Bezpečnost elektronických platebních systémů

Security of electronic payment systems

Bc. Matyáš Markusík

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Matyáš Markusík**
Osobní číslo:	**A10859**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost elektronických platebních systémů**

Zásady pro vypracování:

1. **Definujte základní pojmy související s problematikou elektronických platebních systémů a jejich bezpečností.**
2. **Zpracujte literární rešerši.**
3. **Popište hlavní technologie elektronických platebních systémů a analyzujte je s ohledem na bezpečnostní rizika.**
4. **U vybrané formy elektronických platebních systémů proveďte komparativní analýzu s důrazem na jejich zabezpečení.**
5. **Prezentujte doporučení pro chování uživatelů elektronických platebních systémů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BERÁNEK, Ladislav. Bezpečnost online systémů a platebních systémů. [online]. Dostupné z: http://ecom.ef.jcu.cz/web/download/teorie/p06-bezpecnost.pdf**
2. **JAMES, Lance. Phishing bez záhad. 1. vyd. Praha : Grada, 2007. 284 s. ISBN 978-80-247-1766-1.**
3. **MÁČE, Miroslav. Platební styk – klasický a elektronický. 1. vyd. Praha : Grada Publishing, a.s., 2006. 220 s. ISBN 80-247-1725-5.**
4. **MATYÁŠ, Vašek, KRHOVJÁK, Jan. Autorizace elektronických transakcí a autentizace dat i uživatelů. 1. vyd. Brno : Masarykova univerzita, 2008. 125 s. ISBN 978-80-210-4556-9.**
5. **SCHLOSSBERGER, Otakar, HOZÁK, Ladislav. Elektronické platební prostředky. Praha : Bankovní institut vysoká škola, 2005. ISBN 80-7265-073-4.**
6. **SMEJKAL, Ladislav. Elektronické peníze. [online]. Ikaros. 2001, roč. 5, č. 10, ISSN 1212-5075. Dostupné z: http://www.ikaros.cz/elektronicke-penize**

Vedoucí diplomové práce:	**Ing. Radek Matušů, Ph.D.** Ústav automatizace a řídicí techniky
Datum zadání diplomové práce:	**24. února 2012**
Termín odevzdání diplomové práce:	**15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá bezpečností elektronických platebních systémů a tím, jaké hrozby a rizika hrozí při jejich používání, a jak jim může člověk svým chováním předejít. Dále zjistíte něco o kryptografické ochraně. Následuje porovnání vybraných druhů elektronických platebních systémů s ohledem na jejich bezpečnost. Na závěr jsem zpracoval dotazník, který se zabývá chováním lidí při používání elektronických platebních systémů.

Klíčová slova: elektronické platební systémy, bezpečnost, internetbanking, kryptografie, skimming, elektronická platební karta.

ABSTRACT

The thesis deals with the electronic payment system security, the threats and risks threating if we use the system and how one can prevent them through his behaviour. In addition you come to know about a cryptographic protection. After that there is a selected electronic payment systems comparison with respect to systems safety. Finally I have elaborated a questionnaire that deals with the human behaviour during the electronic payment systems use.

Keywords: electronic payment systems, safety, internet banking, cryptography, skimming, electronic credit card.

Víra změní můj svět!

Chtěl bych poděkovat svému vedoucímu práce Ing. Radku Matušů Ph.D., za ochotu rady a připomínky, které mi během tvorby diplomové práce poskytl. Dále bych rád poděkoval svým rodičům, kteří mě podporovali při studiu na vysoké škole a byli mi po celou dobu studia oporou.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Diplomová práce se zabývá bezpečností elektronických platebních systémů a tím, jak by se měl člověk chovat, aby nedošlo k jejich zneužití. Smyslem mojí práce tedy bylo popsat rizika, která hrozí při jejich používání a následně popsat bezpečnostní opatření a chování lidí, kteří je používají.

Při psaní diplomové práce jsem si nemohl nevšimnout toho, jak jsou hackeři a padělatelé vynalézaví. Neustále vytvářejí nové programy, zařízení a podvody, aby se dostali k našim účtům. Většinou se jedná o specialisty ve svém oboru, kteří pracují v organizovaných skupinách.

Zajímavá musí být také práce programátorů a techniků vytvářejících programy a zařízení, které zabezpečují elektronické platební systémy. Ti se denně setkávají s novými způsoby a zařízeními, pomocí kterých se pachatelé dostanou k účtu nebo hotovosti. Proto musejí rychle reagovat vytvářením nových programů a technologií, aby útokům zabránili.

Člověk je schopen použít základní bezpečnostní opatření k tomu, aby ochránil svůj počítač, přístup k účtu nebo platební kartu. Ušetří tak sobě a bance starosti a policii práci s vyšetřováním.

Práce je rozdělena na teoretickou a praktickou část. Teoretická část je rozdělena na pět kapitol, v kterých se zabývám elektronickými platebními systémy, jejich bezpečností a riziky, jež jim hrozí. V praktické části řeším tuto situaci z pohledu obyčejného člověka. Zabývám se tím, jak může svým chováním pomoci nebo zamezit zneužití elektronických platebních systémů.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÉ PLATEBNÍ SYSTÉMY

Při používání elektronických platebních systémů probíhá komunikace mezi klientem obchodníkem a bankou elektronickou formou. Jedná se o komunikační cesty, jako je např. Internet, telefonní linka, GSM síť a jiné. Tento typ platebních systému šetří čas bance, která nemusí jednat s klientem osobně, ale takém klientovi, jež neztrácí čas návštěvami banky. Elektronické platební systémy tak slouží ku prospěchu všech zúčastněných stran.

Mezi první elektronický platební systém můžeme zařadit telefonní bankovnictví. Telefon ovšem nebyl pro bankovnictví příliš spolehlivý prostředek, klient se identifikoval pouze jménem a známým hlasem nebo smluveným kódem a autentizace se prováděla pomocí hesla. Poté se začal používat fax, kde se pro zabezpečení používalo jména a číslo klienta, číslo účtu a pro autentizaci kódové tabulky. Bohužel technika nebyla dokonalá, a tak byly někdy faxem vytištěné příkazy nečitelné. Klient musel v chybných případech ihned reagovat přeposláním.

Základní zlom nastal v používání počítačů, které dokáží zpracovat téměř všechna data. Klienti mají účetní programy, v kterých si sami vedou účetnictví. V této souvislosti vzniká myšlenka, proč znovu přepisovat data, která se už někde zpracovala, a proč je tisknout a znovu nosit do banky k dalšímu zpracování. O myšlenku vyhnout se tomuto opakovanému pořizování dat se začaly zajímat firmy zabývající se vytvářením programů a firmy vyrábějící příslušenství k počítačům. Softwarové firmy začaly připravovat komunikační programy.

Na začátku se data předávala v textových souborech v tzv. kontrolních větách, což byly řetězce znaků s přesně stanovenou strukturou, které obsahovaly zabezpečovací kód pro daný den. Pro první přenos souborů se používaly diskety. Pro banku to tedy znamenalo přenášení velkého objemu dat přímo do systému k zaúčtování bez využití lidského faktoru na přepážce banky. Postupem času se začalo využívat přenosu dat z počítače do počítače.

Zavedení elektronického podpisu odstartovalo vznik složitějších programů, přičemž jeho prostřednictvím mohly banky nabízet svým klientům větší a pohodlnější obsluhu účtů. Došlo k rozšíření komunikace s bankou na 24 hodin denně a 7 dní v týdnu. Výrazně se rozšířilo spektrum služeb. Ke komunikaci se používají tzv. komunikační servery, pomocí kterých komunikace probíhá. Z bankovního systému jsou do nich přenášena data pro klienty. Tato data si klienti stahují dle svých potřeb ale zásady “klasického platebního styku“ zůstávají pro tuto formu bankovnictví zachovány. [3]

2 DRUHY ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

V této kapitole si řekneme, jaké druhy elektronických platebních systémů existují, jak je můžeme rozdělit a také si popíšeme jejich princip.

V dnešní době máme možnost využívat různé druhy elektronických platebních systémů, které lze rozdělit dle několika hledisek. Já jsem zvolil rozdělení dle použité technologie na: *platební karty, elektronické platební terminály, systém elektronické peněženky, homebanking, internetbanking, GSM banking a phonebanking*.

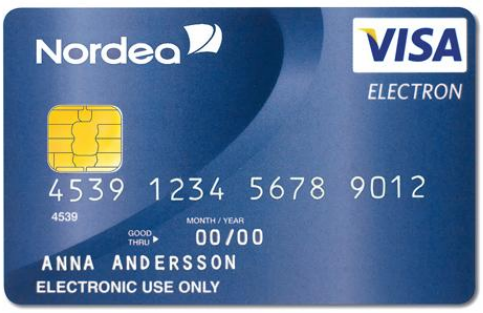
2.1 Platební karty

Je tomu již více než deset let, co se u nás začaly ve velkém množství vydávat platební karty. Postupem času se staly součástí našich životů a u většiny běžných účtů je jejich vydání téměř povinnou součástí.

Platební karty dělíme dle několika hledisek. Nejzákladnější je však dělení dle způsobu provedení na *elektronické* a *embosované platební karty*.

2.1.1 Elektronické karty

Patří mezi nejrozšířenější typ platebních karet u nás. Do této skupiny řadíme karty VISA Electron, či Maestro. Jsou použitelné jen pro transakce, které jsou online ověřeny v kartovém centru, tedy pouze pro výběry z bankomatů a platby u obchodníků disponujících elektronickým platebním terminálem. Výhodou tohoto typu karet je nízká cena, nízké poplatky za její blokaci při ztrátě, či odcizení karty a téměř nulová možnost zneužití zablokované karty. [7]



Obr. 1. VISA Electron [28]

2.1.2 Embosované karty

Do této skupiny patří karty VISA Classic, či MasterCard. Poznáte je podle toho, že mají všechny údaje (číslo karty, majitel, platnost) plasticky vyraženy. To umožňuje jejich použití i u obchodníků, kteří nemají elektronický terminál, ale pouze tzv. imprinter. Platba probíhá tak, že obchodník vloží kartu do imprinteru a otiskne veškeré údaje z karty na účet, který poté zákazník podepíše. Každý obchod má nastaven výši útraty, kterou mohou jeho zákazníci provést kartou, aniž by museli platbu ověřit telefonem. Embosované karty lze použít na více místech než karty elektronické. [5], [7]

Obr. 2. VISA Classic [29]

Obr. 3. Imprinter [30]

2.2 Elektronické platební terminály

Jsou to elektronická zařízení, pomocí kterých můžeme provádět platební transakce. Setkáváme se s nimi především při platbě elektronickou platební kartou.

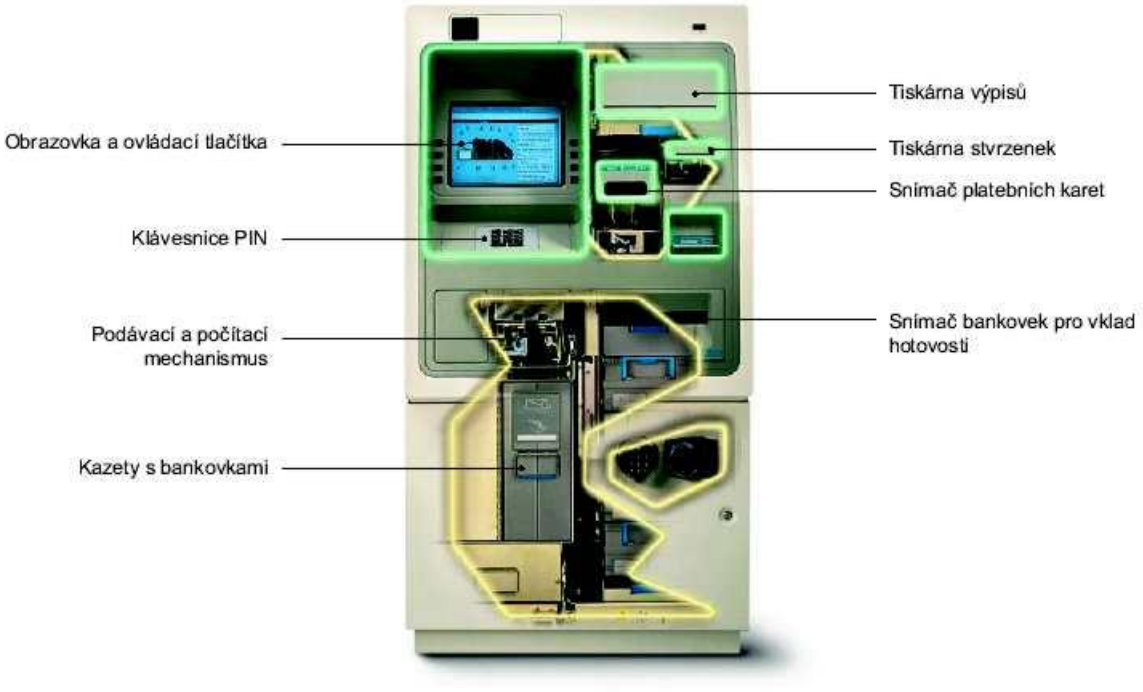
2.2.1 Bankomat

Bankomat je samoobslužné zařízení, které vydává držitelům platebních karet peněžní hotovost z běžných nebo úvěrových účtů, popřípadě poskytuje další služby.

Zavedení bankomatů umožnilo snížit provozní náklady bank, protože efektivně nahradily práci pokladníků a ušetřily plochu nutnou pro pokladny a jejich zázemí na pobočkách. To umožnilo obsloužit více klientů při nižších nákladech a napomohlo snížit počet bankovních poboček.

Vzhledem ke složitosti technologie se výrobou bankomatů dnes zabývá asi deset firem. Největšími dodavateli bankomatů v Evropě jsou společnosti NCR, Diebold a Wincor – Nixdofr, které dohromady kontrolují asi 80% trhu.

V současné době se zavádí již pátá generace peněžních automatů, které využívají internetové technologie. Ta umožňuje např. vydávat poštovní známky, vstupenky, jízdenky nebo sledovat výsledky sportovních zápasů. [8]



Obr. 4. Bankomat [31]

2.2.2 Transakční terminál

Jde o samostatné zařízení, které nepřijímá ani nevydává hotovost, ale slouží pouze k provádění bezhotovostních transakcí např. příkaz k úhradě z účtu, dobití kreditu mobilního telefonu.

Přes transakční terminál lze platit faktury a účty, které mají čárový kód. Doma dostanete poštou fakturu například za plyn, která obsahuje čárový kód. Když ji přiložíte ke čtečce terminálu, automaticky se načtou údaje pro platbu. Nevýhodou je, že neexistuje norma, která by určovala, jak má čárový kód vypadat. Takže bohužel ne všechny doklady automat načte.

Druhou možností je pohodlná platba poštovních poukázek, které se vloží do čtecího otvoru, terminál poukázku přijme, naskenuje a automaticky vygeneruje příkaz k úhradě. Údaje k transakci je možné ručně editovat a změnit, takže můžete ovlivnit například výši částky, kterou opravdu zaplatíte, oproti částce na poštovní poukázce. [9]

Obr. 5. Transakční terminál [31]

2.2.3 Mobilní platební terminály

Mobilní platební terminál uživateli poskytuje komplexní funkcionalitu pro mobilní sběr dat. Pomocí tohoto zařízení můžeme provádět platební transakce, tisk stvrzenek a dokladů, to vše v jednom zařízení.

Je vhodný zejména pro firmy z dopravního a logistického odvětví.

Obr. 6. BIP-1300 [32]

2.2.4 Čtečky elektronických platebních karet

Čtečky elektronických platebních karet jsou zařízení, která dokáží přečíst údaje uložené na elektronických platebních kartách a tím jednoznačně identifikovat majitele karty. Jedná se o malé přístroje, což je jedna z hlavních výhod čteček.

Čtečky rozdělujeme na kontaktní a bezkontaktní. U kontaktních čteček musí majitel karty kartu vložit do čtečky. U bezkontaktní čtečky to není třeba, stačí přiložit kartu cca 5cm od zařízení, které tak identifikuje majitele.

2.2.4.1 Kontaktní čtečka elektronických platebních karet

Jsou vhodné pro použití v supermarketech, či kamenných obchodech. Můžeme je připojit k telefonní lince, internetu či SIM kartě.

Některé čtečky využívají technologie bluetooth, čehož lze využít např. v hostinských zařízeních.

Obr. 7. Kontaktní čtečka [33]

2.2.4.2 Bezkontaktní čtečka elektronických platebních karet

Bezkontaktní technologie dává možnost zákazníkům platit kartou nákupy nepřesahující 500 Kč. Karta se přiloží do vzdálenosti cca pěti centimetrů od čtečky a po pípnutí je transakce ukončena. Obchodník u těchto plateb účtenku nevydává automaticky, ale na vyžádání zákazníka. Bezkontaktní karty mají stejnou úroveň ochrany jako standardní platební karty. [10]

Obr. 8. Bezkontaktní čtečka [10]

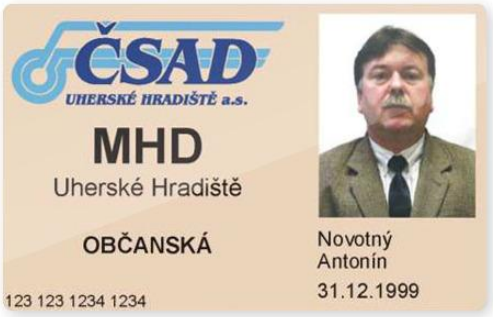
2.3 Systém elektronické peněženky

Elektronické peněženky, používají tzv. elektronické peníze. Tyto peníze znamenají „uloženou hodnotu“ či předplacený platební mechanismus pro výkon plateb, který se provádí prostřednictvím elektronických platebních terminálů.

