Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomiky

Diplomová práce

Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta

Bc. Naděžda GASIORKOVÁ

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra ekonomiky

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Gasiorková Naděžda

Provoz a ekonomika

Název práce

Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta

Anglický název

Economic aspects of payment card security from the client's perspective

---

Cíle práce

Hlavním cílem je vymezení ekonomických aspektů bezpečnosti platebních karet z pohledu klienta. Na základě vymezení aspektů následně stanovení závěrů, názorů a doporučení při užívání platebních karet. Dílčími cíli jsou seznámení, analýza a doporučení v oblastech historie platebních karet, včetně jejich ochraných prvků, historie podvodů s kartami, současných podvodů (včetně podvodů přes elektronické bankovnictví), s tím jak se těmto podvodům bránit.

Metodika

Literární rešerše je sepsána na základě informací získaných prostudováním odborné literatury dostupné v Městské knihovně Praha, Knihovně SIC na České zemědělské univerzitě a v knihovně Vysoké školy ekonomické. Také je využito internetových zdrojů informací z oblasti bezpečnosti platebních karet – metoda prostudování a analýzy dokumentů. Pro vymezení ekonomických aspektů bezpečnosti platebních karet z pohledu klienta je provedeno dotazníkové šetření a jeho statistické vyhodnocení.

Harmonogram zpracování

Literární rešerže - prvá část: 3/2012 až 8/2012
Detailní metodika a dokončení druhé částí literární rešerže: 8/2012 až 10/2012
Vlastní práce, analytická část: 10/2012 až 12/2012
Vlastní práce, syntéza poznatků, návrhy a doporučení: 12/2012 až 2/2013
Odevzdání poslední verze práce vedoucímu práce ke konečnému posouzení: 15. 3. 2013

Rozsah textové části

50 – 70 stran.

Klíčová slova

kreditní karta, debetní karta, ochranné prvky, bankomaty, pojištění karty, rizika, bezpečnost, ekonomika

Doporučené zdroje informací

[1]: JUŘÍK, Pavel. Platební karty, velká encyklopoedie 1870-2006. vyd. 1 Praha: Grada Publishing, 2006. 296 s. ISBN 8024713810.
[2]: ELY PLISCHKE, Simona. Penize.cz [online]. 27. 04. 2007 [cit. 2012-02-23]. Jak došly platební karty do českých zemí aneb historie karet plná zajímavostí. Dostupné z WWW:http://www.penize.cz/platebni-karty/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti
[3]: www.Csa.cz [online]. 1998-2010 [cit. 2012-02-23]. OK Plus - věrnostní programy. Dostupné z WWW: <http://www.csa.cz/cs/portal/loyalty_programs/ ffp_okplus/ffp_ homepage.htm>.
[4]: JUŘÍK, Pavel. Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet. 1. vyd. Praha: Grada, 2003. 312 s. ISBN 8024706857.
[5]: CHARLES, Arthur. How ATM fraud nearly brought down British banking. The register [online]. 25. srpna 2005 [cit. 2012-03-07]. Dostupné z: http://www.Theregister.co.uk/2005/ 10/21/phantoms_and_rogues/
[6]: MÁČE, Jaroslav. Platební styk – klasický a elektronický. vyd. Praha - Grada Publishing, 2006. 220 s. ISBN 8024717255.

Vedoucí práce

Škubna Ondřej, Ing.

Termín odevzdání

březen 2013

prof. Ing. Miroslav Svatoš, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 23.11.2012

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 31. 3. 2013 _____

Poděkování

Ráda bych touto cestou poděkovala panu inženýru Ondřeji Škubnovi a paní inženýrce Heleně Řezbové za dobré vedení v průběhu zpracování této diplomové práce.

Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta

---

Economic aspekts of security of payment cards from the client´s perspective

Souhrn

Tématem této diplomové práce jsou „Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta“, se zaměřením na bezpečnost platebních karet. Jelikož téma zabezpečení našich finančních prostředků je vždy velmi aktuální a diskutované. Práce je rozdělena na dvě části.

První část se věnuje historickému vývoji platební karet, představuje ochranné prvky platební karty, které jsou zajišťovány karetními asociacemi, bankou a klientem. Kapitola číslo 5 se věnuje historii podvodů, další kapitola, pak rizikům, které jsou s platební kartou spojené a nakonec podvody, které jsou v současné době nejčastější, Jsou jimi zejména skimming, phishing, offline a online zneužití platební karty.

Ve druhé části autorka provedla výzkum u 121 respondentů. Výzkum byl proveden dotazníkovou metodou a zjišťuje, jaká je bezpečnost platebních karet z pohledu klientů bank, jaké mají požadavky na zabezpečení karet a kolik Kč jsou ochotni klienti zaplatit za bezpečnost své platební karty.

Klíčová slova: kreditní karta, debetní karta, podvod, rizika, ochranné prvky, bankomaty, pojištění, rizika, podvod, bezpečnost, ekonomika.

Summary

The topic of this thesis is "Economic Aspects of Security cards from the client's perspective," focusing on the security of payment cards. As the issue of security of our financial resources is always up to date and discussed. The thesis is divided into two parts.

The first part deals with the historical development of payment cards and payment cards security features that are provided by card associations, banks and client himself. Chapter No. 5 is devoted to the history of fraud, the next chapter is about the risks that are associated with credit card and finally fraud which are currently the most common. The most common are skimming, phishing, online and offline payment card misuse.

In the second part the author did research among 121 respondents. The research was conducted using questionnaires and determines what the security of payment cards is in terms of bank clients, what are the requirements for security cards and how much they are willing to CZK clients pay for the security of their credit cards.

Keywords: Credit card, debit card, fraud, risk, protective devices, ATMs, insurance, risk, fraud, security, economy.

OBSAH

1 Úvod

Již v mé bakalářské práci jste se mohli dočíst různé zajímavosti o platebních kartách jako jedné z forem bezhotovostního platebního styku. A jelikož je toto téma stále aktuální a velice mě zajímá, rozhodla jsem se, že i svou diplomovou práci budu věnovat platebním kartám. Tato práce se zabývá hlavně jejich bezpečností. V dnešní moderní době, kdy rozvoj nových technologií a jejich snadná dostupnost s sebou přináší nová a nová rizika, je nutné jim čelit. Stále se objevují nové technologie, obchodníci stále hledají nové příležitosti. Karetní systémy stojí spoustu peněz, vznikají bezkontaktní karty, předplacené karty, nové služby u platebních terminálů u bankomatů. Ale umíme se my, běžní uživatelé bránit před podvody? Víme jak? Jsme schopni chápat potřebu zabezpečení? Jsem schopni tuto potřebu ekonomicky ohodnotit?

Díky tomuto stavu se vyskytují nové hrozby. Naneštěstí se zcela nepodařilo vymýtit staré hrozby. Především nedostatečná nebo zcela chybějící legislativa a dále její malá vynutitelnost nemůže účinně bojovat s narůstající kriminalitou. Proto samy banky vydaly desatero doporučení, jak pracovat s platební kartou a tím se částečně snaží ochránit své klienty.

Hlavní důvod vedoucí ke zneužívání platebních karet je lidský faktor. Mezi námi jsou lidé, kteří si svůj PIN od karty zkrátka a dobře nejsou schopní zapamatovat. Proto pro usnadnění si jej napíší do mobilu nebo na papírek a uschovají spolu s kartou do peněženky. Která je pak snadnou kořistí pro zloděje a tudíž, i velice snadným způsobem, jak se dostat k vašim penězům. Díky tomu, že naše společnost velmi rychle přešla a stále přechází na bezhotovostní platby, stává se tato finanční sféra zajímavá pro páchání trestné činnosti.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem diplomové práce je vymezení ekonomických aspektů bezpečnosti platebních karet z pohledu klienta. Práce je rozdělena do dvou částí – literární rešerše a vlastní výzkum.

Cílem teoretické části práce je na teoretické úrovni rozebrat problematiku bezpečnosti platebních karet od jejího vzniku až po současnost. Literární rešerše je zaměřena na historii platebních karet, ochranné prvky, historii podvodů prováděných s platebními kartami, se současnými podvody a s tím jak se těmto podvodům bránit.

Vlastní část se zabývá výzkumem ekonomických aspektů bezpečnosti platebních karet z pohledu klienta. Provedení výzkumu dotazníkovým šetřením zjišťuje, zda se klienti zajímají o bezpečnost své platební karty. Cílem této části je vyvrátit nebo potvrdit stanovená tvrzení.

Závěrem je provést celkové zhodnocení.

2.2 Metodika práce

Literární rešerše byla sepsána na základě informací získaných prostudováním odborné literatury dostupné v Městské knihovně Praha, Knihovně SIC na České zemědělské univerzitě a v knihovně Vysoké školy ekonomické. Dále různých internetových stránek z oblasti bezpečnosti platebních karet – metoda prostudování dokumentů.

Pro vymezení ekonomických aspektů bezpečnosti platebních karet z pohledu klienta bylo provedeno dotazníkové šetření a statistické vyhodnocení. Výhodou dotazníkového šetření je anonymita, proto lze získat upřímnější a objektivnější informace. Výzkum byl rozdělen do tří částí. **V první části** byl sestaven dotazník, ve

kterém byly použity uzavřené a polozavřené odpovědi, ve kterých si respondenti mohly vybrat ze dvou a více možností.

Dotazník byl zpracován podle metodiky pana Hynka Jeřábka – Úvod do sociologického výzkumu a Miroslava Dismana – Jak se vyrábí sociologická znalost.

Před sestavením dotazníku, byla sestavena čtyři tvrzení, která výsledky dotazníku vyvrátila nebo potvrdila. Jimi jsou:

1. Respondenti, kteří utratí nejčastěji do 1000Kč nevyužívají službu pojištění proti zneužití karty.
2. Každý, kdo vlastní platební kartu by chtěl, aby mu banka vyčíslovala, kolik měsíčně zaplatí za bezpečnost.
3. Nejvíce respondentů by bylo ochotno zaplatit za bezpečnost 25 – 44Kč měsíčně.
4. Nejvíce respondentů považuje za nejrizikovější způsob používání platební karty platbu přes internet.

Autorka rozhodla o metodě získání dat pomocí elektronického strukturovaného dotazníku. Po prostudování dokumentů a literatury byl sestaven dotazník o 13. otázkách – z nichž 2 jsou polozavřené a ostatní uzavřené otázky. Úvodem se autorka představila, představila svůj dotazník, jeho cíl a požádala o jeho vyplnění. Poté následovaly demografické otázky a samotné otázky dotazníku. Otázky byly položeny přímo a jasně, otázky nejsou vícehlavňové, nevyskytují se v nich slova, kterým by studenti nerozuměli. V dotazníku dále nebyly použity otázky obsahující dvojí zápor, žádná z otázek neobsahovala možnost odpovědi nevím. Na počátku dotazníku byly umístěny otázky lehčí – proto, aby dotazovaný byl ochotný dále pokračovat ve vyplnění. Ve střední části byly umístěny těžší a významnější otázky. Dotazník je ukončen opět lehčími otázkami. Každá otázka dotazníku byla očíslována a taktéž i každá strana dotazníku.

Poté autorka provedla pilotní šetření v okruhu rodiny a blízkých přátel. Ověřila si tím, zda navržený výzkumný nástroj a zvolená strategie sběru dat mohou být bez problémů použity, zda nejsou v dotazníku chyby (gramatické, chybějící otázky či možnost odpovědi), zda se některé odpovědi nepřekrývají. Po vyhodnocení dotazníku byly opraveny zjištěné chyby a autorka přistoupila k hlavnímu sběru dat.

Ve druhé části byl dotazník vložen na internetový portál survio.cz a posléze jeho odkazová adresa, která je http://www.survio.com/survey/d/D2C8I0T0Y3B7M7D6V, pomocí emailu odeslán respondentům různých věkových kategorií a vzdělání. Dotazníky byly přebrány a neúplné dotazníky (chyběla odpověď) vyřazeny z výzkumu a otázky s odpovědí ne, na první otázku – Vlastníte platební kartu, byly taktéž vyjmuty z konečného hodnocení. Ke konečnému zpracování bylo použito 118 z původních 121.

Ve třetí části proběhlo zpracování dat pomocí sloupcových grafů. Pro vyhodnocení byly otázky rozděleny do 3 částí, ke každé části bude vytvořen vlastní závěr. Tyto závěry slouží k zpřehlednění vyhodnocení dotazníku a vytvoření celkového závěru diplomové práce.

3 Počátky platebních karet

3.1 Historický vývoj ve světě

Spojené státy americké se oprávněně považují za kolébku platebních karet. Pro rozvoj obchodu se koncem 90. let 19. století začaly používat cestovní šeky, peněžní poukázky, **úvěrové známky a kovové úvěrové** známky, jež byly právě předchůdcem platebních karet. V tomto období vznikl také bezhotovostní platební styk na cestách a v obchodech díky cestovním šekům a poštovním poukázkám. Thomas Cook je vynálezce **cestovních šeků**. Roku 1891 zavedla cestovní šeky dopravní a kurýrní společnost American Expres (Juřík, 2006).

