Univerzita Palackého v Olomouci

Filozofická fakulta

ELEKTRONICKÉ BANKOVNICTVÍ V ČR Z POHLEDU BEZPEČNOSTI REALIZOVANÝCH TRANSAKCÍ

Bakalářská diplomová práce

Studijní program: Francouzština se zaměřením na aplikovanou ekonomii

Vedoucí práce: Ing. Zdeněk Puchinger

Autor: Lenka Turecká

Olomouc 2010

Univerzita Palackého v Olomouci

Filozofická fakulta

Prohlášení

Místopřísežně prohlašuji, že jsem diplomovou práci na téma: "Elektronické bankovnictví v ČR z pohledu bezpečnosti realizovaných transakcí" vypracovala samostatně pod odborným dohledem vedoucího diplomové práce a uvedla jsem všechny použité podklady a literaturu**.**

V Olomouci dne……..... Podpis……....

Poděkování:
Chtěla bych poděkovat Ing. Puchingerovi za cenné připomínky a odborné rady, kterými přispěl k vypracování této bakalářské práce.

OBSAH

ÚVOD:

Není to tak dávno, kdy lidé nad pojmy GSM bankovnictví, homebanking, internetbanking a dalšími pouze nechápavě kroutili hlavami a tvrdili, že to není nic pro ně, že je to otázkou daleké budoucnosti. Sotva než se nadáli, staly se tyto pojmy a inovace běžnou součástí jejich životů a drtivá většina si ani už nedokáže představit život bez nich. Možná, že si to jen spousta z nás neuvědomuje, jak moc nám tyhle vymoženosti usnadňují každodenní starosti a povinnosti. Lidé si neuvědomují, že ještě před pár lety stáli ve frontách v bankách a na poštách, že spěchali, aby nezmeškali jejich otevírací dobu a úřední hodiny. Je to také možná tím, že stejně jako se mění a vyvíjejí nové technologie, stejně tak se vyvíjejí lidé a věci, které dnes nechápeme a myslíme si, že jsou pro nás zbytečné, se časem stanou neoddělitelnou životní součástí, stejně jak se jí stalo elektronické bankovnictví ve všech svých podobách.

I tohle je důvod, proč jsem si pro svou bakalářskou práci vybrala téma Elektronické bankovnictví v České Republice z pohledu bezpečnosti realizovaných transakcí. Elektronické bankovnictví proto, že je to pro mě zajímavá oblast bankovnictví, která se neustále vyvíjí a nikdy nebudeme moci říct, že o ní známe a víme vše, co se znát dá. V České Republice proto, že zde žiji a myslím, že Česká Republika není v tomto oboru na takové úrovni jako jiné země. A na bezpečnost se zaměřím zejména z toho důvodu, že je to neustále ožehavé téma ve společnosti, protože nikdo nechce přijít o své finanční prostředky a odborníci neustále přemýšlejí jak peněžní transakce zabezpečit proti podvodníkům.

Má práce se bude týkat elektronického bankovnictví obecně, jeho vývoje od prvních platebních karet na světě, přes bankovnictví pomocí telefonů až po bankovnictví pomocí internetu. Zaměřím se na různé komunikační kanály elektronického bankovnictví, na jejich popis, rizika, ale na jejich zabezpečení a využívání.

Vzhledem k tomu, že v dnešní době lidé nejvíce využívají pouze dva komunikační kanály elektronického bankovnictví a to platební karty a internetbanking, zaměřím se detailně na jejich popis, rizika a hlavně na jejich zabezpečení celosvětově, ale zejména na území české Republiky.

Platební karty a internetbanking patří i k nástrojům bezhotovostního platebního styku, který se v poslední době velmi rozšířil po celém světě.

Pokrok globálních metod bezhotovostních plateb je nesporný. Karty, převody, šeky, nové prostředky platby po internetu, platby mobilním telefonem a další jsou k dispozici všem uživatelům. Podle "World Payments Report 2008" (Světové zprávy o platebních prostředcích 2008) provedené společností Capgemini (Royal Bank of Scotland (RBS) a European Financial Management and Marketing Association (EFMA)) představují karty 54% celosvětového objemu plateb. Tento způsob platby je na druhém místě za hotovostním prostředkem s ročním růstem mezi roky 2001 a 2006 16% celosvětově a 11% v Evropě. Elektronické platební transakce rovněž zaznamenaly výrazný vzrůst s přibližně 210.000 miliony transakcí na celém světě.[1]

Když používáme takové způsoby plateb, jsme si však vědomi všech rizik, kterým jsme vystaveni?

I to je důvod proč se budu věnovat tomu, jak jsou platební karty v České Republice zabezpečeny a také jejich dostupnosti u českých bank. Dále pak pomocí statistik a čísel porovnám vydávání a využívání platebních karet v České Republice a také představím pár příkladů podvodů na platebních kartách.

Cílem této části mé práce ale bude zjištění toho, jak jsou čeští uživatelé platebních karet informováni o bezpečnosti jejich karet. K tomuto výzkumu použiji snad tu nejjednodušší metodu formou dotazníku s uzavřenýma otázkami.

Dále se má práce bude týkat stavu internetového bankovnictví v České Republice. Rozeberu různé možnosti zabezpečení internetbankingu z pohledu uživatele, ale také popíšu ty nejznámější a nejpoužívanější druhy zneužívání internetbankingu a důvěry klientů různými podvodníky. Cílem pro mě zde bude srovnání zabezpečení přístupu k internetbankingu u různých českých bank a také zjištění názoru českých uživatelů na bezpečnost internetového bankovnictví. K dosažení těchto cílů použiji klasickou metodu výzkumu pomocí dotazníku s uzavřenýma otázkami a také pomocí sémantického diferenciálu, která se založena na porovnání.

[1] http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf

1. POJEM ELEKTRONICKÉ BANKOVNICTVÍ

Elektronické bankovnictví jako pojem se do společnosti vžil pro elektronické označení komunikace mezi bankami a jejich klienty. Klient při vyřizování svých bankovních operací nepřichází do osobního kontaktu s pracovníky banky, ale provádí operace ze svého technického terminálu nebo z jiného dostupného zařízení. Je to trend, který jde ruku v ruce s rozvojem informačních a telekomunikačních technologií. To je i důvod proč elektronické bankovnictví nemůže mít přesnou, taxativně vymezenou definici. Jeho obsah se totiž aktuálně vyvíjí spolu s ostatními komunikačními technologiemi.

Charakteristické rysy služeb zařazovaných do oblasti elektronického bankovnictví jsou následující:

- k poskytování služeb dochází prostřednictvím elektronického kanálu,
- na jedné straně je klient s určitým technickým vybavením a na druhé straně je buď přímo automatický systém banky, nebo pracovník obsluhující tento systém,
- klient musí být při elektronické komunikaci vždy jednoznačně identifikovatelný a jeho právo vykonat požadovanou operaci je vždy ověřeno určitým autorizačním mechanismem,
- nejčastějšími operacemi jsou zde tuzemský platební příkaz a stav peněz na účtu.

Výhodou pro klienta je ušetřený čas /nemusí navštívit banku, nepřetržitý pracovní provoz/ a může s bankou komunikovat z různých míst. Banka rovněž ušetří, a sice na transakčních nákladech.

Nevýhodou pro klienta je nutnost mít a umět ovládat patřičné technické vybavení. Banka se v prvních fázích při zavádění patřičných systémů potýká s vysokými finančními náklady, problémem je rovněž nutnost jednoznačné identifikace klienta bez osobního kontaktu a vysoké nároky na bezpečnost komunikace.[2]

[2] http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm

2. VÝVOJ ELEKTRONICKÉHO BANKOVNICTVÍ

I když elektronické bankovnictví není zrovna nejnovější záležitostí, jeho historie také nepatří k těm nejbohatším.

Jako počátek elektronického bankovnictví se zpravidla považuje vznik debetních platebních karet, díky kterým jsou transakce účtovány téměř okamžitě nebo s minimálním časovým odstupem.

První platební karta byla vydána roku 1914 americkou telefonní společností Western Union Telegram Company. Zákazník díky ní mohl telefonovat a posílat telegramy a vyúčtování za služby dostal vždy až na konci měsíce. Tyto služby pak jednoduše zaplatil buď šekem, nebo jednorázovým příkazem z banky. Poskytováním „bezplatných“ služeb si společnost Western Union Telegraph Company snažila získat věrné zákazníky a přijmout je k častějšímu využívání služeb. Z tohoto důvodu se karty nazývají věrnostní.

Roku 1928 zavedly některé firmy plechové karty, na kterých bylo vyraženo jméno klienta a číslo karty, které se díky mechanice při placení otiskly na prodejní doklad.

Karty splnily svůj účel, lákaly lidi k častějším nákupům a bezhlavému utrácení peněz, které zastavila až Velká hospodářská krize roku 1929. Karty se znovu objevily na konci 30. let, na jejich dalším rozvoji měly zásluhu hlavně letecké společnosti. V roce 1936 se šest amerických leteckých společností domluvilo na projektu UATP, díky kterému zavedly úvěrové karty pro obchodní cestující. Ti mohli využívat služeb leteckých společností se značnými slevami.

Slibný rozvoj platebních karet sice zastavila druhá světová válka, ale v roce 1948 se karty UATP staly mezinárodně uznávanými.

V roce 1950 byla vyrobena první univerzální platební karta. S nápadem tuto kartu vyrobit přišel jako první Frank McNamara po nemilé zkušenosti se zapomenutou peněženkou v restauraci. Založil proto klub s názvem DinersClub. Tento klub poskytoval svým klientům úvěrové karty pro placení v restauracích a obchodech, s kterými měl klub uzavřenou smlouvu. Klub platil jídlo za své klienty a každý měsíc jim poslal vyúčtování se 14- ti denní splatností. Bohužel karta neměla žádný limit čerpání a společnost se po 3 letech ocitla ve ztrátě.

Obrázek 1: První platební karta na světě[3]

Avšak pravou bankovní platební karta byla vydána v roce 1951 v New Yorku Franklin National bankou. Byla vydávána zdarma důvěryhodným klientům, kteří na základě smlouvy spláceli své závazky buď do 30, 60 nebo 90 dnů. Karta nesla jméno svého držitele a výši limitu a při placení se u banky telefonicky ověřovalo finanční krytí. Od roku 1953-54 vydalo tuto kartu asi 100 bank, ale kvůli nezkušenostem ji v roce 1957 vydávalo už jen pouze 27 bank.

Plastové bankovní karty, jaké známe dnes, začala v roce 1959 vydávat Bank of America. Karty měly velký úspěch hlavně z hlediska bezpečnosti, bohužel kvůli neukázněnosti klientů splácet své závazky byly ze začátku velmi ztrátové. Tomuto pomohla politika George Waterse, který vynakládal velký tlak na neplatiče, zavedl nové postupy, ale hlavně zvýšil roční poplatky. Tyto karty už umožňovaly placení pomocí mechanických snímačů- imprinterů.

Protože byl projekt této banky úspěšný, poskytla jej v roce 1966 i ostatním americkým bankám a i bance ve Velké Británii. Díky tomuto se platební karty dostaly do podvědomí i v Evropě.

Ovšem první platební karta na území tehdejšího Československa byla vydána v roce 1988 Živnostenská banka jako dispoziční kartu k tuzexovému účtu a jako první banka u nás se stala členem mezinárodní společnosti a v roce 1991 vydala první VISA kartu u nás.

[3] *Pramen:* http://www.penize.cz/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti (Plischke, 2007)

Obrázek 2: První platební karta na území ČR

První platební kartu na našem území vydala ***v roce 1988*** *Živnobanka jako dispoziční kartu k* ***tuzexovému účtu****.*[4]

Od roku 1989 vydávala svým klientům Česká státní spořitelna ke sporožirovému účtu karty pro výběr z bankomatů. Tento rok také znamenal transformaci české ekonomiky z centrálně plánované na tržní a to se odrazilo jak v klasickém bankovnictví, tak i v zavádění moderních komunikačních kanálů v elektronickém bankovnictví.[5]

S nástupem techniky a jejím rozvojem ale vznikaly čím dál větší požadavky na přenášení informací. Začínaly se využívat dostupné prostředky pro vzdálenou komunikaci. První velkou změnu zaznamenal telefon. Ale nebyl to zrovna nejspolehlivější komunikační prostředek. Klient se identifikoval pouze jménem, známým hlasem nebo smluveným kódem a autentizace byla prováděna pomocí hesla. Později se začal používat fax. Pro

[4] *Pramen:* http://www.penize.cz/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti

[5] http://www.penize.cz/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti

zabezpečení identifikace se používalo jméno a číslo klienta, číslo účtu a pro autentizaci kódové tabulky. Technika ale nebyla nejdokonalejší a tak občas faxem vytištěné příkazy nebyly čitelné a jako prvek zabezpečování se zvolilo potvrzování telefonem, což bylo nepříjemné a klient musel v chybných případech reagovat přeposláním.

Revoluční zlom nastal logicky s používáním počítačů, které umožňují zpracovat téměř všechna data. Díky tomu vznikla myšlenka, proč přepisovat a tisknout data a nosit je následně do banky k dalšímu zpracování? Díky tomu začaly softwarové firmy připravovat komunikační programy.

V počátcích byla data přenášena pomocí tzv. kontrolních vět, což byly řetězce znaků se stanovenou strukturou se zabezpečovacím kódem pro ten daný den. První soubory se přenášely na disketách. Po disketách přišly na řady přenosy dat z počítače do počítače pomocí BBS (Bulletin Board Service) stanice.