Rozdělujeme je *hardware - based* (elektronické peněženky) a *software - based* (digitální, elektronická hotovost, e-cash). [6]

2.3.1 Hardware - based

Tento systém elektronické peněženky umožňuje vlastníkovi bezhotovostní platby za odebrané služby nebo zboží. Placení elektronickou peněženkou vypadá tak, že obchodník ji přiloží ke čtecímu zařízení, to zjistí kolik je v systému peněz a automaticky si odebere požadovanou částku. Pokud dojdou majiteli elektronické peněženky peníze, může si doplnit v bance nebo v některém jiném terminálu, který má spojení s provozovatelem peněženky. Například dobití elektronické peněženky, kterou vlastní autobusové dopravy např. ČSAD Uherské Hradiště a.s., je možné ve všech autobusech tohoto dopravního podniku, nebo na jeho stanicích s pokladnou umožňující také elektronický výdej jízdenek. [11]



Obr. 9. Hardware – based [34]

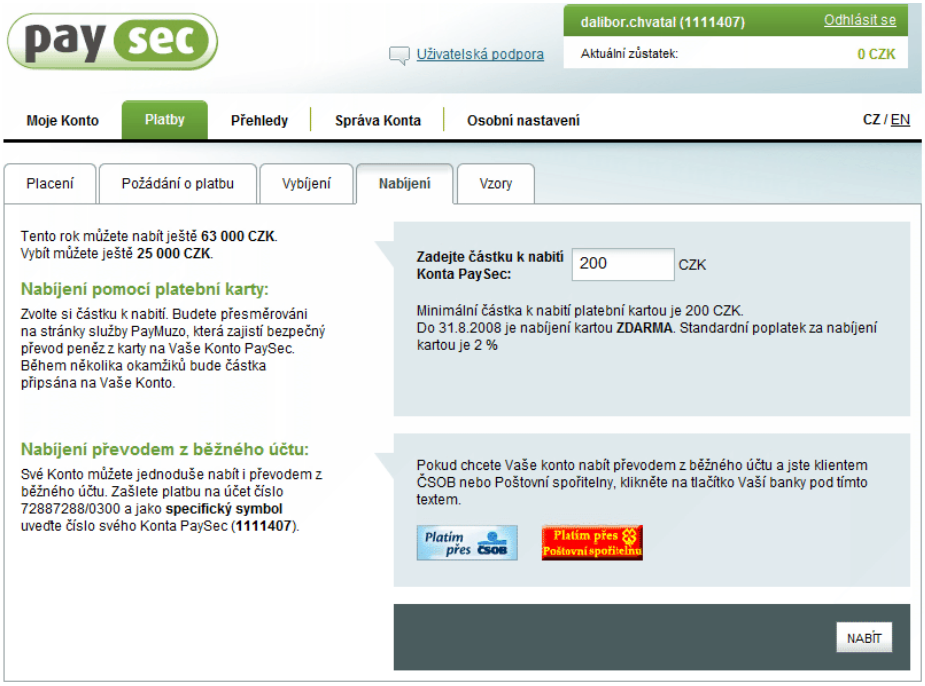
2.3.2 Software – based

U této formy elektronických peněženek se jedná především o jejich využití při platbách na internetu.

Nejznámější je v dnešní době systém elektronických peněženek PayPal, v České republice však patří mezi nejrozšířenější český platební portál PaySec, který vznikl v roce 2008. Tento platební systém umožňuje okamžité a bezplatné platby na celém světě.

Peníze na portál můžete dostat buď bankovním převodem anebo pomocí platební karty. Převod z bankovního účtu trvá maximálně dva pracovní dny, převod z karty je okamžitý a s penězi lze ihned disponovat.

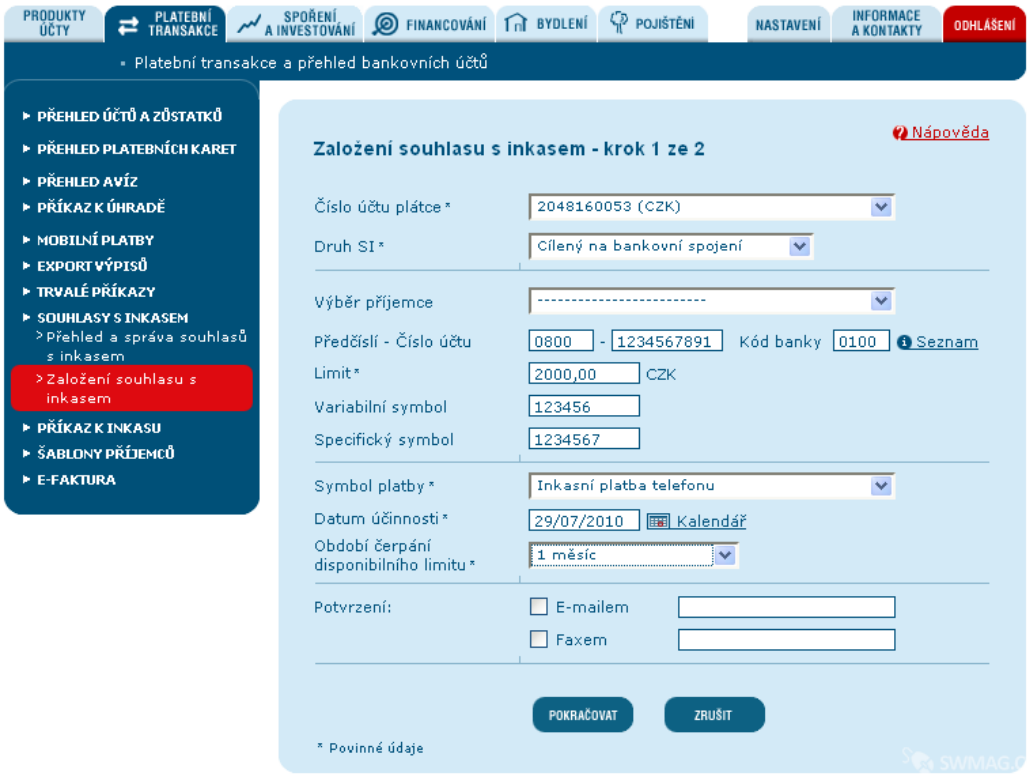
Bankovky a mince jsou zde zastoupeny unikátními čísly, vydávanými pověřenými institucemi. Tato čísla reprezentují částky peněz, je možné je znovu používat, ale nejdou kopírovat. [3], [9]



Obr. 10. Uživatelské rozhraní PaySec [27]

2.4 Internetbanking

Umožňuje komunikaci klienta s bankou prostřednictvím počítače, mobilního telefonu (s nainstalovaným internetovým prohlížečem) připojeného k internetu. Klient se přihlašuje do systému banky. Pro ověření oprávněnosti k provádění požadovaných úkonů prostřednictvím elektronického klíče nebo přes elektronické podpisy a digitální certifikáty se přihlásí na webové stránky své banky a může přímo zadávat pokyny bance.

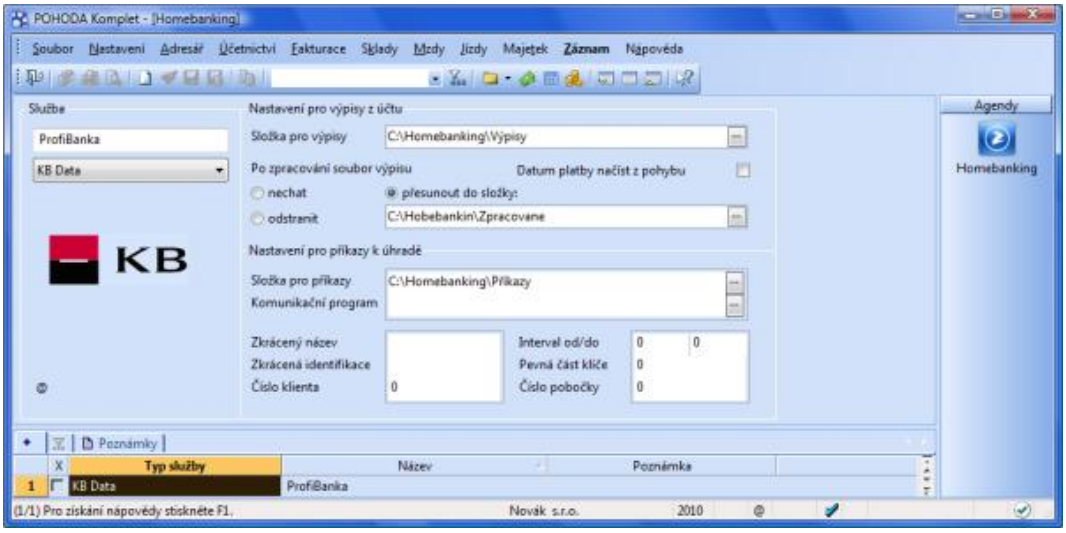


Obr. 11. Internetbanking prostředí SERVIS 24 [17]

Internetbanking umožňuje uskutečňovat obdobné služby jako telefonní bankovnictví tj. zadávání příkazů, založení termínovaného vkladu, informace o stavech na účtech a obecně o produktech a službách poskytovaných bankou. Klientovi přináší velkou výhodu v podobě online informace. [3]

2.5 Homebanking

Homebanking umožňuje spojit se s bankou pomocí speciálního programu, který si musíme nejprve do počítače nainstalovat. Nejvíce ho využívají firemními klienti, ale jeho nabídka je otevřena i soukromým klientům.



Obr. 12. Homebanking prostředí POHODA [35]

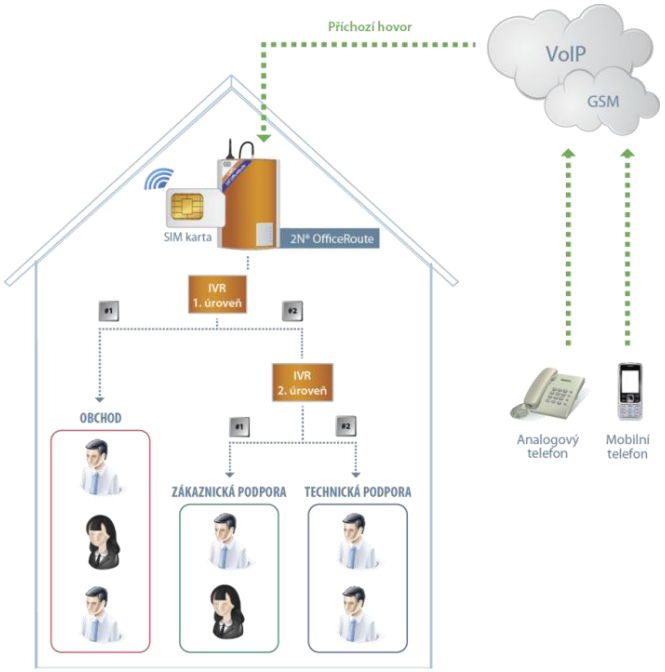
Homebanking byl oblíbený do konce 90. let minulého století, kdy ještě internetové bankovnictví nebylo tolik rozšířeno. Postupem času internetové bankovnictví homebanking téměř nahradilo. Homebanking dnes preferují klienti, kteří z různých důvodů nemohou nebo nechtějí používat přístup do banky přes internet. [12]

2.6 Phonebanking

Prostřednictvím telefonu můžete kdekoli na světě zjišťovat zůstatky na svém účtu a provádět transakce. V některých bankách mluvíte s živým člověkem, v jiných na vaše pokyny reaguje hlasový automat (v tomto případě potřebujete telefon s tónovou volbou).

Banka po telefonu může mít několik úrovní. Pasivní varianta nabízí pouze zjišťování zůstatků na účtu. Aktivní verze navíc umožňuje zadávání příkazů k úhradě i inkasu, měnové konverze, zakládání spořících či termínovaných vkladů a další služby.

Po vytočení čísla telefonní banky se vám ozve hlasový automat, který vás požádá o v identifikaci. Ve většině případů to bývá prostřednictvím klientského čísla a PIN, který jste obdrželi od vaší banky. Poté můžete provádět transakce. Pokud mluvíte s operátorem, probíhá přihlášení obdobným způsobem, čísla se však nemusí vyťukávat pomocí klávesnice na telefonu, ale nadiktujete je telefonnímu bankéři. Služby, které využívají hlasové automaty, většinou nabízejí omezený rozsah služeb, jsou však k dispozici nepřetržitě. Telefonní bankéři mají v některých bankách omezenou pracovní dobu a ve zbývajícím čase se i zde setkáte s automatem. [7]



Obr. 13. Hlasový automat [36]

2.7 GSM banking

Komunikace mezi klientem a bankou probíhá pomocí SMS zpráv prostřednictvím služby SIM Toolkit. GSM banking umožňuje provádět veškeré bankovní operace prostřednictvím speciálně nahraného menu v mobilním telefonu. Jeho rozsah záleží na spolupráci operátora a banky. Jestliže máte svou banku v mobilním telefonu, můžete ji navštěvovat kdykoliv, bez omezení.

Obr. 14. Menu [7]

Ovládání bankovního konta je jednoduché. Funguje podobně jako procházení menu telefonu. Nabídka funkcí v bankovním menu je u většiny bank téměř totožná. Když do bankovního menu vstoupíte a zvolíte z nabídky operaci, kterou budete chtít provést, budete vyzváni k zadání bezpečnostního bankovního kódu PIN, který jste si zvolili v bance, ten také chrání soukromé informace, které mohou z banky přijít na telefon.

GSM banking má svoji *pasivní část* tj. zůstatky, úrokové sazby, devizové kurzy atd. a *aktivní část* tj. příkazy k úhradě, povolení inkasa, zakládání termínovaných vkladů atd.. [3], [11]

V této kapitole jsme zjistili, s jakými druhy elektronických platebních systému se můžeme v dnešním světě setkat a na jakém principu fungují. Mezi nejstarší a zároveň nejpoužívanější patří bezesporu elektronické platební karty, s kterými se naučili zacházet i naši prarodiče. Postupně se rozšiřuje také internetbanking a systém elektronické peněženky hardware – based.

3 ŠIFRY A PROTOKOLY PRO ELEKTRONICKÉ PLATEBNÍ SYSTÉMY

V této kapitole se dozvíme, s jakými šiframi a protokoly se můžeme setkat u elektronických platebních systémů.

Šifry a protokoly používáme k zabezpečení komunikace mezi zákazníkem, obchodníkem a bankou. Pro potřeby elektronických platebních systémů se používají různé protokoly a šifry. My si řekneme něco o těch nejpoužívanějších, jako je např. protokol SSL.

K tomu, abychom lépe porozuměli protokolům pro elektronické platební systémy, bude dobré seznámit se se základními pojmy kryptografie, které nám pomůžou pochopit jejich smysl.

Kryptografie - neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. [13]

Symetrický klíč - vysílač i přijímač sdílí jeden stejný klíč k šifrování a dešifrování.

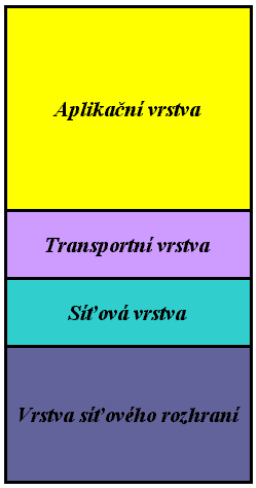
Veřejný klíč - je volně přístupný a je určen pro šifrování dat.

Soukromý klíč - zná jen jeho majitel a slouží k dešifrování.

Digitální obálka - zajišťuje bezpečný přenos a doručení symetrického klíče od vysílače k příjemci.

Certifikační autorita - je subjekt, který vydává digitální certifikáty.

Síťový protokol TCP/IP - se používá po celé síti Internet a skládá se z několika vrstev.

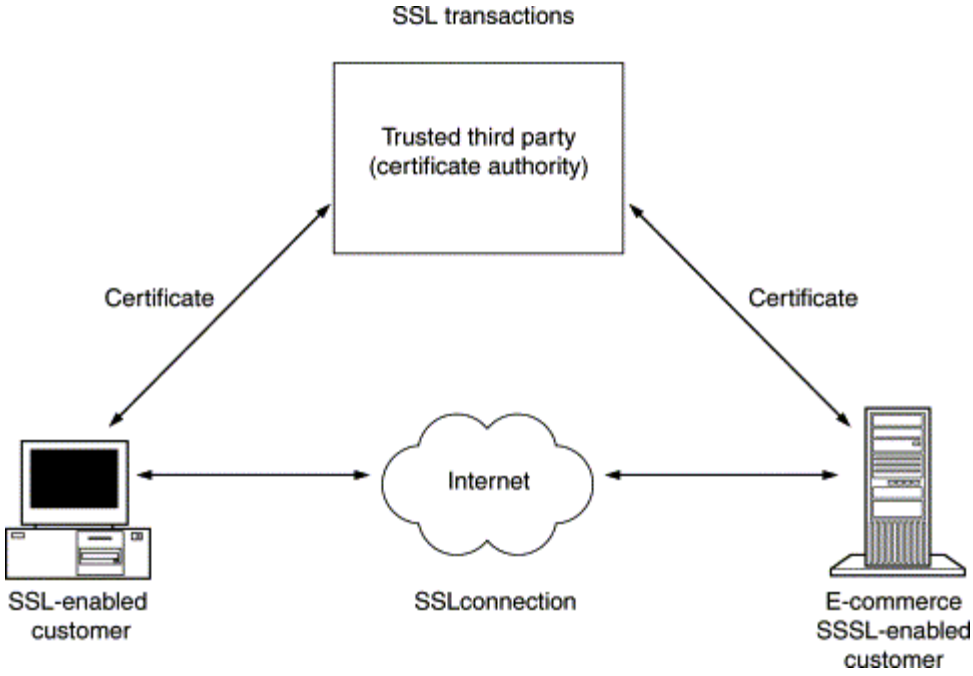


Obr. 15. TCP/IP [37]

3.1 Secure Sockets Layer (SSL)

SSL protokol je vrstva, která je vložená mezi vrstvu transportní a aplikační. Poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran.