Před více než 140 lety byly zavedeny Metal chase coins, metal credit tokens – kovové úvěrové mince nebo známky. Těmito mincemi umožňovali obchodníci nákup svým zákazníkům na tzv. sekyru. Úvěrové poukázky jsou považovány za Evropské předchůdce platebních karet. Objevily se v roce 1880 ve Velké Británii a vydávala je společnost Proviant Clothing Group pro použití ve vybraných obchodech. První platební karty přicházejí během let 1868 – 1914. Tyto karty sloužily k prokázání slevy nebo bezplatné služby, byly oboustranně potištěné a papírové. **První platební kartu** vydala společnost Western Union Telegraph Company v roce 1914. Zákazníkům byla poskytnuta zdarma a umožňovala telefonovat, posílat telegramy s možností zaplatit je až na konci měsíce. Díky malé trvanlivosti papírových karet vznikly plechové karty, které byly podobné identifikačním štítkům Americké armády, v roce 1928. Roku 1947 byla vydávána karta pod názvem Air Travel Card, která byla označena jako první mezinárodně platnou úvěrovou kartonu na světě. Roku 1950 vznikla první univerzální platební karta. V té době vznikla společnost Diners Club International a byla to právě ona, kdo stál u zrodu první univerzální karty (Juřík, 2003).

Karta, jež se velmi podobala dnešní platební kartě, spatřila světlo světa v roce 1951, kdy první banka Franklin Change Plan vydala platební kartu, jež obsahovala

jméno majitele a výši uvěrového limitu. Plastová karta se objevila až roku 1960, tu vynalezla společnost American Express a to z důvodů větší bezpečnosti. Tyto karty bylo těžší padělat a také zrychlovaly platbu. O 5 let později měla svou první plastovou kartu i Evropa. Vydala ji společnost National Provincial Bank sídlící ve Velké Británii. Velká Británie, Švédsko a Finsko se staly prvními zeměmi na Evropském kontinentu, které začaly vydávat platební karty. Barvlays Bank byla první bankou, která začala vydávat Barclayscard jako první mimo USA a také zavedla první bankomaty na světě. Francouzská společnost SOVAC začala vydávat jako první zlaté karty Carte d´Or. Ovšem největší rozmach zlatých karet byl v roce 1981, kdy je masově začali vydávat MasterCard a VISA. V 70. a 80. letech byl vynalezen magnetický proužek, magnetický záznam, zavedeny bankomaty, platební terminály a moderní centra s výpočetní technikou. V těchto letech získali platební kartu i studenti. Roku 1974 vznikla první debetní karta, jež vydala Amazona Bank. Platinová karta byla vydána až v roce 1984 společností American Express a ještě prestižnější kartou se staly karty Signia, Mastercard Word a VISA Signiture Card. Pomocí těchto karet bylo klientům zajištěno využívání exkluzivních služeb. U těchto karet je na přední straně pro větší bezpečnost laserem vypálen vzorový podpis. Počítače umožnili bankám v 60. a 70. letech 20. století automatizovat bankovní služby, současně byly impulzem pro vznik čipových karet (Juřík, 2006).

3.2 Historický vývoj v České republice

Československo se v 60. létech stalo první ze zemí bývalého bloku Sovětského svazu, která přijala plastové platební karty. Akceptovat jsme je začali už v roce 1965. První transakce byla provedena až dne 24. 10. 1968. Tehdy někdo zaplatil pomocí Diners Card za služby v pražské pobočce Čedok (www.penize.cz/platebni-karty).

Karty, které se u nás vyskytovaly před pádem komunismu, byly jen a výhradně v držení cizinců. Z toho vyplývá, že firma Čedok, jakožto jediná společnost, která byla ve styku s cizinci, byla pověřena **akceptací platebních karet**. Paní Eva Kárníková, ředitelka společnosti Diners Club Czech říká: „Na začátku 90. Let,

částečně z podnětu ČNB, vznikaly v bankách útvary, které se začaly společně zabývat jednotným mezinárodním systémem placení.“ Zajímavostí je, že už v tu dobu Česká spořitelna vlastnila svůj systém off-line bankomatů. Živnostenská banka drží prvenství ve vydávání platebních karet. První VISA kartu tato společnost vydala již v roce 1991 k tuzexovému účtu. Roku 1989 Česká spořitelna vydala první **kartu do bankomatu.** 4. února 1991 bylo založeno Mezinárodní sdružení pro bankovní karty. Po rozpadu Československa se rozdělilo na Sdružení pro bankovní karty v Čechách a Združenie pre bankovné karty na Slovenku. Jedná se o zájmové sdružení bank, jejichž zájmem je rozvoj platebních karet v České republice a koordinace prací, souvisejících s tímto rozvojem (Juřík, 2003).

„Vznik bankovních karet je tak u nás spojen s aktivitami třech skupin: Českou spořitelnou a jejími off-line bankomaty na výběr hotovosti. Živnostenskou a její vydanou VISA kartou a jednotlivými bankami, které se v rámci dnešního Sdružení pro bankovní karty staly vydavateli produktů společnosti EuroCard/MasterCard.“ Shrnuje Eva Kárníková (www.penize.cz/platebni-karty).

Druhým dechem tato odbornice na platební karty dodává, že díky Čedoku získaly Komerční banka a Česká spořitelna obrovskou výhodu, když odkoupily a převzaly obchodníky Master Card a z této výhody těží až do dnes, kdy mají **bonitní korporátní klientelu** (www.penize.cz/platebni-karty).

V roce 1994 se u nás začaly také objevovat první platební terminály v obchodech a v roce 1995 bankomaty společnosti VISA.

V 90. letech vznikly **Kobrandové karty**, které vydává společně banka a komerční organizace. U nás ji v roce 2001 vydala firma České aerolinie. Je to karta pro klienty, kteří sbírají body za lety. Dnes tato společnost vydává členské, stříbrné, zlaté i platinové karty klientům podle nalétaných mil s ČSA nebo s jejich partnery z aliance SkyTeam (www.csa.cz).

I přesto, že banky věděly, že platební karty se stanou nedílnou součástí života, jejich vývoj podcenily. Ani obchodníci nebyli příliš "draví" do zapojení se do tohoto systém. České obyvatelstvo platební karty nedrželo, tudíž obchodníci neměli terminály, pokud neobchodovali s cizinci. Češi netušili, proč mají karty držet, když s nimi nemohou nikde zaplatit. Počátkem 90. let tvořily 90% obratu karty vydané v zahraničí, jimiž cizinci platily hlavně v prodejnách skla, starožitností, autopůjčovnách, restauracích a hotelech. V dnešní době, je převážná část obratu tvořena v hypermarketech. Česká spořitelna vydala roku 1998 první **kreditní kartu**, kterou měli možnost obdržet pouze velmi bonitní klienti této banky. Od roku 2000 se datuje u nás „rozjezd kreditek". Tohoto roku vstoupila na trh dnešní HVB Bank a vydala kreditní kartu Maxim. **Roky 2001 - 2002** jsou tedy považovány za skutečný start kreditních a charge karet u nás (www.penize.cz/platebni-karty).

4 Ochranné prvky platebních karet

Stejně jako bankovky a mince mají své ochranné prvky, tak i platební karty musí být takto chráněny před zneužitím. Ochranné prvky hrají velkou roli. Platební karty se vyrábějí z plastikového materiálu a musí odpovídat mezinárodním normám a standardům. Výrobu plastových platebních karet zajišťují pouze certifikované tiskárny bankovek a jiných cenin, kterých je na světě asi kolem 45. Tyto tiskárny musí splnit nejpřísnější bezpečnostní požadavky. Karetními společnostmi je předepsána objednávka, certifikace a výroba. Dále tyto společnosti ručí za splnění ISO norem a bezpečnostních parametrů karty. Platební karta není regulována podrobně zákonem. Dílčí úpravu obsahuje zákon č. 124/2002 Sb., o platebním styku, ve znění pozdějších předpisů, který upravuje vydávání a používání elektronických platebních prostředků, avšak z pohledu ochrany spotřebitele (Máče, 2006).

Klient, banka, obchodník i karetní asociace by měli mít zájem na ochraně platební karty. Ochranné prvky, o kterých budu dále mluvit, jsou technického typu, ale k jejich ověření nepotřebuje nikdo zvláštní školení ani technické zařízení a jsou snadno ověřitelné.

4.1 Bezpečnost zajišťována karetními asociacemi

Karetní asociace vydávají prostřednictvím bank platební karty. Podle ISO normy číslo 7810 musí mít karta **rozměr** 85,595 x 53,93 x 0,76 mm. Jsou povoleny odchylky v řádech milimetrů. Karta se skládá z tří vrstev PVC, které jsou odolné proti mechanickému namáhání, různým teplotám (- 36°C do 50°C), různé vlhkosti, chemickým vlivům a neobsahují toxické látky. Stanoveny jsou i poloměry zakřivení rohů karty, dislokace magnetického proužku, dislokace případně použitého mikročipu a další. Karta odlišných rozměrů není příslušným snímacím zařízením v České Republice akceptována (aplikace.mvcr.cz).

4.1.1 Líc karty

Číslo platební karty je prvek na první řádku platební karty. Obsahuje šestnáct číslic. Tento počet číslic je obvyklý pro většinu karet, ovšem toto číslo může být vyšší i nižší. První číslo, popřípadě dvojčíslí určuje druh karty. Ostatních 5 číslic značí vydavatele a posledních osm až třináct číslic označují klienta. A poslední číslice má kontrolní charakter.

BIN je označení pro identifikační číslo banky. Tento identifikátor obsahuje 4 čísla a velmi často bývá natištěno pod číslem karty a malým, neembosovaným písmem. Může ale být i nad číslem karty. Toto číslo je na kartu vytištěno už při její výrobě (finance.idnes.cz).

Platnost karty je vyznačena na druhém řádku platební karty, spolu s číslem BIN. Tento řádek můžeme mít maximální počet 19 znaků. Platnost může být na kartě vyznačena dvojím způsobem. Prvním způsobem je vyznačení počátku i konce platnosti karty a to ve tvaru MM/YY – MM/YY. Druhý způsob vyznačuje jen konec platnosti a to ve stejném tvaru MM/YY. Karty v České republice mají obvyklou platnost do 3 let (Juřík, 2001).

Dalším prvkem, který naleznete na kartě, je **jméno držitele**, které bývá na třetím řádku. Maximální počet znaků v tomto řádku je 19.

Po řádku se jménem držitele karty následuje řádek se **jménem společnosti**, která požádala o vydání platební karty. Maximální počet znaků je též 19. Například Česká spořitelna, ČSOB, ING Money Bank atd.

Hologram je další prvek objevující se na kartě. Povinně ho musí mít jen embosované karty. Je to trojrozměrný obraz, který se mění při manipulaci proti světlu, a mění barvu i tvar. Naleznete ho na přední straně platební karty, výjimečně by mohl být i na rubu karty. Poprvé se hologram objevil v roce 1981, kdy ho začala na kartu dávat společnost MasterCard. Hologram společnosti MasterCard zobrazuje

obě polokoule, společnost VISA má na hologramu letící holubici a některé karty, jakou jsou Maestro, Diner club hologram vůbec nemají. Již při výrobě hologramů musí být kladen velký důraz na bezpečí. Jsou proto vyráběny pouze jedinou tiskárnou na světě a to pro každou asociaci zvlášť. Každý má své evidenční číslo a bezpečnostním transportem jsou předávány dále do výroby karet (Juřík. 2006).

Na přední straně platební karty také nalezneme **logo** příslušné asociace, podle něhož lze jednoznačně určit produkt karty. Například VISA, MasterCard, American Expres nebo Dinners Club. Logo může být uvedeno v levém horním rohu, ale výjimečně by mohlo být uvedeno i na rubové straně karty. **Čip** rovněž zaujímá prostor na přední straně, jež je dán normou. Tuto normu je nutné dodržet zejména pro bezchybné provádění transakcí na zařízeních vybavených čipovou čtečkou.

Neobvyklými prvky, které bychom zde také mohly nalézt je fotografie, embosovaný ochranný prvek, jméno společnosti, které byly karty vydány – u služebních karet.

4.1.2 Rub karty

Na zadní straně nalezneme už jen málo ochranných prvků. Jsou jimi podpisový proužek, magnetický proužek, CVV kód, místo pro doplňující logo či text, kde můžeme najít například linku podpory pro držitele karty.

Magnetický proužek na kartě slouží jako záznamové médium pro uložení potřebných dat k provádění elektronických transakcí. V 60. letech se začal používat magnetický proužek, jehož norma byla v roce 1974 definována pomocí ISO 7810 a 7816, a bylo zavedeno strojově čitelné písmo OCR 7B (Juřík, 2001).

Má dvě nebo tři záznamové stopy s kapacitou až 1288 bitů (Dvořák, 2005).

Podpisový proužek je určen pro vzorový podpis majitele karty, který by měl sloužit k ověření majitele při platbě. Proužek je vyroben ze speciálního papíru, který při jakémkoliv pokusu o mechanickou, tepelnou či chemickou změnu originálního

podpisu velmi znatelně změní svou strukturu. Případný pokus o padělání podpisového proužku jasně identifikujete, pokud se po odstranění vrchní citlivé papírové vrstvy objeví nápis VOID, který je pevně vytištěn pod podpisovým proužkem.

CVV kód je třímístné číslo, kterým se verifikují platby přes internet. (totalmoney.etrend.sk)

4.2 Bezpečnost zajišťována bankou

Banka hraje velkou roli v ochraně platebních karet. Jedna část ochrany spočívá ve vybrané technologii banky, druhá ve vztahu ke klientovi a třetí část je bezpečnost bankomatů. Nejdůležitější roli zde hraje Česká národní banka, která vydává pravidla pro vydávání a užívání elektronických platebních prostředků, tedy i platebních karet, pro emisní banky.

Prvním nástrojem pro ovlivnění bezpečnosti je výběr vhodného klienta neboli **scoring**. Tento nástroj obsahuje ověření totožnosti klienta, což je důležité kvůli podvodným žádostem o vydání platební karty. Zjištění bonity klienta, monitorování chování klienta, schopnost včasného zjištění zhoršení jeho finanční situace, dobře propracovaný systém správy a vymáhání pohledávek. Scoring banka využívá hlavně u kreditních karet a karet charge, kde je klientovi zároveň poskytován úvěr. V tomto případě musí banka umět řídit úvěrové riziko. Banka si ověřuje, zda žadatel nemá záznam ve společné databázi rizikových klientů – Credit Bureau (Juřík, 2006).