Elektronický podpis odstartoval vznik složitějších programů, jejichž prostřednictvím banky mohou klientům nabízet větší a pohodlnější obsluhu svých účtů. Spektrum služeb se výrazně rozšířilo. Aby byla komunikace funkční, byly v bankách instalovány tzv. komunikační servery, pomocí nichž komunikace probíhá. Z bankovního systému jsou do nich přenášena data pro klienty a ti si je následně dle svých potřeb a možností stahují. Samozřejmě ale základní principy smluvních vztahů při vedení běžného účtu. Obsahové náležitosti příkazů a další zásady klasického bankovního platebního styku zůstávají i pro tuto formu bankovnictví zachovány. [6]

[6] *Pramen: Máče M., Platební styk klasický a elektronický, Grada 2006*

3. PROSTŘEDKY VZDÁLENÉHO PŘÍSTUPU

Prostředky vzdáleného přístupu jsou produkty umožňující využívat klasické bankovní produkty elektronickou cestou. Z hlediska podstaty těchto produktů se nejedná o produkty nové, pouze proces jejich sjednání, využití či ukončení se převedl plně či z části do elektronické podoby.

Produkty vzdáleného přístupu rozlišujeme podle následujících hledisek:

- **formy vzdáleného přístupu**- zdůrazňuje se forma komunikačního kanálu s bankou. V současné době se využívají zejména: platební karty, phonebanking, internetbanking, homebanking a GSM banking,
- **možnosti vzdáleného přístupu**- produkty platebního styku rozlišujeme na pasivní (umožňují pouze získávání informací od banky) a aktivní (navíc umožňují provádět i platební operace).

Tabulka 1: Realizace vzdálené komunikace klient- banka[7]

Způsob ovládání účtu	**Konkrétní realizace**
Elektronické (přímé) bankovnictví	Homebanking (pomocí komunikačních programů)
	Internetbanking (přes Internet)
Telefonní bankovnictví	Call centrum (živí operátoři)
	IVR (komunikace s hlasovým automatem)
	SMS zprávy
	GSM- SIM toolkit
	WAP

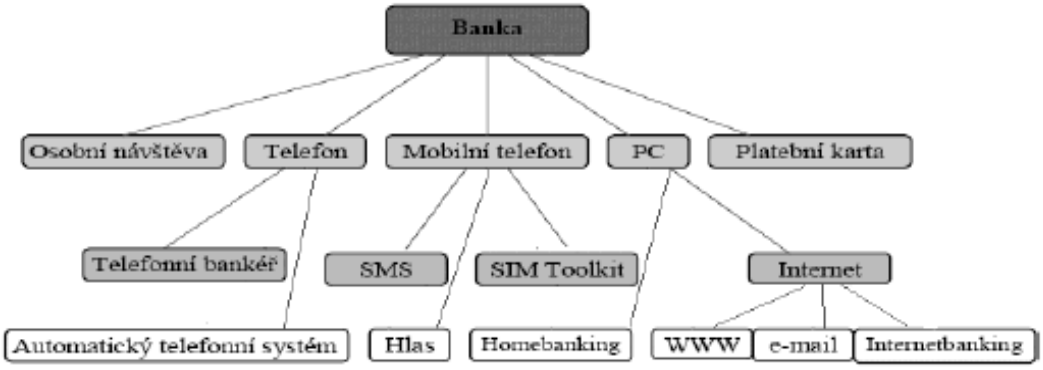
[7] *Pramen: Máče M., Platební styk klasický a elektronický, Grada 2006*

3.1 KOMUNIKAČNÍ KANÁLY ELEKTRONICKÉHO BANKOVNICTVÍ

Vzhledem k tomu, že rozdíly mezi poplatky za prováděné transakce na přepážkách banky a za transakce realizované pomocí přímého bankovnictví jsou markantní, banky vyloženě nutí své klienty k tomu, aby služeb přímého bankovnictví využívali čím dál častěji. Neznamená to ale pouze výhody pro klienty bank, ale také pro banky samotné. Díky využívání elektronického bankovnictví se výrazně snižují náklady bank, uvolňují se místa u přepážek a vede to k lepší osobní komunikaci mezi klienty a pracovníky banky.

Jako klienti se můžeme vybrat z jedné kombinace těchto distribučních kanálů.

Schéma č. 1: Možnosti komunikace s bankou



Pramen: Přádka M., Kala J., Elektronické bankovnictví, ComputerPress, 2000, str. 5

Obrázek 3: Možnosti komunikace s bankou

3.1.1. PLATEBNÍ KARTY

Platební karty jsou nejstarším a dnes i nejrozšířenějším způsobem, který umožňuje vzdálený přístup k účtu elektronickou cestou. Je to nástroj k bezhotovostní platbě. Na líce karty je uvedeno logo a název platebního systému, ke kterému daná karta náleží, logo banky, číslo karty, platnost a jméno držitele karty. Na rubu pak najdeme místo pro podpis držitele karty v tzv. podpisovém proužku a magnetický proužek. Platební karty se zpravidla vyrábějí z 3 vrstev netoxického PVC o rozměrech 85,6 x 54 x 0,76 mm. Tyto vlastnosti karty udává mezinárodní norma ISO 3554.

Podle technologie záznamu dat a systému ověření platby se karty dělí na elektronické, embosované, internetové a čipové.

3.1.1.1 Druhy platebních karet

Platební karty se dělí z různých hledisek a to zejména:

- dle způsobu zúčtování,
- dle způsobu provedení,
- dle vydávající asociace,
- dle použitelnosti,
- dle technologie.

Pokud jde o členění karet dle asociace, která kartu vydává. Mezi nejvýznamnější karetní společnosti patří: Maestro, VISA, Eurocard / Mastercard. Karty ale rovněž emitují společnosti jako Diner´s Club, American Express, Japan Credit Bureau, atd.

Ovšem základním kritériem pro členění karet je členění dle způsobu zúčtování, karty dělíme na karty:

- **debetní:** typ karty**, díky** kterému lze vybírat hotovost z účtu nebo platit u obchodníka, pokud je na účtu dostatek peněz. K zúčtování dochází téměř okamžitě po provedené transakce nebo maximálně do několika dní. Suma se odečítá přímo z účtu klienta.

- **kreditní:** umožňuje nákup zboží na úvěr. Úvěr se čerpá pomocí revolvingového (opakující se) úvěrového limitu, který automaticky obnovuje po splacení dlužné částky.
  Minimální výše splátky úvěru je bankou stanovena na 5-10% z dlužné částky a úvěrový limit je stanoven dle bonity klienta.

- **charge:** fungují obdobně jako kreditní karty. Při zúčtování, které je obvykle stanoveno k určitému datu (obvykle 14-30 dní) se musí jednorázově splatit celá dlužná částka. Výhodou je, že nebývá účtován úrok.

- **nákupní úvěrové:** jedná se o kreditní karty. Ty ale nejsou vydávány bankovními institucemi.

Dále karty členíme dle použitelnosti na karty:

- **domácí (tuzemské):** slouží k výběru z bankomatu nebo platbu u obchodníka na území dané země. Banky od jejich vydávání v poslední době upouštějí.
- **mezinárodní:** platí nejen na území dané země, ale i v zahraničí.

Podle způsobu provedení se karty dělí na:

- **embosované:** karty s tzv. reliéfním (plastickým) písmem. Tyto karty umožňují nákup i v prodejnách, které nejsou vybaveny elektronickým terminálem. Obchodník sejme pomocí imprinteru (mechanický snímač) otisk všech údajů vyražených na kartě a zákazník je potvrdí svým podpisem. S těmito kartami lze nakupovat ve více obchodech.

- **elektronické:** nejčastěji používané karty. Banky je většinou vydávají zdarma k účtu a jsou určeny pro výběr hotovosti z bankomatu nebo pro platbu u obchodníka s elektronickým platebním terminálem. Nevýhodou je zatím omezená použitelnost v prodejnách.

V současné době existují 3 způsoby technologií, podle kterých jsou karty vyráběny:

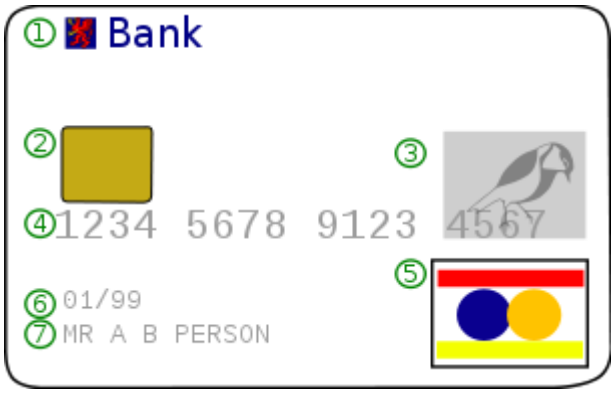
- **karta s magnetickým proužkem:** je na zadní straně karty a slouží jako médium pro záznam identifikačních údajů při elektronických transakcích. Tento proužek je složen ze tří stop, přičemž každá stopa má určenou strukturu dat a účel použití (např. jedná-li se o vnitrostátní, mezinárodní, offline nebo online transakci)

- **karta s čipem:** obsahuje zabudovaný kompresor s uloženými daty k identifikaci klienta. Sice je mnohem bezpečnější, za to existuje mnohem míň míst, kde s ní lze platit. Průkopníkem čipových karet byla Francie, v České Republice se čipová karta objevila až v roce 2002 u Komerční banky. V budoucnu by měly být čipem vybaveny všechny karty, díky tomu banky ponesou větší zodpovědnost za jejich zneužití.

- **hybridní karta:** obsahuje magnetický proužek i čip. Má výhody obou předešlých karet. Je bezpečnější a lze ji použít na všech obchodních místech. Je možné, že v budoucnu budou všechny platební karty vydávány jako hybridní.

3.1.1.2 Bezpečnost platebních karet

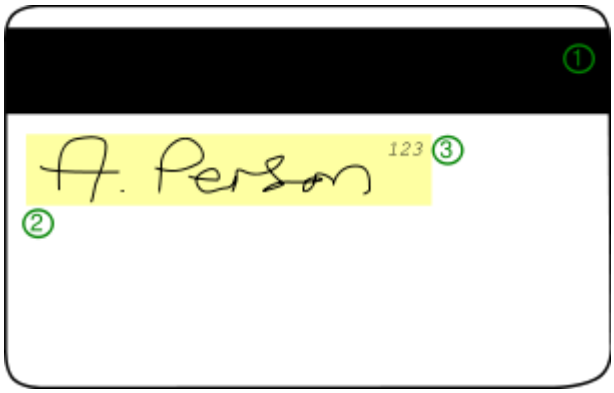
Základním ochranným prvkem karty je její číslo, které je jedinečné. Kromě tohoto kódu má každá karta ještě na zadní straně magnetický proužek, na kterém jsou uložena podstatná data. Jelikož většina uživatelů, kteří platí na internetu kartou, nemá čtečku platebních karet, je na kartě umístěn ještě jeden prvek. Tomuto prvku se říká Card Verification Value nebo Card Verification Code, zkráceně CVV nebo CVC. Užívá se pro zvýšení ochrany při elektronických platbách.



Obrázek 4: Bezpečnostní prvky na platební kartě

Bezpečnostní prvky na klasické platební kartě:

1. Logo banky
2. EMV čip
3. Hologram
4. Číslo kreditní karty
5. logo vydavatele karty
6. Platnost karty
7. Jméno majitele



Obrázek 5[8]: Zadní strana platební karty

Na zadní straně platební karty je zpravidla:

1. magnetický proužek
2. podpisový vzor
3. kód CVC

[8] http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta#Popis_a_ochrann.C3.A9_prvky

3D- secure

Díky 3D secure jsou elektronické platby v dnešní době už naprosto bezpečné. Umožňují ho dva největší vydavatelé platebních karet na světě MasterCard a VISA. Údaje z platebních karet se při nakupování na internetu zasílají zašifrované přímo do banky. Obchodníkovi nejsou tedy poskytovány žádné informace o zákazníkovi a zaniká zde riziko zneužití karty. Navíc zákazník, který má platební kartu se systémem 3D secure může proces autentizace rozšířit o další údaje, které zná pouze on sám a nikdo jiný tedy kartou zaplatit nemůže. Zákazník platící tímto typem karty je vždy automaticky vyzván k zadání dodatečných údajů, které si sám nastavil.

Zodpovědnost za transakci a její bezpečnost je plně na bance.

3.1.1.3 E-PENÍZE

„**Elektronický platební prostředek** je platebním prostředkem, který uchovává peněžní hodnotu v elektronické podobě a který je přijímán jako platební prostředek i jinými osobami, než jeho vydavatelem.“[9]

S nástupem internetu v 90. letech se vedle prvních pokusů o realizaci přímého bankovnictví začaly objevovat i první platební systémy (EPS). Všechny tyto systémy měly jedno společné- snažily se na trh uvést jakousi formu specifického elektronického platebního nástroje, který by umožnil převádět subjekty mezi sebou během jen několika vteřin, bez ohledu na skutečné hranice států. Jejich jedinou podmínkou bylo připojení k internetu.

