Masarykova univerzita

Ekonomicko-správní fakulta

Studijní obor: Finanční podnikání

Elektronické bankovnictví

Autor: Eva Hřebíčková
Rok a místo zpracování: Brno, 2007

1. Elektronické bankovnictví

Elektronické bankovnictví v podobě, kterou známe dnes, vzniklo v druhé polovině 90. let. Reagovalo tak na rozvoj informačních technologií, jež se postupně stávají nedílnou součástí života občanů i firem. Elektronické bankovnictví (e-banking, přímé bankovnictví, direct banking) využívá výhod moderních technologií a dovoluje komunikovat klientovi banky elektronickou formou bez nutnosti navštěvovat její fyzickou pobočku. Klient může svůj bankovní účet ovládat 365 dní v roce, 24 hodin denně. E-banking je efektivní a úsporný nástroj na obsluhu existujících klientů finančních institucí. Cílem e-bankingu je zajištění flexibilního, otevřeného a samoobslužného kanálu, kterým klient může naplňovat své každodenní potřeby spojené s jeho účtem, ať už se jedná o bankovní služby či o informace. Snadné ovládání účtu a neustálý přehled o jeho stavu jsou hlavní výhody e-bankingu pro klienty.

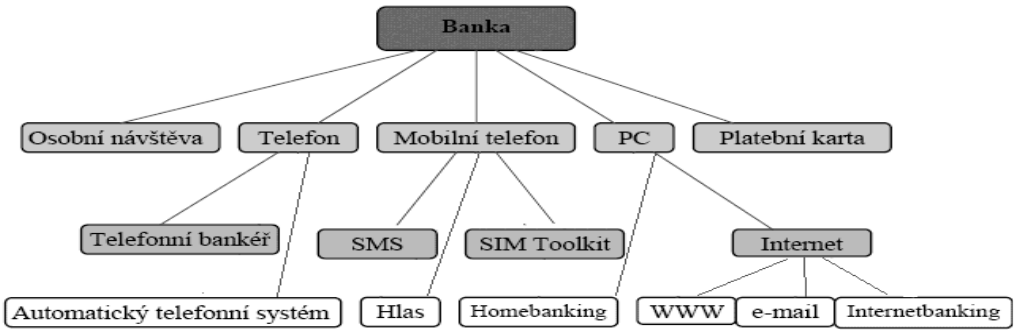
Banky k zavádění systémů elektronického bankovnictví vede hlavně zatraktivnění služeb a možná úspora nákladů. Banky se snaží přetáhnou klienty společností, které nedostatečně reflektují na nové možnosti a nenabízejí svým klientům takovéto služby. Pro určitou část klientely (zejména pro finančně dobře zajištěné zákazníky) je rychlost služeb a úspora času významným faktorem při rozhodování. Hlavním důvodem je ale snižování nákladů spojených s velkým počtem poboček a zaměstnanců v nich. Jde však o dlouhodobý proces v horizontu spíše let než měsíců.

Základními charakteristickými rysy služeb patřících do oblasti elektronického bankovnictví jsou:

- služby jsou poskytovány prostřednictvím elektronického kanálu,
- na jedné straně je klient s určitým technickým vybavením a na druhé straně je automatický systém banky nebo pracovník obsluhující tento systém,
- klient je jednoznačně identifikovatelný a jeho právo vykonat požadovanou operaci je ověřeno autorizačním mechanismem,
- nejčastěji používanými operacemi jsou tuzemský platební příkaz a zjištění stavu peněz na účtu.

Banky mohou elektronicky komunikovat s klientem prostřednictvím různých technologických prostředků. Následující tabulka ukazuje možnosti komunikace klienta s bankou. Klient může využívat všech kanálů elektronické komunikace, zpravidla však volí pouze určitou kombinaci, která je pro něj nejpohodlnější.

Možnosti komunikace s bankou



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

1.1. Phonebanking (telebanking, telefonní bankovnictví)

Telefonní bankovnictví, jak už název napovídá, umožňuje přístup do banky prostřednictvím telefonního přístroje. Nezáleží na tom, zda pevného či mobilního, důležitým ukazatelem jsou použité hlasové služby. Pod phonebanking spadají dva typy komunikace. Prvním je hovor s telefonním bankéřem (skutečnou osobu) a druhý je komunikace s hlasovým automatem. Banka po telefonu může mít několik úrovní. Pasivní varianta je spojena pouze se zjišťováním zůstatků na účtu, s poskytováním informací o pohybu na účtech, o produktech a službách banky, o aktuálních úrokových sazbách a o devizových kurzech bank. Aktivní verze umožňuje navíc zadávání příkazů k úhradě i k inkasu, měnové konverze, zakládání spořících či termínových vkladů, atd. Většina bank na českém trhu poskytuje alespoň nějaký typ phonebankingu.

Telefonní bankéř

Komunikace s telefonním bankéřem prostřednictvím tzv. call centra umožňuje současným nebo i potenciálním klientům získat odpovědi na otázky, které jsou spojeny s jejich účtem v bance. Klient se může bankéře zeptat na cokoliv, a ten by měl být schopen podat kvalifikovanou odpověď. Právě fakt, že klient komunikuje s živým operátorem, je největší výhodou systému. Vždyť bankéř je schopen zodpovědět všechny otázky a klient si může nechat dopodrobna vše vysvětlit. Většinou je volání na taková centra bezplatné, takže klient se může v klidu zeptat na cokoliv beze strachu z telefonních poplatků. Nevýhodou může být, že některé banky neposkytují 24 hodinový servis a informace jsou klientům podávány jen v pracovní dobu.

Obdobou call centra je i e-mailové centrum, kam zákazníci mohou posílat své dotazy. Ty samozřejmě fungují non-stop, ale obsluha vyřizuje odpovědi postupně. Proto je doba odpovědi různá, někdy trvá několik hodin, jindy pár dnů, ale může se stát, že odpověď nepřijde vůbec. Navíc při komunikaci s centrem je někdy třeba poslat několik dotazů, než se tazatel dostane k jádru věci, což pochopitelně stojí zbytečně spoustu času.

