankovky, do té doby uložené z trezoru bankomatu, vydány. Současné bankomaty jsou on-line napojeny na autorizační systém, který ověřuje pravost informací uložených na platební kartě, správnost PIN a dostatečný zůstatek hotovosti na účtu klienta. Kromě standardních funkcí umožňuje bankomat provádět některé nepeněžní funkce, jako jsou jednoduché platební příkazy, výpisy z účtu, změny PIN a vkládání peněz jako depozit. To se může provádět i tzv. inteligentní metodou, kdy jsou bankovky automaticky rozpoznány přímo v bankomatu a jsou klientovi připsány na účet.

Bankomaty můžeme rozdělit na dva základní typy – na vnitřní, které najdete třeba na pobočkách bank nebo v obchodních centrech, a venkovní, které jsou na ulici. Oba typy mohou být buď zabudované ve zdi, nebo volně stojící. Přístroje umístěné v interiérech snesou teplotu do + 5 stupňů Celsia, ty venkovní odolávají až dvacetistupňovým mrazům.

Obrazovka

zprostředkovává komunikaci mezi zákazníkem a bankomatem. V okamžiku, kdy do něj vložíte kartu, se zobrazí menu s nabídkou dostupných služeb.

Klávesnice

slouží k zadávání všech číselných údajů – od zadání PIN až po čísla mobilů nebo faktur, ale také pro potvrzení transakcí.

Počítač

je umístněn za obrazovkou. Zaznamenává všechny transakce a současně je propojen s dalšími systémy v bance. Provozovatel tak může přímo z kanceláře kontrolovat, jestli je v bankomatu ještě dost peněz, nebo je třeba jej doplnit.

Bezpečnostní kamera

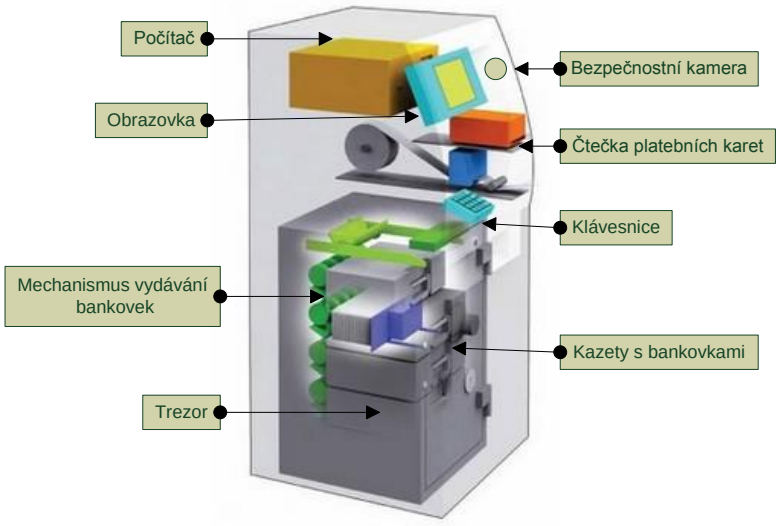
spouští se v okamžiku vložení karty do bankomatu. Je to ochrana pro případ, že by z bankomatu chtěl peníze vybírat někdo na falešnou kartu.

Trezor

tvoří celou spodní část bankomatu. V něm jsou umístěny kazety s penězi a také šuplík na poškozené bankovky.

Kazety v bankomatu

mohou být dvě, ale třeba i čtyři. V každé z nich jsou bankovky jiné hodnoty, proto některé bankomaty například neumějí vydat 1800 korun, ale jen 1500 korun. Poškozené bankovky, které přístroj nedokáže z kazety dopravit do podavače peněz, se ukládají ve speciálním šuplíku. [27]



Obrázek 11 Bankomat [27]

3.1.4.3 Platební terminál

Někdy je označován jako POS terminál (z angličtiny Point of Sale) a slouží k provádění bezhotovostních bankovních transakcí platební kartou. Důvodem k jejich zavedení bylo snížení administrativní činnosti obchodníků. Podle typu a technologie umí akceptovat všechny typy karet.

Každý platební terminál se skládá z několika částí. Jsou jimi čtečky karet (magnetického proužku, čipu a v nejlepším případě obou), displej zobrazující požadované a zadané informace, klávesnice pro ovládání terminálu, tiskárnu a další zařízení. Komunikace probíhá většinou pomocí protokolu TCP/IP (UTP kabelem). V případě použití bezdrátového platebního terminálu, zařízení přibývá. Jde-li o GPRS komunikaci, musí terminál obsahovat SIM kartu a technické vybavení umožňující datovou komunikaci. Další komunikační cesty metody jsou WIFI, Bluetooth, či telefonní kabel. [28]

Obrázek 12 Platební terminál [28]

3.1.4.4 Platbomat

Zařízení se do jisté míry podobá bankomatům, ale neobsahuje žádnou hotovost a umožňuje klientovi zadat rychle a levně příkazy k úhradě. Pracuje tak, že klient vloží do platbomatu platební kartu, zadá příslušný PIN k této kartě. Platba se následně pomocí tohoto kódu autorizuje (= podepíše). Platbomat je opatřen čtečkou čárových kódů, takže v případě, že je příkaz k úhradě opatřen čárovým kódem, dochází ke zrychlení úhrady požadované transakce. [29]

3.1.4.5 Platba kartou prostřednictvím internetu 3D secure

Pro využití karty pro platby na internetu lze využít jak kartu kreditní, tak debetní. Podmínkou je aktivace služby, neboť banky standardně vydávají karty bez možnosti využití této funkce. Platba probíhá pomocí rozhranní internetového bankovnictví, kdy po přihlášení a vybrání příslušného menu je zákazník vyzván k zadání:

- čísla platební karty
- datum platnosti (expirace) karty, tedy údajů o platnosti karty
- CVC2 kódu
- dalšího údaje k ověření totožnosti např. tel. číslo, na které je doručen SMS klíč k potvrzení transakce.

Obrázek 13 Platba kartou prostřednictvím internetu [30]

Pro zvýšení bezpečnosti zavedla společnost Visa platební systém 3D secure, který pod názvem SecureCode adaptovala i společnost Mastercard. Bezpečnost zajišťuje tak, že údaje na své kartě neposkytuje nakupující obchodníkovi, ale jako prostředník mezi těmito účastníky obchodu stojí banka. Přenos informací o kartě probíhá pomocí HTTPS protokolu, který údaje klienta zakóduje tak, že si nikdo kromě banky údaje nemůže přečíst. Zákazník mající kartu vydanou pod systémem 3D - secure navíc může rozšířit proces autentizace při placení o další údaje, které zná pouze on a nikdo jiný jeho kartou nezaplatí, i kdyby si zkopíroval obvyklé údaje kreditní karty (číslo, datum expirace, kontrolní číslo). Zákazník platící tímto typem karty je pak vždy vyzván k zadání dodatečných údajů, které si nastavil. Teprve po zadání odpovídajících údajů je transakce provedena. [30]

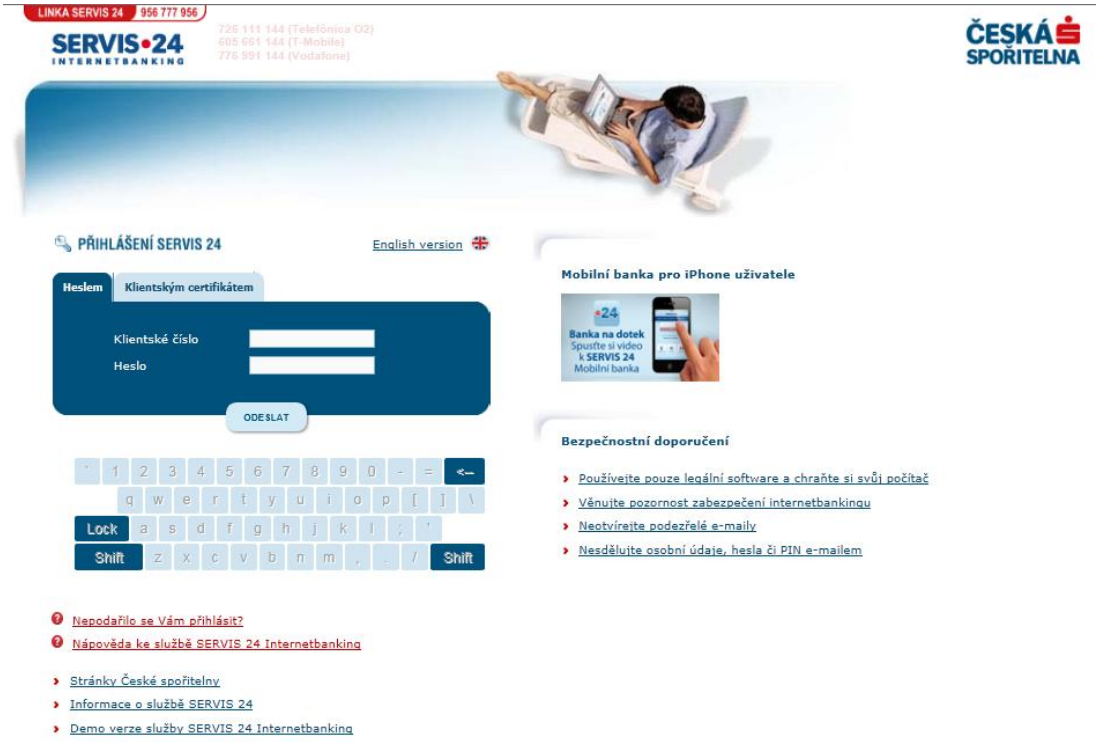
Obrázek 14 Logo 3D secure [30]

3.2 Internetové bankovnictví

Internetové bankovnictví, jehož synonyma jsou též internetbanking či přímé bankovnictví, je nečastěji používanou formou elektronického bankovnictví. Do forem elektronického bankovnictví dále řadíme:

- homebanking
- GSM banking
- phonebanking
- WAP banking
- TV banking

Internetové bankovnictví vnáší určitou kvalitu a komfort pro komunikaci mezi klientem a bankou. Ten získává informace o svém účtu bez časového a prostorového omezení v prostředí internetového prohlížeče z kteréhokoliv místa na světě. Podmínkou je pouze podmínka dostupnosti internetového připojení. Klient, který žádá tuto službu od své banky, získá sadu identifikačních údajů zpřístupňující dané operace přes webové rozhraní dané banky. Po otevření internetových stránek banky je pak vyzván k zadání údajů k identifikaci (zpravidla uživatelské jméno či klientské číslo a heslo) má pak klient možnost v reálném čase uskutečňovat operace se svým účtem v závislosti na individuálních podmínkách jednotlivých bank. [10]



Obrázek 15 Prostředí internetového bankovnictví [29]

Banky nabízejí různé úrovně zabezpečení a liší se též jejich postoj k bezpečnějším, ale nákladnějším řešením. Některé nabízejí vyšší úroveň zabezpečení jako standard, jiné si ji nechají dobře zaplatit. Při výběru banky, u níž chce klient využívat i internetové bankovnictví, by měl způsob zabezpečení hrát důležitou roli.

Důležitá je též otázka odpovědnosti banky za případnou škodu. Odpovědnost při zneužití je sice právně postavena na klienta, banky se však vzhledem k obavám z negativní reklamy často přiklánějí k dohodě a škodu uhradí. Tím, kdo může bezpečnost svým přístupem nejvíce ovlivnit, ale stále zůstává především klient.

UŽIVATELSKÉ JMÉNO A HESLO

Uživatelské jméno a heslo je nejjednodušším, ale zároveň nejméně bezpečným způsobem zabezpečení internetového bankovnictví. Banky od tohoto způsobu upouštějí, některé umožňují v tomto případě pouze pasivní operace (tj. zjistit stav a pohyby na účtu, nikoli však zadávat platební příkazy). Zabezpečení je náchylné nejen na vyzrazení hesla a uživatelského jména, ale také na „odposlech“ klávesnice.

SMS KÓD

Kód zasílaný prostřednictvím SMS zpráv je nejoblíbenějším způsobem zabezpečení. Využívají se dvě možnosti - klasická SMS zpráva, která je méně bezpečná a šifrovaná SMS s využitím tzv. SIM Toolkitu. V tomto případě je třeba dbát na bezpečnost mobilního telefonu. Kritickým bodem je též změna čísla telefonu, na které se SMS zprávy zasílají. Aby byl systém bezpečný, je třeba mít možnost změnit číslo telefonu pouze na pobočce po ověření totožnosti klienta.

CERTIFIKÁT

Podpisový certifikát uložený v souboru slouží k ověření identity klienta. Jeho nevýhodou je možnost zkopírování certifikátu a jeho následného zneužití. Certifikát by měl být uložen na přenosném médiu, které uživatel připojuje k počítači při využívání internetového bankovnictví. Zásadní chybou je uložení certifikátu na pevném disku v počítači, nebo dokonce na internetu. Bezpečnější jsou certifikáty na čipové kartě či iKey tokenu.

CERTIFIKÁT NA ČIPOVÉ KARTĚ

Certifikát na čipové kartě či iKey tokenu má tu výhodu, že ho nelze zkopírovat. Případný útočník by musel získat kartu i hesla, která ji chrání.

PIN KALKULÁTOR

PIN kalkulátor je generátor hesel pro vstup a pro ověření transakcí. Klient pro ověření pokynu musí zadat atributy transakce i do kalkulátoru a na jejich základě je mu vygenerován PIN. Jedná se o jeden z nejbezpečnějších způsobů ověření.

