Bezpečnostní a ekonomické aspekty elektronického bankovnictví

Richard Guriča

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Richard Guriča**
Osobní číslo:	**A11811**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnostní a ekonomické aspekty elektronického bankovnictví**
Téma anglicky:	**The Safety and Economic Aspects of Electronic Banking**

Zásady pro vypracování:

1. **Popište problematiku elektronického bankovnictví jako součásti elektronického obchodu.**
2. **Popište problematiku přímých bankovních systémů, elektronických peněženek a platby kartou.**
3. **Na modelové struktuře znázorněte problematiku bezpečnostních a ekonomických aspektů podnikání – zaměřte se na nejvýznamnější průlomy bezpečnosti v oblasti e-bankingu.**
4. **Popište nové trendy zabezpečení v oblasti elektronického bankovnictví.**
5. **Navrhněte doporučení v problematice zneužití elektronického bankovnictví a zdůvodněte toto řešení.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **POLOUČEK, S. a kol. Bankovnictví. Praha: C.H. Beck, 2006. 716 s. ISBN 8071794627.**
2. **PŘÁDKA, M., KALA, J.: Elektronické bankovnictví: Rady a tipy. 1. vyd. Praha: ComputerPress, 2000. 166 s. ISBN 80-7226-328-5.**
3. **BEZPEČNĚ-ONLINE.CZ: Jak se bránit podvodům: Podvody při online nákupech. Bezpečně-online.cz [on-line]. [cit. 2012-02-06]. Dostupné na WWW:[http://www.bezpecne-online.cz/pro-ucitele-a-rodice/nakupovani-na-internetu/jak-sebranit-podvodum/207-3].**
4. **CENTRUM KYBERNETICKÉ OCHRANY ČR: Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015. Centrum kybernetické ochrany ČR[on-line]. [cit. 2012-01-10]. Dostupné na WWW:[http://www.govcert.cz/docDetail.aspx?docid=21667313&docType=ART].**
5. **OŠKRDALOVÁ, Gabriela. Modelování bezpečnostních rizik elektronického obchodu a elektronického bankovnictví [online]. Brno, 2012 [cit. 2015-01-26]. Dostupné z: http://is.muni.cz/th/50546/esf_d/Disertacni_prace__vc._priloh.pdf. Disertační práce. MASARYKOVA UNIVERZITA.**

Vedoucí bakalářské práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **3. června 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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

ABSTRAKT

Hlavní částí bakalářské práce je elektronický obchod a elektronické bankovnictví. Jejich využití, bezpečnost a ekonomické aspekty. V této práci jsou popsány a srovnány možnosti využití elektronického obchodu a elektronického bankovnictví, zhodnocení jejich rizika prolomení bezpečnosti a jejich bezpečnostní opatření. Dále je analýza nových trendů v oblasti zabezpečení. V poslední části je návrh doporučení v oblasti zneužití elektronického bankovnictví.

Klíčová slova: Elektronický obchod, elektronické bankovnictví, rizika, bezpečnost

ABSTRACT

The main focus of bachelor thesis are e-shop and e-banking. Their use, safety and economic aspects. In this work there are described and compared possibilities of using e-shop and e-banking, analysis of security risk and their safety . As next is analyzed new form of security. At last part is proposal recommendation on abuse of electronic banking.

Keywords: E-banking, e-shop, risk, security

Rád bych poděkoval vedoucímu mé práce doc. Ing. Jiřímu Gajdošíkovi CSc., za mnoho rad a času, který si našel pro mé konzultace.

OBSAH

ÚVOD

Peníze jsou pro každého člověka důležitým statkem už od dávných dob. Postupem času se podoba peněz rozvíjela a způsob jejich využití se stával stále více efektivnější. Poté se začalo objevovat bankovnictví, jakožto služba pro člověka, resp. Pro různé formy společností. Nároky na banky se stále zvyšovaly, a aby si banky udržely klienty, musely se přizpůsobovat jejich požadavkům.

S příchodem informační technologie dostalo bankovnictví úplně novou tvář. Přes internet je možné nakupovat, prodávat, sdělovat informace, tak se začalo pracovat s myšlenkou, že se přes internet dají spravovat i finance. Bankovnictví se tedy spojilo s internetem a vzniklo přímé bankovnictví. Zpočátku sice byli klienti nedůvěřiví a měli z využívání tohoto systému strach, ale postupem času zjistili, že je to mnohem rychlejší a pohodlnější než osobní vyřizování na pobočkách. Obdobný osud mělo využívání dalších prvků, které patří do elektronického bankovnictví, jako jsou platební karty a jiné. Klienti se postupně naučili používat tyto prostředky pro manipulaci s jejich finančními prostředky a nyní už jsou součástí jejich každodenního života.

Důvodem k výběru tématu Bezpečnostní a ekonomické aspekty elektronického bankovnictví je zájem o tuto problematiku. Cílem mé bakalářské práce je představit si všechny systémy elektronického bankovnictví. Ať už jde o zmiňované přímé bankovnictví a veškeré systémy, které jsou v něm zahrnuty, tak i platební karty, ale i další možnosti spadající pod elektronické bankovnictví jako jsou mobilní mikroplatby nebo elektronické peněženky. Dále se zaměřuji na jejich bezpečnostní prvky, na otázku jaká rizika jsou s využitím jaké metody spojená a jak je minimalizovat. Následně uvádím pro srovnání několik českých bank a zaměřuji se na stupeň jejich zabezpečení a jejich poplatkovou politiku, a nakonec vyhodnocuji, která banka je v čem výhodnější pro klienta. Na závěr mé práce představuji návrh doporučení pro uživatele elektronických bankovnictví, jak zacházet se zařízením, které používají, aby riziko zneužití bylo co nejmenší.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÝ OBCHOD

Pojem elektronický obchod obecně znamená typ podnikání, který využívá elektronických prostředků. Patří sem jak obchodování s hmotným i nehmotných zbožím, tak obchodování se službami, ale také všechny související kroky jako reklama, uzavření smluv, jejich plnění, a to včetně prodejní podpory a služeb.

Z právního hlediska se jedná o projevy vůle - právní jednání – směřující k uzavírání smluv, které jsou realizovány pomocí počítačových sítí

1.1 Rozdělení elektronického obchodu

Elektronický obchod dělíme do následujících kategorií:

- Podle účastníků
    - Obchodování mezi podniky/obchodníky navzájem – **B2B** (business to business)
    - Spotřebitelské smlouvy s koncovými zákazníky – **B2C** (business to customer)
    - Obchod mezi dvěma nepodnikateli/spotřebiteli navzájem, např. elektronické aukce – **C2C** (customer to customer)
    - Obchody, kdy zákazník oslovuje podnikatele, např. definuje zboží a vyzývá obchodníky k podání nabídek – **C2B** (customer to business)
    - Vztahy ke státní správě (eGovernment), např. elektronické podání daňového přiznání, byť se zde nejedná o obchod, ale spíše činnosti, které mimo jíné s obchodem souvisejí – **B2A, C2A** (business/customer to administration)
- Podle otevřenosti použitého média
    - Uzavřené transakce – obchod po uzavřených sítích
    - Otevřené transakce – obchod mezi otevřeným počtem účastníků
- Podle způsobu plnění
    - Přímé e-obchody – objednávka, placení i dodávka nehmotných statků se uskutečňuje výhradně prostřednictvím elektronických prostředků

- Nepřímé e-obchody – objednávka, uzavření smlouvy nebo i placení se uskutečňuje prostřednictvím elektronických prostředků, dodávka zboží se děje tradičními prostředky [1].

Vzhledem k tématu mojí bakalářské práce se v kapitole o elektronickém obchodu zaměříme na kategorii **B2C** tedy business to customer. Podíváme se na výhody a nevýhody jak z pohledu zákazníka, tak z pohledu prodávajícího.

1.2 Elektronický obchod B2C

Jedná se o druh elektronického obchodu, kdy si zákazník vybírá své zboží nebo službu prostřednictvím internetových stránek prodávajícího podnikatele. Zboží si zde může koupit a také rovnou zaplatit. Jde tedy o obchod bez přímého kontaktu s prodávajícím. Zákazník si může zvolit způsob úhrady [2].

Nejzákladnější možnosti placení jsou:

- Bankovní převod
- Dobírka
- Platební karta (při platbě předem nebo také při osobním odběru)
- Hotovost při osobním odběru
- Elektronická peněženka

1.2.1 Výhody a nevýhody B2C

Výhody z pohledu zákazníka:

- Časová úspora
- Široký výběr zboží od různých prodejců
- Nižší ceny než v kamenných obchodech
- Nakupovat lze 24/7 356 dní v roce
- Nakupovat lze z jakéhokoliv místa na Zemi s přístupem na internet.

Nevýhody z pohledu zákazníka:

- Nelze vyzkoušet a fyzicky prohlédnout vybrané zboží
- Zboží není ihned u zákazníka, zákazník musí čekat na doručení
- Neosobnost nákupu

Výhody z pohledu prodávajícího:

- Snížení nákladů
- Zvýšení efektivnosti
- Rychlé přizpůsobení podmínkám trhu
- Přístupnost k potenciálním zákazníkům

Nevýhody z pohledu prodávajícího:

- Velká konkurence
- Nutné investice (reklama, propagace)
- Obtížné udržení zákazníků
- Anonymita zákazníků

1.3 Elektronický obchod v ČR

Nakupování přes internet se stává pořád oblíbenějším jak ve světě, tak i v naší republice. Lidé už vnímají nákupy přes e-shopy, jako samozřejmou součást běžného života. Podle průzkumu jednou do roka nakoupí 79 % českých internetových uživatelů a utratí v průměru za jeden nákup 1634 korun. Lidé podle průzkumu nakupují na internetu hlavně z důvodu ušetření času [3].

Obraty internetových obchodů v české republice májí stálý růst od roku 2001. Mezi nejúspěšnější roky podle Asociace pro elektronickou komerci APEK patří obrat mezi rokem 2009, kdy české internetové obchody utržily 27 miliard korun, a rokem 2010, kdy byl obrat o 6 miliard korun vyšší. Stejný nárůst 6 miliard je také mezi rokem 2011 a 2012. Úplně nejvyšší nárůst obratu lze však spatřovat v posledních letech. V roce 2012 to bylo 43 miliard korun a v roce 2013 dokonce 57 miliard což je nárůst o 14 miliard korun. Podle serveru probyznys.info bude obrat za rok 2014 asi 80 miliard korun [4].

Tab. 1. Obrat internetových obchodů v ČR [4]

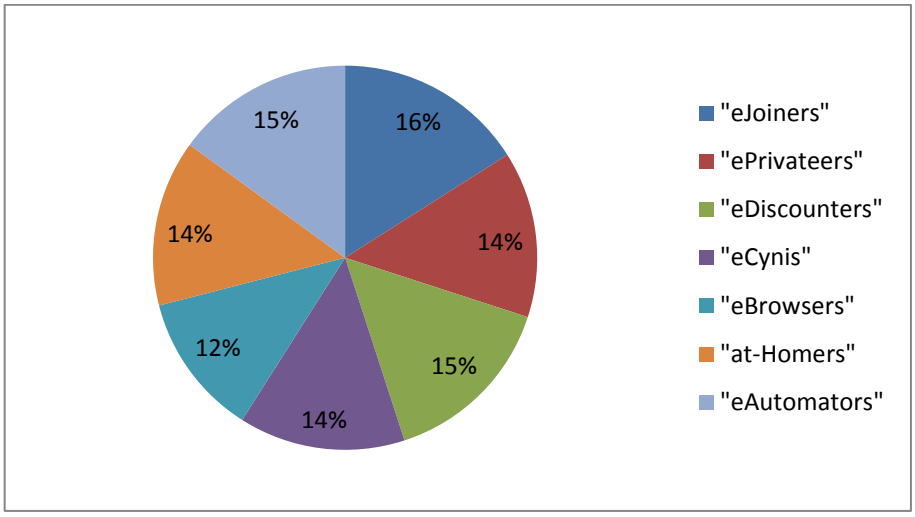
Rok	Obrat (mld. Kč)	Přírůstek (mld. Kč)
2001	1	-
2002	2	1
2003	4	2
2004	7	3
2005	10	3
2006	14	4
2007	18	4
2009	27	5
2010	33	6
2011	37	4
2012	43	6
2013	57	14

1.4 Zákazníci internetových obchodů

Společnost Flexo-Hiner podnikla výzkum s názvem eCommerce Benefits Monitor, který zkoumal motivaci zákazníků internetových obchodů. Podle tohoto výzkumu lze zákazníky rozdělit do těchto skupin [5]:

- eJoiners – takový druh zákazníka, který ví, že je internet nejlepší místo pro nákup
- ePrivateers – zákazník, jemuž se líbí poskytované soukromí, které internet nabízí a využívá ho k nákupu zboží, které by si v kamenných obchodech nekoupili
- eDiscounters – zákazník, který využívá výhod internetu k vyhledávání nejnižších cen. Tedy je pro něj motivací úspora peněz
- eCynis – zákazník, který po nákupu na internetu nebyl z tohoto nákupu nadšen
- eBrowsers – zákazník, který vyhledává informace on-line, ale nakupuje off-line
- at-Homers – zákazník, který považuje možnost nákupu z domova za nejvyšší přínos nakupování přes internet

- eAutomotors – zákazník, který si vychutnává efektivitu moderního automatizovaného nákupního procesu na internetu



Obr. 1. Jednotlivé druhy zákazníků [5]

2 ELEKTRONICKÉ BANKOVNICTVÍ

Elektronické bankovnictví jako součást elektronického obchodování představuje moderní způsob komunikace klienta s bankou, respektive moderní způsob poskytování a využívání jednotlivých typů bankovních služeb elektronickou cestou. Důležitou součástí elektronického bankovnictví jsou platební karty a jiné systémy, které umožnují činit různé bankovní operace bez nutnosti být fyzicky přítomní v bance [6].

2.1 Vznik elektronického bankovnictví

Za počátek elektronického bankovnictví můžeme považovat vznik takzvaných debetních platebních karet, u kterých jsou transakce účtovány okamžitě nebo s minimálním časovým zpožděním. Firma Wester Union Telegraph Company jako první vydala platební kartu, která sloužila k zasílání telegramů bez nutnosti okamžité platby. V roce 1950 firma Diners Club International vybrala 200 klientů, kterým dala první univerzální kartu. První banka, která otestovala platební kartu, byla o rok později The Franklin National Bank z New Yorku. Při platbě touto kartou klient musel podepsat účet a prodejce ověřil, jestli podpisy na kartě a na účtu jsou stejné [7].

S vývojem výpočetní technologie, se začaly objevovat první bankomaty a obchodníci platby platebními kartami již zpracovávali elektronicky. Postupem času se elektronické bankovnictví vyvíjelo. Přibylo phone banking, GSM banking, Internet banking, Homebanking, a také nejmodernější způsob elektronického bankovnictví SmartPhone banking, jemuž bude věnována bližší pozornost níže.

2.2 Rozdíl mezi elektronickým a klasickým bankovnictvím

Rychlý rozvoj informačních technologií a především internetu se samozřejmě promítá i do oblasti bankovnictví a finančních služeb. Jejich bouřlivý vývoj přinesl nové možnosti zprostředkování bankovních a finančních služeb klientům pomocí počítačové nebo mobilní komunikace.

Rozdíly mezi elektronickou a klasickou bankou:

- Rozdílné způsoby dorozumívání klienta a banky – v klasických kamenných bankách je důležitý fyzický kontakt s klientem banky, u elektronického bankovnictví probíhá komunikace přes internet nebo jiný komunikační prostředek

- Náklady banky – provoz internetového bankovnictví je levnější než provoz kamenné pobočky.
- Dostupnost služeb a jejich kvalita – klasické pobočky bank mají určitou provozní dobu, takže klient je omezen časem, kdy si může do banky přijít něco vyřídit. Naopak službu internetového bankovnictví má klient dostupnou 24 hodin denně 365 dní v roce. A může být kdekoliv na světě, pokud má přístup k internetu [8][6].

Uvedené příklady jsou těmi nejdůležitějšími rozdíly mezi těmito druhy bankovnictví.

2.3 Platební karty

Platební karty jsou v dnešní době nejpoužívanější a také nejrozšířenější část internetového bankovnictví. Jsou dnes již naprosto standartním produktem, který banky nabízejí svým zákazníkům. Slouží k vzdálenému přístupu k účtu klienta banky přes elektronickou cestu, zejména k bezhotovostní úhradě spotřebních výdajů a k výběru hotovosti [9].

2.3.1 Druhy platebních karet

Máme několik možností, jak můžeme platební karty dělit. A to z hlediska jejich výroby, podle způsobu zúčtování transakce a technických zařízení, v nichž lze platební kartu použít. Každý druh platebních karet krátce rozebereme a charakterizujeme si jej, a to proto, abychom později mohli probrat jejich bezpečnostní rizika [9].

Platební karty tedy dělíme podle:

- Způsobu zúčtování transakcí
    - Debetní karty – jsou nejrozšířenějším druhem platebních karet. Debetní karta je taková karta, která se vydává k běžnému účtu za účelem výběru hotovosti nebo k úhradě plateb za nakoupené zboží či službu. Ihned po zaplacení je klientovi z běžného účtu odečtena částka, kterou zaplatil. Klient tedy může zacházet jen s tolika penězi, na kolik má nastavený minimální povolený zůstatek. Držiteli této karty není poskytnut žádný úvěr [10].
    - Kreditní, úvěrové karty – klient může kreditní kartu využít ke stejným úkonům jako debetní kartu. Kreditní karta, ale navíc umožnuje klientovi čerpat spotřebitelský úvěr. Tudíž si klient vlastně půjčuje od banky finance, k placení do výše úvěrového limitu, který je předem stanoven. Tento úvěr pak splácí. Většina bank poskytuje tyto úvěry bezúročně, tedy pokud klient splácí ve stanoveném termínu.