Hlasový automat

Automatizovaný telefonním systému funguje na principu tónové volby a hlasových příkazů. Po vytočení čísla služby je zákazník navigován pomocí hlasového menu až ke službě, kterou si přeje uskutečnit. Výhodou je 24 hodinový přístup, 7 dní v týdnu. Některé banky dovolují pouze provádět pasivní operace (tedy zjišťovat pohyby na účtech a zůstatky), jiné poskytují i operace aktivní, klient může zadávat jednoduché bankovní příkazy apod. Nevýhodu těchto systémů lze spatřovat v nízké uživatelské přívětivosti (nejsou user friendly).

Výhody a nevýhody
+ k dispozici prakticky kdekoliv
+ telefonní automat k dispozici 24 h denně, 7 dní v týdnu
- telefonní operátor k dispozici pouze v pracovní době
- operace zaznamenávány – riziko odposlechu
- nízká uživatelská přívětivost u automatu
- zvyšují se ceny za komunikaci s telefonním bankéřem
- jednotlivé služby nabízejí různé typy transakcí, ne vždy ale všechny (omezené menu u automatických služeb)

Bezpečnost
Telefonní bankovnictví lze používat z kteréhokoli telefonního přístroje. Autentifikace (ověření, zda se jedná o osobu, za kterou se telefonující vydává) klienta se liší podle toho, zda ji provádí hlasový automat (zpravidla se udává uživatelské jméno a heslo, obě číselně), nebo osobní bankéř (vedle uživatelského jména chce jen několik číslic z hesla a přeptá se na pár osobních údajů, které porovná s informacemi v bankovním systému). Osobní bankéř může, dokonce musí, v případě pochybností o vaší totožnosti odmítnout vykonání vámi požadovaného příkazu. Jste-li to opravdu vy, kdo volá, nezbývá než zkusit zavolat znovu.

Hovor je při využívání telefonního bankovnictví nahráván bankou (což je v pořádku), ale může být odposlechnut i další osobou. Pravděpodobnost, že k tomu dojde, je poměrně malá. Hůře se odposlouchávají hovory z mobilních telefonů než z pevné linky.

1.2. GSM banking

S rozvojem mobilních technologií a rozšířením mobilních přístrojů mezi obyvatelstvo se začal prosazovat GSM banking, jako služba přinášející klientům přístup do banky odkudkoliv a kdekoliv. Také u této služby existují dva druhy. První je SIM Toolkit a druhou je SMS Banking.

SIM Toolkit

Zde banka do vašeho mobilního telefonu (na SIM kartu) nahraje vlastní bankovní aplikaci, která se objeví v menu vašeho telefonu. Při nahrávání aplikace je SIM karta zašifrovaná a nelze z ní získat žádné údaje, ani když vám ukradnou telefon. Současně je přístup k této aplikaci chráněn zvláštním bankovním PIN, které se nazývá BPIN. Potom vám tedy stačí nalistovat v menu aplikace správnou položku a vybrat některou ze základních služeb (např. zjišťování zůstatku na účtu, přehled historie pohybů na účtu, přehled kursů, zadávání příkazů). Na konec obdržíte informaci o vámi vybrané službě, a to buď formou textové zprávy na mobilní telefon, nebo formou e-mailu do e-mailové schránky, která je předem definovaná.

SMS banking

Dalším druhem služby je SMS banking, jehož výhodou je použitelnost u všech mobilních telefonů, bez ohledu na operátora. Komunikace probíhá pouze prostřednictvím SMS zpráv. Na první pohled to nevypadá příliš bezpečně, ale banka i k této aplikaci může vydávat tzv. autentizační kalkulátor, s jehož pomocí si vygenerujete speciální kód, který vložíte do struktury SMS zprávy. Nevýhodou je složitější manipulace, protože SMS zprávy musíte posílat přesně ve formátu daném bankou. Např. U částka účet_debet účet_kredit splatnost [Vvar_symbol] [Kkonst_symbol] [Sspec_symbol] [MAC]. Zadávání tedy vyžaduje velkou pozornost, abyste se nepřepsali.

Na pomezí internetového a GSM bankovnictví je ještě tzv. PDA bankovnictví, tedy přístup k účtu z kapesního počítače připojeného na internet (většinou pomocí mobilního telefonu). Tento způsob je ve srovnání s GSM banking přehlednější (díky větší zobrazovací ploše).

Výhody a nevýhody
+ k dispozici prakticky kdekoliv
- nelze u všech bank zřídit s libovolným operátorem
- jednotlivé služby nabízejí různé typy transakcí, ne vždy ale všechny (omezené menu)
- problémem může být i mobilní telefon (starší modely jsou nevyhovující)
- za SMS zprávy se operátorovi platí
- složitá manipulace u SMS bankingu (speciální formát)

Bezpečnost
Komunikace mezi bankou a zákazníkem probíhá prostřednictvím kódovaných a šifrovaných SMS zpráv. Každá bankovní SIM karta má svůj šifrovací klíč, prostřednictvím kterého se provádí zabezpečení komunikace s bankou. Tento klíč je uložen v chráněné oblasti SIM karty a je dostupný pouze po zadání správného kódu BPIN. Odeslaná zpráva z mobilního telefonu je přijata bankou pouze tehdy, pokud je zašifrována správným šifrovacím klíčem.

1.3. W@P banking

W@P banking je velice zajímavá, protože je s tímto systémem možné poměrně pohodlně a hlavně odkudkoliv a kdykoliv ovládat účet. Rozšiřuje tak možnosti Internetbankingu, který je vázán na počítač připojený k síti. Systém se podobá internetovému rozhraní, avšak využívá mobilní telefony se systémem W@P (Wireless Application Protocol). Jeho možnosti jsou omezeny nevelkým množstvím informací, které jsou telefony schopny zobrazit, a také omezenou rychlostí přenosu dat. Rozšíření W@P bankingu proto není na takové úrovni, která by se od takového systému dala očekávat. W@P banking je spíše považován za dočasné řešení před přechodem na třetí generaci mobilních telefonů. Ve spojení s bankou byla u nás tato technologie poprvé představena v roce 2000 eBankou (dříve Expandia bankou).