TAN

TAN kódy jsou jednorázové kódy zasílané zpravidla poštou, které slouží k ověření klienta i potvrzení transakce. Klientovi je vydána vždy sada hesel (zpravidla 50 až 100), po jejichž spotřebování obdrží nová. Tento kód tvoří unikátní, zpravidla 6místné číslo, kterým se potvrdí bankovní operace. Po potvrzení je TAN kód neplatný a je potřeba příště použít jiný. Tento systém je poměrně bezpečný, nebezpečím je ale případná ztráta kódů.

USB TOKEN

Jako tokeny jsou označována hardwarová zařízení, která obsahují určité bezpečnostní údaje. Bez připojeného tokenu tedy není možná autorizace uživatele. Většinou se jedná o tokeny připojitelné k USB a slouží tedy jako klíč, který je třeba mít u sebe vždy, když

chceme operovat s bankovním účtem. Výhody a nevýhody mají také mnoho společného s klíči v realitě: bez klíče se nemůže autorizovat oprávněná ani neoprávněná osoba. Naopak pokud získá útočník můj klíč a jednalo by se o jediný způsob zabezpečení, získal by tím přístup i k mému účtu. V některých případech by dokonce stačilo pouze informace obsažené v tokenu zkopírovat na jiné médium. V současné době se ovšem tato metody vždy kombinuje ještě s dalším prvkem zabezpečení. V dřívějších dobách byl také občas problém s možností připojit svůj token, protože některé starší typy počítačů nepodporovaly USB konektory. Tento problém v dnešní době už naštěstí není potřebné řešit.

ČASOVĚ ZÁVISLÝ TOKEN

Dalším bezpečnostním prvkem pro přístup do internetového bankovnictví je časově závislý token. Ten generuje v určitém časovém okamžiku (zpravidla 1 minuta) nový jednorázový autorizační klíč. Pro přístup je pak vyžadováno přístupové heslo, PIN a vygenerovaný token kód. [31]

3.2.1 Internetové bankovnictví – smartphone, tablet

V poslední době se stále více hovoří o smartbankingu, tedy speciálních aplikacích, které jsou určené pro mobilní telefony a umožňují ovládat účty v bance či pojišťovně. Stále více telefonů s operačními systémy (nejčastěji Android, iOS, Windows7 či některým další) a disponují přístupem na internet, což je služba, která se vzhledem ke snižujícím se cenám za připojení a zvyšujícím se požadavkům na přístup k informacím kdykoli a odkudkoli těší poměrně velké oblibě. Ostatně když se podíváme na datové balíčky nabízené jednotlivými operátory, tak je možné konstatovat, že jde o oblast, kde je konkurence snad možná největší. V tomto kontextu je pochopitelné, že uživatelé vyžadují, aby mohli ke svým účtům přistupovat z mobilních zařízení. V zásadě nemusí jít jen o obyčejné získávání informací o aktuálním stavu peněz na účtu, ale také o realizaci plateb, změnu limitů nebo celkovou komunikaci s bankou. Samozřejmě by neměl chybět přístup k aktivaci služeb jako je pojištění, blokace karty či žádosti o zřízení nové karty. Dobře pojatý smartbanking není jen o pohodlném a rychlém přístupu k informacím, ale také představuje velice důležitý pilíř bezpečnostní, například onu možnost pružně měnit limity pro výběr či platbu kartou, realizovat pokročilé autorizace plateb nebo rychle zablokovat zcizenou kartu. Velice zajímavou kategorií služeb jsou pak ty, které s bankovnictvím přímo nesouvisí, ale uživateli mohou přijít vhod jako dobrý zdroj informací – může jít o spojení

s GPS a poskytnutí informací o nejbližším bankomatu, pobočce nebo dalších informací. Na obrázku je ukázka přihlášení a menu smartbankingu UniCredit Bank.

Obrázek 16 Smartbanking Unicredit Bank [32]

Ke stažení a přihlášení jsou třeba 2 SMS s linkem pro stažení aplikace a s aktivačním kódem. Po stažení aplikace proběhne první přihlášení, při kterém je uživatel vyzván k zadání aktivačního kódu, který obdržel prostřednictvím SMS. Při prvním přihlášení si zvolí PIN a ten si zapamatuje, protože jej bude nadále používat pro přihlašování do svého mobilního bankovnictví. Jako nepřihlášený klient můžete prohlížet mapu bankomatů a mapu poboček bank, případně volat na call centrum, jehož číslo vidíte v přihlašovacím okně. [32]

3.3 Platební systémy jako elektronické peněženky

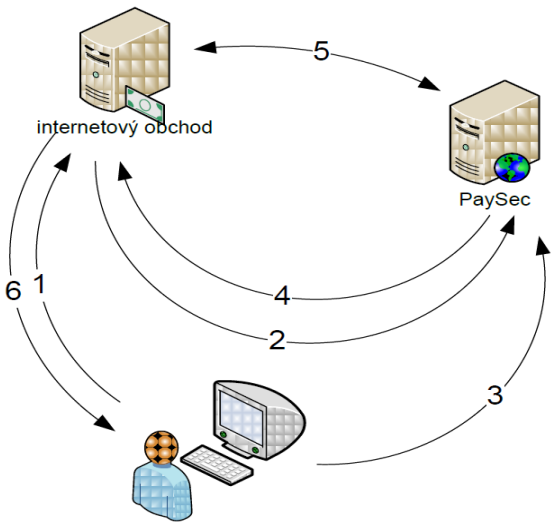
Elektronické peněženky jsou určeny pro všechny druhy transakcí v prostředí internetu a fungují podobně jako bankovní účet, ovšem jde o on-line elektronické platební systémy a platební transakce jsou tedy neporovnatelně rychlejší a obvykle i výrazně levnější. Jako nejznámější elektronické peněženky, z nichž všechny jsou k dispozici i v české lokalizaci, je možné uvést celosvětově známý PayPal, dále pak Moneybookers, GoPay, PayPay či česká PaySec od ČSOB a mPeníze od mBank. Pro fungování elektronických peněženek v České republice byl zcela přelomový rok 2002, který přinesl platnost nového zákona č. 124/2002 Sb., jež stanovil, že platební systémy a tedy i elektronické peněženky smí provozovat v České republice pouze držitelé bankovní licence, což se poté stalo důvodem zániku některých elektronických peněženek u nás. Na elektronickou peněženku je možno

převést finanční prostředky z jiné elektronické peněženky, dále převodem peněz z bankovního účtu (a to na stanovený bankovní účet pod variabilním symbolem identifikující konkrétní elektronickou peněženku), či platební kartou přes platební bránu. Peníze z elektronické peněženky je potom možno odeslat na jinou elektronickou peněženku či bankovní účet. Z účtu elektronické peněženky lze platit na platební bráně přesměrované při objednávce přímo ze stránek internetových obchodů, dále je umožněno účet elektronické peněženky ovládat přes webové rozhraní služby či u některých poskytovatelů elektronických peněženek (např. PayPal či PayPay) i pomocí příkazů v SMS zprávách, nebo pomocí e-mailu. Některé elektronické peněženky nabízejí dokonce možnost napojení na bankovní účet zákazníka a strhávání požadované částky přímo z jeho bankovního účtu. Příkladem budiž elektronická peněženka PayPal, která umožňuje napojit účet elektronické peněženky na platební kartu zákazníka a při platbě částku strhnout z jeho platební karty, resp. bankovního účtu. [33]

3.3.1 PaySec

Systém PaySec je někdy nazýván českou verzí PayPal. Jedná se o projekt ČSOB ve spolupráci s Poštovní spořitelnou. Systém neodečítá peníze za platby přímo účtu, který má uživatel zřízený v bance ale nejdříve musí mít zřízený konto PaySec. Pro placení je pak nutné konto nabít libovolnou částkou. Způsoby pro nabití konta PaySec jsou dva. Buď může jít o klasický převod z běžného účtu, nebo s pomocí platební karty přes službu PayMuzo. Z toho vyplývá, že není nutné, aby uživatel disponoval účtem banky ČSOB nebo Poštovní spořitelny. Na obrázku níže je zobrazen průběh úhrady prostřednictvím platební brány PaySec. [34]

Průběh platby PaySec



Obrázek 17 Průběh platby PaySec [34]

1. Zákazník v internetovém obchodě vybere zboží a zvolí platbu prostřednictvím platební brány PaySec.
2. Internetový obchod přesměruje internetový prohlížeč zákazníka na platební bránu (rozcestník platebních metod) a předá jí informace o požadované platbě. Přesměrování musí provedeno tak, aby se rozcestník platebních metod PaySec zobrazil přes celé okno prohlížeče a v URL bylo uvedeno URL platební brány PaySec.
3. Zákazník si na platební bráně vybere platební metodu PaySec. Zákazník bude přesměrován na přihlášení do svého PaySec konta. Po zadání přihlašovacího jména a hesla do systému PaySec potvrdí transakci. V případě transakce vyšší než limit, který si zákazník nastavil, ještě autorizuje transakci pomocí SMS. Peníze jsou převedeny na konto obchodníka.
4. Internetový prohlížeč uživatele je přesměrován zpět na adresu, která byla předána platební bráně jako jeden z parametrů. Platební brána zašle zpět identifikaci provedené platby (nebo informaci o zamítnutí platby zákazníkem).
5. Pokud bylo vráceno číslo provedené platby, internetový obchod si prostřednictvím webové služby Verify Transaction Is Paid (ověří, že byla transakce skutečně provedena. Tento krok je nezbytný k bezpečnému ověření skutečného stavu

provedení transakce. Ověření transakce musí být provedeno ihned po zavolání návratového URL e-shopu a to tak rychle, aby e-shop mohl na stránce, kterou klientovi zobrazí po jeho návratu z platební brány PaySec mohl rovnou zobrazit odpověď, kterou získal pomocí tohoto ověření transakce. Typicky během maximálně jednotek sekund.

6. Zákazníkovi je zobrazena informace o úspěšném nebo neúspěšném provedení transakce a zaplacené zboží (služba, obsah) je předáno k odeslání (stažení a podobně). [34]

Poplatky za služby

Tabulka 1 Poplatky za služby PaySec [34]

Typ platby	Kolik stojí
Vedení Konta PaySec	Zdarma
Platba na jiné Konto PaySec	Zdarma
Platba za nákup	Zdarma
Přijetí platby od obchodníka	Zdarma
Odeslání peněz Platbou na požádání	Zdarma
Autorizace platby pomocí SMS	Zdarma
Přijetí peněz pomocí Platby na požádání	Zdarma
Přijetí platby prostřednictvím Darovacího Platebního tlačítka	1 Kč Příjemce obdrží částku sníženou o poplatek.
Nabití převodem z běžného účtu (platebním příkazem)	Zdarma
Nabití automatickým dobitím z běžného účtu (inkasem)	1 Kč Poplatek je odečten ve chvíli vygenerování inkasního požadavku. V případě neprovedeného dobití se poplatek nevrací.
Nabití platební kartou	2 % z nabíjené částky
Vybití na běžný účet v ČSOB/Poštovní spořitelně	Zdarma
Vybití na běžný účet v jiné bance	2 Kč
Připsání PaySec Bonusu	Zdarma
Identifikace	Zdarma

3.3.2 PayPal

Systém PayPal je elektronický platební prostředek. Účet v systému si lze představit jako běžný bankovní účet, který se dá ovšem přímo napojit na miliony internetových obchodů

po celém světě a přesun peněz z účtu na účet probíhá okamžitě. Dá se říci, že na internetu mají všichni stejnou banku – PayPal. Systém je ideální pro nákup a prodej zboží za malé a střední částky, nejčastěji bývá spojován s internetovou aukční síní eBay, kde funguje jako hlavní platební prostředek pro desetitisíce transakcí denně. Na PayPal účet lze přesunout peníze nejlépe platební kartou. Tím pádem PayPal může fungovat jako brána pro příjem platebních karet – částku, která se strhne zákazníkovi z účtu, obchodník okamžitě vidí na svém PayPal účtu. PayPal přijímá všechny hojně používané druhy platebních karet. Následně je možné si peníze nechat poslat na bankovní účet běžným bankovním převodem. Výhodou použití PayPalu pro prodej na internetu je instantní funkčnost – obchodník může během hodin zprovoznit přijímání platebních karet. A přitom je možné kompletně vynechat jednání s bankami či jinými bránami pro jejich přijímání. [35]

Typy účtů

PayPal nabízí tři typy účtů. Jsou jimi Personal Account (osobní účet), který je zdarma, ale neumožňuje příjem plateb uskutečněných pomocí kreditních či debetních karet. Dále Premier Account, který již není zdarma, ale umožňuje přijímání všech způsobů plateb. Posledním typem účtu je Business Account, který je vhodný pro on-line obchodování v rámci společnosti a který také umožňuje příjímání všech způsobů plateb.

Personal Account

Jedná se o osobní účet, který je vhodný například pro posílání plateb, placení za zboží na eBay nebo pro on-line předplatné. Jak již bylo řečeno, neumožňuje ovšem příjímání plateb uskutečněných platebními kartami. Na druhou stranu se však neplatí za odeslané ani přijaté platby. Účet též umožňuje využívání služeb programu „Ochrany kupujícího“ (PayPal Buyer Protection), což je program, kde PayPal nabízí pomoc kupujícím, kteří se cítí prodávajícím poškozeni – PayPal se účastní vyjednávání a pomáhá problém řešit.

