JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Katedra obchodu a cestovního ruchu

Studijní program: B6208 Ekonomika a management

Studijní obor: Obchodní podnikání

Online bankovnictví a spotřebitelé

Vedoucí bakalářské práce
Ing. Viktor Vojtko, Ph.D.

Autor
Martin Kakaš

2011

Zadání práce

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Online bankovnictví a spotřebitelé“ vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47 b zákona č. 111/1998 Sb. v plném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly, v souladu s uvedeným ustanovením zákona č. 111/1998 Sb., zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 31.3.2011

…….

Martin Kakaš

Poděkování

Tímto bych chtěl velmi poděkovat celému kolektivu pedagogů z Jihočeské univerzity, Ekonomické fakulty za kvalitní přípravu a pomoc při mé práci a studiu. Především bych chtěl poděkovat vedoucímu bakalářské práce *Ing. Viktoru Vojtkovi, Ph.D.* za cenné profesionální rady, připomínky a metodické vedení práce. Dále bych chtěl poděkovat manažerce týmu *Veronice Neudörflové* a *Ing. Milanu Prokešovi* z pobočky ČSOB na Lannově třídě 3/11 v Českých Budějovicích za umožnění a získání praktických zkušeností.

Obsah

Úvod

Informační technologie a pokrok doby přinášejí do našich životů faktory, které nám napomáhají využívat služby, zaměřené na jednoduchost a urychlení jejich chodu.

Změnou prošly i poskytované bankovní služby. Pro přístup jsou používána zařízení, které jsou běžnému uživateli dostupná. Konstrukce umožňují přihlášení ke svému bankovnímu účtu online a uživatel tak může veškeré operace provádět z domova či práce.

Internetové bankovnictví poskytovaly banky již od počátku vzniku internetu, kdy ale jejich využití nebylo v takové míře, v jaké je nyní. Dnes je online bankovnictví využíváno převážně mladými lidmi a lidmi ve středním věku, což je způsobeno zejména větší znalostí informační techniky. Online bankovnictví je velmi spekulované téma, které je proloženo jistými výhodami i nevýhodami pro uživatele.

Pro připojení k internetu jsou uzpůsobena různá zařízení, nejčastěji jsou to stolní nebo přenosné počítače, mobilní telefony, tablety, PDA. Zejména chytré mobilní telefony se stávají s postupem času trendem, které svými aplikacemi jsou dosti podobné osobním počítačům a časem by se takto uzpůsobené aplikace měly sbližovat do jednoho podobného celku. Je otázkou času, kdy se počet uživatelů mobilních telefonů, přihlašujících se z nich ke svému bankovnímu účtu, vyrovná uživatelům, kteří se přihlašují přes internet z počítače.

Téměř 56% domácností je připojeno k internetu a využívají jej jako součást svého života **[9]**. Mají tak nabízenu jedinečnou možnost použití virtuálních služeb. Důležitou součástí každé domácnosti je nakládání se svými úsporami a finančními prostředky. Nejčastěji je využíváno právě online bankovnictví prostřednictvím internetu. Tato služba je čím dál více žádána a využívána pro svou jednoduchost, nenáročnost na čas a jednoznačně i dostupnost.

Jako každá věc, má i internetové bankovnictví svou negativní i pozitivní stránku. Negativem je přílišná nedůvěra lidí, právě v onu neosobní komunikaci, která je často doprovázena strachem a obavami z odcizení či poškození. V případě naplnění těchto obav není služba uživateli ve většině případů dále využívána. Pozitivem je snaha

bankovní instituce eliminovat útoky proti hackerům a co nejlépe zareagovat na pokrytí služeb takovým zabezpečením, které je u těchto služeb nutné. Snahou bankovních institucí je v uživatelích vzbudit dojem, že služba je bezpečná a spolehlivá. Kroky k zabezpečení jsou nutné i ze strany uživatelů internetového bankovnictví. Zejména uživatelé, kteří využívají tzv. home banking, internet banking, prostřednictvím internetu, by měli být obezřetní. Zabezpečením je využití některých antivirových programů a jiných podpůrných programů pro ochranu osobního počítače, před zákeřnými útoky.

Cílem mé práce je zhodnocení stavu internetového bankovnictví a na základě výzkumu stanovit opatření pro zlepšení jeho chodu.

1. Literární rešerše

1.1 Moderní trend bankovnictví

Vývoj služeb a produktů, které poskytují banky je ovlivněn a neustále ovlivňován pokrokem doby. Technický pokrok si žádá neustálý běh kupředu. Velkým trendem současné doby, je co nejvíce usnadnit a zrychlit komunikační kanály a komunikaci samotnou. Nejčastěji se tak děje za podpory elektronických systémů, a to v celosvětovém měřítku. Velký rozvoj zaznamenalo i internetové bankovnictví. Významným cílem je zvýšení úrovně poskytovaných služeb klientům banky, umožněním vzdáleného a nepřetržitého přístupu k bankovním produktům 24 hodin denně, 7 dní v týdnu, 365 dní v roce. Výrazným pozitivem je také urychlení bankovních operací, které jsou při pohledu zpět, dnes na vysoké úrovni **[27]**.

Internetové bankovnictví urychluje průběh bankovních transakcí a operací, které vedou ke snížení nákladů bank, což ho činí levnějším v provozu a také do jisté míry bezpečnějším **[33]**. Klient není omezován žádnou pracovní dobou jednotlivých poboček bank v daných lokalitách, nemusí čekat v dlouhých frontách u bankovních přepážek a má zcela volný přístup k účtu **[34]**.

1.2 Banky

Při pohledu do reálného ekonomického světa jsou banky řazeny do podnikatelských subjektů. Jejich prioritní cíl se příliš neliší od cílů jiných podnikatelských subjektů. Bankovní prioritou je maximalizace tržní hodnoty a to v dlouhodobém časovém horizontu. Banky se stávají finančními zprostředkovateli, kteří zajišťují peněžní toky mezi ekonomickými subjekty **[18]**. Nejvíce jsou zastoupeny na finančním trhu, kde působí jako důležitý článek. Banka přijímá vklady od firem, obyvatelstva a veřejného sektoru v neomezené míře, aby mohla poskytovat půjčky a úvěry **[40]**.

Bankovní instituce jsou tedy organizace, které mají oprávnění k provádění bankovních operací a transakcí, starají o přijímání vkladů, poskytování úvěrů a umožňují další bankovní služby **[37]**.

Oblasti, na které se zaměřují banky dnes, jsou snižování nákladů a hledání úspor při vyšší efektivnosti práce a preciznosti řízení procesů. V jejich moci je pružná a rychlá reakce na podněty trhu a klientely. Své pracovní nasazení proto přesouvají do finančně výhodnějších oblastí s kladeným důrazem na zabezpečení a udržení anonymity **[40]**.

Důležitým zaměřením je také snaha o odlišení služeb od konkurence a získání více zákazníků **[20]**.

1.2.1 Bankovní systém

Bankovní systém je nedílnou součástí tržní ekonomiky **[19]**. Tento termín lze definovat jako veškeré banky nacházející se na území určitého státu, které podléhají zákonným ustanovením včetně jejich mezivztahů. V ekonomice plní bankovní systém dva nejzákladnější úkoly a to makroekonomické a mikroekonomické **[18]**.

Peníze do hospodářství jsou zajišťovány pomocí bank, které se tak stávají bližšími partnery s ostatními sektory hospodářství oproti jiným sektorovým vazbám **[19]**.

Bankovní systém je rozdělován podle hlediska rozlišení na jednostupňový a dvoustupňový systém. Dalšími specifickými systémy je univerzální bankovní systém a oddělený bankovní systém **[18]**.

Jednostupňový bankovní systém je datován jako nejstarší. Neexistovala zde centrální banka a banky samy byly nucené vykonávat makroekonomické a mikroekonomické funkce **[40; 18]**.

Dvoustupňový bankovní systém vykazoval přítomnost centrální banky, která byla prvním stupněm tohoto systému. Obchodní banky zajišťovaly stupeň druhý **[18]**. Systém vykazoval mnoho cílů, z nichž jedním bylo zabezpečení měnové stability, dále byly zajištěné i jiné makroekonomické funkce. Postavení bank bylo v roli uskutečňovatelů mikroekonomických funkcí dvoustupňového bankovního systému se ziskovým principem **[40]**.

Univerzální bankovní systém je založen na principu, kdy banky provádějí komerční i investiční činnosti, zatímco **oddělený bankovní systém** rozděluje na základě legislativy investiční a komerční obchody **[18]**.

1.2.1.1 Centrální banka

Centrální banka má velmi významné postavení v moderním bankovnictví, stává se vrcholným článkem bankovní soustavy. Snahou centrální banky je prioritně zabezpečit měnovou stabilitu **[19]**. Ve vztahu k vládě, ostatním bankám a samotnému státu je postavení ústřední banky upraveno zákonem 6/1993 Sb. O České národní bance v platném znění **[40]**.

Centrální bankou v České republice se nazývá Česká národní banka (ČNB)
Kromě hlavního cíle má centrální banka i druhotné cíle **[37]**:

- vydávání bankovek a mincí
- kontroluje a řídí činnost ostatních bank, jejich poboček
- reguluje peněžní oběh a snaží se o jeho plynulý chod
- dohled a kontrola bankovního systému
- provádí další činnosti dle zákona

Nejvyšší orgán ČNB je rada, která je sedmičlenná a jmenuje ji prezident České republiky na lhůtu 6 let. Orgánem nad touto radou je guvernér ČNB. Tím je od 1.7. 2010 Miroslav Singer **[19; 5]**.
ČNB má na starost kromě cílů i plnění některých dalších funkcí **[19]**. **Emisní funkce** pro ČNB představuje právo vydávat bankovky a mince a to i pamětního charakteru. Z hlediska právního předpisu si stanovuje také rozměry, nominální hodnoty a produkci měny **[37]**. V širším pojetí zde můžeme zahrnout i řízení peněžního oběhu **[19]**.

Funkce banky bank, centrální banka ČR je bankou pro ostatní banky, reguluje a monitoruje jejich dodržování předpisů, může jim poskytovat úvěry, postihuje a pokutuje, vydává licence včetně jejich odebírání **[19]**. Přijímá také vklady od ostatních bank a vede jejich účty **[40]**. **Funkce banky státu**, je pro stát důležitá, protože státní účty jsou vedeny pod ČNB, která může poskytovat státu úvěry, poradenskou činnost

v oblastech měnové politiky. Dále zatupuje stát v mezinárodních měnových a finančních institucích **[19]**..

1.2.2 Bankovní služby

Bankovní účty jsou tvořeny vklady uživatelů bank, kteří zde ukládají své finanční prostředky. Všechny akce od velikosti uložené částky přes výběr finančních prostředků až po zjištění částky, která na bankovním účtu zbývá, jsou v záznamech bankovní instituce. Za uložené peníze v bance je přinášen uživateli úrok, který navyšuje zůstatek na bankovním účtu.

Uživatelé mají mnoho důvodů, proč takto ukládají peníze, ale nejběžnější je právě onen důvod získání úroku **[37]**. Osobně bych s autorem nesouhlasil, protože úroky jsou nízké a poplatky za některé služby jsou převyšující než očekávání zákazníků, tudíž z toho plyne pro ně malý zisk.

Klientské účty mohou mít různé formy odvíjející se od jejich účelu použití za jimiž byly zřízeny. **Běžný účet** bychom charakterizovali jako účet k vkladům a výplatám hotovostí. Jedná se o nejběžnější formu platebního styku. Splácení a evidování čerpaného úvěru je typické pro **úvěrový účet**, zatímco **kontokorentní účet** je kombinací předešlých dvou účtů. Uživatel tak má možnost čerpat finanční prostředky do sjednané výše za určitých předem dohodnutých podmínek. Vkladový účet slouží k vkladům volných finančních prostředků klientely a **depotní účet** umožňuje evidenci cenných papírů v úschově nebo jsou spravovány bankovní institucí **[30]**.

1.2.3 Podmínky vedení účtu v České republice

Podmínky k vedení účtu a povinnosti banky a klientely v jejich vzájemných vztazích upravují Obchodní podmínky pro vedení účtu. Obchodní podmínky pro vedení účtu vycházejí ze Smlouvy o vedení účtu, která je sepsána mezi klientem a příslušnou bankou. Ty jsou upraveny právními předpisy, jimiž jsou v ČR zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 124/2002 Sb., o platebním styku, ve znění

pozdějších předpisů, vyhláška č. 62/2004 Sb. a dále z obchodních všeobecných podmínek, které vydala Česká národní banka **[30]**.

1.2.4 Platební systémy

Následný bezhotovostní platební styk mezi různými bankami je zajišťovaný některým z těchto dvou systémů:

Korespondentský systém vyjadřuje, přímé spojení bank přes navzájem otevřené účty platebního styku

Zúčtovací systém (Clearing) představuje systém, kdy jedna z bank je zúčtovacím místem pro obchodní bankovní instituce, které jsou s ní propojeny skrze vlastní účty platebního styku. V ČR je využíván druhý systém **[26]**.

1.3 Přímé bankovnictví

Online bankovnictví, někdy také uváděno jako přímé bankovnictví, umožňuje klientovi banky, který využívá tyto služby, provádět bankovní operace se svým účtem online. Je mu tak umožněno přehledné sledování pohybu peněz na jednom či více jeho účtech prostřednictvím telekomunikačních či datových sítí z pohodlí svého domova nebo pracovní kanceláře **[25]**. Pro vzájemnou komunikaci klienta a banky je využívána celosvětová síť internet **[16]**.

Služby bank prováděné pomocí online bankovnictvím umožňují kromě sledování toků peněz, realizovat pasivní i aktivní operace v těchto oblastech:

- monitorování zůstatků na účtech
- zadávání jednorázových nebo trvalých příkazů k úhradám
- informovanost o výběru z platebních karet
- výpisy z účtů

Obecně by se dalo říci, že je zde zaznamenána veškerá aktivita, která se s účtem provede **[27]**.

Ve většině případů každá banka požaduje po uživatelích za operace provedené přímým bankovnictvím nižší poplatky než za stejné operace provedené u přepážky banky **[16]**.

S rostoucím vývojem moderních informačních technologií jsou banky nuceny přecházet na nové koncepce a nové úrovně poskytovaných služeb prostřednictvím formy samoobslužného bankingu. Hlavními důvody jsou zejména rostoucí náklady na personální zajištění bank, neustálá klesající loajalita zákazníků vůči bankám a monstrózně narůstající konkurence na poli bankovních obchodů s privátní klientelou **[33]**.

1.3.1 Druhy přímého bankovnictví

Internetové bankovnictví je soubor služeb, kterými manipulujeme s bankovním účtem prostřednictvím osobního počítače a sítě Internet, ke které je tento osobní počítač připojen **[25]**.

Jednotlivé druhy přímého bankovnictví lze dělit podle různých hledisek dle:

- nároků na vybavení
- podle způsobu zabezpečení
- způsobu provedení
- použité technologie

Pro základní rozdělení uvádím přímé bankovnictví členěné z hlediska nároků na vybavení. Z hlediska nároků na vybavení můžeme přímé bankovnictví rozdělit na tzv. internet banking a home banking **[25]**. Dále pak na mobil banking a PDA banking.

- **home banking –** je zprostředkovaná komunikace mezi klientem konkrétní banky a bankou skrze počítač přes modem a telefonní linku **[27]**. Tefonní linka s vytáčeným připojením je v současné době nahrazována vysokorychlostním internetem, kupříkladu ADSL nebo oblíbenými bezdrátovými sítěmi. Veškeré operace platební styku mezi klientem a bankou jsou pouze na elektronické bázi **[26]**. Od internet bankingu se liší tím, že do osobního počítače uživatele je vložen speciální program, který dodá banka. Přes tento dodaný program probíhá

komunikace **[27]**. Přístupnost k bankovnímu účtu je pouze z konkrétního počítače, na kterém je program nainstalován **[16]**. Výhodnější stránkou je lepší integrace do softwaru a programů třetích stran (např. ekonomický či účetní software) **[25]**.

- **internet banking –** pro provoz je postačující osobní PC s webovým prohlížečem a přístupem k internetu. Výhodou je, že uživatel má ke správě svého účtu a bankovnictví přístup z kteréhokoliv počítače připojeného k této síti, zatímco varianta home banking je omezena na konkrétní počítač a bankovní software **[25]**.
- **mobil banking –** nejjednodušší cestou přístupu k online bankingu je mobilním telefonem a lze tak odkudkoliv a kdykoliv získat informace o stavu konta, o produktech, úrocích a dalších službách. Zabezpečení je zajištěno nejčastěji ověřením totožnosti skrze PIN a osobní heslo, hovory jsou dále nahrávány **[29]**. **WAP banking (Wireless application protocol) –** jedná se převážně o obdobu internet bankingu, je uzpůsobený speciálně pro mobilní telefony. Nutností pro využívání této služby je také sjednaná smlouva s příslušnou bankou **[16]**. Služba je málo využívaná z důvodu vyšších pořizovacích nákladů **[27]**.
- **PDA banking –** jedná se především o novější formu internetového (webového) bankovnictví, které je určené pro kapesní počítače. Moderní kapesní počítač je v podstatě miniaturizace osobního počítače, který ale obsahuje pouze připojení k síti prostřednictvím tzv.Wifi (bezdrátového připojení k síti internet **[14]**. Základ PDA bankingu spočívá ve zjednodušené formě webového obsahu, který musí být přizpůsoben velikosti zobrazovacího panelu (displeje) kapesního počítače. Převážně se jedná o textovou formu webového rozhraní. V současnosti zatím tento způsob bankovnictví není příliš rozšířen **[25]**. S rostoucím vývojem mobilních zařízení, jsou kromě bezdrátových sítí Wifi, využívané také sítě 3G, které mají téměř 100% pokrytí.