Výhody a nevýhody

+ stejné možnosti jako Telebanking a GSM banking

+ WAP je součástí většiny v současnosti používaných mobilních telefonů

- nízká rychlost připojení k internetu

Bezpečnost

WAP banking je chráněn autorizačním klíčem anebo v současnosti i elektronickým podpisem, který je založen na obdobném principu jako zaručený elektronický podpis.

1.4. Homebanking

Homebanking (někdy také nazývané PC banking) je rozhraní, umožňující ovládání účtu pomocí počítače. To je velmi pohodlné pro majitele účtu, jenž může provádět prakticky všechny operace ze svého PC. Tato forma práce s účtem je nejen pohodlná, ale také se vyznačuje vysokou bezpečností. Služba je zabezpečena jednak heslem, a také autorizačním certifikátem, který je nainstalován v počítači klienta. Tento certifikát je speciální software dodávaný bankou, bez něhož nelze spojení navázat. Přenos mezi počítačem a bankou je navíc většinou kódovaný. Spojení po té probíhá přes modem či internet. Protože služba vykazuje vysoký stupeň spolehlivosti a bezpečnosti, nabízí klientům poměrně širokou paletu služeb. Kromě možnosti zadávat příkazy a provádět další operace s účtem obvykle nabízí přístup do databáze banky a vyhledávání služeb, číselníků bank, kurzovních lístků a úrokových sazeb. Navíc je možné aplikaci propojit ekonomickým a účetním systémem firmy, což umožňuje automatické předávání platebních příkazů a výpisů z účtu.

Hlavní nevýhodou je nutnost jednat pouze prostřednictvím jednoho počítače, na kterém je nainstalován příslušný software. To omezuje koncové zákazníky a systém tak ztrácí na popularitě. Poplatky za možnost použití homebankingu také patří k těm vyšším. Tato služba je učena spíše pro podnikatele a firmy, nepodnikajícím fyzickým osobám bude vyhovovat více internet banking.

Výhody a nevýhody

+ vhodné pro klienty, kteří musí zpracovávat větší objem plateb a potřebují neustálý přehled o stavu účtu
+ nejvyšší stupeň zabezpečení ze všech forem elektronického bankovnictví
+ program banky lze napojit na vlastní účetní systém, čímž se umžní automatické předávání platebních příkazů a výpisů z účtu
- vázán na určitý počítač daných parametrů
- vysoké náklady

Bezpečnost

V případě homebankingu je úroveň zabezpečení značně vysoká – jednak se volá na speciální číslo (data tedy nejdou přes internet), jednak data jsou digitálně podepisována a šifrována (konkrétní způsob se u jednotlivých bank liší) a přihlášení do sítě banky probíhá pomocí hesel uživatele a autorizačního certifikátu. Po několika neautorizovaných pokusech o spojení s bankou by pak došlo k zablokování klienta.

1.5. Internetbanking

Nejnovějším přírůstkem mezi systémy elektronického bankovnictví je možnost ovládat účet přes Internet pouze s použitím internetového prohlížeče. Internet banking je rozhraní, velice podobné homebankingu, ale odbourávající jeho hlavní nevýhodu. Není totiž vázáno na konkrétní počítač. Komunikace s finanční institucí je možná prostřednictvím jakéhokoli

počítače, který je napojen na Internet. Klient používá uživatelské jméno a heslo. Toto rozhraní je velice běžné a je pro klienta pohodlné, neboť může komunikovat a obchodovat odkudkoli. Tím, že klient získal možnost připojit se k bance z kteréhokoliv počítače připojeného k Internetu, ztratil možnost propojit tento systém se svým účetním systémem.

U některých bank můžete za poplatek dostat tzv. autentizační lokátor, se kterým si přístupový kód vygenerujete před každým přihlášením, můžete se setkat i s identifikací klienta pomocí kódů uložených na čipové kartě. Poslední možností pak je uložení bezpečnostního certifikátu přímo v počítači, ze kterého se připojujete (věnuji se podrobněji v oddílu bezpečnost).

U některých aplikací je velice obtížné určit, zda patří ještě do skupiny internetbanking nebo homebanking. Některé banky totiž umožňují klientům přistupovat k účtu prostřednictvím Internetu, ale ti musejí mít na svém počítači nainstalovaný speciální software. Zmíněné aplikace připomínají vzhledem a funkcemi spíše homebanking, na druhou stranu data putují přes Internet, takže by bylo logické zařadit je k internetbankingu. Hranice mezi těmito službami ještě není přesně definována. Zařazení služby není pro uživatele tak důležité, internet banking se postupně rozšiřuje mezi klienty bank a stává se velmi oblíbeným.

Výhody a nevýhody
+ spojení s bankou je možné z kteréhokoli počítače připojeného k síti internet
+ není nutná instalace speciálních programů
+ obsluha relativně snadná
+ neomezený přístup 24 hod denně, 7 dní v týdnu
- bezpečnost
- nelze propojit s účetním systémem firmy

Bezpečnost
Internet patří k velice snadno zneužitelným a napadnutelným kanálům. Přesto se dá říci, že internetové bankovnictví je bezpečné a míra zabezpečení se samozřejmě odvíjí jak od využívání určitých bezpečnostních standardů, tak od potřeb kladených na bezpečnost transakce. Jiné požadavky na bezpečnost bude mít privátní klient realizující prostřednictvím internetu převody malých sum, jiné mezinárodní firma.