Premier Account

Umožňuje jak posílání, tak i přijímání plateb na vlastní jméno - tedy na jméno fyzické osoby (ne organizace). Tento typ účtu umožňuje již e-commerce na vlastních Internetových stránkách a to pomocí nákupního košíku PayPal. K tomuto typu účtu se již vztahuje tzv. „Ochrana prodávajícího“ (Seller Protection), což je program, který prodávajícímu kompenzuje ztráty v případě, že kupující změní svůj úmysl a žádá své peníze zpět – specifické problémy spojené s programem ochrany kupujícího. K dispozici je také

možnost integrace s Back-End aplikacemi, která umožní potvrzení transakce v reálném čase pomocí komunikace server-server.

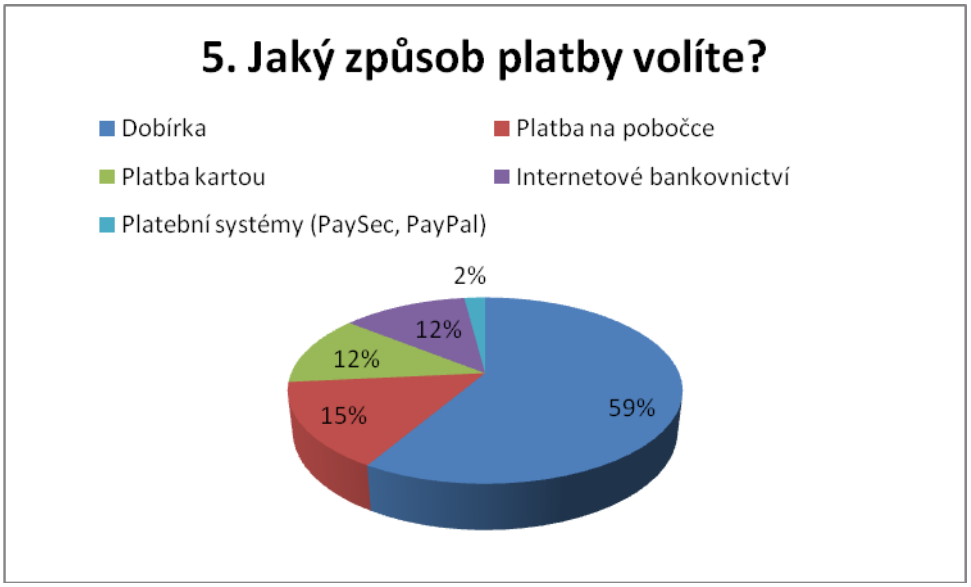
Business Account

Jedná se již o účet vhodný pro on-line obchodování na vyšší úrovni. Nabízí vše jako Premier Account, ale má navíc další výhody, mezi něž kromě jiných patří, že jméno organizace se objevuje na výpisech platebních karet zákazníků. Také se lze k jednomu PayPal účtu přihlašovat pod několika uživatelskými jmény, z nichž každé má jinou úroveň přístupu. [37]

3.4 Klasické platební systémy

Ačkoliv by se mohlo zdát, že tento způsob plateb je v ČR na ústupu, stále udržují majoritní podíl. KPS jsou používány zejména v obchodním modelu B2B. Mezi nejtypičtější zástupce KPS řadíme dobírkovou platbu. Zákazník si jí volí zejména proto, že má jistotu, že mu bude zboží skutečně odesláno. Pro obchodníka je dobírka poměrně nákladná a pracná záležitost. Částka, kterou si Česká Pošta účtuje za dobírkovou platbu je 14 Kč. Tím se stává jedním z nejdražších používaných platebních systémů. Také časová náročnost je vysoká. Musí být vystaven podací list a složenka zasílaná společně se zbožím. Vysoké procento má dobírka díky přirozené nedůvěře českých zákazníků platit za zboží předem. Zajímavým jevem je fakt, že při druhém nákupu na stejném obchodě se zákazník už nebojí využít jeden z nabízených elektronických platebních systémů, protože za předpokladu korektního přístupu, si obchodník už získává jeho důvěru. Mezi další KPS patří: [38]

- platba hotově
- platba při převzetí zboží
- dobírkou
- platba poštovní poukázkou



Obrázek 18 Jakým způsobem platíte v internetovém obchodě [vlastní]

4 LEGISLATIVA

Právní úprava elektronického obchodování je problematická z pohledu orientace, neboť svým rozsahem zasahuje do mnoha zákonů a právních předpisů. V současné době není upraven žádnou právní normou, která by jednoznačně stanovila pravidla v oblasti elektronického obchodování.

Jediným dokumentem týkající se elektronického obchodu je Bílá kniha o elektronickém obchodu. Cílem dokumentu je popsat, jak je možné odstranit identifikovatelné legislativní bariéry rozvoje elektronického obchodu, a specifikovat postupy, kterými lze zajistit jeho hladké a bezpečné fungování.

Problematika nákupu v internetových obchodech je upravena především občanským zákoníkem (zákon č. 40/1964 Sb. ve znění pozdějších předpisů) a obchodním zákoníkem (zákon č. 513/1991 Sb. ve znění pozdějších předpisů). Pro internetový obchod je důležitá zejména úprava obchodování vyplývající z Občanského zákoníku, která stanoví speciální podmínky pro tzv. nákup „na dálku“ (tj. nákup prostřednictvím zásilkového nebo internetového obchodu). [49, 50]

Zákazník elektronického obchodu je chráněn zákonem č. 101/2000 Sb., o ochraně osobních údajů. „*Pro účely tohoto zákona se rozumí osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*.“ *[51]*

Dalším právním předpisem je Zákon č. 227/2000 Sb., O elektronickém podpisu, v platném znění, který definuje zaručený elektronický podpis jako údaje

- jednoznačně spojené s podepisující osobou
- umožňující identifikaci podepisující osoby
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat [48]

Zákon č. 124/2002 Sb., O platebním styku, který definuje provádění převodů peněžních prostředků, vydávání a užívání elektronických platebních prostředků, vznik a provozování platebních systémů. [52]

Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů. Zákon reguluje nevyžádanou elektronickou inzerci, spam, a povoluje zasílat obchodní sdělení pouze podle takzvaného systému opt-in, tedy pouze s výslovným souhlasem adresáta. Nevyžádaná obchodní sdělení návrh zákona zakazuje. Smyslem této úpravy je posílit ochranu soukromí a zabránit tomu, aby příjemci zpráv měli výdaje spojené s přijímáním spamu. Za zasílání nevyžádaných obchodních sdělení, spamu, stanovuje zákon sankci ve výši až 10 000 000 Kč ukládanou Úřadem pro ochranu osobních údajů. [53]

Zákon 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů. Upravuje především povinnosti prodávajících ve vztahu ke spotřebitelům. Jde o obecný zákon vztahující se na veškeré výrobky, vedle něj existují ještě zvláštní předpisy pro vybrané druhy výrobků. Nejdůležitější paragrafy (§3 - §20) se týkají povinností prodejce při prodeji výrobků a poskytování služeb (např. zásada poctivosti prodeje a zákaz nekalých a klamavých praktik). Jeho obsahem jsou předpisy o reklamacích, jejich lhůtách a podmínkách. [54]

II. PRAKTICKÁ ČÁST

5 DOTAZNÍKOVÝ VÝZKUM

Být držitelem platební karty nebo majitelem běžného účtu přináší bezesporu mnoho výhod. Technické řešení ze strany bankovních institucí lze považovat za poměrně dobře zpracované a tak se pachatelé trestné činnosti spjaté elektronickými finančními prostředky zaměřují na koncové uživatele. Ti mnohdy slepě uvěří jakýchkoliv výzev útočníků k odeslání citlivých údajů, nebo přímo finanční hotovosti. Proto jsem se rozhodl provést analýzu o povědomí uživatelů o bezpečnostních hrozbách, které by jim mohli způsobit nemalé starosti.

Účastníci anonymního dotazníkového výzkumu byli požádáni o vyplnění 17 otázek. První tři se týkali stručné charakteristice osoby (pohlaví, věk, vzdělání). Další otázky byly zaměřeny na internetovou bezpečnost, způsoby uchování citlivých údajů, a zda jsou informováni o svých právech a možnostech bezpečného nákupu.

Dotazníky byly distribuovány mezi dotazované papírovou formou. Jeho náhled je možný v příloze P I. Konečný počet dotázaných, kteří se výzkumu aktivně účastnili, se zastavil na čísle 143. Následně jsem provedl vyhodnocení a výsledky jsem zpracoval v programu MS Excel formou grafů, které jsou zpracovány v příloze P II. Tyto výsledky jsem následně použil v praktické části.

6 BEZPEČNOSTNÍ RIZIKA

I přes dlouhý vývoj se v oblasti zabezpečení bankovních transakcí a platebních karet nedocílilo stoprocentního zabezpečení. Na problematiku bezpečnosti můžeme obecně nahlížet ze dvou pohledů. Vedle sebe zde stojí technický aspekt a lidský faktor. Oba jdou ruku v ruce, a pokud klopýtá jeden z nich, objevuje se potenciální riziko. Uživatelský přístup je otázkou konkrétní informovanosti, zodpovědnosti a údržby počítače, přes který klient přistupuje do internetového bankovnictví. Naopak zabezpečení jako takové je téměř výhradně v rukou banky.

Na druhé straně pak stojí jednotlivec (hacker či skimmer), nebo častěji skupina lidí, která pro peníze či s cílem obecně škodit provádí nejrůznější aktivity. Například může jít o rozesílání nevyžádaných e-mailů, distribuci malware, nebo chyby v JavaScriptu. Do počítačů běžných uživatelů internetu se tak mohou dostat spamy s nejrůznějším obsahem včetně virů a trojských koní. Ty pak škodí a samovolně se aktivují v uživatelově počítači. Vzhledem k tomu, že internet nezná hranice, pochází tyto skupiny z různých koutů světa – převážně ze zemí bývalého Sovětského svazu, Číny, ale také z amerického kontinentu.

V tabulce 2 je znázorněna kategorizace hackerů dle Požára (2010, s. 284)

Tabulka 2 Pachatelé kybernetické kriminality [9] [vlastní]

Kiddiots / script Kiddies	Jsou na nejnižší úrovni v páchání této trestné činnosti. Dokážou nalézt na internetu kód a upravit jej pro spuštění nové varianty viru.
Tvůrce virů	Lépe ovládá programování na vyšší úrovni. Píše viry a zveřejňuje je na internetu nebo dokáže spustit virový útok elektronickou poštou.
Příležitostný hacker	Tvůrce virů se zapojuje do světa elektronického zločinu. Pracuje většinou jako programátor či v oboru informačních technologií.
Profesionální hacker	Ten se živí krádežemi kreditních karet, změnou webových stránek, či dokonce elektronickým vydíráním.
Phisher	Vytváří falešné webové stránky, ze kterých získává hesla pomocí metod sociálního inženýrství. Podvodem pak získává velké částky peněz z účtu.
Nájemný počítačový pachatel kybernetické kriminality	Ten nabízí své znalosti tomu, kdo nabídne nejvyšší cenu za jeho služby.

Zisky organizovaného zločinu již podle odhadů z roku 2009 přesáhly zisky drogových kartelů. V roce 2011 se jejich zisky v celosvětovém měřítku odhadovaly na 114 miliard dolarů. To ovšem není konečné číslo, protože k tomuto údaji je nutné přičíst i náklady organizací obnovit stav, který trval před útokem a další náklady na ztrátu času, které oběti utrpí. V tomto případě je částka odhadována na 274 miliard dolarů. Níže jsem uvedl nejčastější typy útoků jak v oblasti platebních karet, tak v prostředí internetu a škodlivého softwaru.

6.1 Platební karty

Zneužití platebních karet lze provést mnoha způsoby, jejichž provedení lze uplatnit mnoha způsoby a záleží na možnostech, znalostech a dovednostech pachatelů trestných činů. V následujícím části se budu zabývat možnými způsoby jak využít platební kartu k nelegální činnosti.

Platební neschopnost

Jde o druh trestné činnosti, kdy oprávněný držitel kreditní karty záměrně přečerpá poskytnuté finanční prostředky a následně vzniklé dluhy nehodlá uhradit. Zjištění totožnosti takových pachatelů nebývá problémem. Jako prevence před výše zmíněným rizikem zneužití spolupracují vydavatelé platebních karet pečlivým vyhodnocením korektnosti žadatelů využíváním interních databází již dříve insolventních klientů.

Fingovaná ztráta karty

Jde o způsob, kdy držitel platební karty oznámí její ztrátu, ale navzdory tomu ji stále využívá k uskutečňování transakcí pro svůj prospěch. Vinu pak přičítá fiktivnímu pachateli. Neoprávněné peněžní transakce jsou možné jen omezenou dobu, poté dojde vydavatelem k blokaci karty.

Nepoctivý nálezce, blízká osoba

Jde o činnost, kdy zloděj či neoprávněný držitel platební karty využije hrubého nedodržení bezpečnostních zásad legálního držitele platební karty a využije PIN kódu uloženého např. v plastovém obalu karty, prostoru peněženky či dat uložených v mobilním telefonu. V tomto případě přichází v úvahu také další rizika zneužití nespokojenými zaměstnanci, rodinnými příslušníky nebo jinými blízkými osobami.