  - Charge karty – jedná se o nejstarší typ placených karet. Umožnuje klientovi nakupovat bez okamžitého placení. Klient obdrží po určité době výpis od vydavatele této karty, který musí zaplatit do udané lhůty. Tuto úhradu platí buď bankovním převodem, šekem nebo ji banka klientovi strhne sama z účtu klienta [9].
  - Předplacené platební karty – karty, které jsou předem nabité určitým finančním obnosem. Klient poté při placení čerpá z tohoto obnosu, dokud nejsou finanční prostředky na kartě vyčerpány. Tedy nejedná se o čerpání z běžného účtu, ale klient je omezen výší nabité částky [9].
- Technických zařízení, v nichž lze platební kartu použít
  - Embosové karty – jedná se o druh karet, na které jsou identifikačni udaje vyraženy neboli embosovány reliéfním písmem. Díky tomuto vyražení mohou být karty použity jak v elektronickém prostředí, tak i v mechanických snímačích obchodníků (impritech). Co se týče použití impritu, tak částka za transakci není odečtena okamžitě, ale trvá to přibližně jeden týden. Karta má určený tzv. autorizační limit, pokud klient při platbě přesáhne tento limit nebo karta vykazuje náznaky padělání, tak je obchodník povinen si ověřit transakci v autorizačním centru banky [11].
  - Elektronické platební karty – platební karty určené pro použití v elektronickém prostředí (ATM, EFT POS) s přímou autorizací (v klasickém případě jde o zadání osobního identifikačního čísla – PIN) [9].
- Technologie na výrobu
  - Embosové karty – (viz výše)
  - Karty s magnetickým záznamem – identifikační údaje u těchto druhů karet jsou zaznamenány na magnetický proužek, což umožní provádět elektronické transakce. Uživatel této karty musí znát její identifikační kód PIN pro umožnění provedení transakce [9].
  - Čipové karty – jedná se o bezpečnější typ platební karty. Nazývají se také smart karty (chytré karty). Karty mají na své přední straně umístěn mikročip, na který jsou zaznamenány identifikační údaje. Do tohoto čipu lze uložit informace potřebné k ověření klienta. Může se také uložit ověřovací prvek jako je otisk prstů. Tyto karty mají programovatelné mikroprocesory s nejvyšším stupněm ochrany uložených dat [9].

  - Karty s laserovým záznamem – data (identifikační údaje a data o provedených transakcích) jsou do podkladové vrstvy karty pomocí laserove technologie vypalovány. Výhodou je vysoká kapacita záznamu, ale nevýhodou je, že tato data jsou snadno kopírovatelná.
- Teritoria
  - Regionální katy – karty, které se dají použít pouze v obchodních sítích vydavatele.
  - Domácí karty – dají se využít pouze k placení v tuzemsku.
  - Mezinárodní karty – dají se použít jak v tuzemsku, tak v zahraničí [6]

2.3.2 Výhody a nevýhody platebních karet

Platební karty jsou dnes velice rozšířené díky jejich výhodám, ale mají také své nevýhody, a to jak z pohledu zákazníků, tak z pohledu obchodníků. V následující části budou tyto výhody a nevýhody blíže popsány.

Přestože platební karty jsou spojeny s mnoha poplatky za jejich užití a rizikem jejich zneužití, mají oproti hotovosti kladné vlastnosti.

Výhody pro klienta:

- Zákazník není limitovaný hotovostí, kterou má u sebe, ale může čerpat své finanční prostředky ze svého účtu
- 24 hodinový přistup ke svým finančním prostředkům
- Bezpečnější než mít u sebe hotovost (po odcizení platební karty nemá zloděj okamžitý přístup k penězům jako je tomu u hotovosti)
- Jednoduché použití
- Velká možnost použití jak v ČR, tak i v zahraničí
- Přehled o provedených platbách (výpis z karty, nebo elektronická kontrola)
- Doplňkové služby (různé výhody nebo slevy při použití karty) [12]

Pro zákazníky existují rovněž následující nevýhody:

- Poplatky za použití platební karty, popř. jiné poplatky spojené s užíváním karty

- Ztráta anonymity
- Možnost zneužití karet při jejich ztrátě (pokud zloděj zjistí PIN, může mít přístup k veškerým finančním prostředkům okradeného)
- Zvýšení výdajů spojených s jednoduchostí použití karty [12]

Dále se podívejme, jak to je z pohledu obchodníka. Nejdříve výhody:

- Není možné, aby zákazník zaplatil třeba falešnou bankovkou, tedy vyšší bezpečnost při placení
- Snadné použití
- Menší náklady
- Možná větší útrata zákazníků (jelikož zákazník není omezen hotovostí, kterou má u sebe, je možné, že utratí víc peněz a koupí si věci, které by bez platební karty nepořídil, právě z důvodu aktuálního nedostatku hotovosti při sobě)
- Klient není anonymní
- Prestiž (obchodníci, u kterých zákazníci mohou platit platební kartou, mají pro ně vyšší prestiž) [12]

Nevýhody z pohledu obchodníků:

- Nutnost platit provize
- Nutnost mít vybavení, které umožnuje provádět platby
- Nutnost mít zaškolené zaměstnance [12]

2.3.3 Ochranné prvky platební karty

Ochranné prvky platebních karet slouží jako ochrana před jejich zneužitím. I když nezajišťují úplnou bezpečnost, jedná se o významnou minimalizaci rizik zneužití. Dnes pro podvodníky zneužití karty znamená velká časová a finanční investice a velké riziko dopadení. Proto se většina z nich této kriminální činnosti raději vyhýbá [12].

Na platebních kartách je několik ochranných prvků, jako číslo platební karty, magnetický proužek, čip, PIN, podpisový proužek, hologram, označení vydavatele, BIN číslo, platnost karty a jméno držitele.

2.3.4 Možnosti použití

Jak již bylo zmíněno, platební karty se především využívají k výběru hotovosti v bankomatech, na pobočkách bank nebo v obchodech a k bezhotovostnímu placení. Se všemi těmito možnostmi se seznámíme, abychom později mohli identifikovat a analyzovat jednotlivá bezpečnostní rizika.

2.3.4.1 Výběr hotovosti v bankomatech

Výběr hotovosti z bankomatů je jedním ze základních způsobů využití platebních karet. Jen v České republice je 5241 bankomatů od různých bank. Nejvyšší počet bankomatů má Česká spořitelna, a to 1312, naopak nejméně má banka OberBank s počtem 12 bankomatů. Při výběru hotovosti probíhá identifikace držitele tak, že zadá osobní identifikační číslo PIN. V dnešní době již bankomaty pracují v on-line režimu, to znamená, že každá transakce je v reálném čase ověřena v autorizačním centru [12].

Tab. 2. Počet bankomatů v ČR [13]

Banka	Počty bankomatů
Česká spořitelna	1546
Poštovní spořitelna	949
ČSOB	893
Komerční banka	734
GE Money Bank	650
UniCredit Bank	208
Citibank	153
Fio banka	143
Raiffeisenbank	128
Sberbank CZ	30
Air bank	29
Oberbank AG	12

2.3.4.2 Výběry na pobočkách bank

Jedná se o výběr hotovosti, který není tolik oblíbený jako výběr z bankomatu. Výběr v pobočkách bank takzvaný cash advance je oproti výběru z bankomatů nevýhodný tím, že kvůli potřebě lidské obsluhy jsou zavedeny vyšší poplatky. Ty mohou činit od 20 Kč až po několik set za jeden výběr, záleží na částce, která je vybrána. Z bezpečnostních důvodů se ale doporučuje využívat tuto službu při výběru vysokých částek [14].

2.3.4.3 Výběry hotovosti v obchodech

Další možnost výběru hotovosti, o které jsem osobně ani nevěděl, je výběr v obchodech. Probíhá to tak, že když zákazník platí svůj nákup, požádá pokladníka o vyplacení zvolené částky v hotovosti. Pokladní mu předá tuto hotovost a částka se připočítá k účtu zákazníka. Takovýto výběr lze provádět pouze v určitých kamenných obchodech. V České republice se jedná o relativně novou službu [15].

2.3.4.4 Bezhotovostní placení na internetu nebo v obchodech

Stále oblíbenější způsob využití platebních karet. Pokud jde o nakupování na internetu výhodou je, že platba je okamžitě provede a obchodník může ještě tentýž, nebo hned další den odeslat zboží zákazníkovi. Co se týká nákupu v kamenných obchodech, ten ma již výše uvedené výhody a nevýhody.

Bezhotovostní placení není nic nového, ale za novinku můžeme označit takzvané bezkontaktní platby. Pokud jsou obchody vybaveny příslušnou technologií pro provádění těchto plateb, zákazník může ušetřit čas, jelikož stačí přiložit kartu k čtečce bez nutnosti jiné manipulace nebo zadání bezpečnostního PIN kódu a platba je provedena během několika málo sekund. Z důvodu bezpečnosti jsou tyto platby určeny jen pro menší částky. V České republice je to částka 500 Kč. Další zabezpečení spočívá v nutnosti zadat po několika bezkontaktních platbách PIN kód i v případě, že částka nepřesahuje 500 Kč

2.3.5 Bezkontaktní nálepka

Jedná se o zmenšeninu platební karty v podobě nálepky. Nálepka se může přilepit na jakékoliv zařízení, která má uživatel stále u sebe, např. mobilní telefon. Nálepka slouží k bezkontaktnímu placení, které se provádí na platebním terminálu obchodníka. Při placení do 500 Kč se nezadává PIN. U plateb nad 500 Kč je nutno PIN zadat. Při platbě touto nálepkou uživatel čerpá ze svého bankovního účtu. Nálepka má tedy vlastnosti jako platební karta. Z bezpečnostních důvodů je možné i u bezkontaktní nálepky nastavit limity maximální utracené částky. Hlavní výhodou tohoto zařízení je to, že uživatel nemusí mít při sobě stále peněženku nebo platební kartu. Pokud má nálepku přilepenou na svém mobilním telefonu (který má většina lidí neustále při sobě), tak může kdykoliv mobil vytáhnout a zaplatit. Další výhodou je veliká rychlost při placení, z důvodu bezkontaktní platby.

2.4 Přímé bankovnictví

2.4.1 Phonebanking

U tohoto typu přímého bankovnictví probíhá komunikace klienta s bankou prostřednictvím telefonu. Klient tedy provádí své bankovní operace pomocí svého vlastního hlasu. Jedná se tedy o komunikaci s živým pracovníkem banky. Pokud klient nechce řešit nijak důležité nebo složíte bankovní situace a jedná se o pouhé zjištění informací ohledně nějaké služby, může být spojen s automatickou hlasovou službou (IVR – Interactive Voice Response), kterou ovládá pomocí tlačítek telefonu. Až pří konaní složitější operaci pomocí tlačítek zvolí možnost spojit s živým pracovníkem. Operace prováděné v přímém bankovnictví se dělí do dvou skupin, a to na aktivní a pasivní operace.

Tab. 3. Aktivní a pasivní operace [2]

Aktivní	Pasivní
Příkaz k úhradě	Zjištění účetního zůstatku
Trvalé příkazy k úhradě	Informace o transakcích
Příkaz k inkasu	Informace o bance (služby, nabídky)
Platby do zahraničí	Informace o pohybech na účtu

2.4.2 GSM banking

V dnešní době, již velice ojedinělý způsob komunikace klienta s bankou. Jedná se o komunikaci prostřednictvím SMS zprávy, které jsou šifrované. Klient tedy pošle svůj požadavek přes SMS zprávu a banka mu odpovídá také skrz SMS zprávu. Nevýhodou využití této služby je to, že klient při zasílaní požadavku musí znát přesná klíčová slova v přesně nadefinované struktuře pro každou bankovní operaci. Další možností komunikace je takzvaný SIM Toolkit. Jedná se o pohodlnější způsob pro uživatele využívajících GSM banking, ale využívat ho může jen ten, kdo má v mobilním telefonu SIM kartu s aplikací přímo od banky. SIM Toolkit zajišťuje šifrování SMS zpráv a při jejich nahrávání je SIM karta zašifrována a nelze zní získat žádné údaje ani po odcizení telefonu [8].

Tab. 4. Operace GSM bankingu (přes SIM Toolkit) [8]

Aktivní	Pasivní
Zadání a zrušení příkazu k úhradě	Informace o stavu účtu
Zadání a zrušení trvalého příkazu	Informace o posledních 5 příjmech a výdajích
Dobíjení mobilního kreditu	Dotaz na kurzy měn
Zadání terminovaného vladu	Dotaz na vybranou úrokovou sazbu terminovaného
	vkladu

2.4.3 WAP banking

Jedná se o další typ komunikace s bankou přes telefon, nicméně je daleko kvalitnější než předchozí uvedené. Na displeji mobilního telefonu se objeví stránka banky, která se dá srovnat s webovými stránkami. Oproti webovým stránkám, jsou stránky přes WAP banking jednodušší (méně obrázků, reklam, tlačítek), přehlednější a přenáší méně dat. Mobilní telefon přenáší data pomocí GPRS a není závislý na SIM kartě [12].

2.4.4 SmartPhone banking

Smartphone banking je nejnovějším typem bankovnictví využívající mobilní telefon. Stává se postupně běžnou součástí našeho života. Přispívá k tomu rostoucí obliba chytrých telefonů, stejně jako ochota finančních institucí ve stále větší míře nabízet řešení pro mobilní platby a bankovnictví. Aby mohl klient využívat tuto službu, musí mít takzvaný „chytrý telefon“ a aplikaci pro přístup do své banky. SmartPhone banking využívá pro komunikaci s bankou bezdrátové Wi-fi sítě nebo mobilního internetu poskytnutého od operátora [16].

Bezpečnost mobilního bankovnictví je provázána se zabezpečením chytrého telefonu jako takového. Pro jeho obecnou ochranu je důležité:

- Zachovat pouze oficiální verze operačního systému
- Instalovat pouze ověřené aplikace a vyhýbat se podezřelým webům
- Nastavit si ochranu heslem, či případně možnost vymazání jeho obsahu na dálku v případě ztráty nebo odcizení
- Pravidelná kontrola účtů a transakcí
- Vyhýbat se neověřeným bezdrátovým sítím

2.4.5 Homebanking

Komunikace klienta s bankou prostřednictvím počítače připojeného k internetu. Klient ale nemůže provádět bankovní operace na kterémkoliv počítači s internetem, ale jen na tom, kde je nainstalován speciální program od banky. Klient může tímto druhem bankovnictví provádět služby jako příkaz k úhradě, zjištění zůstatku, konverze měn atd. [12].

2.4.6 Internetbanking

Jedná se o komunikaci klienta s bankou pomocí počítače připojeného k síti internet. Na rozdíl od Homebankingu se lze spojit s bankou odkudkoliv na světě, kde je počítač. Není nutné mít nainstalován žádný specifický program. Můžeme říct, že InternetBankng umožnuje provádět podobné operace jako tomu bylo u telefonního bankovnictví. Velikou výhodou je však webové prostředí, neboť zrakové vjem je jednodušší a je lépe přijímán než sluchový. Nevýhodou možnosti připojení z různého PC je velká možnost zneužití. Proto tento typ komunikace vyžaduje vysoký stupeň zabezpečení. Používají se různé způsoby autentizace a autorizace transakcí, např. uživatelské číslo a PIN, heslo s možností nastavení limitu, pro nadlimitní transakce používaní autentizačního kalkulátoru [12].

2.5 Elektronická peněženka

Elektronická peněženka slouží k platbám v internetových obchodech. Hlavní výhodou a důvodem využívání této služby je bezpečnost, rychlost a jednoduché použití. Při platbě elektronickou peněženkou, zákazník neudává své citlivé informace. Stačí použít jméno a heslo pro zaplacení.

Dobíjení elektronické peněženky je možné provést z kteréhokoliv účtu v libovolné bance. Z bezpečnostních důvodů se doporučuje vkládat do peněženky jen takové množství financí, kolik zákazník potřebuje k běžným platbám. Snižuje se tím riziko peněz, že klient přijde při případném zneužití o vyšší částku. To je další výhoda oproti platebním kartám, u kterých při zneužití může klient přijít o veškeré finanční prostředky na svém účtu. Další způsob zabezpečení je možnost nastavit si platební limit, při jehož překročení nestačí pro platbu zadat jméno a heslo, ale musí dojít k potvrzená platby pomocí mobilního telefonu [17].

2.5.1 Možnosti použití

Elektronické peněženky se používají tam, kde je rozhodující rychlost platby a jednoduchost obsloužení, aby bylo možné odbavit co nejvíce zákazníků. Používá se proto pro mikroplatby (úhrada služeb či produktů do určité nízké sumy, zpravidla do částky v přepočtu pět set korun.)

2.6 Mobilní mikroplatby

Dalším druhem, který můžeme zařadit do elektronického bankovnictví, jsou takzvané mobilní mikroplatby. Tento druh plateb umožňuje platit bezhotovostně a elektronickou cestou menší částky, a to většinou v řádech několika set korun českých proto jsou nazývány mikroplatby. Uživatel ale nečerpá své finanční prostředky ze svého účtu, nejedná se tedy o přímé bankovnictví, nýbrž čerpá finanční zdroje buď ze svého mobilního kreditu, kdy je platba odečtena z jeho nabité kreditní částky, nebo pokud má uživatel paušál při zaplacení mikroplatby se tato částka připíše k účtu jeho paušálu. Tedy pokud uživatel platí měsíční paušál 1000 Kč a zakoupí například jízdenku hromadné dopravy za 15Kč, jeho měsíční paušál bude 1015 Kč.

2.6.1 Možnosti použití

Mikroplatby se v dnešní době chytrých telefonů používají většinou pro nákup mobilních aplikací nebo her. Dále se dají také využít pro nákup hudby nebo filmů. Mají také své místo při koupi jízdenek městské hromadné dopravy, jízdenek na autobus nebo vlak.