1.3.2 Bezpečnost internetového bankovnictví

Na prahu nového tisíciletí zloději už nebudou provádět bankovní útoky pomocí pistole a páčidla. Již dnes se používají metody, které mají promyšlený záměr a nevykazují násilné chování či slyšitelné zvuky, jako tomu bývalo donedávna zvykem. Pachatelé činů jsou prostřednictvím internetu v určité anonymitě a otevírá se jim cesta k proniknutí a odhalení slabých míst v bankovním systému s cílem obohacení se na vlastní účet **[33]**.

Nejčastějšími prohřešky se stávají situace, kdy dochází k připojení k online bankovnictví na nezabezpečeném počítači nebo neúmyslném vyzrazení přístupových informací. Tímto pak doslova hazardujeme s našimi financemi **[34]**. Na místě je právě ona opatrnost a hlavně dodržování určitých bezpečnostních pravidel a podmínek, které by měl uživatel dodržovat v zájmu své bezpečnosti **[32]**. Různé typy zabezpečení jsou omezené na zařízení, které uživatel online bankovnictví vlastní. Podle toho je také uzpůsobena míra ochrany před případnými zákeřnými útoky a lze s určitostí říci, že zabezpečení u telefonického a internetového bankovnictví nepřináší totožné možnosti **[25]**. Hrozbu v tomto případě představují nejrůznější typy virů, červů, trojských koní a ostatních alternativ představující potencionální nebezpečí **[24]**.

Zvyklostí zejména českých bank je uživatelům přímého bankovnictví nabízet jako součást jejich služeb základní způsob zabezpečení a za veškeré zabezpečení vyššího řádu jsou si uživatelé nuceni připlatit **[25]**.

1.3.3 Typy útoků

Mezi bankovní priority téměř každé banky patří ochrana osobních údajů a informací, protože informace jsou důležitou součástí provozního chodu banky **[33]**.

Eliminaci internetového napadení k získání informací může do jisté míry ovlivnit i sám uživatel jeho chováním na síti internet, průběžnou kontrolou a opatrností.

Mezi nejčastější typy útoků patří tzv. phishing, pharming, spyware **[25]**. Phishing pochází z anglického slova „ fishing“, které je v překladu rybařit, či rybaření. **[34]**. Jeho existence je datována od roku 1995, ale jeho největší rozmach započal až od roku 2003, kdy byly napadány velké instituce **[23]**. Cílem phishingu je ulovení

informací **[34]**. Útok je konstruován tak, že uživateli je prostřednictvím e-mailové zprávy poslána žádost jménem bankovní společnosti o zaslání osobních informací nebo o změnu přihlašovacích údajů ke svým účtům prostřednictvím internetových stránek. Avšak zpráva či případná změna údajů na stránkách, která se tváří navenek opravdově, je podvrhem k získání cenných informací. Stránka se může tvářit naprosto identicky s přihlašovacím oknem opravdové bankovní služby banky **[32]**. Uživatel tak v domněnce, že opravdu komunikuje s bankovní institucí, předá informace. Útočníci tak získávají snadno citlivá data a údaje ke zneužití a odcizení peněz z bankovního účtu **[25]**. Phishing je v dohledné době postupně nahrazován tzv. whalingem. Z anglického překladu to znamená velrybaření, kdy se útočníci zaměřují na větší úlovky z důvodu vynakládání stejné síly s větším přínosem. Zaměřují se na několik málo cílů, s důkladnou intenzitou **[34]**.

Promyšlenější metodou je pharming, kde hlavní snahou útočníka je automatické přesměrování na vlastní stránky, které jsou falešným napodobením webových stránek banky **[25]**. Přesměrování je řešeno na bázi, kdy se pachatelé nabourají do systému doménových jmen a provedou přesměrování na podvodnou stránku **[13]**. Tím jsou získávány přihlašovací údaje k útokům. Druhou a více nebezpečnou variantou může být v podobě prostředníka mezi skutečným uživatelem a konkrétním systémem online bankovnictví. Pouze údaje o autorizaci jsou zaslány v pořádku, zatímco údaje z oblasti transakcí jako jsou čísla bankovních účtů, velikost transakčních částek jsou zneužity pachatelem **[25]**.

Spyware je speciálně napsaný program, který prostřednictvím sítě internet odesílá data **[31]**. Někdy je také přezdívaný jako „data miner“, neboli „důl na informace“ a svou škodlivostí může mít na svědomí i kolaps počítačů **[6]**. Jeho běh se děje za zády uživatele, který tento jev nemá možnost postřehnout. Úkolem je monitorovat činnost uživatelů a na základě toho sbírat informace o veškeré aktivitě **[25]**. Stává se tak programem, který narušuje soukromí uživatele **[6]**. Do počítače se program dostává prostřednictvím trojských koní a nejrůznějších škodlivých kódů, které jsou součástí programů **[25]**. Převážně se jedná o programy typu **shareware,** programy u kterých je bezplatně umožněno volné šíření a používání. V případě trvalého používání

je placen registrační poplatek autorovi programu **[1]**. Ten může být v podobě **adware,** kdy je program poskytován za sníženou cenu nebo ve variantě zdarma, ale obsahuje v sobě integrovanou reklamu **[2]**. Možností je i průběh bez vědomí uživatelů, ale s vědomím autorů programu, kteří jej vytvořili. Spyware bychom zařadili do množiny **malware,** kam řadíme viry, trojské koně, tedy do skupiny programů, které na počítači běží bez souhlasu uživatele a poškozují nebo znepříjemňují jeho práci a funkční vlastnosti. Stávají se tak postrachem, jelikož jsou posílány různé informace (navštívené stránky, přístupová hesla a ostatní cenná data) určitému uživateli, který s nimi dále pracuje **[31; 3]**.

Další technikou nefyzického napadení je využití sociálního inženýrství. Pachatel na oběť v podobě uživatele působí psychologicky, snaží se mu důvěrně vsugerovat, že je někdo jiný s cílem zneužití. Uživatel je tak zmanipulován k vyzrazení informací, popřípadě aby vykonal určitý úkon **[39]**.

1.4 Chování spotřebitelů na internetu

Spotřební chování je spojeno s chováním zákazníků a jejich jednáním, které podmiňuje i okolní prostředí **[22]**.

Zásadním činitelem téměř každé banky, která chce být úspěšná, je predikce a péče o své klienty a uspokojování jejich potřeb. Nejdůležitějším faktorem bankovní instituce je klientela, ať už se nachází přítomna ve fyzické formě nebo komunikuje prostřednictvím distribučních kanálů. Pro banku jsou zákazníci důležití, dá se říci, že životně důležití.

Produkty, služby, které banky nabízejí, jsou cílové, po stránce uzavření obchodu, ale prioritou je také udržení klientely v dlouhodobých vztazích a spolupráce. Zejména v dnešní velké konkurenci bank je čím dál těžší si zákazníky udržet.

Klienty ve vztahu s bankou ovlivňují různé faktory, které bychom mohli rozdělit do těchto kategorií:

Psychologická, představující faktory motivační, osobních zkušeností a postojů (víry).

Osobní, zde hraje významnou roli věk, zaměstnaní, životní styl člověka, osobnostní předpoklady, ekonomické zařazení.

Sociální, kam bychom zařadili rodinu, společenské postavení a postavení člověku ve společenské formě.

Kulturní, tvořena zásadami a kodexy, postavením člověka v komunitě, kulturním vyzráním oblasti, ve které člověk žije.

Chování jedince ve vztahu k penězům je závislé na určité věkové skupině. Potřeby, které člověk má, se v průběhu jeho života mění. Tento tzv. životní cyklus klienta lze popsat v následujících bodech:

- věk do 14 let, uživatelé v tomto věku jsou ovlivněni rozhodnutím svých rodičů, převážně nejčastějším produktem je spoření
- věk 14 – 18 let, rozhodnutí rodičů je v tomto bodě na jistém úpadku a u jedince narůstají zájmy o moderní technické formy placení (platba kartou)
- věk 18 - 25 let, je charakterizován vstupem do pracovního poměru, kdy narůstají nároky na splnění potřeb, úvěry, půjčky, využití elektronického bankovnictví
- věk 25 – 45 let, člověk v této fázi nejvíce využívá služeb spoření, pojištění, vkládání finančních prostředků do svého života (bydlení, automobil)
- věk 45 – 60 let, příprava na stáří, s kterou souvisí opět využití různých programů spoření. U uživatele roste zájem také o různé formy pojištění
- nad 60 let, využití nenáročných a jednoduchých služeb **[41]**. S autorem bych v tomto tvrzení osobně nesouhlasil, protože jsou důležité také finanční možnosti uživatele a nemusí to nutně znamenat jen využití nenáročných a jednoduchých služeb.

1.4.1 Zdroje informací pro klienty

Proces hledání informací spotřebiteli může mít různou rozmanitost a podobu.

Vnitřní hledání informací je založené na podstatě připomenutí či oživení konkrétních informací, které se nacházejí v paměti spotřebitele. Jedná se o střípky či vjemy, které byly v paměti již před nějakým časem uloženy.

Vnější hledání informací je charakterizováno jako děj, kdy spotřebitel získává informace z jeho širokého okolí, které poté ovlivňují jeho spotřebitelské chování. Působí zde hned dva faktory: zvýšená pozornost a aktivní vyhledávání. Zvýšená

pozornost identifikuje přicházející informace v oblasti problému, které se v průběhu bližšího poznání v okolí člověka objevují. Zatímco aktivní vyhledávání je převážně na snaze spotřebitele získat veškeré možné informace o dané problematice a možnostech řešení **[21]**.

1.4.2 Psychologie klientů pro výběr služby (kybernetický prostor)

Virtuální realita, někdy též nazývána jako kyberprostor, je zastoupena pomocí moderních počítačových technologií. Je vytvořena jako identická kopie reálného světa a také ho ve svém způsobu zastupuje. Velmi významnou roli také hraje počítačové rozhraní. Pomocí speciálních přístrojů jsou lidé schopni slyšet, hmatat, hovořit, vidět a nacházejí se v rolích a možnostech, které jim reálný svět nenabídne.

Virtuální prostor se na rozdíl od reálného prostoru liší tím, že je nám zcela ve většině případů podřízen, jsou mu pouze zadány příkazy, které mají za cíl naplnění určitých potřeb, které virtuální realita splňuje.

Z hlediska dokonalosti je možné virtuální realitu rozdělit na pasivní a aktivní virtuální realitu. **Pasivní virtuální realitu** bychom mohli chápat jako prostředí, které jedinec nijak neovlivňuje a jeho chování je pouze v roli konzumenta. Tento jedinec může mít i pocit, že se v prostředí nachází sám. **Aktivní virtuální realita** umožňuje přesunutí se z pasivní role do aktivní role průzkumníka, což vzbuzuje pocit jedinečnosti a důležitosti.

Budoucnost spěje k většímu využívání virtuální reality, ale stále tento prostor bude závislý na lidském faktoru, tedy na lidech, kteří naprogramují stroje a přístroje tak, aby plnily touhy a přání a dokázaly je zobrazit. Nabízí se tedy možnost k vytvoření zcela nového světa se zcela novými cestami. Avšak mohou se stát i situace, kdy člověk přestane rozlišovat reálný a virtuální svět a v případě reálného života nebude schopný zadané úkoly řešit **[15]**.

1.5 Identifikace uživatele

Úlohou tohoto procesu je určení totožnosti majitele. Proces probíhá ve dvojím smyslu. Buď je udána identifikace na základě samotného uživatele, nebo se identifikační systém snaží automaticky vyhledat příslušnou totožnost v množině již známých uživatelů. Množinou je myšlena rozsáhlá databáze, která obsahuje různé prvky záznamů o uživatelích (např. binometrické údaje, otisky prstů, identifikační kódy). Identifikace je mnohem náročnější proces než autentizace, protože s rostoucím rozsahem databáze, klesá míra identifikace a také samozřejmě rychlost vyhledávání shody **[25]**.

1.5.1 Autentizace

Autentizace je charakterizována jako proces, při kterém je uživatelem předloženo objektivní tvrzení o své identitě (např. vložením identifikátoru), kdy jsou srovnány binometrické údaje, které byly zadány uživatelem s binometrickými údaji, které jsou uloženy v databázi **[25]**.

1.5.1.1 Způsoby autentizace

Existují tyto druhy autentizace **[25; 7]**: uživatelské jméno a heslo
elektronický podpis
sms klíč

Uživatelské jméno a heslo

Jedná se o nejzákladnější variantu ověření identity uživatele. Vhodné je, aby heslo, obsahovalo minimální požadovanou délku, kombinaci čísel a velkých a malých písmen. V případě špatného zadání hesla po několika pokusech je dočasně zablokován účet a pro jeho odblokování je nutné navštívit banku **[25]**.

Elektronický podpis

V případě zřízení této služby je obdržena čipová karta, na kterou jsou automaticky vygenerovány osobní certifikáty elektronického podpisu. Karta je zabezpečena pomocí PIN a pro komunikaci s počítačem slouží čtečka čipových karet **[7]**.

SMS klíč

Samotný autorizační kód je zaslán SMS zprávou na mobilní telefon uživatele. Jeho struktura je tvořena z malých písmen a číslic a tvoří 9 místný alfanumerický řetězec (například: qvr – 22b-8h7). Z bezpečnostních důvodů je stanovený limit pro jeho zadání na 10 minut. Takto zaslaný kód je vepsán do určeného pole internetového bankovnictví a tlačítkem „odeslat“ je příkaz k autorizaci odeslán ke zpracování **[7]**.

1.5.2 Autorizace

Autorizaci bychom mohli rozlišit na dva samostatné procesy, které spolu vzájemně souvisí.

Autorizace uživatele v sobě skýtá oprávnění, které je přiřazeno systémem, aby bylo umožněno pracovat v jeho prostředí. Systém dále diriguje uživateli kroky, které jsou mu povoleny a které nikoliv. Autorizace většinou následuje po procesu autentizace.

Autorizace transakce představuje stupeň související s autentizací a autorizací uživatele, který provádí transakci s autentizací dat při provádění transakce **[25]**.

1.6 Ochrana uživatele

Téměř každý běžný uživatel počítače věří v důvěryhodnost počítačových výstupů více, než by bylo dobré, ale otázku bezpečnosti si až tak neuvědomuje. Jednak tím, že si volí snadná až rychle zapamatovatelná hesla k proniknutí, poskytuje interní informace prostřednictvím emailů nebo na informačních zdrojích, které by jinak normálně nezveřejnil.

Za vinu je tomu dávána nízká úroveň zkušeností uživatelů, kteří umí právě tolik, aby mohli vykonávat konkrétní práci s počítačem. Okolnosti v podobě hrozeb

si neuvědomují. Jsou často v domnění, že se jim nikdy nic nestalo a tento pocit je v tomto ještě utvrzuje. V případě, když nastanou problémy, chyba je házena z uživatele na nekvalitní a neúčinné antivirové programy, ochranné systémy programů a chyba v podobě uživatele není z jejich strany přiznána. Na vině je právě, ale i uživatel, který svým chováním mohl těmto problémům předejít **[17]**.

1.6.1 Antiphishingová obrana

Tato podvodná technika používaná na internetu, má různé formy obrany. Z pohledu uživatele je důležité jeho chování na internetu a udržování bezpečnostních pravidel. Po softwarové stránce používání speciálních ochranných programů, které detekují a odstraňují phishing **[31]**.

Firma Billeo vyvinula obranu na principu ochrany již ve fázi sběru, kdy poškození vstoupí na podvrhující webové stránky. Základem je plug-in do internetového prohlížeče, který porovnává URL navštívené stránky s databází známých phishingových stránek. Plug-in obsahuje „semafor“, který upozorňuje na stránky příslušnými barvami. V případě zelené barvy je stránka bezpečná, v případě červené je objeveno nebezpečí útoku **[23]**.

Firma Microsoft ve svých internetových prohlížečích Internet Explorer verze 7 a vyšších, implementovala volitelný filtr útoků phishingu, který filtruje a upozorňuje na falešné webové stránky a v případě potřeby stránky zablokuje. Aktualizace je prováděna vícekrát za hodinu, aby se předešlo navštívení nebezpečné stránky **[32]**.

1.6.2 Hesla

Nejznámějším prostředkem k identifikaci uživatelů se používají hesla. Hesla se rozlišují na statická a dynamická.

Statická hesla jsou pomalu na ústupu z důvodu jejich nedostatečné míry zabezpečení, které sice v době jejich používání dostačovala, ale dnes nikoliv. V praxi se tato hesla používala při ověření identity do informačních systémů, přístupu při výběru finančních částek z bankomatů apod.

Postupně jsou nahrazovány **dynamickými hesly**, které se stávají spolehlivějšími a bezpečnějšími. Každé přihlášení je měněno dle stanoveného algoritmu a nelze tak použít jedno stálé heslo. Heslo je pokaždé měněno za jiné, čímž je zajištěna ochranná bariéra a lze tak předejít přístupu jiné osoby než vlastníkovi. Úroveň a síla zabezpečení je volena vlastníkem **[35]**.