Princip spočívá v tom, že kupující pošle serveru požadavek na SSL spojení, spolu s informacemi o nákupu IO. Server pošle kupujícímu odpověď na jeho požadavek, která obsahuje IO + certifikát serveru. Podle přijatého certifikátu si kupující ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru. Na základě informací, které kupující doposud obdržel, vygeneruje základ šifrovacího klíče, ten zakóduje veřejným klíčem serveru a pošle mu ho. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče a z tohoto základu vygenerují server i kupující hlavní šifrovací klíč. Kupující a server si vzájemně potvrdí, že od teď se jejich komunikace bude šifrovat tímto klíčem. Je vytvořeno bezpečné spojení, které je šifrované vygenerovaným šifrovacím klíčem a aplikace dále komunikují přes šifrované spojení. [14]

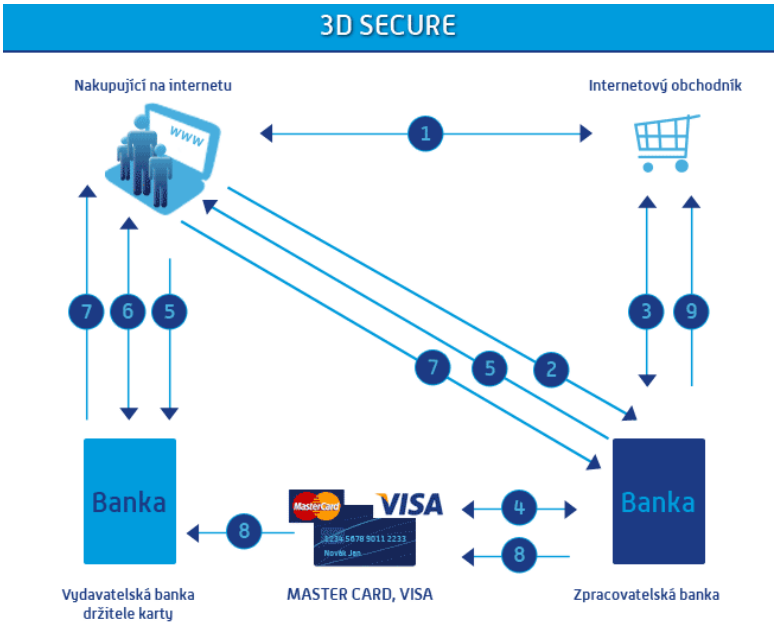


Obr. 16. SSL [38]

3.2 Visa 3-D Secure

Visa 3-D Secure je bezpečnostní protokol určený především pro platební karty. Princip VISA 3D Secure protokolu spočívá v centralizovaném autentizačním přístupu, kdy všechny autentizační požadavky směřují z obchodníkovy strany do VISA adresáře, který udržuje informace o všech uživatelích. Dále směruje požadavek na příslušného uživatele. Vydavatel karty komunikuje s držitelem karty díky jeho prohlížeči, v kterém se sbírají autentizační detaily. Vydavatel je následně potvrdí a pošle zpět obchodníkovi jako autentizační odpověď.

3-D Secure je tedy mechanismus autentizující držitele karty. Každá karta zadaná do platební brány se zkontroluje příslušnou asociací MasterCard nebo VISA. Kontroluje se, zda je pro kartu požadována autentizace držitele karty, či nikoliv. V případě, kdy je požadována autentizace, je držitel přesměrován na systém vydavatelské banky, kde potvrdí svoji identitu sdílenou s vydavatelem karty. Výsledek autentizace je dále předán zpět do platební brány. [14]



Obr. 17. VISA 3D SECURE [39]

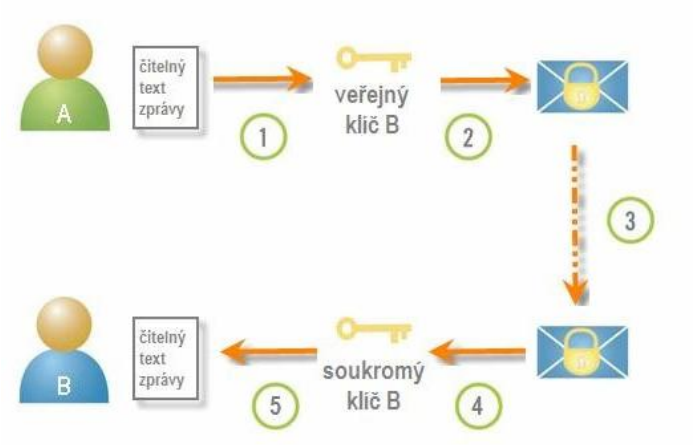
3.3 SIM application toolkit

Je to aplikační protokol, který definuje vlastní komunikaci mezi SIM kartou a mobilním telefonem. Veškerá komunikace mezi nimi má podobu příkazů, kterými SIM žádá telefon o vykonání nějaké funkce (např. zobrazení kontaktu, odeslání SMS), na které dostává od telefonu odpověď, a také událostí, kdy telefon informuje SIM, resp. aplikaci o nějaké nestálé události, např. výběru v menu aplikace uživatelem nebo přijetí hovoru.

Pro dodavatele aplikace a mobilního operátora je největší výhoda v nezávislosti na použitém mobilním telefonu, množství podporovaných mobilních telefonů a především uživatelská jednoduchost. [15]

3.4 Digitální podpis

Odesílatel i příjemce mají svůj soukromý klíč. Přitom mají oba dva přístup k veřejnému klíči, který je pro oba stejný. Odesílatel pomocí veřejného klíče zprávu zašifruje a poté pošle příjemci, který ji dešifruje pomocí svého soukromého klíče. Zpráva, která je zašifrovaná veřejným klíčem je neprolomitelná a není ji možné tímtéž klíčem dešifrovat. Proto můžeme veřejný klíč předat odesílateli nechráněným kanálem anebo jej zveřejnit. [1]



Obr. 18. Digitální podpis [1]

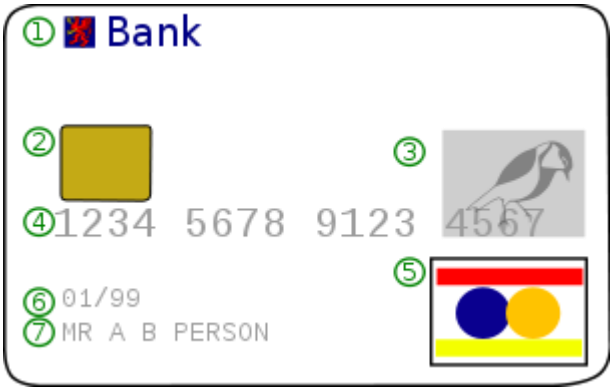
V této kapitole jsme se dozvěděli, jaké protokoly se nejvíce využívají při komunikaci s elektronickými platebními systémy. Nejpoužívanější je protokol SSL, který se používá např. u internetbankingu nebo homebankingu.

4 BEZPEČNOST ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

V této kapitole se dozvíte něco o bezpečnosti elektronických platebních systémů. Což znamená, jak instituce, které nám poskytují nějakou ze zmíněných služeb elektronických platebních systému, chrání naše informace a data, které mezi sebou přenášíme, před třetími osobami.

4.1 Bezpečnost elektronických platebních karet

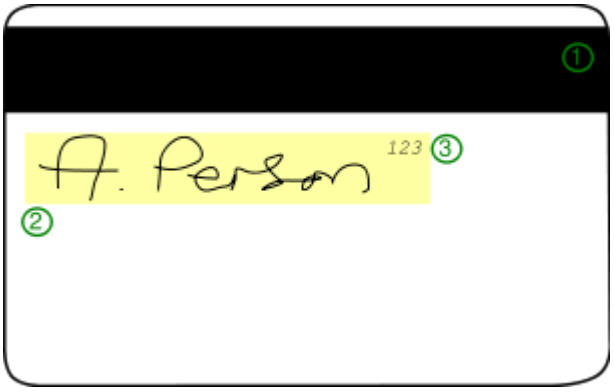
Když mluvíme o bezpečnosti elektronických platebních karet, máme tím na mysli především jejich ochranné prvky, které mají ztěžovat padělatelům jejich duplikaci. Na přední straně se jedná o tyto ochranné prvky:



Obr. 19. Přední strana [40]

1) ***Logo banky*** - na kartě je umístěno logo banky, která platební kartu vydala.
2) ***Čip*** - umožňuje vysoké zabezpečení, které využívá dynamické šifrovací algoritmy, je na něm uložen PIN a také je díky němu možné nasazení karet pro elektronické transakce bez nutnosti ověření v centru.
3) ***Hologram*** - bezpečnostní prvek, který je tvořen speciální fólií s cíleně deformovaným povrchem.
4) ***Číslo karty***
5) ***Logo vydavatele karty***
6) ***Platnost karty***
7) ***Jméno držitele karty***

Na zadní straně nalezneme:



Obr. 20. Zadní strana [40]

1) ***Magnetický proužek*** - jsou na něm uloženy údaje o kartě a jejím držiteli, které jsou potřebné pro provedení platby či výběru z bankomatu. Magnetický proužek neumožňuje tak vysoké zabezpečení uložených dat jako čip.
2) ***Podpisový vzor*** - podpis majitele karty.
3) ***CVC kód (Card Verification Code)*** - dodatečné číslo, které se užívá pro zvýšení ochrany.

Další bezpečnostní prvky na platebních kartách jsou ***fotografie*** a ***čárové kódy***.

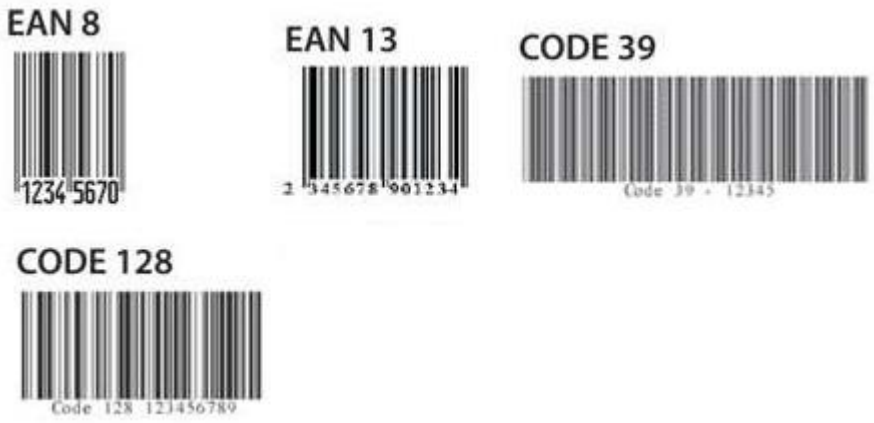
Čárový kód - jeho sejmutím snadno identifikujeme majitele karty. Používá se několik druhů čárových kódů.

EAN 8 – má pevnou délku se zakódovanými 7 znaky a + 1 kontrolní číslicí. Typ znaků je numerický, minimální šířka čárového kódu je minimálně 20 mm.

EAN 13 – má pevnou délku se zakódovanými 12 znaky a + 1 kontrolní číslicí. Typ znaků je numerický, minimální šířka čárového kódu je minimálně 25 mm.

CODE 39 – má proměnnou délku podle počtu znaků, typ znaků je alfanumerický, je nutné kalkulovat minimálně 3,75 mm na znak.

CODE 128 – má proměnnou délku podle počtu znaků, typ znaků je alfanumerický, je nutné kalkulovat minimálně 3,75 mm na znak. [16]



Obr. 21. Druhy čárových kódů [16]

4.2 Bezpečnost elektronických platebních terminálů

Bezpečnost elektronických platebních terminálů je dána především čtecím zařízením, které snímá autentizační údaje z čipu karty a také správným zadáním PIN na klávesnici.

Ověření správných údajů se provádí pomocí protokolu VISA 3D Secure, který ověřuje ve své databázi správnost údajů.

Poblíž terminálů, které jsou stále na jednom místě tj. bankomaty, transakční terminály, stacionární platební terminály v obchodech, bývají instalovány bezpečnostní kamery, které monitorují pohyb kolem těchto zařízení. Ve většině případů jsou také denně kontrolovány bezpečnostní službou.

Obr. 22. Pohled z kamery poblíž bankomatu [31]

4.3 Bezpečnost systémů elektronické peněženky

U *hardware - based* jde z hlediska bezpečnosti především, jako u platebních karet o bezpečnostní údaje, které jsou vytištěny na elektronické peněžence (jméno, číslo karty, logo vydavatele, datum platnosti atd.). I když v tomto případě můžeme říci, že se jedná spíše o legitimační údaje. V peněžence máme sice umístěn čip, ale není na něm uložený PIN, slouží pouze k identifikaci majitele, který jej přiloží ke čtecímu zařízení.

Naproti tomu u *software – based* musíme zabezpečit přístup k účtu, bezpečnost dat a spojení mezi zákazníkem a obchodníkem. K tomu se využívá šifrování a bezpečnostních protokolů. Pro zajištění bezpečnosti komunikace se ve většině případů používá šifrování pomocí technologie SSL. Pro navázání šifrované komunikace se někdy navíc používá certifikát serveru vydaný certifikační autoritou.

Největší výhodou je, že prodejce se při placení elektronickou peněženkou nedostane ke kartě ani účtu např. na PaySec, a tak je téměř vyloučeno zneužití obchodníkem.

4.4 Bezpečnost internetbankingu

Při přihlašování do účtu je třeba provést autentizaci. U aplikace SERVIS 24 je možnost zadání hesla virtuální klávesnicí. Uživatelské jméno ve většině případů přiděluje banka ve formě speciálního kódu. Pro první přihlášení dostává klient jednorázové heslo od

banky. Toto heslo musí ihned po přihlášení změnit. Pro tvorbu hesla mají banky svá pravidla, která určují např. počet znaků, počet číslic, které musí heslo obsahovat.

Další možnost je autentizace pomocí osobního certifikátu, který nám vystaví banka. Osobní certifikát má podobu souboru a může být uložen na přenosném médiu např. USB flash disku, CD nebo na čipové kartě. Tento soubor se musí před provedením transakce nahrát do počítače. [7]

Obr. 23. Virtuální klávesnice [17]

Při několikanásobném špatném zadání hesla se může účet zablokovat, to záleží na bance, která vydala aplikaci.

Před samotnou platbou se provádí autorizace např. pomocí SMS zprávy, kdy majitel účtu zadá při vytváření účtu v bance číslo svého mobilního telefonu, na který mu v případě, že chce provést transakci přes internetbanking, přijde SMS zpráva s kódem. Tento kód zadá do příslušného okna v rozhraní internetbankingu. [4]

Pro základní bezpečnost musí být zajištěno, aby příkaz k bankovní operaci nebyl nikým upraven. Proto se používá šifrování pomocí technologie SSL. Pro navázání šifrované komunikace je navíc použit certifikát serveru banky vydaný důvěryhodnou certifikační autoritou, který zajistí, že skutečně komunikujete s bankou a ne s někým, kdo se za aplikaci internetového bankovnictví pouze vydává.

4.5 Bezpečnost homebankingu

Homebanking má výhodu v tom, že tuto aplikaci dodává a vyvíjí sama banka. Takže si při vývoji software sama určí, jak bude program pracovat, jaké se použije zabezpečení a jak bude aplikace komunikovat s jejich serverem.

Při zřizování homebankingu si musí každý klient vytvořit digitální podpis. Tudíž je třeba klientovi vygenerovat veřejný a soukromý klíč. Veřejný klíč je zaregistrován v bance a soukromý klíč, který je většinou uložen ve formě osobního certifikátu na čipu karty, obdrží klient. V době, kdy probíhají transakce, musí být karta vždy připojena k počítači. Např. pomocí čtečky karet. Čipová karta je navíc chráněna heslem, které musí klient zadat při jejím připojení.

Data poté putují směrem k bance prostřednictvím internetu. Pro zabezpečení toku dat se většinou používá protokol SSL. [17]

4.6 Bezpečnost phonebankingu

Na začátku každého telefonního hovoru je provedena bezpečnostní procedura, která se skládá z identifikace a ověření totožnosti volajícího. Veškeré hovory jsou automaticky nahrávány a archivovány.

Samotný přístup do telefonního bankovnictví je omezen zadáním čísla Vaší debetní nebo kreditní karty a T-PIN, telefonního identifikačního čísla, které si zvolí každý klient. T-PIN je nutné používat při každém spojení s telefonní bankovní službou a je ho možné kdykoli změnit.

Dalším typ zabezpečení, které můžeme použít, je nastavení denních limitů pro aktivní operace na účtu.

Banka má také právo, zablokovat uživateli přístup k účtu, a to v případě, že zadá třikrát během jednoho dne špatné přihlašovací údaje. [18]

4.7 Bezpečnost GSM bankingu

Jako základní prvek bezpečnosti je samotný PIN telefonu. Dále uživatel mobilního telefonu obdrží v bance při aktivaci služby GSM Banking speciální číselný kód BPUK a na základě tohoto kódu si zvolí osobní přístupový kód BPIN. Správným zadáním kódu BPIN je podmíněno provedení všech bankovních operací.

Komunikace mezi zákazníkem a SIM kartou probíhá prostřednictvím protokolu SIM Toolkit.

Přenos dat je zabezpečen šifrováním. Každá bankovní SIM karta má svůj šifrovací klíč, prostřednictvím kterého se provádí zabezpečení komunikace s bankou. Tento klíč je uložen v chráněné oblasti SIM karty a je dostupný pouze po zadání správného kódu BPIN. Klient i banka sdílí společný tajný klíč, kterým se zprávy šifrují. Ten je na jedné straně uložen ve formě certifikátu na uživatelově SIM kartě a na druhé straně je uložen v systému banky.

K autentizaci může zákazník použít i tzv. autentizační kalkulátor. Jeho princip spočívá v tom, že banka vygeneruje autentizační kód a spolu se zprávou jej předá příjemci. Tento způsob přihlášení je nejbezpečnější, protože použité heslo je vždy jednorázové. [9]

Obr. 24. Autentizační kalkulátor [41]

Dozvěděli jsme se, jaké zabezpečení, ať už softwarové např. autentizace nebo hardwarové např. ochranné údaje, se používají u elektronických platebních systémů. A jestli jsme je doposud nepoužívali, tak bychom měli začít.

5 BEZPEČNOSTNÍ HROZBY A RIZIKA PŘI POUŽÍVÁNÍ ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

V této kapitole si řekneme s jakými hrozbami a riziky se můžeme při používání elektronických platebních systémů setkat. Může se jednat o fyzické napadení např. krádež nebo napadení hackerem např. phishing. Všechny metody si popíšeme níže.