Elektronické peníze neměly nikdy ambice nahradit skutečné peníze, měly je pouze nahrazovat při vykonávání malých finančních plateb, tzv. mikroplateb, kdy by použití skutečných peněz stálo velké transakční náklady. Elektronické peníze se tak staly potencionálními konkurenty již zavedených platebních nástrojů jako je šek, směnka, cestovní šek nebo, a to především! platební karta.

[9] Máče M., Platební styk klasický a elektronický, GRADA, 2006, s. 167

Elektronické peníze se dají rozdělit podle několika hledisek. Například podle jejich povahy je dělíme na:

- **token- based elektronické peníze**- jsou opravdovou virtuální kopií skutečných peněz. Jsou v předem definovaných hodnotách, které je třeba pro rozměnění poslat do vydávající banky. Každé minci je přidělena jedinečná číselná (registrační) hodnota, jejíž existence má zabránit tzv. doublespending efektu (možnosti použít jednu minci pro zaplacení dvakrát). Typický příklad je Ecash od firmy Digicash.

- **balance- based elektronické peníze**- jsou častější a v podobě kladného nebo záporného zůstatku na elektronickém účtu. Typickým příkladem je český internetový platební systém I LIKE Q.

Dále můžeme elektronické peníze dělit podle jejich implementace:

- **card- based elektronické peníze**- tyto peníze jsou uloženy na nějakém přenosném médiu, typicky to bývá karta obsahující mikročip. Tato karta zajišťuje různé kryptografické funkce a dá se s ní platit i v běžném životě. Příkladem jsou předplacené karty Mastercard a VISA.

- **software- based elektronické peníze**- spravují se přes software nainstalovaný v počítači nebo v PDA. Typické použití je přes síť nebo internet.

A také je dělíme podle povahy emitenta na:

- **nebankovní elektronické peníze**- jejich emitentem není banka a jako takové nepodléhají dozoru centrální banky,
- **bankovní elektronické peníze**- vydává je právnická osoba s bankovní licencí dle ustanovení §6 zákonu o bankách.

I když to na první pohled nemusí být dost jasné a e- peníze se můžou zdát jako skvělé řešení elektronických plateb, nesou s sebou také pár nevýhod. První nevýhodou je to, že abyste mohli e- peníze použít, musíte první převést vaše skutečné peníze, což může trvat i několik dní. Elektronické peníze prakticky neobíhají, některé oběhnou pouze jednou

a zanikají, díky už zmíněné obavě z doublespendingu. Elektronické peníze nejsou pojištěny a už vůbec nejsou úročeny.

3.1.2 TELEFONNÍ BANKOVNICTVÍ

Telefonní bankovnictví neboli phonebanking nebo také telebanking, se stalo po platebních kartách historicky druhou formou elektronického bankovnictví.

Telefonický platební styk je založen na komunikaci s bankou prostřednictvím telefonu tak, že klient komunikuje hlasem s živými pracovníky banky (telefonní bankéř) nebo tlačítky buď s živým operátorem nebo hlasovým informačním systémem IVR.

Klienti mohou tuto formu bankovnictví použít všude tam, kde normálně používají svůj telefon.

Služby telefonního bankovnictví nabízí ke svým produktům téměř všechny banky. Liší se o sebe nabízenými produkty a také poplatky za služby. Zatímco u některé banky si po telefonu zjistíme zůstatek účtu nebo pošleme peníze na jiný účet, u jiné banky po telefonu vyřídíme i to, co je možné pouze při návštěvě pobočky.

Bankovní operace (a to nejen při telefonním bankovnictví) můžeme rozdělit na *aktivní* a *pasivní*.

Obecně se dá říct, že *pasivní operace* prakticky nemění stav klientova účtu. Patří mezi ně údaje o bance a jejích produktech, ale také stav klientova účtu, transakční historie, atd.

Naopak aktivní operace se týkají účtu klienta. Patří mezi ně například příkazy k úhradě, atd.

Ve smlouvě o elektronickém bankovnictví si navíc klient sám rozhodne a podepíše nejen operace, které bude chtít realizovat prostřednictvím phonebankingu, ale také finanční limity pro určité období.

3.1.2.1 Rozdělení telefonního bankovnictví

Při využívání telefonního bankovnictví se vám nabízí dvě možnosti. Buď můžete své jednodušší požadavky vyřídit pomocí hlasového automatu, tzv. *IVR systému* anebo ty složitější operace vyřídit s pomocí živého pracovníka banky, tzv. *telefonního bankéře*. Pro banku bývá logicky finančně výhodnější automat.

Pokud klient využívá služby *Call centra*, žádá prostřednictvím telefonu operátora o vykonání dané transakce. Není třeba mít speciální vybavení, stačí vám jakýkoliv funkční telefon. Výhodou call centra je široká nabídka služeb. Ovšem pro banku je call centrum značně nevýhodné, zejména kvůli nákladům na jeho provoz. I přesto, že banky svá centra provozují téměř 24 hodin denně, 7 dní v týdnu v několika světových jazycích, snaží se své klienty motivovat k využívání telefonních automatů.

Interactive voice systém (IVR) je založen na vykonávání bankovních operací pomocí menu, z jehož nabídky si sami vybíráte pomocí tlačítek vašeho telefonního přístroje s tónovou volbou.

Po vstupu do menu jsou klientovi automatem přehrány jeho možnosti. Jedná se většinou o pasivní operace, ale spousta bank tímto způsobem provádí už i operace aktivní.

V menu bývá ale také možnost spojit se s telefonním bankéřem pro případ, že automat váš požadavek nebude umět vyřídit.

Samozřejmě, že tato možnost je velmi výhodná pro banky, co se týče nákladů, ale pro některé netechnické povahy klientů se může zdát také dost nevýhodná.

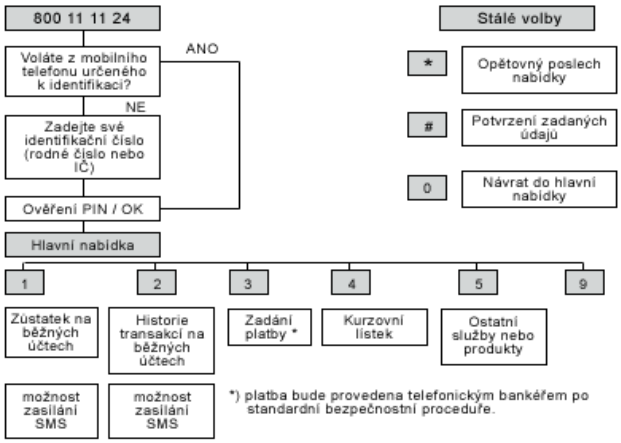
3.1.2.2 Bezpečnost telefonního bankovnictví

Zatímco při osobní návštěvě si může bankéř zkontrolovat osobní doklady klienta, při telefonním bankovnictví je třeba hledat jiné alternativy zabezpečení.

A banky proto používají různá zabezpečení proti zneužití. Přihlášení se do telefonního systému banky se skládá ze dvou částí: zadání identifikačních znaků klienta a osobního bezpečnostního hesla klienta. Pro zvýšení ochrany se u některých bank můžeme setkat s třístupňovým zabezpečením: identifikační číslo klienta, PIN a heslo.

Poté je klient vpuštěn u systému, díky kterému vyřídí své požadavky.

Po určité době si kvůli zvýšení bezpečnosti systém sám vyžádá změnu číselného hesla neboli PINu. Také je možné nastavit maximální limit pro převod peněžních prostředků. Navíc je každý hovor bankou z bezpečnostních důvodů nahráván.



Obrázek 6: Schéma menu u expresní linky Komerční banky[10]

3.1.3 GSM BANKOVNICTVÍ

Ani telefonní bankovnictví se nepřestalo vyvíjet a s příchodem digitálních technologií se dočkalo značných změn. Díky tomu vzniklo i GSM bankovnictví. GSM bankovnictví je založeno na komunikaci s bankou prostřednictvím mobilního telefonu prakticky kdykoliv a odkudkoliv.

GSM banking klientům umožňuje zadávat základní platební operace a zjišťování zůstatku na účtu, méně pak jim umožňuje zřizování trvalých příkazů a jiných složitějších operací.

Asi to je také hlavní důvod, proč není GSM banking natolik u klientů oblíbený jako Internetbanking nebo telefonní bankovnictví.

3.1.3.1 Rozdělení GSM bankovnictví a jeho bezpečnost

Mobilní telefon hravě poslouží klientovi při telefonním spojení ať už s telefonním bankéřem nebo s hlasovým automatem. Mobilní telefony ale také zvládají komunikaci pomocí textových zpráv SMS (short message service), technologie GSM SIM Toolkit anebo WAP.

[10] http://www.kb.cz/cs/seg/seg1/products/express_line.shtml

Na základě těchto technologií se rozděluje GSM bankovnictví:

- **GSM SIM Toolkit**- je velmi pohodlná a progresivní technologie. SIM Toolkit je softwarové rozhraní, které je nahráno v mobilním telefonu klienta a zobrazuje mu pouze ty služby, které má aktivovány. Celá aplikace je šifrována, takže se klient nemusí bát úniku informací, ani v případě zcizení telefonu. Bankovní transakce lze provádět po zakoupení speciální SIM karty a aktivaci na pobočce banky. Poté má klient kromě základního menu v telefonu zobrazeny i aktivní služby banky. Menu SIM Toolkit je zpracováno uživatelsky velmi přijatelným způsobem.

  Pro přístup ke službám bude nutný BPUK, který klient obdrží při aktivaci služeb na pobočce banky a díky kterému si založí vlastní BPIN, díky kterému se bude do aplikace přihlašovat. Pokud je ale BPIN třikrát po sobě zadán špatně, je přístup k bankovní aplikaci a citlivým položkám blokován. Pro odblokování slouží BPUK, pokud je ale i ten desetkrát po sobě zadán špatně, SIM karta již dále není pro bankovní operace použitelná.

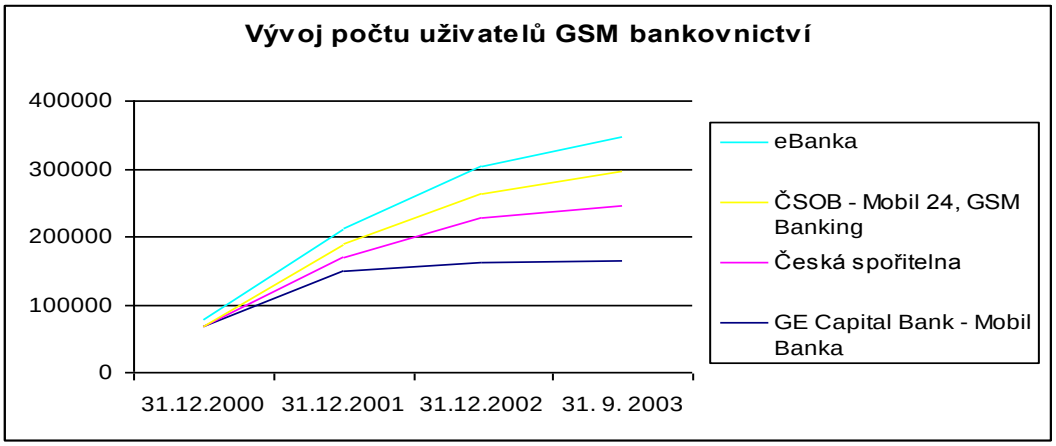
  Co se týče zabezpečení komunikace mezi uživatelem (mobilním telefonem) a serverem na straně banky, je bezpečnost zajišťována pomocí šifrování na principu tzv. symetrického šifrování. Tajný šifrovací klíč je používán na obou stranách komunikace.

  U GSM bankovnictví má jeden klíč k dispozici banka a druhý je uložen na SIM kartě uživatele. Tam jsou operace ještě navíc chráněny zadáním BPINu. Svoji funkci zde má i heslo BPUK pro případ, že by byla SIM karta zcizena.

- **SMS banking**- výhodou je použitelnost u všech mobilních telefonů a operátorů. Komunikace s bankou probíhá pouze prostřednictvím SMS zpráv. Klienti mohou bát o dění na svém účtu informováni buď automaticky, nebo na vyžádání. Díky SMS bankovnictví klienti mohou zadávat bance jak pasivní, tak i aktivní operace. Aktivní operace je ale nutno také zajistit proti zneužití. Jednou z možností je vydání speciálního kalkulátoru k aplikacím, který sám vygeneruje kód, který poté klient odešle bance přes SMS. Další možnost zabezpečení je pomocí elektronického klíče. Klíč se ale musí ke klientovi nějak dostat, čímž ale operátoři přetěžují svou síť.

Řešením může být klientovo trvalé napojení na speciální SMS centrum, založené jen pro účely SMS bankovnictví.

- **WAP banking-** tento druh bankovnictví se přibližuje spíše k internetovému bankovnictví, protože se do WAP (Wireless Application Protocol) prohlížeče musí zadat webová stránka banky, odkud je možné účet, po zadání přihlašovacího hesla a jména, ovládat. WAP je v podstatě obdoba internetových stránek bank. Protože používání WAP bankingu nezávisí na SIM kartě, ale na připojení přes GPRS, není realizace platebních operací nijak závislá na mobilním operátorovi. Bezpečnost zde závisí na přihlašovacím jméně a hesle a také opět na šifrování. Šifrování je zde ale na lepší úrovni, než kterou nám poskytuje SIM Toolkit. Přístup k internetu pomocí WAP není ale závislý pouze na mobilním telefonu. Tuto aplikaci nám poskytují i pagery, osobní digitální organizmy anebo palubní počítače osobních automobilů. WAP banking je tedy na pomezí GSM bankingu a internetového bankovnictví. Bohužel se ale moc neprosadil. Z počátku nebyly mobilní telefony na úrovni, aby poskytovaly kvalitní a rychlé připojení a v dobách, když už takové mobilní telefony máme, se objevily jiné a lepší druhy internetového bankovnictví, které jsou ve srovnání pořád rychlejší, efektivnější a hlavně levnější.