Po tomto ověření následuje podepsání smlouvy a **vydání klientovi platební karty.** Karta je klientovi vydána na pobočce banky nebo mu bude zaslána poštou, zaslána do zahraničí nebo si ji vyzvedne na jiné pobočce. V tomto případě záleží na klientovi, který způsob si zvolí. O týden později mu je poslán poštou do vlastních rukou PIN ke kartě. V tomto případě už může klient používat svou kartu bez obav.

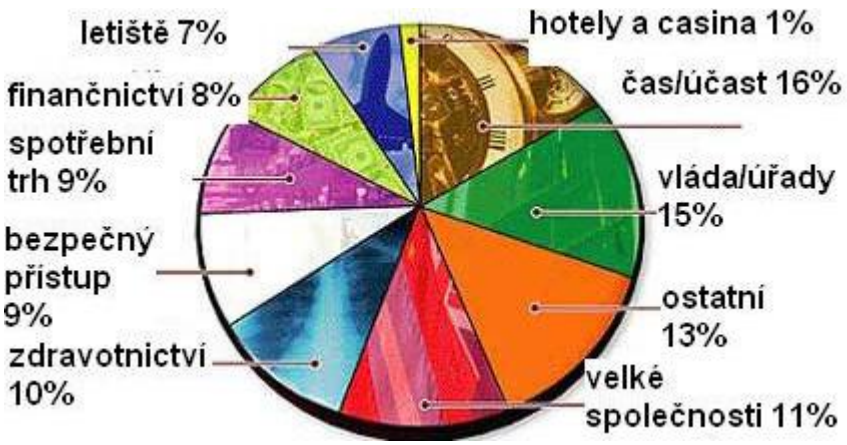
Vydavatelské banky často nabízejí současně s vydáním karty i její **pojištění**, které obvykle kryje právě takové finanční ztráty, za které vydavatel (banka) neodpovídá (tedy např. finanční ztráty vzniklé před ohlášením ztráty karty), a které kryje i další možné náklady, např. poplatky za zablokování karty. Takové pojištění je pro držitele výhodné, jeho cena je relativně nízká. Jako u všech smluv je třeba se i zde důkladně seznámit s podmínkami pojistné smlouvy, které mohou být u různých vydavatelů karet různé (www.financnivzdelavani.cz).

Další oblastí, kterou by se měla banka zabývat, jsou bezpochyby **bankomaty**. Bankomaty by měly být stále zdokonalovány, jelikož jsou velmi oblíbeným terčem zlodějů peněz. Různé podvody na bankomaty jsou rozebírány dále v kapitole 6. Jedná se především o Skimming, Lisabonskou smyčku a Shimming. Některé bankomaty, především ty nové už dokážou rozeznat cizí předmět vložený do čtečky a upozorní tak své řídící centrum. Další možností obrany je naprogramování bankomatu, aby se sám vypnul při zaznamenání cizího objektu a nastavení vibrací karty při jejím vtahování do ATM (bankomatu). Díky této vibraci je znemožněno načíst údaje z magnetického proužku nelegálním zařízením, které by se pak daly zneužít.

Pokud klient používá platební kartu, dochází k ověřování jeho totožnosti. Ověřování by mělo být založeno na třech základních principech, jimiž jsou: něco, co zná jen klient, něco, co má fyzicky pouze klient a něco, co má k dispozici pouze klient pro identifikaci. **Něco, co zná jen klient** – je heslo, PIN a podpis. PIN je číselná kombinace obsahující minimálně čtyři čísla. Je generována bankou a Českou poštou dodána klientovi do vlastních rukou. PIN – Based je označení pro autorizaci klienta pomocí PINu. Tuto číselnou kombinaci by klient v žádném případě neměl nikomu svěřovat, nikam si ho ukládat a ani zapisovat. Neměl by ho nosit současně s platební kartou. Jinak umožňuje zlodějům bezproblémový přístup k finančním prostředkům na účtu klienta. Někteří vydavatelé umožňují individuální volbu a změnu PIN držitelem karty (Juřík, 2003).

Historicky nejstarší způsob ověřování totožnosti je **podpis**, který se umisťuje na podpisový proužek, o kterém už jsem mluvila v kapitole Ochranné prvky platebních karet. Jako nejdokonalejší metoda ověření totožnosti jsou označovány **biometrické prvky**, jež mají tyto vlastnosti: snadné pořízení, snadné ověření vzorku, nepřenositelnost, nenapodobitelnost, stabilnost. Jsou to tedy trvalé fyzické nebo psychické vlastnosti jedince. Nevýhodou je nákladnost a komplexnost, chybovost a nutnost zabezpečení databáze. Výhodou je silná metoda, možnost kombinace s hesly, odolnost vůči krádežím. Mezi tyto prvky se řadí například fotografie, rozpor podpisu, otisk prstu, snímání oční duhovky, rozbor hlasu, využití vlastností jako tvar ruky nebo obličeje či způsob chůze.

Graf č. 1 – Uplatnění biometriky



Zdroj: www.systemonline.cz

Podíl technologií biometrických systémů je následující: rozpoznání hlasu 6%, rozpoznání obličeje 11%, rozpoznání duhovky 16%, dynamické snímání podpisu 6%, snímání otisků prstu 36% a geometrie ruky 27% (www.systemonline.cz).

V příloze číslo 1 naleznete podrobně rozebrány jednotlivé systémy. Biometrické systémy založené na fyziologických charakteristikách, kde jsou uvedeny různé typy biometrie – otisk prstu, geometrie ruky, sítnice, duhovka, obličejové znaky, DNA, tvar ucha, rozpoznání žil na zápěstí, charakteristika hlasu, podpisové

charakteristiky (dynamika) a charakteristiky psaná na klávesnici, dále je zde popsáno rozhraní s uživatelem, výhody, nevýhody, přesnost a objem dat v Bytech.

4.3 Bezpečnost zajišťována klientem

Pro zajištění bezpečnosti financí ze strany klienta vydaly banky **Desatero bezpečnosti**, které obsahuje tyto body:

1. „Chraňte svůj certifikát v souboru nebo na čipové kartě
2. Používejte bezpečné heslo / PIN
3. Ochraňujte své heslo / PIN
4. Nastavte si zasílání zpráv a sledujte historii svého přihlašování
5. Pravidelně aktualizujte operační systém, prohlížeč a veškeré programové vybavení
6. Používejte svůj počítač
7. Používejte programy, které chrání Váš počítač, jako jsou antivirové programy, anti-spywarové programy a osobní firewally
8. Nenavštěvujte neznámé stránky a nestahujte z internetu neznámé soubory
9. Otvírejte pouze důvěryhodné e-maily
10. Kontaktujte nás při jakýchkoliv pochybnostech“ (www.mojebanka.cz).

Certifikát je „přístupový klíč“ k vašemu účtu. Porušením tohoto pravidla se dopustíte i v případě, že obsluhujete své i firemní účty přes přímé bankovnictví (používáte jeden a ten samý certifikát) a sdělili byste ho ve firmě kolegovi. Ke zvýšení této bezpečnosti banky nabízejí čipové karty MůjKlíč. Bezpečným PINem se stává kombinace velkým a malých písmen, číslic, speciálních znaků

a mělo by mít minimálně osm znaků. Doporučuje se odborníky měnit **PIN** po určitých časových intervalech. Nezapisovat ho do mobilu, diáře, na kartu ani na poznámkové papírky. Komerční banka poskytuje svým zákazníkům zasílání zpráv, pro kontrolu historie plateb provedených z účtu nebo platební karty. Dále k přihlašování je nevhodnější používat pouze svůj počítač, na kterém pravidelně instalujete soubory, které odstraňují chyby. Pravidelně aktualizujte i **antivir**, dále je vhodné používat i anti - spywarový program. Nikdy nesdělujte pomocí e-mailu své důvěrné údaje – osobní údaje, PIN, heslo, kód. Banky tyto údaje nikdy nevyžadují. Jedná se ty o tzv. Phishing, o kterém bude hovořeno v 7. kapitole této práce. Pokud objevíte nějaké nesrovnalosti, nebo pochybujete při práci s internetovým bankovnictvím, ihned kontaktujte svou banku (www.bankovni poplatky.com).

Stejně tak existuje i **Desatero zásad plateb v zahraničí**:

1. „Nenechávejte platební kartu nikdy bez dozoru a buďte ostražití před všudypřítomnými zloději. Za žádných okolností nikomu nesdělujte PIN, ani obsluze v restauraci či recepci v hotelu
2. Platební kartu je vhodné ukládat ve vnitřních kapsách blízko těla, v pouzdrech, apod. Noste platební kartu odděleně od osobních dokladů a peněz. Pravidelně kontrolujte, zda kartu máte.
3. Nikdy nedávejte kartu obchodníkovi jako zástavu, třeba v půjčovně aut nebo mopedů. V podezřelých provozovnách raději plaťte v hotovosti, nebo upozorněte policii.
4. Sledujte obchodníka při manipulaci s kartou a v žádném případě nenechte číšníka v restauraci nebo recepčního v hotelu, aby vám s kartou zmizel z dohledu. Snadno si může opsat číslo karty, její exspiraci a především CVV nebo CVC kód na zadní straně karty napravo od podpisu. Tyto údaje pak umožní zloději nakoupit např. v internetových obchodech.
5. Zbystřete svoji pozornost, pokud by se prodavač v obchodě pokoušel kartu načíst kvůli jedné transakci v několika různých terminálech. Je třeba mít

na paměti, že bankovní terminály vždy vydávají potvrzení o platbách, a to i v případech, když neproběhnou. Pokud tedy z terminálu nevyjede žádné potvrzení, může to být znamením, že jde o podezřelou transakci.

6. Vždy je třeba zkontrolovat, zda karta, kterou vám vrátil obchodník nebo personál hotelu či restaurace, je doopravdy vaše. Uschovávejte si doklady o všech transakcích pro případnou reklamaci a ihned po návratu z dovolené je srovnejte s údaji na bankovním výpise.
7. Při výběru z bankomatu si nejprve prohlédněte otvor, do kterého vkládáte kartu. Pokud vypadá nestandardně, zvolte raději jiný bankomat. Vybírejte vždy sami, při zadávání PIN kódu do bankomatu si zakryjte druhou rukou klávesnici a řiďte se výhradně pokyny na obrazovce. Nikdy neuschovávejte opsaný PIN kód společně s platební kartou. Nikdy nevěřte pověrám typu „Když zadáte PIN obráceně, … Když stornujete platbu ihned po zadání PIN, …“ atd. Základní proces výběru z bankomatu je stejný všude na světě…
8. Kartu používejte nejlépe v bankomatech uvnitř nebo v malé blízkosti od bankovních poboček. Tyto bankomaty často hlídají kamery, které mohou zaznamenat, kdyby někdo k přístroji připevnil čtecí zařízení.
9. Pokud by bankomat vaši kartu zadržel a nevysvětlil to informací na lístečku nebo na obrazovce, od bankomatu neodcházejte a spojte se s bankou nebo případně i s policií. Stejný postup platí, pokud z bankomatu nevyjely bankovky, protože v něm může být instalováno zařízení, které peníze zadržuje.
10. V případě ztráty nebo krádeže oznamte událost okamžitě bankovnímu operátorovi na bezplatné infolince a kartu ihned zablokujte. Pokud vaši kartu někdo zneužije, můžete případně ještě před odjezdem na dovolenou zmenšit ztráty nastavením maximálního denního limitu pro provedení bankovních transakcí. Vhodné je i zřízení pojištění proti ztrátě karty (některé karty jej mají automaticky v sobě). (www.bankovnipoplatky.com).“

4.4 Skutková podstata trestného činu

Různé typy podvodů vedou ke stále novým technologiím výroby a vzniku stále nových ochranných prvků. Vše závisí na vzájemné spolupráci jak kreditních asociací, tak bank, policie i veřejné moci státu. Ochranná opatření musí být stanovována tak, aby pachatelé museli vynaložit stále více času a finančních prostředků k jejich překonání. Vývoj ochranných prvků a opatření se nemůže nikdy zastavit, vždy musí být o krok napřed před zloději. Jelikož platební karty jsou považovány za cenný papír, upravuje jejich skutkovou podstatu **Český trestní zákon č. 14/1961 Sb.** a to v paragrafu 140 – 142 kde se hovoří o padělání a pozměňování peněz, udávání padělaných a pozměněných peněz, výrobě a držení padělatelského náčiní. Jedná se tedy o paragrafy hovořící výhradně o penězích. Ovšem paragraf 143 tato ustanovení rozšiřuje ochranu §140 – 142 též penězům jiným než tuzemským, tuzemským a cizozemským bezhotovostním platebním prostředkům, jakož i tuzemským a cizozemským cenným papírům. Do této skutkové podstaty spadá i padělání platebních karet. Tento samý zákon upravuje i skutkovou podstatu neoprávněného držení platební karty. § 249 výslovně říká: „Kdo si neoprávněně opatří nepřenosnou platební kartu jiného, identifikovatelnou podle jména nebo čísla, nebo předmět způsobilý plnit její funkci, bude potrestán odnětím svobody až na dvě léta, nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty (business.center.cz/business/pravo/zakony/trestni _zakon).“

Další zákon, který upravuje trestnou odpovědnost je **Zákon č. 284/2009 Sb., o platebním styku.** Den 4. prosince 2001 na základě tohoto zákona, konkrétně § 16, vydala Česká národní banka Vzorové obchodní podmínky pro vydávání a užívání elektronických platebních prostředků. Paragraf číslo 16 určuje, jak vysoký počáteční kapitál musí mít instituce, která chce poskytovat platební službu podle paragrafu 3. Paragraf 3 pak definuje Platební službu (business.center.cz/business/pravo/zakony).