1.6.2.1 Novodobé prvky zvyšující zabezpečení hesla

Přicházející novinkou jsou tzv. **tokeny** (viz. Příloha č.1), které vznikly jako inovační stupeň zabezpečení před krádežemi kryptografických údajů. Na rozdíl od běžného USB flash disku, který byl zabezpečen hardwarově nebo softwarově před krádeží dat, které na něm byly uložené, jsou tokeny na vyšší úrovni, kdy je kombinováno více funkcí na jednom USB tokenu. Klasicky obsahují datové uložiště, jako jsme tomu byli zvyklí u USB flash disků a dále obsahují kryptografické údaje. Kryptografické údaje slouží k identifikaci vlastníka, přístupu k autentizaci na pc. Tokenů je celá řada a neustále se zdokonalují. Základním principem je vygenerování jednorázového přístupového hesla, které se neustále mění. Dalším prvkem jsou tokeny s RFID čipy, kdy v případě vzdálení uživatele od počítače by byl odhlášen automaticky. Neposlední novinkou jsou tokeny na bázi otisků prstů, z kterých je vygenerován unikátní kód, který zvyšuje zabezpečení **[25]**.

1.6.3 Antispywarové programy

Při existenci programů na odstranění virů je obdoba i pro spyware **[6]**. Antispywarové programové vybavení je důležitou součástí k detekci a následnému odstranění škodlivě napsaných programů pro krádeže informací a dat z hostitelských počítačů. Tyto programy jsou spuštěny buď vědomě či nevědomě, většinou jsou součástí volně šiřitelných programů (freeware), vyskakovacích oken prohlížečů internetu a jiných uživatele obtěžujících forem **[16]**.

Součástí některých antivirových programů je antispyware, který kupříkladu nabízí firma Grisoft, spol. s. r. o. produktem antivirového programu AVG. Jako další formy štítu a ochrany lze použít produkty Spyware Doctor nebo bezpečnostní produkty

firmy Microsoft **[16]**. Mezi které patří Windows Defender, který je poskytován jako součást novějších operačních systémů Windows **[28]**. Mezi uživateli je nejoblíbenější program Ad-Aware od firmy Lavasoft, který poskytuje jak placenou tak i volnou verzi pro uživatele. Placená verze má navíc modul Ad-Watch, který v reálném čase na pozadí počítače kontroluje a monitoruje nežádoucí stavy. Knihovny programu procházejí častou automatickou aktualizací **[6]**.

1.6.4 Antiviry

Ochranou proti nežádoucím programům, které byly vytvořeny za účelem poškození příslušného počítače nebo odcizení dat nacházejících se na pevném či vyměnitelném médiu, byly vytvořeny antivirové programy neboli antiviry **[16]**. Po instalaci antivirového programu je obrana zajištěna od samotného zapnutí počítače a je aktivní po celou dobu, kdy je počítač zapnut **[11]**.

Virus je speciálně naprogramovaný program, který se šíří po počítači, aniž by si uživatel toho všiml, dokáže vytvářet své identické kopie a využívá pro své šíření nějaký hostitelský program. Mezi počítači dochází k přenosu viru právě programem hostitele nebo jinými způsoby **[16]**. Dnes se většina virových infekcí šíří sítí internetu. Viry mohou mít podobu klasických spustitelných aplikací, obrázků, dokumentů apod. Tyto programy bývají velmi nebezpečné a jejich záměrem je smazání dat z pevného disku počítače, vyměnitelných médií nebo změnu přístupových hesel. Pro odhalení, identifikaci a následné odstranění virů slouží antivirové programy. Antiviry obsahují velké databáze virových či potencionálních hrozeb a na základě této databáze jsou nebezpečí eliminována. Důležitým faktorem je průběžná a neustálá aktualizace antivirové databáze, aby byla zajištěna co nejlepší ochrana. V současnosti jsou aktualizace prováděny automaticky z internetu, případně si je uživatel může provádět sám z CD a DVD příloh počítačových časopisů **[10]**. Mezi nejznámější antivirové programy, které poskytují placené i volné verze antivirových programů patří: AVG firmy Grisoft, NOD32 od firmy Eset, Norton AntiVirus firmy Symantec **[16]**. Klasické počítačové viry jsou pomalu na ústupu a jejich ničivé účinky přebírají červy (worms), které jsou šířeny převážně sítěmi, tudíž i internetem **[31]**.

1.6.5 Antistealth

Jedná se o specializované vyhledávací programy rootkitů na již infikovaných počítačích. Principem rootkitů je maskování a skrývání nebezpečných programů v podobě virů, trojských koňů, spywaru. Aktivace je uskutečněna při spuštění operačního systému a nelze tak tuto hrozbu běžnými prostředky zjistit. Obranou proti těmto zákeřným technologiím jsou antivirové programy AVG a NOD32, jejichž rezidentní štíty vytváří pro stealth nepropustnou bariéru. Firma Microsoft ve svém novém operačním systému Windows Vista již tuto obranu řešila a měla by být také jeho součástí **[16]**.

2. Cíle a metodika práce

2.1 Cíl práce

Zhodnotit využívání internetových bankovních účtů mezi spotřebiteli. Zjistit jejich pozitiva a negativa. Na základě analýzy a sběru dat formou online dotazování zhodnotit a navrhnout případná opatření pro zlepšení služeb v oblasti internetového bankovnictví.

2.2 Metodika

Výchozím opěrným bodem mé bakalářské práce bude studium odborné literatury, odborných časopisů, knih a odborných článků na internetových stránkách. Po nastudování řešené problematiky z odborných zdrojů jsem stanovil hlavní cíl práce a vymezil hypotézy práce.

K sekundárním datům jsem dospěl studií uvedených literárních zdrojů a odborných výzkumů. Primární data jsem získal vlastním výzkumným šetřením. Výzkumné šetření hlavního výzkumu bylo prováděno pomocí online dotazování prostřednictvím internetu a osobním dotazováním na pobočce banky ČSOB. K hlavnímu výzkumu jsem provedl doplňující otázky, které byly položeny dotazovaným pouze na pobočce ČSOB v Českých Budějovicích.

Zjištěné výsledky jsem zpracoval v tabulkách a grafech a zhodnotil současný stav v dané problematice.

Na základě zjištěných dat jsem stanovil případná obecná doporučení pro banky a konkrétní doporučení pro pobočku ČSOB na Lannově třídě 3/11 v Českých Budějovicích. Významné doporučení pro pobočku ČSOB v Českých Budějovicích bylo ekonomicky zhodnoceno pro případ realizace.

Svou práci jsem završil závěrem a zhodnocením. Ve kterém jsem shrnul získaná data a problematiku internetového bankovnictví, které jsem doložil přílohami.

2.2.1 Hypotézy

H1 Online bankovnictví využívá více než 60% dotazovaných.

H2 60% dotazovaných, kteří používají internetové bankovnictví si myslí, že online bankovnictví je bezpečné.

H3 Osobní počítač je v 70% nejpoužívanějším zařízením pro přihlášení do služeb online bankovnictví.

H4 Dotazovaní, kteří používají online bankovnictví, mají z 80% zajištěno zabezpečení osobního zařízení.

2.2.2 Dotazník

Kvantitativní šetření bylo prováděno pomocí online dotazníku, prostřednictvím internetové volně dostupné aplikace Google dokumenty (Google Docs) a také osobním dotazováním v pobočce ČSOB na Lannově třídě 3/11 v Českých Budějovicích. Dotazník (viz. Příloha č. 2) obsahoval celkem patnáct otázek, složených z deseti uzavřených otázek, čtyř polouzavřených a jedné otevřené otázky. V uzavřených otázkách měli dotazovaní zvolit pouze jednu odpověď, vyjma otázek (U jaké banky jste zákazníkem? Jaké zařízení pro online bankovnictví používáte? Jaké pravidelně aktualizované prvky používáte pro osobní zabezpečení počítače?), kde byla možnost volby více odpovědí. Vedle hlavního výzkumu jsem provedl vedlejší výzkum s doplňujícími otázkami (viz. Příloha č.4). Celkově bylo pět doplňujících otázek a snahou bylo získat od respondentů hlubší odpověď na danou problematiku. Všechny doplňující otázky vedlejšího výzkumného šetření byly polouzavřené.

Dotazníkové šetření prostřednictvím internetu bylo prováděno v období od 20. ledna do 18. března 2011. Dotazníkové šetření a vedlejší výzkumné šetření prováděné na pobočce ČSOB se uskutečnilo v období od 21. února do 18. března 2011. Výsledky z průzkumu byly poskytnuty pobočce ČSOB na Lannově třídě 3/11 v Českých Budějovicích a dále centrále ČSOB se sídlem Radlická 333/150 v Praze. Budou využity pro interní účely.

2.2.3 Charakteristika souboru

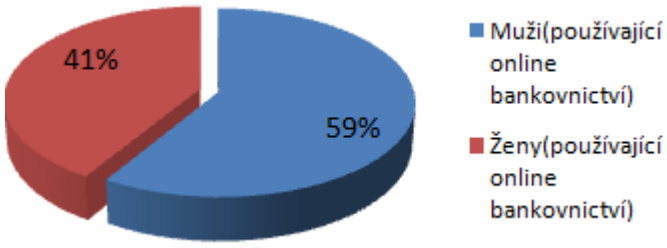
Plánovaný počet výzkumného souboru byl stanovený na 500 dotazovaných (100 prostřednictvím Google Docs, 400 osobním dotazováním). Plánovaný výzkumný soubor byl překročen a tvořilo jej celkem 600 dotazovaných (103 dotazovaných prostřednictvím aplikace Google Docs, 497 dotazovaných osobním dotazováním v pobočce ČSOB) bez ohledu na věkové kategorie a demografické údaje. Z celkového počtu 497 dotazovaným na pobočce ČSOB bylo položeno 46 dotazovaným pět doplňujících otázek vedlejšího výzkumu. Dotazovaní z vedlejšího výzkumu měli pouze jeden bankovní účet. Z výsledků hlavního průzkumu vyplývá, že byla převaha mužů nad ženami.

Tab. č. 1: Rozdělení dotazovaných dle pohlaví

Jaké je Vaše pohlaví?	**Počet** (Bez ohledu na používání online bankovnictví)	**Počet** (Používající online bankovnictví)	**Počet** (Nepoužívající online bankovnictví)
Muž	365	238	127
Žena	235	167	68

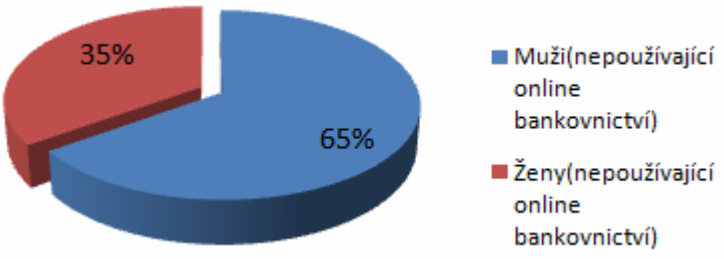
Tabulka ve druhém sloupci vystihuje rozdělení dotazovaných dle pohlaví bez ohledu, zdali používají nebo nepoužívají internetové bankovnictví.

Graf č. 1: Rozdělení dotazovaných dle pohlaví (používající online bankovnictví)



Z celkového počtu 405 (100%) dotazovaných, kteří používají služeb internetového bankovnictví, je počet mužů 238 (59%) a počet žen 167 (41%).

Graf č. 2: Rozdělení dotazovaných dle pohlaví (nepoužívající online bankovnictví)

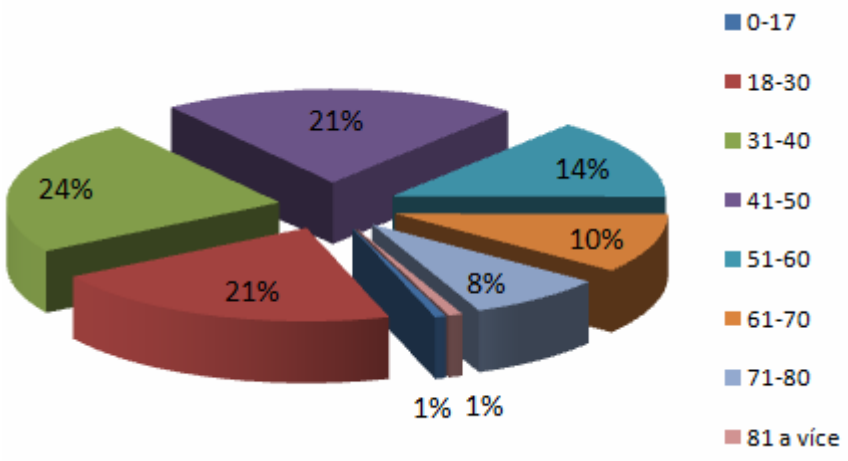


Z celkového počtu 195 (100%) dotazovaných, kteří nepoužívají služeb internetového bankovnictví, je počet mužů 127 (65%) a počet žen 68 (35%). Zejména je tento stav ovlivněn věkovými kategoriemi, kdy u mužů a žen, klesá zájem o používání moderních technologií.

Tab. č. 2: Věkové kategorie dotazovaných

Jaký je Váš věk?	**Počet**
0-17	4
18-30	127
31-40	142
41-50	127
51-60	84
61-70	62
71-80	49
81 a více	5

Graf č. 3: Věkové kategorie dotazovaných



Z celkového počtu 600 (100%) dotázaných byli 4 (1%) ve věku mezi 0 - 17 lety, ve věku 18-30 let bylo 127 (21%). Větší část tvořila věková kategorie mezi 31- 40 lety a to s počtem 142 (24%), zatímco věk mezi 41-50 lety měl shodný počet 127 (21%) jako kategorie 18-30 let. Menšího zastoupení byli dotazovaní ve věku 51 - 60 let v počtu 84 (14%), ve věku 61-70 v počtu 62 (10%). Věková kategorie 71-80 let byla zastoupena 49 (8%) respondenty. 81 a více let odpovědělo 5 (1%) dotázaných.

2.2.4 Výzkumné otázky

1. Využíváte online bankovnictví?
2. Jak často využíváte online bankovních služeb?
3. U jaké banky jste zákazníkem?
4. Z jakého důvodu používáte online bankovních služeb?
5. Setkal/a jste se někdy s kriminalitou v souvislosti s Vaším účtem?
6. Jak jste postupoval/a a s jakým výsledkem? (V případě, že se dotazovaný setkal s kriminalitou na účtu)
7. Považujete online bankovnictví za bezpečné?
8. Dáváte si při přihlášení ke službě online bankovnictví pozor na případná rizika?
9. Jaké zařízení pro online bankovnictví používáte?
10. Jaké pravidelně aktualizované prvky používáte pro osobní zabezpečení počítače?

11. Z jakého důvodu nepoužíváte online bankovnictví? (V případě, že dotazovaný nevyužíval online bankovnictví)

12. Jaké je Vaše pohlaví?

13. Jaký je Váš věk?

14. Místo Vašeho trvalého bydliště?

15. Z jakého kraje pocházíte?

2.2.5 Vedlejší výzkumné otázky

1. Čeho se nejvíce obáváte v internetovém bankovnictví?

2. Jak jste spokojen/a s poplatky za internetové bankovnictví?

3. Který poplatek považujete za „nesmyslný“ (v rámci internetového bankovnictví)?

4. Jakou změnu byste uvítal/a v internetovém bankovnictví?

5. U jaké banky jste zákazníkem?

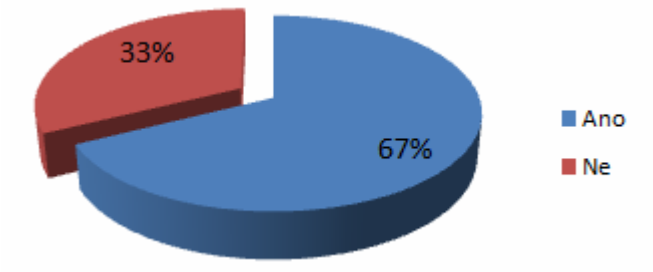
2.3 Výsledky výzkumu

Výsledky neodpovídají pořadí výzkumných otázek v dotazníku.

Tab. č. 3: Využití online bankovnictví

Využíváte online bankovnictví?	Počet
Ano	405
Ne	195

Graf č. 4: Využití online bankovnictví

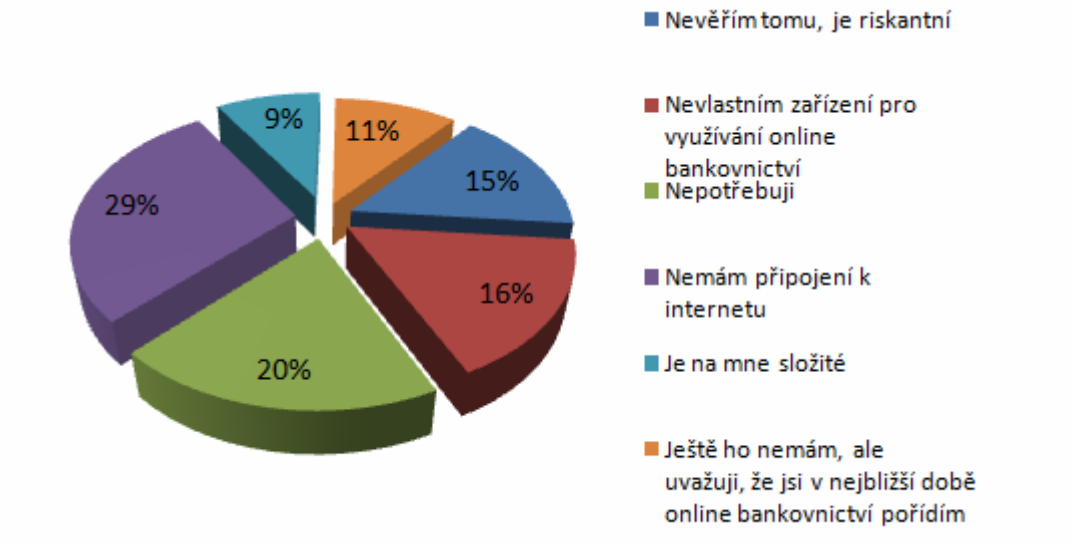


Z celkového počtu 600 (100%) dotazovaných je využíváno online bankovnictví u 405 (67%) případů. U 196 (33%) případů této služby není dotazovanými využíváno.