Obrázek 7: Vývoj počtu uživatelů GSM bankovnictví

Pramen: upravený graf dle údajů ze serveru Měšec.cz[11]

[11] ZÁMEČNÍK, P.: *Přímé bankovnictví na vzestupu.* Měšec.cz [on-line]. 2003. Dostupný na < http://www.mesec.cz/clanky/prime-bankovnictvi-na-vzestupu/> [cit. 2006-05-14]

3.1.4 HOMEBANKING

Homebanking (PC banking)je založen na propojení osobního počítače klienta, na kterém je nainstalován speciální program, s počítačem banky prostřednictvím datové sítě.

Protože je tato komunikace oboustranná, je zajištěn přenos dat od klienta k bance a naopak, dochází k velkým časovým a finančním úsporám.

Cesta k vytvoření homebankingu byla poměrně jednoduchá. Dříve se formuláře vyplňovaly osobně na pobočkách bank, což bylo neefektivní a nepraktické. Proto banky začaly do svých systémů své formuláře vkládat, klient si je pouze v pohodlí domova vytisknul a vyplnil a až poté je odnesl do banky. Tento způsob ale nebyl moc efektivní ani o moc úspornější. Hlavně kvůli tomu, že se úředníci nevyhnuli tomu, že data z formulářů museli i nadále do systému banky přepisovat ručně. Proto banky klientům poskytly počítačové programy, které jim umožnily zadávat transakce elektronicky a tyto informace uložit na děrný pásek, později magnetický pásek nebo disketu. S touto disketou přišel klient i s vytištěným, vyplněným a podepsaným formulářem do banky a úředník už pouze načetl data do systému banky z diskety. Tento způsob sice zjednodušil nahrávání dat do systému banky, ale stále ještě vyžadoval přítomnost klienta a úředníka na půdě banky. Navíc tento způsob mohli využívat pouze významní klienti.

Banky tedy klienty vybavily programem, který i v off- line režimu umožňuje zadávat informace o transakcích, ale místo uložení dat na disketu se klientův modem spojí s modemem banky a informace si navzájem vymění. Tento program umí přenášet data oboustranně. Protože ale klient už nemusí chodit do banky a podepisovat formuláře, je třeba také tento systém rádně zabezpečit. Za prvé je důležité autentizovat klienta, tzn. ověřit, zda ten, co se za daného klienta vydává, jím opravdu je. Za druhé je také potřeba, aby informace o požadovaných transakcích (či posledních provedených transakcích) nemohl nikdo přečíst ani modifikovat.

Homebanking nabízí jeden z nejlepších systémů zabezpečení ze všech forem elektronického bankovnictví. Přihlášení do bankovního systému probíhá pomocí hesla uživatele a autorizačního certifikátu. Celá komunikace mezi klientem a bankou probíhá přes kódovaný kanál.

3.1.4.1 Výhody a nevýhody homebankingu

Je jasné, že největší výhodou homebankingu je to, že pokud chceme provést jakoukoliv bankovní transakci, nemusíme kvůli tomu stát ve dlouhých frontách v bankách, ale všechno můžeme zařídit z pohodlí domova. Není to hlavní výhoda jen pro jednotlivce ale také pro firmy, které takové operace zadávají i několikrát denně. Homebanking tedy umožňuje vykovávat veškeré bezhotovostní transakce a také nám poskytuje dokonalý přehled o historii těchto transakcí.

Další výhodou je, že možnost propojení platebního styku s účetnictvím klienta. To znamená, že klient může automaticky platební operace zadávané do banky přeposlat i do svého účetního programu a zase naopak, z účetního programu na zpracování bance.

Výhodou také může být i propojení homebankingu s internetem. To znamená, že např. podnikatel před zahraniční cestou zadá na svém počítači před odjezdem příkazy k úhradě. Poté je možné v zahraničí po připojení se na internet a stvrzení transakcí elektronickým podpisem, příkazy odeslat do banky. Odpadá tímto povinnost mít u sebe jeden konkrétní počítač s bankovním programem.

Za hlavní nevýhodu homebankingu můžeme považovat to, že je vázán na konkrétní počítač, ale i to že pro instalaci a zacházení s programem je třeba aspoň špetka technologického talentu. Dále je také třeba modem nebo jiné připojení na Internet a i poplatky za připojení s bankou nejsou nejlevnější. Naštěstí je doba spojení velmi krátká, netrvá víc než několik desítek sekund, protože transakce je možné zadat do programu dopředu a s bankou se spojit už pouze na samotné odeslání dat.

3.1.5 INTERNETBANKING

Říká se, že mobilní telefony a internet odbourávají lidskou komunikaci. To by ale v bankovnictví nemuselo až tak moc vadit. A navíc internet jako celosvětová počítačová síť se sám jako komunikační kanál přímo nabízel. Z pohledu nákladů je internet vzhledem k jeho vysokorychlostnímu připojení, tím nejlevnějším způsobem spojení klienta a banky, co se nákladů týče. Transakce provedená tímto způsobem je několikanásobně levnější než transakce provedená např. přes telefon, a vhledem k pohodlí domova je úspornější i časově.

Internetové bankovnictví tedy znamená přístup k účtu pomocí internetu. Není zde potřeba žádný speciální software jako u homebankingu. Stačí vám k tomu pouze připojení na internet a internetový prohlížeč s technologií 128 bitového šifrování. To ale není žádný problém, protože v dnešní době mají počítače už standardně nainstalovány i výkonnější verze. Možná v dřívějších dobách se zdál jako problém i přístup k internetu, ale dnes s téměř všudypřítomným připojením WiFi už to není důvod k obavám. Navíc internetové připojení už dálno není otázkou velkých finančních nákladů.

V dnešní době je nepoužívání internet bankingu spíše bráno jako nevýhoda. A když už nemáte přístup k počítači s připojením na internet, alternativou jsou pro vás samoobslužné zóny.

Internetové aplikace bank se samozřejmě od sebe liší. Existuje ale jistý standard služeb, které vám přes internet poskytují téměř všechny banky:

- zadávat tuzemské i zahraniční příkazy k úhradě/ inkasu,
- kontrolovat historii pohybů na účtu,
- zadávat, měnit či rušit trvalé příkazy,
- zadávat jednorázové příkazy k úhradě,
- zobrazení zůstatku na účtu,
- elektronické výpisy zdarma.

3.1.5.1 Samoobslužné zóny

Jedná se o terminály, podobné bankomatům, které mají svůj vlastní operační systém. Nabídnou vám to co váš osobní počítač, pokud chcete využívat internetové bankovnictví. Oproti bankomatům jsou ale mnohem dokonalejší a umožňují nám vykonávat spoustu platebních operací. Tyto terminály jsou přístupné 24 hodin denně a umožňují provádění jako pasivních, tak i aktivních platebních operací. Pro přístup k těmto terminálům se využívá platební karta, pro provádění transakcí platební karta v kombinaci s autorizačním zařízením.

Jejich nevýhodou jsou ovšem ale velké náklady na jejich provoz a také vázanost k jednomu místu. Na druhou stranu je pro banku v určitých lokalitách výhodnější zřídit terminál, než pobočku.

Efektivnější ovšem je spojit terminál s bankomatem. Občané jsou zvyklí na výběry hotovosti z bankomatu a rozšíření služeb by určitě jen přivítali. Vzhledem ale k vysoké pořizovací ceně si myslím, že těchto zařízení nebude mnoho.

3.1.5.2 PDA bankovnictví

PDA je možnost být ve spojení s bankou kdykoliv a kdekoliv, která se vyvinula společně s vývojem telekomunikačních zařízení. PDA neboli Personal Digital Assistant je malý kapesní počítač, který nám krom jiného umožňuje i přístup do banky. Tuto službu zavedla jako první u nás eBanka v roce 2003. Je možné operace provádět pomocí jakéhokoliv kapesního počítače, který má přístup na internet. Jediné omezení je zde z hlediska bezpečnosti. Proto podmínkou je internetový prohlížeč podporující protokol SSL (Secure Sockets Layer), který zabezpečuje přenos dat sítí internet s pomocí šifrování.

Možnosti zjednodušené bankovní aplikace jsou široké, ne ovšem kompletní. Prostřednictvím PDA můžeme provádět tyto platební operace:

- historie účtu a zůstatek na účtu,
- historie blokace platebních karet,
- zadání a přehled jednorázových platebních příkazů,
- zadání a přehled trvalých platebních příkazů,
- založení termínovaného vkladu,
- založení revolvingového termínovaného vkladu,

- přehled termínovaných vkladů.

Přihlašování do systému probíhá jako u klasické internetové verze přes klientské číslo a přístupový kód. Samotné prohlížení účtu je ale odlišné. Je totiž založeno na autentizaci každé stránky, do které chcete vstoupit. To znamená, že nestačí zadat klientské číslo a heslo jen jednou, ale pokaždé když chcete vstoupit do nové stránky. Toto omezení bylo ale také jediným řešením jak zajistit kompatibilitu pro všechny typy kapesních počítačů bez nutnosti dalších instalací.

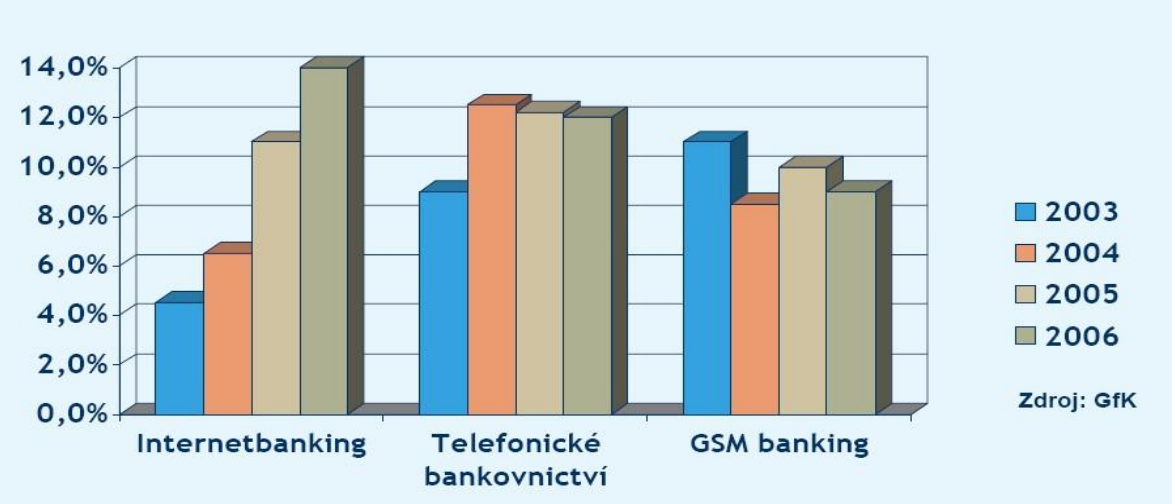
Obrázek 8: PDA banking[12]

..

[12] http://www.arbes.com/en/products/obs/modules/mobile/img/bog_pda_card_full.png

3.1.6 Srovnání využívání komunikačních kanálů elektronického bankovnictví

V následujícím grafu můžeme porovnat využívání komunikačních kanálů elektronického bankovnictví od roku 2003 do roku 2006. Můžeme vidět, jak postupem času lidí plynule upouštěli od používání GSM bankingu a postupně začínali využívat služeb moderní techniky, a to internetbankingu.



Obrázek 9: Nejužívanější kanály přímého bankovnictví od roku 2003 do roku 2006

Zdroj: http://www.csob.cz/WebCsob/Csob/Servis-pro-media/PB_CSOB_ELB_vysledky_studie_NMS.pdf

4. BEZPEČNOST ELEKTRONICKÉHO BANKOVNICTVÍ

I přestože má elektronické bankovnictví své nesporné výhody, musíme se zamyslet i nad tím, že jeho užívání sebou nese značná rizika, která se musí eliminovat. Tato rizika se týkají zejména dostatečného zabezpečení přístupu k účtu, zamezení proti zneužití neoprávněnou osobou, bezpečný přenos dat ale také zejména bezpečné chování uživatelů elektronického bankovnictví.

Vzhledem k velkému počtu uživatelů elektronického bankovnictví, patří otázka bezpečnosti mezi hlavní priority bank. Banky díky elektronickému bankovnictví šetří své náklady, a čím více důvěry od klientů se jim dostane, tím lépe na tom budou finančně. Bohužel jsou při výběru jednotlivých bezpečnostních prvků ovlivňovány mnoha faktory, mezi které patří mimo jiné i jednoduchost, funkčnost, ovladatelnost, důvěryhodnost, rychlost a v neposlední řadě i cena.

Je zřejmé, že se tyto faktory částečně vylučují, banky tedy musejí hledat optimální rovnováhu, která bude nejlépe vyhovovat jí samotné ale také klientům.

V dnešní době se za běžný standard považuje monitorování veškerých aktivit v systému, což představuje ochranu proti nejslabšímu článku systému- člověku.