Vzorové obchodní podmínky pro vydávání a užívání elektronických platebních prostředků mají doporučující charakter. Cílem těchto podmínek

je ochrana držitelů platební karty s důrazem na snížení odpovědnosti držitelů za zneužití platebních karet. „Základem pro přípravu Vzorových obchodních podmínek bylo Doporučení Evropské komise 97/489/ES o elektronických platebních prostředcích. Právě vzhledem k jeho charakteru se Česká republika Evropské komisi zavázala k jeho transpozici formou doporučení centrální banky (www.cnb.cz).“

Pouze Komerční banka snížila tuto odpovědnost držitele. Držitel po nahlášení odcizení karty neručí vůbec za krádež při on-line transakcích. V případě sprinterů ručí za transakce do půlnoci toho dne, kdy nahlásil ztrátu. V plném rozsahu držitel karty ručí za krádež v případě, že prozradil svůj PIN (http://www.kb.cz/file/cs /produktove-listy/kreditni-karta-visa-electron-p.products).

5 První podvody s platebními kartami

Zneužívání platebních karet začalo ve stejnou dobu, jako vznikly první karty. Jakákoliv nová technologie na zabezpečení, zrychlení nebo zpříjemnění používání karet přinesla i nové možnosti podvodů. **První podvody** spojené s platebními kartami se objevily už v 60. létech ve Spojených Státech Amerických, když se karty začaly vydávat i klientům, kteří o ni vůbec nestáli a nebyli schopni splácet své dluhy. Původně odhadované ztráty banky Bank of America byly 4%, ale ve skutečnosti se vyšplhaly až na 22%. Tato ztráta představovala 8.8 milionů zlatem krytých dolarů. Zajímavé na tom bylo to, že karty chodily lidem do schránek, aniž by si ji domluvili s bankou nebo dokonce podepsali smlouvu. Proto jim i soud dával za pravdu, když se dlužníci domnívali, že nemusí platit své úvěry z karty. Existovaly také organizované gangy, které se specializovaly na vykrádání poštovních schránek. Snadno tak získaly ještě nepoužité platební karty BankAmericard. Karty posléze začali krást i pracovníci pošt a prostitutky. Toto všechno bylo způsobeno tím, že karty se mezi lidi dostaly velice rychle, aniž by byla zajištěna jejich bezpečnost. Nebyly vytvořeny potřebné zákony, které by vymezovaly zločiny spáchané zneužitím kreditních karet (Juřík, 2006).

Neexistovalo ještě ani zajištění PINem a jakákoliv transakce byla provedena **pouze proti podpisu**. Což bylo pro zloděje usnadněním, jelikož ukradli ještě nepodepsanou kartu, kterou mohli krásně využívat. A jelikož byly karty nové, měly obvykle kredit v hodnotě 1000 dolarů. Banka Bank of America nebyla jediná, která byla okrádána. V té samé situaci se nacházely i banky Wells Fargo Bank, která hlásila ztrátu 28 milionů dolarů v letech 1967-1970. Citibank přišla o 11 milionů, Banker Trust 21 milionů dolarů a mnoho dalších bank bylo ve stejné situaci. Celkové ztráty všech bank vydávajících platební karty činila 425 mil. dolarů v roce 1970. Ve stejném roce byl přijat v USA zákon o zákazu rozesílání nevyžádaných karet do poštovních schránek, který podepsal prezident Nixon (finance.idnes.cz/historie-platebnich-karet-podvody).

Dalším způsobem jak lidé přicházeli a troufám si říct, že ještě dnes přicházejí o peníze, jsou opakované **platby pod autorizační limit.** Na počátku platebních karet existovaly počítače jen málo a internet byl ještě v nedohlednu. Byla – li karta odcizena nebo padělána, měl pachatel o něco snazší možnost zcizení peněz než dnes. Tehdejší autorizační limity byly velmi vysoké, činily většinou až 50 dolarů. V tu dobu probíhalo velmi pomalu zúčtování transakcí a velmi pomalu se aktualizovaly seznamy zablokovaných či zneužitých platebních karet. První seznamy začala vydávat banka Dinners Club v 50. letech a měli podobu tištěných knih obsahujících čísla karet. I přesto měl zloděj asi týden času, než zjistily, že karta je kradená. Teprve vznik terminálů, které disponovaly aktuálními seznamy, zamezily používání odcizených karet. Ani **první bankomaty** nebyly ochuzeny o krádeže. Historicky první bankomat se objevil v pobočce londýnské Barclays Bank 27. června 1967 (Juřík, 2006).

Tyto bankomaty fungovaly na základě děrných štítků, které si klient obstaral na pobočce a po jeho vložení do bankomatu získal hotovost. Z důvodu nepraktičnosti a nízkému zabezpečení se takto vybírala hotovost po dobu 3 let. Izraelský gang totiž brzy rozluštil algoritmus zabezpečení a ve velkém začal vybírat hotovost. Až po této události vynalezla firma IBM magnetický proužek a nové bankomaty. Velice závažné zneužívání karet se objevilo na počátku 90. let a má je na svědomí **Andrew Stone** (www. Theregister.co.uk).

V tuto dobu byl magnetický proužek standardem v ochraně karet. Andrew Stone byl IT expert, který ale profitoval ze slabin bezpečnostního systému platebních karet. Objevily se stížnosti klientů na záhadné výběry z jejich účtů. Oběti ani nemohly dát tento případ k soudu, jelikož nebylo možné přesvědčivě určit, že byl použit při výběru PIN. Bezpečnostní expert Alistair Kelman u soudu, kde zastupoval na 2000 klientů, uvedl způsob, kterým Stone postupoval při krádežích. Stone využil skutečnosti, že číslo účtu na magnetickém proužku je magneticky přepisovatelné a vyzkoušel přepsat své číslo manželčiným. Vznikla tak karta, která obsahovala jeho PIN a číslo účtu manželky. Když tuto kartu vložil do bankomatu a zadal svůj PIN,

autorizoval tak výběr z manželčina účtu. Pak už jen stačilo získat další a další celá čísla účtu, kterých se v okolí bankomatů, v odpadkovém koši vyskytovalo nespočetné množství a skandální případ byl na světě. V roce 1996 Andrew Stone, počítačový bezpečnostní poradce od Hampshirea ve V. Británii, byl odsouzen za kradení více než 1milión liber (v té době ekvivalentní k nám $1.6 milión) na pět let a šest měsíců (www.theregister.co.uk).

6 Rizika spojená s používáním platebních karet

6.1 Podvod bez přítomnosti platební karty

Již z názvu vyplývá, že podvody bez přítomnosti karty, jsou takové, kde není majitel platební karty fyzicky přítomen na místě manipulace s kartou. Nejčastěji jsou tyto transakce uskutečněné při telefonních, písemných nebo internetových objednávkách zboží či služeb. K vysokému výskytu těchto neoprávněných transakcí dochází z důvodu toho, že obchodník nemá možnost zkontrolovat identitu zákazníka. Podvodníci získávají data ze **zahozených či zkopírovaných potvrzení o transakci,** případně různými podvody, které jsou uvedeny v kapitole 7. Majitel se o krádeži peněz nedozví, dokud se nepodívá nebo mu nepřijde výpis z účtu.

„Banky a vydávající instituce mají k dispozici řadu možností, jak čelit podvodům bez fyzické přítomnosti karty:

- v souladu s pravidly kartových asociací se na karty s magnetickým proužkem tiskne třímístný kontrolní kód do podpisového proužku na zadní straně karty, který je při platbě bez přítomnosti karty obchodníkem požadován jako autentizace skutečnosti, že klient má kartu ve svém držení;

- zavedení nového prvku autentizace pro bezpečné platby - technologie 3D Secure, která umožní autentizaci držitele karty anebo obchodní společnosti (pro její využívání je nutná registrace u kartové asociace – VISA označuje tuto technologii jako "Verified by VISA", MasterCard jako "MasterCard Securicode)";

- rozšíření výhradně čipových karet při provádění plateb na internetu - k provádění plateb po internetu bude zapotřebí čtečka čipové karty připojená k počítači, ze kterého je transakce prováděna; tato čtečka zprostředkuje autentizaci oprávněného držitele karty;

- využívání inteligentních počítačových programů, které mohou sledovat chování platební karty a rozpoznat neobvyklé typy transakcí, resp. upozornit na četnější výskyt transakcí bez přítomnosti karty na jednotlivé kartě nebo u konkrétní obchodní společnosti;

- někteří vydavatelé karet nabízejí další způsoby ochrany před podvody bez přítomnosti karty:

    - úplný zákaz transakcí bez přítomnosti karty provedených na základě telefonní, písemné, faxové nebo elektronické objednávky;
    - omezení maximální výše transakcí bez přítomnosti karty;
    - umožnění platby bez přítomnosti karty jen na vyžádání (dočasné odblokování na základě žádosti držitele karty a následné zablokování);
    - vydání virtuální karty se sníženými limity, která je určena pouze pro platby bez přítomnosti karty“ (www.bankovnikarty.cz-Podvod_bez_ přítomnosti_karty).

6.2 Padělky karet

Padělaná karta **je definována** jako karta vyrobená a personalizována bez souhlasu vydavatele. Nebo taková karta, která byla vydána právem, ale později vizuálně upravena či pozměněna po stránce elektronických dat. Ke zkopírování může docházet u obchodníka, který si před vrácením karty zkopíruje magnetický proužek. Dále také v bankomatu, kde je umístěno kopírovací zařízení. K tomu podvodu dochází nejčastěji u bankomatů, v barech, restauracích, u čerpacích stanic nebo v hotelech. Na území České republiky se objevuje tento nelegální způsob získávání peněz stále častěji. Jednou z možností, jak zamezit takovým to situacím je zavedení čipových karet, kde čip zamezí kopírování údajů. Druhou možností jsou inteligentní programy v počítačích, které umožňují sledování chování platební karty, a rozpoznají tak neobvyklé transakce – částku, čas, místo (www. bankovnikarty.cz - Podvody_padělanou_kartou) .

6.3 Podvodná žádost o kartu

Je podvod, který vychází z jiného podvodu a tím je **odcizení identity** – tedy odcizení osobních údajů a použití jich k dalšímu podvodu. Podvodník tak může zažádat o otevření účtu a vydání platební karty. Druhým způsobem pro využití odcizené identity je převzetí účtu klienta. Pachatel se vydává za majitele účtu a platební karty a ve snaze podvést banku žádá o změnu parametrů karty nebo účtu. Nejčastěji tak mění například adresu a potom žádají o vydání nové platební karty.

Sdružení bankovních karet dává doporučení jak se chránit před odcizením identity:

- „Dávejte pozor na to, jakým způsobem se zbavujete dokumentů, které obsahují osobní údaje a údaje o vaší kartě či vašem účtu.
- Potvrzení o výběru z bankomatu, výpisy, informace o zůstatku na účtu a prodejní doklady uchovávejte alespoň po dobu 2 měsíců pro možnost reklamace.
- Před vyhozením všechny dokumenty vždy roztrhejte nebo rozdrťte, apod.“ (www.bankovnikarty.cz - Podvody_se_zcizenou_identitou).

6.4 Zneužití nedoručené karty

Tato situace nastává v době, kdy karta není doručena majiteli a to z důvodu špatné přepravy od vydavatele k majiteli. Majitel tuto situaci nemůže ovlivnit, ale může ji zavčasu pomoct odhalit. Klient ví, že mu karta má přijít, pokud mu tedy v předpokládaném čase nepřijde, měl by kontaktovat banku. Pro zamezení tohoto způsobu podvodu, který se dnes stává už jen ojediněle, posílají banky karty v neaktivním stavu, aktivní se stává až po aktivaci klientem dle pokynů banky. Nejdůležitějším krokem je poslání karty a PINu zvlášť a s časovým odstupem (www.bankovnikarty.cz - Podvody_kartou_ztracenou_v_poště).

6.5 Úvěrové ztráty

Úvěrové ztráty jsou takové, které způsobí bance klient z důvodu **neschopnosti splatit** své výdaje, které realizoval svou platební kartou. Základní ochranou pro banky je znalosti bonity klienta a schopnost včasné zjištěné zhoršující se finanční situace klienta, na kterou by měli banky umět rychle zareagovat. Většina klientů má proto s bankou sjednán limit, který nemůže překročit. Při platbě je vždy potřebná autorizace, tedy zda je požadovaná operace krytá finančním limitem klienta. V případě debetních karet je zjišťován zůstatek na běžném účtu. V případě překročení limitu nebo zůstatku na účtu není platba autorizována (Juřík, 2006).

7 Platební karty a jejich nejčastější podvody

Součástí bezpečnosti je potřeba znát, čemu se bránit, proto autorka zařadila do své práce kapitolu o nejčastějších podvodech spojených s platebními kartami. Mezi nejčastější podvody patří Skimming, Lisabonská smyčka, Shimming, napadení terminálů, Offline a online zneužití údajů z platební karty, Shoulder surfing, snižovací programy a viry, Phishing, Pharming, telefonní phishing, krádež identity a převzetí účtu, nalezení kradené karty. Každý z těchto druhů podvodů je dále rozvinut.