Tab. č. 4: Důvody nepoužití online bankovnictví

Z jakého důvodu nepoužíváte online bankovnictví? (V případě, že dotazovaný nevyužíval online bankovnictví)	**Počet**
Nevěřím tomu, je riskantní	30
Nevlastním zařízení pro využívání online bankovnictví	32
Jiné:	
Nepotřebuji	38
Nemám připojení k internetu	56
Je na mne složité	18
Ještě ho nemám, ale uvažuji, že si v nejbližší době online bankovnictví pořídím	21

Graf č. 5: Důvody nepoužívání online bankovnictví

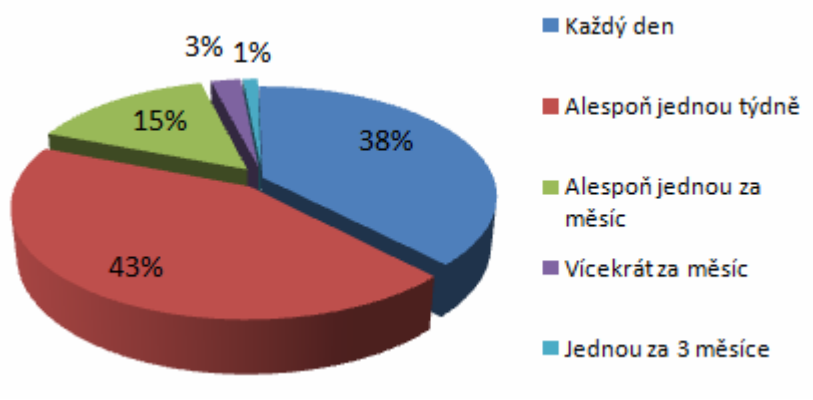


Z celkového počtu 196 (100%) dotazovaných, kteří nepoužívají online bankovnictví, má v tuto službu nedůvěru 30 (15%), 32 (16%) nevlastní zařízení pro využívání online bankovnictví. Dále jej 38 (20%) nemá potřebu jej používat a 56 (29%) nemá připojení k síti internet. 18 (9%) vypovědělo, že tato služba je zbytečně složitá. V počtu 21 (11%) případů uvažuje v nejbližší době o zřízení a používání online bankovnictví.

Tab. č. 5: Četnosti použití online bankovnictví

Jak často využíváte online bankovních služeb?	Počet
Každý den	154
Alespoň jednou týdně	175
Alespoň jednou za měsíc	61
Vícekrát za měsíc	10
Jednou za 3 měsíce	5

Graf č. 6: Četnosti použití online bankovnictví

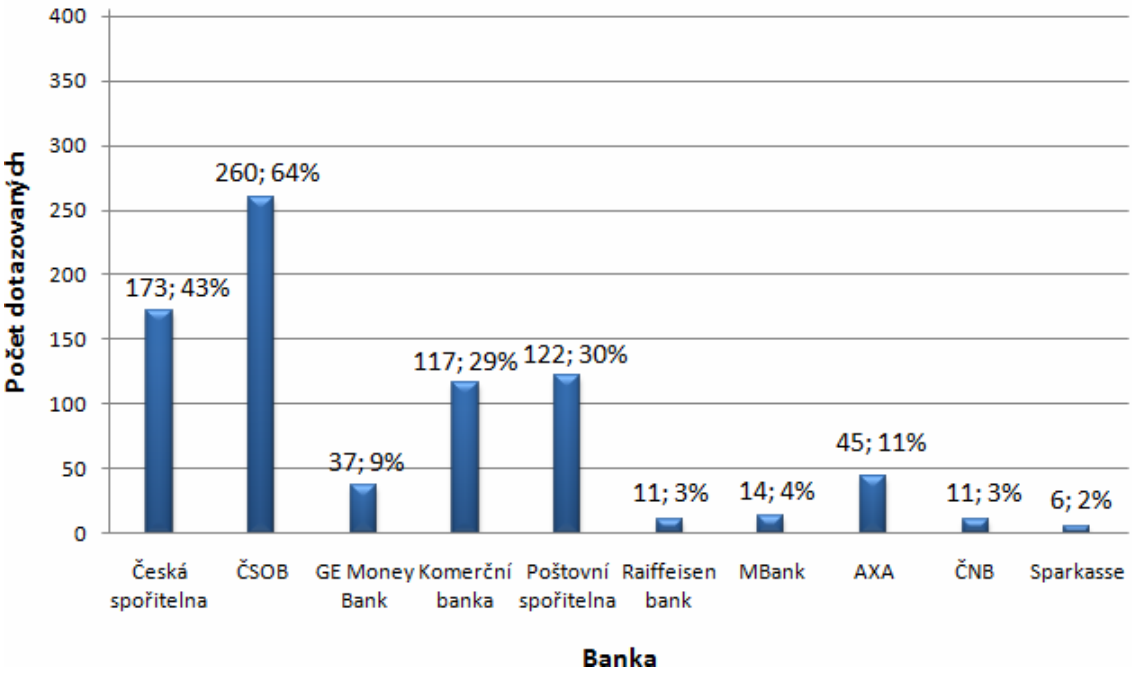


Z celkového počtu 405 (100%) dotazovaných, kteří používají online bankovnictví, používá 154 (38%) internetové bankovnictví každý den. Minimálně jednou týdně využívá 175 (43%), zatímco minimálně jednou za měsíc je využívá 61 (15%) dotazovaných. Vícekrát za měsíc je využito 10 (3%) uživateli a jednou za 3 měsíce používá 5 (1%) uživatelů.

Tab. č. 6: Využití jednotlivých bank

U jaké banky jste zákazníkem? (možno i více odpovědí)	**Počet**
Česká spořitelna	173
ČSOB	260
GE Money Bank	37
Komerční banka	117
Poštovní spořitelna	122
Raiffeisen bank	11
MBank	14
AXA	45
Jiné:	
ČNB	11
Sparkasse	6

Graf č. 7: Využití jednotlivých bank

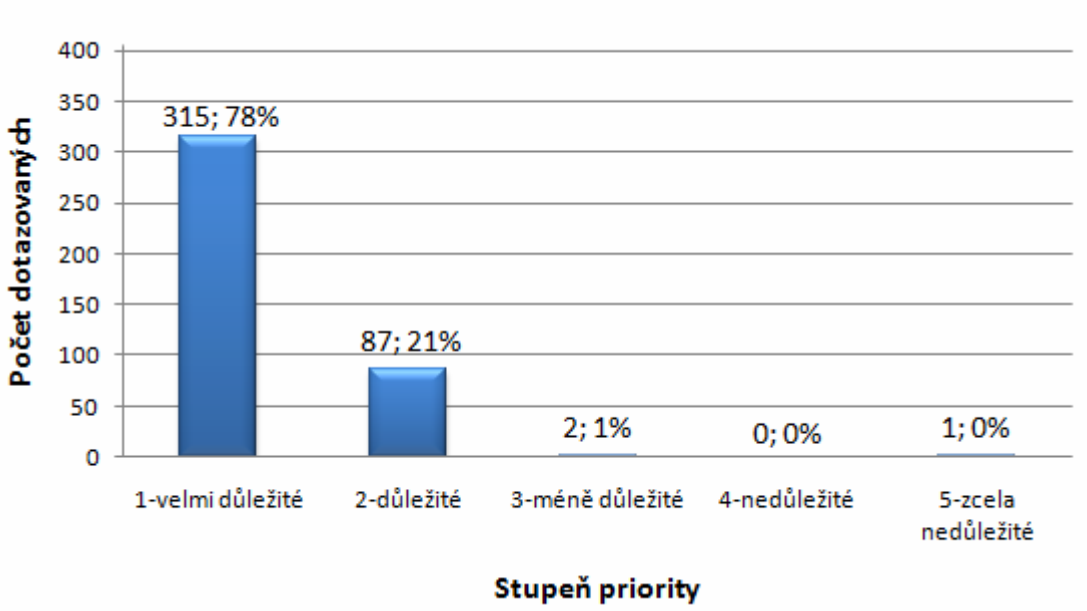


Z celkového počtu 405 (100%) dotazovaných, kteří používají internetové bankovnictví je Česká spořitelna využita ve 173 (43%) případech, ČSOB využívá 260 (64%). Dále GE Money Bank v 37 (9%) a Komerční banku používá 117 (29%). Poštovní spořitelnu označilo 122 (30%) případů. Raiffeisen banku používá 11 (3%), mBanku 14 (4%), AXA má poměr 45 (11%). Využití ČNB je vyčísleno na 11 (3%) a banka Sparkasse je využita pouze v počtu 6 (2%).

Tab. č. 7: Důležitost faktoru úspory času pro použití online bankovnictví

Z jakého důvodu používáte online bankovních služeb?(hodnoťte na škále jako při známkování ve škole důležitost jednotlivých důvodů, 1-velmi důležité, 5-zcela nedůležité)	**1 (velmi důležité)**	**2 (důležité)**	**3 (méně důležité)**	**4 (nedůležité)**	**5 (zcela nedůležité)**
Úspora času	315	87	2	0	1

Graf č. 8: Důležitost faktoru úspory času pro použití online bankovnictví

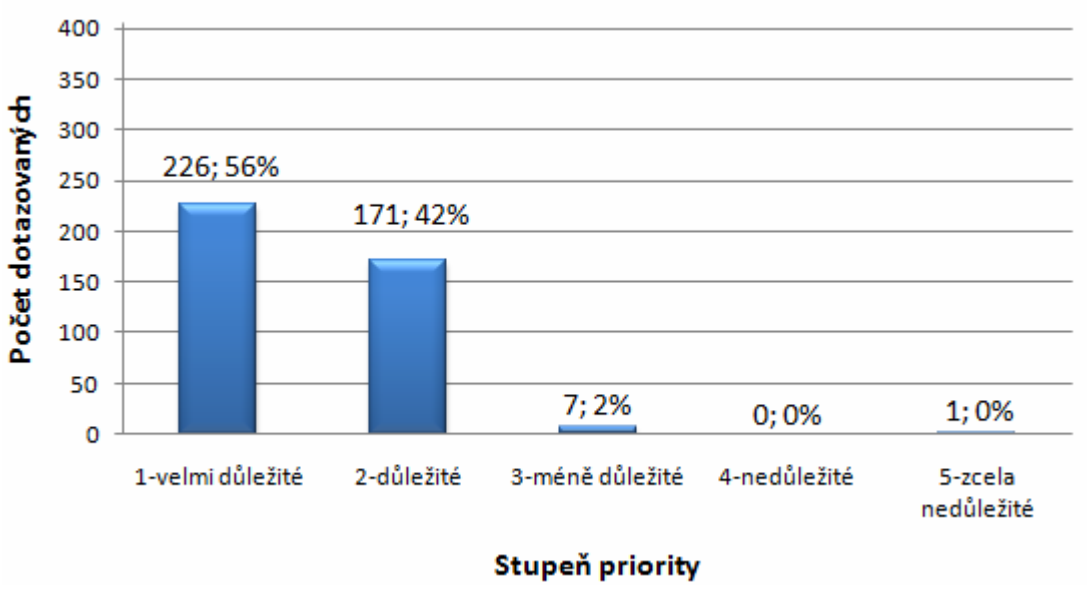


Z celkového počtu 405 (100%) jich odpovědělo 315 (78%), že úspory času při použití online bankovnictví jsou pro ně velmi důležité. Pro 87 (21%) je uspoření času oproti návštěvě přepážky důležité. Urychlení času je méně důležité pouze pro 2 (1%) dotazované, zatímco nedůležité nebylo pro žádného dotazovaného 0 (0%). Pro 1 (0%) se jevila úspora času jako zcela nedůležitá při používání této služby.

Tab. č. 8: Důležitost faktoru pohodlí pro použití online bankovnictví

Z jakého důvodu používáte online bankovních služeb?(hodnoťte na škále jako při známkování ve škole důležitost jednotlivých důvodů, 1-velmi důležité, 5-zcela nedůležité)	**1 (velmi důležité)**	**2 (důležité)**	**3 (méně důležité)**	**4 (nedůležité)**	**5 (zcela nedůležité)**
Pohodlí	226	171	7	0	1

Graf č. 9: Důležitost faktoru pohodlí pro použití online bankovnictví

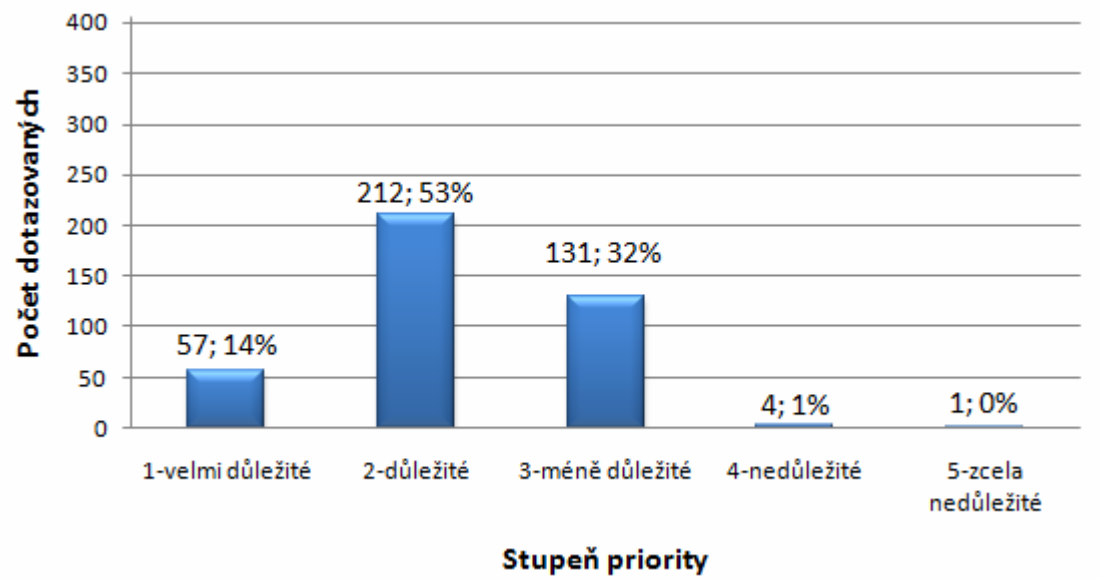


Z celkového počtu 405 (100%), kteří používají internetové bankovnictví, pohodlí při používání online bankovnictví označilo jako velmi důležité 226 (56%), pro 171 (42%) se jeví jako důležité. V 7 (2%) případech označili dotazovaní pohodlnost jako méně důležitý faktor pro používání této služby a v 1 (0%) případě bylo označeno pohodlí jako zcela nedůležité.

Tab. č. 9: Důležitost faktoru nižších poplatků pro použití online bankovnictví

Z jakého důvodu používáte online bankovních služeb?(hodnoťte na škále jako při známkování ve škole důležitost jednotlivých důvodů, 1-velmi důležité, 5-zcela nedůležité)	**1 (velmi důležité)**	**2 (důležité)**	**3 (méně důležité)**	**4 (nedůležité)**	**5 (zcela nedůležité)**
Nižší poplatky	57	212	131	4	1

Graf č. 10: Důležitost faktoru nižších poplatků pro použití online bankovnictví

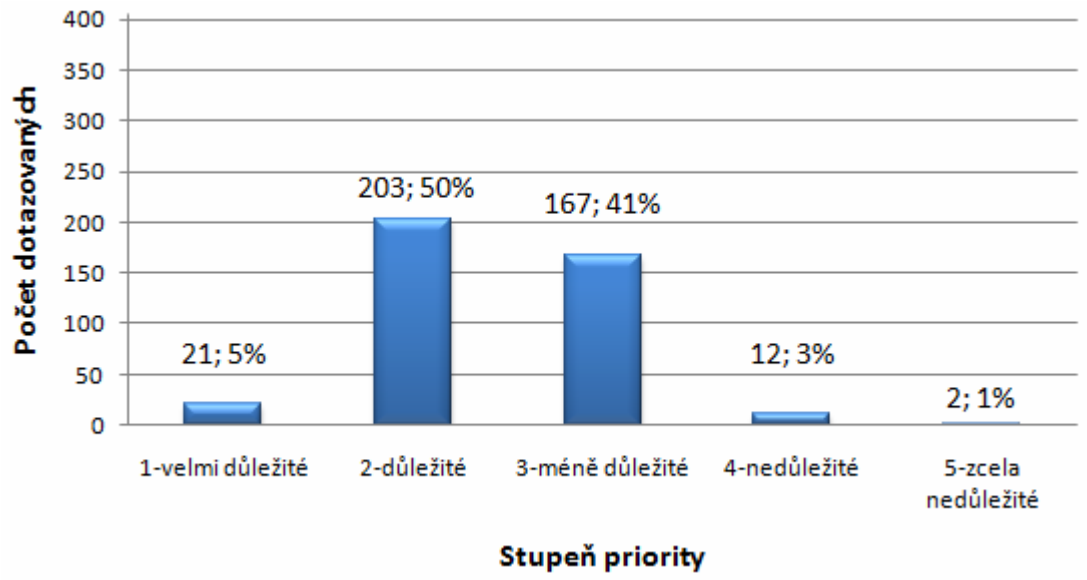


Z celkového počtu 405 (100%) se jeví nižší poplatky pro 57 (14%) jako velmi důležité. Váhu důležité přidělilo tomuto faktoru 212 (53%), méně důležité je pro 131 (32%). Nedůležité se zdá pro 4 (1%) dotazované a jako zcela nedůležité jej neoznačil žádný dotazovaný 0 (0%).