4.1. Hlavní způsoby zabezpečení

Základním a hlavní úkolem zabezpečení elektronického bankovnictví je ověření totožnosti člověka, který žádá o přístup. Jedná se tedy o identifikaci a následnou autentizaci osoby.

Identifikace spočívá v rozpoznání identity systémem na základě určitého identifikátoru. Je spojena s osobou uživatele, reprezentuje ji a je známa i jiným osobám. Zpravidla se jedná o jméno a příjmení.

Autentizace znamená prověření proklamované identity osoby, lze ji provést pomocí:

- hesla; elektronického klíče; certifikátů; biometrických vlastností: otisky prstů, struktura duhovky, analýzy hlasu.[13]

[13] ŘÍHA, Daniel. *Elektronické bankovnictví*. [s.l.], 2006. 59 s. Bakalářská práce. Masarykova univerzita v Brně.

5. ELEKTRONICKÉ BANKOVNICTVÍ V ČESKÉ REPUBLICE

Vzhledem k tomu, že máme mnoho komunikačních kanálů elektronického bankovnictví, zaměřila bych se v následující části pouze na ty nejvíce využívané. Mezi ně patří bezpochyby platební karty a internetbanking.

5.1 PLATEBNÍ KARTY V ČESKÉ REPUBLICE

V dnešní době je v České republice používání platebních karet poměrně rozšířené pro výběr hotovosti z bankomatu a bezhotovostní platbu za zboží a služby. Nejrozšířenější kartové společnosti jsou Eurocard/ Mastercard a VISA. Debetní kartu má více než 61 % obyvatel starších 15 let, kreditní kartu více než 5 % obyvatel. V České republice se nachází zhruba 3 500 bankomatů a na cca 50 000 místech je možno platit kartou.[14]

5.1.1 Bezpečnost platebních karet a jejich dostupnost v ČR

Není takového platebního prostředku, aby k němu neexistovaly padělky a nedělaly se s ním podvody. Naštěstí situace v České republice byla vždy díky infrastruktuře, pomalu a ohleduplněji se rozvíjejícího trhu a mezibankovní spolupráci lepší než v jiných zemích. Již v r. 1992 se podařilo prosadit do trestního zákona ustanovení o trestnosti padělání platebních karet, jejich neoprávněného držení a podvodů s nimi.

[14] ŽÁKOVÁ PETROVÁ, H.: *Finanční služby v České republice: průvodce pro cizince*. 1. vyd. Praha : Multikulturní centrum Praha, o.s., 2006. 50 s. ISBN 80-239-6725-8. Dostupné i online na URL <http://www.migraceonline.cz/finance/cestina.pdf>

Tabulka 2: Podezřelé transakce- procentní body a basis points (BP)

Rok	2001	2002	2003	2004	2005	2006	2007 (1. pol.)
ČR -%	0,073	0,057	0,064	0,040	0,013	0,027	0,023
ČR - BP	7,3	5,7	6,4	4	1,3	2,7	2,3
Evropa - BP						8,6	8,4

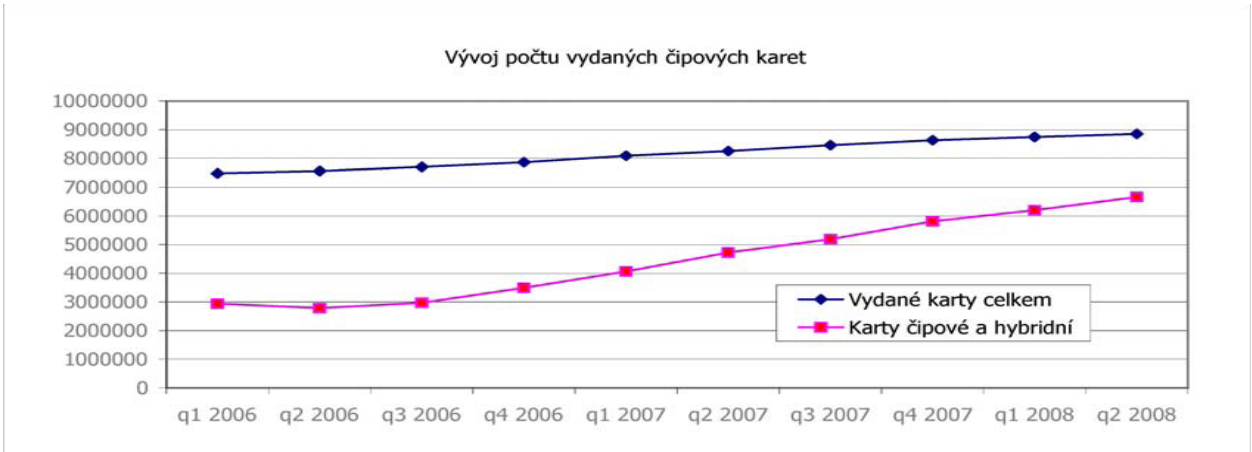
Procentní body vyjadřují poměr celkového objemu podvodných případů, nahlášených vydavatelskými bankami, k celkovému objemu obratů uskutečněných v akceptační infrastruktuře u obchodníků a v síti bankomatů na území ČR kartami MasterCard a VISA. Výši skutečných finančních ztrát vzniklým bankám nebo obchodníkům v ČR se zmíněnou a včasnou spoluprací daří v mnoha případech významně snížit.[15]

Podívejme se ale i na dostupnost těch nejbezpečnějších platebních karet v České Republice. V současné době jsou v České republice asi nejdostupnější tzv. čipové a hybridní karty. Co se ale týče bezpečnosti, můžeme brzy očekávat i bezkontaktní karty, díky jejichž technologii nemusíte při placení vydávat kartu z rukou s díky tomu také zamezit jejímu možnému zneužití. Tento typ karty už je u českých bank k dostání. Bohužel dostupnost terminálů na tento typ placení je momentálně velmi nedostačující. Hudbou budoucnosti u nás je zřejmě autentikační karta s biometrií i čtyřfaktorová autentifikace. K ověření autenticity slouží 4 faktory a to:

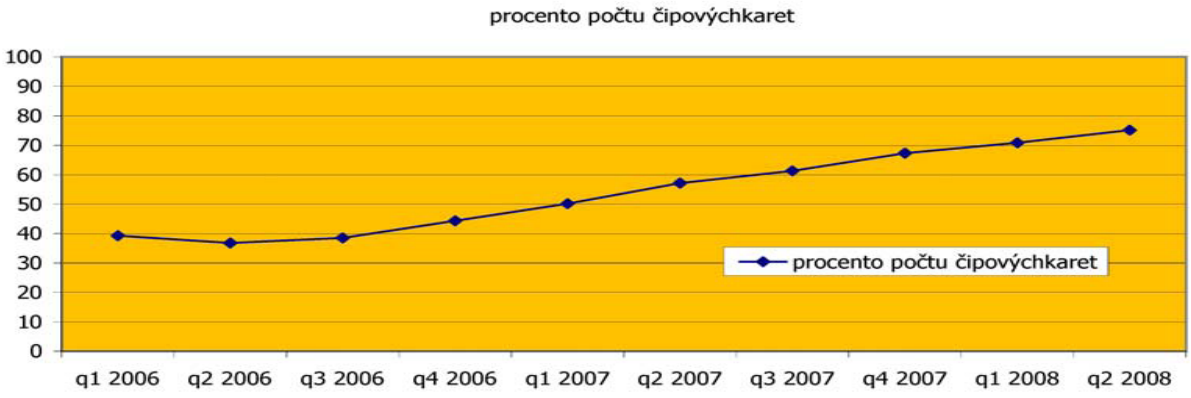
* co máte (kartu, podpis),
* co víte (PIN),
* co získáte jako jedinečný prvek (dynamický PIN, jednorázové heslo),
* čím jste (biometrický znak).

[15] http://www.bankovnikarty.cz/pages/czech/profil_cr.html

Pod značkou MobilKey je nabízena karta, nabízející všechny tyto faktory, přičemž biometrickým znakem je otisk prstu. Otisk je snímaný dynamicky na specielní čtečce umístěné na kartě.[16]



Obrázek 10: Vývoj počtu vydaných čipových karet



Obrázek 11: Procento počtu čipových karet[17]

[16] http://cardmag.cardzone.cz/archiv/cm1_2009.pdf
[17] http://cardmag.cardzone.cz/archiv/cm1_2009.pdf

5.1.2 Vydávání platebních karet v ČR

V České Republice jsou vydávány převážně karty systémů MasterCard a Visa. Následující tabulka zahrnuje i karty American Express, Diners Club a karty společnosti CCS vydané v ČR.

Tabulka 3: Počty vydaných platebních karet

Počty vydaných karet	**2005**	**2006**	**2007**	**2008**	**2009**
Počet karet celkem	7 390 357	7 865 227	8 623 124	8 931 872	9 054 308
z toho čipové	2 830 302	3 488 627	5 811 912	7 242 426	7 891 543
kreditní (včetně charge)	971 911	1 261 606	1 648 977	1 711 205	1 681 981
debetní	6 418 446	6 603 621	6 974 147	7 220 667	7 372 327

5.1.3 Využívání platebních karet v ČR

Následující údaje charakterizují používání platebních karet českých vydavatelů k platbám u obchodníků a výběrům hotovosti v bankomatech a to a jak v ČR, tak v zahraničí.

Tabulka 4: Využívání platebních karet v ČR[18]

Platby kartou u obchodníků:	**2005**	**2006**	**2007**	**2008**	**2009**
Počet plateb	99 756 686	116 890 828	137 899 579	169 254 912	194 231 582
Objem plateb (tis. Kč)	114 584 198	133 746 846	155 830 892	188 964 124	200 924 496
Průměrná platba (tis. Kč)	1,149	1,144	1,130	1,116	1,034

[18] http://cardmag.cardzone.cz/aktual/pages/0_karty_v_cislech.html

5.1.4 Podvody na platebních kartách v ČR

- Podvody ztracenou nebo zcizenou kartou: jsou podvody, kdy se originální platební karta dostala mimo fyzickou kontrolu oprávněného držitele. Podvodník se snaží použít odcizenou nebo nalezenou kartu stejně jako oprávněný držitel. Někdy se podvodník ani nesnaží napodobit podpis, jindy využívá i odcizených nebo padělaných osobních dokladů držitele karty.

Občas dochází i k podvodnému zadržení karty a to cíleným nevrácením karty ze strany obchodníka či umístěním zařízení před či přímo do čtečky bankomatu, které kartu zadrží (tzv. libanonská smyčka).

Zneužití ztracené či zcizené karty patří v České republice mezi nejčastější kartové podvody.

- Podvody padělanou kartou: padělaná karta je karta, která byla vyrobena a personalizována bez souhlasu vydavatele nebo taková, která byla právoplatně vydána, ale později byla vizuálně upravena nebo byla pozměněna její elektronická data.[19]

Jedním ze způsobů padělání karet je tzv. skimming, což je postup, při kterém jsou údaje o kartě zkopírovány z magnetického proužku na jinou kartu bez vědomí právoplatného držitele karty. V prvním kroku se data zkopírují a ve druhém se nahrají na novou padělanou kartu. Tohle se nejčastěji děje:

- u obchodníků, kde nepoctivý pracovník obchodní společnosti zkopíruje obsah magnetického proužku před vrácením karty zákazníkovi, a poté získaná data využije nebo předá dále k výrobě padělané karty,
- u bankomatu, kde podvodníci umístí speciální kopírovací zařízení, které zkopíruje všechna data z magnetického proužku karty.
-

Tento druh podvodu se v posledních letech objevuje na území České republiky stále častěji. Z dosavadních zkušeností vyplývá, že ke zkopírování údajů z magnetického proužku karty dochází nejčastěji u bankomatů, v barech, restauracích, u čerpacích stanic a

[19] http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Druhy_podvodů

někdy i v hotelech. Při odhalení neoprávněné transakce kontrolou výpisu či na základě upozornění vydavatelem může být oprávněný držitel karty vyzván k jejímu odevzdání za účelem dalšího vyšetřování.[20]

- Podvod bez přítomnosti karty: je to typ podvody, kdy platební karta nebo držitel karty nejsou fyzicky přítomni na místě transakce. Podvodníci využívají získaná data k provedení nákupu pomocí písemné, telefonní, faxové nebo internetové objednávky. Vzhledem k tomu, že obchodník nemá možnost fyzicky zkontrolovat kartu, je tento typ podvodu velmi oblíbený. Podvodníci obvykle data o kartě získávají ze zahozených nebo zkopírovaných potvrzení o transakcích, jejich podvodným vyžádáním např. e-mailem (phishing), z fiktivních internetových obchodů, vykrádáním databází s údaji o provedených transakcích (database hacking), apod. Obdobně jako u podvodu padělanou kartou se právoplatný držitel karty o podvodu nedozví, dokud neobdrží výpis s rozpisem transakcí.
- Podvody se zcizenou identitou: dochází k ní podvodně získaných osobních údajů. Podvodník může s pomocí zcizených osobních údajů zažádat o otevření účtu či vydání karty. I přestože se tento druh podvodu v České Republice téměř nevyskytuje, ve světě jeho četnost neustále narůstá.
- Vishing: s rozvojem zákaznických center, vybavených automatizovanou hlasovou službou a s tím, jak si zákazníci zvykli na jejich automatické telefonní odpovídače, se i podvodníci posunuli na vyšší technologickou úroveň. Snaží se vylákat důvěrné informace po telefonu, hlasem, proto se mu dostalo označení vishing (voice + fishing).[21] První zprávy o této metodě se datují už od června roku 2006, ale v loňském i letošním roce jsou zaznamenány stále častější podvody v anglicky mluvících zemích a je jen otázkou, kdy se dostane i do České Republiky.
- SmiShing: Dalším vývojovým krokem v obalamutění spotřebitelů je využívání mobilních telefonů k zasílání textových zpráv (SMS) s obdobným varováním a výzvou, aby klient zavolal na určené telefonní číslo. Název je odvozen z „sms phishing“.[22] Lze použít jak k vylákání čísla karty, tak čísla účtu, spolu s doplňujícími informacemi, jako je PIN, adresa, rodné číslo nebo číslo sociálního pojištění, apod. Záminka ke zpětnému telefonátu může být různá: pokus o zneužití