5.1 Krádež

Jednou z největších hrozeb jsou v tomto směru kapsáři, ti při krádeži nacházejí v taškách, kabelkách či peněženkách platební karty. Nejčastějším způsobem, jakým se takovýto pachatel může dostat k cizí hotovosti je zjištění dat o platební kartě. Je to především PIN kód, který je potřeba k přístupu na účet a následnému vybrání hotovosti. Někteří lidé jej mají napsaný na papírku v peněžence a v některých případech dokonce přímo na platební kartě. Tímto chováním napomáhají zlodějům, kterým stačí přijít k bankomatu a pohodlně vybrat.

Obr. 25. Krádež peněženky [42]

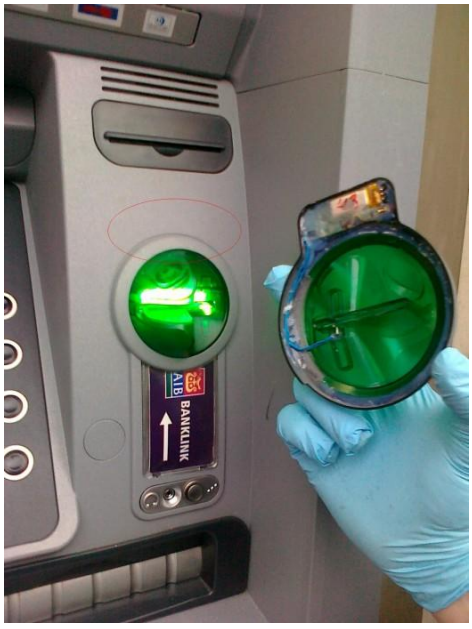
5.2 Dotekové senzory

Jedná se o ojedinělý způsob získání PIN. Ten spočívá v tom, že pachatel nainstaluje senzory na klávesnici bankomatu nebo na vstupní dveře do samoobslužné zóny. Účelem je opět získání PIN. Bývá kombinován s účelovou krádeží, přepadením nebo jiným způsobem, jak se dostat ke kartě postiženého.

5.3 Skimming

Při tomto podvodu pachatelé elektronicky zkopírují originální údaje z magnetického proužku karty na jinou kartu, bez vědomí právoplatného držitele karty. Zařízení se montuje na štěrbinu, do které se vkládá karta nebo formou různých nástavců napodobujících originál nebo formou panelu, který bývá montován na originální součást bankomatu. Zařízení pro odpozorování PIN kódu bývá umísťováno do horního panelu bankomatu (kamera, mobilní telefon) nebo se používá falešná klávesnice, která je samostatně nebo formou celého panelu montována na originální klávesnici nebo panel bankomatu. Při kopírování dochází k záznamu PIN a dalších údajů o držiteli karty. Nedochází ovšem ke kopírování všech ochranných prvků např. kódu a zneužití vyrobeného padělku platební karty bez těchto ochranných prvků, např. pro výběr z bankomatu, kde je kontrolována tzv. druhá stopa, je nemožné. Ve světě ale také existují banky, ve kterých bankomat ochranné prvky svých karet nekontroluje a tak je možné padělek použít k úspěšnému výběru.

Nebo např. někteří obchodníci na internetu je také nevyžadují, takže pak není problém platit skimmovanými kartami. [19]



Obr. 26. Nástavec pro kartu [43]

Obr. 27. Falešná klávesnice [44]

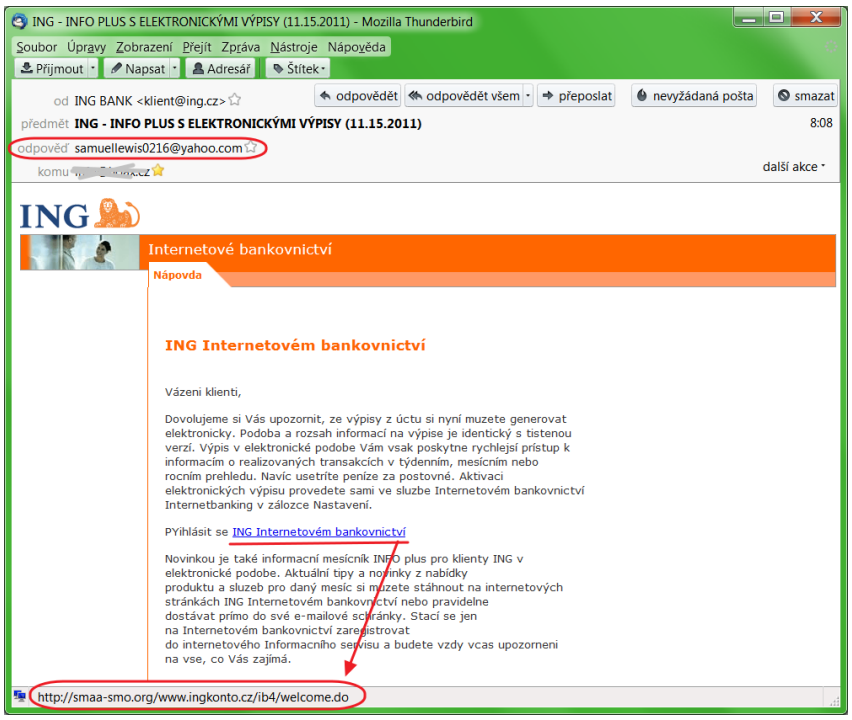
5.4 Padělky karet

Pachatelé vyrábějí padělky karet bez existence bankovního účtu, které jsou v drtivé většině napojené na skutečný účet nějakého majitele. Majitel obvykle nemá tušení o zneužití své karty. Platební karty obsahují mnoho kvalitních zabezpečovacích prvků, které rychle odradí amatérské padělatele karet. Proti organizovaným skupinám jsou však plastové karty bezradné z toho důvodu, že pachatelé disponují stejnou technologií jako výrobci karet. V tom případě je nutné použít vyhodnocování transakcí pomocí programu, který dokáže v určitých případech odhalit podezřelé transakce a včas držitele karty informovat o jejím možném zneužití. [9]

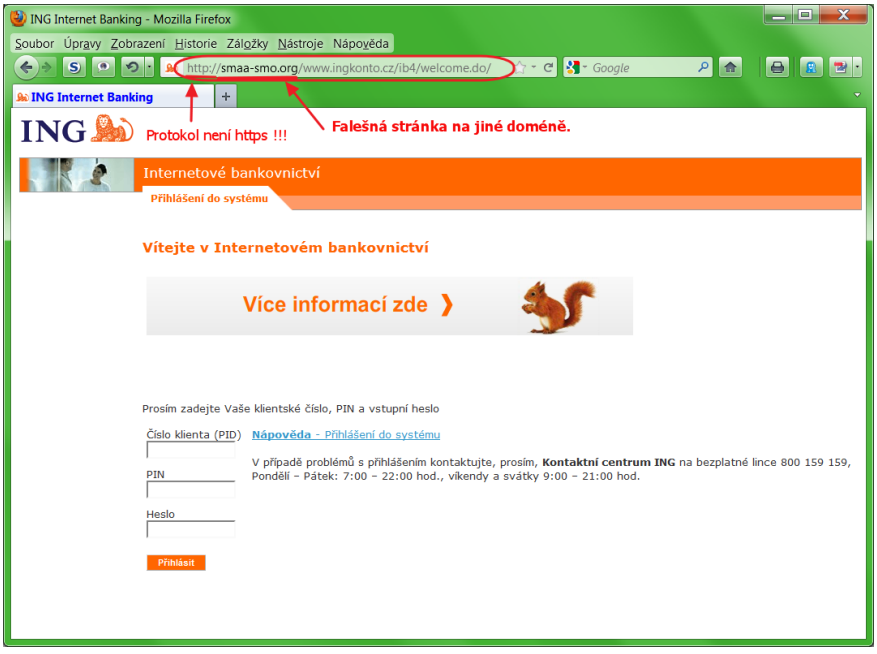
5.5 Phishing

Jedná se o internetovou formu podvodu, při které se snaží podvodníci vylákat z uživatelů internetového bankovnictví jejich přístupové údaje k účtům a zneužít je pro svoje obohacení.

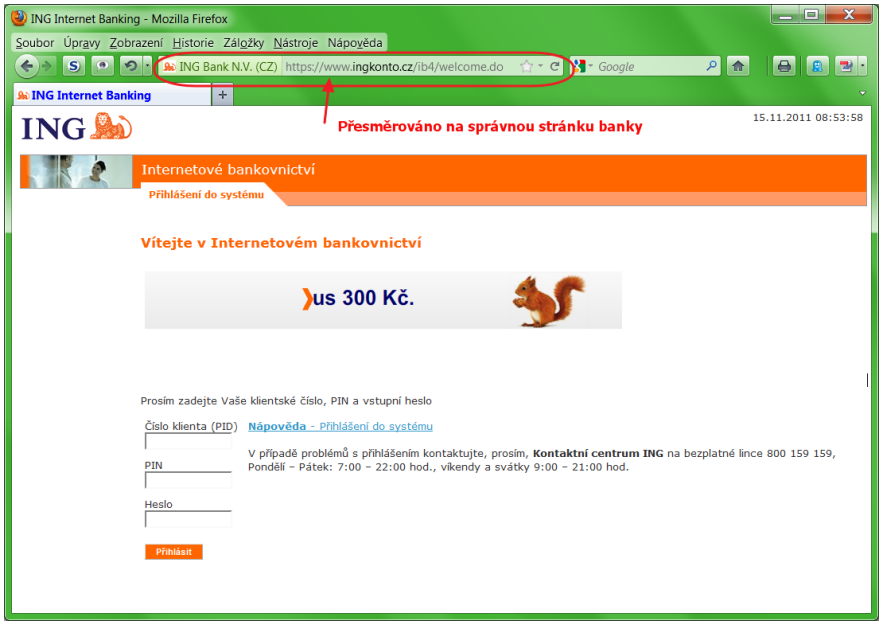
K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vzbuzují dojem, že jsou odeslány přímo z banky uživatele a snaží se jej přesvědčit, aby kliknul na odkaz. V případě že neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde jsou po něm požadovány, přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Když je uživatel naivně vyplní, tak získají tato data podvodníci, kteří je následně využijí pro svůj prospěch. [2]



Obr. 28. Phishing 1 [45]



Obr. 29. Phishing 2 [45]



Obr. 30. Phishing 3 [45]

5.6 Spoofing

V České republice není tato technika dosud rozšířena. Spoofing znamená doslovně napálit, převézt, vodit za nos. Patří zde ty nejnebezpečnější zbraně hackerů, kteří chtějí neoprávněně proniknout do cizích sítí. Podstatou tohoto podvodu je, že se určitý uzel v síti vydává za „někoho jiného“. V důsledku tzv. „osahávání“ serverů nebo lokálních sítí mohou být za určitých podmínek zjištěna citlivá data, která mohou být následně zneužita. [20]

5.7 Trashing

Jedná se o jeden z dalších „moderních“ způsobů podvodů, který je rovněž založen na zjištění citlivých údajů. Název je odvozen od anglického trash tj. koš. V podstatě jde o „vybírání odpadků“, z nichž lze zjistit řadu zajímavých informací. Patří zde přístupová hesla, zdrojové kódy apod. Proto je nutné být pečlivý a data řádně skartaci dokumentů a zabezpečit jejich odvoz a skladování. A to jak ve fyzické, tak i v elektronické podobě. [20]

5.8 Zneužití osobou blízkou

Jedná se o provádění neoprávněných platebních transakcí nebo výběrů z bankomatu blízkými příbuznými, dětmi, přáteli, spolupracovníky. Zjistit údaje o platební kartě pro ně může být velmi snadné a zneužití platební karty poté jednoduché.

5.9 Zneužití osobou cizí

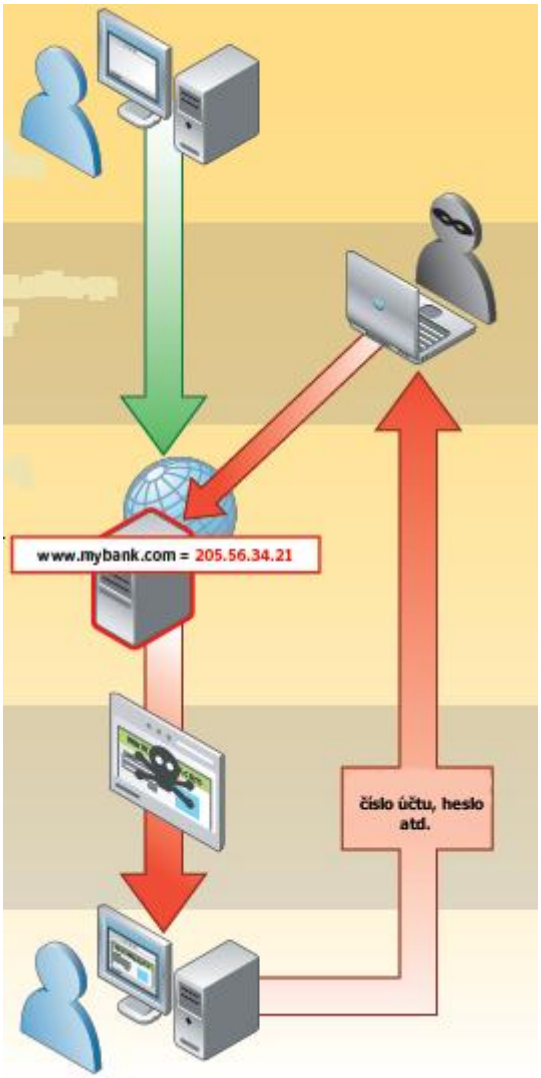
K zneužití dochází obvykle při odcizení nebo ztrátě platební karty. K zneužití osobou cizí však může dojít i při transakcích, kdy se ve většině případů jedná o součinnost podvodníka a podvedené osoby, a to tím způsobem, že si většinou starší občané nevědí rady s obsluhou bankomatu nebo platbou a nabídne se „pomocník“, který jim pomůže např. s výběrem hotovosti. Takový “pomocník“ poté neoprávněně výběr nebo zneužije citlivých údajů platební karty. [20]

5.10 Zneužití držitelem karty

Jde o úmyslné provedení výběru z bankomatu nebo platební transakce, kterou následně dotyčná osoba popře. Tyto podvody nebývají časté, ale dochází k nim. Držitel karty se v takovém případě i vystavuje riziku trestního postihu.

5.11 Pharming

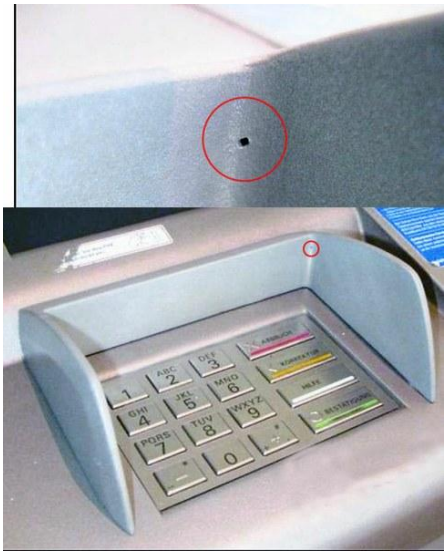
Metoda Pharming spočívá ve využívání speciálních počítačových programů, jež uživatele při přihlášení do internetového bankovnictví přesměrují na stránky, které jsou na rozdíl od phishingu k nerozeznání podobné jako stránky jeho banky, ale doopravdy jsou pouze jejich napodobeninou. Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu po napsání URL banky do prohlížeče. Tady poté uživatele požádají o zadání přihlašovacích hesel a kódů. Když tak klient učiní, mohou se pachatelé přihlásit do internetbankingu pod jeho jménem, a v případě že klient nemá nastaveno další zabezpečení (např. potvrzování transakcí pomocí autorizační SMS nebo klientský certifikát), mohou mu nepozorovaně převést peníze z jeho účtu. [20]



Obr. 31. Pharming [46]

5.12 Skrytá kamera

Za pomoci miniaturní skryté kamery, instalované např. přímo na bankomatu, nebo v jeho blízkosti podvodník zjišťuje PIN. Často se vyskytuje v kombinaci s libanonskou smyčkou nebo skimmingem, někdy při platbě u obchodníka. Je důležité si uvědomit, že skrytou kamerou může být i kamera na mobilním telefonu, kdy může při nepozorném použití platební karty dojít k nahrání jak čísla karty, doby platnosti, CVCV kódu, podpisu, a to např. při platbě „ve frontě“ u obchodníka, kdy osoba, která stojí poblíž, může prostřednictvím mobilního telefonu tyto údaje zjistit. [20]



Obr. 32. Skrytá kamera [47]

5.13 Libanonská smyčka

V dnešní době se jedná již o ojedinělý způsob, kterým se stane to, že platební karta se nedostane do bankomatu, ale ani zpět. Pachatele nainstalují na bankomat speciální dodatečné zařízení, v kterém karta zůstane. Podvodník se nachází v těsné blízkosti a postiženému nabídne „pomoc“ s podmínkou zadání PIN. Ta se ovšem nezdaří a klient odchází bez karty, kterou podvodník následně vytáhne zpět a zneužije ji, než může dojít k její blokaci. Proti tomuto způsobu dnes většinou existuje účinná obrana, kterou banky implementovaly na bankomaty, v podobě dodatečným ochranných adaptérů. [20]

Obr. 33. Libanonská smyčka [48]

5.14 Hradecká lišta

V roce 2008 se objevil v České republice nový druh podvodu, tzv. „Hradeckou lištu". Jednalo se o falešnou zádržnou lištu (zjištěna poprvé na bankomatech v Hradci Králové), nebo falešný nástavec, který překrýval otvor pro výdej peněz na bankomatu. Na liště nebo nástavci byla z vnitřní strany přilepena oboustranná lepicí páska, čehož si uživatel, který přišel k bankomatu, nevšiml. Poté vložil kartu do vstupního otvoru a zadal potřebné údaje pro výběr peněz. Karta vyjela zpět, peníze však nikoliv, protože jsou přilepeny na vnitřní straně zádržné lišty nebo nástavce. Pachatelé si pak počkají, lištu odtrhnou a peníze si vezmou. [11]

Obr. 34. Hradecká lišta [11]

5.15 Keyloogers

Keyloggery jsou aplikace, které jsou instalované v počítači uživatele bez jeho vědomí. Umožňují tak útočníkovi odposlechy klávesnice u přihlašovacích formulářů. Aplikace keyloggeru sama o sobě není pro počítač nebezpečná, ve většině případů je odhalena antivirem. Přesto banky v současné době nabízejí možnost zadání přihlašovacích údajů přes virtuální klávesnici, díky níž se riziko odposlechu minimalizuje. [21]

5.16 Zneužití obsluhou CCTV

Systémy CCTV jsou umísťovány v kavárnách, na budovách poblíž bankomatů, kde monitorují pohyb kolem těchto zařízení. Obsluha CCTV může tento systém zneužít k páchání trestné činnosti. Např. osoba sedící v kavárně zadá do prohlížeče přihlašovací údaje k internetbankingu nebo PIN u bankomatu, čehož může obsluha využít ve svůj prospěch a následně pracovat s těmito údaji. Např. si poslat finanční částku na svůj účet. Případy zneužití obsluhou CCTV jsou však ojedinělé.