Bezpečnost internetového bankovnictví zahrnuje tři aspekty - identifikaci banky, identifikaci klienta a zabezpečení přenosu dat. Identita banky je ověřována certifikátem, který vydává nezávislá instituce (nejčastěji VeriSign nebo I.CA). Klient tak má jistotu, že stránky, jejichž prostřednictvím komunikuje s bankou, patří skutečně jí. Přenos dat je ve všech bankách řešen šifrováním na vysoké úrovni a lze jej považovat za dostatečně bezpečný.

Poslední část zabezpečení - identifikace klienta banky - je nejvíce viditelná a rozhoduje i o uživatelském pohodlí aplikace. Nejčastěji se využívá zabezpečení uživatelským jménem a heslem nebo certifikátem uloženým v souboru. Pokud má banka bezpečnější varianty přístupu (např. autentizační kalkulátor), jsou často brány jako nadstandardní a banka si za ně nechává platit. A klienti je nepoužívají: podle bank klienti preferují větší jednoduchost služby, a to i za cenu nižší bezpečnosti. Obecně platí, že čím vyšší je bezpečnost, tím menší je komfort pro klienta.

<u>Základní úrovně ochrany</u>

V ČR neexistuje produkt internetového bankovnictví, který by byl zcela nezabezpečený. Banky dávají klientovi na výběr, jaké riziko je ochoten přijmout a kterou metodu si zvolí. Zájem o technické prostředky zajišťující nadstandardní bezpečnost není mezi klienty příliš

velký, a to zřejmě kvůli poplatkům: např. u ČS vydání čipové karty se čtečkou stojí 670 korun, vygenerování klientského certifikátu na rok 320 korun.

Existuje několik úrovní ochrany, které budou popsány v dalším textu.

Uživatelské jméno (číslo) + heslo

Tento způsob přihlašování je nejjednodušší, ale nejméně bezpečný, nepomůže ani dostatečně dlouhé heslo. Dle průzkumu tuto metodu využívá téměř 80 procent uživatelů internetového bankovnictví v ČR.

Nevýhodou této varianty je, že případnému útočníkovi stačí znát pouze jméno a heslo, aby se dostal k účtu. Napadne-li počítač škodlivý kód schopný sledovat stisknuté klávesy (keylogger), oba tyto údaje snadno získá a může je odeslat podvodníkovi. Pokud není nutné následnou platbu autorizovat, představuje to velké riziko. Některé banky zvyšují bezpečnost tím, že pro zadání hesla je možné použít grafickou klávesnici, která je ovládaná myší. I tento způsob ale dokáže trojský kůň monitorovat.

Pokud klient zvolí tento základní způsob přihlášení, měl by se aktivně zajímat o doplňující bezpečnost, jako je např. nastavení denního limitu, automatické zasílání informačních SMS po každém zadání aktivní transakce či při změně zůstatku, možnost poskytování informací o provedených finančních transakcích (prostřednictvím e-mailu, SMS nebo faxu).

Autorizace SMS klíčem

K potvrzení každé jednotlivé transakce banka zašle unikátní kód v podobě textové zprávy na předem zaregistrované mobilní číslo. U eBanky, ČSOB, KB, ČS (od října 2006) je SMS klíč nutný pro všechny transakce bez ohledu na jejich výši. Výhodou je, že pokud dojde k útoku hackera, bez mobilního telefonu klienta nemůže provést žádnou transakci.

U KB se ale jedná o statický SMS kód, který platí po celou dobu přihlášení uživatele do internetbankingu. Autorizační SMS kód bude uživatel zadávat pouze při první aktivní operaci v rámci jednoho přihlášení; to znamená, že pokud bude klient zadávat více příkazů k úhradě za sebou, stačí mu zadat autorizační SMS kód jen při první autorizaci platby. Je zde určité riziko, že SMS kód může být odposlechnut.

ČSOB svým klientům nabízí možnost zvolit si SMS klíč také pro přihlášení do aplikace internetbanking.

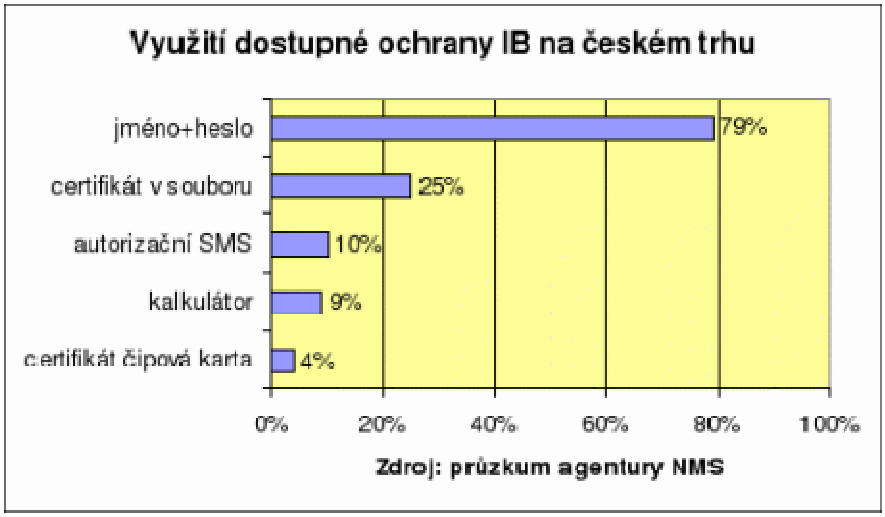
Elektronický podpis

Pro přihlašování a podepisování transakcí potřebuje klient elektronický podpis - osobní certifikát klienta uložený v souboru nebo na čipové kartě. Tento způsob klade vyšší požadavky na bezpečné uložení a používání certifikátu. Základním pravidlem je neukládat certifikát na disk. Vždy by měl být nahraný na nějakém externím médiu (disketa, CD, USB disk), které bude připojeno jen při přistupování k účtu – po ukončení práce je nutno médium z počítače vždy vyjmout.