3 EKONOMICKÉ A BEZPEČNOSTNÍ POROVNÁNÍ ELEKTRONICKÉHO BANKOVNICTVÍ

V teoretické části mé práce byly vybrány tři české banky. Dvě největší (Česká spořitelna a Československá obchodní banka) a jedna menší pro lepší srovnání (UniCredit Bank). V teoretické části budou přestaveny tyto banky, ukážeme si, jaké internetové bankovnictví nabízí, jaké funkce nabízí a kolik klientů využívá jejich služby. V praktické části mé práce bude představeno jaké bezpečnostní a ekonomické aspekty tyto banky nabízí a bude porovnáno, která banka je nejbezpečnější a která finančně nejvýhodnější pro běžného klienta.

3.1 Česká spořitelna, a. s.

Česká spořitelna vznikla v roce 1992 a od roku 2000 je členem Erste Group. Disponuje nejširší sítí poboček bankomatů v České republice. Česká spořitelna byla první bankou, která u nás zavedla bezkontaktní karty a vytvořila síť pro jejich využití [21].

Tab. 5. Základní fakta k 30.6.2014 [20]

Aktiva celkem	900,3 mld. Kč
Počet klientů	5 091 139
Počet aktivních klientů přímého bankovnictví	1 668 303
Počet poboček	644
Průměrný počet zaměstnanců finanční skupiny České spořitelny	10 474
Počet karet	3 146 490
Počet bankomatů	1 546

Pro poskytování elektronického bankovnictví využívá Česká spořitelna službu SERVIS 24 Internetbanking a službu BUSINESS 24 Internetbanking, která je nabízena podnikatelům. Pro naše porovnání byla vybrána služba SERVIS 24.

Klienti můžou využít službu následovně [20]:

- Sledovaní informací o účtech
- Historie transakcí
- Zadávání plateb (jednorázové, hromadné, inkasní, trvalé atd.)
- Import plateb
- Mobito

- E-faktury
- Informace o spoření
- Informace o úvěrech
- Přehled pojistných smluv
- E-shop České spořitelny

V počtu nabízených služeb SERVIS 24 Internetbanking zdaleka přesahuje standardně poskytované služby jiných bank.

3.2 Československá obchodní banka, a. s.

Československá obchodní banka, a. s. působí jako univerzální banka v České republice. ČSOB byla založena státem v roce 1964 jako banka pro poskytování služeb v oblasti financování zahraničního obchodu a volnoměnových operací. V červnu 1999 došlo k její privatizaci. V červnu 2000 ČSOB převzala Investiční a poštovní banku (IPB). Po odkoupení minoritních podílů se v červnu 2007 jediným akcionářem ČSOB stala KBC Bank. Do konce roku 2007 působila ČSOB na českém i slovenském trhu. Slovenská pobočka byla oddělena 1. ledna 2008 [22].

Tab. 6. Základní fakta k 31. 12. 2014 [23]

Aktiva	854 872 401 Kč
Klienti	2,9 mil.
Pobočky	243
Bankomaty	1047
Uživatelé internetového bankovnictví	1,5 mil

I při hodnocení této banky se zaměříme na internetové bankovnictví. ČSOB k tomu poskytuje službu ČSOB InternetBanking 24. Pro podnikatele poskytuje službu s názvem ČSOB BusinessBanking 24. Stejně jako u přechozí banky se zaměříme jen na jednu z poskytovaných služeb a to InternetBanking 24. Nejprve se podívejme, jaké funkce poskytuje tato služba:

- Informace o účtu
- Běžné platební procesy
- Informace o podílových fondech a investicích
- Informace o penzijním připojištění

- Správa uvěrových produktů
- Žádosti o úvěrové produkty
- Informace o hypotéce
- Zasílání informačních SMS a e-mailů
- Dobíjení kreditu předplacených SIM karet mobilních operátorů
- Služby pro platební karty

3.3 UniCredit Bank Czech Republic and Slovakia, a.s.

UniCredit Bank zahájila svoji činnost na českém trhu 5. listopadu 2007. Vznikla integrací dvou doposud samostatně působících bankovních domů HVB Bank a Živnostenské banky. Od prosince 2013 UniCredit Bank v České republice a na Slovensku poskytuje bankovní produkty a služby pod jednotným obchodním názvem UniCredit Bank Czech Republic and Slovakia, a.s. [24]

Tab. 7. Základní fakta ke dni 31. 12. 2014 [25]

Aktiva celkem	508 616 mil. Kč
Počet klientů	550 000
Počet klientů využívajících internetové bankovnictví	200 000
Počet poboček	173
Počet bankomatů	225

UniCredit Bank nabízí službu pro internetové bankovnictví s názvem Online Banking. Pro firemní zákazníky má službu s názvem BusinessNET. Budeme se opět zabývat službou pro obyčejné klienty, tedy Online Bankingem. Klienti mohou využít toto internetové bankovnictví k následujícím účelům:

- Přehled o účtech a transakcích na účtech
- Běžné platební procesy
- Přehled o debetních a kreditních kartách a karetních transakcích
- Přehled cenných papírů a jejich historie
- Zobrazení všech poboček a bankomatů na mapě
- Zasílání zpráv a e-mailů o nejrůznějších událostech na účtech
- Možnost uložení platby do šablony pro pozdější použití
- Možnost přednastavit si šablony plateb

- Podání žádosti o úvěry
- Možnost zručení nezaúčtované platby
- Tvorba vlastního menu

3.4 Bezpečnostní rizika a podvody – teoretické hledisko

Tato část práce byla také rozdělena do dvou částí. Teoretická část bude zaměřena na seznámení s typy bezpečnostních rizik a podvodů. Kde se s jakým typem podvodu můžeme setkat a co způsobují. V praktické části bude předvedeno, jak tyto podvody prakticky probíhají a jaké bezpečnostní kroky proti nim banky provedly.

3.4.1 Libanonská smyčka

Tento podvod spočívá v tom, že je upraven bankomat. Podvodník vloží do bankomatu jednoduché zařízení, které je schopno zadržet platební kartu, pokud je vložena do bankomatu. Ovšem karta bez znalosti PINu není tak hodnotná jako když podvodník tento kód zná. Proto spolu s Libanonskou smyčkou používají další podvody, které jim pomáhají zjistit tento PIN kód. Metody spojené s použitím libanonské smyčky probere níže. Podoba libanonské smyčky je zachycena na Obr.2. [27]

Obr. 2. Lisabonská smyčka [26]

3.4.2 Skrytá kamera

Podstatou tohoto typu podvodu je zjištění PIN kódu pomocí malých skrytých kamer. Podvodník nejčastěji umisťuje tuto kameru na bankomaty. Potenciální oběť pak při použití

bankomatu zadává svůj PIN kód, který je zachycen na kameru. Získání PINu podvodníkům ale k zneužitím platebních karet nestačí, a právě proto bývá tato metoda skryté kamery spojována současně například s libanonskou smyčkou. Podvodník tedy získá jak platební kartu, tak i její PIN kód. Tato metoda ovšem bývá použita i tak, že jakmile získá podvodník kód, snaží se oběti kartu odcizit. [27]

3.4.3 Dotekové senzory

Podstata této metody je stejná jako u skrytých kamer, tedy získat PIN kód od oběti. V tomto případě ale podvodník využívá dotekových senzorů, které umísťuje na klávesnici bankomatů. Senzory pak zaznamenávají klávesy, které držitel platební karty při zadávání PINu stiskl. Stejně jako u skrytých kamer tato metoda vyžaduje použití ještě nějaké metody pro získání platební karty oběti.

3.4.4 Skimming

Jedná se o získávání údajů z platebních karet a jejich následné využití při výrobě padělané karty. Podvodník získá tyto citlivé údaje zkopírováním z magnetického proužku z platební karty, a to bez zjištění oběti. Místa, kde se nejčastěji můžeme setkat s kopírováním platebních karet, jsou podle Policie České republiky hlavně bankomaty, ale také u nepoctivých obchodníků, kteří si při placení kartou sami kartu zkopírují a zneužijí nebo předají tyto citlivé údaje jiným podvodníkům. Tito podvodníci pak vyrobí padělky karet. [28]

Obr. 3. Ukázka skimmingovacího zařízení [28]

3.4.5 Phishing

Oproti přechozím způsobům podvodů je tento druh jiný v tom, že nevyužívá žádných zařízení, ale zneužívá důvěřivosti lidí. A to tak, že se podvodník vydává za zaměstnance banky, osloví klienta a chce po něm, aby mu řekl své citlivé údaje. Zdůvodněním často bývá, že nabízí zvýšení zabezpečení pro klienta, aktualizaci softwaru, zvýhodnění podmínek, nebo jiné zvýhodnění služeb. [29]

Podvodníci využívají ke kontaktu klienta různé metody. Těmito metodami jsou e-mail, klasický dopis do schránky nebo telefon (volání nebo přes SMS). Nejčastější je metoda v internetovém prostředí, kdy je vytvořena webová stránka, které je velice podobná originálu bankovního webu. Po klientovi se pak žádá, aby na této webové stránce vyplnil své citlivé informace. Dalším trikem k větší důvěryhodnosti stránky je také podobná URL adresa stránky. Změna bývá často jen v některém písmenu, nebo je přidána pomlčka.

3.4.6 Pharming

Tento druh podvodu je oproti Phishingu novější a daleko nebezpečnější. Pharming využívá napadení Domain Name Systém (DNS), a díky tomu může podvodník převádět určité webové stránky, které uživatel zadá na svoje podvodné. Většinou podvodník využívá stránek banky napadené oběti a převádí je na své, které jsou k nerozpoznání od originálu. Oběť si teda myslí, že je na stránkách své banky a zadává přihlašovací údaje, které jsou přeposlány podvodníkovi. [26]

4 NOVÉ TRENDY ZABEZPEČENÍ V OBLASTI ELEKTRONICKÉHO BANKOVNICTVÍ

4.1 Biometrika

Pokud jde o nové trendy v internetovém bankovnictví, které se teprve rozvíjejí, tak je to určitě biometrika. Tento druh zabezpečení spočívá v tom, že využívá odlišnosti každého člověka. Každá část lidského těla jako otisk prstu nebo oko a další je jedinečná, a proto může sloužit k identifikaci. Biometriku můžeme rozdělit na dvě části [19]:

- **Psychologické identifikátory –** do této části patří otisky prstů, oční sítnice, duhovka, DNA, tvář
- **Behaviorální identifikátory –** biometrika zaměřená na rozpoznání hlasu nebo rukopisu

V biometrii se často setkáváme s výrazy identifikace, verifikace nebo srovnání. Proto si je vysvětleme:

- **Identifikace –** Uživatel nemusí překládat žádný jiný doklad nebo jiný důkaz o své identitě. Předá pouze svůj biometrický znak, který je pak porovnán v databázi, a určí identitu ověřované osoby.
- **Verifikace –** Nestačí pouze zadat biometrický znak. Uživatel musí nejprve předložit kartu s identifikačními údaji. Biometrický údaj se poté nemusí hledat v celé databázi, ale porovnává se pouze s tím, jehož identita byla prokázána kartou.
- **Srovnání –** Určuje stupeň shodnosti.

4.1.1 Metody biometriky

Fotografie – tuto metodu využívá například Citibank u svých platebních karet. Je to vlastně pomocný nástroj pro verifikaci. Fotografie může být jak zepředu karty, tak také zezadu.

Otisk prstu – tato metoda se využívá pro ověření vstupu do určitých bezpečnostních prostor. V dnešní době už zařízení pro ověřování otisků prstů dokáží rozpoznat, zda ověřovaná osoba je živá nebo po smrti. Nelze tedy uříznou prst zesnulé osobě a použít jej ke vstupu do oblasti.

Rozpoznání hlasu – tato metoda se využívá v Jihoafrické republice, kde banka First National Bank využívá tento způsob na svých bankomatech. Probíhá to tak, že klient banky příjde k bankomatu, vloží svoji kartu a bankomat ho vyzve k přečtení několika čísel. Po vyslovení těchto náhodných čísel zařízení udělá rozbor hlasu, a pokud se shoduje s majitelem karty, povolí mu manipulaci s penězi [19].

Sítnice – každý člověk má jedinečnou sítnici, tudíž představuje dobrý způsob pro ověřování. V bankovnictví se tento způsob zatím nevyužívá. Proto slouží tento způsob biometrie spíše pro ověřování při vstupu do tajných prostor [19].

Tab. 8. Porovnání biometrických metod [vlastní]

Biometrie	Bezpečnost	Přesnost	Náklady	Rychlost	Velikost čtečky
Krevní řečiště prstu	Vysoká	Vysoká	Nízké až střední	Vysoká	Malá až střední
Krevní řečiště dlaně	Střední až vysoká	Střední až vysoká	Nízké až střední	Střední	Malá až střední
Otisk prstu	Střední	Střední	Nízké	Střední	Malá
Črty obličeje	Nízká	Nízká	Střední	Střední	Velká
Oční duhovka	Vysoká	Vysoká	Střední až vysoké	Střední	Velká

4.1.2 Biometrika v budoucnosti

Lze nepochybně očekávat, že se biometrika v budoucnu dočká dalšího vývoje Je to dobrý způsob pro ověření identity k přístupu jak do bankovnictví, tak i do jiných zařízení nebo prostor. Dá se říct, že klasické zadávaná hesel již představuje starší typ zabezpečení, a nyní je řada pro něco nového. V dnešní době se biometrika využívá i pro přístup do mobilních telefonů. Společnost Apple vydala telefon Iphone 5s, který má v sobě zařízení pro rozpoznání otisku prstu pro přístup do telefonu. Takže se dá předpokládat, že i další výrobci začnou využívat biometrii. A biometrie u telefonu nemusí spočívat pouze v sejmutí otisku

prstů, ale díky fotoaparátům, které dnešní telefony obsahují, i v zařízení na rozpoznání obličeje.

II. PRAKTICKÁ ČÁST

5 EKONOMICKÉ A BEZPEČNOSTNÍ POROVNÁNÍ ELEKTRONICKÉHO BANKOVNICTVÍ NABÍZENÝCH V ČESKÉ REPUBLICE

5.1 Kritéria pro porovnání

V teoretické části byly představeny tři banky, v této praktické části bude pozornost zaměřena na jejich porovnání podle určených kritérií. Prvním kritériem bude jejich zabezpečení a druhým náklady. Nejdříve bude pojednáno o tom, jakými bezpečnostními a ekonomickými aspekty určené banky disponují, a v závěru kapitoly bude zhodnoceno, která banka je v těchto oblastech nejsilnější.

5.1.1 Zabezpečení

Při využívání IB, je stupeň jeho zabezpečení z mého pohledu nejdůležitějším aspektem. Empiricky lze vysledovat, že jedním z hlavních faktorů při výběru banky je její důvěryhodnost. Uživatelé se totiž u těchto ověřených bank nemusí strachovat o ztrátu svých finančních prostředků. V porovnání zabezpečení jsem se zaměřil na formu přihlašování do systému.

5.1.2 Ekonomické aspekty

Stejně jako stupeň zabezpečení i cena, která souvisí s využitím IB, je důležitým faktorem při rozhodováni uživatelů, kterou banku si zvolí. V tomto kritériu jsem se zaměřil na veškeré poplatky spojené s využitím IB. Pro srovnání jsem si zvolil dva typy klientů. A to klienty, kteří pravidelně využívají služeb IB, a ty kteří ho využívají méně.

Pravidelně využívající:

- 10 příchozích plateb do jiné české banky
- 10 odchozích plateb do jiné české banky
- 5 trvalých příkazů do jiné české banky
- 5 informačních SMS zpráv o zůstatku na účtu
- Informace o výpisu z účtu prostřednictvím e-mailové zprávy

Občasně využívající:

- 3 příchozí platby z jiné české banky
- 3 odchozí do jiné české banky

- 2 trvalé příkazy do jiné české banky
- 1 informační SMS zpráva o zůstatku na účtě
- Informace o výpisu z účtu prostřednictvím e-mailové zprávy

Dále budou porovnány poplatky spojené s použitím platební karty. Kritéria k porovnání budou měsíční poplatky za využití platební karty, poplatky spojené s výběrem hotovosti z bankomatů, a na závěr poplatky za nákup přímo u obchodníka. K porovnání byly vybrány debetní karty, které patří s nejčastěji používaným.

5.2 Srovnání nabídek vybraných bank

5.2.1 Česká spořitelna, a. s. – bezpečnostní a ekonomické aspekty

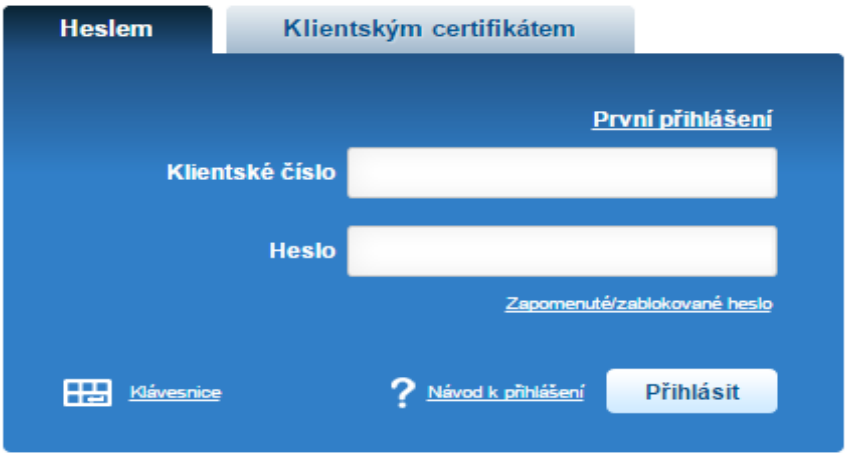
Co se týče bezpečnosti internetového bankovnictví, banka využívá šifrování komunikace pomocí SSL certifikátu, všechny e-maily a elektronické výpisy jsou zabezpečeny digitálním podpisem. Dalším bezpečnostním aspektem je možnost nastavení maximální částky, se kterou je možno během jednoho dne manipulovat. Pokud by byla částka překročena, finanční operace (platba, výběr hotovosti) by nemohla proběhnout.