5.17 Zneužití pomocí internetu

Karta bývá také často zneužita při placení na internetu. Hlavní problém spočívá v riziku přístupu narušitele do databáze obchodníka, který v ní má uloženou evidenci karet všech svých zákazníků. V České republice je toto riziko prakticky vyloučeno vzhledem k provozování internetových plateb pomocí VISA 3D Secure. S tímto rizikem se můžeme setkat spíše u amerických a asijských obchodníků.

Dalším rizikem je zjištění přihlašovacích údajů za pomocí speciálních programů, které sledují přihlášení do všech druhů účtů na internetu, v případech, kdy se hacker naboural do heslem opatřené sítě. V sítích, kde je možnost se volně připojit např. v internetových kavárnách nebo restauracích, nemusí heslo od sítě zjišťovat. Zde je riziko napadení hackerem mnohem větší.

5.18 Odposlech hovoru

Toto riziko hrozí především u phonebankingu. Spočívá ve zjištění identifikačních údajů uživatele v době, kdy sděluje své přihlašovací údaje operátorovi. Pachatel může údaje zjistit např. pomocí štěnice, což je malý mikrofon, který se umístí v místnosti, kde se sledovaná osoba pohybuje nebo pomocí směrových mikrofonů, které umožnují odposlech na desítky metrů. V případě směrových mikrofonů, nesmí být však odposlouchávaná osoba v místnosti. Další hrozbou je laserový mikrofon. Neviditelný laser se nasměruje doprostřed okenní tabule, kde osoba hovoří. Při hovoru se vytváří mechanické vlnění, které působí na okenní tabuli. Toto vlnění nepatrně hýbe okenní tabulí, což snímá laser. Tento signál jde poté do dekodéru, kde se převede na řeč.

Obr. 35. Směrový mikrofon [49]

Obr. 36. Štěnice [50]

V dnešní době vynalézavost pachatelů nezná mezí. Napomáhá jim k tomu i doba, která jde neustále dopředu a s ní i čím dál vyšší hardwarová a softwarová úroveň zařízení, pomocí kterých se pachatelé dobývají do elektronických platebních systémů. Proto je důležité provádět bezpečnostní opatření a tím zamezit jejich činnosti.

II. PRAKTICKÁ ČÁST

6 DOPORUČENÍ PRO CHOVÁNÍ UŽIVATELŮ ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

Při používání elektronických platebních systémů, je důležité dbát na jejich bezpečné používání a manipulaci. Z tohoto důvodu si řekneme něco o tom, jak elektronické platební systémy bezpečně používat, aby nedošlo k jejich zneužití. Když budeme tyto zásady dodržovat, snížíme tím riziko jejich zneužití na minimum.

6.1 PIN/heslo

PIN (personal identification number) nebo-li osobní identifikační číslo a heslo slouží k jednoznačné identifikaci klienta. Zadání PIN je spojeno s vložením elektronické platební karty do čtečky karet nebo do bankomatu. PIN zadáváme také při práci GSM bankingem a s phonebankingem, když jej sdělujeme operátorovi nebo vyťukáváme na klávesnici mobilního telefonu.

Heslo zadáváme při práci s internetbankingem, homebankingem a systémem elektronické peněženky hardware – based. Zpravidla jej zadáváme do příslušného okna aplikace, kterou vytvořila instituce, jež nám službu poskytuje.

6.1.1 Výběr PIN/hesla

U PIN elektronické platební karty se jedná většinou o kombinaci čtyř číslic. Nedoporučuje se dávat heslo 1 2 3 4, ale mnoho si jej volí z důvodu snadného zapamatování. To však nedoporučuji. Tuto kombinaci totiž zloději zkouší, jako jednu z prvních možností. Stejné zásady platí i pro PIN mobilního telefonu. Tu je ale možnost zadat až šest číslic, záleží na typu mobilního telefonu.

PIN by tedy neměl obsahovat čtyři po sobě jdoucí číslice. Mohl by vypadat např. takto 8164 nebo 2391.

Většina uživatelů volí svá hesla tak, aby si je snadno zapamatovala. Jedná se např. o rodná čísla, jména svých dětí, rodinných příslušníků, či partnerů. Takto zvolená hesla jsou pro pachatele snadno zjistitelná, a proto se doporučuje volit hesla „bezpečnostní“.

Zásady volby bezpečnostního hesla jsou následující:

a) heslo má obsahovat 8 – 20 znaků,
b) volit velká i malá písmena,
c) používat číslice.

Heslo by tedy mohlo vypadat následovně 2Ab698FIpL23An nebo 158aD56l. Se zjištěním takového hesla bude mít i zkušený hacker potíže. Potřeboval by k tomu mnoho času a výkonný počítač.

U PIN a hesla se doporučuje, alespoň jednou do roka je měnit.

6.1.2 Manipulace s PIN/heslem

Lidé si často nepamatují PIN ani heslo a z tohoto důvodu si je zapisují na nevhodná místa, které jsou bohužel většinou velice nápadná. Toho může snadno využít pachatel a zneužít tak jejich hlouposti.

Proto bychom neměli PIN/ heslo:

a) nikomu sdělovat,
b) nikde zaznamenávat.

Když se rozhodneme PIN/heslo sdělit druhé osobě, tak bychom jí měli důvěřovat. V případě, že si tyto údaje někam napíšeme, tak by se mělo jednat o bezpečné místo. **Mezi místa kam si rozhodně PIN/heslo nezaznamenávat patří:**

a) elektronická platební karta,
b) peněženka,
c) mobilní telefon,
d) místo poblíž počítače,
e) počítač,
f) příruční zavazadlo.

Když si PIN/heslo zaznamenáme na nějaký z výše uvedených předmětů, hrozí riziko jeho zneužití při krádeži, či vloupání. Z toho vyplývá, že je nejlepší si tyto údaje zapamatovat!

6.1.3 Jak si zapamatovat heslo?

Téměř každý člověk dnes používá desítky hesel o různých délkách a bezpečností. Problém nastává v tom, jak si je všechny zapamatovat. K tomu slouží různé techniky a pomůcky. Mezi ně patří:

a) mnemotechnické pomůcky,

b) správci hesel.

6.1.3.1 Mnemotechnické pomůcky

Pomocí této jednoduché metody si lze vytvořit a zapamatovat heslo nebo PIN za několik málo minut. Smysl této metody spočívá ve vytvoření pomůcky, která nám pomůže si heslo zapamatovat. Pomůckou může být kombinace, říkanka, vzpomínka nebo událost, ze které si heslo logicky odvodíme.

a) Příklad vytvoření hesla:

např. písnička: **S**kákal **p**es **p**řes **o**ves **p**řes **z**elenou **l**ouku.

Použijeme první písmena slov. Heslo tedy bude SPPOPZL.

b) Příklad vytvoření PIN:

Např. pomocí písmena L. Použijeme při tom pohyb po klávesnici, přičemž výchozí číslo je 1. Heslo tedy bude 1,4,7,8. Kdybychom začali u číslice dva, bude heslo 2,5,8,9.

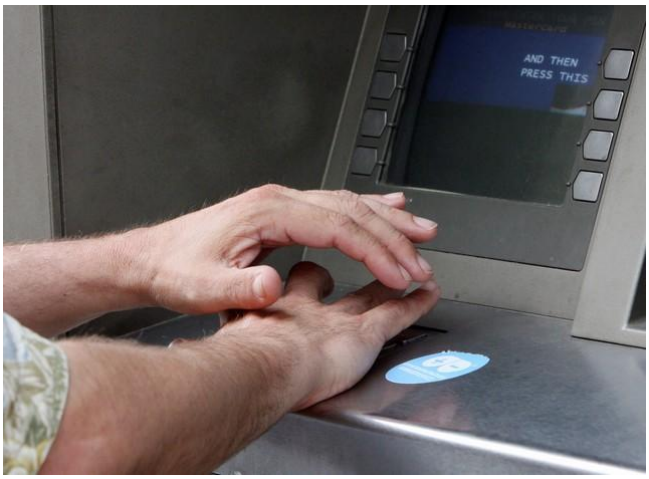
6.1.3.2 Správce hesel

Jedná se o program sloužící k ukládání hesel, PIN a dalších informací. Může se jednat o aplikaci, kterou je třeba nainstalovat nebo může být dostupná na Internetu. Princip spočívá v uložení všech záznamů do programu. Když se spoléháme výhradně na správce hesel, tak je nutné pamatovat si přihlašovací údaje do tohoto programu.

6.1.4 Zadávání PIN/hesla

Při zadávání PIN/hesla bychom měli také dodržovat určité bezpečnostní zásady. **Takže při zadávání by měl člověk:**

a) být ostražitý,
b) zakrývat klávesnici např. rukou,
c) být střízlivý,
d) nebýt pod vlivem omamných a psychotropních látek.



Obr. 37. Správné zadávání PIN [51]

Když všechno shrnu, tak bychom si měli zvolit bezpečný PIN/heslo, které budeme minimálně jednou za rok měnit, nebudeme ho nikomu sdělovat a nikam zaznamenávat! Při zadávání budeme dodržovat bezpečnostní zásady! Když nebudeme tyto doporučené postupy dodržovat, může dojít k zneužití elektronických platebních systémů.

6.2 Ochrana elektronické platební karty

Při používání elektronické platební karty bychom se měli vyvarovat situacím, do kterých se může karta dostat, proto **bychom měli kartu chránit před:**

a) ztrátou,
b) krádeží,
c) mechanickým poškozením.

6.2.1 Ochrana před ztrátou/krádeží

Před ztrátou/krádeží se lze bránit např. tím, že budeme kartu dávat vždy na stejné místo např. do peněženky. V případě, že máme kartu v peněžence, je vhodné ji mít pro větší bezpečnost ještě např. v batohu či kabelce. Když toto nedodržíme a pohybovali bychom se např. v dopravních prostředcích, mohla by nám karta nebo peněženka lehce vypadnout nebo při větším pohybu osob v autobuse či vlaku, by nám ji mohl kapsář nepozorovaně ukrást.

Také se nedoporučuje nosit kartu v ruce, mohli bychom ji někde odložit a zapomenout na ni. Dále bychom neměli kartu nikomu půjčovat a nedovolit personálu, aby ji odnesl z našeho dohledu. Kartu, peněženku nebo příruční zavazadlo, kde máme kartu uloženou, nikde neodkládejte a mějte ji na bezpečném místě!

V případě, že kartu ztratíme nebo nám ji někdo odcizí, je nutné zavolat do banky a tuto událost nahlásit. Banka kartu ihned zablokuje a případnému zloději je k ničemu. Kartu lze také pojistit proti zneužití a máme také možnost nastavit limit, což znamená, jaký obnos můžeme denně vybrat, nebo jakou částku smíme za daný den převést.

6.2.2 Ochrana před mechanickým poškozením

Na internetové stránce dostupné na http://www.mesec.cz/clanky/crash-test-platebnich-karet/ jsem se dočetl, že kartu prakticky nejde uvést do nefunkčního stavu. Když nebudeme kartu vkládat do hrnce s vařící vodou, nebudeme s její pomocí odstraňovat námrazu z čelního skla auta, bude karta funkční.

6.3 Ochrana informací při práci s PC

Při používání internetbankingu, homebankingu a systému elektronické peněženky software – based je důležité zabezpečit PC proti napadení hackerem. Hacker může zjistit pomocí speciálních programů identifikační údaje uživatele a poté je zneužít.

Těmto situacím můžeme předejít, když budeme mít v PC aplikace jako je:

a) brána firewall,
b) antivirový program,
c) antispyware.

6.3.1 Firewall

Česky řečeno „bezpečnostní brána“, je vlastně software, který odděluje provoz mezi dvěma sítěmi tj. naší domácí a internetem, přičemž propouští jedním nebo druhým směrem data podle předem určených a definovaných pravidel. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele.

Obr. 38. Firewall [52]

6.3.2 Antivirový program

Antivirový program sleduje všechny nejdůležitější vstupní/výstupní místa, kterými by viry mohly do počítačového systému proniknout. Pokud se jedná o viry samotné, můžeme říci, že jde o nežádoucí a ve většině případů škodící kód, který se cíleně šíří.

Antivirový program vyhledává a kontroluje data na základě virové databáze. V současnosti vznikají nové viry a jejich mutace téměř každý den proto, musí výrobce na tuto situaci reagovat 24 hodin denně. Virová databáze je tedy průběžně aktualizována a je k dispozici uživatelům ke stažení. [22]

6.3.3 Antispyware

Antispyware je program, který odstraňuje a blokuje programy, jež se bez vědomí uživatele nainstalují do počítače a poté pomocí internetu odesílají data uživatele bez jeho vědomí.

6.3.4 Aktualizace operačního systému a antivirového programu

Je důležité pravidelně aktualizovat operační systém a antivirový program, aby jejich účinnost byla co nejvyšší. Aktuální informace o případných hrozbách a nových virech na internetu bychom měli pravidelně sledovat, nalezneme na těchto internetových stránkách:

a) www.microsoft.com/cze/security

b) www.virovyradar.cz

6.3.5 Volba PC pro práci s elektronickými platebními systémy

Pro práci s internetbankingem, homebankingem a systémem elektronické peněženky software - based používejte pouze bezpečné počítače, které máte plně pod svou kontrolou, tím mám na mysli počítače, u kterých máte možnost ovlivnit jejich bezpečnostní nastavení. Za bezpečný počítač se dá považovat domácí a firemní počítač, který máte přidělen a pracujete na něm pouze Vy.

Nedoporučuji používat počítač např. v internetové kavárně, protože nevíme nic o jeho nastavení.

6.3.6 Obrana proti phishingu/pharmingu

Proti těmto způsobům útoku se ubráníme tak, že nebudeme otvírat podezřelé emaily a nebudeme vyplňovat žádné formuláře, ve kterých bude vyžadováno vyplnění našich přihlašovacích údajů, např. do internetbankingu. Banka nebo instituce, která nám poskytuje některý z elektronických platebních systémů, nevyřizuje tyto záležitosti přes email, nýbrž osobně na pobočce.

Důležité také je navštěvovat pouze známé a důvěryhodné stránky a vyvarovat se stahování neznámých souborů z internetu, zejména s příponou EXE, do svého počítače. Tyto soubory mohou poškodit váš počítač. [2]

6.4 Obrana proti odposlechu

Když u phonebankingu sdělujeme své heslo operátorovi, hrozí odposlech pomocí štěnice, směrových mikrofonů nebo laserového mikrofonu. Proti tomu se můžeme bránit pomocí instalace šumových generátorů. Šumový generátor vytváří akustický šum. Tím v chráněných prostorách znehodnocuje případné snímání hlasu mikrofonem nebo jakýmkoliv jiným zařízením.

Obr. 39. Šumový generátor [53]

6.5 Obrana proti odposlechu klávesnice

Jedná se o situaci, kdy nám někdo bez našeho vědomí nainstaluje do počítače program, který odposlouchává klávesnici. Tedy přesně ví, co právě píšeme, a může tak zjistit, naše identifikační údaje, např. od internetbankingu. Proti tomu se lze bránit používáním virtuální klávesnice, kterou nabízí k použití např. Česká spořitelna.

6.6 Visuální kontrola bankomatu

Při používání bankomatu bychom měli provést jeho vizuální kontrolu. Může na něm být nainstalovaná skrytá kamera, dotykový senzor, falešná klávesnice, libanonská smyčka, hradecká lišta nebo skimmovací zařízení.

6.7 Nastavení limitů

Při založení účtu si můžeme nastavit denní limit. To znamená, jakou maximální částku smíme za jeden den vybrat. Je to účinná obrana, když nám např. kartu někdo ukrade, tak může vybrat pouze částku ve výši limitu.

6.8 Zasílaní informací o pohybech na účtu

V dnešní době nabízejí téměř všechny banky službu, pomocí které se dozvíte o veškerých operacích na vašem účtu nebo s vaší platební kartou. Informace se posílají mailem nebo SMS zprávou.

Dozvěděli jsme se, jak si zvolit bezpečný PIN/heslo, jak se chovat a na co si dát pozor při používání elektronických platebních systémů. Když si vštípíme do paměti tyto zásady a opatření a budeme dodržovat pravidla bezpečného používání, snížíme tak riziko jejich zneužití na minimum.

7 KOMPARATIVNÍ ANALÝZY ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ S OHLEDEM NA JEJICH ZABEZPEČENÍ

7.1 Internetbanking

Pro srovnání jsem si vybral FIO internetbanking od FIO banky, SERVIS 24 od České spořitelny, Internet banku s mobilním klíčem a Internet banku s certifikáty od GE Money.

7.1.1 FIO internetbanking

Aplikace internetbankingu u FIO banky je vybavena vícestupňovou ochranou před zneužitím. Samotný vstup je chráněn uživatelským jménem a heslem. K přihlášení lze použít virtuální klávesnici. Při každé peněžní transakci musí být provedena autorizace pomocí unikátních klíčů chráněných dalším heslem majitele nebo jednorázovým kódem, který zašle banka SMS zprávou na klientem zvolené telefonní číslo. Pro větší ochranu může klient zvolit kombinaci obou autorizací. [23]

Obr. 40. FIO Internetbanking [23]

7.1.2 SERVIS 24

K identifikaci používá jedinečné bezpečnostní prvky. Klientské číslo a heslo, lze také použít klientský certifikát. Heslo můžete zadat pomocí klávesnice počítače, nebo pomocí virtuální klávesnice.