Krádež a navrácení

Z názvu je patrné, že jde o metodu, kdy je oprávněnému držiteli karta zcizena a poté navrácena. Ten ovšem netuší, že s kartou bylo nelegálně nakládáno a proto neprovede blokaci. Zpravidla pak následuje výběr veškerých finančních prostředků.

Vydání karty na základě padělaných dokladů

Do této skupiny patří podvodné žádosti vydání kreditní karty na základě padělaných (popř. pozměněných) osobních dokladů. V případě, že je karta vydána neexistující osobě, dochází k odčerpání finančních prostředků. Následná identifikace pachatele je velmi obtížná.

Skimming

Název skimming je odvozen z angl. data skimming sbírání dat. Podle Policie ČR jde od roku 2009 o nejčastější způsob zjištění dat uložených na kartě. Pachatelé skimmovací zařízení instalují přímo do otvoru pro kartu v bankomatu. Běžný uživatel si jej vůbec nevšimne. Při jeho použití zpravidla nedochází k fyzickému odcizení platební karty a poškozený se o vzniklé újmě nedozví okamžitě. Pachatelům nabité údaje stačí k vytvoření duplikátu karty.

Skimmovací zařízení je v převážné většině případů tvořeno z části, která dokáže přečíst magnetickou kartu při jejím vložení do bankomatu, a z části (např. minikamera či upravená klávesnice), která sejme PIN kód zadaný uživatelem bankomatu (viz obr. č. 1). Čísla 3 a 4 na obrázku značí umístění skimmovací zařízení. Pachatelé se při své činnosti zaměřují výhradně na určité typy bankomatů, na které lze skimmovací zařízení nainstalovat. Jedná se o jakousi část, popř. sestavu elektronického zařízení (např. minikamera či upravená klávesnice), které se stane součástí bankomatu a které sejme identifikační údaje karty včetně PIN kódu. Dokáže tedy po vložení platební karty do bankomatu přečíst jeho magnetickou část a uchovat nebo odeslat údaje z karty. [39]

Obrázek 19 Skimming, falešná klávesnice [39]

Jako bezpečnostní opatření proti skimmingu se začaly instalovat ochranná zařízení (FDI - Fraudulent Device Inhibitor) pro štěrbinu na vkládání karty do bankomatu. Antiskimmovací nástavce mají zpravidla zelenou barvu a ukládají se na štěrbinu, do které klient vkládá kartu při výběru z bankomatu.

Obrázek 20 Nástavec proti skimmingu [39]

Skimmovací zařízení nemusí být instalováno pouze na bankomatu. Méně nápadný způsob je například umístnění zařízení v kamenném obchodě, kde je zákazník méně ostražitý a při realizaci platby se soustředí na to, aby nebyl vidět PIN. Skimmovací zařízení je platebních terminálů jen těžko odhalitelné.

Rozšíření skimmovacích zařízení bezesporu přispívá také jeho snadná dostupnost. V zahraničních internetových obchodech existuje celá řada možností jak si dané zařízení opatřit. Dle informací dostupných z internetových obchodů bylo zjištěno, že nejvíce zařízení pochází z Číny a Pákistánu. Pro ukázku jsem zvolil nabídku internetové ho obchodu alibaba.com. [39]

card reader/skimm
We manufacture and sell **skimmers** ....
Brand Name: **Skimmer**

Min. Order: 1 Piece **FOB Price:** EUR 2000-3500 / Piece
Category: Service Equipment | Vending Machines
RelatedKeywords: Skimmer

Obrázek 21 Nabídka skimmingu [40]

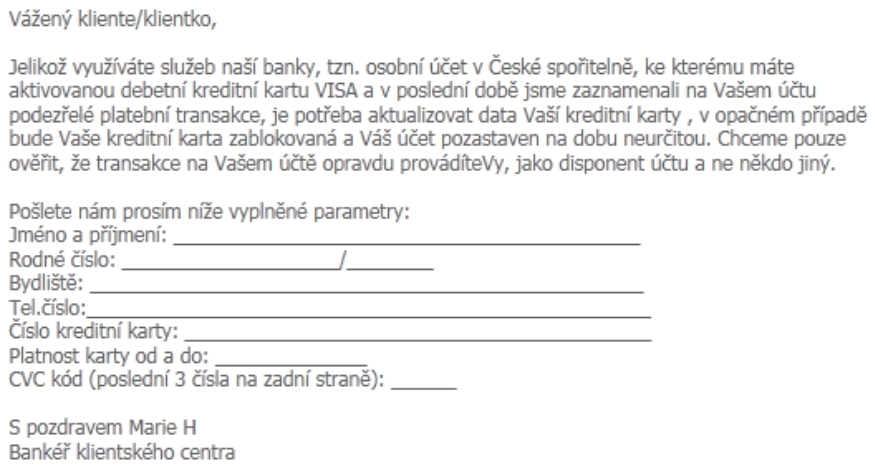
6.2 Počítačová kriminalita

6.2.1 Útoky na uživatele

Jde o útoky, které využívají neznalosti, chyb a sociálního cítění uživatelů. Snaží se pod záminkou vystupování pod smyšlenou institucí nebo osobou vylákat z uživatelů citlivé informace vedoucí k přístupu do prostředí internetového bankovnictví zneužité osoby.

Phishing

Česky se překládá jako „rybaření“. Postup podvodníků připomíná rybaření, jelikož rozešlou e-maily na mnoho náhodných adres (jako když rybáři hodí sítě do vody) a čekají, kdo se nachytá a sdělí důvěrné informace. Pojmy, které tuto metodu charakterizují, jsou také carving nebo brand spofing. Jde o šíření falšovaného e-mailu příjemci, který klamavým způsobem napodobuje legální instituci (zpravidla banku) ve snaze vyzvědět od příjemce důvěrné informace jako číslo platební karty, PIN, CVV kód nebo číslo bankovního účtu. Takový e-mail navádí uživatele, aby navštívil webové stránky či odpověděl na příchozí zprávu a předal tak nevědomky důvěrné informace, které pak pachatel využije pro svůj prospěch. Nemusí jít jen o bankovní účty, ale také účty ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužít jejich služeb (PayPal, eBay, Skype, Google). [6, 41]



Vážený kliente/klientko,

Jelikož využíváte služeb naší banky, tzn. osobní účet v České spořitelně, ke kterému máte aktivovanou debetní kreditní kartu VISA a v poslední době jsme zaznamenali na Vašem účtu podezřelé platební transakce, je potřeba aktualizovat data Vaší kreditní karty , v opačném případě bude Vaše kreditní karta zablokovaná a Váš účet pozastaven na dobu neurčitou. Chceme pouze ověřit, že transakce na Vašem účtě opravdu provádíteVy, jako disponent účtu a ne někdo jiný.

Pošlete nám prosím níže vyplněné parametry:
Jméno a příjmení: _____
Rodné číslo: _____/_____
Bydliště: _____
Tel.číslo:_____
Číslo kreditní karty: _____
Platnost karty od a do: _____
CVC kód (poslední 3 čísla na zadní straně): _____

S pozdravem Marie H
Bankéř klientského centra

Obrázek 22 Phishingový email [41]

Typickými znaky phishingového e-mailu:

- snaží se vyvolat dojem, že byl odeslán organizací, z jejíchž klientů se snaží vylákat důvěrné informace. Tohoto se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.
- text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty.
- v textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky banky. Ve skutečnosti ale odkazuje na jiné místo, kde jsou umístěny podvodné stránky.
- jestliže klient klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky banky. Na podvodných stranách je připraven formulář, kde jsou požadovány důvěrné informace – čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě, přihlašovací údaje ke službám apod.

Z dotazníkového šetření byly zjištěny následující zkušenosti uživatelů s phishingem.

Obrázek 23 Zkušenosti dotazovaných s phishingem [vlastní]

Pharming

První podoba pharmingu je sice efektivní, ale pro podvodníka, který chce jejím prostřednictvím získat citlivé údaje, značně obtížná. Spočívá v tom, že klient zadá ve svém internetovém prohlížeči nějakou adresu. Nedojde ale k jejímu překladu na správnou adresu, ale na adresu, kterou zadali podvodníci. Spojení s bankou je přesměrováno na jiný kanál, jehož www stránky, připravené podvodníky, jsou velice podobné oficiálním stránkám klientovy banky. Při přihlášení klienta ke komunikaci s bankou získají podvodníci citlivé údaje a bude následovat odčerpání finančních prostředků s klientova účtu.

Druhá podoba pharmingu je pro podvodníka jednodušší, a proto je i více používána. Lze se jí ale snáze ubránit. Spočívá v tom, že podvodníci napadají jednotlivé počítače. Pharming se do klientova počítače může dostat jako trojský kůň, který je poslán v příloze nějakého e - mailu, může být stažen apod.

Ochranu proti pharmingu můžeme v zásadě rozdělit do dvou skupin. První skupina spočívá v softwaru. Znamená to např. používat vysoce kvalitní antivirový program, provádět jeho pravidelnou aktualizaci, používat silný firewall atd. Druhá skupina spočívá v samotném klientovi, který s počítačem pracuje a lze je velice stručně shrnout pod výraz obezřetnost, obezřetnost a zase obezřetnost. Znamená to nestahovat z internetu neznámé aplikace, otevírat odkazy v e-mailech apod.

Uživatel může rozpoznat podezřelé stránky taky, že internetbanking se chová na první pohled nestandardně. Může požadovat po klientech údaje, které běžně k přihlášení nepotřebují. Na možné zneužití může upozorňovat také adresní řádek. Pokud neobsahuje obvyklou webovou adresu vaší banky, je to známka, že může jít o podvodnou webovou stránku. Na pravost upozorňuje také certifikát (šifrování HTTPS) zabezpečení vaší banky. [41]

Obrázek 24 Zkušenosti dotazovaných s pharmingem [vlastní]

Spoofing

Ke své činnosti využívá překladu jména serveru na odpovídající IP adresu, útočí tedy na DNS (Domain Name System). Pokud pak uživatel ve svém internetovém prohlížeči zadá adresu například www.ceskasporitelna.cz, nedojde k překladu na odpovídající IP adresu 194.50.240.70, nýbrž nějakou jinou. Pokud by se totiž útočníkovi podařilo změnit DNS záznam výše zmiňované imaginární banky www.ceskasporitelna.com, přesměruje se komunikace na jiný stroj, jiné stránky, které však na první pohled nelze rozpoznat od originálu. Nic netušící uživatel tedy zadá požadované přihlašovací údaje a předá tak útočníkovi údaje pro vstup na účet.

Trashing

Je to další z „moderních“ způsobů podvodů; je rovněž založený na zjištění citlivých dat. Název je odvozen od anglického trash (koš). Jde v podstatě o „vybírání odpadků“, z nichž lze zjistit řadu „zajímavých“ informací. Výjimkou nejsou přístupová hesla, zdrojové kódy

apod. Proto je nutné pečlivě dbát na řádnou skartaci dokumentů a zabezpečte nějak odvoz a skladování „odpadních informací“, a to jak ve fyzické, tak i v elektronické podobě. [41]

Malware

Pojem „malware“ pochází ze spojení dvou anglických slov – „malicious“ (nebezpečný, škodlivý) a „software“ (programové vybavení počítače). Jedná se o společné označení pro škodlivé počítačové programy, jejichž účelem je průnik a případné poškození počítače bez vědomí jeho majitele. Mezi malware dále řadíme: [3]

Rootkity

Rootkity jsou počítačové programy, které mají za úkol skrýt další nebezpečný software před zrakem uživatele a znemožnit (nebo co nejvíce ztížit) jeho odstranění z napadeného počítače. Uživatel si tedy nemusí být vůbec vědom, že je jeho počítač napaden. Rootkity obvykle pracují pod administrátorským účtem a využívají mnoho různých technik k maskování. Dokážou skrýt své soubory i běžící procesy nebo se vydávat za legitimní součásti operačního systému. Obvykle také obsahují různé kontroly, zda rootkit a jím chráněná aplikace běží. Pokud se je uživatel pokusí ukončit, rootkit se postará o okamžité opětovné spuštění. Rootkity jsou využívány především trojskými koňmi, kde je žádoucí, aby uživatel nezpozoroval napadení svého počítače. [3]

Trojské koně

Stejně jako trojský kůň v řecké mytologii, je i počítačový trojský kůň nástroj, který útočníkovi umožní nepozorovaně „obsadit“ Trojské koně jsou počítač oběti. Napadený počítač poté může být útočníkem zcela ovládán. Útočník může pracovat se soubory a programy stejně, jako by fyzicky seděl u napadeného počítače. Navíc může sledovat veškerou činnost uživatele – ať už přímým sledováním pracovní plochy nebo ukládáním záznamů o stisknutých klávesách a spuštěných programech. Trojské koně se sami nešíří, ani nenapadají jiné počítačové programy. Jejich šíření obvykle zajišťují červy a viry, které po napadení počítače trojského koně stáhnou z předem zadané adresy a nainstalují. Útočníkovi pak už jen stačí se k trojskému koni vzdáleně připojit. Aby uživatel nezpozoroval napadení, využívají trojské koně rootkitů pro své maskování. [3]

Keylogger

Tento pojem by šel do češtiny přeložit jako odposlech klávesnice. Může být prováděn dvojí způsobem. První variantou je nainstalování programu (např. Freekeylogger, ActivityMon, Safetica), které slouží k uchování všech hesel, které uživatel zadá. Pachatel tak může využít volně přístupných prostor jako například internetové kavárny, knihovny či areálové studovny a poté provést „sběr“ shromážděných dat.