Tab. č. 10: Důležitost faktoru jednoduchosti a srozumitelnosti pro použití online bankovnictví

Z jakého důvodu používáte online bankovních služeb?(hodnoťte na škále jako při známkování ve škole důležitost jednotlivých důvodů, 1-velmi důležité, 5-zcela nedůležité)	**1 (velmi důležité)**	**2 (důležité)**	**3 (méně důležité)**	**4 (nedůležité)**	**5 (zcela nedůležité)**
Jednoduchost a srozumitelnost	21	203	167	12	2

Graf č. 11: Důležitost faktoru jednoduchosti a srozumitelnosti pro použití online bankovnictví

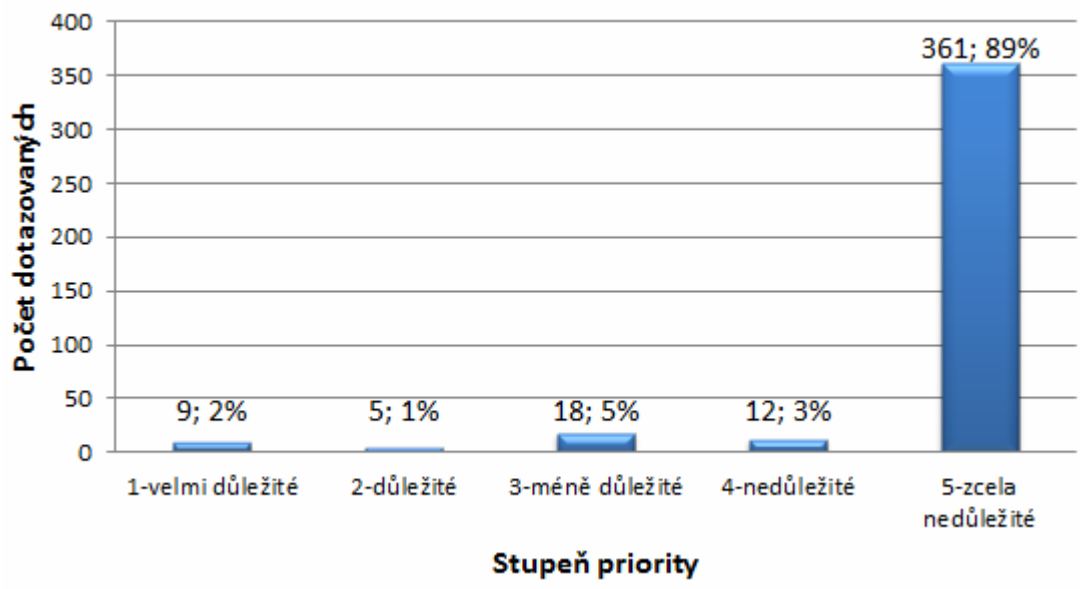


Z celkového počtu 405 (100%) je přívětivé v jednoduchosti a srozumitelnosti pro 21 (5%), kteří jej označili jako velmi důležitý faktor. Pro 203 (50%) je jednoduchost a srozumitelnost důležitá, naopak pro 167 (41%) je to méně důležité. Za nedůležitost v jednoduchosti a srozumitelnosti považuje 12 (3%) a za zcela nedůležité je považováno pouze ve 2 (1%) případech.

Tab. č. 11: Důležitost faktoru dostupnosti pobočky pro použití online bankovnictví

Z jakého důvodu používáte online bankovních služeb?(hodnoťte na škále jako při známkování ve škole důležitost jednotlivých důvodů, 1-velmi důležité, 5-zcela nedůležité)	**1 (velmi důležité)**	**2 (důležité)**	**3 (méně důležité)**	**4 (nedůležité)**	**5 (zcela nedůležité)**
Dostupnost pobočky	9	5	18	12	361

Graf č. 12: Důležitost faktoru dostupnosti pobočky pro použití online bankovnictví

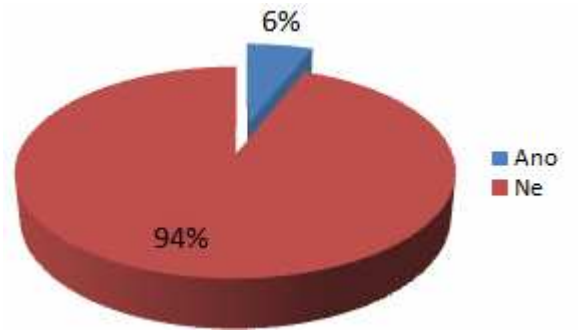


Z celkového počtu 405 (100%), kteří využívají internetové bankovnictví, je dostupnost pobočky banky za velmi důležitou považována v 9 (2%) případech. Důležité je prioritou pro 5 (1%) případů a méně důležité je považováno u 18 (5%). Za nedůležitou jej považují ve 12 (3%) případech a pro 361 (89%) se zdá jako zcela nedůležité.

Tab. č. 12: Četnost kriminality na účtu

Setkal/a jste se někdy s kriminalitou v souvislosti s Vaším účtem? (Kriminalitou je zde myšleno: odcizení finančních prostředků z účtu, krádeže přihlašovacích údajů, nevyžádané podvodné emailové zprávy žádající změnu přihlášovacích údajů)	**Počet**
Ano	24
Ne	381

Graf č. 13: Četnost kriminality na účtu

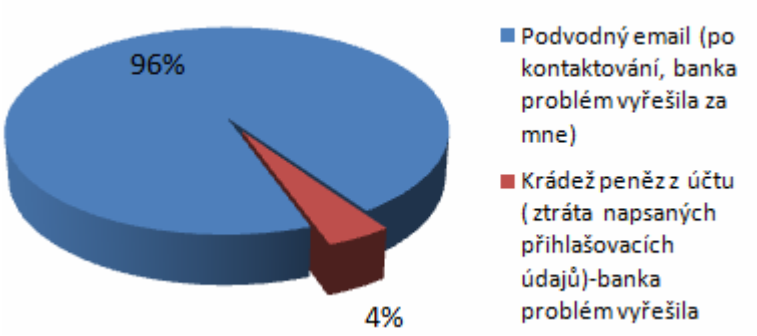


Z celkového počtu odpovědí 405 (100%) se setkalo s kriminalitou 24 (6%) uživatelů online bankovnictví. 381 (94%) uživatelů se s kriminalitou v souvislosti s jejich účtem nesetkalo.

Tab. č. 13: Postupy při setkání s kriminalitou (pouze v případě, že se uživatel s kriminalitou setkal)

Jak jste postupoval/a a s jakým výsledkem? (V případě, že dotazovaný se setkal s kriminalitou v souvislosti s jeho účtem)	**Počet**
Podvodný email (po kontaktování, banka problém vyřešila za mne)	23
Krádež peněz z účtu (ztráta napsaných přihlašovacích údajů) - banka problém vyřešila	1

Graf č. 14: Postupy při setkání s kriminalitou (pouze v případě, že se uživatel s kriminalitou setkal)



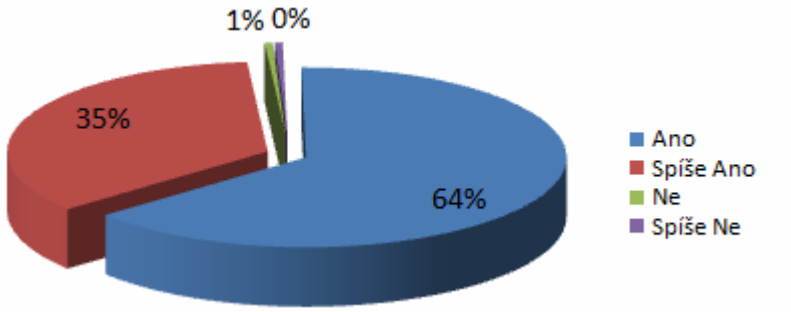
Z celkového počtu 24 (100%) se jednalo ve 23 (96%) případech o podvodné emaily, které však po kontaktování příslušné banky byly urychleně vyřízeny za uživatele. V 1 (4%) případě se jednalo o ztrátu finančních prostředků z účtu z důvodu neopatrnosti uživatele, který ztratil přihlašovací údaje na papírku, který měl uložen

ve své peněžence, banka opět problém řešila s uživatelem a vyřídila ho bezodkladně za uživatele.

Tab. č. 14: Úsudek o bezpečnosti online bankovnictví

Považujete online bankovnictví za bezpečné?	Počet
Ano	260
Spíše Ano	141
Ne	2
Spíše Ne	2

Graf č. 15: Úsudek o bezpečnosti online bankovnictví

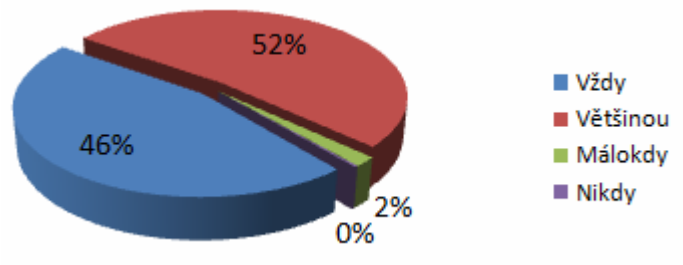


Z celkového počtu 405 (100%) považuje 260 (64%) online bankovnictví za bezpečné, 141 (35%) za téměř bezpečné. Pouze 2 (1%) uživatelé jej považují za nebezpečné a 2 (0%) za zcela nebezpečné.

Tab. č. 15: Četnost uvědomění rizik při přihlášení k online bankovnictví

Dáváte si při přihlášení ke službě online bankovnictví pozor na případná rizika? (Případnými riziky je myšleno:přesměrování na podvodnou stránku, odcizení přihlašovacích údajů, odcizení peněz z účtu)	**Počet**
Vždy	186
Většinou	211
Málokdy	7
Nikdy	1

Graf č. 16: Četnost uvědomění rizik při přihlášení k online bankovnictví

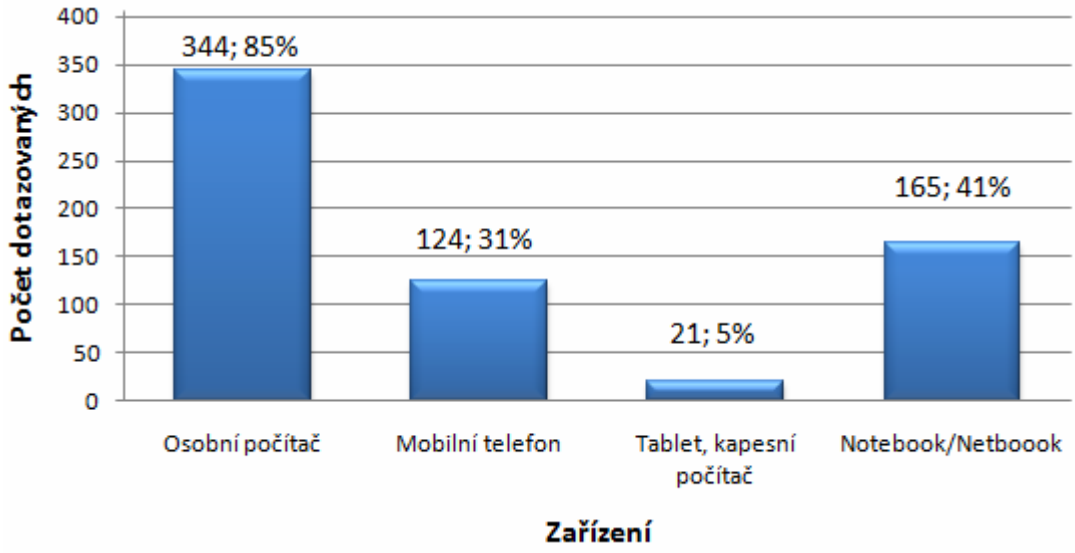


Z celkového počtu 405 (100%) si uvědomuje při přihlášení 186 (46%) uživatelů případná rizika vždy a většinou 211 (52%). Ti, kteří přemýšlí o případných rizicích při přihlášení málokdy, jsou vyjádřeni v počtu 7 (2%). Zatímco pouze 1 (0%) je neopatrný a případná rizika si neuvědomuje nikdy.

Tab. č. 16: Používané zařízení pro online bankovnictví

Jaké zařízení pro online bankovnictví používáte? (možno i více odpovědí)	**Počet**
Osobní počítač	344
Mobilní telefon	124
Tablet, kapesní počítač	21
Notebook/Netboook	165

Graf č. 17: Používané zařízení pro online bankovnictví

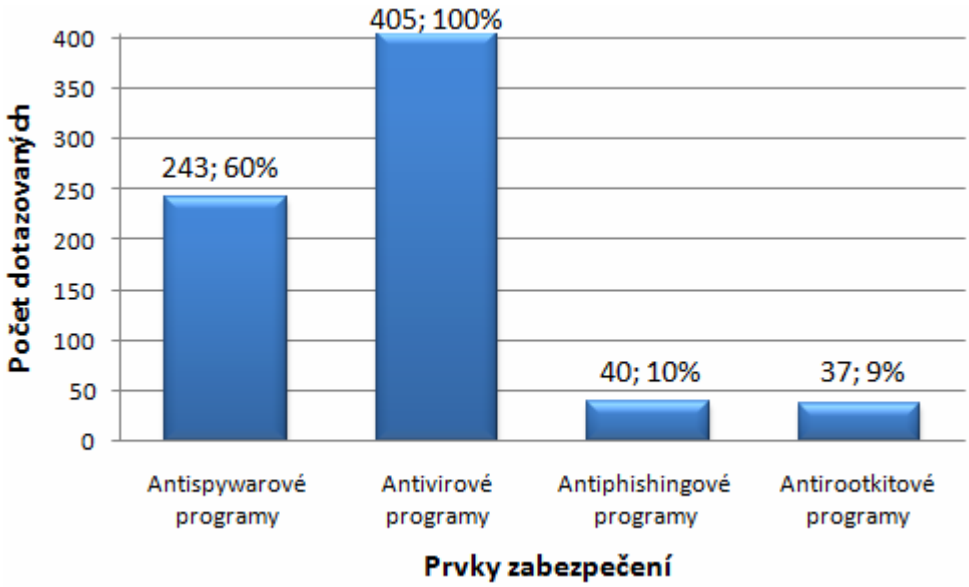


Z celkového počtu 405 (100%) dotazovaných, kteří využívají služeb internetového bankovnictví, je osobní počítač využíván v 344 (85%) případech, mobilní telefon ve 124 (31%). Dále tablet nebo kapesní počítač je využit ve 21 (5%) případech a notebook či netbook v 165 (41%) případech.

Tab. č. 17: Používané pravidelně aktualizované prvky zabezpečení pro online bankovnictví

Jaké pravidelně aktualizované prvky používáte pro osobní zabezpečení počítače? (možno více odpovědí)	**Počet**
Antispywarové programy (SpyBot, SuperAntispyware, Spy Emergency, Spyware Terminator, Ad-Aware, Norton Antivirus...)	243
Antivirové programy (Avast, AVG, ESET NOD 32,Kaspersky Anti-Virus, F-Secure, Panda Antivirus, Norton Antivirus....)	405
Antiphishingové programy (ESET NOD 32, G DATA Antivirus, Norton Antivirus....)	40
Antirootkitové programy (Panda Antirootkit, SysProt AntiRootkit, AVG AntiRootkit....)	37

Graf č. 18: Používané pravidelně aktualizované prvky zabezpečení pro online bankovnictví

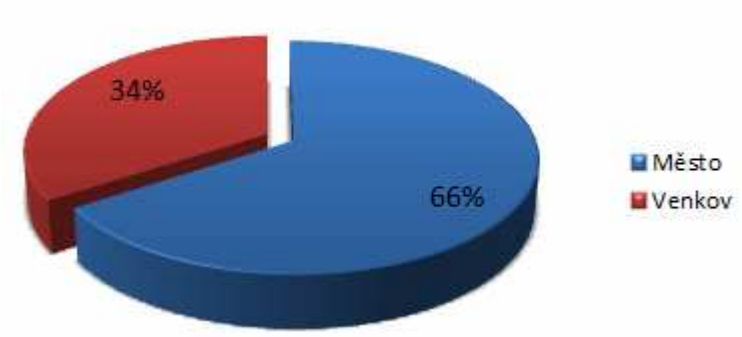


Z celkového počtu 405 (100%) uživatelů používajících online bankovnictví jsou antispywarové programy použity ve 243 (60%) případech, antivirové programy ve 405 (100%). Další nezbytnou ochranou jsou antiphishingové programy, které jsou využity ve 40 (10%) případech a antirootkitové programy v 37 (9%).