U všech aktivních transakcí je nutné provést autorizaci. Ta se provádí pomocí autorizačního SMS kódu, emailu či klientského certifikátu. [17]

Obr. 41. SERVIS 24 [17]

7.1.3 GE Money

Aplikace se nazývá Internet Banka a je zabezpečena nejmodernějšími technologiemi. Identita stránek banky je ověřována nezávislou certifikační autoritou VeriSign. GE Money nabízí dva druhy zabezpečení. [24]

7.1.3.1 Internet Banka s mobilním klíčem

Přístup do aplikace je možný po zadání přihlašovacího jména, hesla a mobilního klíče. Každý aktivní požadavek je nutné potvrdit mobilním klíčem, který Vám banka zdarma zašle na Váš mobilní telefon registrovaný v bance. [24]

Obr. 42. Internet Banka s mobilním klíčem [24]

7.1.3.2 Internet Banka s certifikáty

U této možnosti je nutné vygenerovat digitální certifikáty, kterými se budete prokazovat při vstupu do Internet Banky či při podepisování transakcí. Přístup je možný po zadání identifikačního čísla a hesla spolu s vloženým digitálním certifikátem. Všechny aktivní operace musí být podepsány digitálním podpisem. [24]

7.1.4 Komparativní analýza

Před vstupem do internetbankingu je ve všech třech případech nutné provést přihlášení. U FIO internetbankingu se vyplňuje uživatelské jméno místo identifikačního čísla. Z hlediska bezpečnosti jde o rizikovější údaj, protože jde snadněji zjistit, než náhodně vygenerované identifikační číslo.

Při přihlášení do Internet Banky od GE Money nelze zadat přihlašovací údaje pomocí virtuální klávesnice. Může tedy dojít k jejímu odposlechu.

U SERVIS 24 máme možnost přihlásit se klientským certifikátem. U Internet Banky musíme zadat přihlašovací údaje a poté vložit mobilní klíč nebo digitální certifikát.

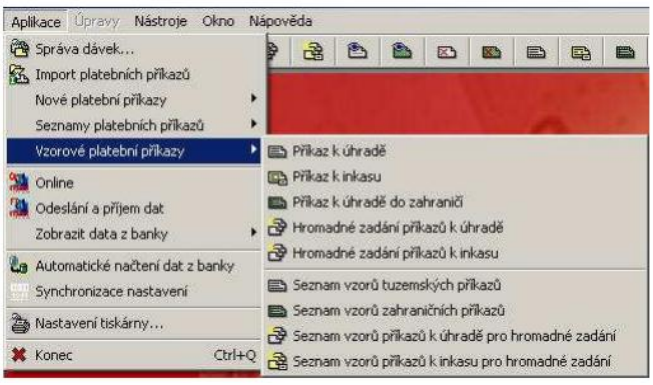
U všech internetbanking systémů je nutné provést autorizaci transakce. Buď pomocí SMS kódu, emailu či klientského certifikátu.

7.2 Homebanking

Pro analýzu jsem vybral MAX Homebanking PS od Poštovní spořitelny a BankKlient od GE Money.

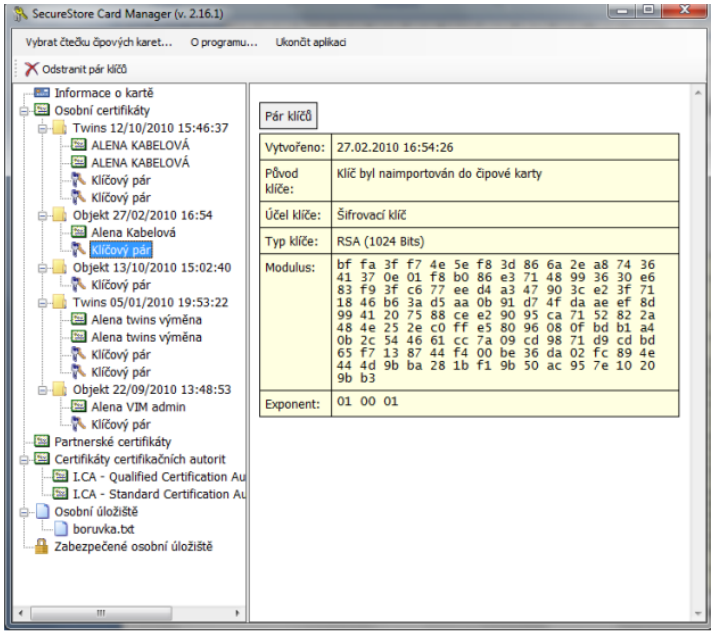
7.2.1 MAX Homebanking PS

Pro spuštění programu je nutné zadat uživatelské jméno a heslo. Tato služba využívá nejvyšší standardy zabezpečení. Všechny finanční transakce musí být opatřeny digitálním elektronickým podpisem osoby, která je oprávněná dané operace podepisovat a odesílat do banky. Certifikát elektronického podpisu je uložen na čipové kartě. [25]



Obr. 43. MAX Homebanking PS [25]

Pro práci s čipovou kartou se používá Správce čipových karet SecureStore, což je samostatný program, který se musí nainstalovat spolu s aplikací MAX Homebanking PS. Pomocí SecureStore měníme PIN, aktivujeme čipovou kartu, generujeme certifikáty a provádíme další operace s čipovou kartou. [25]



Obr. 44. SecureStore [25]

7.2.2 BankKlient

Pro přihlášení musíme zadat uživatelské jméno a heslo. Platby jsou autorizovány elektronickým podpisem založeným na principu tajného a veřejného klíče. Vysoká bezpečnost dat je zajištěna přenosem dat internetem zabezpečeným kanálem, používá se protokol SSL. [24]

Obr. 45. BankKlient 9 [24]

GE Money používá ke generování elektronického podpisu vlastní program BankKlient 9, pomocí kterého se také ovládá veškerá práce s účtem.

Obr. 46. Generování elektronického podpisu [24]

7.2.3 Komparativní analýza

U obou homebanking systému je nutné přihlášení a autorizace pomocí elektronického podpisu. U MAX Homebanking PS je elektronický podpis uložen na čipové kartě a generujeme jej programem SecureStore. Pro generování elektronického podpisu u aplikace BankKlient slouží program BankKlient 9.

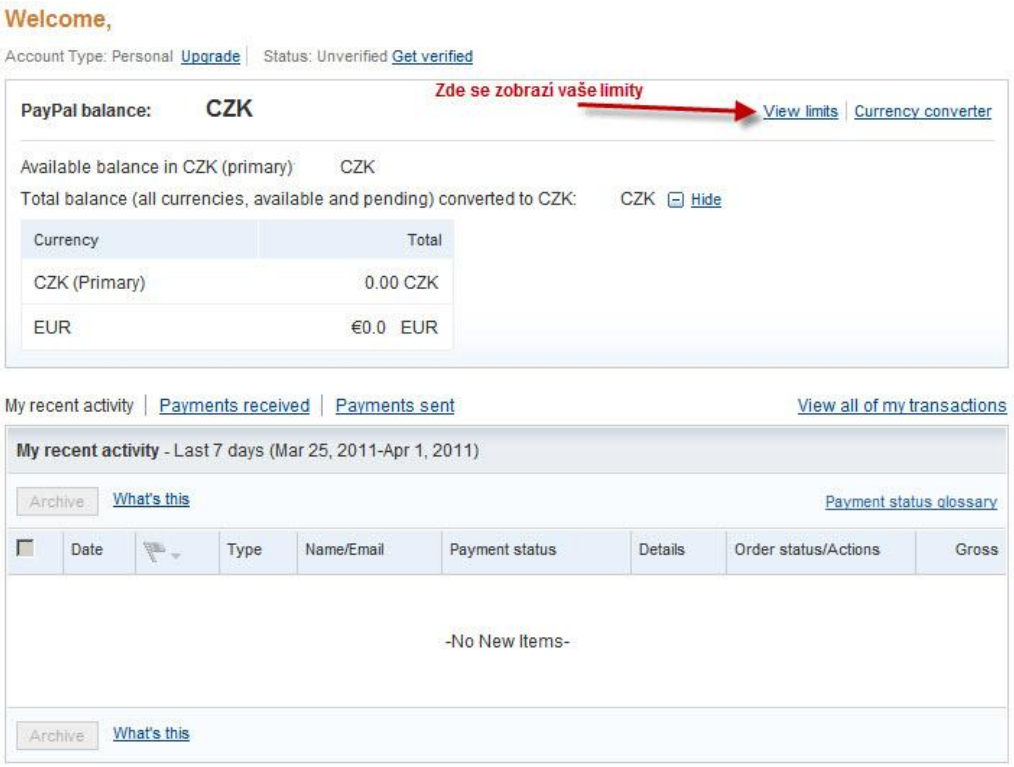
7.3 Systém elektronické peněženky Software – based

U systému elektronické peněženky Software - based budu porovnávat aplikaci PayPal s českou aplikací PaySec.

7.3.1 PayPal

PayPal automaticky šifruje důvěrné informace pomocí protokolu SSL. Ještě před registrací nebo přihlášením jejich server zkontroluje, zda používáme schválený internetový prohlížeč. Když se informace dostanou na stránky PayPal, umístí se na server, který je střežen fyzicky i elektronicky. PayPal servery jsou připojeny za firewallem a nejsou přímo připojeny k internetu, takže naše soukromé informace jsou k dispozici pouze oprávněným počítačům.

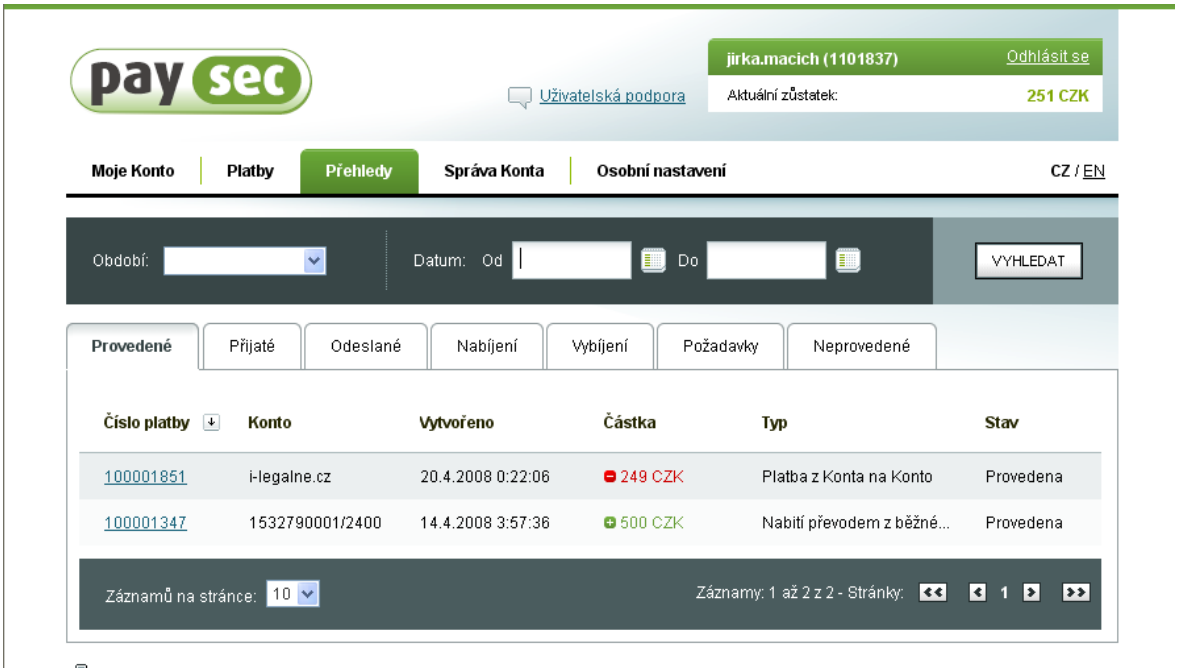
Při provádění transakcí příjemce nikdy nevidí čísla bankovních účtů nebo čísla kreditních karet. Jde vidět pouze e-mailová adresa, datum registrace, a zda jsme dokončili PayPal proces ověřování. [26]



Obr. 47. Účet PayPal [26]

7.3.2 PaySec

K vstupu do programu musí uživatel zadat uživatelské jméno a heslo. Pro zajištění bezpečnosti komunikace se používá šifrování pomocí technologie SSL. Pro navázání šifrované komunikace PaySec používá certifikát jejich serveru vydaný certifikační autoritou. Při platbě větší, než je nastavený limit, se provádí autorizace pomocí SMS zprávy. [27]



Obr. 48. Účet PaySec [27]

7.3.3 Komparativní analýza

Pro přihlášení do obou systémů je nutné přihlášení. U PayPal i PaySec probíhá komunikace se zákazníkem pomocí protokolu SSL. PayPal navíc ověřuje, jestli máme vyhovující internetový prohlížeč. Oba dva systémy po provedení transakce neukazují čísla bankovních účtů nebo čísla kreditních karet. Příjemce vidí pouze identifikační údaje o platbě.

V této kapitole jsme se dozvěděli, jaké jsou bezpečnostní opatření konkrétních aplikací skutečných bank či institucí, v čem se liší a v čem se shodují. Také jsme zjistili, jak se do aplikací přihlašovat a jakým způsobem provádět autorizace.

8 DOTAZNÍK

Na základě mého tématu jsem vytvořil dotazník, který je dostupný z http://bezpecnost-elektronickych-pl.vyplnto.cz. Dotazník je zaměřen především na chování uživatelů při používání elektronických platebních systémů a obsahuje celkem 23 otázek.

Dotazník vyplnilo 128 lidí. Z toho 77 mužů a 51 žen s věkovým průměrem 25 let.

8.1 Analýza dotazníku

Pouze 6% dotázaných nepoužívá žádný z elektronických platebních systémů. Nejvíce lidí používá platební kartu (86%) a internetbanking (80%).

Platební kartu před ztrátou či krádeží chrání 97% tázaných, ale svůj PIN/heslo sdělilo druhé osobě celých 25% tázaných, což je poměrně vysoký počet. Mezi pozitiva bych zařadil to, že si 85% tázaných pamatuje svůj PIN a pouze 1% tázaných jej nosí spolu s kartou. Při zadávání PIN je vždy ostražitých 73% tázaných a 46% tázaných zakrývá klávesnici rukou. Pouze 21% tázaných si mění pravidelně PIN, což je hodně malé číslo, zato v podnapilosti použilo některý z elektronických platebních systémů 54% tázaných nejvíce platební kartu 35% tázaných. Dobrá zpráva je, že 74% tázaných chrání svůj počítač firewallem, ale 15% tázaných nemá ponětí, co tento pojem znamená. Elektronickým platebním systémům důvěřuje 87% tázaných ale 66% tázaných pouze, když dodržují bezpečnostní pravidla.

Při analýze dotazníku jsem zjistil, že některá bezpečnostní pravidla se dodržují více a některá méně. S výsledky jsem ale spokojen nebyl. Je to možná i tím, že lidé neznají většinu bezpečnostních opatření, a tudíž je ani nenapadne je používat.

Celý dotazník s výsledky a grafy najdete v příloze.

ZÁVĚR

Tato diplomová práce se zabývá jedním z aktuálních témat, a to bezpečností elektronických platebních systémů. Každý člověk by měl být informován o tom, jaké rizika při jejich používání hrozí. Člověk může těmto rizikům předejít, když bude dodržovat zásady jejich bezpečného používání. Z tohoto důvodu jsem se je snažil popsat všechna rizika a způsoby, jak by se měl člověk chovat, aby elektronické platební systémy nebyly zneužity.

Úvodní část práce pojednává o základním rozdělení elektronických platebních systémů. Dnes nejvíce používaným elektronickým platebním systémem jsou elektronické platební karty, které používá většina z nás. Na druhé místo bychom mohli zařadit internetbanking, pomocí kterého můžeme v kteroukoliv dobu spravovat svůj účet.

V třetí části se zabývám protokoly a aplikacemi, které se používají při práci s elektronickými platebními systémy. Například protokol SSL slouží k bezpečnému přenosu dat pomocí internetu od banky ke klientovi a naopak.

Nejdůležitější je však samotná bezpečnost elektronických platebních systémů. To znamená, jak je instituce, které nám je vydaly, chrání před zneužitím třetí osobou. K tomu slouží např. identifikace v podobě uživatelského jména a hesla nebo autorizace před provedením transakce.

V elektronických platebních systémech koluje obrovské množství peněz. Toho se snaží využít různí hackeři a padělatelé. Ti vytvářejí speciální programy a zařízení, pomocí kterých se chtějí k těmto penězům dostat. V páté kapitole jsem se proto pokusil popsat nejvíce takových hrozeb, zařízení a způsobů zneužití.

V praktické části jsem zpracoval „příručku uživatele elektronických platebních systémů“. Popsal jsem např., jak si správně zvolit PIN/heslo a jak s ním zacházet. Také jak zabezpečit svůj osobní počítač nebo platební kartu. V sedmé kapitole jsem si vybral produkty (aplikace) některých bank, u kterých jsem provedl analýzy s ohledem na jejich bezpečnost.

Na konci diplomové práce jsem provedl analýzu dotazníku, který jsem vytvořil. Jednalo se o dotazník zaměřený na používání elektronických platebních systémů s ohledem na chování lidí, kteří je využívají. S výsledky jsem však nebyl spokojen, i když se většina lidí snaží chovat obezřetně při jejich používání.

ZÁVĚR V ANGLIČTINĚ

This thesis deals with one of the current issues, namely the electronic payment systems security. Everyone should be informed about the electronic payment use risks. One can avoid the risks, if observes the safe use principles. For this reason I have tried to describe all the risks and how one should behave not to electronic payment systems misuse.

The introductory part deals with the basic electronic payment systems division. Nowadays the most used electronic payment system is an electronic payment card most of us use. In the second place we could include the internet banking we can use to manage our account anytime.

In the third part there I deal with protocols and applications that are used to do with the electronic payment systems. For example, the SSL protocol is used for the secure data transmission via the Internet from a bank to a client and vice versa.

The electronic payment systems security is the most important. That means how the systems are protected against a third parties misuse by the institutions that issue the protocol. To protect them there is for example the identification via user name and password or an authorization before the transaction.