Druhou variantou je odposlech pomocí elektromagnetických vln. Ty jsou vyzařovány z klávesnice (nezáleží na druhu připojení, mění se jen intenzita vyzařování) při stisku jednotlivých kláves. Dekódovací software pak přiřadí k jednotlivým pulzům znaky. Byly provedeny měření, které na vzdálenost 20m dokázaly dekódovat 95% znaků. Aktivní ochrana proti tomuto způsobu trestné činnosti je zavedení tzv. virtuálních klávesnic, které již dnes využívají všechny banky.

Obrázek 25 Virtuální klávesnice [29]

Nigérijské dopisy

Jedná se o řetězový e-mail, který požaduje pomoc pro nemocného, opuštěná zvířata, nebo jakékoliv jiné způsoby zkonstruované pro apelování na smysly čtenáře. Ale tyto e - maily nejsou ničím jiným než formou podvodu. Tyto dopisy mají formu e - mailu informujícího příjemce, že vyhrál loterii nebo slosování nebo žádající o pomoc při vyhnutí se dani z příjmu

za značnou odměnu. Ve skutečnosti se pokouší podvést uživatele, která je pak požádán

o zaslání určitého množství peněz pro zaplacení celních poplatků, spotřebních daní, odměny úředníkům apod.

6.2.2 Útoky skrze JAVAscript

Zde je ochrana proti zcizení dat složitější z důvodu, že pachatel využívá vlastností programovacího jazyka. JavaScript představuje jednu ze základních webových technologií, která poskytuje moderním webovým stránkám interaktivitu. Tvůrci webových stránek využívají JavaScriptu k tvorbě dynamických nabídek (menu), různých náhledů obrázků, při ověřování formulářů, apod. Základním znakem JavaScriptu je jeho spouštění na straně uživatele. JavaScript je do webových stránek integrován pomocí tzv. skriptů. Skript je kousek programového kódu, který obsahuje instrukce pro jednotlivé akce. Ke spuštění skriptu dochází až po úplném stažení a zobrazení webové stránky. Poté již má JavaScript přístup ke všem prvkům stránky a může je aktivně měnit – to je případ již zmíněného menu. JavaScript může také aktivně odesílat různé informace. Toho se například využívá u formulářů, kde dochází k odeslání dat, aniž by se musela celá stránka znovu načíst ze serveru.

6.2.2.1 ClickJacking

Název útoku by se dal přeložit jako „ukradené kliknutí“, což přesně vystihuje princip, jakým je útok prováděn. Vše je založeno na překrytí určitého prvku (např. tlačítka) jiným prvkem. Uživatel tedy na tento nový prvek klikne, jelikož od něj očekává akci původního tlačítka. Překrytí může být vytvořeno pomocí několika oken prohlížeče, nebo vložením průhledného rámu do stávajícího okna. Tento rám poté může zobrazovat pouze ten prvek, který má být nahrazen. Uživatel tedy vůbec nezpozoruje, že kliká na jiné tlačítko. Tento útok postihuje veškeré webové prohlížeče i značnou část webových aplikací. Jako praktická ukázka útoku sloužil při jeho představování příklad, kdy uživatel klikáním na tlačítka webové stránky nevědomky povolil přístup ke své webové kameře a mikrofonu v aplikaci Flash. [42]

Obrázek 26 Zkušenosti dotazovaných s clickjackingem [vlastní]

6.2.3 DoS

je typem útoku, který je namířen proti serveru, resp. celé síti připojené k internetu s cílem ochromit jejich provoz. Jde o útoky, při nichž je z mnoha míst vysláno velké množství požadavků na jeden server, který se pod jejich náporem zhroutí. Někdy je DoS útok použit jen jako pomocná akce k zahlazení stop, restartování vzdáleného počítače apod. DoS útok (Distributed Denial of Service) jsou variantou DoS útoku, který je však prováděn souběžně z velkého množství počítačů. S pomocí tisíců počítačů na celém světě, které se nakazily škodlivým kódem a vytvořily tak botnet, je možno zahltit podnikové severy tisíci elektronických zpráv, čímž se zablokují veškeré skutečné transakce a komunikace serveru. Pachatelé poté kontaktují provozovatele elektronického obchodu, ve kterém požadují finanční obnos pod hrozbou opakovaného útoku. Tento typ vydírání zaznamenal rozkvět zejména v posledních letech, kdy roste počet sítí, které zločinci mohou vzdáleně řídit a ovládat. Je tedy zřejmé, že tento typ útoky může mít pro provozovatele e - shopu fatální důsledky. [43]

7 ODHAD DALŠÍHO VÝVOJE

Odhad budoucího vývoje je ovlivněn několika faktory, které se zavedením nových technologií a prostředků přímo souvisí. Jejich primární funkcí je bezpečnost, jejich rozšíření, zlepšení funkcí, či tvořit systém uživatelsky pohodlnější.

7.1 Platební karty

V oblasti platebních karet se během minulého roku začala využívat možnost úhrady prostřednictvím bezkontaktních plateb. Jedná se o novou platební technologii, která je založena na technologii NFC (viz. kapitola 3.3.5). V porovnání s platbou v hotovosti je bezkontaktní platba mnohem rychlejší, pohodlnější i bezpečnější způsob placení. Bezkontaktní platba trvá jen pár sekund a je vhodná především pro placení nákupů do 500 Kč (do výše této částky není třeba zadávat PIN).

Aby bylo možné kartu akceptovat, je třeba ji přiložit velmi blízko ke snímači (vzdálenost 2 – 5 cm), což eliminuje možnost načtení informací jiným zařízením. Během transakce si předají karta a terminál zašifrované bezpečnostní údaje. Tím je zajištěno, že karta nemůže být zneužita použitím neautorizovaného terminálu nebo jiným čtecím zařízením. Zvýšení bezpečnosti je docíleno také tím, že PIN už držitel nemusí zadávat tak často jako dřív, čímž se výrazně sníží riziko, že ho někdo odpozoruje. Stejně tak je to s dalšími citlivými údaji jako je číslo karty, jméno majitele, datum ukončení platnosti a CVV/CVC kód.

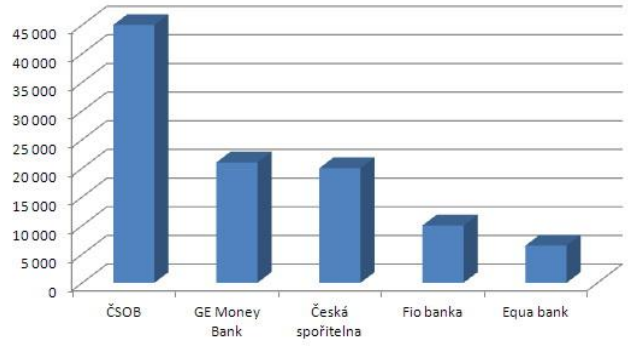
Nosičem nemusí být jen platební karta, NFC čipy se implementují také do nálepek (zpravidla mobilní telefon), klíčenek, hodinek, náramků nebo prstenů. [44]

Obrázek 27 Zařízení s technologií NFC [44]

I když u nás je možnost bezkontaktních plateb novinkou, ve světě jde již o běžnou praxi a jejich rozšiřitelnost v celosvětovém měřítku roste. V roce 2011 bylo vydáno 320 milionů bezkontaktních karet a jejich roční nárůst se odhaduje mezi 15 – 20 %. Lze tedy předpokládat, že v následujících letech se trendy v oblasti bezhotovostního styku budou ubírat tímto směrem.

7.2 Internetové bankovnictví a platební systémy

Novinkou v této oblasti je řízení internetového bankovnictví prostřednictvím mobilního telefonu. Zatímco ještě před několika lety mobilní bankovnictví v podstatě neexistovalo a objevovaly se jen první kroky s technologiemi GSM či WAP, v dnešní době se rozšiřují zařízení jako smartphony a tablety a uživatelé očekávají stejné funkce jako u počítače. Je tedy pochopitelné, že bankovní instituce se zaměřili na tuto oblast a v polovině loňského roku umožnili řízení svých účtů prostřednictvím těchto zařízení. Ovládání těchto účtů se provádí pomocí aplikací, které se liší dle banky, u které je účet zřízen. Počet uživatelů raketově roste a dle údajů ČSÚ byly uskutečněny transakce v objemu 560 milionů Kč. Na obrázku je znázorněn počet uživatelů smartbankingu k dubnu 2012.



Obrázek 28 Vývoj smartbankingu [45]

Především pro poměrně krátkou dobu funkčnosti nebyly prozatím zjištěny závažnější útoky na tyto typy zařízení. Do budoucna lze ovšem předpokládat, že se budou stávat čím dál častěji předmětem trestné činnosti. U počítače je totiž celá řada možností, jak transakce zabezpečit, kdežto u smartphonů jsou tyto možnosti značně omezené. V telefonech totiž uživatelé nepoužívají antiviry či firewally, a mobilní zařízení nepodporují ani další bezpečnostní prvky jak např. USB tokeny. Většina aplikací tedy využívá pro autorizaci pouze hesla, ale do budoucna se uvažuje o autorizaci, která by probíhala ve dvou či více krocích. [45]

8 NÁVRHY PRO BEZPEČNÝ NÁKUP

V této kapitole jsem stanovil návody a postupy, jejichž dodržování by mělo vést k minimalizaci možných rizik spojených s nákupem v elektronickém obchodě a finančních transakcí prováděných jak platební kartou tak prostřednictvím internetového bankovnictví či elektronických peněženek. V této kapitole budu vycházet z internetových stránek asociací. [46,47]

8.1 Certifikáty elektronických obchodů

Internetových obchodů neustále přibývá a pro zákazníka může být proto poměrně zmatečné vybrat si ten, který by jeho důvěru nezklamal. Pro lepší orientaci a záruku bezpečného nákupu existuje několik typů certifikátů, které by měly dodat zákazníkovi určitou jistotu, že obchod splňuje kritéria vedoucí ke zvýšení vzájemné důvěry a eliminaci rizik spojených s nákupem u nepoctivých prodejců.

8.1.1 Certifikáty APEK

Cílem asociace APEK (Asociace pro elektronickou komerci) je soustavně podporovat rozvoj elektronického obchodování v České republice. Mezi členy patří největší české internetové obchody, přední softwarové společnosti a finanční instituce.

Certifikovaný obchod

Certifikovaný obchod je dlouholetým projektem, který přináší záruky pro nakupující na internetu a zároveň vylepšuje obsahovou kvalitu e - shopů. APEK Certifikovaný obchod je prvním ze dvou stupňů certifikátů, který Asociace vystavuje na základě testování. APEK zaručuje zákazníkům internetovým obchodů, že certifikovaný obchodník splňuje základní pravidla bezpečného a bezproblémového nákupu v souladu s platnou legislativou, jejichž úroveň je stanovena certifikačními pravidly:

- úplné a pravdivé informování spotřebitele o provozovateli internetové obchodu (sídlo obchodníka, kontakty na odpovědné osoby, apod.)
- úplné a pravdivé informování o zboží a cenách, včetně všech poplatků
- jakým způsobem probíhá nákup (nákupní řád, obchodní podmínky)

- důležité informace o vyřízení objednávky (způsob dodávky, možnosti placení, cena poštovného a balného)
- jak probíhá reklamace (reklamační řád)
- komunikace se zákazníky (odpovídá na e-maily, telefonáty, apod.)
- splňuje zákonné požadavky, dané zejména směrnicemi Evropského parlamentu a Rady, občanským zákoníkem a dalšími normami.

Obrázek 29 Logo APEK certifikovaný obchod [48]

Certifikát kvality

O získání APEK se může ucházet každý držitel značky Certifikovaný obchod. Zatímco v případě certifikátu Certifikovaný obchod je kontrola zaměřena především na formální stránku e-shopu (hlavně na soulad obchodních podmínek a všech postupů s platnou legislativou), testování v průběhu procesu certifikace Certifikátu kvality klade důraz na průběh samotného nákupu a nabízené služby.

Hlavním cílem Certifikátu kvality je nabídnout objektivní hodnocení e-shopu pro zákazníky a tím rozpoznání obchodů, které disponují velkou kvalitou služeb. Pro obchodníky je naopak připravena zpětná vazba ve formě textového protokolu a zároveň marketingově zajímavá značka.

Obrázek 30 Logo APEK certifikát kvality [48]

8.1.2 Sdružení na ochranu spotřebitelů

Program SAOP (spotřebitelský audit obchodních podmínek) byl vytvořen Sdružením obrany spotřebitelů ČR (SOS) za účelem zvýšení obecného povědomí o spotřebitelských právech mezi podnikateli, ale i širší spotřebitelské veřejnosti. Právě proto, že podnikatelé jsou těmi, kteří spotřebitelská práva uvádějí v život prostřednictvím svých obchodních podmínek, je nutné tyto obchodní podmínky mít v souladu s příslušnými právními předpisy.