Přihlašování ke službě SERVIS 24 Internetbanking probíhá tak, že klient zadá své klientské číslo a heslo. Je možné, aby klientovi byla zaslána také přihlašovací SMS, ale to není povinné, klient si musí sám tuto službu aktivovat. Z důvodu vyšší bezpečnosti je možné zadávat přihlašovací údaje pomocí grafické klávesnice. Je tím eliminována například hrozba keyloggeru. Pokud jsou údaje zadány třikrát za sebou špatně, dojde k zablokování internetbankingu. Co se týče složení hesla, musí mít minimálně 8 znaků. Přitom minimálně dva znaky musí být písmena a také dva znaky musí být číslice. Další možnost pro přihlášení, kterou SERVIS 24 podporuje, je přihlášení klientským certifikátem. Klient, který chce využívat tuto službu, musí mít uzavřenou smlouvu o poskytnutí vyššího typu zabezpečení, instalovanou čtečku karet a příslušný software. Pro přihlášení zadává klient PIN kód.

Dalším prvkem bezpečnosti je automatické odhlášení při 10 minutové nečinnosti v systému. Před ohlášením přijde upozornění ve formě okénka s textem.

Česká spořitelna nabízí autorizaci transakce dvěma způsoby. A to autorizační SMS nebo autorizace pomocí klientského certifikátu. U první zmiňované autorizace přijde při zadání transakce klientovi na mobil SMS s kódem, který musí zapsat pro schválení transakce. Kód má platnost jednu hodinu. Limit transakce při tomto způsobu je 200 000 Kč za den. Pokud klient zadá pětkrát nesprávně autorizační kód, jeho internetový účet se zablokuje asi na 60

minut. U druhého způsobu autorizace musí klient zadat PIN čipové karty. Tady je možno nesprávně zadat pouze tři PIN kódy a dojde k zablokování.



Obr. 4. Přihlášení ke službe Servis 24 internetbanking [30]

Tolik k zabezpeření. Další složkou v porovnání jsou ekonomické aspekty, tedy poplatky spojené s využitím služby. Přehled těchto cenových nákladů je uveden v následující tabulce.

Tab. 9. Poplatky za službu SERVIS 24 [31]

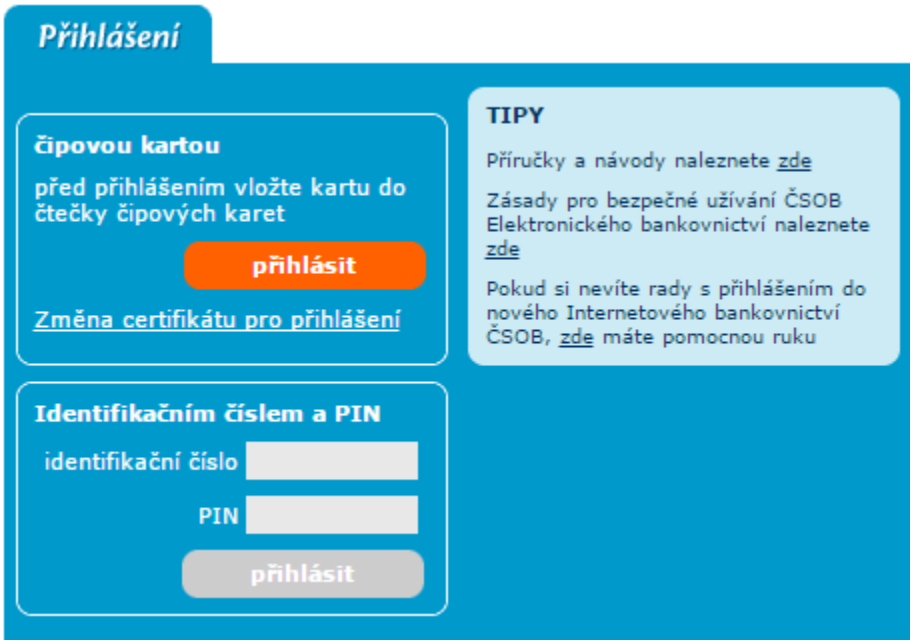
Zřízení služby a zrušení	zdarma
Změna údajů ve smlouvě	zdarma
Aktivace, deaktivace každého dalšího sporožirového nebo běžného účtu	zdarma
Odblokování přístupu do služby Internetbanking	zdarma
Vygenerování bezpečnostního kódu	zdarma
Poskytování služby	25 Kč
Opětovné vygenerování a zaslání bezpečnostních údajů	100 Kč
Příchozí platba	7 Kč
Odchozí platba do jiné tuzemské banky	7 Kč
Trvalý příkaz do jiné tuzemské banky	5 Kč
Zaslání potvrzení transakce, výpis z historie transakcí a detailu účtu	
E-mailem	zdarma
Faxem	10 Kč
Poštou	25 Kč
Zaslání SMS	
Autorizační	zdarma
Konfirmační	zdarma
Přihlašovací	2 Kč
Informační	2 Kč
Zůstatková	2 Kč
Zaslání SMS upozornění o nově přijaté e-faktuře/e-dokumentu	2 Kč
Čtečka čipových karet	350 Kč

Čipová karta	350 Kč
Klientský certifikát s roční platností	
Vygenerování	350 Kč
Obnova v termínu	350 Kč
Obnova mimo termín	450 Kč

5.2.2 Československá obchodní banka, a. s. – bezpečnostní a ekonomické aspekty

Služba pro svoji bezpečnost využívá pro komunikace šifrování. Stejně jako tomu bylo u přechozí banky nabízí nastavení limitů částky pro denní finanční manipulaci. Rovněž nabízí týdenní limit. U denního limitu je maximální možnost 1 500 000 Kč při autorizaci přes SMS kód. U týdenního limitu je to pak 3 000 000 Kč.

Pokud se chce klient přihlásit do internetového bankovnictví, má dvě možnosti. První je přihlášení pomocí identifikačního čísla, PIN kódu a SMS klíče. Po zadání identifikačního čísla a PIN kódu přijde klientovi autorizační kód v podobě SMS zprávy. Tento kód má platnost 10 minut. Pokud klient zadá pětkrát za sebou nesprávný SMS klíč, bude přístup do internetového bankovnictví zablokován. Pro odblokování musí klient navštívit pobočku banky. Druhý způsob přihlášení je pomocí čipové karty s elektronickým podpisem. Tady dochází k zablokování po třech nesprávně zadaných kódech. Pro odblokování klient nemusí do pobočky, ale stačí zadat PUK kód.



Obr. 5. Přihlášení do ČSOB InternetBanking 24 [32]

Další prvek bezpečnosti, který banka nabízí je přehled o přihlášeních do systému. Jedná se o seznam všech až 50 přihlášení za posledních 30 dní. Klient si tedy může ověřit, jestli se někdo jiný v nějaký okamžik nepřihlásil do jeho účtu. Automatické odhlášení probíhá vždy, když je klient nečinný 20 minut. A nyní se dostáváme k ekonomickým aspektům ČSOB, které jsou zadány opět do tabulky.

Tab. 10. Poplatky za službu InternetBanking 24 [33]

Zavedení služby	zdarma
Měsíční poplatek za vedení služby	20 Kč
Příchozí platby z jiné tuzemské banky	zdarma
Odchozí platby do jiné tuzemské banky	3 Kč
Trvalý příkaz do jiné tuzemské banky	3 Kč
Potvrzovací zprávy, ČSOB Info 24	
SMS zprávy pro přihlašování a potvrzování transakcí	zdarma
SMS zprávy zaslané v rámci služby ČSOB Info 24	2 Kč
E-mailove zprávy v rámci služby ČSOB Info 24 v rámci všech kont	zdarma
E-mailove zprávy v rámci služby ČSOB Info 24 mimo osobní konta	1 Kč
Fax	10 Kč
Pošta	20 Kč
Ostatní služby	
Opětovné poskytnutí PIN	100 Kč
Vydání čtečky karet	500 Kč
Vydání a obnova bezpečnostního certifikátu pracovníkem banky	400 Kč
Vydání a obnova bezpečnostního certifikátu internetovým bankovnictvím	200 Kč
Mimořádná obnova bezpečnostního certifikátu (před koncem platnosti)	400 Kč

5.2.3 UniCredit Bank Czech Republic and Slovakia, a.s. – bezpečnostní a ekonomické aspekty

Rozdíl v bezpečnosti oproti předchozím bankám je v tom, že pro přihlášená do internetového bankovnictví nenabízí možnost přihlášení pomocí certifikátu. Přihlášení do systému je podmíněno zadáním uživatelského čísla a kódu z bezpečnostního klíče. Tento klíč může mít podobu Smart Klíče, SMS klíče či takzvané kalkulačky. Způsob zabezpečení si klient sám zvolí na pobočce při zřizování produktu.

5.2.3.1 Smart Klíč

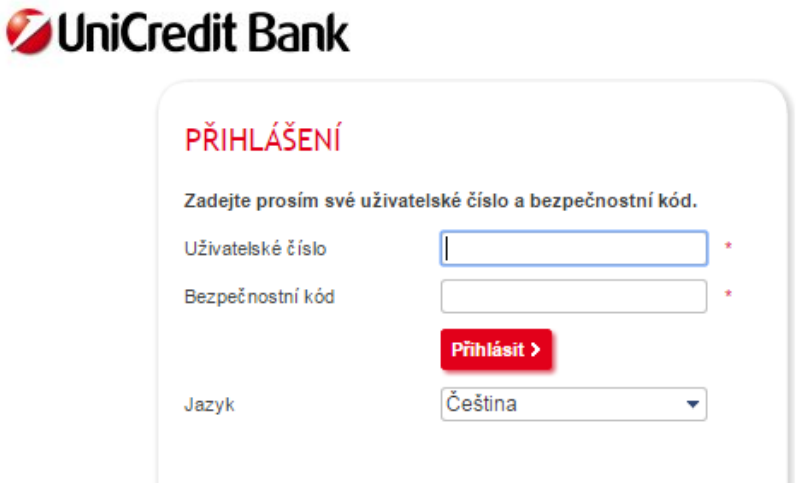
Mobilní aplikace, která generuje jednorázové časově omezené kódy. Majitelé chytrých zařízení mohou získat Smart klíč stažením aplikace Smart Bankingu z Google Play nebo App Store.

5.2.3.2 *SMS klíč*

Kódy pro přihlášení a platby jsou doručovány prostřednictvím SMS. Kód má časově omezenou platnost

5.2.3.3 *Bezpečnostní klíč (PIN kalkulátor)*

Přídavné zařízení ve tvaru kalkulačky, které se aktivuje pomocí PINu a vygeneruje kód pro přihlášení nebo podpis platby.



Obr. 6. Přihlášení do služby Online Banking [34]

UniCredit Bank nabízí informativní SMS nebo e-mail, který kontaktuje při každém přihlášení do účtu klienta. Tedy další bezpečnostní prvek banky. UniCredit Bank také nabízí stejně jako předchozí banky bezpečnostní limit pro denní transakci, který činí 500 000 Kč.

Poplatky spojené s uživáním internetového bankovnictví jsou opět zaznamenané do tabulky pro větší přehlednost.

Tab. 11. Poplatky za službu Online Banking [35]

Zřízení služby	zdarma
Měsíční užívání	70 Kč
Zrušení	zdarma
Příchozí platby z jiné tuzemské banky	6 Kč
Odchozí platba do jiné tuzemské banky	6 Kč
Trvalý příkaz do jiné tuzemské banky	6 Kč
Ostatní poplatky	
Zasílání informační SMS zprávy	1,90 Kč
Zasílání informační e-mailové zprávy	zdarma

Nástroje pro přihlášení a podepisování transakcí	
Smart klíč	zdarma
SMS klíč – sada 100 SMS	90 Kč
Token (kalkulačka) – předání a incializace	490 Kč
Změna nastavení uživatele	zdarma
Blokace/odblokace přístupu uživatele k přímému bankovnictví	zdarma
Nastavení profilu pro mezinárodní použití	1000 Kč

5.3 Celkové porovnání a vyhodnocení

V této poslední části kapitoly, jsou shrnuty veškeré informace, které byly při vypracování této bakalářské práce zjištěny, a je provedeno celkové vyhodnocení, podle výše zmíněných údajů.

První kritérium, které bylo vybráno pro vyhodnocení, je rovněž to nejdůležitější, tedy úroveň zabezpečení. Po prozkoumání jednotlivých systému mohu říct, že stupeň zabezpečení je u všech bank na vysoké úrovni, což souvisí také s vysokou mírou veřejnoprávní regulace bankovnictví jako takového. Všechny banky, které byly porovnávány, nabízejí aspoň jeden z nadstandartních systémů zabezpečení. Ať už je to přihlašování podle certifikátu spojené s využitím čipových karet nebo nějakého druhu PIN kalkulátoru. Pokud se zaměříme čistě na způsob přihlášení do systému, tak Česká spořitelna nabízí jako jediná možnost přihlášení pomocí grafické klávesnice. Toto je velice dobrá metoda neboť vylučuje riziko spojené s použitím keyloggeru

Tab. 12. Bezpečnostní prvky [vlastní]

Název banky	Uživatelské číslo, heslo	Autorizační certifikát	Čipová karta	PIN kalkulátor	Grafická klávesnice	Automatické odhlášení
Česká spořitelna	Ano	Ano	Ano	NE	ANO	ANO
ČSOB	ANO	ANO	ANO	NE	NE	ANO
UniCredit bank	ANO	NE	NE	ANO	NE	ANO

Druhá oblast pro srovnání se týkala výše poplatků účtovaných bankami za poskytování jejich služeb IB. Spočítali jsme, kolik u které banky zaplatí za využívání internetového bankovnictví klient, který využívá pravidelně tuto službu, ale také méně aktivní klient.

Jedná se o poplatky, které tito klienti zaplatí za měsíční využití služeb internetového bankovnictví. Poplatky se týkají pouze využití internetového bankovnictví, k celkové ceně není přičtena částka za měsíční vedení osobního účtu.

Tab. 13. Náklady/Poplatky za využití IB [vlastní]

Název banky	Náklady pravidelného uživatele	Náklady občasného uživatele
Česká spořitelna SERVIS 24	200 Kč	79 Kč
ČSOB Internet Banking 24	75 Kč	39 Kč
UniCredit Bank Online Banking	230 Kč	120 Kč

U kritéria zabezpečení byly porovnávané banky na velice podobné úrovni. Kdybychom měli hodnotit banky bodově od 0 – 10, kdy 10 je nejlepší hodnocení, všechny porovnávané banky by dosáhly hodnocení 10. U nákladů tomu však tak není. V nákladech na měsíční využití poskytované služby internetového bankovnictví skončilo nejlépe ČSOB, která má nejnižší měsíční poplatek a to 20 Kč za vedení Internet Banking 24. Celkově i poplatky za příchozí, odchozí platby a trvalé příkazy jsou nejnižší. Pokud by klient chtěl vyšší třídu zabezpečení, ať už klientský certifikát nebo PIN kalkulátor připlatil by si tyto částky:

Tab. 14. Cenová nákladnost vyššího bezpečnostního stupně [vlastní]

Název banky	Čipová karta	Čtečka karet	Platnost certifikátu 1 rok
Česká spořitelna	350 Kč	350 Kč	350 Kč
ČSOB	250 Kč	250 Kč	400 Kč
Název banky	Smart klíč	SMS klíč (100 ks)	PIN kalkulátor
Unicredit Bank	zdarma	90 Kč	490 Kč

Dalším kritériem v oblasti poplatků je využití platební karty, v našem případě debetní karty. V tomto porovnání jsou zahrnuty měsíční poplatky za vedení karty, výběr hotovosti v bankomatu a platba v obchodech. V porovnání jsou základní debetní karty vydávané k běžnému účtu.

Tab. 15. Poplatky za debetní kartu [vlastní]

Název banky	Vedení karty (ročně)	Výběr hotovosti z vlastních bankomatů	Výběr hotovosti z bankomatů ostatních bank	Bezhotovostní platba u obchodníka
Česká spořitelna	400 Kč	5 Kč	40 Kč	zdarma
ČSOB	540 Kč	6 Kč	35 Kč	zdarma
UniCredit Bank	500 Kč	5 Kč	30 Kč	zdarma

Pro zjištění, která z uvedených bank je nejvýhodnější, byli opět zvoleni dva klienti, jeden s pravidelným využitím obou možností výběru hotovosti a klient s občasným využitím obou druhů výběru:

Klient 1:

- 30 výběrů hotovosti z bankomatů vlastní banky ročně
- 20 výběrů z hotovosti z bankomatů ostatních bank

Klient 2:

- 15 výběrů hotovosti z bankomatů vlastní banky
- 5 výběrů z hotovosti z bankomatů ostatních bank

Tab. 16. Poplatky za debetní kartu klienta 1 [vlastní]

Klient 1	Výběr hotovosti z vlastních bankomatů	Výběr hotovosti z bankomatů ostatních bank	Vedení karty	Celkem
Česká spořitelna	150 Kč	800 Kč	400 Kč	1350 Kč
ČSOB	180 Kč	700 Kč	540 Kč	1420 Kč
UniCredit Bank	150 Kč	600 Kč	500 Kč	1250 Kč

Tab. 17. Poplatky za debetní kartu klienta 2 [vlastní]

Klient 2	Výběr hotovosti z vlastních bankomatů	Výběr hotovosti z bankomatů ostatních bank	Vedení karty	Celkem
Česká spořitelna	75 Kč	200 Kč	400 Kč	675 Kč
ČSOB	90 Kč	175 Kč	540 Kč	805 Kč
UniCredit Bank	75 Kč	150 Kč	500 Kč	725 Kč

Při porovnání, která banka je výhodnější pro užívání platební karty musíme toto porovnání rozdělit do dvou skupin. Pokud klient pravidelně využívá výběr hotovosti jak u své tak u jiné banky, nejvýhodnější pro něj je zvolit UniCredit Bank, která obstála nejlépe. Pokud klient nevyužívá výběr hotovosti pravidelně, tak nejvýhodnější je zvolit Českou spořitelnu. Nejhůře obstála ČSOB, která nebyla nejvýhodnější ani pro jednoho z porovnávaných klientů.