In the electronic payment systems there lots of money circulates. Different hackers and counterfeiters try to use it. They create special programs and facilities to get this money. Therefore in the fifth chapter there I have tried to describe most of those threats, devices and ways of abuse.

In the practical part there I have elaborated "The electronic payment systems user guide". There I describe for example how to properly choose a PIN / password, how to handle it and also how to secure your personal computer or credit card. In the seventh chapter there I had chosen some banks products (applications) that I have analysed with respect to their safety.

At the end of the thesis I have analysed the questionnaire I had created. The questionnaire focuses on the electronic payment systems use with respect to the behaviour of people who use them. But I have not been satisfied with the results even though most people try to act cautious when using them.

SEZNAM POUŽITÉ LITERATURY

[1] BERÁNEK, Ladislav. Bezpečnost online systémů a platebních systémů. [online]. Dostupné z: http://ecom.ef.jcu.cz/web/download/teorie/p06-bezpecnost.pdf

[2] JAMES, Lance. Phishing bez záhad. 1. vyd. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1766-1.

[3] MÁČE, Miroslav. Platební styk – klasický a elektronický. 1. vyd. Praha: Grada Publishing, a.s., 2006. 220 s. ISBN 80-247-1725-5.

[4] MATYÁŠ, Vašek, KRHOVJÁK, Jan. Autorizace elektronických transakcí a autentizace dat i uživatelů. 1. vyd. Brno: Masarykova universita, 2008. 125 s. ISBN 978-80-210-4556-9.

[5] SCHLOSSBERGER, Otakar, HOZÁK, Ladislav. Elektronické platební prostředky. Praha: Bankovní institut vysoká škola, 2005. ISBN 80-7265-073-4.

[6] SMEJKAL, Ladislav. Elektronické peníze. [online]. Ikaros. 2001, roč. 5, č.10, ISSN 1212-5075. Dostupné z: http://www.ikaros.cz/elektronicke-penize

[7] O financích. *Peníze.cz* [online]. 2000 - 2012 [cit. 2012-05-14]. Dostupné z: http://www.penize.cz/

[8] Bankomat. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012 [cit. 2012-05-14]. Dostupné z: http://cs.wikipedia.org/wiki/Bankomat

[9] Průvodce finančním světem. *Měšec.cz* [online]. 1998 – 2012 [cit. 2012-05-14]. Dostupné z: http://www.mesec.cz/

[10] Bezkontaktní čtečka. In: *Finanční noviny* [online]. 2011 [cit. 2012-05-14]. Dostupné z: http://www.financninoviny.cz/os-finance/zpravy/cs-zacne-od-pondeli-vydavat-bezkontaktni-platebni-karty/694472&id_seznam=

[11] O financích. *Zlatakoruna.cz* [online]. 2003 - 2012 [cit. 2012-05-14]. Dostupné z: http://www.zlatakoruna.info/

[12] *Produkty elektronického bankovnictví* [online]. Pardubice, 2010 [cit. 2012-05-14]. Dostupné z: http://dspace.upce.cz/bitstream/10195/37103/1/MullerovaM_Produkty%20elektronickeho_PD_2010.pdf. Bakalářská práce. Universita Pardubice.

[13] Kryptografie. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012 [cit. 2012-05-14]. Dostupné z: http://cs.wikipedia.org/wiki/Kryptografie

[14] O bezpečnosti. *Security-portal.cz* [online]. 2005-2012 [cit. 2012-05-14]. Dostupné z: http://www.security-portal.cz/

[15] SIM Application Toolkit - Stará technologie pro nové aplikace. In: *Hw.cz* [online]. 2004 [cit. 2012-05-14]. Dostupné z: http://www.hw.cz/produkty/sim-application-toolkit-stara-technologie-pro-nove-aplikace.html

[16] Plastové karty. In: *Best a Print* [online]. -2012 [cit. 2012-05-14]. Dostupné z: http://www.bestaprint.cz/karty

[17] Česká spořitelna. *Csas.cz* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.csas.cz/banka/appmanager/portal/banka?_nfpb=true&_pageLabel=subportal01

[18] Telefonní bankovnictví. In: *Citibank Česká republika* [online]. 2011 [cit. 2012-05-14]. Dostupné z: http://www.citibank.cz/czech/gcb/personal_banking/czech/static/telefonni_bankovnictvi.htm

[19] SKIMMING. In: *Policie České republiky* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://www.policie.cz/clanek/skimming.aspx

[20] Technické členění podvodů. In: *Podvody v e-bankovnictví* [online]. 2009-2012 [cit. 2012-05-14]. Dostupné z: http://www.prevencepodvodu.cz/podvodne-praktiky/technicke-cleneni-podvodu.php

[21] Phishing aneb rhybaření. In: *EMAG* [online]. 2008 [cit. 2012-05-14]. Dostupné z: http://www.emag.cz/phishing-aneb-rhybareni/

[22] O antivirech. In: *Antivirismus boje proti virům* [online]. 2007 [cit. 2012-05-14]. Dostupné z: http://antiviry.unas.cz/antiviry.html

[23] FIO banka. *FIO banka* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://www.fio.cz/

[24] O GE Money. *GE Money Česká republika* [online]. 2001-2012 [cit. 2012-05-14]. Dostupné z: http://www.gemoney.cz/ge/cz/1/pujcky/expres-pujcka?gemid1=5393&AgentID=21557

[25] ERA. *Poštovní spořitelna* [online]. 2012 [cit. 2012-05-14]. Dostupné z: https://www.erasvet.cz/

[26] O PayPal. *PayPal* [online]. 1999-2012 [cit. 2012-05-14]. Dostupné z: https://www.paypal.com/cz

[27] PaySec. *PaySec* [online]. 2007-2012 [cit. 2012-05-14]. Dostupné z: http://www.paysec.cz/

[28] VISA Electron. In: *Amino* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://www.amino.dk/forums/t/106888.aspx

[29] VISA Classic. In: *UniCreditBank* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.unicreditbank.cz/cz/obcane/karty/kreditni-karty/embosovana-kreditni-karta-s-moznosti-charity.html

[30] Imprinter. In: *Quaronline* [online]. 2010-2012 [cit. 2012-05-14]. Dostupné z: http://www.quaronline.com/bacaladera-imprinter-card.php

[31] Idnes.cz. *Http://www.idnes.cz/* [online]. 1999-2012 [cit. 2012-05-14]. Dostupné z: http://www.idnes.cz/

[32] BIP-1300 Computer. In: *RACO industries* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.racoindustries.com/pidion-bip-1300-mobile-computer-features.htm

[33] Kontaktní čtečka. In: *ČSOB* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.csob.cz/cz/firmy/Podnikatele/Platebni-karty/Stranky/Platebni-terminal-pro-prijimani-platebnich-karet.aspx

[34] Elektronická peněženka. In: *ČSAD Uherké Hradiště* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://www.csaduh.cz/content-img/karta-obcanska.jpg

[35] POHODA. In: *Stormware* [online]. 2011 [cit. 2012-05-14]. Dostupné z: http://www.stormware.cz/pohoda/homebanking.aspx

[36] Hlasový automat. In: *2N* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.2n.cz/cz/produkty/umts-produkty/officeroute/pripadove-studie/

[37] Tcp/ip. In: *Síťový protokol TCP/IP* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.maturita.cz/referaty/informatika/tcp_ip.htm

[38] SSL. In: *Tech republic* [online]. 2008 [cit. 2012-05-14]. Dostupné z: http://www.techrepublic.com/blog/networking/ssltls-certificates-perspectives-helps-authentication/644

[39] VISA 3D Secure. In: *Platební systémy* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://platebni-systemy.webnode.cz/news/nova-sluzba-payu/

[40] Platební karty. In: *Wikimedia* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://upload.wikimedia.org/wikipedia/commons/7/76

[41] Autentizační kalkulátor. In: *Alsoft* [online]. 2012 [cit. 2012-05-14]. Dostupné z: https://sig1.alsoft.cz/eCobra.Demo/Content/Images/Catalog/GO3.png

[42] Krádež peněženky. In: *Udalosti112* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.udalosti112.cz/pic/2011-06-02kradez.jpg

[43] Skimmovací zařízení. In: *Sociable* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://sociable.co/wp-content/uploads/2011/02/removed-aib-atm-skimming-device-522x696.jpg

[44] Falešná klávesnice. In: *Europol* [online]. 2011 [cit. 2012-05-14]. Dostupné z: https://www.europol.europa.eu/sites/default/files/images/card_skimming_02.preview.jpg

[45] Phishing. In: *Hoax* [online]. 2010 [cit. 2012-05-14]. Dostupné z: http://www.hoax.cz/phishing/ing---info-plus-s-elektronickymi-vypisy-11152011/

[46] Pharming. In: *Barbobe* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.barbone.cz/picture/logo/bezpecnost/image_13d.png

[47] Skrytá kamera. In: *Chip* [online]. 2009 [cit. 2012-05-14]. Dostupné z: http://www.chip.cz/images/2010/12/08/bankomati.jpg/image_preview/bankomati.jpg

[48] Lisabonská smyčka. In: *Webgarden* [online]. 2009 [cit. 2012-05-14]. Dostupné z: http://media0.webgarden.name/images/media0:4cab1e5850fd0.jpg/Libanonsk%C3%A1%20smy%C4%8Dka%201.jpg

[49] Směrový mikrofon. In: *Hyperinzerce* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://img2.hyperinzerce.cz/x-cz/inz/4576/4576357-parabolicky-smerovy-mikrofon-stetoskopicky-1.jpg

[50] Štěnice. In: *Zbozizreklam* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.zbozizreklam.cz/Fotografie/Zbozi/Original/stenice.jpg

[51] Zadávání PIN. In: *Ahaonline* [online]. 2011 [cit. 2012-05-14]. Dostupné z: http://img.ahaonline.cz/img/18/full/802100_bankomat-ruce.jpg

[52] Firewall. In: *Blogspot* [online]. 2011 [cit. 2012-05-14]. Dostupné z: http://3.bp.blogspot.com/-FzZ5f4TC31Q/T2HwCzBKBCI/AAAAAAAAAFY/eClW6eBDyNQ/s1600/firewall.jpg

[53] Šumový mikrofon. In: *odposlechy24* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://www.odposlechy24.cz/files/images/252_230_png-2.jpg

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCTV	Closed Circuit Television
SIM	Subscriber Identity Module
PIN	Personal Identification Number
GSM	Groupe Spécial Mobile
USB	Universal Serial Bus
IP	Internet Protokol
DNS	Domain Name System
URL	Uniform Resource Locator
PC	Personal Computer
tj.	to je
atd.	a tak dále
např.	například

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

1. Jste?

muž žena

2. Věk?

0 - 18 let 19 - 30 let 31 - 50 let 51 let a více

3. Nejvyšší dosažené vzdělání?

základní vyučen s maturitou vysokoškolské

4. Jaké druhy elektronických platebních systému používáte?

Zvolte alespoň jednu možnost, maximálně 5 možností.

platební kartu phonebanking internetbanking GSM banking homebanking nepoužívám elektronickou peněženku

5. Máte platební kartu?

ano ne

6. Platební kartu mám od:

0 - 15 let 16 - 21 let 22 - 30 let 31 let a více

7. Ztratili jste někdy platební kartu?

ANO NE

8. Byla Vám někdy platební karta odcizena?

ANO NE

9. Nosíte platební kartu u sebe?

○ ano, používám ji denně ○ ano, používám ji několikrát týdně ○ ne, pouze když potřebuji vybrat peníze ○ ne, kartu mám, ale nepoužívám ji

10. Platební kartu máte uschovanou?

○ v peněžence ○ v kapse ○ v batohu, kabelce či tašce ○ Jiná odpověď: _____

11. Sdělil/a jste někomu svůj PIN či heslo?

○ partnerovi ○ kamarádovi ○ rodinnému příslušníkovi ○ cizímu člověku ○ nesdělil

12. Píšete si někde PIN?

☐ na platební kartu ☐ do mobilu ☐ mám ho v peněžence spolu s kartou ☐ mám ho označený na bezpečném místě ☐ pamatuji si ho ☐ Vlastní odpověď: _____

13. Jste ostražití při zadávání PIN?

○ ano ○ ano, klávesnici zakrývám rukou ○ jak kdy ○ ne

14. Měníte si pravidelně heslo či PIN?

○ jednou za půl roku ○ jednou za rok ○ ne

15. Používáte internetbanking?

○ ano ○ ne

16. Používáte firewall?

ano ne nevím, co to je

17. Heslo od internetbankingu máte?

v hlavě označené na bezpečném místě na papíře u počítače na pracovní ploše počítače Vlastní odpověď:

18. Obsluhujete internetbanking či homebanking před druhými osobami?

před partnerem před kamarády před rodinou před cizími lidmi ne Vlastní odpověď:

19. Používáte elektronickou peněženku?

ano ne

20. Kde využíváte elektronickou peněženku?

v autobuse ve vlaku ve škole Vlastní odpověď:

21. Který z elektronických platebních systému je podle Vás nejvíce zranitelný?

platební karta internetbanking phonebanking homebanking GSM banking elektronická peněženka Vlastní odpověď:

22. Použili jste někdy v podnapilosti některý z elektronických platebních systémů?

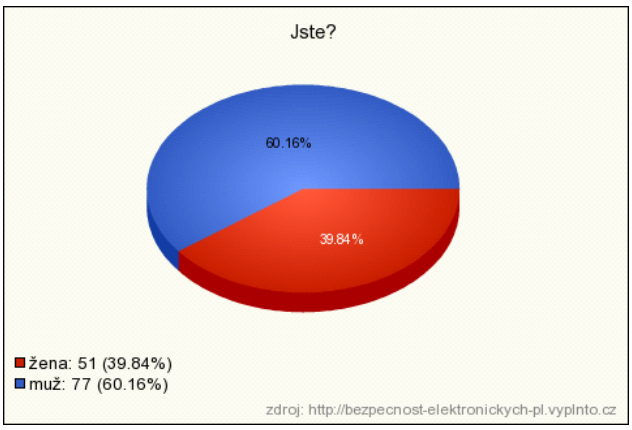
ano ano, především platební kartu ne

23. Důvěřujete elektronickým platebním systémům?

ano ano, když dodržuji bezpečnostní pravidla ne

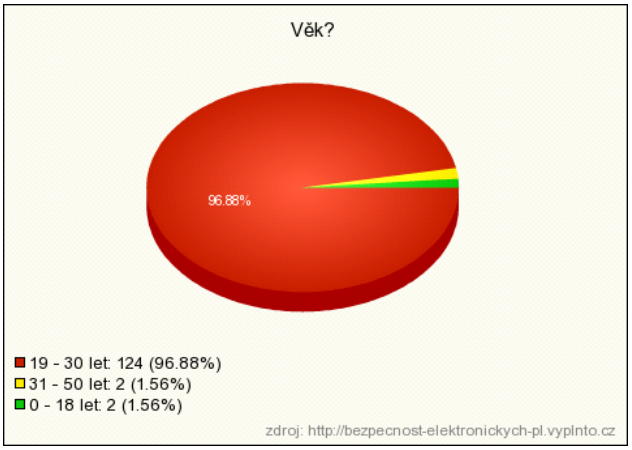
PŘÍLOHA P II: GRAFY DOTAZNÍKU

1)



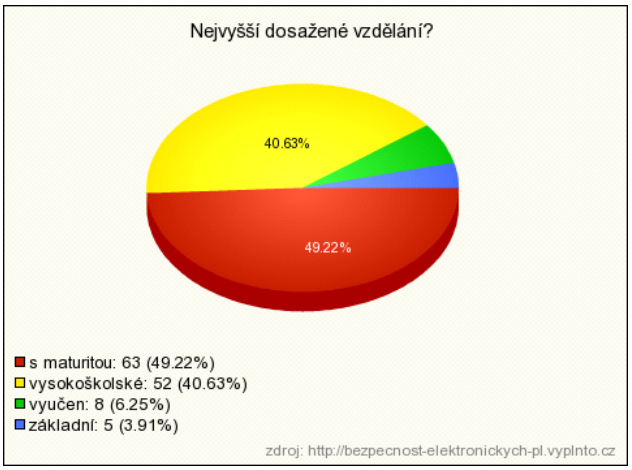
Graf 1. Muž/žena

2)



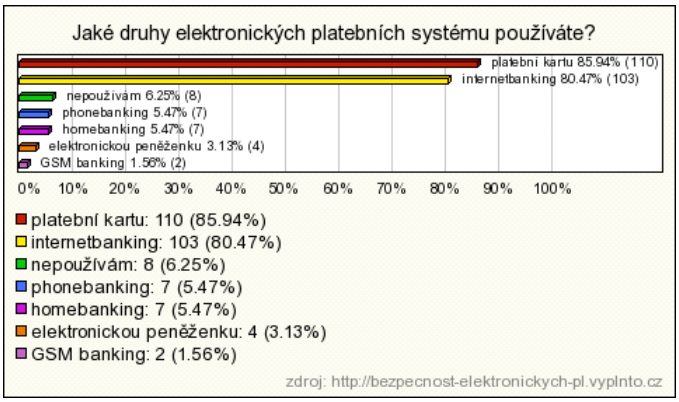
Graf 2. Věk

3)



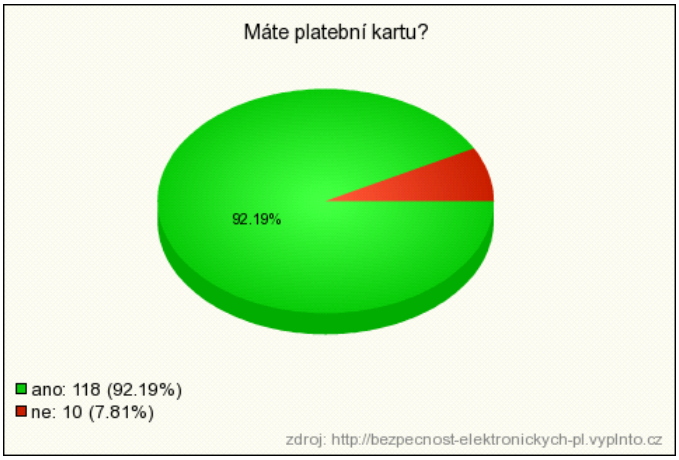
Graf 3. Vzdělání

4)