Tab. č. 18: Dotazovaní dle původu trvalého bydliště

Místo Vašeho trvalého bydliště?	Počet
Město	395
Venkov	205

Graf č. 19: Dotazovaní dle původu trvalého bydliště

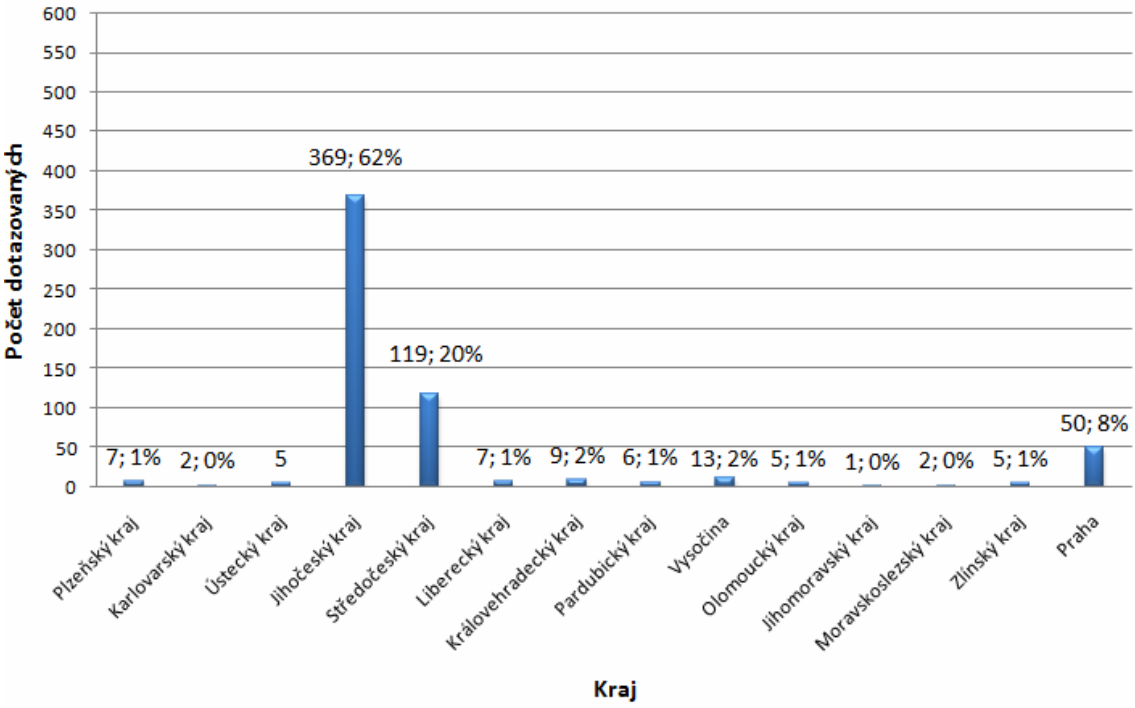


Z celkového počtu všech 600 (100%) respondentů, pocházelo 395 (66%) dotázaných z města. Z venkova pocházelo 205 (34%) dotázaných.

Tab. č. 19: Dotazovaní dle krajů

Z jakého kraje pocházíte?	Počet
Plzeňský kraj	7
Karlovarský kraj	2
Ústecký kraj	5
Jihočeský kraj	369
Středočeský kraj	119
Liberecký kraj	7
Královehradecký kraj	9
Pardubický kraj	6
Vysočina	13
Olomoucký kraj	5
Jihomoravský kraj	1
Moravskoslezský kraj	2
Zlínský kraj	5
Praha	50

Graf č. 20: Dotazovaní dle krajů



Z celkového počtu 600 (100%) všech dotazovaných, pocházelo z Plzeňského kraje 7 (1%) dotazovaných. Z Karlovarského kraje pocházely 2 (0%) dotazovaní a z Ústeckého kraje 5 (1%). Převahu měl Jihočeský kraj, kde bylo 369 (62%) respondentů a Středočeský kraj zaujímal druhé místo v počtu 119 (20%) dotázaných. Z Libereckého kraje bylo dotázáno 7 (1%), z Královehradeckého kraje 9 (2%), Pardubického kraje 6 (1%). Vysočina byla v počtu 13 (2%) dotazovaných, Olomoucký kraj v 5 (1%), z Jihomoravského kraje pocházel pouze 1 (0%) respondent. V Moravskoslezský kraj odpověděli 2 (0%) dotázaní, ve Zlínském kraji 5 (1%) a v Praze 50 (8%).

3. Vyhodnocení online výzkumu

Cílem v prováděném hlavním výzkumném šetření bylo zjistit, zdali dotazovaní využívají služeb internetového bankovnictví či nikoliv, v případě, že jej využívají, jim byly pokládány otázky četnosti využití, důvody obliby internetového bankovnictví, bankovní instituce, kterých využívají a jaké prvky používají pro spojení s těmito službami. Nedílnou součástí bylo také zjištění, jak jsou obezřetní v jejich používání. Dále od respondentů, kteří používají online bankovnictví či nikoliv byly zjišťovány demografické údaje, jakého jsou pohlaví, věkové kategorie, z jakého kraje pocházejí a zdali jsou z města či venkova.

U uživatelů, kteří nepoužívali internetové bankovnictví, byl zjišťován důvod jejich jednání. Otázka v dotazníku byla polouzavřená, proto zde mohl respondent v případě nevybrání nabízených možností uvést vlastní názor a na jeho základě jsem mohl stanovit i případné alternativy.

K hypotéze 1: Online bankovnictví využívá více než 60% dotazovaných, což v dotazníku vysvětluje výzkumná otázka (Využíváte online bankovnictví?). Frimmel v průzkumu Zkušenosti s elektronickým bankovnictvím zjistil, že ze 141 respondentů internetového bankovnictví jej využívá 124 (99,2%) případů a zbytková procenta připadala na ostatní služby elektronického bankovnictví **[12]**. V mém průzkumu odpovídalo celkem 600 dotazovaných a ve 405 (67%) případech je této služby respondenty využíváno.

Hypotéza 1**:** Online bankovnictví využívá více než 60% dotazovaných, byla proto potvrzena.

K hypotéze 2: 60% dotazovaných, kteří používají internetové bankovnictví si myslí, že online bankovnictví je bezpečné. V dotazníku jej vysvětluje výzkumná otázka (Považujete online bankovnictví za bezpečné?). Z výzkumného šetření, které jsem provedl, vyšlo, že z celkového počtu 405 (100%) respondentů považuje 260 (64%) online bankovnictví za bezpečné a 141 (35%) za téměř bezpečné. Průzkum dle Frimmela **[12]** uvádí problematiku bezpečnosti v otázce (Jak jste spokojen(a) se zabezpečením elektronického bankovnictví?), kde z celkového počtu

125 (100%) bylo označeno jako výborné v 51 (40.8%) případech. Tohoto výsledku Frimmel **[12]** ve svém výzkumu dosáhl pravděpodobně na základě menšího počtu dotazovaných respondentů.

Hypotéza 2**:** 60% dotazovaných, kteří používají internetové bankovnictví si myslí, že online bankovnictví je bezpečné, byla proto potvrzena.

K hypotéze 3: Osobní počítač je v 70% nejpoužívanějším zařízením pro přihlášení do služeb online bankovnictví. V dotazníku jej vysvětluje výzkumná otázka (Jaké zařízení pro online bankovnictví používáte?). Z celkového počtu 405 (100%) dotazovaných, kteří využívají služeb internetového bankovnictví, je osobní počítač využit v 342 (85%) případech.

Hypotéza 3**:** Osobní počítač je v 70% nejpoužívanějším zařízením pro přihlášení do služeb online bankovnictví, byla potvrzena.

K hypotéze 4: Dotazovaní, kteří používají online bankovnictví, mají z 80% zajištěno zabezpečení osobního zařízení. V dotazníku jej vysvětluje výzkumná otázka (Jaké pravidelně aktualizované prvky používáte pro osobní zabezpečení počítače?). Z celkového počtu 405 (100%) respondentů, používajících online bankovnictví, používají všichni dotazovaní určitý prvek zabezpečení. Antispywarový program používá 243 (60%) případů, antivirový program každý dotázaný využívající služeb internetového bankovnictví tedy 405 (100%). Antiphisingový program je využit ve 40 (10%) případech a antirootkitový program v 37 (9%).

Hypotéza 4**:** Dotazovaní, kteří používají online bankovnictví, mají z 80% zajištěno zabezpečení osobního zařízení, byla potvrzena.

3.1 Diskuse

Dle osobního zjištění je internetové bankovnictví využíváno zejména mladými lidmi a lidmi ve středním věku. Dle mého průzkumu nejčastěji jej využívají věkové kategorie (18-30 let, 31-40let, 41-50 let). V porovnání s průzkumem Zkušenosti s elektronickým bankovnictvím **[12]**, kde věkové kategorie od 21 do 30 let a od 31 do 45let mají největší četnost. S postupně rostoucím věkem od 51 let dle mého průzkumu a od 46let dle průzkumu Frimmela **[12]** je o tyto služby klesající

zájem, což je způsobeno podle výsledků mého průzkumů, počítačovou způsobilostí, nevlastněním připojení k internetu či nepotřebností těchto služeb a částečnou roli zde hrají i obavy a nedůvěra.

Dle Frimmela **[12]** v průzkumu není řešena otázka četnosti použití online bankovnictví za den, týden, měsíc či více měsíců, ale vystihuje zde četnost použití v letech, kde z celkového počtu 125 (100%), jej déle než 5 let používá 66 (52,8%) uživatelů, od 1 roku do 3 let 29 (23,2%) dotázaných, zatímco od 4 let do 5 let 26 (20,8%) a do 1 roku 4 (3,2%) dotázaní.

Z celkového počtu mých 405 (100%) dotazovaných, kteří používají online bankovnictví, používá 154 (38%) internetové bankovnictví každý den. Zde se ukazuje ona výhoda přístupu 24h denně, 7dní v týdnu, 365 dní v roce. Minimálně jednou týdně využívá 175 (43%), zatímco minimálně jednou za měsíc je využívá 61 (15%) dotazovaných. Vícekrát za měsíc je využito 10 (3%) uživateli a jednou za 3 měsíce používá 5 (1%) uživatelů, kteří zejména kontrolují převážně stav svého účtu.

Důležitost jednotlivých faktorů pro použití služeb online bankovnictví hraje také významnou roli, průzkumy byly shodné v možnostech nabízených odpovědí (úspora času, pohodlí, dostupnost pobočky) a u průzkumu Online bankovnictví a spotřebitelé byly dále nabízeny další možnosti nižších poplatků, jednoduchosti a srozumitelnosti, které plnily funkci odpovědi jiné v průzkumu dle Frimmela **[12]**. Jako hlavní prioritu považují dotázaní v průzkumu „ Zkušenosti s elektronickým bankovnictvím “ **[12]** pohodlnost, a to v počtu 112 (89,6%) případů ze 125 (100%) uživatelů online bankovnictví, na rozdíl od mého průzkumu, kde bylo zjištěno, že pohodlí je velmi důležitým faktorem pro 226 (56%) případů ze 405(100%) uživatelů, kteří používají internetové bankovnictví. Z čehož lze usuzovat, že internetové bankovnictví přináší, jistou velmi významnou výhodu oproti návštěvě pobočky.

4. Návrhy opatření a doporučení

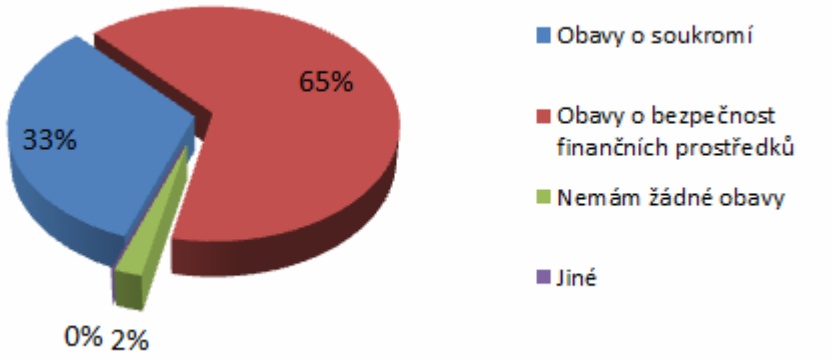
4.1 Obecné doporučení pro banky

Na základě výzkumu z doplňujících otázek vedlejšího výzkumu (viz. Příloha č. 4) jsem zjistil, že obecně banky nevzbuzují u populace internetového bankovnictví dojem z bezpečné služby. Obavy z bezpečnosti vycházejí ze zkušeností uživatelů – čemu nerozumí, toho se bojí.

Tab. č. 20: Obavy z internetového bankovnictví

Čeho se nejvíce obáváte v internetovém bankovnictví?	Počet
Obavy o soukromí	15
Obavy o bezpečnost finančních prostředků	30
Nemám žádné obavy	1
Jiné	0

Graf č. 21: Obavy z internetového bankovnictví



Z celkového počtu 46 (100%) respondentů, kteří odpověděli na doplňující otázky, má obavy o soukromí 15 (33%) dotázaných. Obavy o bezpečnost finančních prostředků uvedlo 30 (65%) respondentů. Žádné obavy nemá pouze 1 (2%) respondent. V případě jiných obav neodpověděl nikdo, tedy 0 (0%).

Návrh: Stálo by za úvahu zvážit zdali by banky neměly v základních službách poskytovat kvalitnější zabezpečení a více informovat uživatele. Doporučením by bylo také poskytovat uživateli licence antivirových balíčků v rámci internetového

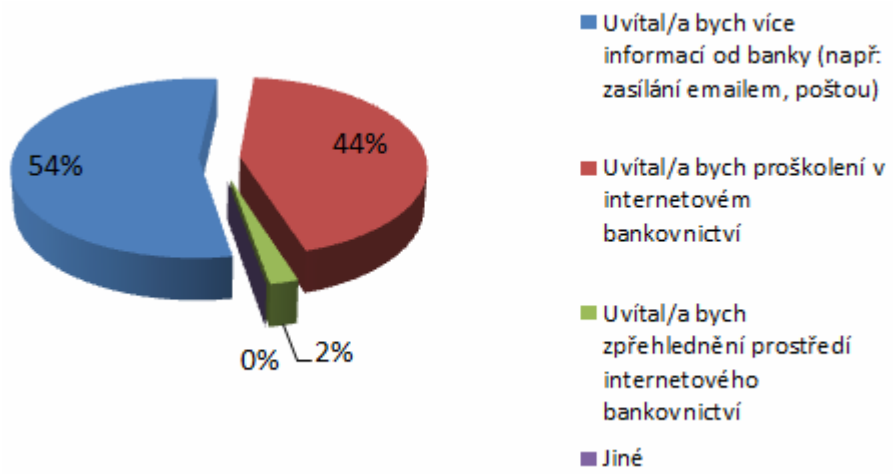
bankovnictví zdarma. U uživatelů a potencionálních zákazníků by tak byl možná vzbuzen dojem většího bezpečí.

Vyjdeme-li z výsledků vedlejšího průzkumu, navrhovanou změnou dotázanými je prioritně komunikace. Komunikace mezi uživatelem a bankou je důležitá. Informovanost uživatelů o nových prvcích zabezpečení, novinkách v oblasti internetového bankovnictví by byla žádoucí na všech pobočkách bank.

Tab. č. 21: Navrhované změny v internetovém bankovnictví dle uživatelů

Jakou změnu byste uvítal/a v internetovém bankovnictví?	**Počet**
Uvítal/a bych více informací od banky (např: zasílání emailem, poštou)	25
Uvítal/a bych proškolení v internetovém bankovnictví	20
Uvítal/a bych zpřehlednění prostředí internetového bankovnictví	1
Jiné	0

Graf č. 22: Navrhované změny v internetovém bankovnictví dle uživatelů



Z celkového počtu 46 (100%) respondentů, kteří odpověděli na doplňující otázky, by uvítalo zasílání bankovních informací 25 (54%) dotázaných. Proškolení v internetovém bankovnictví by uvítalo 20 (44%) respondentů. Zpřehlednění prostředí internetového bankovnictví uvedl pouze 1 (2%) dotázaný. Jiné navrhované změny nebyly zodpovězeny, tedy 0 (0%).

Návrh: Myslím si, že dotázaní by uvítali více informací od banky. Stálo by za zvážení, hromadné rozesílání bankovních informací na emailové schránky uživatelů či poštou.

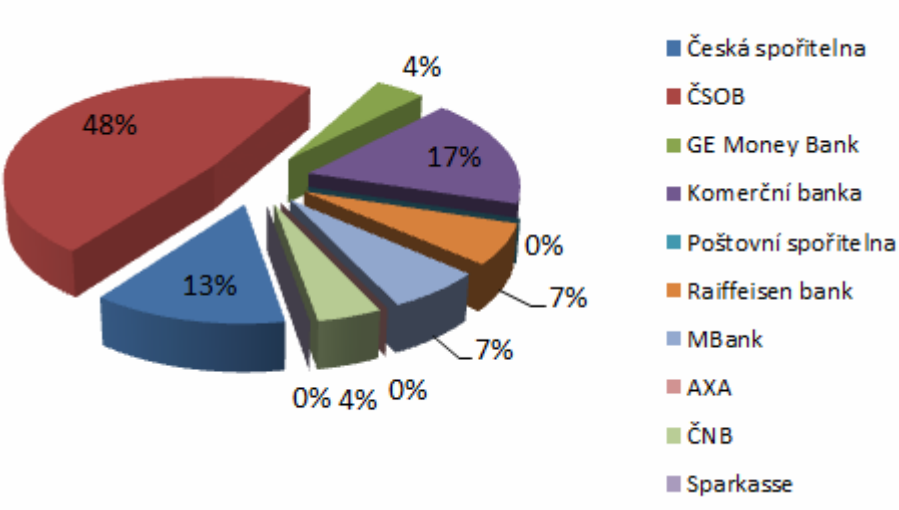
4.2 Doporučení pro pobočku banky ČSOB v Českých Budějovicích

Při návrzích na doporučení pro pobočku ČSOB na Lannově třídě v Českých Budějovicích jsem vycházel z doplňujících otázek vedlejšího výzkumu.