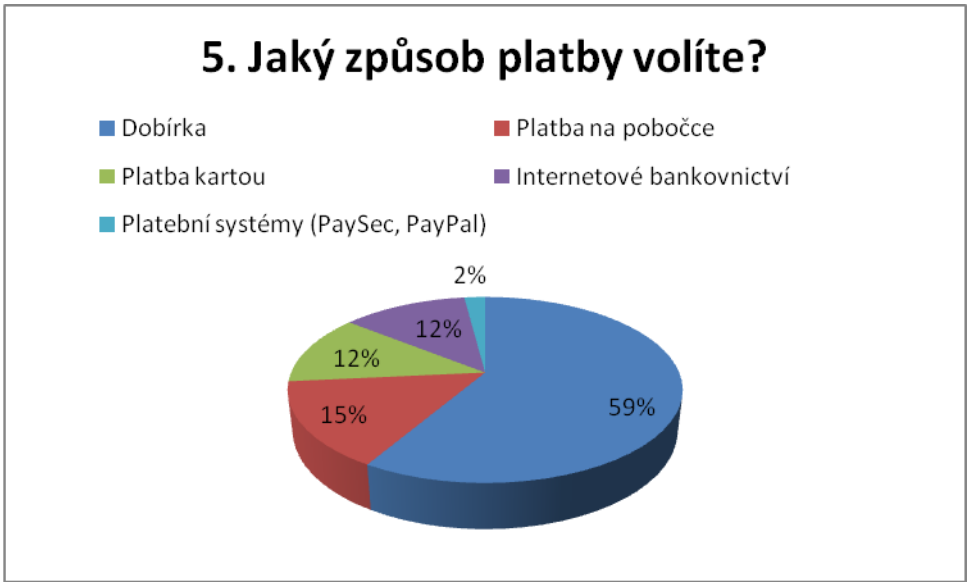
Obrázek 31 Povědomí uživatelů o APEK a SOS [vlastní]

SOS nabízí provedení spotřebitelského auditu jejich obchodních podmínek, který spočívá zejména v konzultaci, opravě a doporučení konkrétních obchodních podmínek. Pakliže podnikatel na základě příslušné smlouvy o SAOP splní požadavky příslušných právních předpisů, obdrží jedinečné logo SAOP, osvědčení o provedení spotřebitelského auditu a bude na něj odkazováno webových stránek SOS (včetně aplikace upozorňující na bezpečné obchody). Podnikatel pak má možnost logo SAOP prezentovat souběžně s jeho auditem prověřenými obchodními podmínkami. Toto logo prokazuje spotřebiteli, že obchodní podmínky na něj aplikované podnikatelem nejsou v rozporu se zákonem a jejich důsledným uplatňováním se domůže svého práva. Podnikatel provedením SAOP dává najevo, že ctí příslušné právní předpisy a SAOP tak zvyšuje jeho dobré jméno. Logo jej zároveň zavazuje k tomu, že se vůči spotřebitelům bude chovat v souladu se zákonem, obchodními podmínkami, a dokonce i v souladu s dobrými mravy.

Obrázek 32 Logo organizace SOS [49]

8.2 Zásady pro použití platebních karet

Je třeba si uvědomit, že platební karta slouží jako prostředek, který může být pachatelem zneužit hned několika způsoby. Proto je nutné dodržovat zásady, které vedou k minimalizaci těchto potencionálních rizik. Jak ukazuje průzkum jednou z nejčastějších pochybení je nedostatečné utajení PINU. Po jejich získání má pachatel neomezený přístup k finančním prostředkům.



Obrázek 33 Uložení PINU [vlastní]

Zásady vedoucí ke snížení rizika zneužití platební karty:

1. PIN je nutné udržovat v naprosté tajnosti a doporučuje se ho nezapisovat a už vůbec ne v blízkosti platební karty. Ač se toto pravidlo může zdát primitivní je prokázáno, že nemalé množství lidí ho má zapsané přímo na obalu karty. Sdělování PIN není vhodné sdělovat ani rodinným příslušníkům. Při případné změně rodinných poměrů a následném zneužití může být zpětné vymáhání dosti problematické

2. Zadávání PINU jak u obchodníka tak při výběru z bankomatu vždy prováděno skrytým způsobem
3. Nikdy nedávat kartu z ruky, v případě, že tato situace nastane, je nutné ověřit, zda jde opravdu o vaši kartu. Doporučuje se také následná kontrola pohybů na účtu
4. Dokumenty, na kterých jsou údaje o kartě, je nutné likvidovat způsobem, který znemožní jejich následnou identifikaci
5. Kartu je vhodné používat u důvěryhodných obchodníků, pokud nemáme k obchodníkovi důvěru, je vhodné použít platbu v hotovosti
6. Provádění pravidelných kontrol pohybu na účtu a změny PINU. Je možné využít tzv. real time kontrol, kdy o provádění jakékoliv transakce je uživatel informován pomocí SMS
7. Ztrátu karty hlásit neprodleně vydavateli, který následně kartu zablokuje. Poplatky za vyřízení nové karty jsou minimální proti možnosti použití karty nepoctivým nálezcem či pachatelem
8. Při výběru z bankomatu se ujistit, zda se v blízkosti nevyskytuje podezřelá osoba. Pokud máme podezření na špatnou funkci bankomatu (skimming), neprodleně informovat buď zřizovatele bankomatu, nebo Policii ČR
9. Chránit údaje na kartě jako je jméno, datum expirace, CVV/CVC, které by mohl pachatel použít při platbě prostřednictvím internetu. Jde především o získání těchto údajů formou phishingu
10. U bezkontaktních platebních karet používat ochranné pouzdro, které snižuje schopnost komunikace s neoprávněným zařízením

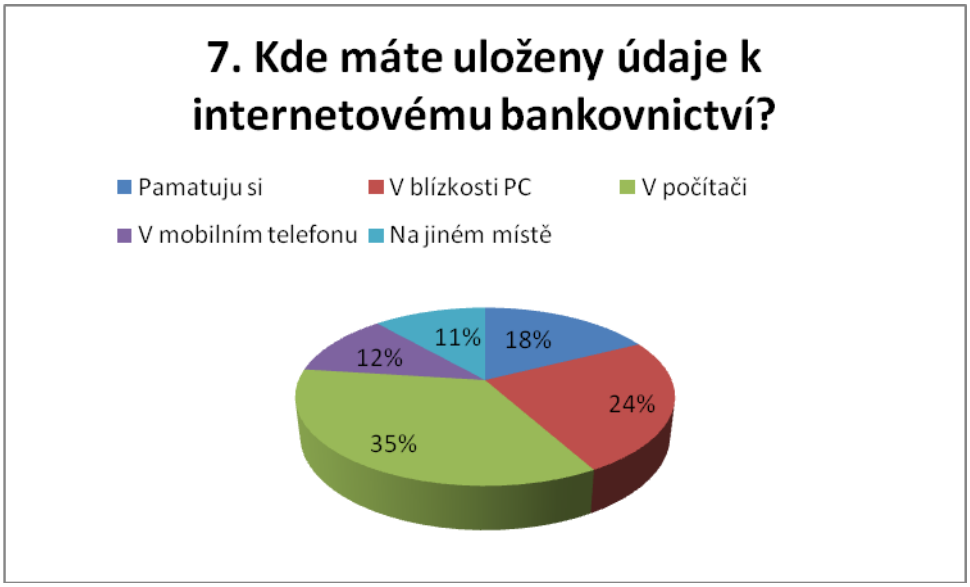
Zvýšení bezpečnostní prvků zpravidla vede ke snížení jednoduchosti při použití. Jedním z opatření, které může uživatel aplikovat je rozložení finančních prostředků na více účtů a používat karty k nim určené. Může jít např. o následující rozložení:

1. Karta určená pro běžné platby v obchodě (disponuje menším finančním obnosem)
2. Karta určená nákupy dražšího zboží
3. Karta určená pro zahraniční cesty

Dalším způsobem může být zřízení účtu, ke kterému není vydána karta následné přečerpávání financí potřebné k uskutečnění transakcí.

8.3 Zásady pro požití internetového bankovnictví

Obecně lze tvrdit, že zabezpečení internetového bankovnictví je tak silné, jak silný je jeho nejslabší článek. Je proto nezbytné věnovat pozornost nejen prvkům autentizace ale také údržbě a provádění kontrol uživatelského počítače. Bylo zjištěno, že stejně jako u platebních karet uživatelé mnohdy nechávají svoje autentizací údaje na očích, což může mít jak pro běžného uživatele, tak pro organizaci fatální důsledky.



Obrázek 34 Přihlášení k internetovému bankovnictví [vlastní]

Níže je navrženo několik postupů pro bezpečnou komunikaci mezi uživatelem a bankou.

1. Pravidelná změna hesla (doporučuje se 1x za měsíc). Při volbě hesla nepoužívat snadno detekovatelné informace jako je rok narození, jméno, informace o bydlišti či telefonní číslo
2. Údaje potřebné k přihlášení nikomu nesdělovat a nenechávat v blízkosti počítače
3. Nereagovat na e-maily, které vyžadují údaje k přihlášení a další citlivé informace
4. Nepřihlašovat se na cizím počítači (areálová studovna, knihovna, internetová kavárna). Můžou zde být nainstalované programy, jejichž primárním cílem je sběr hesel. Takto zabezpečené stránky začínají předponou „https://“ na začátku a ikony zámku na konci adresy řádku

5. Provádět pravidelně aktualizace operačního systému dle aktualizací poskytovaných vydavatelem systému
6. Používání a aktualizace antivirových programů, doporučuje se alespoň 1x týdně provést kontrolu PC
7. Při vstupu na stránky banky ověřit zda jde o zašifrované, a tedy bezpečné přihlašování.
8. Zřízení peněžního limitu pro online bankovní transakce
9. Nepřihlašovat se do internetového bankovnictví pomocí nezabezpečené WIFI sítě
10. Pravidelně kontrolovat stav na účtu

ZÁVĚR

S prudkým rozvojem internetu se paralelně s ním začaly vyvíjet nová odvětví, která jsou na jeho možnostech přímo závislé. Jedním takovým je rozvoj elektronického podnikání a s ním spjatých elektronických finančních prostředků. Dnes již velmi těžko najdeme člověka, který by nedisponoval alespoň platební kartou, k níž bývá zpravidla zřízen běžný bankovní účet. Spojení těchto dvou aspektů otevírá majiteli nové možnosti ke správě svých finančních prostředků. V práci jsem se zaměřil především na bezpečnost z pohledu uživatele. Technické řešení ze strany bankovních institucí lze považovat za poměrně dobře zpracované a tak se pachatelé trestné činnosti spjaté elektronickými finančními prostředky zaměřují na koncové uživatele. Ti mnohdy slepě uvěří jakýchkoliv výzev útočníků k odeslání citlivých údajů, nebo přímo finanční hotovosti. Je tedy zřejmé, že na problematiku bezpečnosti lze obecně nahlížet ze dvou stran. Vedle sebe stojí technický aspekt a lidský faktor. Oba jdou ruku v ruce, a pokud klopýtá jeden z nich, objevuje se potenciální riziko. Uživatelský přístup je otázkou konkrétní informovanosti, zodpovědnosti a údržby počítače, přes který klient přistupuje do internetového bankovnictví. Naopak zabezpečení jako takové je téměř výhradně v rukou banky.

Cílem bakalářské práce bylo přiblížit možnosti, jakými způsoby je možné realizovat úhradu za vybrané zboží v internetovém obchodě z pohledu bezpečnosti. Úvod práce je věnován seznámením se základními pojmy z oblasti elektronického podnikání a šifrování, které hraje klíčovou roli v komunikaci mezi klientem a bankou. Dále jsou čtenáři přiblíženy jednotlivé platební systémy. V kapitole elektronické peněženky jsem analyzoval PaySec jako nejrozšířenější platební systém u nás a PayPal jako jeho druhou celosvětově rozšířenou verzi.

V praktické části se zabývám možnými riziky související s danou problematikou. Jsou zde popsány možné příčiny vzniku nežádoucích situací, opírající se o dotazníkový výzkum, jehož výsledky jsou prezentovány v přílohách P I a P II této práce

Věřím, že tato práce poskytne čtenáři kompletní přehled o dané problematice a ozřejmí mu důvody preventivních opatření, které jsem v této práci prezentoval.

CONCLUSION

The rapid development of the Internet resulted in a parallel development of new industries that are directly dependent on its possibilities. One such is the development of e-business and related electronic financial resources. Nowadays, it would be very difficult to find a person without holding at least a credit card to which a standard bank account is usually set up. The combination of these two aspects opens new opportunities to the owner to manage his/her funds. In the thesis, I have focused primarily on safety from the user's perspective. The technical solution of banking institutions can be considered as relatively well elaborated and therefore the criminals focusing on electronic financial resources target the end users. The latter often blindly believe any prompts of online attackers to send sensitive data, or even cash. Thus it is obvious that safety issues can generally be viewed from two sides. There is the technical aspect and the human factor. Both go hand in hand and if one of them stumbles, a potential risk arises. User access is a matter of specific awareness, responsibility and maintenance of computers through which clients access online banking. On the contrary, security as such is almost entirely in the hands of banks. The aim of the Bachelor's thesis was to bring near the possibilities of the ways how you can pay for selected goods in online shop in terms of safety. The introduction is devoted to familiarization with the basic terms of e-business and encryption, which plays a key role in communication between the client and the bank. In addition, readers are provided with more details on individual payment systems. In the chapter on electronic wallets, I analyzed PaySec as the most widespread payment system in our country and PayPal as its second extended version used worldwide. In the practical part, I have dealt with possible risks associated with the issue. There are described the possible causes of undesirable situations based on a questionnaire survey with the results presented in Appendices P I and P II of this thesis. I believe the thesis will provide readers with a complete overview of the issue and make clear the reasons for preventive measures presented in this work.