5.3.1 Kterou banku zvolit

Jak bylo řečeno výše, v oblasti zabezpečení jsou všechny porovnávané banky na vysoké úrovni. Je znát, že pro všechny banky je toto kritérium velice důležité a nepodceňují ho. Jedinou výhodu má podle mého názoru Česká spořitelna s použitím grafické klávesnice. Tedy pokud chce uživatel k bezpečnosti něco navíc, měl by zvolit právě Českou spořitelnu. Domnívám se, po dospění k závěru, že úroveň zabezpečení je u všech porovnávaných bank velmi obdobná, že by bylo vhodné pro výběr správné banky přidat další kritérium, kterým je přehlednost a srozumitelnost služby pro uživatele. Prizmatem tohoto kritéria bych doporučil ČSOB, jejíž systém je velice jednoduchý, působí přátelsky a přehledně.

Pokud jde o poplatky spojené s využíváním internetového bankovnictví, tak jasným vítěz na tomto poli je ČSOB. Jak pro pravidelného uživatele, tak i občasného uživatele vyjde z finančního hlediska ČSOB nejpříznivěji. Je výhodnější i v případě pořízení vyššího stupně zabezpečení. Ale ukázalo se, že ČSOB není tak výhodná při používání platebních karet, kdy z porovnávaných bank skončila nejhůře. V mém zhodnocení jsem zjistil, že aby bylo možné zvolit nejvýhodnější banku, tak si musí klient nejdříve uvědomit, jaké služby bude nejvíce využívat. A podle toho se pak rozhodnout, která banka je pro něj nejlepší. Z mého osobního hlediska jako student, který nevyužívá tak často výběru hotovosti ale spíše internetového bankovnictví je nejvýhodnější ČSOB.

6 BEZPEČNOSTNÍ RIZIKA A PODVODY – PRAKTICKÉ HLEDISKO

V teoretické části byly popsány nejpoužívanější hrozby v elektronickém bankovnictví. V praktické bude ukázáno, jak tyto podvody prakticky probíhají, bude to znázorněno na modelových strukturách. U bezpečnostních kroků, které se liší u uvedených bank, budou tyto kroky porovnány.

6.1 Libanonská smyčka

Celý podvod probíhá asi tak, že podvodník si vybere bankomat, a poté upraví jeho část pro platební kartu zmiňovaným zařízením. Pak čeká na svoji oběť. Pokud držitel karty (tedy oběť) vloží svoji platební kartu do bankomatu, zařízení ji uzamkne tak, že ji už nepůjde z bankomatu vyjmout. Karta tedy zůstane zachycena v libanonské smyčce. To je chvíle pro podvodníka, který, jakmile uvidí, že držitel karty vzdá svůj boj o kartu, přistoupí k bankomatu a kartu si vezme. Pro větší přehlednost byl tento podvod zaznamenán do modelové struktury.

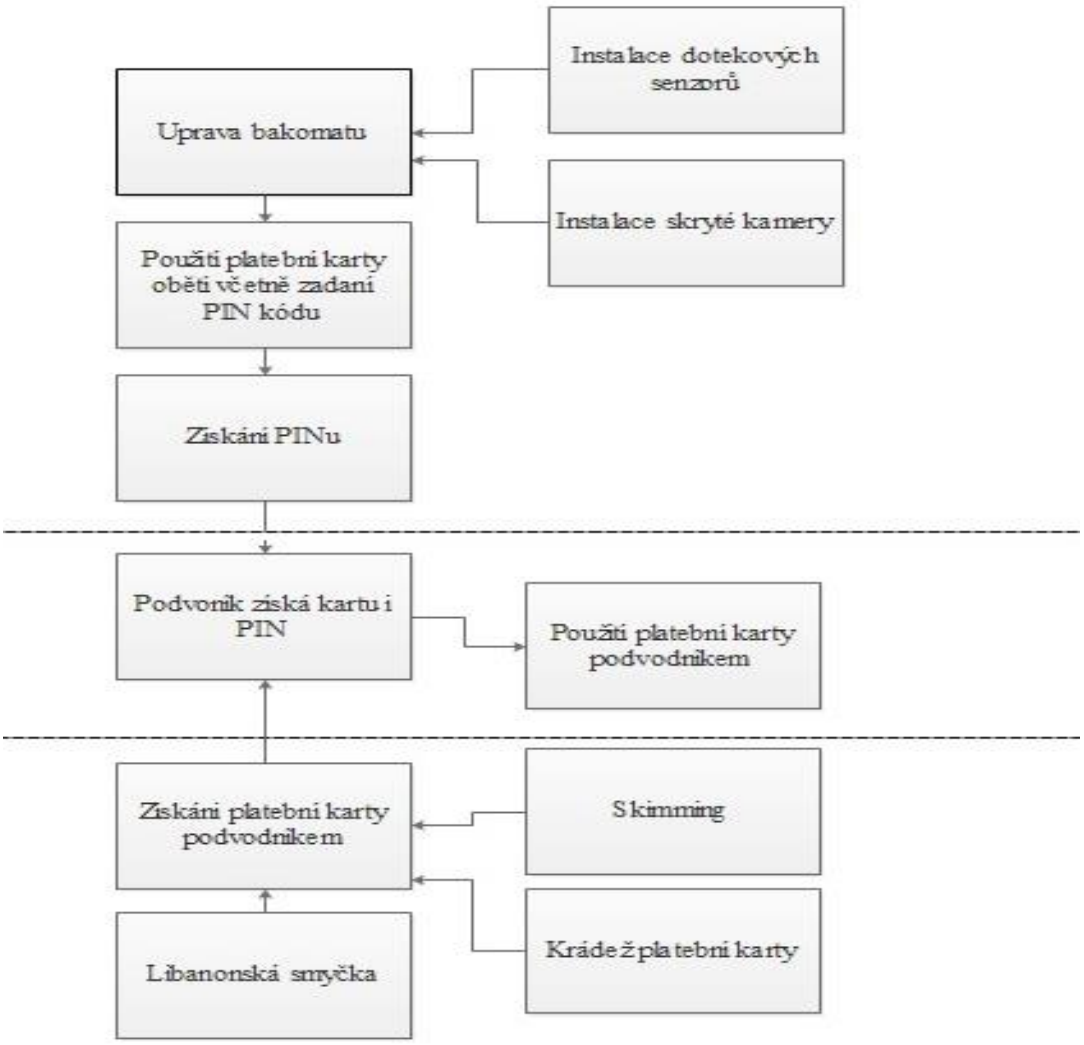
Obr. 7. Modelová struktura použití Libanosnké smyčky [vlastní]

6.1.1 Zabezpečovací kroky

U tohoto druhu podvody se zabezpečovací kroky bank nijak neliší. Zabezpečení probíhá tak, že provozovatel bankomatu přidá na bankomat speciální zařízení. Toto zařízení je nástavec, který se přidá na místo pro vkládání platebních karet. Tento nástavec má speciální tvar, který zabrání instalací jiného zařízení.

6.2 Skryté kamery a dotekové senzory

Jedná se o druhy podvodů, které se používají společně s libanonskou smyčkou, aby podvodník získal jak platební karty, tak číslo PIN kódu. Tento podvod byl znovu zaznamenán do modelové struktury.



Obr. 8. Modelová struktura využití skryté kamery nebo dotekových senzorů [vlastní]

Na modelové struktuře vidět, jak jsou různé podvody spojovány, aby podvodník dosáhl co nejvyšší úspěšnosti se zneužitím karty.

6.2.1 Zabezpečovací kroky

U tohoto podvodu je problém v zavedení bezpečnostních prvků z pohledu bank. Není možné přidat nějaké nástavné zařízení, které by zabránilo podvodníkům instalaci skrytých kamer (mohou být umístěny kdekoliv, nemusí být přímo na bankomatu) nebo dotekových senzorů. Jediným možným krokem je pravidelná kontrola bankomatů nebo platebních terminálů. Z tohoto důvodu byl proveden návrh bezpečnostního doporučení pro uživatele bankomatů a platebních terminálu.

6.2.2 Návrh bezpečnostního doporučení pro snížení rizika skrytých kamer a dotekových senzorů

Pokud jde o riziko spojené s použitím skrytých kamer, tak ochrana je jednoduchá. Každý kdo zadává svůj PIN kód, by měl druhou rukou zakrývat klávesnici. Dalším prvkem bezpečnosti by měla být kontrola zařízení, ale i jeho okolí před jeho použitím. Pokud bude zařízení vypadat upraveně, tak by nemělo být použito. Pro vyloučení rizika spojeného s dotekovým senzorem, by mělo být zkontrolováno, jestli se na klávesnici zařízení nejsou odnímatelné předměty. Při dodržení těchto pravidel riziko zneužití je minimální.

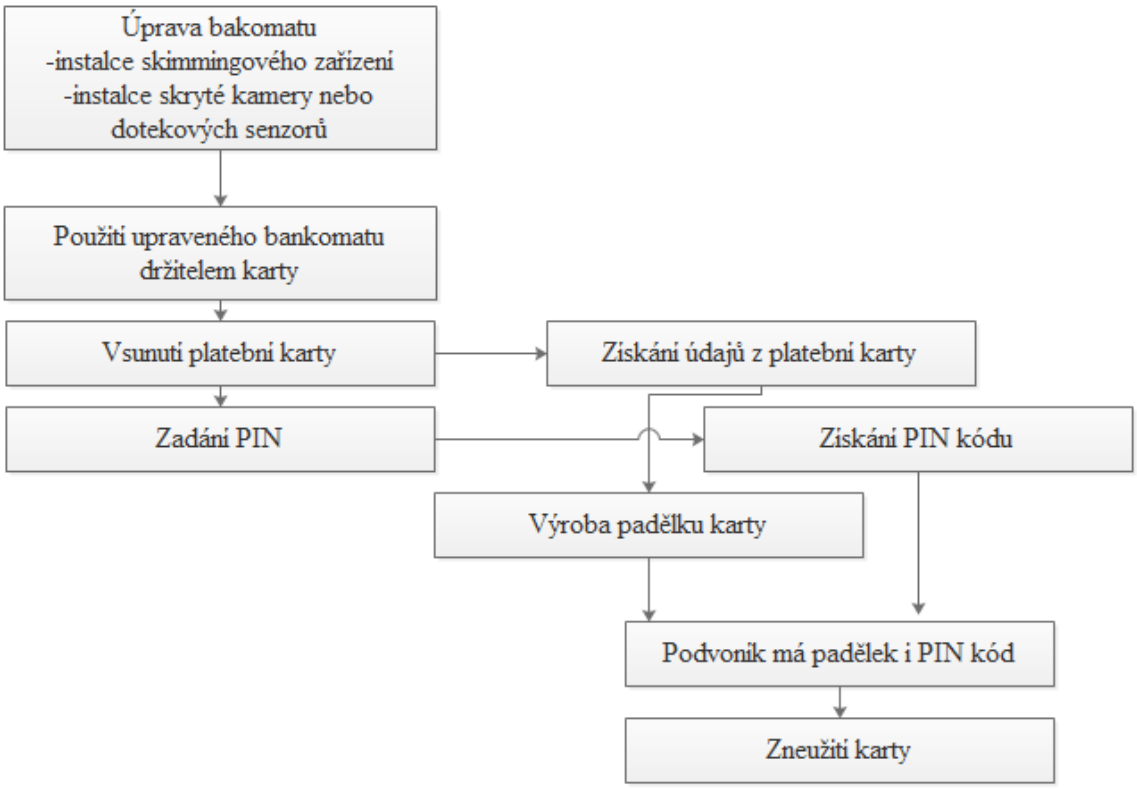
6.3 Skimming

Použití skimmingu můžeme rozdělit na dvě části, protože každá má jiný postup. Tedy skimming použitý u bankomatu a skimming použity přímo u prodejce.

Při použití na bankomatu je skimmovací zařízení zabudováno do místa pro vložení platební karty. Skimmovací zařízení je vlastně přídavný nástavec, pokud je do něho vložena karta, dokáže z této karty zkopírovat citlivé údaje.

Pokud se jedná o skimming použitý přímo u prodejce nebo obchodníka, jsou používány dvě metody. První metoda je připojení skimmovacího zařízení přímo na platební terminál. Druhá metoda využívá nepozornosti zákazníka. Tedy obchodník třeba klientovi řekne, že mu přestal fungovat terminál, že si musí odnést kartu, aby ji ověřil, například v kanceláři a, přitom dojde k jejímu zkopírování.

Také tento druh podvodu bývá podvodníky spojován s dalšími metodami, aby získali jak citlivé informace, tak popřípadě PIN kód. Využívají tedy navíc opět skryté kamery nebo dotekové senzory.

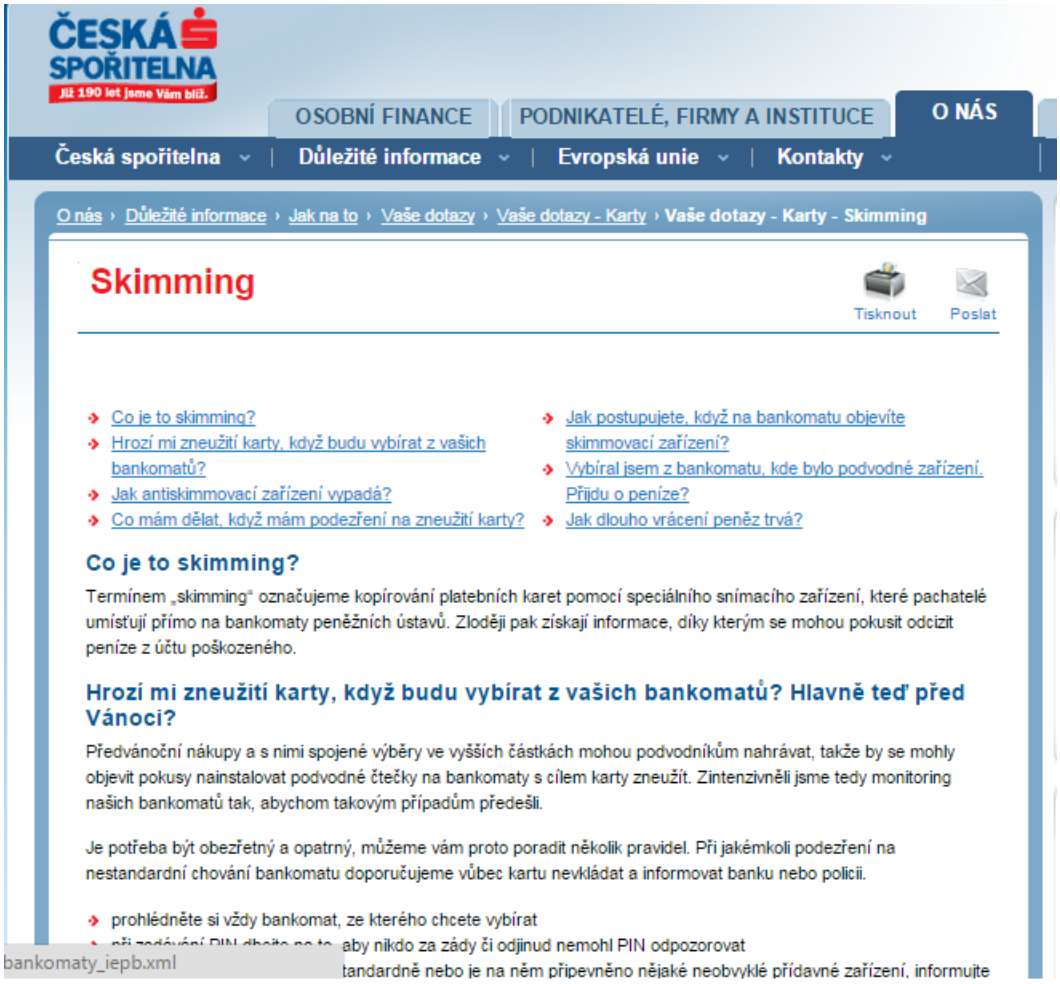


Obr. 9. Modelová struktura Skimmingu [vlastní]

6.3.1 Zabezpečení

Pro zabezpečení banky využívají speciální zařízení neboli úprava bankomatu, která je schopná zmenšit riziko skimmingu. Ale úplné odstranění rizika zatím není možné. Pokud jde o funkci speciálního zařízení proti skimmingu, jde o tzv. antiskimmovací zařízení, které se také přikládá před vstup pro platební kartu a tím by mělo zabránit instalaci dalších přídavných zařízení pro kopírování údajů z platebních karet. Z bezpečnostních důvodů by měl každý, kdo chce využít bankomat sám zkontrolovat, jestli mu nepřijde bankomat upraven.

Pokud jde o banky porovnávané v mé práci. Tak jako jediná Česká spořitelna na svých stránkách uvádí informace o skimmingu, jakých bezpečnostních pravidel se mají jejich klienti držet, jak skimmingové zařízení poznají a informují o jejich bezpečnostních opatřeních, které proti skimmingu Česká spořitelna využívá.



Obr. 10. Informace České spořitelny o skimmingu [36]

Podle mého názoru, informovat klienty o možné hrozbě je důležitým faktorem. Ať už pomocí webové stránky, informačních zpráv anebo zobrazení informací o hrozícím riziku přímo na bankomatu. Tímto bezpečnostním prvek se řídí například britská Barclays Bank, která na svých bankomatech varuje své klienty.