Tab. č. 22: Dotazovaní dle banky – vedlejší průzkum

U jaké banky jste zákazníkem?	Počet
Česká spořitelna	6
ČSOB	22
GE Money Bank	2
Komerční banka	8
Poštovní spořitelna	0
Raiffeisen bank	3
MBank	3
AXA	0
ČNB	2
Sparkasse	0

Graf č. 23: Dotazovaní dle banky – vedlejší průzkum

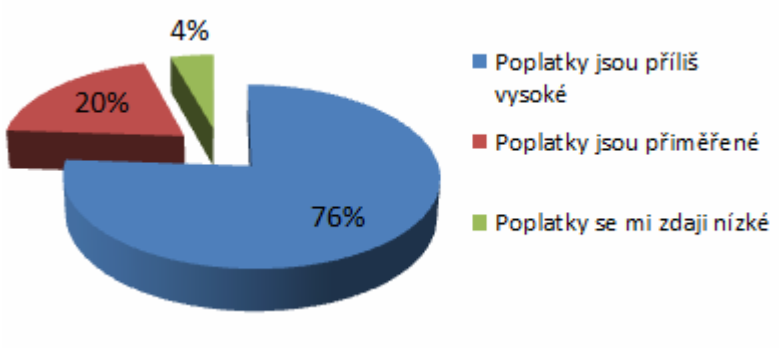


Z celkového počtu 46 (100%) respondentů, kteří odpověděli na doplňující otázky, uvedlo 22 (48%) dotázaných ČSOB jako svou banku. Lze na tomto základě stanovit případná doporučení pro pobočku ČSOB v Českých Budějovicích.

Tab. č. 23: Spokojenost s poplatky internetového bankovnictví

Jak jste spokojen/a s poplatky za internetové bankovnictví?	**Počet**
Poplatky jsou příliš vysoké	35
Poplatky jsou přiměřené	9
Poplatky se mi zdají nízké	2

Graf č. 24: Spokojenost s poplatky internetového bankovnictví



Zjištěním různých názorů při dotazování jsem dospěl k výsledku, že z celkového počtu 46 (100%) respondentů, kteří odpověděli na doplňující otázky, uvedlo 35 (76%) respondentů bankovní poplatky jako příliš vysoké. Faktory, které naopak nutí platit tyto poplatky, bych shrnul do dvou základních skupin.

1.skupina – online bankovnictví je typické, zejména svým pohodlným charakterem, které většina lidí využívá pro usnadnění svého života. Ve většině případů, vše, co děláme v našem životě si chceme, co nejvíce usnadnit a právě faktory, které toto usnadnění nesou, přinášejí jisté náklady navíc. Proto jsme si ochotni za určité služby připlatit i přes náš nesouhlas.

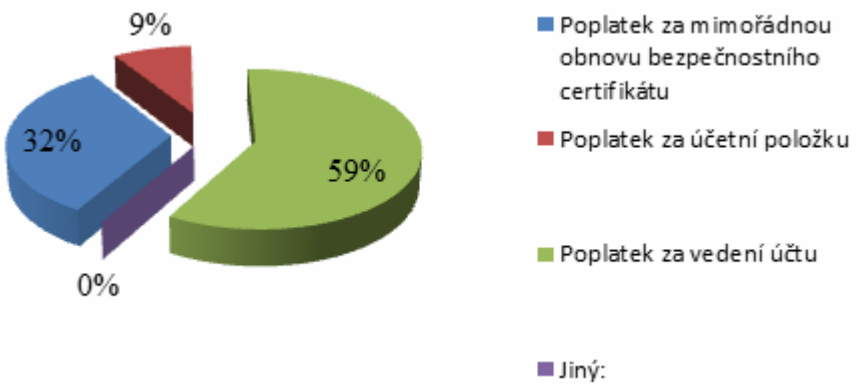
2.skupina – žijeme ve světě, který se přizpůsobuje moderním technologiím a projevuje se to i na uživatelích. Slovo být „in“ vyjadřuje uživatele, který i přes částečnou nepotřebnost využívá kupříkladu platby kartou, využívá internetového bankovnictví, má zřízen bankovní účet, který už se již dnes stal jistou samozřejmostí i v zaměstnání pro vyplacení mezd.

Vezmeme-li v potaz výše uvedené skupiny, výše poplatků má své opodstatnění. Ale chtěl bych poukázat na existenci tzv. „nesmyslných poplatků“.

Tab. č. 24: Nesmyslné bankovní poplatky dle uživatelů

Který poplatek považujete za nesmyslný (v rámci internetového bankovnictví)?	Počet
Poplatek za mimořádnou obnovu bezpečnostního certifikátu	19
Poplatek za účetní položku	4
Poplatek za vedení účtu	23
Jiný	0

Graf č. 25: Nesmyslné bankovní poplatky dle uživatelů



Z celkového počtu 46 (100%) respondentů, kteří odpověděli na doplňující otázky, uvedlo 23 (59%) dotázaných jako nesmyslný, poplatek za vedení účtu. Dle tvrzení dotázaných je příliš vysoký a v poskytovaných službách se nijak tento výdaj neprojevuje. Dále je zde poplatek za mimořádnou obnovu bezpečnostního certifikátu, který uvedlo 19 (32%) dotázaných.

Návrh: Osobně bych navrhoval, aby banka u poplatku za mimořádnou obnovu bezpečnostního certifikátu a poplatku za vedení účtu uvažovala o jejich snížení.

Za povšimnutí stojí také důležitý fakt, že dotázaní by uvítali na pobočce ČSOB na Lannově třídě v Českých Budějovicích proškolování v internetovém bankovnictví. Vyplývá to z výsledků mého vedlejšího výzkumu, kdy vycházím z tab. č. 21 a grafu č. 22. Návrh pro pobočku ČSOB uvádím na základě tab. č. 22 a grafu č. 23.

V prostorách banky se nacházejí zasedací místnosti, kde probíhají porady a školení zaměstnanců. Většina poradenských služeb je na pobočce řešena v rámci

osobních bankéřů, kteří dle mého názoru na přepážce nemají dostatek času věnovat se zákazníkovi potřebný čas, který by vyžadoval. Tyto služby jsou poskytovány také formou online, což dle mého názoru nenahradí osobní komunikaci a zcela nepokryje dotazy od zákazníků. Samostatná služba poradenství a školení v internetovém bankovnictví se na pobočce nenachází.

Návrh: Proto bych navrhoval zřízení samostatné služby v oblasti poradenských služeb a školení v zázemí internetového bankovnictví. Pobočka banky disponuje zasedací místností pro porady, která je vybavena jak technikou, tak i kapacitním prostorem. V ní by mohly probíhat právě ony poradenské služby a školení a v následném ekonomickém zhodnocení bylo toho využito.

Poradenské služby a školení by prováděli na pobočce 4 zaměstnanci (2 pro fyzické osoby a 2 pro podnikatelské osoby). V ekonomickém zhodnocení a návrhu se zejména budu věnovat fyzickým osobám. Náplní práce poradenských služeb na pobočce by bylo školení uživatelů internetového bankovnictví, které by probíhalo vždy dvakrát za 14 dní po dobu 2 hodin. Zde by školicí zaměstnanec provedl názorné ukázky přihlášení do služby a základních funkcí internetového bankovnictví, další část školení by byla věnována dotazům a připomínkám uživatelů. Školicí pracovníci by byly proškolováni v rámci školení, které by v bance probíhalo vždy dvakrát v týdnu a byla by tak zajištěna jejich pracovní způsobilost. Mimo školení by zaměstnanec byl k dispozici na pobočce pro případné řešení problémů s internetovým bankovnictvím a poskytoval by rady v dané problematice. Zaměstnanec, který by vyjel do terénu, by měl v náplni práce řešení případných problémů s nastavením internetového bankovnictví a také by na domluvených služebních schůzkách poskytoval veškerou pomoc, jako pracovník na pobočce.

Zaměstnancům by byl poskytnut služební automobil značky ŠKODA Fabia Classic START 1.2 TSI, pro služební schůzky s klienty do okruhu 20km od pobočky banky. Jeden ze 2 zaměstnanců by působil přímo na pobočce. Pracovní doba těchto zaměstnanců by byla v době od 9 - 17h, tedy 8 hodinová pracovní doba.

Takto vynaložené náklady by byly pro banku jistým navýšením, ale myslím si, že zřízení služby přinese kladné výsledky.

4.3 Ekonomické zhodnocení

Vše je ve fixních nákladech.

Náklady na zaměstnance

Tabulka 25 Náklady za 1 měsíc (poradenské služby přímo na pobočce)

Název položky mzdy	Sazba	Hodiny	Částka
Měsíční mzda		160	19 000
Odměna			1 000
Pojistné na sociální zabezpečení zaměstnavatel	25 % z 20 000		5 000
Pojistné na zdravotní pojištění zaměstnavatel	9 % z 20 000		1 800
Reálné náklady banky:			**26 800 Kč**

Tab. č. 26: Náklady za 1 měsíc (poradenské služby v terénu)

Název položky mzdy	Sazba	Hodiny	Částka
Měsíční mzda		160	20 000
Odměna			1 000
Pojistné na sociální zabezpečení zaměstnavatel	25 % z 21 000		5 250
Pojistné na zdravotní pojištění zaměstnavatel	9 % z 21 000		1 890
Reálné náklady banky:			**28 140 Kč**

Služební automobil

Byl zakoupen automobil ŠKODA Fabia Classic START 1.2 TSI za cenu **200 000 Kč bez DPH [4]**.

Doba odpisování je 5 let, roční odpisy by činily 200 000/5 = 40 000 Kč

Měsíční odpisy by činily 40 000/12 = **3 333 Kč bez DPH**

Měsíčně by automobil najel průměrných 500 km a cena nafty je 33 Kč/l

Průměrná spotřeba tohoto automobilu činí 5,2 l/100 km **[4]**.

Náklady za pohonné hmoty (měsíčně) = (5,2 x 5) x 33 = 858 Kč s DPH **= 687 Kč bez DPH**

Povinné ručení

Technické parametry vozidla byly zadány do kalkulačky výpočtu povinného ručení a s využitím povinného ručení u ČSOB Pojišťovny by činila roční výše na 4 401 Kč s DPH **[8]**.

V případě měsíční výše splátky = 367 Kč s DPH = **294 Kč bez DPH**

Havarijní pojištění

Technické parametry byly zadány do kalkulačky výpočtu havarijního pojištění **[38]**. V případě zvoleného povinného ručení od ČSOB bylo zvoleno havarijní pojištění od téže banky.

Částka havarijního pojištění ČSOB Dominant s krytím 60/60 mil. Kč činí 5 025 Kč jako roční pojistné.

Měsíční pojistné by činilo 5 025/12 = 419 Kč s DPH **= 336 Kč bez DPH**

Ostatní náklady

Náklady na tisk + toner do tiskárny (měsíčně) = **2 000Kč bez DPH**

Náklady na údržbu vozidla + případné opravy (měsíčně) = **1 000 Kč bez DPH**

Měsíční provozní náklady banky:

Náklady na zaměstnance včetně odměn + měsíční odpisy automobilu + náklady na pohonné hmoty + povinné ručení + havarijní pojištění + ostatní náklady = (26 800 + 28 140) + (3333 + 687 + 294 + 336) + (2 000 + 1 000) = **62 590 Kč**

Závěr

Cílem mé bakalářské práce bylo zhodnotit využívání internetových bankovních účtů mezi spotřebiteli a zjistit jejich pozitiva a negativa. Na základě analýzy a sběru dat formou online dotazování zhodnotit a navrhnout případná opatření pro zlepšení služeb v oblasti internetového bankovnictví. Cíl byl splněn.

Z výsledků šetření, které probíhalo formou online dotazování, prostřednictvím služby Google Docs a osobním dotazováním na pobočce ČSOB na Lannově třídě 3/11 v Českých Budějovicích, jsem dosáhl výsledku, že internetové bankovnictví je využíváno u 67% (405) uživatelů z celkového počtu 100% (600). Je zde viditelné, že online bankovnictví má svou působnost na poli bankovních služeb a je uživateli využíváno. Z tvrzení dotázaných z vedlejšího výzkumu jsem také zjistil nespokojenost s bankovními poplatky, resp. označovaných jako „nesmyslné poplatky“. Osobně si myslím, že pokud si bankovní instituce chtějí udržet stávající zákazníky a přivádět nové zákazníky, měly by provést kroky, které by jim je pomohly udržet a přilákat. Osobně jsem v návrzích uvedl krok, který by mohl pomoci. Eliminují-li se negativní stránky, osobně si myslím, že využití internetového bankovnictví bude narůstat s postupem času.

33% (195) uživatelů z celkového počtu 100% (600) nepoužívalo internetové bankovnictví, zejména se jednalo o starší věkové kategorie dotázaných. Mezi těmito 33% (195) dotázaných, byli také zákazníci, kteří by internetové bankovnictví využívali, ale je na ně příliš složité. Na tomto základě a provedeného vedlejšího výzkumu jsem stanovil svá případná opatření a návrhy.

Případná opatření a návrhy v podobě, které jsem vypracoval v rámci mé bakalářské práce, byly získány ze zkušeností a informací z výsledků hlavního a vedlejšího výzkumu provedeného na pobočce ČSOB na Lannově třídě 3/11 v Českých Budějovicích. Jeden z projektů jsem ekonomicky zhodnotil pro případ orientačních provozních nákladů při realizaci tohoto projektu. Domnívám se, že zákazníci banky mají zájem o online bankovnictví a tento návrh by jim pomohl získat potřebné zkušenosti a informace pro jejich následné použití.

Výsledky průzkumu byly poskytnuty manažerce týmu Veronice Neudörflové působící na pobočce ČSOB na Lannově třídě 3/11 v Českých Budějovicích pro interní účely pobočky a dále centrále ČSOB se sídlem Radlická 333/150 v Praze.

Nároky na požadavky internetového bankovnictví neustále rostou. Snahou bank je neustálá péče o zákazníky a zvyšování kvality poskytovaných služeb. Očekáváním zákazníků je služba, která je pokryta zabezpečením a jednoduchá na ovládání. Očekáváním bank je naopak kvantitativní množství spokojených zákazníků, při splnění bankovních snah o udržení zákazníků. Jen tak se vytváří kvalitní řetězec spolupráce, mezi bankou a zákazníkem. Očekávání je ale naplněno i při splnění a uvědomění povinností zákazníků, tj. opatrnost, dodržování bezpečnosti při přihlašování.

Summary

With the development of information technologies are brought into our lives factors, which gradually transformed into increasingly use virtual services. These services are designed to assist benefit from the services faster, more affordably, with a focus on friendly operation with high security. Great twist on the Internet bears the establishment, which started a new era of service.

Progressive changes were also virtual services in the banking field. Very fast and modern service is Internet banking, sometimes called online banking. Are used to access devices that are commonly available to users. This is mainly for personal computers, laptops, smart phones, PDAs. Construction equipment is designed to run banking applications and allows you to log into your bank account online. Users can all transactions with financial resources to carry out 24 hours a day, 7 days a week, 365 days a year, from the comfort of work or home. This eliminates the visit to the branch bank and waiting in long queues. Some banks offer online banking due to a personal account without charge, some with a fee, but the fees are high.

Internet Banking Bank provided since the beginning of the internet. Usage has been the extent to which it is now, but today it is the internet banking modern trend of each bank. Today, online banking, used mainly by young people and people in middle age, which is mainly due to greater knowledge of information technology.

In particular, smart phones are becoming the latest trend that their applications are quite similar to personal computers. Time would be so tailored applications should converge to a similar unit.

Security is of paramount concern in the financial management of Internet banking customers. Banks perform a variety of measures to prevent its breaking, thus providing assurance and customer satisfaction. Banks aim is to make money from clients have been as much coverage of quality security. Protection should be ambidextrous, so it is important that the user takes steps to protect its facilities, which used to login to internet banking.

Claims to the requirements of Internet banking to grow steadily. Banks aim is a permanent customer care and quality of their services. Customer expectations are services that are covered by such security, which is expected of them and must also be simple and clear to use. Expectations of banks, by contrast, the quantitative number of satisfied customers. Just creating a string of good cooperation between the bank and the customer. The expectation is, but also filled with fulfillment and customer awareness of responsibilities. In particular, care and safety compliance logging.

Použitá literatura

[1] *ABZ.cz: Slovník cizích slov* [online]. *2006 Shareware* [cit. 2011-11-3] Dostupné z WWW: <http://slovnik-cizich slov.abz.cz/web.php/hledat?typ_hledani=prefix&cizi_slovo=shareware>.

[2] *ABZ.cz: Slovník cizích slov* [online]. *2006 Adware* [cit. 2011-11-3] Dostupné z WWW: <http://slovnik-cizich-slov.abz.cz/web.php/hledat?typ_hledani=reverse&cizi_slovo=adware>.

[3] *ABZ.cz: Slovník cizích slov* [online]. *2006 Malware* [cit. 2011-11-3] Dostupné z WWW: <http://slovnik-cizich-slov.abz.cz/web.php/hledat?typ_hledani=reverse&cizi_slovo=malware>.

[4] *CENTRIA.SKODA-AUTO.com: Porsche Inter Auto CZ České Budějovice* [online]. *2010 Fabia Classic TSI START 1.2 TSI 63 kW 5-stup. mech.* [cit. 2011-11-3] Dostupné z WWW: < http://centria.skoda-auto.com/CZE/porschecb/services/Pages/NewCarsDetail.aspx?carid=199192&returnurl=http%3a%2f%2fcentria.skoda-auto.com%2fcze%2fporschecb%2fPages%2fhome.aspx >.