SEZNAM POUŽITÉ LITERATURY

MONOGRAFIE:

[1] BROŽ Jiří, Michal HRADECKÝ. *Platební prostředky, jejich ochrana a padělání* 1. vyd. Praha: tiskárna MV p.o., 2008, ISBN 80-7312-055-0.

[2] ČANDÍK, Marek. *Základy informační bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-218-1.

[3] HARRIS, Shon, Allen HARPER, Chris EAGLE, Jonathan NESS a Michael LESTER. *Manuál hackera*. Praha: Grada, 2008. ISBN 978-80247-1346-5.

[4] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.

[5] JUŘÍK, Pavel. *Platební karty - Velká encyklopedie*. Praha: GRADA, 2006. ISBN 80-2470-685-7.

[6] LANCE, James, Lubomír DLOUHÝ. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 80-247-1766-2.

[7] MÁČE, Miroslav. *Platební. styk klasický. a elektronický*. Praha: Grada, 2006. ISBN 80-2471-725-5.

[8] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[9] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[10] PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví*. Praha: Computer Press, 2000. ISBN 80-7226-328-5.

INTERNETOVÉ ZDROJE:

[11] *Ministerstvo pro místní rozvoj* [online]. 2007 [cit. 2012-05-20]. Dostupné z: http://www.mmr.cz/CMSPages/GetFile.aspx?guid=1841f1d3-28ca-4be7-8d0a-14d2d4c14fbb

[12] Historie EO. *Marketingové noviny* [online]. 2006 [cit. 2012-05-15]. Dostupné z: http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=43

[13] Nakupování prostřednictvím internetu. *Český statistický úřad* [online]. 2011 [cit. 2012-05-15]. Dostupné z: http://www.czso.cz/csu/2011edicniplan.nsf/p/9701-11

[14] Pojmy E-business. *E-commerce* [online]. 2002 [cit. 2012-05-15]. Dostupné z: http://www.e-komerce.cz/ec/ec.nsf/0/26ef1f70044846bec12569d5004f9ce7

[15] Dělení e-shopů. *Oxid-eshop* [online]. 2002 [cit. 2012-05-15]. Dostupné z: http://www.oxid-eshop.cz/e-shopy-a-jejich-deleni-z-hlediska-typu-prodeje-d629/?urlparam=s=2

[16] Šifrovací metody. *Západočeská univerzita* [online]. [cit. 2012-05-17]. Dostupné z: www.kvd.zcu.cz/cz/materialy/9PSDS/sifrovani.doc

[17] Hashovací funkce. *Kryptografie* [online]. 2009 [cit. 2012-05-17]. Dostupné z: http://www.kryptografie.wz.cz/data/hash.htm

[18] *MD 5 a SHA-1* [online]. 2010-2012 [cit. 2012-05-23]. Dostupné z: http://www.pocet-znaku.cz/hash

[19] *Co je EDI* [online]. 2007 [cit. 2012-05-23]. Dostupné z: http://www.edipax.cz/Article.aspx?A_ID=71&A_Title=Co%20je%20EDI?&C_ID=591&C_Name=EDI&P_ID=&C1_ID=591&C1_Name=EDI

[20] *Dělení karet* [online]. 2011-2012 [cit. 2012-05-23]. Dostupné z: http://www.novesluzby.cz/pojisteni-a-finance.201/platebni-karty-debetni-kreditni-embosovana.20496.html

[21] *Platební karty*. Penize.cz [online]. 2010 [cit. 2012-05-17]. Dostupné z: http://www.penize.cz/15744-platebni-karty-a-jejich-druhy

[22] *Příručka držitele karty* [online]. 2011 [cit. 2012-05-20]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/Prirucka_drzitele_PK.pdf

[23] *Karty s magnetickým pruhem* [online]. 2008 [cit. 2012-05-17]. ISSN 1803-6007. Dostupné z: http://pandatron.cz/?535&karty_s_magnetickym_pruhem

[24] Mikrokontroléry a čipové karty [online]. 2011 [cit. 2012-05-17]. ISSN 1803-6007. Dostupné z: http://pandatron.cz/?2631&mikrokontrolery_a_cipove_karty

[25] *Karta nové generace* [online]. 2011 [cit. 2012-05-17]. Dostupné z: http://aktuality.cardzone.cz/TZ_MasterCard_8-6-2010.pdf

[26] *Přijímání platebních karet* [online]. 2009 [cit. 2012-05-17]. Dostupné z: http://www.rb.cz/attachements/pdf/firemni-finance/podnikatele-a-firmy/platebni-styk/Pokyny_pro_akceptaci_10_09-new.pdf

[27] *Jak funguje bankomat* Jinova [online]. 2009 [cit. 2012-05-17]. Dostupné z: http://www.jinova.cz/jak-funguje-bankomat

[28] *Platební terminály* Systemonline.cz[online]. 2011 [cit. 2012-05-17]. Dostupné z: http://www.systemonline.cz/zpravy/platebni-terminaly-jako-moderni-zpusob-placeni-z.htm

[29] *Česká spořitelna* [online]. 2012 [cit. 2012-05-17]. Dostupné z: www.csas.cz

[30] *3D secure* [online]. 2007 [cit. 2012-05-17]. Dostupné z: http://www.shopcentrik.cz/slovnik/3d-secure.aspx

[31] *Internetové bankovnictví* [online]. 2009 [cit. 2012-05-17]. Dostupné z: http://earchiv.chip.cz/cs/earchiv/vydani/r-2008/internetove-bankovnictvi-kde-je-bezpecne.html

[32] *Smartbanking* [online]. 2012 [cit. 2012-05-17]. Dostupné z: http://www.finparada.cz/clanek.aspx?ID=284

[33] *Bezpečnost online systémů* [online]. 2011 [cit. 2012-05-17]. Dostupné z: http://ecom.ef.jcu.cz/web/download/teorie/p06-bezpecnost.pdf

[34] *PaySec* [online]. 2007-2012 [cit. 2012-05-17]. Dostupné z: www.paysec.cz

[35] *Paypal* [online]. 1999-2012 [cit. 2012-05-20]. Dostupné z: https://www.paypal.com/

[37] *Platební systémy* [online]. 2010 [cit. 2012-05-20]. Dostupné z: http://www.cihar.cz/

[38] *Netshoper* [online]. 2009-2010 [cit. 2012-05-20]. Dostupné z: http://www.netshopper.cz/cz-vyzkumy/vyzkum-netshopper-dobirka-vevodi-ceskemu-internetu.aspx

[39] *Skimming* [online]. 2010-2012 [cit. 2012-05-20]. Dostupné z: http://www.cybersecurity.cz/data/skimming.pdf

[40] *Alibaba* [online]. 1999-2012 [cit. 2012-05-20]. Dostupné z: http://www.alibaba.com/trade/search?Country=&IndexArea=product_en&fsb=y&SearchText=card+reader+skimmer

[41] *Bezpečný internet* [online]. 2008-2010 [cit. 2012-05-20]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[42] *O clickjacking* [online]. 2012 [cit. 2012-05-20]. Dostupné z: http://www.grafika.cz/art/vse/clickjacking.html

[43] *O DOS útocích* [online]. 2012 [cit. 2012-05-20]. Dostupné z: http://www.ikaros.cz/elektronicka-informacni-kriminalita

[44] *Nové trendy* [online]. 2012 [cit. 2012-05-20]. Dostupné z: http://www.ikaros.cz/trendy-v-internetove-bezpecnosti-2012

[45] *O smartbanking* [online]. 2005-2012 [cit. 2012-05-20]. Dostupné z: http://www.bankovnipoplatky.com/smartbanking-v-ceskych-bankach-v-roce-2012-17181.html

[46] *O APEK* [online]. 2012 [cit. 2012-05-20]. Dostupné z: http://www.apek.cz/

[47] *O SOS* [online]. 2006-2012 [cit. 2012-05-20]. Dostupné z: http://spotrebitele.info/

LEGISLATIVA:

[48] Zákon číslo 227/2000 Sb., o elektronickém podpisu, v platném znění.

[49] Zákon číslo 40/1964 Sb., ve znění pozdějších předpisů (Občanský zákoník).

[50] Zákon číslo 513/1991 Sb., ve znění pozdějších předpisů (Obchodní zákoník).

[51] Zákon číslo 101/2000 Sb., o ochraně osobních údajů.

[52] Zákon číslo 124/2002 Sb., o platebním styku.

[53] Zákon číslo 480/2004 Sb., o některých službách informační společnosti.

[54] Zákon číslo 634/1992 Sb., o ochraně spotřebitele.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APEK	Asociace pro elektronickou komerci
CA	Certifikační autorita
CPU	Procesor (Central Processing Unit)
ČR	Česká republika
DNS	Systém doménový jmen (Domain Name Server)
EDI	Elektronická výměna dat
EEPROM	Typ paměti – mazatelná (Electrically Erasable PROM)
HTTP	Hypertextový protokol (HyperText Transfer Protokol)
ISO	Organizace pro tvorbu norem (International Standard Organisation)
NFC	Near Field Communication
PIN	Bezpečnostní kód (Personal Identification Number)
RAM	Operační paměť (Random Acces Memory)
RFID	Technologie bezdrátové komunkace (Radio Frequency Identification)
ROM	Typ paměti (Read Only Memory)
SOS	Sdružení na ochranu spotřebitelů
SIM	Čip mobilního telefonu (Subscriber Information Module)
SSL	Bezpečnostní vrstva (Secure Socket Layer)
SMS	Krátké textové zprávy (Short Message Service)
TCP/IP	Internetový protokol (Transmission Control Protocol/Internet Protokol)
USB	Typ sběrnice (Universal Seriál Bus)
UTP	Typ kabeláže (Unshielded Twisted Pair)
WIFI	Technologie bezdrátového připojení (Wireless Ethernet Compatibility Aliance)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

1. Pohlaví
   - Muž
   - Žena
2. Váš věk
   - 18 – 30
   - 30 – 50
   - 50 a více
3. Dosažené vzdělání
   - Základní
   - Vyučen
   - S maturitou
   - Vysokoškolské
4. Jak často nakupujete v internetovém obchodě?
   - Zatím jsem v IO nenakupoval
   - Výjimečně (1x za rok)
   - Méně často (1x za měsíc)
   - Často (1x za měsíc)
   - Velmi často (několikrát za měsíc)
5. Jaký způsob platby volíte?
   - Dobírka
   - Platba na pobočce
   - Platba kartou
   - Internetové bankovnictví
   - Platební systém (PaySec, PayPal)

6. Kde máte uložen PIN platební karty?

- Pamatuju si
- Na platební kartě
- V peněžence
- V mobilním telefonu
- Na jiném místě

7. Kde máte uloženy údaje k internetovému bankovnictví?

- Pamatuju si
- V blízkosti PC
- V počítači
- V mobilním telefonu
- Na jiném místě

8. Setkali jste se někdy s phishingem? (email, který po Vás vyžadoval citlivé informace)

- Ano
- Ne
- Nevím

9. Setkali jste se někdy s pharmingem? (www stránka, která nebyla šifrována)

- Ano
- Ne
- Nevím

10. Setkali jste se někdy s clickjackingem (po kliknutí na potvrzovací tlačítko jste byli přesměrováni na jiné www stránky)

- Ano
- Ne
- Nevím

11. Kontrolujete, zda je stránka Vašeho IB šifrována? (https)
    - Ano
    - Ne
12. Stal jste se obětí e - kriminality?
    - Ano
    - Ne
13. Pokud odpověď ano uveďte kým (např. pachatel, zaměstnanec, rodinný příslušník)
14. Jaká finanční hotovost Vám byla odčerpána? (v případě, že dvě otázky výše ano)
    - Méně jak 1 000 Kč
    - 1 000 – 5 000 Kč
    - 5 000 – 25 000 Kč
    - Více
15. Kde se přihlašujete do IB?
    - Pouze doma
    - VŠ kolej
    - Areálová studovna
    - Internetová kavárna
    - Knihovna
    - Jiné veřejné místo