Vyšší bezpečnost poskytuje klientský certifikát uložený na čipové kartě. V tomto případě je nutné si pořídit čtečku čipových karet. Výhodou je nemožnost odcizení soukromého klíče bez fyzického odcizení čipové karty (klíč nelze z karty vyexportovat). Platí opět zásada, že karta se po použití vyjme ze čtečky a bezpečně uloží.

Elektronický kalkulátor

Mezi bezpečné systémy patří kalkulátory, které generují pokaždé jiný originální přístupový kód pro potvrzení transakcí. Klienti si nemusí nic instalovat do počítače, ale musí si koupit zařízení např. v podobě malé kalkulačky. Kalkulačka je přenosná a je chráněna čtyřmístným heslem. Po zadání hesla a stisknutí příslušného tlačítka vygeneruje šestimístný kód, který klient aplikuje pro vstup do internetbankingu. Pro každou aktivní transakci musí být vygenerováno nové číslo.



Autorizace klienta při vstupu na účet

Banka	Jméno+heslo	Cerifikát	Čip. karta	SMS kód	Kalkulátor
Citibank	ano				ano
Česká spořitelna	ano	ano	ano	ano	ano
ČSOB	ano	ano	ano	ano	
E-banka		ano		ano	ano
GE Money Bank	ano	ano		ano	
HVB Bank					ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano	ano	ano	ano	
Raiffeisenbank	ano	ano		ano	
Volksbank	ano	ano			
Živnostenská banka	ano	ano	ano	ano	

Zdroj: autor

Výsledky testu internetového bankovnictví v roce 2006

Kritériem hodnocení byly cena, funkce, uživatelská přívětivost a standardní zabezpečení, přičemž všechny faktory měly stejnou váhu.

2005

Pořadí	Banka
1.	eBanka
2.	Raiffeisenbank
3.	ČSOB
4.	Česká spořitelna
5.	Živnostenská banka
6.	BAWAG Bank CZ
7.	Komerční banka
8.	GE Money Bank
9.	HVB Bank
10.	Volksbank CZ
11.	WSPK
12.	Citibank

2006

Pořadí	Banka
1.	eBanka
2.	Raiffeisenbank
3.	Komerční banka
4.	Živnostenská banka
5.	Česká spořitelna
6.	Volksbank CZ
7.	Poštovní spořitelna
8.	ČSOB
9.	GE Money Bank
10.	BAWAG Bank CZ
11.	WSPK
12.	HVB Bank
13.	Citibank
14.	Oberbank AG

2. Situace v České republice

Rok 2006 přinesl do povědomí české veřejnosti to, že zabezpečení internetových finančních stránek na obou stranách vztahu banka-klient není nikdy dost a je stále co zlepšovat. Tentokrát se technologií znalí pachatelé pokusili vykrást účty některých klientů v Komerční bance a České spořitelně, zřejmě našli slabé místo "na klientském konci" tohoto přímého kanálu. Banky reagovaly promptně zvýšením autentizační ochrany přístupu k účtům. Podobný proces probíhá i v mnoha vyspělých zemích na západ od našich hranic - právě i tam se v posledních několika letech aktivizovali i-bankovní piráti.

Mezi množstvím spamových zpráv, které se pokoušejí o tzv. phishing (krádež identity s cílem zneužít ji například při pokusu o přístup na účet přes internetové bankovnictví), se v posledních letech objevovaly po celém světě miliony rozesílaných e-mailů stejného znění - pachatelé-odesilatelé se tvářili třeba jako Citigroup nebo Raiffeisenbank a žádali o jakési potvrzení správnosti osobních údajů. Tyto phishingové e-maily jistě dobře znají i mnozí čeští uživatelé internetu. Daleko nebezpečnější jsou však způsoby získávání informací, o nichž klient ani nemusí vědět - v podobě programu či obrázku si stáhne trojského koně, který loví z jeho počítače údaje a posílá je neznámo kam.

Na pořadu dne tak je v České republice zvyšování úrovně bezpečnosti autentizace a nabádání klientů k dostatečné ochraně počítače proti maligním prográmkům ze sítě.

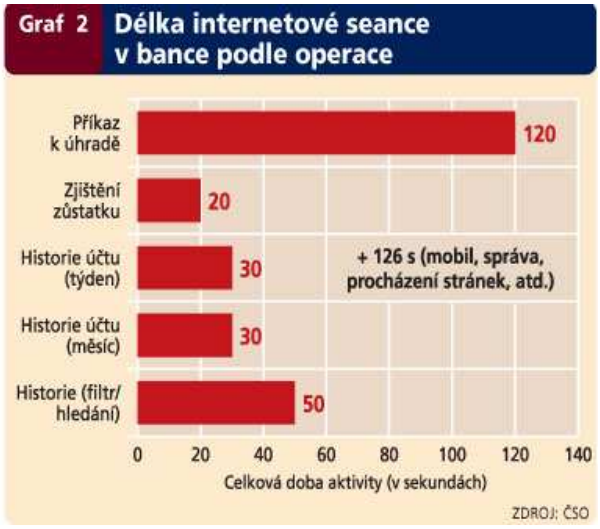
Přesto internetové bankovnictví v ČR předbíhá ostatní kanály pro přístup do bank. Internet se teprve loni stal nejužívanějším kanálem přímého bankovnictví. Ještě předloni a o rok dříve vévodilo přímým kanálům telefonické ovládání účtu a ještě o rok dříve vedl dokonce mobilní telefon (GSM banking). Dnes vede internet (prudký nárůst za poslední tři roky) před telefonem (po nárůstu poslední dva roky stagnace až mírný ústup) a GSM bankingem (o něco větší ústup).