[20] http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html
[21] voice- z anglického slova hlas, fishing- z anglického slova rybařit, chytat ryby
[22] sms- short message service, phishing- podobně jako fishing

čísla účtu/karty nebo přijetí refundace na dříve provedenou transakci. Tyto podvodné pokusy se tváří velmi realisticky, protože často obsahují varování před vyzrazením osobních informací, což u napadené osoby vyvolá přesvědčení, že jej skutečně volá jeho banka/finanční instituce. U libovolné záminky je navíc zdůrazněna naléhavost zpětného volání upozorněním na poplatek, např. 2 USD za den, pokud nebude záležitost vyřešena.[23]

Podvody s platebními kartami se také liší podle místa uskutečnění na:

- **Podvody u obchodníka**:
    - Skimming- je typ podvodu, při němž jsou údaje o kartě z magnetického proužku zkopírovány na jinou kartu bez vědomí držitele. Pracovník obchodní společnosti může během platby použít miniaturní zařízení ke zkopírování údajů o kartě, které dále slouží k platbám bez přítomnosti majitele nebo k výrobě padělané karty. Ke skimmingu nejčastěji dochází v barech a restauracích, na čerpacích stanicích nebo v hotelech. Podvodníci se obvykle i kromě údajů na magnetickém proužku získat i PIN. Ke skimmingu může dojít i na jiném místě než na prodejně. Například lidé převlečení za příslušníky policie předstírají, že kontrolují pravost karet. Ve skutečnosti používají miniaturní skimmovací zařízení a požádají i o sdělení PINu.

    - Transakce neautentikovaná držitelem karty- neautentikovaná transakce je transakce provedená bez vědomí jejího držitele. Kdokoliv se dostane k údajům o kartě, může iniciovat platbu bez vědomí držitele. K neautentikované transakci může dojít zároveň s oprávněnou transakcí za přítomnosti platební karty i jejího držitele, kdy pracovník společnosti může nepozorovaně provést transakci na stejnou nebo i jinou částku (tzv. multiple imprint).

[23] http://cardmag.cardzone.cz/archiv/cm1_2010.pdf

- Terminál a PIN- natypování PINu je autentifikační procedura, která ověřuje oprávněnost držitele k použití karty. Jde o doplnění nebo nahrazení autentifikace podpisem. Je totiž velmi snadné PIN při zadávání odpozorovat nebo držiteli podstrčit jinou klávesnici. Tento typ podvodu ale nelze uskutečnit bez přítomnosti karty.

- **Podvody u bankomatu:**
  - Skimming u bankomatu-tento druh podvodu patří v současnosti k nejzákladnějším u bankomatu. Podvodníci často umístí speciální čtecí zařízení před štěrbinu čtečky magnetického proužku v bankomatu. Ilegálně nainstalovaná kamera je umístěna nad klávesnicí a snímá PIN. S padělanou kartou potom můžou podvodníci provádět stejné transakce jako její právoplatný držitel.

  - Zařízení na zachycení karty- podvodník vloží do štěrbiny čtečky karty zařízení, které zachytí a zadrží kartu klienta. Podvodník vystupuje jako náhodná kolemjdoucí osoba, která se snaží majiteli karty pomoci a vyzve ho k opětovnému natypování PINu a zapamatuje si jej. Jakmile klient vzdá další pokusy o navrácení karty a odejde, podvodník vyjme celé zařízení i s kartou. Neoprávněný výběr hotovosti uskuteční podvodník téměř okamžitě, dříve než klient nahlásí danou událost své bance. Mohou nastat situace, kdy je karta v bankomatu zadržena z kvalifikovaných důvodů. Držitel karty je však o tom vždy informován prostřednictvím obrazovky bankomatu.

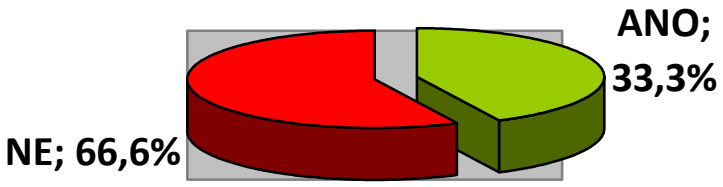
  - Uchovávání PINu v blízkosti karty- tohle je snad základní chyba, které se držitelé platebních karet dopouštějí. Pokud třeba například zloděj odcizí celou tašku nebo peněženku, nic už mu nebrání ve zneužití platební karty, pokud má majitel poznamenaný PIN někde v její blízkosti.

5.1.5 Bezpečnost platebních karet z pohledu uživatele

Součástí mé práce je i výzkum zaměřený na bezpečnost platebních karet z pohledu uživatele. Při hledání informací k mé práci se mi nikde nepodařilo najít informace o tom, jaké zabezpečení platebních karet nabízejí české banky. To ve mně vzbudilo zvědavost, jestli jsou uživatelé platebních karet dostatečně informováni o jejich bezpečnosti. Tímto nemám na mysli PIN kód a hesla, která používají při placení platební kartou, ale jestli uživatelé znají technologie zabezpečení jejich karet.

Zeptala jsem se tedy 30 uživatelů platebních karet ve věku v rozmezí od 20 do 50 let, jestli jsou si vědomi toho, jak je platební karta, kterou skoro denně používají zabezpečena. Výsledek výzkumu mě nijak zvláště nepřekvapil.

Výsledky ankety na otázku: Víte, jak je Vaše platební karta zabezpečena z pohledu technologie?



Obrázek 12: Výsledky ankety se zaměřením na bezpečnost platebních karet

Celá jedna třetina dotázaných neměla ani ponětí o tom, že existují nějaké platební karty s magnetickým proužkem, čipové či hybridní. A když si zakládali bankovní účet, tak je ani nenapadlo se v bance zeptat na zabezpečení jejich platební karty. Ti dotázaní, kteří odpověděli ANO, ale zároveň uvedli, že se na zabezpečení jejich platební karty museli zeptat sami ze své vlastní vůle. Pouze jeden jediný člověk potvrdil, že mu bezpečnost platební karty popsala a tu nejbezpečnější mu nabídla sama banka. Nabízí se tedy otázka, zda se klienti sami ochuzují o informace spojené se zneužíváním jejich bankovních účtů a následné ztrátě financí nebo jestli by neměla banka sama klienty o možnostech zabezpečení informovat. Je totiž všeobecně známo, že nedostatek informací způsobuje

většinu špatných rozhodnutí a následně i problémy s nimi spojené. Je totiž nelogické zajímat se o zabezpečení platebních karet až potom, co o peníze přijdeme.

5.2 ZABEZPEČENÍ INTERNETOVÉHO BANKOVNICTVÍ V ČECHÁCH

Používání internetu v bankovním styku se stalo fenoménem posledních let. Každá z bank nabízí vlastní formu internetového bankovnictví, která je podle nich zaručeně bezpečná vůči zneužití.

Bezpečnost internetového bankovnictví zahrnuje 3 aspekty: identifikaci banky, identifikaci klienta a zabezpečení přenosu dat. Identita banky je ověřována certifikátem, který vydává nezávislá instituce. Klient tak má jistotu, že stránky, díky kterýmž komunikuje s bankou, patří skutečně jí. Přenos dat je ve všech bankách řešen šifrováním na vysoké úrovni a lze jej považovat za dostatečně bezpečný.

Poslední část zabezpečení, identifikace klienta banky, je nejvíce viditelná a rozhoduje i o uživatelském pohodlí aplikace. Nejčastěji se používá zabezpečení pomocí uživatelského jména a hesla nebo certifikátem uloženým v souboru. Pokud banka využívá bezpečnější zabezpečovací systémy jako např. autentizační kalkulátor, jsou často brány jako nadstandardní a banka si za jejich používání nechává zaplatit. To může znamenat i to, že je klienti nepoužívají v tak hojné míře. Obecně totiž platí, že klienti preferují větší pohodlnost služby a to i za cenu menší bezpečnosti. Čím vyšší je totiž bezpečnost, tím menší je komfort pro klienta.

5.2.1 Základní úrovně ochrany

V České Republice neexistuje produkt internetového bankovnictví, který by byl zcela nezabezpečený. Banky dávají klientovi na výběr jaké riziko je ochoten podstoupit a kterou metodu zabezpečení přijme. Zájem o nadstandardní prostředky zvyšující bezpečnost není mezi klienty bohužel velmi velký a to zřejmě kvůli poplatkům.

Uživatelské jméno (číslo) a heslo:

S ohledem na jednoduchost je bohužel téměř jisté, že tento způsob přihlašování je nejméně bezpečný. Vše, co útočník potřebuje je pouze ono heslo a uživatelské jméno. Pokud je počítač napaden škodlivým kódem (keylogger), který pozná druh klávesy podle stisku, lehce už jej pak pošle útočníkovi. Pokud navíc není nutnost následnou platbu autorizovat, jedná se o velké riziko. U některých bank je bezpečnost zvýšena tzv. grafickou klávesnicí, při níž se používá myš. I tento způsob zabezpečení umí bohužel monitorovat počítačový vir trojský kůň.

Pokus si klient zvolí tento základní způsob zabezpečení, měl by se informovat o doplňujících možnostech bezpečnosti, jako jsou například denní limit, automatické zasílání SMS při zadání jakékoliv aktivní platební operace nebo při změně zůstatku účtu, možnost poskytování informací o provedených finančních transakcích (prostřednictvím e-mailu, SMS nebo faxu).

Autorizace SMS klíčem:

K potvrzení každé peněžní transakce banka klientovi odešle klíč na předem zaregistrované telefonní číslo. Pro každou transakci banka klientovi pošle nový SMS klíč. Téměř u každé české banky je tento klíč pro používání internetového bankovnictví nutný. Výhodou je i to, že pokud se podvodník naboural do účtu klienta banky, potřebuje k provedení transakce i klientův mobilní telefon.

U Komerční banky se například ale jedná o statický klíč, který platí po celou dobu přihlášení uživatele do internetbankingu. Znamená to, že stejný autorizační kód zadá při prvním, ale i při posledním příkazu k úhradě. To s sebou přináší riziko, že tento kód může být odposlechnut a následně zneužit.

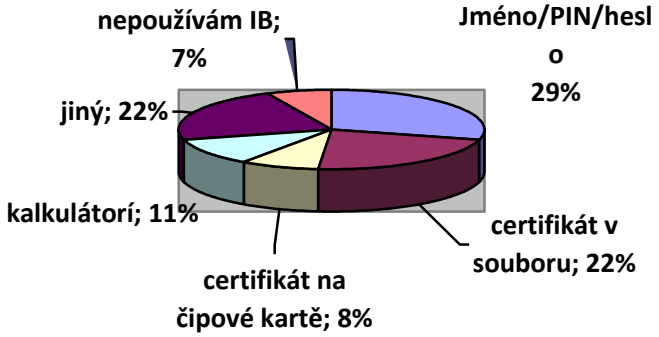
Elektronický podpis:

Elektronickým podpisem rozumíme tzv. osobní certifikát klienta, který je uložený na přenosném médiu nebo na čipové kartě. Tento způsob klade vyšší požadavky na bezpečnost při uložení a používání certifikátu. Základním pravidlem je to, že certifikát by neměl být nikdy uložen na disk počítače, ale klient by jej měl mít na externím disku (disketa, CD, USB disk), které by mělo být používané pouze v případě přístupu k účtu.

Vyšší bezpečnost klientovi poskytuje certifikát uložen na čipové kartě. K tomuto druhu je ale za potřebí pořízení si čtečky čipových karet. Výhodou je nemožnost odcizení osobního klíče klienta bez odcizení čipové karty, jelikož klíč nelze z karty vyexportovat.

Elektronický kalkulátor:

Mezi další bezpečné systémy patří kalkulátory, které pokaždé vygenerují originální přístupový kód pro potvrzení transakcí. Není nutná instalace do počítače, klient si pouze pořídí zařízení v podobě „kalkulačky“, která je přenosná a je chráněna čtyřmístným heslem. Po zadání hesla a stiskem tlačítka zařízení samo vygeneruje šestimístný kód, který je nutný v internetbankingu zadat při každé aktivní transakci.



Obrázek 13: Využívání úrovně zabezpečení internetbankingu[24]

[24] Dle ankety ze serveru http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/

5.2.2 Způsoby zneužití internetbankingu

Většina naší populace myslí, že právě jim se podvod na jejich bankovním účtu vyhne. Bohužel to ale nejsou právě účty miliardářů, které bývají nejčastěji zneužity. Hackeři[25] svá mnohdy milionová konta sbírají z účtů drobných střadatelů, kteří si bohužel většinou svou finanční ztrátu zaviní sami svou neopatrností a důvěrou.