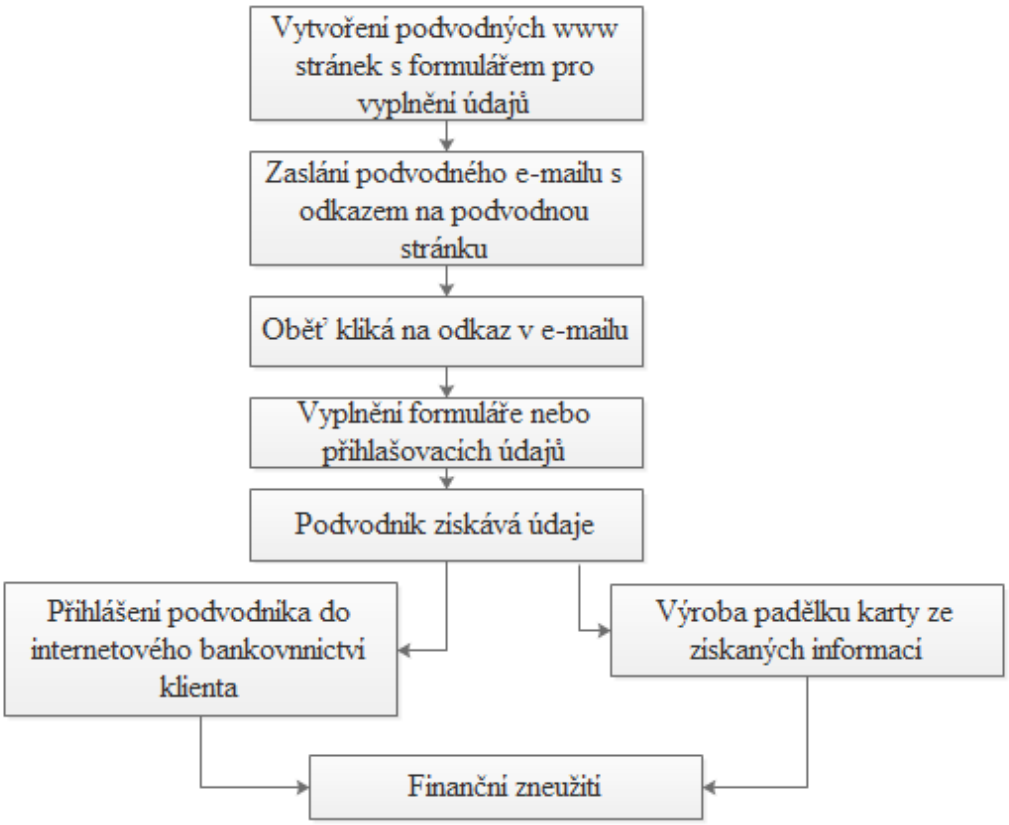
6.4 Phishing

Výhodou phishingu pro podvodníky je v tom, že mohou oslovit velkou řadu potencionálních obětí a tím se zvyšuje pravděpodobnost, že někdo tomuto podvodu uvěří, a udělá, co je po něm žádáno.

Obr. 11. Podvodný e-mail (pharming) [37]

Obr. 12. Podvodná stránka České spořitelny [37]

Na Obr. 11 a 12 můžeme vidět typickou ukázku phishingu. Oběť obdrží podvodný e-mail s odkazem na podvodníkem vytvořenou webovou stránku, která je k nerozeznání od originálu. Pokud se oběť přes tuto webovou stánku přihlásí, informace jí zadané se odešlou podvodníkovi, a ten je následně může zneužít. Jediný faktor, který ukazuje na podvrh této stránky, je odkaz s brazilskou doménou. Pro větší přehled je celý průběh zaznamenaný na modelu.



Obr. 13. Modelová struktura pharmingu [vlastní]

6.4.1 Zabezpečení

Proti tomuto druhu podvodu reaguji porovnávané banky následovně.

Česká spořitelna na svých webových stránkách pravidelnou informací o hrozících nebezpečí phisgingu. Nejenom informuje ale daný „phishing útok“ také dopodrobna popisuje a také doporučuje jak na takový „útok“ zareagovat.

23.4.2015
Varujeme před další verzí phishingu
Rádi bychom vás upozornili na novou podobu podvodného e-mailu (tzv. phishingu). Zpráva vzbuzuje dojem, že byla zaslána Českou národní bankou a požaduje po klientovi ověření původu jeho peněz. Zpráva je podvodná a jejím cílem je pouze vylákání osobních údajů klientů.

16.4.2015
Upozornění na opakující se phishingový útok
Upozorňujeme na opakující se šíření podvodného emailu (tzv. phishingu. Zpráva vyzývá příjemce k úhradě dlužné částky, která vznikla v důsledku využívání bankovního produktu

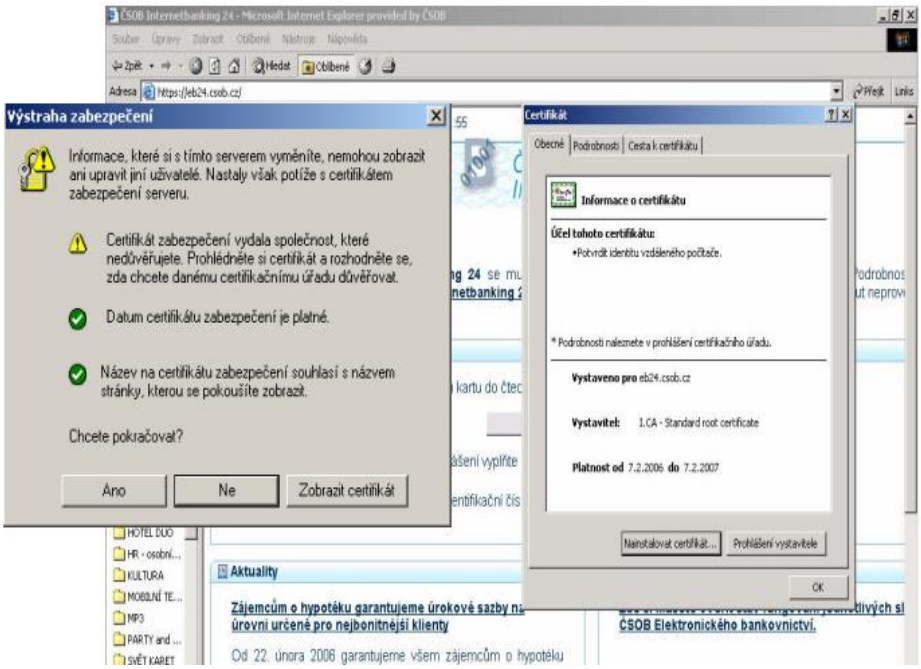
9.4.2015
Upozornění na možné zneužití internetového bankovnictví prostřednictvím Facebooku
Opět upozorňujeme na možné zneužití internetového bankovnictví prostřednictvím sociální sítě Facebook. Pachatelé se jejím prostřednictvím snaží vylákat přihlašovací údaje k internetovému bankovnictví klienta.

3.4.2015
Upozorňujeme na nové chování počítačového viru
Upozorňujeme na novou podobu a chování počítačového viru, který v napadeném počítači klientovi zobrazí po přihlášení do internetového bankovnictví informaci o chybné platbě, která byla připsána na jeho účet. Dále klienta informuje, že z tohoto důvodu je jeho účet dočasně zablokován, dokud nepotvrdí vrácení připsané platby zpět potvrzením tlačítka „pokračovat". Důrazně varujeme před jakoukoliv reakcí na tuto obrazovku, útočníci se touto formou snaží získat z klientova účtu jeho vlastní peníze.

Obr. 14. Varování České spořitelny před Phishingem [36]

Součástí bezpečnostních opatření je pro klienty banky dostupný seznam bezpečnostních pravidel jak využívat elektronické bankovnictví.

Pokud jde o ČSOB, reaguje podobně jako Česká spořitelna, informováním o hrozícím nebezpečí přímo na svých webových stránkách. Součástí opatření ČSOB je také seznam bezpečnostních pravidel jak využívat elektronické bankovnictví, a také návod jak si ověřit pravost stránky přes certifikát. Toto opatření zabraňuje riziku, že by se klient přihlásil do svého IB prostřednictvím falešné stránky.



Obr. 15. Návod od ČSOB jak ověřit pravost stránky [38]

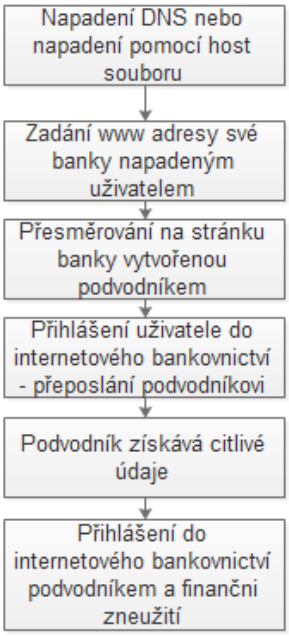
Opatření třetí porovnávané banky UniCredit Bank je opět velice podobné. Na svých webových stránkách varují před možnou hrozbou. UniCredit Bank upozorňuje své klienty, že veškeré citlivé údaje spojené s využitím elektronického bankovnictví zajišťují pouze jejich zaměstnanci, a to jen formou dopisu nebo osobně na pobočce, nikdy prostřednictvím internetu.

6.4.2 Porovnání bezpečnostních opatření bank při phishingu

Bezpečnostní prvky všech tří bank jsou na vysoké úrovni. Všechny varují, že nikdy nevyžadují po svých klientech citlivé informace prostřednictvím e-mailu. A pokud je zjištěna hrozba, tak na svých stránkách o tomto riziku své klienty informují. Součástí varování bývá i zasláni informací o aktuální hrozbě přímo do internetového bankovnictví klienta. Takže není nutno pravidelně navštěvovat stránky banky a vyhledávat nová rizika. I když bezpečnost je u všech prakticky stejná, nejvíce se mi líbil systém České spořitelny, který nabízí celou databázi hrozeb, která je pravidelně aktualizovaná. Na rozdíl od zbývajících dvou bank, které nemají vlastní databázi, a informace na jejich stránkách si musí klient sám vyhledat.

6.5 Pharming

Podoba pharmingu, která byla popsána v teoretické části je velice účinná, ale také velice obtížná pro realizaci. Proto se více využívá druhý způsob pharmingu, který je jednodušší. Princip je v tom, že se podvodník snaží o zapsaní adresy jeho vytvořených webových stránek s příslušnou doménou do tzv. host souboru, který pracuje v určeném operačním systému, podobně jako DNS. Tento soubor obsahuje IP adresy a jim odpovídající domény. Podvodník může napadnout počítač oběti různými způsoby. Přes e-mail, který obsahuje trojského koně, nebo pokud si oběť stáhne nějakou podvodníkem vytvořenou podvodnou aplikaci, která vypadá jako velice užitečná, ale také jen pouhým kliknutím na odkaz na internetu.



Obr. 16. Modelová struktura použití pharmingu [vlastní]

Existuje ještě jeden způsob použití pharmingu a to tak, že webové stránky vytvořené podvodníkem slouží jako prostředník. To znamená, že jsou přeposílány pouze autorizační údaje do skutečného systému banky. Pokud se uživatel přihlásí na podvodné stránce, dostane se do svého internetového bankovnictví ale údaje jako například velikost platby a číslo účtu může podvodník měnit.

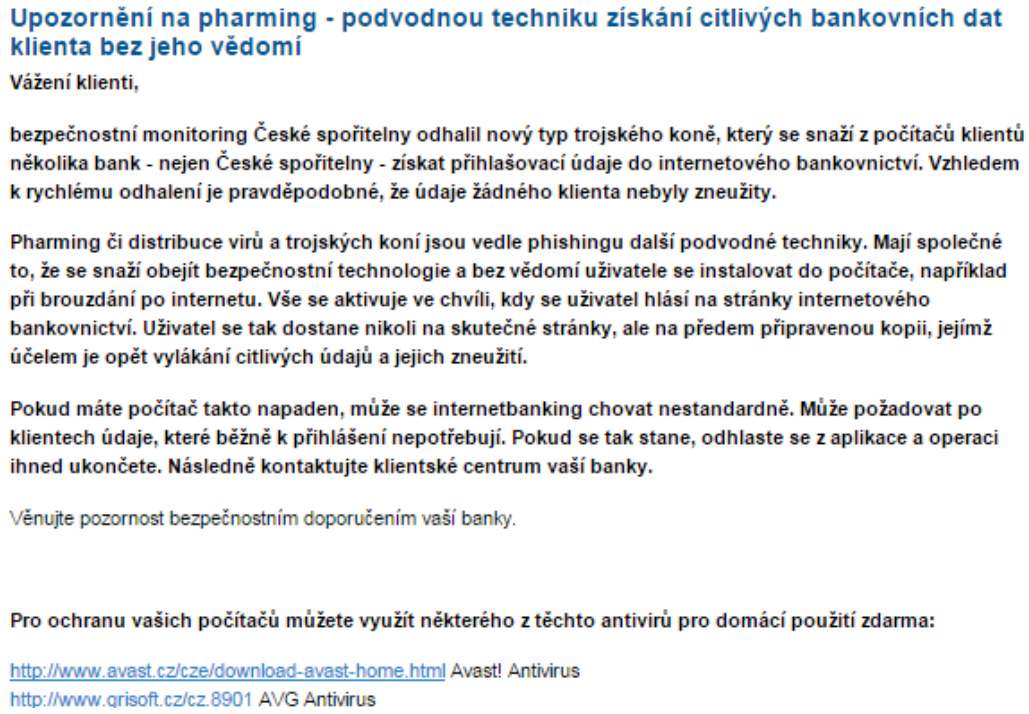
6.5.1 Zabezpečovací kroky

Banky obecně pro snížení rizik napadení pharmingem poskytují různé doplňkové nástroje pro docílení větší bezpečnosti, jako jsou autorizační SMS pro potvrzování transakcí nebo využití klientských certifikátu. Tyto metody již byly v mé práci popsány. Tímto je zabezpečeno, že pokud podvodník dokáže získat přihlašovací údaje, nemůže manipulovat s převody peněz. Dalším bezpečnostním doporučením je, že každý, kdo využívá internetové bankovnictví na svém počítači, by měl mít kvalitní antivirový program a používat firewall.

6.5.2 Porovnání bezpečnostních opatření bank při pharmingu

Pokud jde o námi porovnávaná banky, tak všechny nabízí nějaký způsob autorizace transakcí. Takže se dá opět konstatovat, že bezpečnost proti tomuto podvodu je na vysoké úrovni u všech bank. Důležité je, aby si klient zvolil nejbezpečnější systém při zakládání svého účtu.

I když všechny porovnávané banky jsou v tomto ohledu bezpečné, tak opět něco na víc přináší Česká spořitelna. Nejenom, že jako jediná na svých webových stránkách informuje o hrozbě pharmingu, ale také doporučuje, které programy si klient může stáhnout pro větší zabezpečení svého počítače. A to jak placené tak programy zdarma.



Upozornění na pharming - podvodnou techniku získání citlivých bankovních dat klienta bez jeho vědomí

Vážení klienti,

bezpečnostní monitoring České spořitelny odhalil nový typ trojského koně, který se snaží z počítačů klientů několika bank - nejen České spořitelny - získat přihlašovací údaje do internetového bankovnictví. Vzhledem k rychlému odhalení je pravděpodobné, že údaje žádného klienta nebyly zneužity.

Pharming či distribuce virů a trojských koní jsou vedle phishingu další podvodné techniky. Mají společné to, že se snaží obejít bezpečnostní technologie a bez vědomí uživatele se instalovat do počítače, například při brouzdání po internetu. Vše se aktivuje ve chvíli, kdy se uživatel hlásí na stránky internetového bankovnictví. Uživatel se tak dostane nikoli na skutečné stránky, ale na předem připravenou kopii, jejímž účelem je opět vylákání citlivých údajů a jejich zneužití.

Pokud máte počítač takto napaden, může se internetbanking chovat nestandardně. Může požadovat po klientech údaje, které běžně k přihlášení nepotřebují. Pokud se tak stane, odhlaste se z aplikace a operaci ihned ukončete. Následně kontaktujte klientské centrum vaší banky.

Věnujte pozornost bezpečnostním doporučením vaší banky.

Pro ochranu vašich počítačů můžete využít některého z těchto antivirů pro domácí použití zdarma:

http://www.avast.cz/cze/download-avast-home.html Avast! Antivirus
http://www.grisoft.cz/cz.8901 AVG Antivirus

Obr. 17. Upozornění na Pharming od České spořitelny [39]

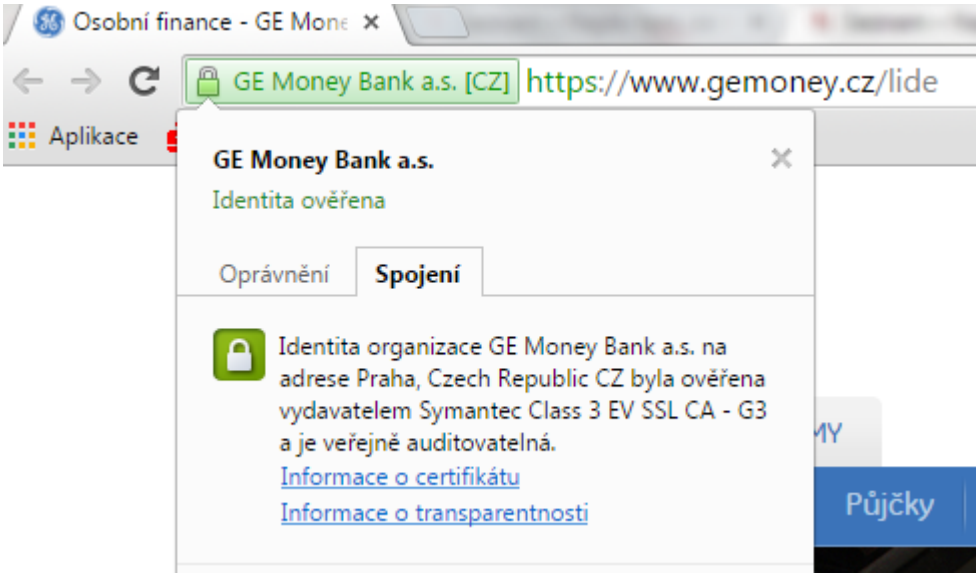
7 DOPORUČENÍ PRO UŽIVATELE PRO SNÍŽENÍ RIZIKA ZNEUŽITÍ

Jak bylo uvedeno výše, elektronické bankovnictví přináší lidem velké výhody a pohodlí, ale také množství hrozeb, které byly rovněž zmiňovány. V této části mé práce se budeme zabývat návrhem doporučení bezpečného zacházení s prostředky elektronického bankovnictví.