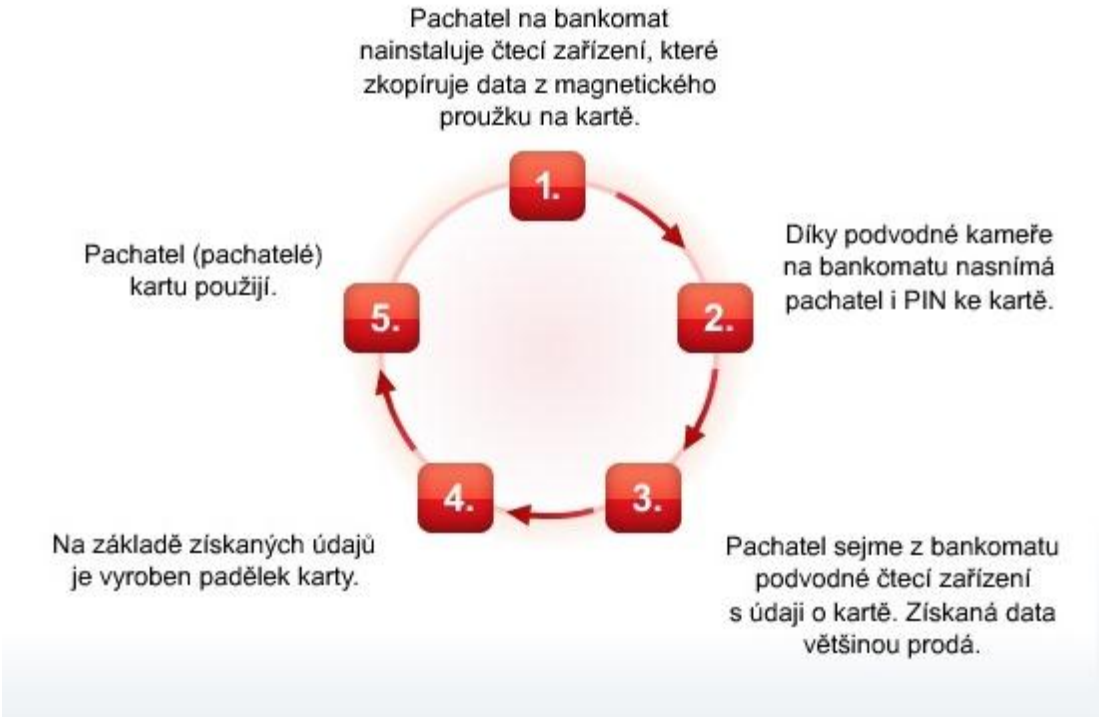
7.1 Skimming

Skimming je podvodné načtení údajů z magnetického proužku na kartě pomocí čtecího zařízení, které je umístěno na bankomatu. Pochází z anglického to skim („sbírat smetanu), přeneseně tedy vytěžit z karty to nejlepší. Skimming je celosvětový fenomén a stojí za ním většinou dobře organizované zločinecké skupiny. První skimmovací zařízení na bankomatech se ve světě objevilo už v 90. letech minulého století, v ČR poprvé v roce 2001. Smyslem a cílem skimmingu je získání karetních dat a ty následně použít pro výrobu padělku platební karty. Kartu pachatelé většinou zneužijí mimo zemi, kde data původně získali. V příloze číslo 2 nalezete obrázek s napadeným bankomatem při skimmingu. **Číslo 1** na obrázku je vstupní otvor, který obsahuje vstupní ochranný nástavec, který má za úkol snižovat možnosti instalování podvodné čtečky. Zámeček, který je vrchu nástavce by měl být vždy vidět celý. Pokud není vidět celý nebo je ikonka zámečku zalitá, obsahuje zařízení ochranný antiskimovací nástavec. Podvodné zařízení bývá ve stejné zelené barvě a je přímo na ochranném nástavci. **Číslo 2** ukazuje abyste při výběru dali pozor na klávesnici, do které vyťukáváte PIN. Při skimmingu se totiž pořizuje záznam zadávání PIN kódu (který z magnetického proužku nedostanete). Bezpečná klávesnice vypadá tak, že klávesy jsou volné, nic je nepřekrývá. Klávesnice je pevně spojena s bankomatem a tvarově přesně lícuje. Skimovací zařízení řeší klávesnici tak, že buď je na bankomatu nainstalovaná podvodná deska,

která je umístěna přes celou pultovou plochu, která tam na pohled nesedí. Nebo je klávesnice přelepena fólií, která slouží k identifikaci závadného PIN kódu. **Číslo 3** označuje horní rám nad obrazovkou bankomatu. Kde při skimování bývá ukrytá podvodná kamera. Správně panel nad obrazovkou a klávesnicí bankomat osvětluje a tato osvětlující část je plochá a neobsahuje žádné jiné barvy. Pokud je zde nainstalovaná kamera, pak je na horním rámu nová lišta v celé jeho délce, která je užší než rám a tvoří nový tvar. Na liště je vidět alespoň jeden otvor o velikosti 1 mm pro objektiv kamery (www.csas.cz - jak-vyzrat-na-skimming).

Následující obrázek popisuje postup skimmingu.

Obrázek č. 1 – Postup pro zneužití karty pomocí skimmingu



Zdroj: www.csas.cz

S tímto zařízením se můžete setkat také všude tam, kde ztratíte svou platební kartu z dohledu. Například v restauracích, u automatů na parkování, u benzínové pumpy, kde se platí pomocí stojanu nebo starší a pozměněné platební terminály, které pracují

s magnetickým proužkem. Zbraní proti autorům skimmingu v rukou bank a policie je i účinná metoda **tzv. data mining.** (Juřík, 2006)

Zde jde o hledání průniku transakcí klientů, kteří nahlásili podezřelé transakce svých karet způsobené zřejmě kopií platební karty. Banka tak analyzuje všechny platební terminály a bankomaty, kde klient používal svou kartu. Snaží se najít takové místo, které by použili všichni stěžující si klienti. Pokud takového místo najdou, naznačuje to, že zde může docházet ke skimmingu.

7.2 Lisabonská smyčka

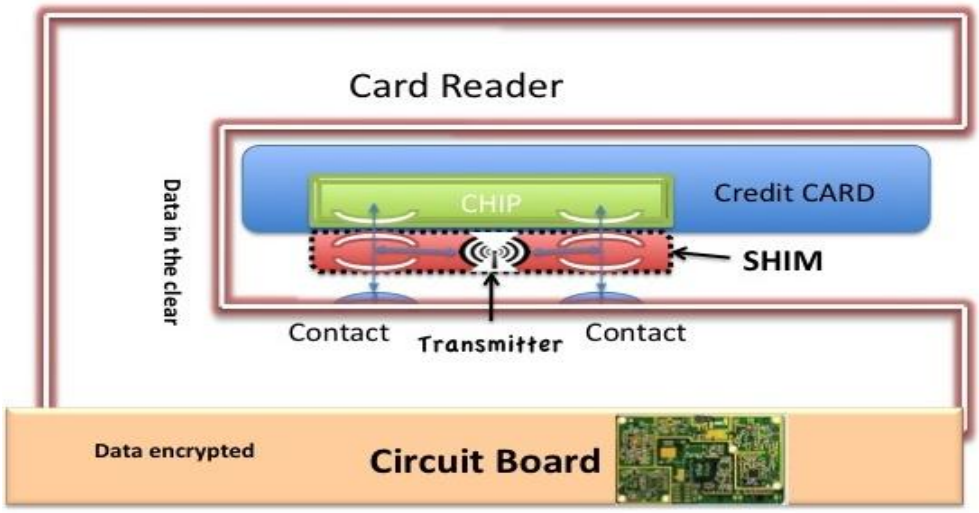
Jedná se o velmi primitivní útok na peníze klientů a zneužívá hlavně nevědomí klientů o existenci tohoto podvodu. Technické zařízení způsobí, že se karta nedostane do bankomatu, ale ani zpět k držiteli karty. Na lisabonskou smyčku je většina českých bankomatů **odolná,** takže se s ní už běžně nesetkáte. V blízkém okolí bankomatu je pachatel, který bankomat sleduje a postiženému držiteli karty ochotně nabídne pomoc při vyproštění karty. Pomoc se "nezdaří" a než je karta držitelem zablokovaná, má pachatel volné ruce k jejímu zneužití. Obrana: Pokud karta uvízne a nelze ji vytáhnout ven, neopouštět bankomat, kartu ihned telefonicky zablokovat a ideálně z místa přivolat pracovníka banky, ostrahu nebo policii. Zde jde opravdu o jakousi smyčku, kterou vynalezli podvodníci v Lisabonu. Podvodníci k tomu používají klasický **film z fotoaparátu**, který se i dnes v době digitální techniky dá ještě velmi snadno koupit. Film do fotoaparátu se přeloží na půl a vyříznou se do něj malá okýnka, která slouží jako háčky pro zachycení platební karty. Takto napůl přehnutý film se zastrčí do otvoru pro kartu v bankomatu a hned následující klient je chycen do pasti. Bankomaty se vybavují speciálními nástavci na otvor pro vložení karty, právě proto, aby nebylo možné nainstalovat zde skimming nebo lisabonskou smyčku. Nástavce jsou charakteristické svým tvarem a nevhodné pro instalaci dalšího zařízení. I samotné nástavce obsahují specifické prvky, které znemožňují jejich padělání (www.mesec.cz).

7.3 Shimming

Shimming je další z možností útoků na **bankomaty**, který nahrazuje klasický skimming. V překladu shimming znamená vypodložení. A právě tento výraz má své opodstatnění. Tento podvod funguje tak, že tzv. dummy kartou podvodník vloží do otvoru na kartu méně než **0.1 mm širokou ohebnou fólii** vybavenou vysílačem a logikou. Jen pro představu vaše kreditní karta je 0,76 mm tlustá, zrnko soli je 0,5 mm silné a lidský vlas je o 0.18 mm tloušťky. Nejmenší objekty, které bez pomoci lidské oko zahlédne, je asi 0,1 mm. Tato ohebná fólie s čipem se přilepí na snímač čipu v bankomatu. Potom co vložíte kartu do bankomatu, je tento obvod přesně mezi čipem na kartě a snímacím zařízením bankomatu a tím funguje jako prostředník. Po zahájení činnosti bankomatu obvod zaznamená veškerou komunikaci a odešle ji podvodníkovi. Ovšem komunikace může být šifrovaná i nešifrovaná. Pokud je komunikace šifrovaná dokáže tento obvod zadržet pokyn od čipu na kartě, sdělující šifrovanou komunikaci a změnit ji na nešifrovanou. Nejčastějším místem tohoto útoku je střední a východní Evropa. O **shimmingu** se dá říct, že je to mistrovské dílo, jelikož výroba takového zařízení vyžaduje profesionální technologické zázemí. Klient nemá možnost poznat, že bankomat obsahuje toto zařízení, veškerá obrana je tedy na výrobcích bankomatů, kteří by měli lépe zabezpečit bankomat (www.net workworld.com).

Obrázek číslo 2 znázorňuje umístění shimmingu v bankomatu.

Obrázek č. 2 – Schéma umístění shimmingu



Zdroj: http://www.networkworld.com/community/node/63544

7.4 Napadené terminály

Napadené terminály se objevily v roce 2008 v západní Evropě. Jednalo se o terminály, které byly už ve výrobně pozměněny a instalovány na různá místa už se zařízením, které je zneužívalo ke krádežím. Jednalo se o závažnou kauzu o **prolomení** do té doby bezpečné čip a PIN technologie. Vyšlo najevo, že čínsko-pákistánský gang instaloval do čerstvě vyrobených terminálů zařízení, které odesílalo data přes GSM rovnou do Pákistánu. Tyto terminály se v tomto roce rozšířily po celé západní Evropě, hlavně tedy do Velké Británie, Irska, Holandska, Dánska a Belgie. Kvůli této aféře udělali experti z Cambridgské univerzity výzkum o bezpečnosti platebních terminálů. V televizní show BBC pak tito vědci předvedli, jak je jednoduché získat PIN moderátora, který použil terminál Ingenico i3300 nebo Dione Xtreme (dva druhy nejrozšířenějších terminálů v Anglii). A skutečně tak udělali, zjistili jak PIN, tak i číslo platební karty, platnost a jiné. Dále tímto výzkumem zjistili, že i platební terminály mohou být zneužívány pomocí shimmingu – tedy vložení obvodu mezi čtecí zařízení a čip platební karty (www.telegraph.co.uk/).

7.5 Offline a online zneužití údajů z platební karty

Velkým rizikem platebních karet je, že obsahují údaje, které jsou dostatečné pro provedení offline transakcí či k transakcím na dálku. Kdokoliv dostane do rukou vaší kartu, dostane se k těmto údajům, může si je zapamatovat, popřípadě zapsat či vyfotit skrytou kamerou a později je **zneužít.** Pouze dvě věci jsou potřeba k těmto transakcím a to je číslo platební karty a CVV kód. Způsoby offline zneužití můžou být přes katalogový prodej či nákup zboží nebo služeb přes telefon. V prvním případě jde o to, že podvodník si objedná zboží a u způsobu zaplacení uvede údaje získané z platební karty, které jsou ovšem kradené. Nic netušící zásilková firma odešle zboží pachateli, který jej může obratem prodat či jinak použít a peníze, které vydělal, se objeví v šedé ekonomice. Obdobným způsobem probíhá i nákup přes telefon, kdy k dokončení objednávky stačí zadat číslo karty, cvv kód a dobu platnosti. Tento problém řeší zásilkové obchody tím, že zboží doručují jen na jméno uvedené na objednávce a na jméno na kartě. Což pro pachatele není problém, protože si může pronajmout vlastní schránku na falešné jméno. Dalším způsobem jak se chránit, je vyhledání čísla v databázi kradených karet. Zde může být problém v tom, že oběť si ani nevšimne, že je její karta zneužívána, neví totiž, že si číslo její platební karty někdo opsal a zjistí to, až když jí záhadně zmizí peníze z účtu. Stejný problém nastává i při obchodování přes internet, což je online služba. Stejně jako v předešlých případech stačí k platbě jen údaje na kartě, fyzickou kartu u sebe mít nemusíte, stačí, když znáte správné údaje. S velkým rozšířením internetu se tyto podvody stávají závažnější a častější než objednávky přes telefon nebo katalogový prodej. Dnes už je tento problém více zabezpečen, jelikož existují speciální **virtuální karty**, kterými se platí pouze na internetu. Tyto karty neexistují ve fyzické podobě, banka vám sdělí jen údaje potřebné pro platbu. Na internetu můžete platit i obyčejnou debetní nebo kreditní kartou, která ale musí být aktivována na platby přes internet (http://www.visa.cz/cz/osobni_karty/vyberte_si_vasi_visa_kartu/).