- Phishing**:** Slovem PHISHING označujeme podvodné e-mailové útoky na uživatele Internetu, jejichž cílem je vylákat důvěrné informace. Nejčastěji jsou to údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům. Nemusí jít jenom o účty přímo bankovní, ale také ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužit jejich služeb. Příkladem může být PayPal, eBay, Skype, Google. Uživatelům internetbankingu přijde důvěryhodně se tvářící e- mail, který vypadá jako od banky. Nabádá k přihlášení se za nějakým účelem na té a té internetové stránce. Stránka se také tváří důvěryhodně a klient na ni z toho důvodu zanese požadovaná data, aniž by si uvědomoval, že od té chvíle má hacker nad jeho účtem absolutní moc. Ještě nedávno klientům banky hradily takové ztráty ze svých účtů, bohužel v současné době se tento fenomén tak rozšířil, že se tímto způsobem ročně ztratí miliony až desítky milionů korun. Banky proto jakoukoliv zodpovědnost odmítají.
    - ZÁKLADNÍ ZNAKY PHISHINGOVÉHO E-MAILU:

1. Snaží se vyvolat dojem, že byl odeslán organizací z jejichž klientů se snaží vylákat důvěrné informace. Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.
2. 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.
3. V textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky organizace (banky). Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěné podvodné stránky.
    - Jestliže vám chodí jménem banky e-maily, které obsahují link, na stránky vyžadující vaše přihlašovací údaje, či údaje ke kartě, je to phishingová

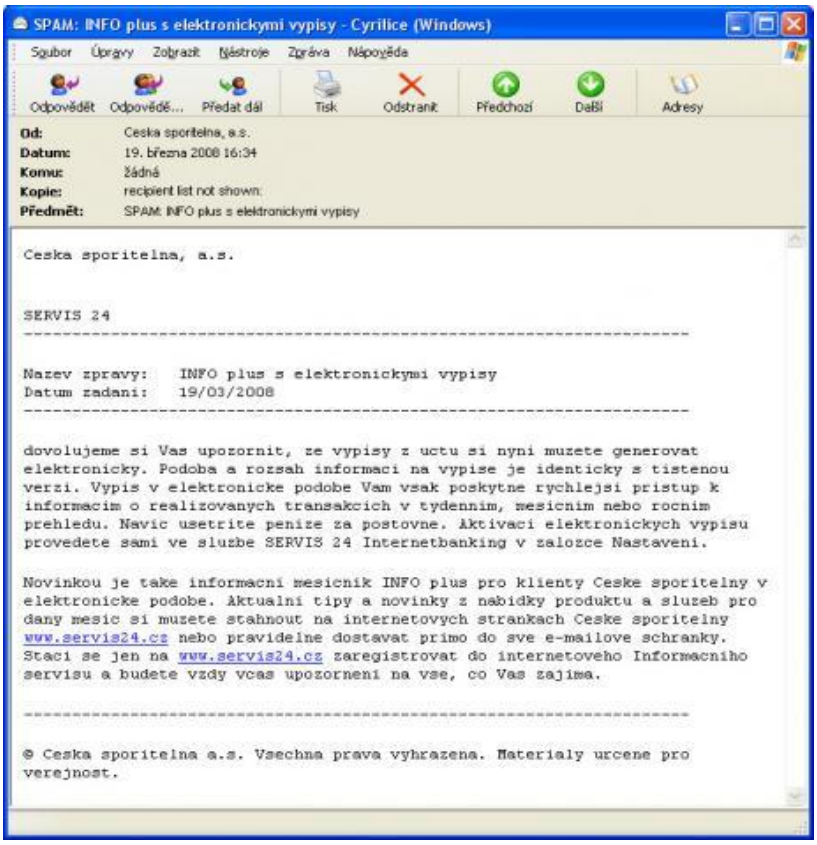
[25] hacker- počítačový specialista nebo programátor s dokonalými znalostmi systému, který si většinou upravuje programy podle svých potřeb. V masmédiích se tento pojem používá pro tzv. počítačové zločince.

zpráva. Banka takové zprávy nikdy nerozesílá a nemá důvod tyto informace od vás požadovat!

- Pokud uživatel klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky organizace (banky). Na podvodných stránkách je připraven formulář, kde jsou požadovány důvěrné informace - čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě, přihlašovací údaje ke službám a podobně.

- Podvodné stránky bývají umístěny na napadených, špatně zabezpečených serverech. Proto ve většině případů bývá v internetovém prohlížeči v poli pro zadání adresy uvedená jiná adresa, která nemá s příslušnou organizací nic společného. Toto je jeden z poznávacích bodů, že se uživatel dostal na podvodnou stránku. Někdy se podvodníci snaží pomocí různých triků tento údaj v adresním řádku zamaskovat.[26]

[26] http://www.hoax.cz/phishing/co-je-to-phishing



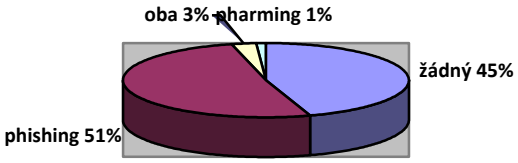
Obrázek 14: Příklad důvěryhodného e-mailu od hackera[27]

První phishingový útok v České Republice byl zaznamenán na klienty banky CitiBank a to v březnu roku 2006. V říjnu 2006 byl proveden první útok i na klienty České Spořitelny. Od počátku roku 2008 začaly masívní útoky na klienty České spořitelny, které se až do Velikonoc stupňovaly. Nejdříve to byly úsměvné pokusy s neumělou češtinou. S největší pravděpodobností se jednalo o strojové překlady a oslovení "Drahoušek zákazník" se stalo oblíbeným sloganem. Další pokusy varovaly před neprovedenou transakcí nebo slibovali odměnu za vyplnění dotazníku. Všechny tyto podvodné e-maily byly psány buď anglicky, nebo nepovedenou češtinou. Zlom nastal až ve chvíli, kdy podvodníci použili velmi jednoduchý trik. Text jednoduše okopírovali přímo ze stránek České spořitelny. Zneužili aktualitu, která varuje před podvodnými e-maily. V textu sice varovali před sebou samými, ale nechyběl odkaz na "verifikaci" svého účtu, který samozřejmě směřoval na podvodné stránky.[28]

[27] http://digitalne.centrum.cz/internet-banking-jak-predejit-utokum/

[28] http://www.hoax.cz/phishing/co-je-to-phishing

- Pharming: je takový nový druh phishingu. Je tím pádem i mnohem nebezpečnější. Ke své činnosti využívá překladu jména serveru na odpovídající IP adresu[29], útočí tedy na DNS (Domain Name System)[30]. Takže pokud uživatel zadá ve svém prohlížeči určitou webovou adresu, na kterou se chce dostat, otevře se mu úplně jiná webová stránka. Tuhle webovou stránku ale nelze rozpoznat od originálu, takže uživatel nic netušíc zadá své přihlašovací údaje a těmi víceméně i obdaruje útočníka.



Obrázek 15: Zkušenosti uživatelů internetbankingu s phishingem nebo pharmingem[31]

- Clickjacking: je označení možného útoku novou metodou hackingu, kdy útočník překryje webové stránky vlastním obsahem. Podstatou útoku je přimět oběť k jedinému kliknutí. Nic netušící oběť jednoduše provádí operace skrze překryvný obsah a nevědomky tak provede operace, které by provést nechtěla.

Tento útok může vést k tomu, že útočník bez vědomí oběti změní například nastavení přehrávače a ovládne na jeho počítači připojenou kameru nebo mikrofon a bude ho moci sledovat a odposlouchávat. Robert Hansen a Jeremiah Grossmann[32] na bezpečnostní konferenci v New Yorku během září 2008 varovali před možností zneužití clickjackingu, jež by mohlo vést k ohrožení bezpečnosti uživatelů nebo k nezákonnému výběru peněz z bankovních účtů potenciálních obětí. O měsíc později izraelský výzkumný pracovník Guy Aharonovsky[33] provedl ukázku útoku prostřednictvím clickjackingu, kdy resetoval

[29] IP adresa je v informatice číslo, které identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol)

[30] DNS je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.

[31] http://www.lupa.cz/clanky/rhybareni-strida-pharming/

[32] Čepička, D. Clickjacking: jaká je šance na úspěšnou obranu [online]. PC World, 2. 1. 2009 [cit. 2009-03-13].
Dostupný z WWW: <http://securityworld.cz/securityworld/clickjacking-jaka-je-sance-na-uspesnou-obranu-97>.

nastavení soukromí v programu Adobe Flash a s využitím webové kamery a mikrofonu nepozorovaně sledoval činnost napadeného uživatele.

Ke zneužití bankovního účtu může dojít prostřednictvím klikání uživatele (třeba v rámci flashové hry), kterým se ve skutečnosti na pozadí originálního webu banky provádí bankovní transakce (například potvrzení odeslané platby z účtu) nebo je umožněn přístup k citlivým datům.

Tento druh podvodného útoku může být možnou vizí budoucnosti útočníků na česká bankovní konta, neboť podle nezávislého bezpečnostního konzultanta Rastislava Turka[34] pouze tři české banky (Komerční banka, Citibank a mBank) mají aplikovanou ochranu proti clickjackingu.[35]

---

[33] Čepička, D. Clickjacking: budeme se bát? [online]. PC World, 9. 12. 2008 [cit. 2009-03-17]. Dostupný z WWW:
<http://pcworld.cz/ostatni/clickjacking-budeme-se-bat-3257>.

[34] Trendy v internetové bezpečnosti: Většina českých bank není odolná proti ClickJackingu [online]. Lupa.cz, 26. 2.
2009 [cit. 2009-03-15]. Dostupný z WWW: <http://www.lupa.cz/zpravicky/vetsina-ceskych-bank-neni-odolna-proticlickjack/>.

[35] KONEČNÁ, Hana. *Trestněprávní aspekty zneužívání vybraných typů elektronického bankovnictví*. [s.l.], 2008-2009. 70 s. Diplomová práce. Masarykova univerzita v Brně. Dostupné z WWW: <http://is.muni.cz/th/134665/pravf_m/>.

5.2.3 Srovnání zabezpečení přístupu k internetbankingu českých bank

V následující tabulce je uvedeno, jaké zabezpečení používají české banky k autentizaci uživatelů internetového bankovnictví.

Tabulka 5: Zabezpečení autentizace internetového bankovnictví

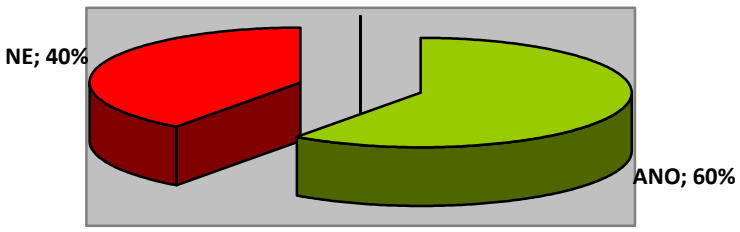
Zabezpečení autentizace internetového bankovnictví[36]						
Banka	**Produkt**	**Uživatelské jméno a heslo**	**Certifikát**	**Čipová karta**	**SMS**	**PIN kalkulátor**
BAWAG Bank	**Bawag direct**	ANO				
Citibank	**Citibank online**	ANO				ANO
Česká spořitelna	**Servis 24 Internetbanking**	ANO		ANO		
ČSOB	**Internetbanking 24**	ANO		ANO	ANO	
eBanka			ANO		ANO	ANO
GE Money Bank	**Internet banka**	ANO	ANO		ANO	
HVB Bank	**Online Banking**					ANO
Komerční banka	**Mojebanka**		ANO	ANO		
Poštovní spořitelna	**Max Internetbanking PS**	ANO			ANO	
Raiffeisenbank	**Internetové bankovnictví**	ANO				
Volksbank	**Internet banking**	ANO				
Živnostenská banka	**Net banka**	ANO	ANO			

[36] http://www.mesec.cz/clanky/jak-je-zabezpecene-internetove-bankovnictvi/

5.2.4 Bezpečnost užívání internetového bankovnictví z pohledu uživatele

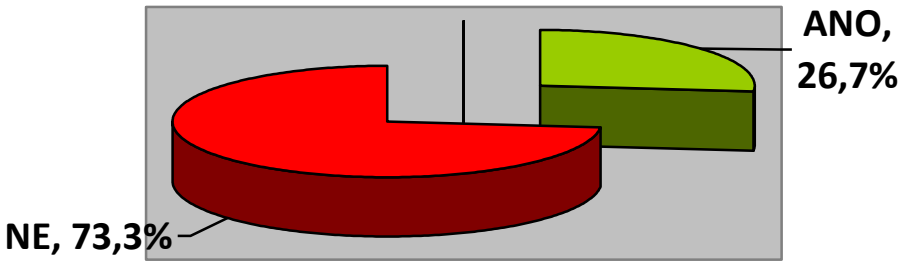
Vzhledem k tomu jak dopadl můj výzkum ohledně znalostí bezpečnosti platebních karet jejich uživatelů, rozhodla jsem se pro další výzkum zaměřený na bezpečnost internetového bankovnictví. Může se zdát, že internetové bankovnictví je velmi oblíbený a využívaný produkt, není tomu ale docela tak. Rozdělila jsem tedy můj výzkum na dvě části. V první části si dotázané rozdělíme na skupiny používající a nepoužívající internetové bankovnictví, v druhé části se zaměřím na důvěru uživatelů internetového bankovnictví v jeho zabezpečení.