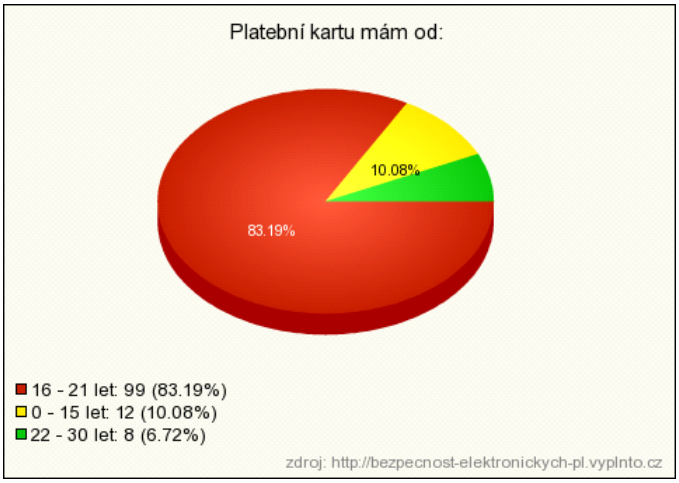
Graf 4. Druhy EPS

5)



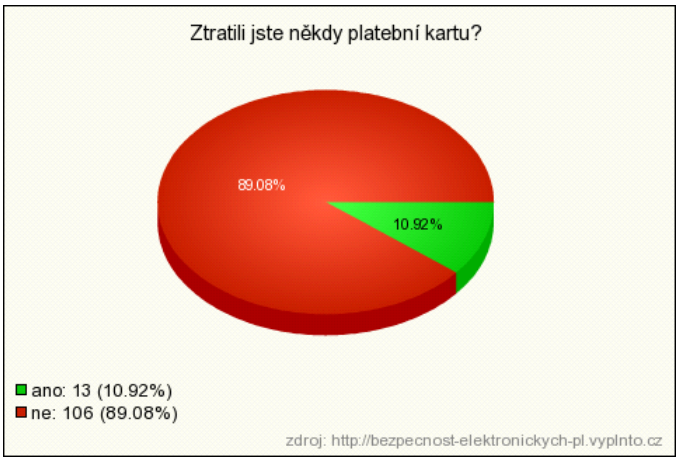
Graf 5. Máte kartu

6)



Graf 6. Kartu mám od

7)



Graf 7. Ztráta karty

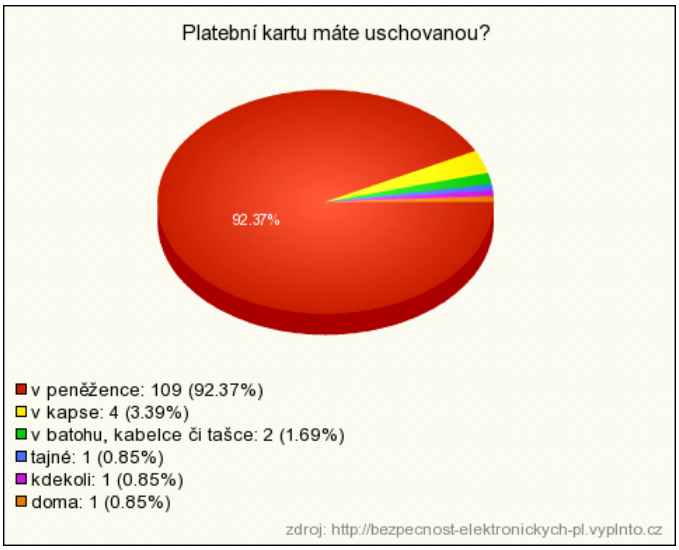
8)

Graf 8. Krádež karty

9)

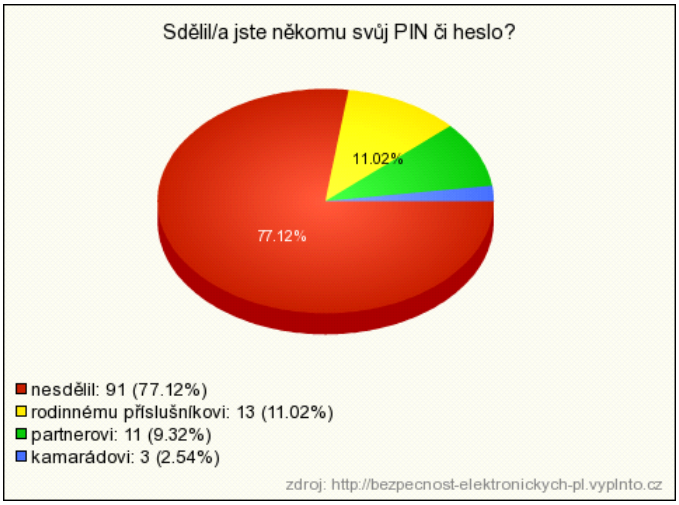
Graf 9. Nosíte kartu u sebe

10)



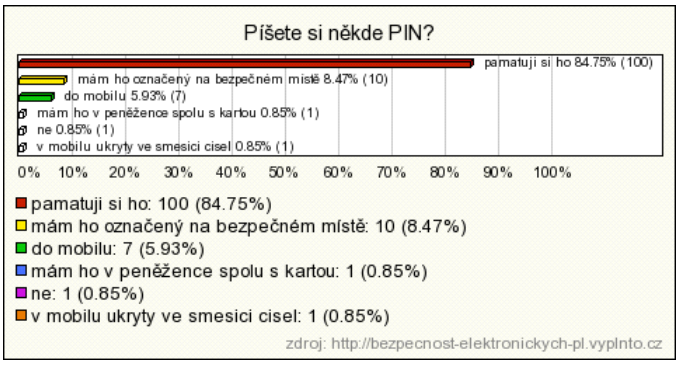
Graf 10. Kartu máte uschovanou

11)



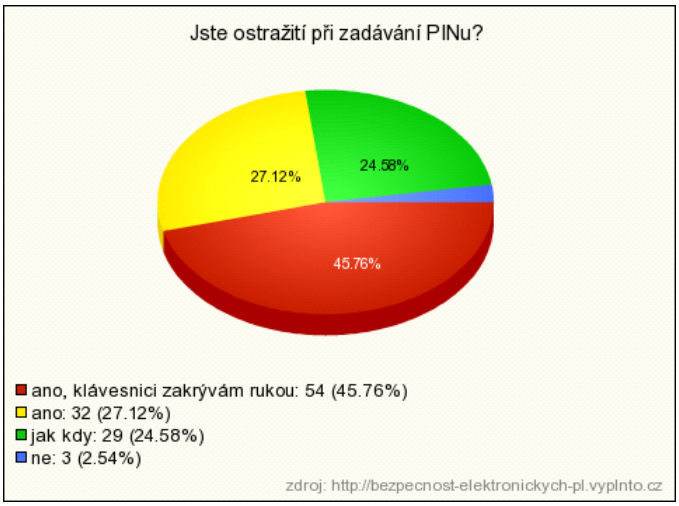
Graf 11. Sdělil jste někomu PIN

12)



Graf 12. Píšete si někde PIN

13)

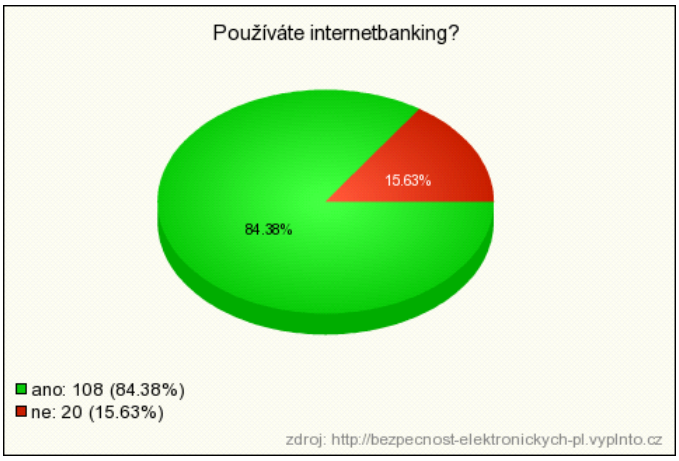


Graf 13. Jste ostražití

14)

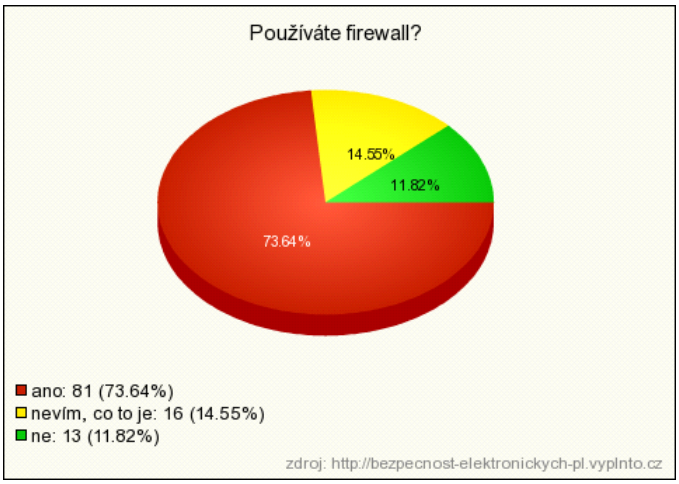
Graf 14. Měníte si PIN

15)



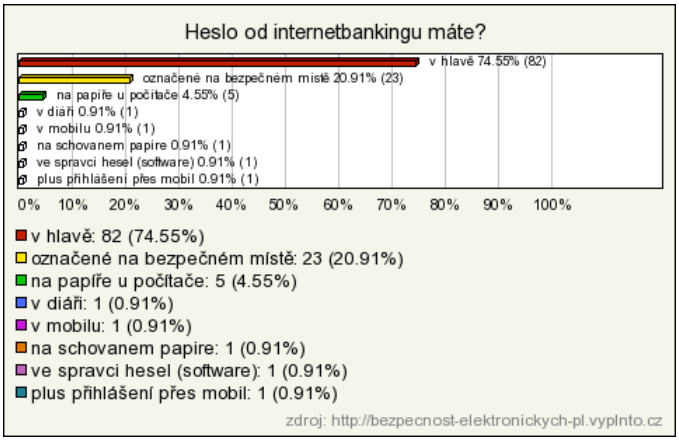
Graf 15. Používáte internetbanking

16)



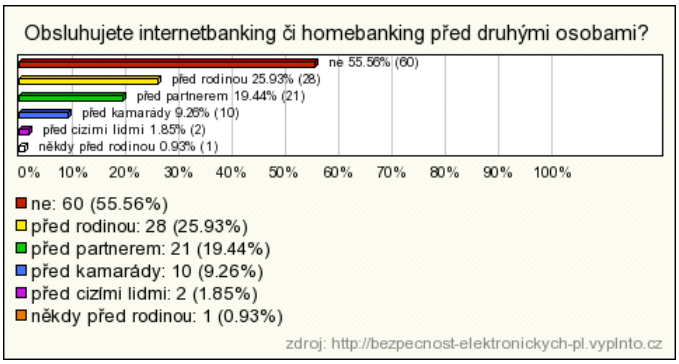
Graf 16. Používáte firewall

17)



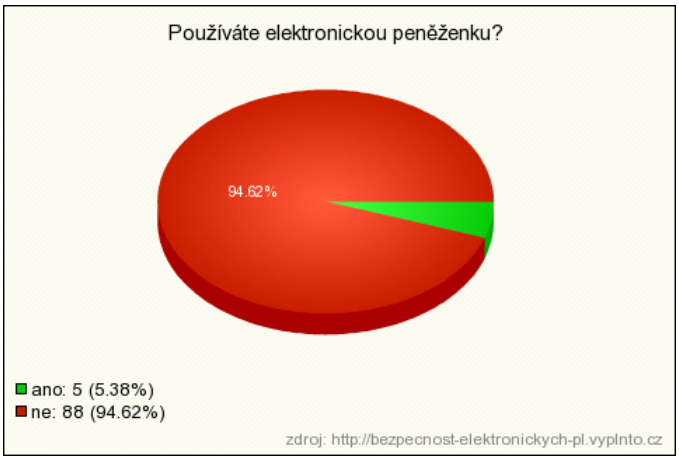
Graf 17. Heslo od internetbankingu máte

18)



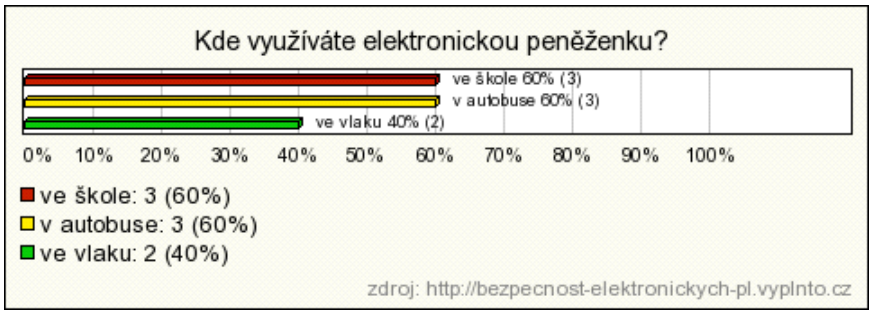
Graf 18. Obsluhujete EPS před druhými osobami

19)



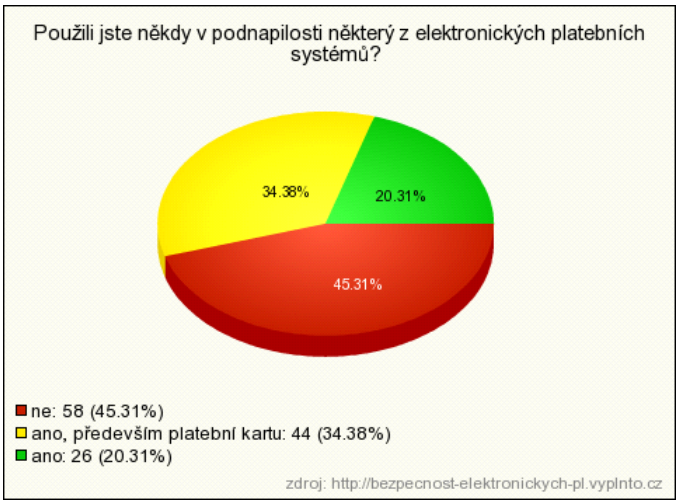
Graf 19. Používáte elektronickou peněženku

20)



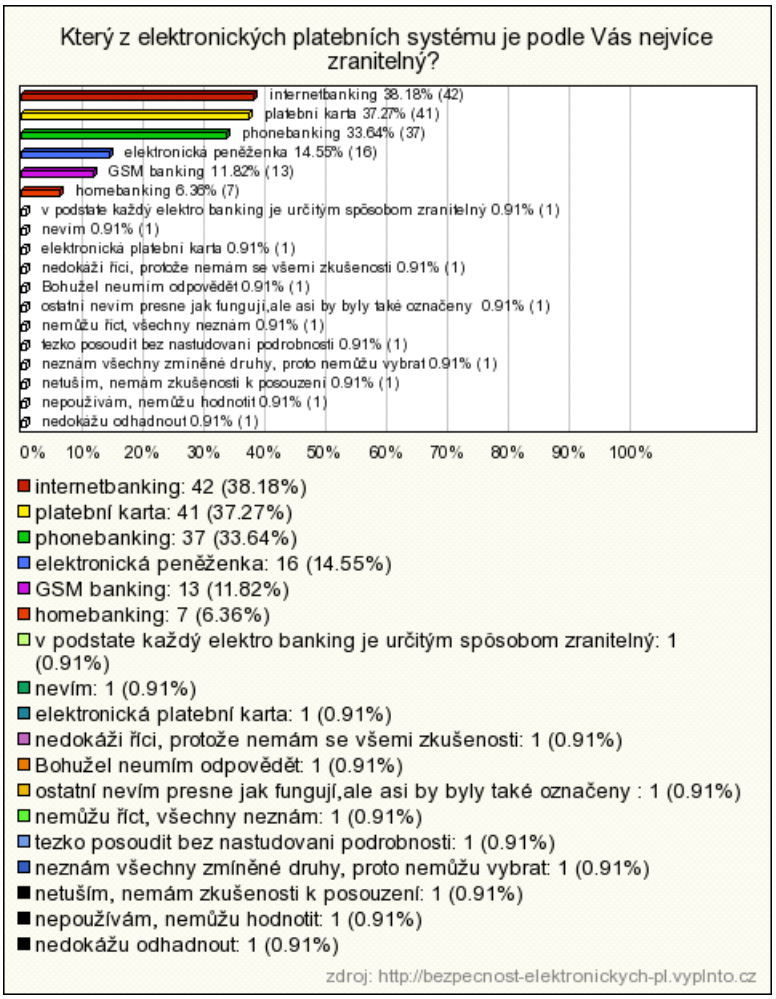
Graf 20. Kde využíváte elektronickou peněženku

21)



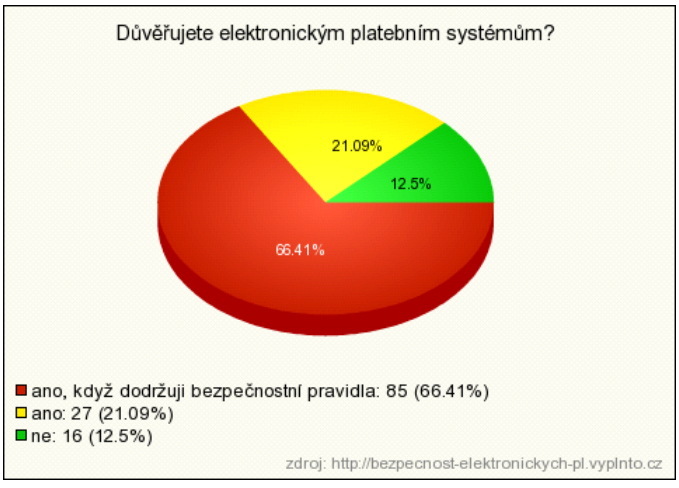
Graf 21. Použití v podnapilosti

22)



Graf 22. Nejvíce zranitelný EPS

23)



Graf 23. Důvěřujete EPS