7.6 Shoulder surfing

Shoulder surfing je asi nejsnadnější způsob jak se dostat k cizím údajům platební karty a následně je použít. Jak už sám název naznačuje, jedná se o **koukání přes rameno**. Pokud nejste opatrní při objednávání zboží na internetu, při katalogovém nákupu nebo při nákupu přes telefon, může vám kdokoliv koukat přes rameno, když zadáváte vaše citlivé údaje o platební kartě, a tím získat spolehlivé údaje. Zjistí tím už mnohokrát zmiňované údaje – číslo platební karty, CVV kód, datum platnosti karty. Ví také, že tato karta je funkční, není zablokovaná pro transakce na internetu, je na ní zůstatek peněz, který lze využít. Takto jsou charakterizovány i podvody způsobené příbuznými. I přesto, že jsou tyto podvody velmi časté, tak nejsou tolik závažné velikostí způsobené škody. Jediným a nejúčinnějším způsobem ochrany dat je dávat si pozor kdo je kolem vás v době kdy používáte platební kartu, nedávat kartu z ruky a nenechávat ji volně ležet na stole či kdekoliv jinde. Toto riziko existuje i v supermarketech nebo místech s velkým průtokem lidí, na kterých se platí velmi často platební kartou (http://volkerroth. com/download/Roth2004c.pdf).

7.7 Spyware, sniffovací programy a viry

Spywere je program, který bez vědomí uživatele odesílá informace z počítače pryč. Toto je skutečný problém 21. století, tedy zranitelnost osobních počítačů a nedostatečná gramotnost uživatelů o počítačové technice. Tento program se často šíří jako adware nebo jak už jsem uvedla bez vědomí uživatelů, ale s vědomím autorů spywere a je často součástí shareware. Pokud si tento program nainstalujete a spustíte, nainstalujete si do počítače právě i spywere. Často se tak stane s programy na stahování hudby a videa od ostatních uživatelů. Jsou to programy, které běží na počítači bez vědomí majitele, a buď ho poškozují, nebo znatelně zhoršují jeho funkci. Že máte tento program nainstalovaný, se dá poznat podle těchto nežádoucích

jevů: vaše domovská stránka, kterou máte nainstalovanou na svém prohlížeči, byla přesměrována na jinou stránku. Když máte pomalý start počítače i internetu. Vyskakují vám ve vyšší míře reklamní okna při surfování na internetu, padají vám Windows systémy, záhadně se vám objevují nové ikony na ploše. Obrana proti těmto nežádoucím softwarům je jednoduchá. Proti spywaru se dá bránit dodržováním několika zásad, které se v podstatě neliší od ochrany proti jakémukoli nežádoucímu softwaru. Jedná se především o používání **antispywarového softwaru** v počítači, firewalu, provádět pravidelně aktualizaci operačního systému a internetového prohlížeče, používat nejnovější verzi preferovaného internetového prohlížeče, jež ve většině případů obsahuje pokročilejší způsoby ochrany uživatele. Dále pak neinstalovat podezřelé programy, neoriginální programy nebo programy z neznámých zdrojů. (www.bezpecnyinternet.cz)

K odstranění těchto programů se používají antispywarové softwary, protože běžný antivirový software je neodhalí. Měli by se používat různé antispywarové programy, protože tyto programy mají různé databáze spywerů. **Sniffovací programy** jsou velmi jednoduché a zaznamenávají každé kliknutí na klávesu počítače. Tyto programy jsou běžné, ale běžný uživatel není schopen je odhalit. Obezřetní by měli být proto uživatelé hlavně veřejných počítačů, do kterých může kdokoliv nainstalovat tyto programy. Ale ani osobní počítače nejsou zcela bezpečné. Stačí, když jej majitel dá do servisu, na vyčištění či přeinstalování. Existuje různá vyspělost těchto programů, u některých si data musí stáhnout sám pachatel a ručně vyhledat hesla, u některých už to za něj udělá program a data mu rovnou odešle pomocí internetu. Je tedy jasné co bude následovat, když pachatel získá například váš přístup do internetového bankovnictví či údaje potřebné pro obchodování přes internet (http://technet.idnes.cz/nejlepsi-antispywarove-nastroje-zavrou-spionum-dvere-pred-nosem).

7.8 Phishing a telefonní phishing

Původ tohoto označení má kořeny v anglickém slově fishing, značícím rybaření, což je více než výstižné. (www.lupa.cz)

Phishing jsou podvodné **e-mailové zprávy**, které mají vzbudit dojem, že byly odeslány z e-mailové adresy banky, která vám vystavila platební kartu. E-mail je obvykle psán anglicky nebo špatnou češtinou, obsahuje odkaz na údajné stránky banky a vyzývají k potvrzení osobních bankovních údajů. Phishingová zpráva může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů či dokonce jako výzkum klientské spokojenosti. Cílem podvodného e-mailu může být získání klientského čísla a hesla adresáta, bezpečnostního kódu nebo například PIN k platební kartě či dalších bezpečnostních údajů a jejich následné zneužití. Že jde o **phishing** poznáte velmi snadno, od banky by vám takový e-mail nikdy nepřišel. Banka o takovýchto důležitých věcech prostřednictvím e-mailu nekomunikuje. Dále banka nikdy neuvádí aktivní odkazy v e-mailové komunikaci. V případě kliknutí na odkaz by se vám neobjevila v adresním řádku internetového prohlížeče adresa například České spořitelny (www.csas.cz, www.servis24.cz). V tomto případě jde tedy o typický případ spamu. Útočníci e-mailové adresy náhodně generují nebo je nakupují na černém trhu. Můžete tedy obdržet e-mail i od banky, u které nejste klientem. Pokud vám takový e-mail přijde, rozhodně na něj neodpovídejte, neklikejte na odkaz a okamžitě se obraťte na banku s tím, že vám tento e-mail došel a že se zcela jistě jedná o phishing. **Telefonní phishing** funguje na stejném principu jako klasický phishing přes e-mailovou korespondenci s tím rozdílem, že probíhá přes telefon. Tento podvod má prvenství v Kanadě. Jedná se o telefonáty údajného oddělení bezpečnosti banky, aby s klientem prodiskutovaly podezřelou transakci. Důvěru si útočník získá většinou tím, že zná číslo vaší karty. Majitel karty je seznámen s „podezřelou“ transakcí a jako řešení mu podvodník nabídne, že když mu sdělí CVV kód, pak tuto transakci stornuje. Klient mu kód poskytne a je ubezpečen, že se pracuje na vrácení problému do původního stavu.

Útočník tedy získal potřebné údaje a může bez obav obchodovat na internetu (www.csas.cz - strucne-o-phishingu).

7.9 Pharming

Pharming bývá do češtiny překládán **jako farmaření** a je to pokročilý způsob phishingu. Nejedná se o žádný e-mail nebo telefonát. Ke své činnosti využívá překladu jména serveru na odpovídající IP adresu, útočí tedy na DNS (Domain Name System). Pokud pak uživatel ve svém internetovém prohlížeči zadá adresu například www.lupa.cz, nedojde k překladu na odpovídající IP adresu 81.31.5.18, nýbrž nějakou jinou, podvrženou – a zde je kámen úrazu. Pokud by se totiž útočníkovi podařilo změnit DNS záznam výše zmiňované imaginární banky www.inetbanka.com, přesměruje se komunikace na jiný stroj, jiné stránky, které však na první pohled nelze rozpoznat od originálu. Nic netušící uživatel tedy zadá požadované přihlašovací údaje a bez větších překážek jimi obdaruje útočníka (www.lupa.cz/clanky/rhybareni-strida-pharming).

DNS servery překládají to, co napíšete do prohlížeče na skutečnou IP adresu, a pokud jsou tyto servery napadeny, pak klient dostává na svůj prohlížeč stránku s jinou IP adresou, protože DNS server dostal příkaz, aby jej zaměnil. Tomuto případu se říká globální pharming. Existuje i lokální pharming, který spočívá v napadení jednotlivého počítače pomocí hosts souboru, který obsahuje každý počítač s operačním systémem Windows. Tento soubor funguje obdobně jako DNS servery. Nejúčinnější ochrana je už mnohokrát zmiňovaný antivir, který byste měli pravidelně aktualizovat. V České republice byla naposledy tímto způsobem napadena Česká spořitelna a to v roce 2007. Do počítače se tak dostane škodlivý software, ten způsobí přepsání IP adresy a přesměrování klienta na falešné stránky internetbankingu. Tyto stránky se chovají jako stránky SERVISU 24 ČS s tím rozdílem, že po uživateli žádají při přihlášení bezpečnostní kód. Ten pro přihlášení standardně nutný není, je však potřeba jej znát pro některé operace s účtem, například pro změnu zadání telefonního čísla pro odeslání autorizační SMS zprávy.

Česká spořitelna doporučuje všem uživatelům, aby při přihlášení na www.servis24.cz zkontrolovali, že jsou skutečně na stránkách této služby. Ověřit pravost stránek je možné snadno: na pravých stránkách je na spodní liště **ikona zámku.** Při rozkliknutí se objeví informace o certifikaci: stránky mají certifikát vydaný pro Českou spořitelnu pro stránky www.servis24.cz renomovanou společností VeriSign. Pokud se klient přihlásil a má o pravosti stránek pochyby, ČS doporučuje ihned kontaktovat linku 844 11 11 44 a účet zablokovat. Asi 50 klientů zatím ČS hlásilo, že se s falešnými stránkami setkalo, ale nikdo z nich nebyl poškozen. Banka přesto zavedla preventivní opatření: změna telefonního čísla pro zasílání autorizační SMS je platná až po 24 hodinách (www.mesec.cz - cs-odvraci-napadeni-sveho-internetbankingu-phishingem-a-pharmingem/).

7.10 Krádež identity, krádež karty a převzetí účtu

Podvodné metody jakou jsou phishing, telefonní phishing nebo pharming, jsou podvody na klienty, kteří jsou velmi důvěřiví. Existují ale i podvody, které jsou připraveny na banky. Útočník se vydává za klienta, aby mohl od banky získat k účtu oběti novou platební kartu. Pokud má banka špatný nebo méně vyvinutý bezpečnostní systém, může se stát, že kartu opravdu útočníkovi zašle. Ale dnes je toto už jen velmi málo pravděpodobné, jelikož dneska banky vydávají karty ve většině případů po osobním navštívení pobočky.

Všemi již výše zmíněnými způsoby podvodů se dá **zcizit identita**. Dalšími způsoby jsou vybírání popelnic podvodníky, kde jsou obrovská množství papírů z bankomatu s číslem účtu a někdy se zde dají nalézt i papírky s PINem. Půjčení karty kamarádovi, nedbalost klienta či jeho nadměrná důvěřivost lidem.

Krádež platební karty je dnes zcela běžná, nejen že ji nosíme všude sebou v peněžence, ale někteří z nás u ní mají rovnou napsaný i PIN. Tím je naše identita, i účet denně ohrožen. Zloděj vám odcizí peněženku, nalezne v ní platební kartu, vy jako oloupená osoba, pokud to tedy hned zjistíte, zablokujete svou kartu. Ovšem i zloději vynalezli v tomto případě efektivní řešení. Zloději totiž žijí v nejistotě, kdo

je chytne za ruku, až budou vybírat peníze z účtu někoho cizího. Přišli proto se scénářem **„hodného samaritána“**. Pachatel tedy zavolá oběti pár okamžiků po krádeži s tím, že nalezl jeho peněženku, ze které zmizela jen hotovost, ale platební karta a doklady tam jsou a že mu ji doručí. Majitel karty, je rád, že se jeho karta našla a zcela zapomene zablokovat kartu a umožní tak pachateli bez obav vybrat peníze u účtu. Dále si pachatel může opsat údaje uvedené na kartě a i po vrácení ji dále zneužívat. Dnes jsou karty standardně chráněny PINem, proto by jej klient nikdy neměl nechávat u karty, nikdy by neměl věřit telefonujícímu pachateli, a vždy kartu zablokovat a nechat si vystavit novou. Pro omezení škody způsobené krádeží identity je důležité, aby si zákazníci pravidelně kontrolovali výpisy a jakoukoliv podezřelou transakci okamžitě hlásili bance. V průměru trvá 467 dní, než oběť přijde na to, že byla okradena. (www.echomagazin.com).

8 Vlastní práce

Vlastní část této práce řeší pomocí dotazníkové metody, jak často a na které operace dotazovaní využívají svou platební kartu. Zda jsou ochotni připlatit si větší částku či mít více číselný PIN kód pro zajištění úplně bezpečnosti platební karty z hlediska zajištění finančních prostředků.

Před sestavením dotazníku byla sestavena čtyři tvrzení, která výsledky dotazníku vyvrátila nebo potvrdila. Jimi jsou:

1. Respondenti, kteří utratí nejčastěji do 1000Kč, nevyužívají službu pojištění proti zneužití karty.
2. Každý, kdo vlastní platební kartu by chtěl, aby mu banka vyčíslovala, kolik měsíčně zaplatí za bezpečnost.
3. Nejvíce respondentů by bylo ochotno zaplatit za bezpečnost 25 – 44Kč měsíčně.
4. Nejvíce respondentů považuje za nejrizikovější způsob používání platební karty platbu přes internet.