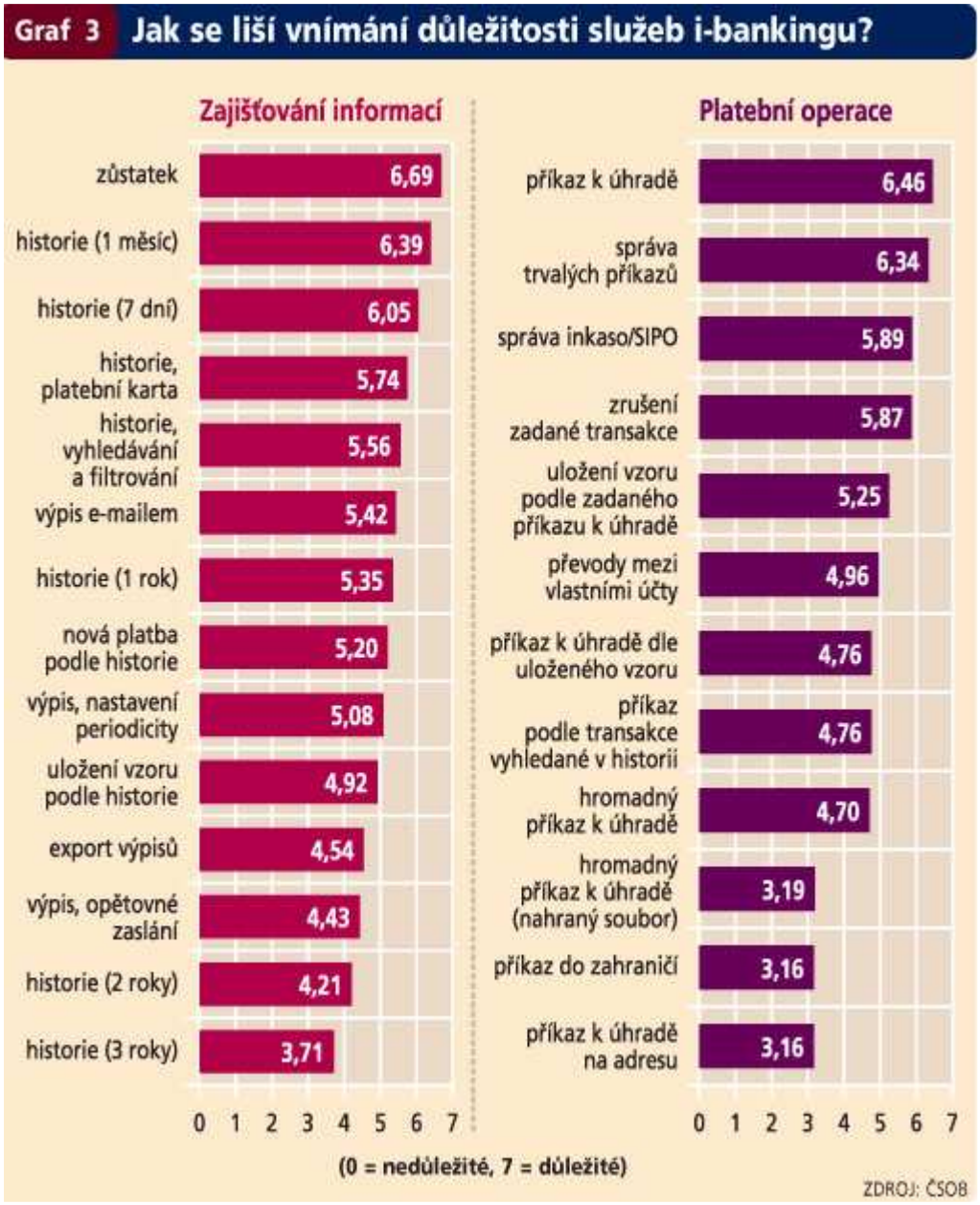
Jednou měsíčně nebo častěji chodí na pobočky vyřizovat své finanční záležitosti stále ještě

zhruba polovina českých bankovních klientů. Tato část se jen velmi nepatrně snížila mezi lety 2004 a 2006. Pětina klientů hlásí návštěvy na pobočkách vícekrát měsíčně. Zatímco v roce 2004 jich bylo těsně přes 20 %, v roce 2006 je to těsně pod 20 %.

Procento klientů, kteří chodí do banky přes internet více než jednou měsíčně, sice rok od roku pomalu narůstá, avšak teprve letos těsně překročí hranici 10 % všech klientů.

Velmi zajímavým zjištěním je také skutečnost, že používání jednoho kanálu přímého bankovnictví vede klienty k tomu, aby se zajímali o další kanály přímého bankovnictví – 23 % respondentů výzkumu se vyjádřilo, že jsou rozhodnuti pořídit si další typ přímého bankovnictví. Přitom nejčastější takový posun vede směrem od neinternetových forem k té internetové - to znamená od bankovního účtu ovládaného přes GSM nebo telefon k ovládání účtu přes internet.





3. Legislativní úprava přímého bankovnictví

Legislativní úprava přímého bankovnictví v České republice není komplexní. Existuje pouze několik právních předpisů upravujících dílčí oblasti. V následujícím textu se na jednotlivé předpisy zaměřím.

Zákon o elektronickém podpisu

Do českého práva byla implementována směrnice Evropského parlamentu a Rady č. 1999/93/ES o zásadách Společenství pro elektronické podpisy (dále jen *"směrnice o elektronickém podpisu"*) zákonem č. 227/2000 Sb., o elektronickém (dále jen *"zákon o elektronickém podpisu"*). Výše uvedená směrnice doplňuje směrnici Evropského parlamentu a Rady č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, která se promítla do českého práva § 40 OZ (z. č. 40/1964 Sb.).

Zákon o elektronickém podpisu vychází z existence dvou typů podpisů: elektronického podpisu a zaručeného elektronického podpisu. Elektronickým podpisem lze rozumět údaje v elektronické podobě, které jsou připojené k datové zprávě, například i naskenovaný podpis. Zaručený elektronický podpis vyžaduje existenci certifikátu, tzn. datové zprávy, kterou vydává poskytovatel certifikačních služeb, a která spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu.