7.1 Návrh doporučení bezpečného zacházení při použití internetu

Základem pro využívání elektronického bankovnictví nebo elektronického obchodu je internet. Proto každý, kdo využívá tuto metodu bankovnictví, by měl dodržovat následující bezpečnostní pravidla pro použití internetu.

1. **Nevěřit všem obdrženým informacím na internetu** – tímto je myšleno nevěřit všem e-mailům, které uživatel dostane do jeho schránky, nebo nevěřit informacím vyčteným na internetových stránkách. Všechny důležité informace by měly být ověřeny.
2. **Nestahovat žádné podezřelé programy nebo aplikace** – uživatel by měl z internetu stahovat jen takový software, o kterém si je jistý, že je nezávadný. Nestahovat žádný software, o kterém uživatel nic netuší a jen se mu jeví jako užitečný. Dále neklikat na žádné neznámé odkazy, většinou obsahují nežádoucí software. Jedná se především o odkazy pro vyzvednutí výhry apod.
3. **Využívat bezpečnou komunikaci https://** - pokud v adresním řádku začíná adresa https://, jedná se o bezpečnou komunikaci mezi prohlížečem a serverem. Pokud ale adresa začínající na http://, jedná se o nezabezpečenou komunikaci. Této by se měl uživatel vyvarovat.
4. **Ověřovat stránky** – o každé webové stránce se dá zjistit, jestli obsahuje certifikát, který potvrzuje pravost stránky. Dozvíme se to tak, že klikneme na symbol zámku, který se nachází většinou u adresního řádku. Po kliknutí se zobrazí, zda stránka obsahuje certifikát a kdo ho vydal.



Obr. 18. Certifikát stránky [40]

5. **Kontrola e-mailů** – uživatel by neměl otvírat a v žádném případě nestahovat přílohy z emailů, o kterých nic neví.
6. **Zapamatování citlivých údajů** – uživatel by si neměl svoje citlivé údaje jako například přihlašovací jména a hesla nikam zapisovat, ale měl by si je pamatovat. Pokud není schopen si tyto údaje zapamatovat, měl by si vytvořit nějakou pomůcku, která mu pomůže se zapamatováním. Pokud ani použitím pomůcky není schopen si údaje zapamatovat a musí si je někam zapsat, měl by velmi pečlivě vybrat místo, kam si je zapisuje.
7. **Bezpečná tvorba hesel –** při tvorbě hesla by měl uživatel dodržovat několik zásad. Heslo by nemělo obsahovat základní informace o něm nebo o osobě jemu blízké, například datum a místo narození nebo jméno. Dále by nemělo jít o nějakou jednoduchou kombinaci jako je „123456“. Heslo by tedy mělo být dlouhé (minimálně 8 znaků) a mělo by obsahovat velká a malá písmena zkombinované se znaky. Další dobrou metodou je použít nějakou větu a zní potom vytvořit heslo. Další metodou vytvoření hesla, může být metoda spojena se známou větou a zní vytvořeného hesla. Jako například věta „**Dvakrát měř, jednou řež“** a tvorba hesla by vypadala následovně **2xm;J5**. Vyměnili jsme tedy slova dvakrát=2x, měř=m, čárka=; jednou=j, řež=5 (5je číslice nad písmenem ř)
8. **Nepoužívat stejná hesla na více stránkách –** uživatel by měl mít jiné heslo jak pro přístup k e-mailu, tak pro přistup například do sociální sítě apod. Pokud by do-

šlo k získání nějakých přihlašovacích údajů, tak by měl podvodník přístup jen k jedné aplikaci a ne ke všem.

9. **Obměna hesla za určitý časový interval –** uživatel by měl svá hesla do důležitých systémů měnit minimálně třikrát do roka. Pokud jde o méně významné systémy, tak by obměna měla být alespoň jednou ročně.
10. **Používat jiné e-mailové schránky na zábavu a pro internetové bankovnictví –** uživatel by měl mít rozdělené své e-mailové schránky, aby neposkytoval svou důležitou e-mailovou adresu (důležitou v tom smyslu, že ji má registrovanou pro banku a jiné důležité instituce) při registraci do nějakých webových stránek.
11. **Nevyužívat automatické přihlášení –** toto doporučení se týká počítačů, které nevlastní uživatel a má k nim přístup někdo jiný. Týká se to taky počítače, který vlastní uživatel, ale má k němu přístup také někdo jiný. Mohlo by dojít ke snadnému zneužití.
12. **Odhlašovat se při opuštění stránky –** pokud je uživatel na stránce, která potřebuje přihlášení, tak při odchodu nestačí jen tuto webovou stránku zavřít, ale z důvodu bezpečnosti by se každý měl ohlásit a ještě si zkontrolovat jestli je opravdu odhlášený.
13. **Kontrolovat počítač –** pokud uživatel využívá na svém osobním počítači internet, měl by zkontrolovat, jestli na počítači není přidáno nějaké zařízení, které by mohlo útočníkovi pomoci získat citlivé údaje.
14. **Nevyjadřovat souhlas bez přečtení podmínek** – uživatel, by neměl dávat souhlas na něco, čemu nerozumí nebo si nepřečetl.
15. **Instalovat jen ověřený software –** uživatel by měl instalovat jen ověřené a důvěryhodné programy. Dále by měl pravidelně aktualizovat svůj operační systém. Nejlepším způsobem je mít u důležitých bezpečnostních softwarů jako je operační systém nastavenou automatickou aktualizaci. Při instalaci softwarů jako internetový prohlížeč je důležité, aby uživatel zvážil úroveň jeho zabezpečení. Opět je zásadní instalovat ověřený software.
16. **Instalovat antivirový program –** každý uživatel, který chce připojit svůj počítač k síti internet, by měl ještě před prvním připojením mít nainstalovaný kvalitní antivir. Tento antivir by měl pravidelně aktualizovat. Zde opět platí, že je důležité mít nainstalovaný takový antivir, který je důvěryhodný. Na internetu je spousta antivirů, které se tváří jako velmi užitečné dokonce i odstraňují konkurenční viry, ale

samy obsahují nežádoucí software. V počítači by měl být nainstalován jen jeden antivirový software. Pokud jsou v počítači dva a více těch programů, tak je možné, že se budou navzájem považovat jako hrozba pro počítač.

17. **Používat FIREWALL –** zde platí to stejné jako u antivirového programu, tedy že by měl být nainstalován dříve než uživatel připojí svůj počítač k internetu. Rozdíl mezi antivirem a firewallem je v tom, že antivir chrání počítač před různými viry nebo červi, ale neochrání počítač například před neoprávněným průnikem do systému. Firewall by měl mít pravidelnou aktualizaci a neměl by se nikdy vypínat. Firewall je síťový uzel skládající se z hardwaru a softwaru, který odděluje veřejnou od soukromé sítě. A propouští data mezi nimi podle určitých pravidel, čímž zabraňuje práci s daty bez toho, aby o tom uživatel věděl.
18. **Používat antispyware –** spyware není přímo vir, tudíž ho antivirový program nedokáže detekovat. Proto pro odstranění spywaru je nutno používat antispyware.
19. **Zabezpečit bezdrátovou síť –** pokud k připojení k internetu používáte vlastní vytvořenou domácí síť, měla by být dostatečně zabezpečena. A to tak, aby žádná nežádoucí osoba neměla přístup k citlivým datům. Tato síť by měla mít dostatečně silné heslo a zapnutá zabezpečení určená pro tuto síť (protokol WPA). Pokud jde o umístění vysílače bezdrátové sítě, měl by být umístěn tak, aby jeho signál nedosahoval do míst, kde již není potřeba.
20. **Pravidelně získávat nové informace –** každý, kdo využívá internet jak pro bankovnictví nebo jiné důležité systémy, by se měl zajímat, jaké nové hrozby na internetu jsou. Podvodníci budou přicházet pořád s novými metodami jak získat citlivé údaje a pokud se uživatel bude o to zajímat a bude znát tyto metody, může se lépe bránit.

7.2 Návrh doporučení bezpečného zacházení pro uživatele elektronického bankovnictví

Výše v této práci jsme se již seznámili s tím, že do elektronického bankovnictví patří jak platební karty, tak i jiné systémy, které slouží k elektronické komunikaci klienty s jejich bankou. Doporučení v problematice zneužití se bude týkat v první části uživatelů, kteří využívají platební karty a v druhé části uživatelů využívajících přímé bankovní systémy.

7.2.1 Návrh doporučení v oblasti zneužití pro držitele platebních karet

1. **Volba spolehlivého vydavatele –** pokud chce klient platební kartu, měl by být při vybírání velice pečlivý a zvolit spolehlivého vydavatele. Pokud si může klient zvolit platební kartu, měl by zvolit tu, která nabízí lepší bezpečnostní prvky. Z důvodu vyšší bezpečnosti by klient neměl volit kartu, která obsahuje pouze magnetický pásek, ale spíše čipovou kartu.
2. **Podpis platební karty –** po obdržení platební karty by měla být karta ihned podepsána majitelem karty, a to v souladu s podpisovým vzorem. Podpis na platební kartě je jedním z jejích ochranných opatření. Pokud by byla karta odcizena bez podpisu, zloděj platební karty by jí pak mohl podepsat sám a tím by dosáhl toho, že by jeho podpis seděl s vzorovým podpisem na platební kartě. Pokud bude karta podepsána majitelem karty, tak bude toto riziko sníženo, protože zloděj karty nedokáže napodobit podpisový vzor na kartě.
3. **Správně uschovaná platební karta –** platební karta by měla být uschována na takovém místě, kde k ní nebude mít přístup nežádoucí osoba. Každý držitel platební karty by si měl uvědomit, že při odcizení platební karty může dojít k zneužití jeho finančních zdrojů.
4. **Ochrana platební karty** – u platební karty hrozí, že bude poškozena jak poškrábáním nebo zlomením, tak i jinými způsoby, které si většina držitelů neuvědomuje. Mezi tyto způsoby patří poškození mobilním telefonem, notebookem nebo třeba magnetem (může být součást oblečení nebo doplňků).
5. **Seznámení s bezpečnostními parametry karty –** každý držitel platební karty, by měl vědět, jaké bezpečností vlastnosti má jeho karta, na co si dávat pozor a naopak z čeho nemít strach.
6. **Kontrola dokumentů od platební karty –** platební karta a citlivé údaje k ní jako je PIN kód, přichází držiteli nejčastěji ve formě obálky odděleně. Držitel karty by měl zkontrolovat, jestli obálka, ve které se nachází PIN kód, přišla nepoškozena. Pokud je obálka poškozena, měl by držitel zažádat o nový PIN ke své kartě. Pokud se chce držitel zbavit dokumentů, které obsahují PIN kód, tak by je měl spálit nebo skartovat, v žádném případě nesmí být pouze vyhozeny do odpadků.
7. **Zapamatování PIN kódu –** velkou chybou z hlediska rizika je nosit PIN kód při platební kartě nebo ho mít uložený ve svém telefonu. Nejbezpečnější způsob je si

svůj PIN kód zapamatovat. Některé banky nabízí možnost zvolit si PIN kód vlastní, což usnadňuje zapamatování. Pokud si zvolí držitel karty tento způsob, neměl by volit nějaké jednoduché kombinace jako je například „1234“. Stejně tak by to neměl být snadno zjistitelný údaj jako rok narození. Pokud si držitel nemůže změnit svůj kód nebo si ho z nějakého důvodu neumí zapamatovat a potřebuje ho mít u sebe, tak by se měl řídit následujícím doporučením: Pokud si svůj PIN ukládá do svého mobilu neukládat si heslo pod názvem „PIN kód“, „heslo ke kartě“ ani jinými názvy, které by usnadnili zloději ho získat. Heslo by mělo být uloženo pod jménem nějaké osoby nebo jako součást telefonního čísla (např. založení kontaktu Jan Novák číslo 774158456 a držitel karty ví, že heslo jsou poslední 4 čísla tedy 8456).

8. **Odlišné PIN kódy při využívání více karet –** důvod je jasný, pokud dojde k odcizení platebních karet je menší riziko, že útočník získá přístup ke všem kartám.
9. **Změna PINu –** za určitý časový interval by mělo dojít ke změně PIN kódu.
10. **Nesdělovat kód –** toto doporučení se týká všech lidí, i těch nejbližších. Tento údaj by měl znát pouze vlastník karty, nikdo jiný. Pokud se setkáte se situací, kdy po Vás někdo bude chtít znát tento údaj, můžete si být jistí, že se jedná o nějaký druh podvodu.
11. **Chránit i ostatní údaje o kartě –** při použití karet pro nákup věcí na internetu není potřeba znát PIN kód. Většinou k takovému nákupu stačí znát číslo platební karty, dobu platnosti a CVV nebo CVC. Tohle jsou všechno údaje, které jsou přímo na platební kartě, a při obyčejném opsání nebo ofocení může být karta zneužita. Proto by každý držitel platební karty měl dávat pozor při manipulaci s kartou a nedávat nikomu kartu do rukou.
12. **Kontrolovat místo použití karty –** pokud chce držitel karty svoji kartu použít například v bankomatu, měl by ověřit, zda je toto místo bezpečné. Ověřit znamená podívat se, jestli bankomat neobsahuje nějaké přidané zařízení (dotekové senzory nebo skryté kamery), které by mohlo sloužit útočníkovi k získání citlivých údajů. Pokud má klient podezření, že bankomat nebo nějaký platební terminál nejsou v pořádku, neměl by dokončit plánovou akci s kartou. Měl by kontaktovat například policii
13. **Soustředit se při použití karty –** pokud majitel právě používá platební kartu, měl by veškerou pozornost věnovat právě tomu. Nemůže se nechat někým rozptylovat

nebo si nechat přerušit svoji pozornost. Pokud je v situaci, kdy se nemůže plně věnovat použití karty (někdo na něj neustále mluví, něco vyžaduje), měl by tento čin ukončit a pokračovat až v situaci, kdy bude mít klid.

14. **Nepanikařit pokud při použití bankomatu dojde k zaseknutí karty –** pokud při použití bankomatu dojde k zaseknutí platební karty a nejde ji nijak vytáhnout, okamžitě kontaktujte Vaši banku a ihned si nechte kartu zablokovat. Nikdy si nenechávejte pomoct od cizí osoby. Nikdy nedocházejte od bankomatu, pokud není karta zablokovaná s tím, že ji necháte zablokovat později.
15. **Zadávat PIN tak, aby to nešlo vidět někým jiným –** pokud právě zadáváte PIN kód, jednou rukou zadávejte PIN a druhou použijte jako zakrytí tak, aby nešlo vidět jaký kód zadáváte. Místo druhé ruky jde použít pro zakrytí třeba kabelka nebo peněženka.
16. **Nepoužívat kartu v přítomnosti jiných lidí –** pokud chcete použít kartu a připadá Vám, že Vás někdo pozoruje a nemáte soukromí, tak akci stornujte a proveďte na jiném místě nebo vyčkejte na soukromí. Hrozí zde jak riziko toho, že chce někdo odpozorovat PIN, tak i snaha zjistit číslo karty. Možné riziko je, že útočník může čekat, až vyberete hotovost a poté se bude snažit ji ukrást.
17. **Při výběru větších částek vybírat peníze přímo na pobočkách bank, nikoli v bankomatu.**
18. **Při použití karty pro nákup v některém z internetových prodejen dodržovat bezpečnostní pravidla –** pokud se rozhodnete pro nákup na internetu, měli by jste vyhledávat takové internetové obchody, které mají certifikát SSL a využívají systém 3D-Secure. Zde si můžete být jistí, že tento obchod splňuje bezpečnostní pravidla pro použití platební karty pro nákup. Tady můžeme zmínit i elektronické peněženky, které byly probírány na začátku této práce. Pokud budete platit prostřednictvím těchto peněženek, nehrozí Vám žádné riziko zneužití platební karty při nákupu, protože do peněženky si dáváte jen určitý malý obnos peněž a peněženka není nijak spojená s Vaším bankovním účtem.
19. **Nepoužívat platební karty v cizích zemích pokud to není nutné –** toho doporučení platí převážně v méně rozvinutých zemí (např. Angola, Somálsko, Nepál), kde můžou být menší bezpečnostní prvky než v zemích rozvinutých. Při nutnosti použití by měl být držitel karty velice opatrný.