8.1 Popis zkoumaného souboru

Dotazník byl rozeslán 121 respondentům. Některé dotazníky byly vyřazeny z důvodu neúplnosti nebo v případě, že dotazovaný odpověděl, že nevlastní platební kartu. Takovéto dotazníky byly 3. Celkový počet použitých dotazníků k vyhodnocení bylo 118. Respondenty se stali lidé různých věkových kategorií, pohlaví i dosaženého vzdělání. Dotazník naleznete v příloze číslo 3.

Dotazník je při vyhodnocování rozdělen na dvě části. První část tvoří obecné otázky – pohlaví, věk, dosažené vzdělání. Druhá část pak všechny ostatní otázky. Ke každé otázce byl vytvořen sloupcový graf, jenž ukazuje, kolik respondentů si vybralo danou odpověď. U otázky číslo 6 a 16 měli respondenti možnost odpovědět více odpověďmi a proto je zde větší množství odpovědí než bylo vyplněných

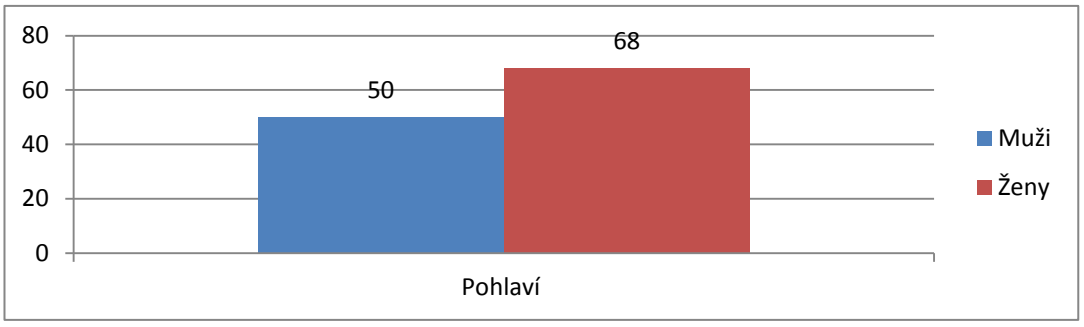
dotazníků. Současně s tímto je druhá část rozdělena na další 3 podčásti z pohledu toho, čím se zabývá, každá část má vytvořen svůj závěr.

8.2 Vyhodnocení dotazníků

8.2.1 První část – základní údaje

První část se věnuje vyhodnocení demografických dotazníkových otázek, jimiž jsou pohlaví, věk a vzdělání.

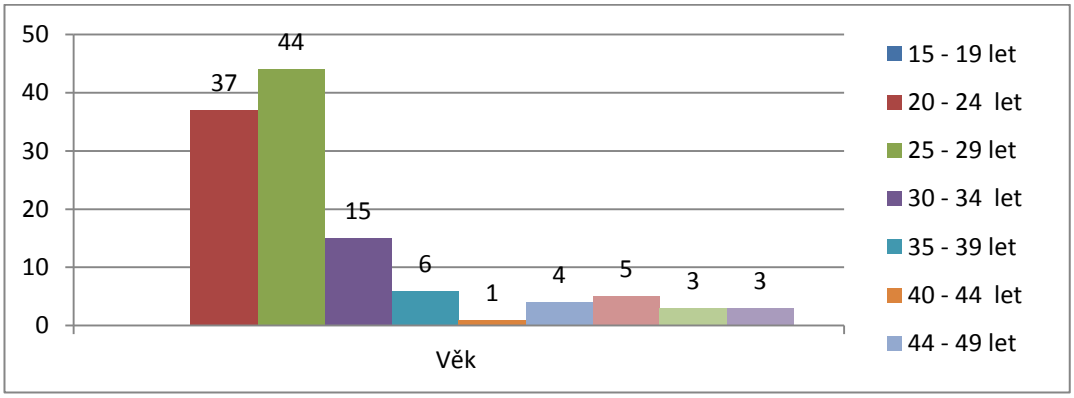
Graf číslo 2: Rozdělení respondentů dle pohlaví (v osobách).



Zdroj: vlastní zpracování

Respondenti byli s ohledem na pohlaví nevyváženi, ze 118 dotazovaných bylo 50 mužů a 68 žen.

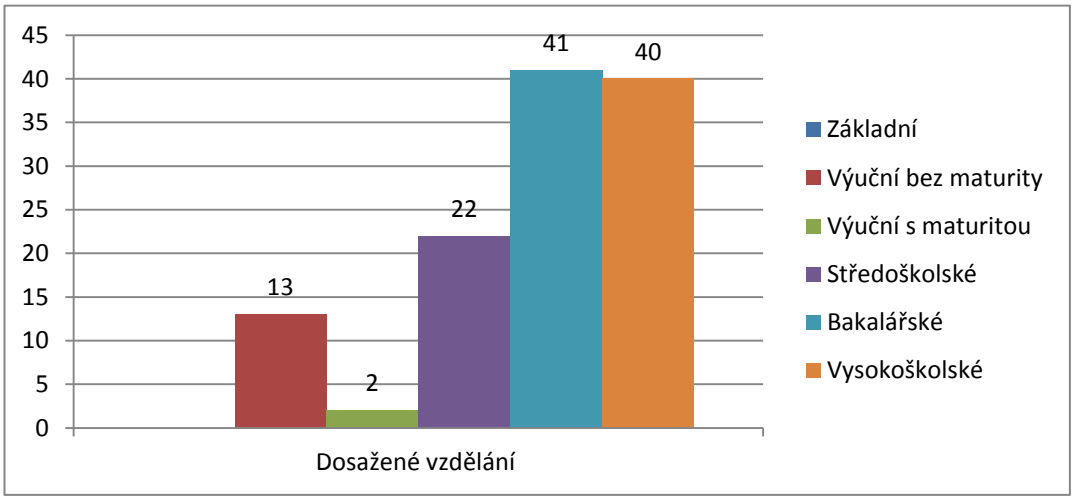
Graf číslo 3: Rozdělení respondentů dle věku (v osobách).



Zdroj: vlastní zpracování

Nejpočetnější skupinou jsou lidé ve věku 25 – 29 let, jež tvoří 37,29 %. Druhou nejpočetnější skupinou, jež se podílela na výzkumu je ve věkovém rozpětí 20 – 24 let. Věková kategorie 35 – 39 let se podílí na výzkumu jen z 5% a lidí nad 60 let je z 2,5%. Naopak věková kategorie 15 – 19 let se zde nevyskytuje.

Graf číslo 4: Rozdělení respondentů dle dosaženého vzdělání (v osobách).



Zdroj: vlastní zpracování

Nejvíce respondentů dosáhlo bakalářského vzdělání, tedy prvního stupně vysoké školy. Tato skupina se podílí 34,75% na tomto výzkumu. Další největší skupinou je skupina vysokoškoláků, jež vystudovali i druhý stupeň VŠ s 33,9%. Téměř o polovinu méně středoškolsky vystudovaných lidí, oproti lidem s titulem bakalář, vyplnilo dotazník. Naopak respondenti s pouze základním vzděláním se zde nevyskytují.

Z těchto otázek vyplývá, že nejvíce respondentů, jež odpovědělo na dotazník, vlastní titul Bc., mají tedy bakalářské vzdělání. Jsou to lidé v rozmezí 25 – 29 let. A největší zastoupení zde mají ženy.

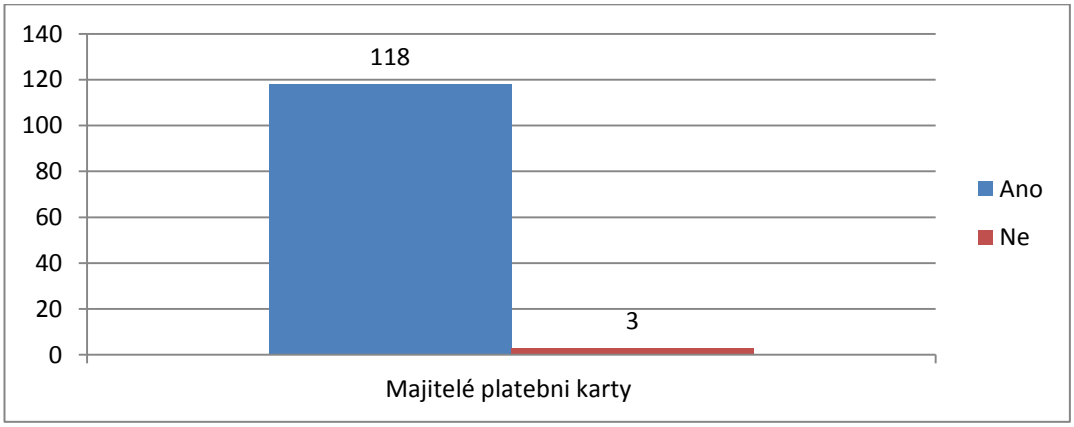
8.2.2 Druhá část – Ekonomické aspekty bezpečnosti platebních karet

Druhá část je rozdělena na další tři podčásti, podle toho čemu se věnují. **První podčást**, otázky 1 – 6, je obecná. **Druhá podčást** obsahuje otázky 7 – 12, jež se věnují použití platební karty a jak často ji respondent používá na danou operaci. **Třetí částí** jsou otázky 13 - 16, které se zabývají vyčíslením, kolik korun měsíčně utratí respondenti za bezpečnosti platební karty a ochotou mít více místný PIN kód.

8.2.2.1 Obecné otázky

1. Vlastníte platební kartu?

Graf číslo 5: Majitele platební karty (v osobách).

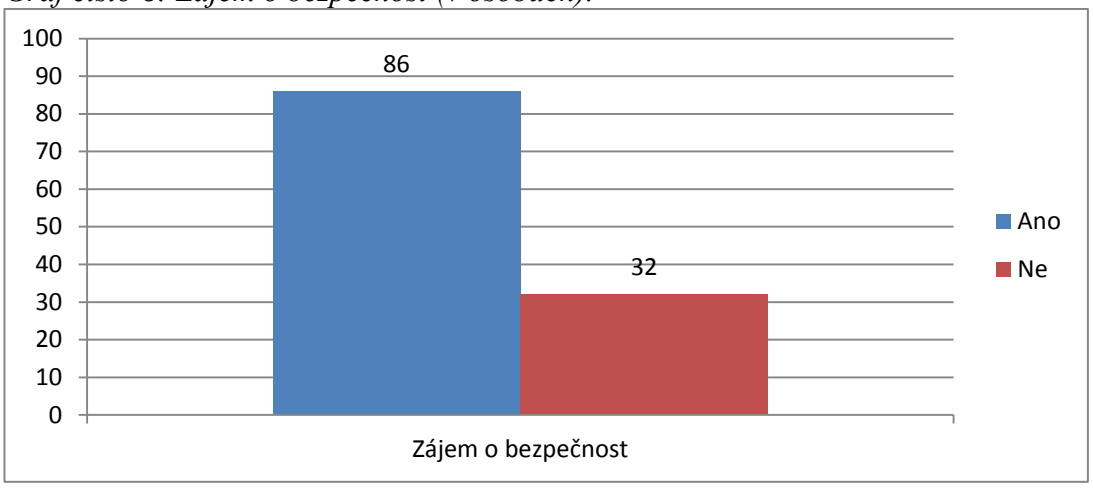


Zdroj: vlastní zpracování

Na otázku – Vlastníte platební kartu? Odpovědělo kladně 118 dotazovaných lidí, naopak 3 lidé odpověděli záporně. Tito lidé byly vyjmuti z konečného zpracování dotazníku.

2. Zajímáte se o bezpečnost své platební karty?

Graf číslo 6: Zájem o bezpečnost (v osobách).

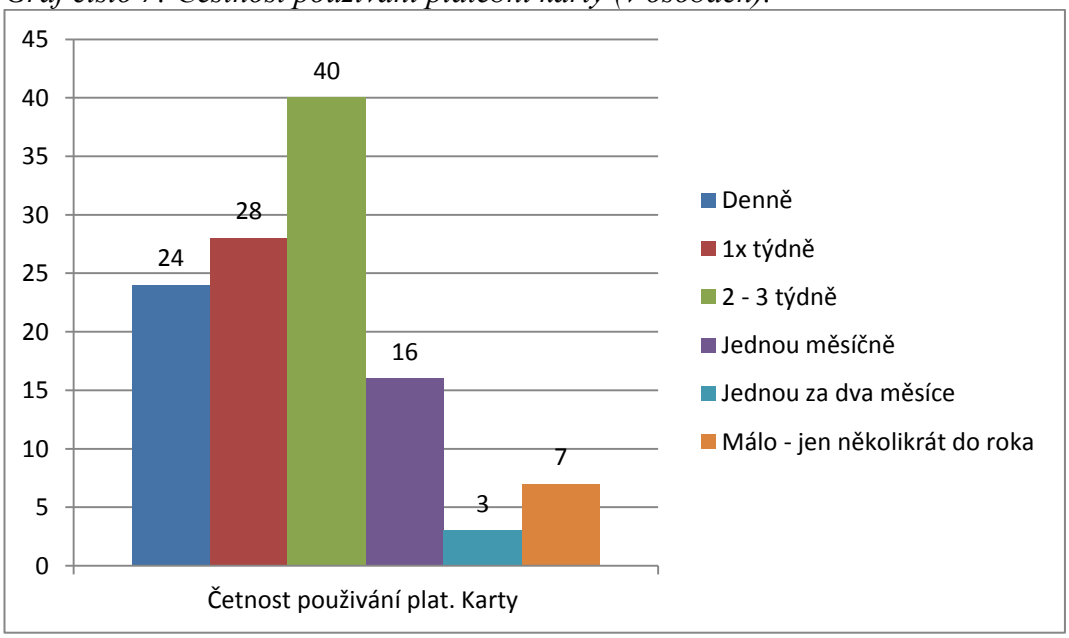


Zdroj: vlastní zpracování

O bezpečnost své platební karty se zajímá 86 lidí (72,88 %). 32 lidí (27,12%) se o ní naopak vůbec nezajímá.