Opatření ČNB č. 2 ze dne 3. února 2004

Zabezpečení vlastního informačního systému banky reguluje Česká národní banka v opatření č. 2 ze dne 3. února 2004 (dále jen "opatření"), ve kterém stanovila požadavky na vnitřní řídicí a kontrolní systém banky, včetně požadavků na interní audit a řízení rizik.

V příloze č. 4 opatření definuje požadavky na informační systémy, které se týkají řízení informačních systémů, analýzy rizik spjatých s informačními systémy, bezpečnost přístupu k informacím a bezpečnost komunikačních sítí (banky a vnější komunikační sítě), fyzické bezpečnosti informačních systémů a provozování informačních systémů.

Banka přijme bezpečnostní politiku informačních systémů a zabezpečí, aby se strategie rozvoje a bezpečnostní politika informačních systémů pravidelně vyhodnocovaly a případně upravovaly. Banka musí provést analýzu rizik spjatých s informačními systémy. V ní definuje aktiva informačních systémů, hrozby, které na ně působí, zranitelná místa informačních systémů, pravděpodobnost realizace hrozeb a odhad jejich následků a protiopatření. Na základě analýzy rizik zavede banka opatření pro fyzickou ochranu aktiv informačních systémů. Připojení sítě, která je pod kontrolou banky, k vnější komunikační síti, která není pod kontrolou banky, musí být zabezpečeno tak, aby se minimalizovala možnost průniku do informačních systémů. V provozovaných informačních systémech se může používat pouze otestované programové vybavení, u kterého výsledky testů prokázaly, že bezpečnostní funkce jsou v souladu s bezpečnostní politikou informačních systémů. Banka zabezpečí zálohování informací a programového vybavení informačních systémů významných pro její fungování. Zálohované informace a programové vybavení musejí být uloženy tak, aby byly zabezpečeny proti poškození, zničení a krádeži.

Zákon o technických požadavcích na výrobky

Dále se v oblasti bezpečnosti informačních systémů aplikují technické předpisy na základě § 3 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů (dále jen "zákon o technických požadavcích"). Technickým předpisem se pro účely zákona rozumí právní předpis, obsahující technické požadavky na výrobky, popřípadě pravidla pro služby nebo upravující povinnosti při uvádění výrobku na trh, při jeho používání nebo při poskytování nebo zřizování služby nebo zakazující výrobu, dovoz, prodej či používání určitého výrobku nebo používání, poskytování nebo zřizování služby.

Českou technickou normou je dle § 4 zákona o technických požadavcích dokument pro opakované nebo stálé použití vytvořený podle zákona a označený písmenným označením ČSN.

Česká technická norma není obecně závazná, a proto její nedodržení není v rozporu se zákonem. Avšak stanoví-li právní předpis dodržovat ČSN, nedodržení ČSN bude porušením právního předpisu. Je tedy třeba, aby vznikl zákon o zajištění bezpečnosti informačních

systémů, který bude odkazovat na ČSN a použití norem bude tudíž povinné. Prozatím se používají nezávazně.

Kromě ČSN zákon o technických požadavcích zmiňuje harmonizované české technické normy, harmonizované evropské normy, tzv. určené normy a zahraniční technické normy.

V systému řízení bezpečnosti informačních systémů se nejen v bankovním sektoru významně prosazuje norma ČSN ISO/IEC18) BS 7799-2:2004 - Systém managementu bezpečnosti informací - Specifikace a s návodem pro použití. Dále se používá norma ČSN ISO/IEC 17799:2005 - Informační technologie - Soubor postupů pro management bezpečnosti informací, která nahradila pět let starou normu nesoucí stejný název. Nová norma z roku 2005 obsahuje přesnější definice obsahu bezpečnostních opatření a definice požadavků na jejich implementaci.

V současné době je uznávaným standardem při zajištění bezpečnosti bankovních systémů ČSN ISO/IEC 15408 (tzv. Common Criteria for Information Technology Security Evaluation).

V případě, že nastanou problémy, je vždy snaha je rychle a efektivně minimalizovat bez poškození dobrého jména banky nebo bez porušení právních předpisů, neboť zcela se jim vyhnout je prakticky nemožné.

Trestní zákoník

Původně byla počítačová kriminalita (computer crime) zaměřena proti fyzické podstatě počítače (například poškozování cizí věci, krádež atd.). Přes první útoky na *"obsah"* počítače (obvykle s úmyslem spáchat podvod bankovní, fakturační aj.) a tzv. softwarové pirátství se vývoj trestné činnosti v oblasti výpočetní techniky dostává do tzv. nové doby počítačového zločinu, která se vyznačuje nástupem osobních počítačů a vznikem počítačových sítí a vzdáleného přístupu, zejména internetu. Objevuje se tzv. distanční trestná činnost a další specifická trestná činnost - informační delikty a ryze internetové delikty.

Platná právní úprava českého trestního práva hmotného stanovuje v § 249b zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů (dále jen "*trestní zákon*"), ve zvláštní části mezi trestnými činy proti majetku v hlavě deváté trestný čin neoprávněného držení platební karty. Dalším trestným činem týkajícím se přímého bankovnictví je trestný čin poškození a zneužití záznamu na nosiči informací (§ 257a trestního zákona).

Nepřijatý nový trestní zákoník (dále jen *"návrh zákona"*) reflektoval na novou dobu počítačového zločinu zavedením skutkových podstat vycházejících z Úmluvy o počítačové kriminalitě ze dne 23. listopadu 2001 a z požadavků praxe: neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací (§ 205 návrhu zákona), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 206 návrhu zákona) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 207 návrhu zákona).