16. Znáte svá práva při internetovém nákupu?

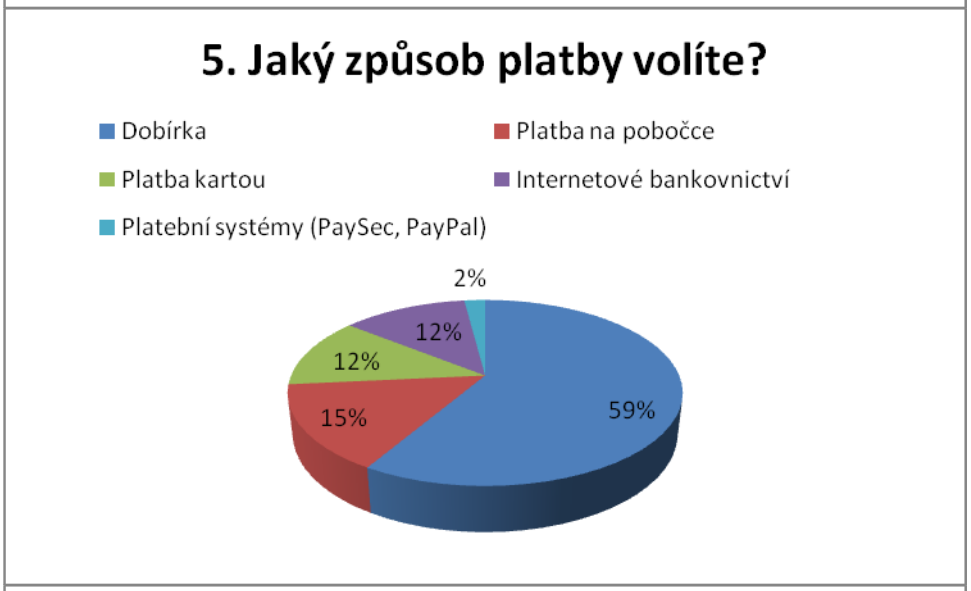
- Ano
- Ne

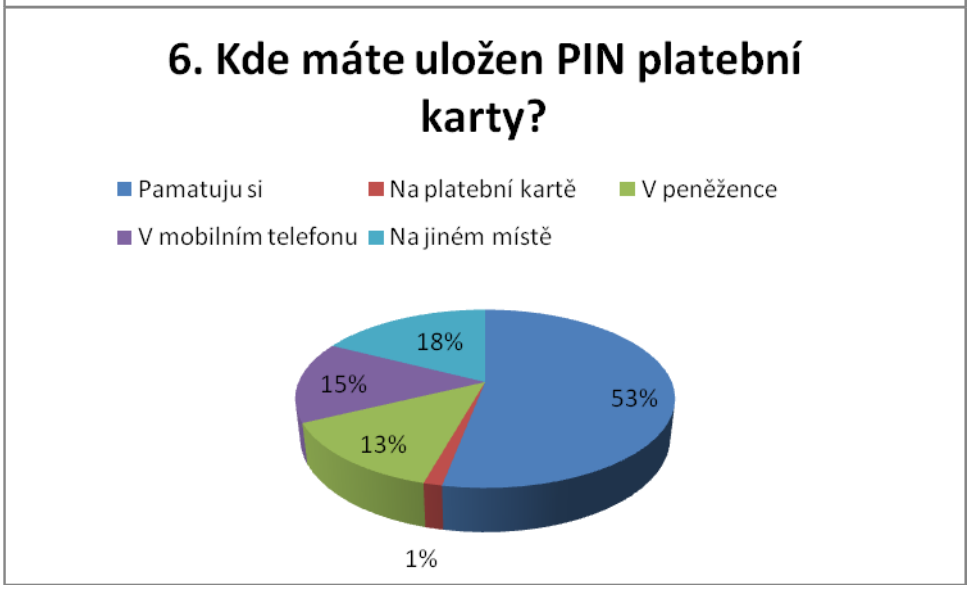
17. Víte jak poznat bezpečný e - shop? (certifikát APEK nebo SOS)

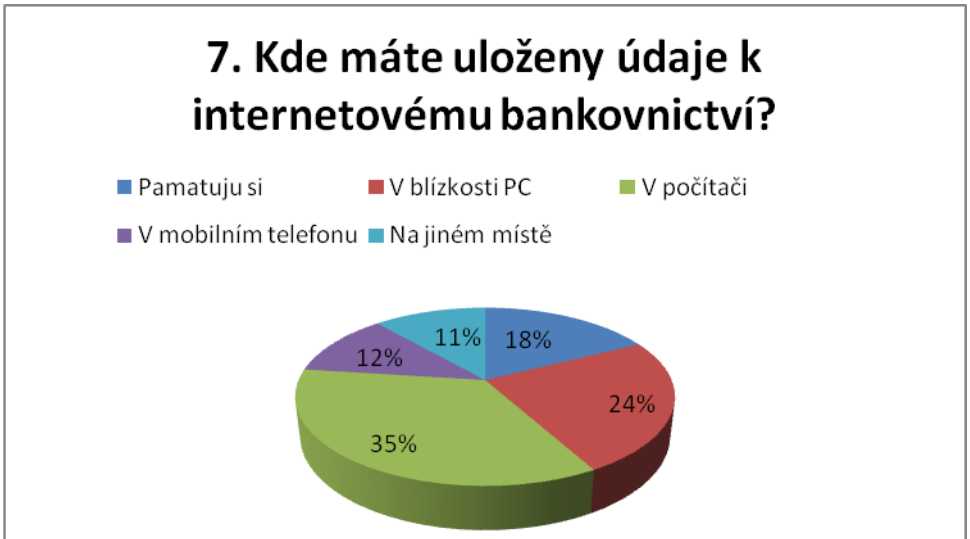
- Ano
- Ne (nikdy jsem o nich neslyšel/a)

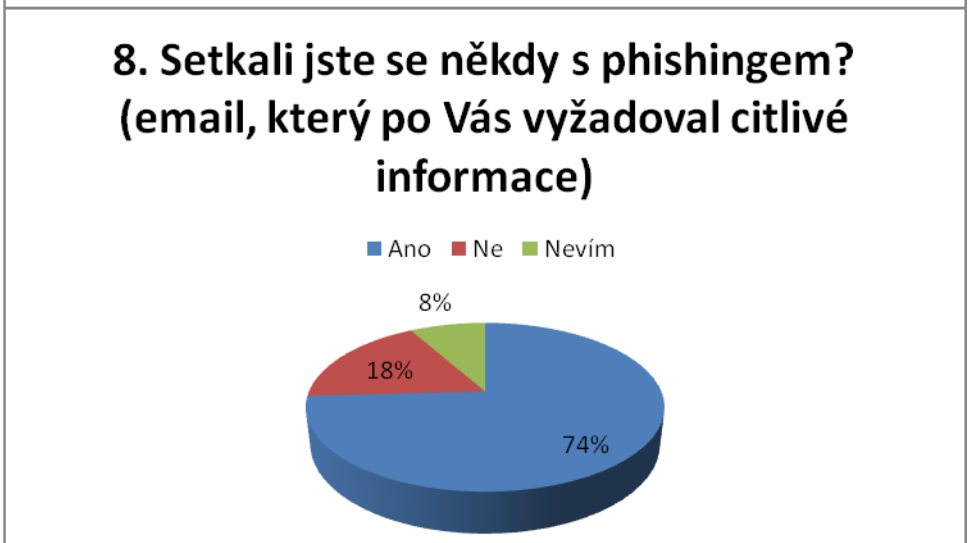
PŘÍLOHA P II: GRAFICKÉ ZNÁZORNĚNÍ VÝSLEDKŮ


4. Jak často nakupujete v Internetovém obchodě?
Zatím jsem v IO nenakupoval(a)
Vyjímečně (1x za rok)
Méně často (několikrát ročně)
Často (1x za měsíc)
Velmi často (několikrát za měsíc)
15%
9%
18%
25%
33%


5. Jaký způsob platby volíte?
Dobírka
Platba na pobočce
Platba kartou
Internetové bankovnictví
Platební systémy (PaySec, PayPal)
2%
12%
12%
15%
59%

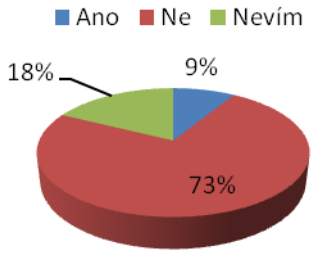

6. Kde máte uložen PIN platební karty?
Pamatuju si
Na platební kartě
V peněžence
V mobilním telefonu
Na jiném místě
18%
15%
53%
13%
1%


7. Kde máte uloženy údaje k internetovému bankovnictví?
Pamatuju si
V blízkosti PC
V počítači
V mobilním telefonu
Na jiném místě
18%
24%
35%
12%
11%

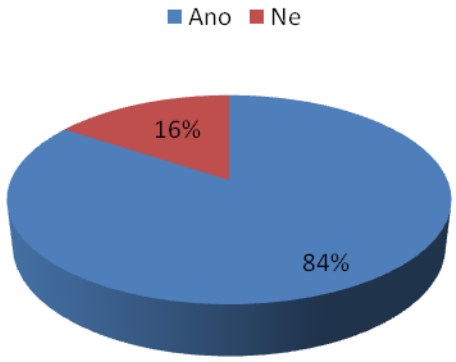

8. Setkali jste se někdy s phishingem? (email, který po Vás vyžadoval citlivé informace)
Ano
Ne
Nevím
8%
18%
74%


9. Setkali jste se někdy s pharmingem? (www stránka, která nebyla šifrována)
Ano
Ne
Nevím
25%
15%
60%

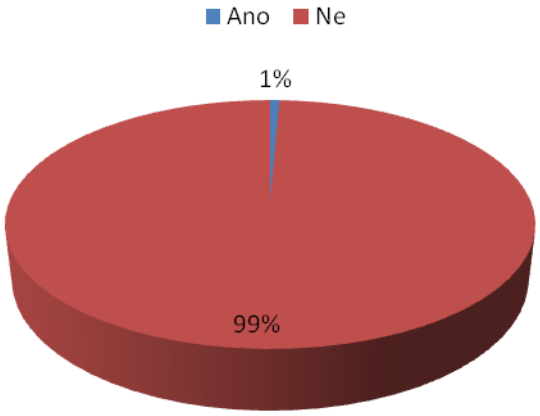
10. Setkali jste se někdy s clickjackingem? (po kliknutí na potvrzovacího tlačítka jste byli přesměrováni na jiné www stránky)



11. Kontrolujete, zda je stránka šifrována? (https)

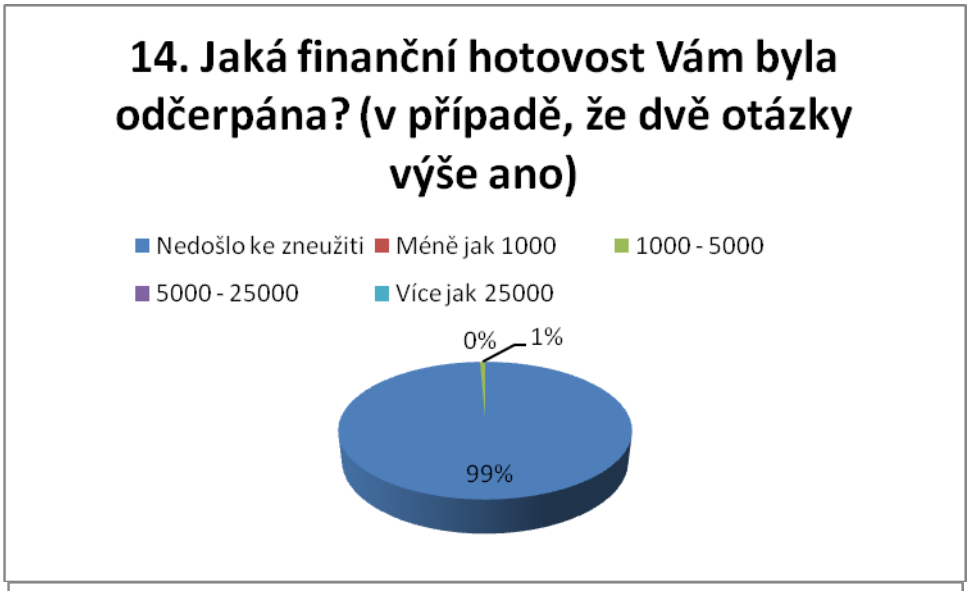


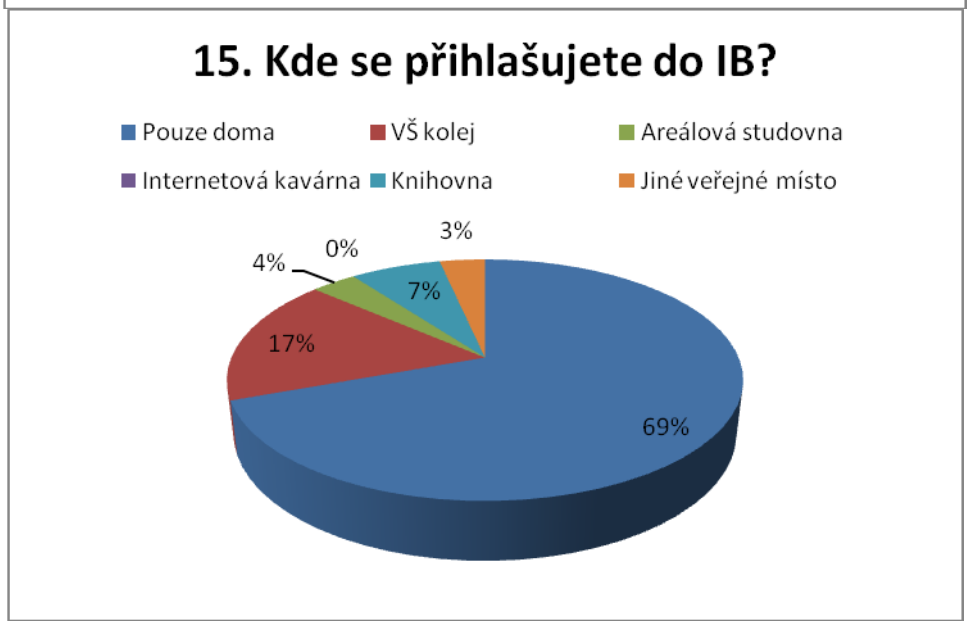
12. Stal jste se obětí e-kriminality?



13. Pokud odpověď ano, uveďte kým (např. pachatel, zaměstnanec, rodinný příslušník)

Odpověď: Rodinný příslušník 1x






16. Znáte svá práva při internetovém nákupu?
Ano
Ne
20%
80%
17. Víte jak poznat bezpečný e - shop? (certifikát APEK nebo SOS)
Ano
Ne (nikdy jsem o nich neslyšel)
44%
56%