[5] *CNB.cz* [online]. *2010 Přehled představitelů ČNB a jejích právních předchůdců.* [cit. 2011-10-3] Dostupné z WWW: <http://www.cnb.cz/cs/verejnost/archiv_cnb/archiv_cnb_guverneri.html>.

[6] CRAIG, P., BURNETT, M. *Softwarové pirátství bez záhad.* Praha: Grada, 2008. 224 s. ISBN 978-80-247-1765-4.

[7] *CSOB.cz* [online]. *2010 Přihlášení do služeb internetového bankovnictví.* [cit. 2011-9-3] Dostupné z WWW: < http://www.csob.cz/cz/Produktovy-katalog/Elektronicke-bankovnictvi/Stranky/Prihlaseni-do-sluzeb-internetoveho-bankovnictvi.aspx#sms>.

[8] *CSOBPOJ.cz* [online]. *2010 Povinné ručení on-line.* [cit. 2011-11-3] Dostupné z WWW: <https://app.csobpoj.cz/sjednaniOPV/smlouva?pg=toVypocet#aPojistne>.

[9] DRAHORÁD, J. *Mediafax.cz* [online]. 31. 3. 2011 *K internetu je v Česku připojeno 56 procent domácností.* [cit. 2011-11-3] Dostupné z WWW: <http://www.mediafax.cz/domaci/3197087-K-internetu-je-v-Cesku-pripojeno-56-procent-domacnosti>.

[10] DUDÁČEK, K., BLÁBOLIL, R. *Poprvé u počítače, aneb, Začínáme pracovat s PC. 10.vydání.* České Budějovice: Kopp, 2007. 128 s. ISBN 80-7232-301-6.

[11] DUNNIGAN F., J. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu. 1. vydání.* Praha: Baronet a.s., 2004. ISBN 80-7214-642-4.

[12] FRIMMEL, J. *Vyplňto.cz* [online]. 6. 2. 2011 *Zkušenosti s elektronickým bankovnictví (výsledky průzkumu)* . [cit. 2011-11-3] Dostupné z WWW: <http://zkusenosti-s-elektronickym-b.vyplnto.cz >.

[13] GÁLA, L., POUR, J., ŠEĎIVÁ, Z. *Podniková informatika. 2. vydání.* Praha: Grada, 2009. 496 s. ISBN 978-80-247-2615-1.

[14] HORSKÝ, R. *Bezdrátové sítě Wi-Fi v rekordním čase. 1.vydání.* Praha: Grada, 2006. 84 s. ISBN 80-247-1790-5.

[15] HUBINKOVÁ, Z. a kol. *Psychologie a sociologie ekonomického chování. 3. vydání.* Praha: Grada, 2008. 280 s. ISBN 978-247-1593-3.

[16] CHROMÝ, J. *Elektronické podnikání. 2.vydání.* Praha: Vysoká škola hotelová v Praze, 2009. 109 s. ISBN 978-80-86578-96-5.

[17] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

[18] KAŠPAROVSKÁ, V. *Banky a bankovní obchody. 1. vydání.* Brno: Mendlova zemědělská a lesnická univerzita v Brně, 2003. 108 s. ISBN 80-7157-652-2.

[19] KLÍMA, J. *Finance a bankovnictví.* Místo neuvedeno: Vysoká škola regionálního rozvoje, 2007, 55 s.

[20] KOUDELKA, J. a kol. *Případové studie ze spotřebního marketingu. 1.vydání.* Praha: Oeconomica, 2007. 116 s. ISBN 978-80-245-1306-5.

[21] KOUDELKA, J. *Spotřební chování a marketing. 1. vydání.* Praha: Grada, 1997. 192 s. ISBN 80-7169-372-3.

[22] KOUDELKA, J. *Spotřební chování a segmentace trhu. 1.vydání.* Praha: Vysoká škola ekonomie a managementu, 2006. 227 s. ISBN 80-86730-01-8.

[23] LANCE, J. *Phishing bez záhad. 1. výdání.* Praha: Grada, 2007. 284 s. ISBN 978-80-247-1766-1.

[24] MACICH, J. *Zabezpečení: první bojová linie.* POČÍTAČ PRO KAŽDÉHO, 2010, č.11, s. 41 – 42.

[25] MATYÁŠ, V. a kol. *Autentizace uživatelů a autorizace elektronických transakcí.* Praha: TATE International**,** 2007. 318 s. ISBN 978-80-86813-14-1.

[26] MÁČE, M. *Platební styk: klasický a elektronický. 1.vydání.* Praha: Grada, 2006. 220 s. ISBN 80-247-1725-5.

[27] PÁNEK, D. *Bankovní služby. 1.vydání.* Brno: Masarykova univerzita v Brně, 2001. 70 s. ISBN 80-210-2691-X.

[28] PECINOVSKÝ, J., PECINOVSKÝ, R. *Windows 7: průvodce začínajícího uživatele.* Praha: Grada, 2009. 224 s. ISBN 978-80-247-3210-7.

[29] PETRJÁNOŠOVÁ, B. *Bankovnictví II. 1.vydání.* Brno: Masarykova univerzita, 2000. 167 s. ISBN 80-210-2503-4.

[30] POLOUČEK, S. a kol. *Bankovnictví. 1.vydání.* Praha: C. H. Beck, 2006. 715 s. ISBN 80-7179-462-7.

[31] PROCHÁZKA, D. *První kroky s internetem. 3.vydání.* Praha: Grada, 2010. 112 s. ISBN 978-80-247-3255-8.

[32] PROCHÁZKA, D. *Windows Vista.* Praha: Grada, 2008. ISBN 978-80-247-2179-8.

[33] PROTIVÍNSKÝ, M. *Bankovní loupeže: přepadení bank, peněžních transportů a kriminalita v bankovnictví. 1.vydání.* Praha: Armex ve spolupráci s TRIVIS, 2001. 278 s. ISBN 80-86244-21-0.

[34] PŘIBYL, T. *(Ne)bezpečné internetové bankovnictví.* POČÍTAČ PRO KAŽDÉHO, 2010, č. 13, s. 42 - 43.

[35] RAK, R., MATYÁŠ, V., ŘÍHA, Z. a kol. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích.* Praha: Grada, 2008. 664 s. ISBN 978-80-247-2365-5.

[36] SEKERKA, B. a kol. *Bankovní transakce. 1. vydání.* Pardubice: Univerzita Pardubice Fakulta ekonomicko-správní, 2005. 140 s. ISBN 80-7194-809-855-785-05.

[37] SEKERKA, B. *Bankovnictví: II. díl. 2. vydání.* Pardubice: Univerzita Pardubice Fakulta ekonomicko-správní, 2005. 79 s. ISBN 80-7194-815-255-791-05.

[38] *SROVNAVAC.cz*[online]. 2010 Povinné ručení porovnání. [cit. 2011-11-3] Dostupné z WWW: <http://www.srovnavac.cz/povinne-ruceni-porovnani/>.

[39] TVRDÍKOVÁ, M. *Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů. 1. vydání.* Praha: Grada, 2008. 176 s. ISBN 978-80-247-2728-8.

[40] ZEMAN, V. *Bankovnictví: pro studijní obor realitní inženýrství. 1. vydání.* Brno: Vysoké učení technické v Brně , Fakulta podnikatelská, 2009.

[41] ZEMAN, V. *Bankovnictví: 2.díl. 1. vydání.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2006. ISBN 80-214-3256-X

Seznam tabulek a grafů

Seznam tabulek

Seznam grafů

Přílohy

Seznam příloh

Příloha 1

Token iKey 2032 USM Smart

Pramen: http://www.systemonline.cz/casopis/2008/10-askon02.jpg

Příloha 2

Schéma šifrování s tokenem iKey řady 2000

Pramen: http://www.lupa.cz/clanky/usb-token-pamatuje-si-hesla-sifruje-neni-bezpecny/

Příloha 3

Dotazník

Dobrý den, Jmenuji se Martin Kakaš a jsem studentem 3. ročníku Ekonomické fakulty Jihočeské univerzity v Českých Budějovicích. Studuji obor Obchodní podnikání a touto cestou bych Vás chtěl požádat o vyplnění následného dotazníku. Dotazník je důležitý pro vypracování mé bakalářské práce na téma: Využití online bankovnictví a spotřebitelé. Dotazník je zcela anonymní a výsledná data budou zveřejněna v mé bakalářské práci a poskytnuta pobočce ČSOB na Lannově třídě 3/11 v Českých Budějovicích.

Děkuji za Váš čas a pravdivé odpovědi

Martin Kakaš

Využíváte online bankovnictví?

- o Ano
- o Ne

Jak často využíváte online bankovních služeb?

- o Každý den
- o Alespoň jednou týdně
- o Alespoň jednou za měsíc
- o Vícekrát za měsíc
- o Jednou za 3 měsíce

U jaké banky jste zákazníkem?(možno i více odpovědí)

- o Česká spořitelna
- o ČSOB
- o GE Money Bank
- o Komerční banka
- o Poštovní spořitelna
- o Reiffeisen bank
- o mBank
- o AXA
- o Jiné:

Z jakého důvodu používáte online bankovních služeb?(hodnoťte na škále jako při známkování ve škole důležitost jednotlivých důvodů, 1 - velmi důležité, 5 - zcela nedůležité)

	1	2	3	4	5
Úspora času	☐	☐	☐	☐	☐
Pohodlí	☐	☐	☐	☐	☐
Nižší poplatky	☐	☐	☐	☐	☐
Jednoduchost a srozumitelnost	☐	☐	☐	☐	☐
Dostupnost pobočky	☐	☐	☐	☐	☐

Setkal/a jste se někdy s kriminalitou v souvislosti s Vaším účtem?(Kriminalitou je zde myšleno: odcizení finančních prostředků z účtu, krádeže přihlašovacích údajů, nevyžádané podvodné emailové zprávy žádající změnu přihlášovacích údajů). ***V případě odpovědi "Ano", přejděte na další otázku, v případě odpovědi "Ne" přeskočte následující otázku.***

- o Ano
- o Ne

Jak jste postupoval/a a s jakým výsledkem?

Považujete online bankovnictví za bezpečné?

- o Ano
- o Spíše Ano
- o Ne
- o Spíše Ne

Dáváte si při přihlášení ke službě online bankovnictví pozor na případná rizika? (Případnými riziky je myšleno: přesměrování na podvodnou stránku, odcizení přihlašovacích údajů, odcizení peněz z účtu)

- o Vždy
- o Většinou
- o Málokdy
- o Nikdy

Jaké zařízení pro online bankovnictví používáte?(možno i více odpovědí)

- o Osobní počítač
- o Mobilní telefon
- o Tablet/Kapesní počítač
- o Notebook/Netbook
- o Jiné:

Jaké pravidelně aktualizované prvky používáte pro osobní zabezpečení počítače? (možno více odpovědí)

- o Antispywarové programy (SpyBot, SuperAntispyware, Spy Emergency, Spyware Terminator, Ad-Aware, Norton Antivirus...)
- o Antivirové programy (Avast, AVG, ESET NOD 32,Kaspersky Anti-Virus, F-Secure, Panda Antivirus, Norton Antivirus....)
- o Antiphishingové programy(ESET NOD 32, G DATA Antivirus, Norton Antivirus....)
- o Antirootkitové programy(Panda Antirootkit, SysProt AntiRootkit, AVG AntiRootkit....)
- o Jiné:

Z jakého důvodu nepoužíváte online bankovnictví?

- o Nevěřím tomu, je riskantní
- o Nevlastním zařízení pro využívání online bankovnictví
- o Jiné:

Jaké je Vaše pohlaví?

- o Muž
- o Žena

Jaký je Váš věk?

- o 0-17
- o 18-30
- o 31-40
- o 41-50
- o 51-60
- o 61-70
- o 71-80
- o 81 a více

Místo Vašeho trvalého bydliště?

- o Město
- o Venkov

Z jakého kraje pocházíte?

- o Plzeňský kraj
- o Karlovarský kraj
- o Ústecký kraj
- o Jihočeský kraj
- o Středočeský kraj
- o Liberecký kraj
- o Královehradecký kraj
- o Pardubický kraj
- o Vysočina
- o Olomoucký kraj
- o Jihomoravský kraj
- o Moravskoslezský kraj
- o Zlínský kraj
- o Praha

Příloha 4

Doplňující otázky vedlejšího výzkumu

1) Čeho se nejvíce obáváte v internetovém bankovnictví? (pouze jedna odpověď)

a) Obavy o soukromí
b) Obavy o bezpečnost finančních prostředků
c) Nemám žádné obavy
d) Jiné:

2) Jak jste spokojen/a s poplatky za internetové bankovnictví? (pouze jedna odpověď)

a) Poplatky jsou příliš vysoké
b) Poplatky jsou přiměřené
c) Poplatky se mi zdají nízké

3) Který poplatek považujete za „nesmyslný“ (v rámci internetového bankovnictví)**?** (pouze jedna odpověď)

a) Poplatek za mimořádnou obnovu bezpečnostního certifikátu
b) Poplatek za účetní položku
c) Poplatek za vedení účtu
d) Jiný:

4) Jakou změnu byste uvítal/a v internetovém bankovnictví? (pouze jedna odpověď)

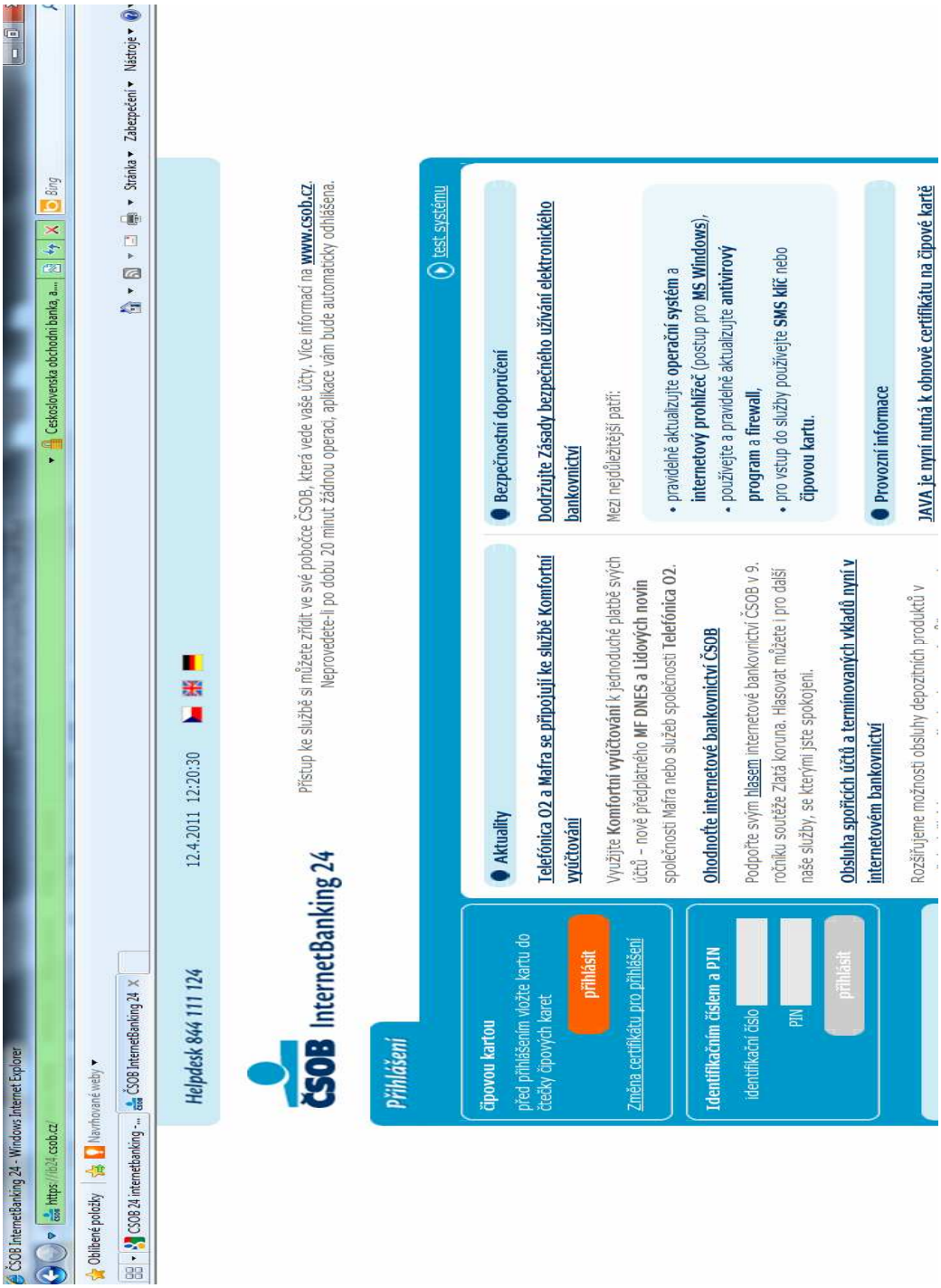
a) Uvítal/a bych více informací od banky (např: zasílání emailem, poštou)
b) Uvítal/a bych proškolení v internetovém bankovnictví
c) Uvítal/a bych zpřehlednění prostředí internetového bankovnictví
d) Jiné:

5) U jaké banky jste zákazníkem? (pouze jedna odpověď)

a) Česká spořitelna
b) ČSOB
c) GE Money Bank
d) Komerční banka
e) Poštovní spořitelna
f) Raiffeisen bank
g) MBank

h) AXA
i) ČNB
j) Sparkasse
k) Jiné:

Příloha 5 Stránka pro přihlášení do ČSOB Internetbanking 24



Pramen: https://ib24.csob.cz/