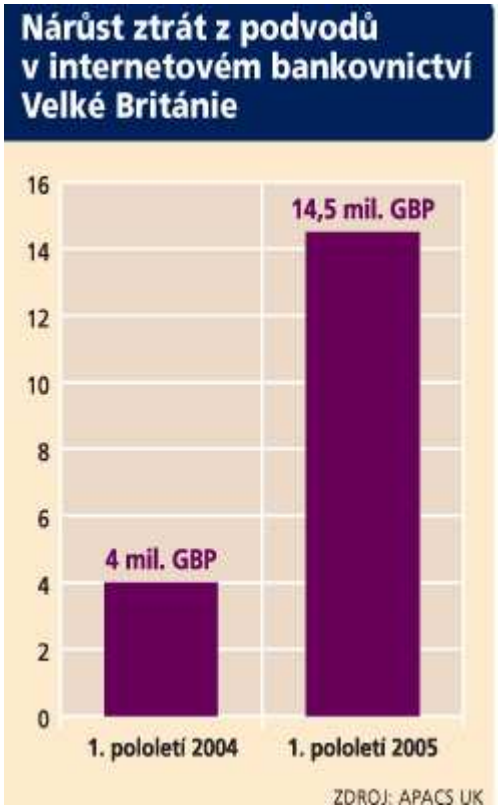
Novodobá počítačová kriminalita se soustřeďuje především na nelegální získávání nehmotných statků, přesto se útokům na vlastní hardware (zařízení) nevyhneme (uvedené krádeže, poškozování cizí věci atd.).

Deset nejčastějších internetových podvodů

Pro ilustraci uvádíme výběr ze stránek www.fraud.org, popisující deset nejčastějších internetových podvodů v roce 2005: internetového bankovnictví se nejvíce týká šestý nejčastější podvod – phishing.

Kategorie	Procento ze všech stížností	Průměrná ztráta
1. Aukce (zboží z aukce zaplaceno, ale nikdy nedodáno, anebo dodáno zboží, jehož vlastnosti byly při lákání klienta podvodně popsány)	42 %	1155 USD
2. Klasický prodej po internetu (zboží zaplaceno, nedodáno, nebo dodáno zboží, jehož vlastnosti byly při lákání klienta podvodně popsány)	30 %	2528 USD
3. Nigerijské nabídky peněz (falešné sliby o převodu velké sumy peněz z účtů například bývalých diktátorů, pokud oslovený zaplatí dopředu poplatek za převod)	8 %	6937 USD
4. Falešné šeky (zaplacení falešnými šeky za zboží nebo práci a instrukce na vrácení peněz převodem)	6 %	4361 USD
5. Loterie/loterijní kluby (požadavky na zaplacení poplatků kvůli údajné výhře v loterii)	4 %	2919 USD
6. Phishing (e-maily, které předstírají, že pocházejí od známého zdroje, například některé banky, žádající o potvrzení osobních dat, mimo jiné první krok ke zneužití účtu ovládaného přes internet)	2 %	612 USD
7. Falešné úvěry s předem placeným poplatkem (falešné nabídky úvěru občanovi nebo podniku, dokonce i těm, kterým by banky nepůjčily, za předem zaplacený poplatek)	1 %	1426 USD
8. Podvody v rámci informačních, erotických a dalších stránek (náklady a/nebo podmínky poskytování služeb nejsou otevřeně uvedeny, nebo jsou uvedeny zavádějícím způsobem)	1 %	504 USD
9. Práce z domova (prodej informačních materiálů na základě falešných slibů práce z domova)	1 %	1785 USD
10. Služby slibující přístup na internet (náklady nebo jiné služby jsou nepravdivě nebo zavádějícím způsobem popsány, nebo služby nejsou nikdy poskytnuty)	1 %	1262 USD

ZDROJ: FRAUD.ORG



Obchodní zákoník

Značná část požadavků na zajištění bezpečnosti přímého bankovnictví náleží do oblasti veřejnoprávní regulace (veřejné bankovní právo, trestní právo aj.). Ze soukromoprávní oblasti práva nelze ale otázku zajištění bezpečnosti zcela eliminovat. Smluvní vztah mezi bankou a klientem o poskytování a využívání služeb přímého bankovnictví se řídí § 269 odst. 2 zákona č. 513/1991 Sb.(ObchZ), ve znění pozdějších předpisů, dále obchodními podmínkami pro vydávání a užívání elektronických platebních prostředků, které jsou s určitými odchylkami stejné jako Vzorové obchodní podmínky pro vydávání a užívání elektronických platebních prostředků České národní banky, a také se mohou řídit tzv. technickými podmínkami pro uživatele služeb přímého bankovnictví. Kromě právně závazných předpisů se banky řídí i nezávaznými pravidly ve formě kodexů nebo standardů aj.

Dojde-li k nefunkčnosi informačního systému, klienti mohou apelovat na banku, aby jej opět uvedla do provozu. Narušení bezpečnosti klientských účtů (nikoliv vinou klienta) může být porušením dohodnutých povinností ze strany banky a může vzniknout protiprávní vztah, s nímž právo spojuje sankční následky.

Literatura

1. Kosiur D., Elektronická komerce, principy a praxe. Brno: ComputerPress, 1998. ISBN 80-7226-097-9.
2. Sculley A., Woods W., B2B Internetová tržiště, revoluce v obchodování mezi fir mami. Praha: Grada Publishing, 2001. ISBN 80-247-0081-6.
3. Ondráček, M.: Elektronické obchodování - diplomová práce. Brno: PEF MZLU v Brně, 2003.
4. Peterek, M.: Elektronické obchodování - diplomová práce. Brno: FI MU, 2003.
5. Klobása, J.: Přímé bankovnictví v ČR a EU – diplomová práce. Brno: MU, 2005.
6. HAJNÍK, F.: Bezpečnost internetového bankovnictví, situace a trendy, Bankovnictví 2/2004, str. 28-29
7. Nové trendy a jejich vliv na bankovní IT, Bankovnictví 2/2004, str. 13
8. Internetové bankovnictví v české kotlině, Bankovnictví 10/2006
9. Problémy internetového bankovnictví očima experta IT, Bankovnictví 11/2006
10. Přádka, M., Kala, J.: Elektronické bankovnictví, ComputerPress, 2000, 166., ISBN 0-7226328-5
11. Internetové bankovnictví na vzestupné linii, bankovnictví 6/2006