Z 50 dotázaných, ve věku v rozmezí od 20 do 50 let, používá internetové bankovnictví pouze 30 dotázaných.



Obrázek 16: Výsledek ankety využívání internetového bankovnictví

Všem zbývajícím uživatelům bylo známo, jak je jejich autentizace a potvrzování aktivních platebních operací zabezpečeno. Zeptala jsem se tedy, jestli také znají úroveň právě jejich zabezpečení. Výsledkem bylo celkem 22 záporných odpovědí a 8 kladných.



Obrázek 17: Výsledky ankety o znalosti úrovně zabezpečení internetového bankovnictví

Z průzkumu tedy vyplývá, že většina uživatelů slepě důvěřuje své bance a ani je nenapadne se o úroveň zabezpečení zajímat. Pokud si všimnete, banky sice ve své nabídce mají popis různých zabezpečení internetového bankovnictví, žádná banka ale už nezmiňuje úroveň svého zabezpečení. Uživatel je tedy mylně přesvědčen o dokonalosti svého zabezpečení.

ZÁVĚR:

Má bakalářská práce byla zaměřena na bezpečnost transakcí prostřednictvím elektronického bankovnictví v České Republice. V mé práci jsem se snažila čtenáře seznámit s pojmem elektronické bankovnictví, s jeho vývojem ale také i s komunikačními kanály, na které se elektronické bankovnictví dělí.

Ke každému komunikačnímu kanálu elektronického bankovnictví patří také jeho stručný popis, popis jeho zabezpečení z pohledu uživatele, rizika, která mohou být s jeho používáním spojena a popřípadě jeho výhody či nevýhody.

Poté jsem se v mé práci zaměřila na hlavní způsoby zabezpečení elektronického bankovnictví a vybrala jsem si jeho dva komunikační kanály k detailnímu popisu.

Prvním komunikačním kanálem jsou platební karty. Tato část se týkala především situace platebních karet v České Republice a to od jejich bezpečnosti a dostupnosti v ČR, přes počty vydaných a používaných platebních karet až po výzkum zaměřený na bezpečnost platebních karet z pohledu jejich uživatele. Výzkumem jsem zjistila, že drtivá většina uživatelů není dostatečně obeznámena s bezpečností platebních karet, které skoro denně používají. Je tedy otázkou, zda je to chyba banky a institucí vydávajících platební karty, které uživatelům neposkytují dostačující informace nebo jestli je to chyba samotných uživatelů. Dle mého názoru by se na toto téma měly jednoznačně více zaměřit banky, neboť čím bezpečnější karty budou vydávat a čím více o nich klienty informují, tím více mohou klientů získat a tím také relativně ztížit práci podvodníkům, kteří čím dál více neoprávněně vybírají finanční prostředky z bankovních účtů klientů bank.

Dále jsem se ve své práci zaměřila na zabezpečení internetového bankovnictví v České Republice. Tato část se týkala zejména základních úrovní zabezpečení z pohledu bankovního, poté jsem se zaměřila na nejznámější druhy zneužívání internetového bankovnictví ať už celosvětově nebo jen v České Republice.

Můj výzkum zaměřený na internetové bankovnictví v Čechách se týkat zjištění a porovnání zabezpečení přístupu k internetbankingu u českých bank a dále se týkal bezpečnosti užívání internetbankingu z pohledu jeho uživatele.

Výsledkem bylo vcelku překvapivé zjištění, že v české Republice zdaleka není tolik uživatelů internetového bankovnictví, jak by se mohlo na poprvé zdát. I přesto, že je to fenomén posledních pár let, lidé si k němu ještě nenašli zcela cestu. Uživatelé internetbankingu se pohybují zejména ve spodní věkové hranici (od 20 do 40 let). Je to

možná i tím, že starší generace se ještě neztotožnila s používáním počítačů, internetu a věcí s nimi souvislými.

Dále jsem zjistila, že když je uživatelům známo, jakým způsobem je jejich internetové bankovnictví zabezpečeno, většina z nich nemá ale ani potuchy o tom na jaké úrovni se zrovna jejich zabezpečení nachází. Dle mého názoru zde dochází ke stejné situaci jako u platebních karet a to, že klienti nejsou dostatečně o bezpečnosti internetového bankovnictví informování nebo si banky samy nejsou jisty, zda právě jejich nabídka je ta nejlepší na trhu a proto raději mlčí a získávají klienty na základě neúplných informací.
Můžeme tedy doufat, že se tato situace do budoucna zlepší. Že banky budou své klienty dostatečně informovat a budou neustále doplňovat své zabezpečení dle nejnovějších výzkumů a možností. Třeba to bude mít v budoucnosti za následek i to, že se nebudeme muset nadále o naše úspory na bankovních účtech obávat a podvodníci už nebudou mít dále možnosti nám je krást.

K tomuto ale bude ještě zapotřebí spousta práce a hlavně ochoty zlepšovat své služby z řad bank a institucí, a většího zájmu o své peníze z řad jejich klientů.

RESUMÉ:

Ma mémoire concerne le système des banques électroniques. Dans mon travail, je présente tous les canals de la communication des clients avec les banques. Je me concentre sur la sécurité de ces canals de la communication, mais aussi sur leurs utilisation et sur leurs préférations. Puis je me préoccuppe de deux canals de la communication les plus préférés; ces sont les cartes de paiements et le cybersystéme des banques. Je décris comment ils sont utilisés, pourquoi ils sont tant préférés dans le monde et aussi comment ils sont sécurisés. Puis je voudrais esquisser une situation des cartes de paiements et du cybersystéme des banques en République Tchèque.Je présente quelques situations quand on peut être truqué en utilisant les cartes de paiements et le cybersystéme des banques Je vais aussi présenter quelques statistiques, qui démontrent l'abus de ces deux canals de la communication dans la République Tchèque.

Ma recherche se concentre sur l'ignorance des habitants tchèques portée sur la sécurisation des leurs moyens de paiements.

ANOTACE:

Název katedry a fakulty:	Katedra aplikované ekonomie, Filozofická fakulta
Název bakalářské práce:	Elektronické bankovnictví v ČR z pohledu bezpečnosti realizovaných transakcí
Vedoucí diplomové práce:	Ing. Zdeněk Puchinger
Počet znaků:	84 808
Počet příloh:	0
Počet titulů použité literatury:	22

Klíčová slova:

elektronické bankovnictví, platební karty, e- peníze, telefonní bankovnictví, GSM banking, homebanking, internetbanking, bezpečnost, elektronický podpis, hesla, Česká Republika

Keywords:

electronic banking, payment cards, e-money, phone banking, GSM banking, internet banking, homebanking, security, electronic signature, passwords, Czech Republic

Anotace:

V mé práci se zabývám alternativou běžného bankovnictví- s elektronickým bankovnictvím. Představíme si komunikační kanály, díky kterým klient komunikuje s bankou i to, jak jsou tyto jednotlivé kanály zabezpečeny. Dále se zaměříme na bezpečnost platebních karet a internetbankingu v České Republice. Pomocí menších výzkumů si doložíme nevědomost českých občanů ohledně zabezpečení jejich platebních prostředků.

Annotation:

My work is concerned with an alternative of ussual banking- with electronic banking. I introduce the communication channels, thanks to whereby the clients can communicate with the bank, and also the channel´s security. I focus on the security of payment cards and internetbanking in Czech Republic. By small researching, I´ll prove the ignorance of czech people concerning in security of their medium of payments.

Seznam tabulek:

Seznam obrázků:

Seznam zkratek:

SMS	short message service
IP adresa	je v informatice číslo, které identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol)
DNS	je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě
IB	internetové bankovnictví
PK	platební karta

Seznam pramenů a použité literatury:

Monografie:

[1] MÁČE, Miroslav. *Platební styk klasický a elektronický*. [s.l.] : Grada, 2006. 220 s. ISBN 8024717255.

[2] PŘÁDKA, M., KALA, J. :*Elektronické bankovnictví: rady a tipy.* 1. vyd. Praha : Computer Press, 2000. 166 s. ISBN 80-7226328-5

[3] ŘÍHA, Daniel. *Elektronické bankovnictví*. [s.l.], 2006. 59 s. Bakalářská práce. Masarykova univerzita v Brně.

[4] KONEČNÁ, Hana. *Trestněprávní aspekty zneužívání vybraných typů elektronického bankovnictví*. [s.l.], 2008-2009. 70 s. Diplomová práce. Masarykova univerzita v Brně. Dostupné z WWW: http://is.muni.cz/th/134665/pravf_m/

[5] PEKÁRKOVÁ, Lucie. *Elektronické bankovnictví, jeho možnosti a další vývoj* [online]. [s.l.], 2006. 60 s. Bakalářská práce. Masarykova univerzita v Brně. Dostupné z WWW: <http://www.citace.com/generator.php?druh=6&ukol=1>.

[6] DANĚK, Ondřej. *Bezpečnost v elektronickém obchodování* [online]. [s.l.], 2007. 54 s. Bakalářská práce. Masarykova univerzita v Brně. Dostupné z WWW: <http://is.muni.cz/th/60931/esf_b/>.

[7] GELETA, Martin. *Bezpečnostní aspekty elektronického bankovnictví* [online]. [s.l.], 2009. 59 s. Bakalářská práce. Bankovní institut vysoká škola Praha. Dostupné z WWW: <http://is.bivs.cz/th/5659/bivs_b/BP_-_Bezpecnostni_aspekty_el._bankovnictvi.pdf?lang=cs>.

Internetové zdroje:

[1] Čepička, D. Clickjacking: jaká je šance na úspěšnou obranu [online]. PC World, 2. 1. 2009 [cit. 2009-03-13].Dostupný z WWW: <http://securityworld.cz/securityworld/clickjacking-jaka-je-sance-na-uspesnou-obranu-97>.

[2] Čepička, D. Clickjacking: budeme se bát? [online]. PC World, 9. 12. 2008 [cit. 2009-03-17]. Dostupný z WWW:<http://pcworld.cz/ostatni/clickjacking-budeme-se-bat-3257>.

[3] ZÁMEČNÍK, P.: *Přímé bankovnictví na vzestupu.* Měšec.cz [on-line]. 2003. Dostupný na < http://www.mesec.cz/clanky/prime-bankovnictvi-na-vzestupu/> [cit. 2006-05-14]

[4] Trendy v internetové bezpečnosti: Většina českých bank není odolná proti ClickJackingu [online]. Lupa.cz, 26. 2.2009 [cit. 2009-03-15]. Dostupný z WWW: <http://www.lupa.cz/zpravicky/vetsina-ceskych-bank-neni-odolna-proticlickjack/>.

[5] PLISCHKE, Simona Ely. Jak došly platební karty do českých zemí aneb historie karet plná zajímavostí. *Peníze.cz* [online]. 2007, 4, [cit. 2010-04-03]. Dostupný z WWW: <http://www.penize.cz/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti>. ISSN 1213-2217.

[6] VÝVOJ ČIPOVÝCH PLATEB V ČESKÉ REPUBLICE. *CardMag* [online]. 2009, 1,[cit.2010-04-03].Dostupnýz WWW: http://cardmag.cardzone.cz/archiv/cm1_2009.pdf

[7] *Www.bankovni karty.cz* [online]. 2008 [cit. 2010-04-03]. Sbk, bankovní karty. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_cr.html>.

[8] Karty v číslech. *CardMag* [online]. 2010, 1, [cit. 2010-04-03]. Dostupný z WWW: <http://cardmag.cardzone.cz/aktual/pages/0_karty_v_cislech.html>.

[9] *Www.bankovni karty.cz* [online]. 2010 [cit. 2010-04-03]. Sbk, bankovní karty. DostupnénaWWW:<http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Druhy_podvodů>.

[10] *Www.ceed.cz* [online]. 2007 [cit. 2010-04-03]. Výukové stránky. Dostupné z WWW: <http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htmv>.

[11] *ČSOB : Trendy elektronického bankovnictví* [online]. 2006 [cit. 2009-02-20]. Dostupný z WWW: <http://www.csob.cz/WebCsob/Csob/Servis-pro-media/PB_CSOB_ELB_vysledky_studie_NMS.pdf>.

[12] DŽUBÁK, Josef. Co je to phishing. *HOAX* [online]. 2009, 1, [cit. 2010-04-03]. Dostupný z WWW: <http://www.hoax.cz/phishing/co-je-to-phishing>.

[13] FELCMAN, Michal. Jak je zabezpečené internetové bankovnictví. *Www.mesec.cz* [online]. 2007, 1, [cit. 2010-04-03]. Dostupný z WWW: <http://www.mesec.cz/clanky/jak-je-zabezpecene-internetove-bankovnictvi/>.

[14] SILLMEN, David. Internet-banking - jak předejít útokům?. *Digitálně.cz* [online]. 2009, 2, [cit. 2010-04-03]. Dostupný z WWW: <http://digitalne.centrum.cz/internet-banking-jak-predejit-utokum/>.

[15] EVROPSKÁ DOKUMENTACE : Současná situace platebních. In *EVROPSKÁ DOKUMENTACE : Současná situace platebních*. [s.l.] : [s.n.], 2008 [cit. 2010-04-10]. Dostupné z WWW: <http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>.