20. **Nastavovat limty –** myšleny jsou limity pro maximální částku prováděných transakcí. Ať už to je na den nebo týden, či jiný časový interval. Pokud by došlo k odcizení karty i s například PIN kódem, útočník pak může vybrat jen tu maximální částku, kterou máte povolenou. Nastavením limitů jde tedy přecházet velkým škodám.
21. **Zamknutí karet –** používejte možnost zamknutí karty, pokud to vaše karta dovoluje. Její zamknutí zabrání jakékoliv manipulaci s kartou. Ať už jde o výběr hotovosti nebo platby, jak v kamenném obchodě, tak i při platbě na internetu. Tato možnost zamykání nebo odemykání karty se nastavuje přímo v internetovém bankovnictví. Je také možné mít nastavené automatické zamykání. Tedy pokud si kartu odemknete a poté provedete nějakou finanční operaci, tak se ihned poté karta opět zamkne.
22. **Kontrolovat účet –** důležitým doporučením v oblasti elektronického bankovnictví je provádět kontrolu svého účtu. Tím je myšleno zkontrolovat transakce, které proběhly, pokud je možno ověřit si historii přihlášení na účet apod. Pokud banka klientovi nabízí možnost zasílání informací o pohybech na účtu nebo o přihlášení do internetového bankovnictví, měl by klient mít tuto informační metodu aktivovanou. Informace mohou být zasílány prostřednictvím SMS zpráv nebo elektronickou poštou.
23. **Okamžitá blokace karty při ztrátě nebo odcizení –** zablokováním karty docílíte toho, že nebude možné, aby ji nějaká jiná osoba zneužila. Právě proto je důležité, aby k zablokování karty došlo ihned poté co zjistíte, že kartu nemáte. Důležité je, aby byl každý seznámený s postupem zablokování ihned po obdržení karty. Zablokování je možné jak přes telefon, tak i přímo na pobočce banky. Nejrychlejším způsobem je telefonické zablokování, proto by číslo, na kterém je blokace možná, mělo být u každého držitele karty uloženo v telefonu. Telefonní číslo je sice uvedené přímo na platební kartě, ale to není příliš užitečné, jelikož při ztrátě karty již číslo nezjistíte.
24. **Získávat nové informace –** tady platí stejné pravidlo jako u předchozích doporučení při použití internetu. Každý držitel karty by se měl zajímat, jaké novinky v oblasti zneužití platebních karet jsou používány, a tím snížit bezpečnostní riziko.

7.3 Návrh doporučení bezpečného zacházení pro uživatele internetového bankovnictví

1. **Zvolit důvěryhodného poskytovatele internetového bankovnictví –** pokud má uživatel zájem o zřízení IB, měl by si vybrat ověřenou a seriózní banku.
2. **Zvolit nejvyšší úroveň zabezpečení –** pokud dostanete možnost si zvolit vlastní třídu zabezpečení, volte vždy tu nejvyšší možnou. Bezpečnost internetového bankovnictví není dobré zlehčovat.
3. **Přečtení smlouvy před podepsáním –** je důležité, aby jste byli seznámeni se všemi podmínkami týkajícími se internetového bankovnictví dříve, něž dojde k podpisu smlouvy.
4. **Používat IB podle pravidel a podmínek stanovených bankou**
5. **Pro vstup do IB využívat jen pravé internetové stránky banky –** neklikat na žádné odkazy na banku přes jiné webové stránky nebo přes odkazy v e-mailu.
6. **Důkladně zacházet s písemnostmi týkajícími se IB –** pokud chcete uložit tyto dokumenty, tak by to mělo být na bezpečném místě. Tyto dokumenty většinou obsahují důležité informace, které by mohly potencionálnímu zloději usnadnit zneužití. Proto vybírejte takové místo, kam se nemůže dostat jiná osoba. Pokud máte v úmyslu vyhodit tyto písemnosti, tak je nevyhazujte pouze do odpadků, ale zničte je (spálení, skartování). Tímto je riziko, že se k nim dostane neoprávněná osoba vynulováno.
7. **Pozor na obálky obsahující přihlašovací údaje –** takováto obálka by měla být naprosto neporušená. Pokud si všimnete, že s ní není něco v pořádku, tak zažádejte o nové přihlašovací údaje.
8. **Zapamatovat si údaje nutné pro přihlášení do IB –** o zacházení s přihlašovacími údaji nebo o tvorbě správných hesel už jsme si říkali. Tady platí ta stejná pravidla jako u předchozích bezpečnostních doporučení.
9. **Nechat si údaje nutné pro přihlášení jen pro sebe –** velice důležité bezpečnostní doporučení. U tohoto druhu doporučení by neměla být žádná výjimka, a to ani v případě nejbližší rodiny.
10. **Opatrně zacházet počítačem pro manipulaci s IB –** na zařízení, která využíváte pro tyto účely, instalujte jen takový software, o kterém jste si jistí, že je bezpečný a ověřený. Vyvarujte se takovým programům, které by mohly obsahovat nebezpečí pro IB.

11. **Pro komunikaci s bankou používat jen vlastní počítač.**
12. **Soustředit se při používání IB –** pokud právě používáte internetové bankovnictví, tak věnujte pozornost jenom tomu, nenechte se někým odlákat nebo zabavit. Pokud nemáte pro tuto činnost klid, tak tuto operaci přerušte a pokračujte v ní později.
13. **Být opatrný při přihlašování –** dbejte na to, aby nikdo nepozoroval zadávání přihlašovacích údajů.
14. **Kontrolovat transakce v IB –** pokud chcete provést nějaký příkaz k úhradě, tak buďte pečliví při zadávání potřebných dat a několikrát si je zkontrolujte.
15. **Neodcházet od přihlášeného IB –** pokud jste přihlášeni do svého internetového bankovnictví a potřebujte nutně odejít, tak se vždy nejprve odhlaste. Nikdy neodcházejte od přihlášeného systému.
16. **Dodržovat doporučení pro používání internetu**
17. **Používat limity –** nastavte si výši maximální částky pro manipulaci během jednoho dne a jednoho týdne a to podle toho, jakou částku pravidelně využíváte. Doporučuje se nastavovat co nejnižší možné limity. Pokud budete potřebovat využít vyšší částku, než jakou povoluje určený limit, tak si ho můžete zvýšit a po provedení finanční operace zase snížit. Velikost limitů se nastavuje přímo v internetovém bankovnictví.
18. **Uschovávat si informace o Vámi prováděných finančních operací a prověřovat si je se zůstatkem na účtu**
19. **Nechat si posílat informace ohledně finančních operací prováděných na účtech –** pokud nabydete jakýchkoli pochybností, ihned reagujte a zkontaktujte se se zaměstnancem banky k tomu určeným a tuto událost vyřešte. Nepodceňujte bezpečnost a raději si všechny pochybnosti ověřujte.
20. **Získávat nové informace –** opět platí, že každý kdo využívá internetové bankovnictví, by se měl zajímat o novinky v bezpečnosti a nových hrozbách, aby byl připraven a vyvaroval se riziku.

ZÁVĚR

Elektronické bankovnictví je velice populární metodou pro komunikaci klienta s jeho bankou. Tato forma bankovnictví je spojena s mnoha výhodami jak pro klienta, tak pro samotnou banku, ale také s nevýhodami, především bezpečnostními riziky a poplatky. Při výběru IB je vhodné, aby byl klient s těmito nevýhodami seznámen, a věděl, co za rizika to obnáší.

Tato práce byla zaměřena na elektronické bankovnictví. Byly popsány varianty elektronického bankovnictví, jako jsou platební karty, elektronické peněženky, mobilní mikroplatby a přímé bankovnictví. Seznámili jsme se s nejvýznamnějšími průlomy bezpečnosti v oblasti elektronického bankovnictví a ukázali jsme si nové trendy v oblasti zabezpečení. Dále byly vybrány tři banky z českého bankovního trhu, a to jak ty největší a nejoblíbenější, tak i menší banka. U těchto bank byla zvolena kritéria, která byla v závěru mé práce porovnána. Tato kritéria byla dvě, a to bezpečnost internetového bankovnictví a následně poplatky spojené s využitím internetového bankovnictví, ale také poplatky spojené s využitím platebních karet. V bezpečnostním kritériu obstály všechny banky výborně. Nedalo se říct, že by některá z porovnávaných bank měla nějakou slabinu v tomto ohledu. V druhém kritériu, tedy v ekonomických aspektech už byly rozdíly znatelné. Každá banka nabízí jiné poplatky, a proto byly navrženy dva typy klientů pro lepší srovnání, která banka je výhodnější, a to pravidelný uživatel IB a občasný uživatel IB. Ukázalo se, že nejlépe obstála ČSOB. Banka byla výhodnější jak z pohledu pravidelného uživatele IB, tak i z pohledu občasného uživatele. Druhá část tohoto kritéria, tedy poplatky za využití platební karty, byla také porovnána na dvou typech klientů. Tady byly výsledky rozdílné. Pro pravidelného uživatele se ukázala nejvýhodněji UniCredit Bank, pro občasného uživatele pak Česká spořitelna.

Cílem tohoto porovnání bylo určit banku, která je nejvýhodnější ve všech kritériích. Zjištění z této práce bylo takové, že žádná banka není nejvýhodnější. Klient si musí nejprve určit, jaké služby bude nejvíce využívat, a podle toho pak zvolit banku

V poslední kapitole této práce byl vytvořen návrh doporučení pro uživatele elektronického bankovnictví. A to jak pro uživatele internetového bankovnictví, tak uživatele platebních karet.

Elektronické bankovnictví se neustále rozvíjí a inovuje. To znamená, že získané vyhodnocení z této práce může být časem změněno. Banky pro získání více klientů budou navrhovat lepší služby a také výhodnější což může změnit jejich celou poplatkovou politiku.

SEZNAM POUŽITÉ LITERATURY

[1] Elektronický obchod. *Businessinfo* [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.businessinfo.cz/cs/clanky/elektronicky-obchod-ppbi-51052.html#!

[2] POUR, Jan, Libor GÁLA a Zuzana ŠEDIVÁ. *Podniková informatika*. Praha: Grada Publishing, 2009. ISBN 978-80-247-2615-1.

[3] Infografika: Stav české e-commerce v roce 2013. *M-journal.cz* [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://www.m-journal.cz/cs/aktuality/infografika--stav-ceske-e-commerce-v-roce-2013__s288x10225.html

[4] APEK: Internetové obchody loni utržily rekordních 33 mld. Kč. *Finance.cz* [online]. 2011 [cit. 2015-05-19]. Dostupné z: http://www.finance.cz/zpravy/finance/293445-apek-internetove-obchody-loni-utrzily-rekordnich-33-mld-kc/

[5] STEINOVÁ, Martina, Miluše HLUCHNÍKOVÁ a Michal PŘÁDKA. *E-Marketing II.: marketingová komunikace na internetu, elektronické obchodování*. Ostrava: Technická univerzita Ostrava, 2003. ISBN 80-248-0351-8.

[6] POLOUČEK, Stanislav. *Bankovnictví*. Praha: C. H. Beck, 2006. ISBN 8071794627.

[7] PEKÁRKOVÁ, Lucie. *ELEKTRONICKÉ BANKOVNICTVÍ, JEHO MOŽNOSTI A DALŠÍ VÝVOJ*. Brno, 2006. Bakalářská práce.

[8] PŘÁDKA, M., KALA, J.: Elektronické bankovnictví : Rady a tipy. 1. vyd. Praha : Computer Press, 2000. ISBN 80-7226-328-5.

[9] OŠKRDALOVÁ, Gabriela. *Modelování bezpečnostních rizik elektronického obchodu a elektronického bankovnictví*. Brno, 2012. Disertační práce. MASARYKOVA UNIVERZITA.

[10] Debetní karty. *MasterCard* [online]. 2011 [cit. 2015-05-19]. Dostupné z: http://www.mastercard.com/cz/osobni-karty/debetni-karty.html.

[11] Embosovaná karta. *Komerční banka* [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://www.kb.cz/cs/lide/obcane/embosovana-karta-mastercard-visa.shtml.

[12] MÁČE, Miroslav. *Platební styk klasický a elektronický*. Praha: Grada, 2006. ISBN 9788024717258.

[13] Bankomaty v ČR. *Kurzy.cz* [online]. 2015 [cit. 2015-05-20]. Dostupné z: http://www.kurzy.cz/banky/bankomaty/.

[14] Za výběr na pobočce zaplatíte až několik set korun. Přesto se stále využívá. *Finance.idnes.cz* [online]. 2009 [cit. 2015-05-20]. Dostupné z: http://finance.idnes.cz/za-vyber-na-pobocce-zaplatite-az-nekolik-set-korun-presto-se-stale-vyuziva-1uf-/karty.aspx?c=A091207_115555_bank_fib.

[15] Vyberte si peníze u pokladny v obchodě. Máte to zadarmo. *Http://finance.idnes.cz/* [online]. 2010 [cit. 2015-05-20]. Dostupné z:

http://finance.idnes.cz/vyberte-si-penize-u-pokladny-v-obchode-mate-to-zadarmo-pft-/karty.aspx?c=A100827_141102_bank_bab

[16] Smartphone banking už má pevnou pozici. Co bude dál? *Finance.cz* [online]. 2012 [cit. 2015-05-20]. Dostupné z: http://www.finance.cz/zpravy/finance/366359-smartphone-banking-uz-ma-pevnou-pozici-co-bude-dal/

[17] Nový trend v placení na internetu: elektronická peněženka. *Finparada.cz* [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://www.finparada.cz/2473-Novy-trend-placeni-na-internetu-elektronicka-penezenka.aspx

[18] Akční plán ke Strategii pro oblast kybernetické bezpečnosti v České republice na období 2011 - 2015. *CENTRUM KYBERNETICKÉ OCHRANY ČR* [online]. 2012 [cit. 2015-05-20]. Dostupné z: http://www.govcert.cz/docDetail.aspx?docid=21667313&docType=ART

[19] Biometrie a bankovnictví. *Patria.cz* [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://www.patria.cz/zpravodajstvi/2657000/biometrie-a-bankovnictvi-skryva-se-budoucnost-ochrany-v-unikatnosti-lidskeho-hlasu.html

[20] Výroční zpráva 2014. *Csas.cz* [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://www.csas.cz/static_internet/cs/Obecne_informace/FSCS/CS/Prilohy/vz_2014.pdf

[21] Profil České spořitelny. *Csas.cz* [online]. 2013 [cit. 2015-05-20]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/profil-ceske-sporitelny-d00014413

[22] O společnosti ČSOB. *Csob.cz* [online]. 2015 [cit. 2015-05-20]. Dostupné z: http://www.csob.cz/cz/Csob/O-CSOB/Profil-CSOB/Stranky/default.aspx

[23] VÝROČNÍ ZPRÁVA 2014. *Csob.cz* [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://www.csob.cz/WebCsob/Csob/O-CSOB/Vztahy-k-investorum/Vyrocni-pololetni-zpravy/Vyrocni-zpravy/VZ_CSOB_2014.pdf

[24] UniCredit Bank Czech Republic and Slovakia, a.s. *Unicreditbank* [online]. 2014 [cit. 2015-05-20]. Dostupné z: https://www.unicreditbank.cz/web/o-bance

[25] Výroční zpráva a účetní závěrka za rok 2014. *Unicreditbank* [online]. 2014 [cit. 2015-05-20]. Dostupné z: https://www.unicreditbank.cz/files/download/vyrocni-zpravy/VZ_UCB_2014_CZ.pdf

[26] Útoky na platební systémy. *Ics.muni.cz/* [online]. 2007 [cit. 2015-05-24]. Dostupné z: http://ics.muni.cz/bulletin/articles/562.html

[27] Jak se bránit podvodům. *Bezpečně-online.cz* [online]. 2012 [cit. 2015-05-24]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/nakupovani-na-internetu/jak-sebranit-podvodum/

[28] SKIMMING. *Policie ČR* [online]. 2010 [cit. 2015-05-24]. Dostupné z: http://www.policie.cz/clanek/skimming.aspx

[29] PHISHING. *HOAX* [online]. [cit. 2015-05-24]. Dostupné z: http://www.hoax.cz/phishing/

[30] Servis 24 Internetbanking. *Česká spořitelna, a.s.* [online]. 2015 [cit. 2015-05-24]. Dostupné z: https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login?execution=e1s1

[31] Ceník pro SERVIS 24 pro soukromou klientelu. *Csas.cz* [online]. 2014 [cit. 2015-05-24]. Dostupné z: http://www.csas.cz/banka/nav/osobni-finance/servis-24---internetbanking/cenik-d00019496

[32] ČSOB InternetBanking 24. *Československá obchodní banka, a.s.* [online]. 2015 [cit. 2015-05-24]. Dostupné z: https://ib24.csob.cz/

[33] Sazebník pro fyzické osoby – občany. *Csob.cz* [online]. 2014 [cit. 2015-05-24]. Dostupné z: http://www.csob.cz/cz/csob/Sazebniky/Stranky/Sazebnik-pro-fyzicke-osoby-obcany.aspx#elb

[34] My UniCredit Banking. *UniCredit Bank* [online]. 2015 [cit. 2015-05-24]. Dostupné z: https://cz.unicreditbanking.net/disp?

[35] Sazebník. *UniCredit Bank Czech republic and Slovakia, a.s.* [online]. 2014 [cit. 2015-05-24]. Dostupné z: https://www.unicreditbank.cz/web/sazebnik

[36] Phishing. *Csas.cz* [online]. 2015 [cit. 2015-05-24]. Dostupné z: http://www.csas.cz/banka/appmanager/portal/banka?_nfpb=true&_pageLabel=phishing&docid=internet/cs/phishing_ie.xml

[37] Čerstvý phishing na Servis24 s kopií webu Spořitelny na brazilské doméně. *Pooh.cz* [online]. 2015 [cit. 2015-05-24]. Dostupné z: http://www.pooh.cz/pooh/tag.asp?tag=%C8esk%E1+spo%F8itelna

[38] Bezpe čnost internetového bankovnictví. *Csob.cz* [online]. [cit. 2015-05-24]. Dostupné z: http://www.csob.cz/webcsob/csob/servis-pro-media/pb_csob_elb_seminar_bezpecnost.pdf

[39] Aktuality. *Csas.cz* [online]. 2008 [cit. 2015-05-24]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_398.xml

[40] GE Money. *GE Money Bank, a.s.* [online]. 2015 [cit. 2015-05-24]. Dostupné z: https://www.gemoney.cz/lide

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APEK	Asociace pro elektronickou komerci
IPB	Investiční a poštovní banka
ČSOB	Československá obchodní banka, a.s.
Mobito	Přehled o elektronických peněženkách
PIN	Bezpečnostní číselný kód
DNA	Genetická informace
IB	Internetové bankovnictví
Antivir	Antivirový program
WPA	Wi-Fi Protected Access – chráněný přístup k Wi-Fi
CVV	Verifikační hodnota karty
CVC	Verifikační kód karty
E-banking	Elektronické bankovnictví
E-shop	Elektronický obchod

SEZNAM OBRÁZKŮ

SEZNAM TABULEK