3. Jak často využíváte platební kartu?

Graf číslo 7: Četnost používání platební karty (v osobách).

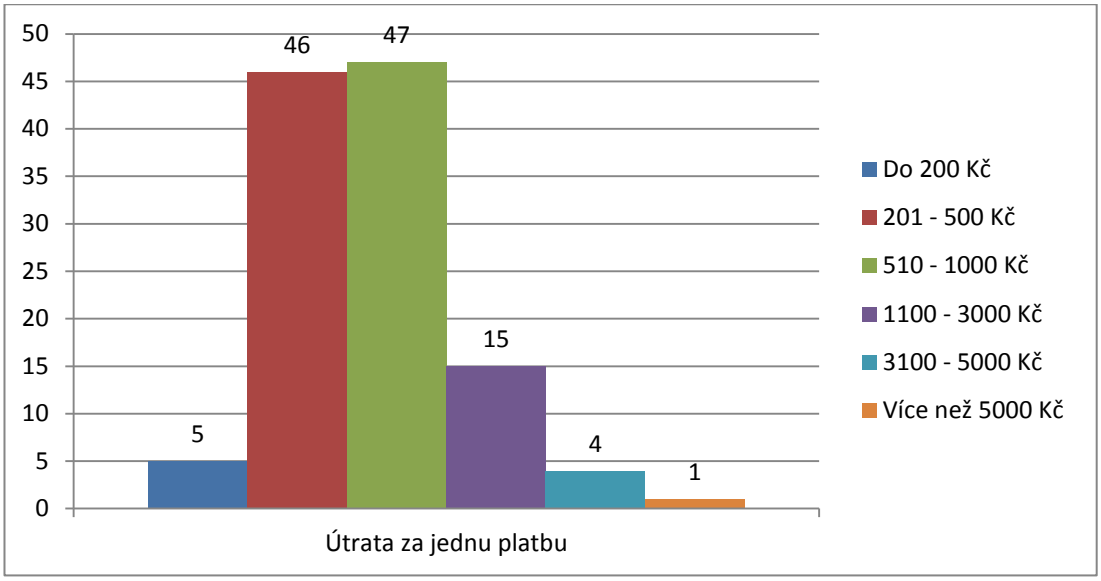


Zdroj: vlastní zpracování

Z grafu je vidět, že lidé využívají své platební karty velmi často. Nejvíce respondentů využívá svou platební kartu 2 – 3 týdně, a to celých 33,9%. 1x týdně svou kartu využívá 23, 73% a denně ji využívá 20,34%. Naopak jen několikrát do roka svou kartu využívá jen 5,9%.

4. Při platbě kartou nejčastěji utratíte (za jednu platbu)?

Graf číslo 8: Útrata za jednu platbu (v osobách).

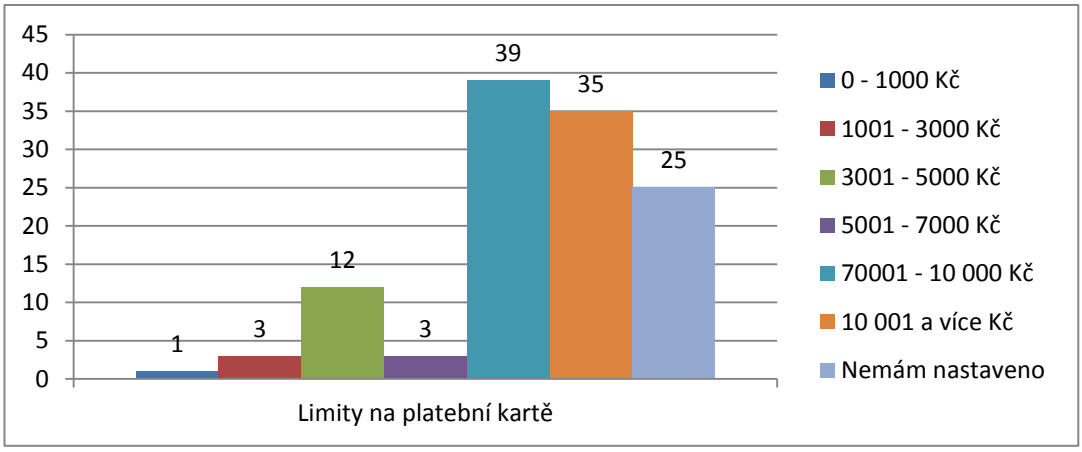


Zdroj: vlastní zpracování

Při otázce, při platbě kartou nejčastěji utratíte (za jednu platbu)?, se jen od jednoho respondenta dostala na první místo částka v rozmezí 510 – 1000Kč, na druhém místě se umístila částka od 201 – 500Kč. Částka 510 – 1000 Kč se na výzkumu podílí z 39,9% a částka 201 – 500 Kč z 39%. Více než 5000Kč za jednu platbu platí 0,8% dotazovaných osob.

5. Jakou denní výši limitu máte nastavenou?

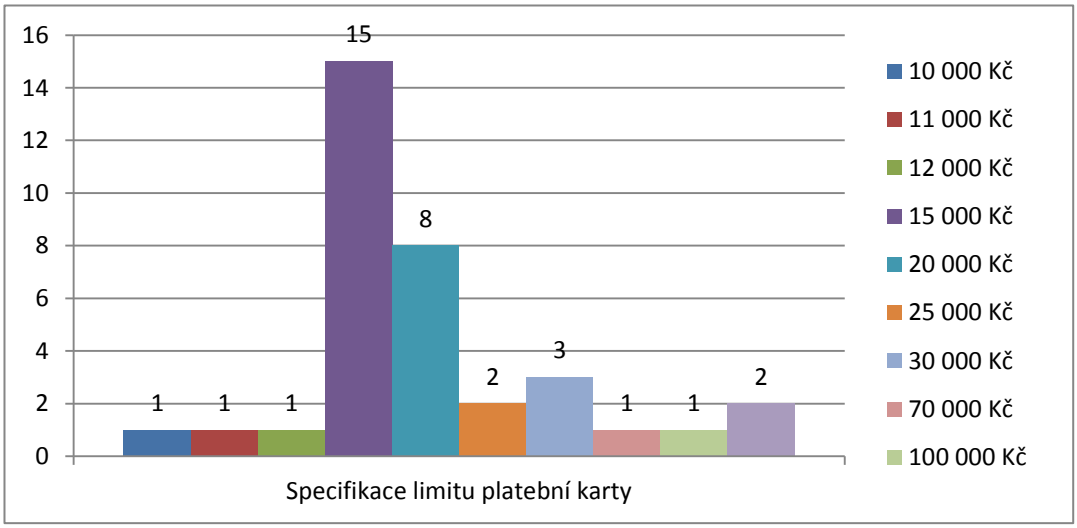
Graf číslo 9: Limity na platební kartě (v osobách).



Zdroj: vlastní zpracování

33% respondentů má nastaven svůj limit v rozpětí 7 001 – 10 000Kč. 29,66% pak v rozpětí 10 001 a více. V případě této možnosti měli dále specifikovat svůj limit. 21, 19% pak nemá limit nastaven vůbec. Odpovědi byly nastaveny do částky 10 001 a více Kč. V případě, že částka byla vyšší, měli respondenti specifikovat sumu. Specifikace naleznete v grafu číslo 10.

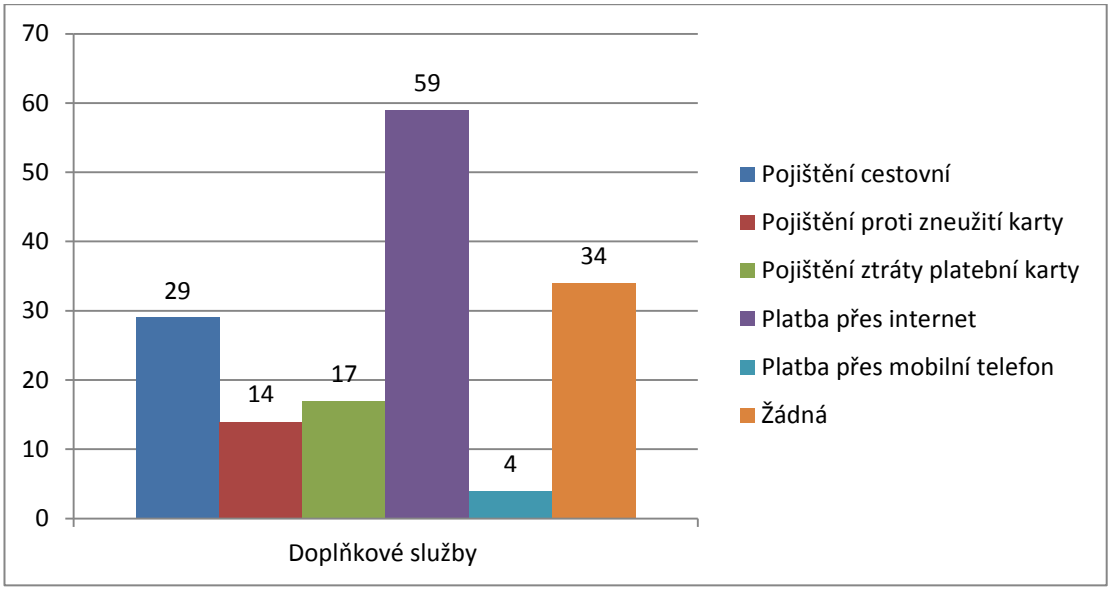
Graf číslo 10: Specifikace limitu platební karty (v osobách).



Zdroj: vlastní zpracování

6. Jaký druh doplňkových služeb využíváte k platební kartě? (možno i více odpovědí)

Graf číslo 11: Doplňkové služby (v osobách).



Zdroj: vlastní zpracování

Celých 50% využívá doplňkovou službu platba přes internet. Na druhé pozici se umístila odpověď žádné – tedy žádnou z uvedených doplňkových služeb nevyužívá 28,8% respondentů. Dále 24,6% dotázaných využívá cestovní pojištění. Jen 3,4% využívají platbu přes mobilní telefon.

Závěr první podčásti

Výsledkem této části dotazníku je, že ze 118 respondentů se jich 86 zajímá o bezpečnost platební karty. Nejčastěji je tito lidé používají 2 – 3 týdně, ale najdou se i tací, kteří svou kartu použijí jen několikrát do roka. Zcela běžně dotázaní svou kartu používají k nákupům od 200 – 1000Kč. To znamená i k běžným nákupům potravin, kin, obědů atd. Méně častěji k nákupům vyšší částky. 33% respondentů má nastaven svůj limit v rozpětí 7 001 – 10 000Kč. 29,66% pak v rozpětí 10 001 a více. Za zmínku stojí odpovědi na denní limit, jako jsou 70 000Kč, 100 000Kč

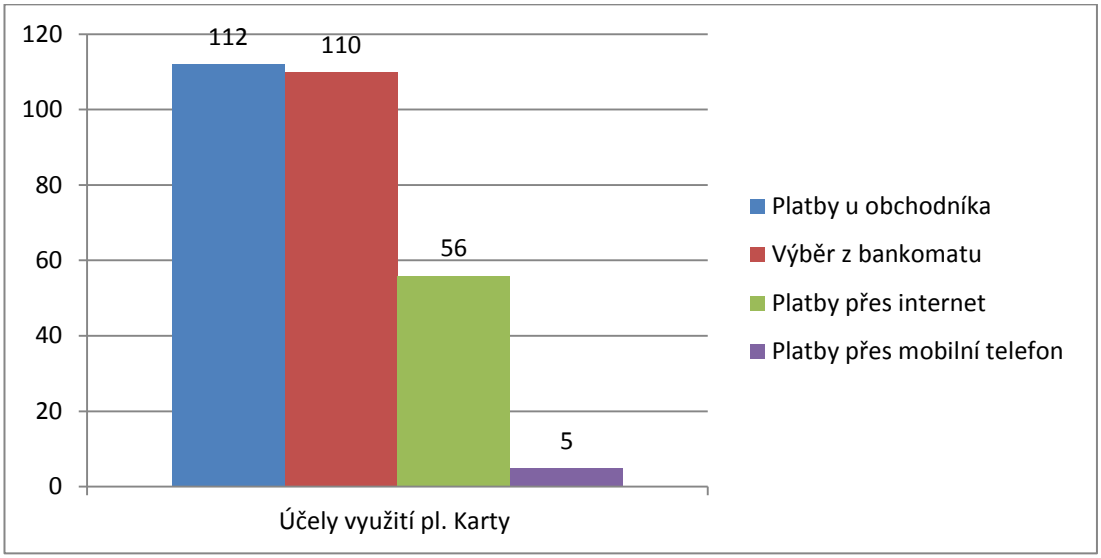
a 1 000 000Kč. Celých 50% využívá doplňkovou službu platba přes internet. Dále 24,6% dotázaných využívá cestovní pojištění.

Tvrzení, že respondenti, kteří utratí nejčastěji do 1000 Kč, nevyužívají službu pojištění proti zneužití karty, se vztahuje k otázkám číslo 4 a 6 a tento výzkum ho vyvrací. V dotazníku uvedlo 98 lidí, že za jednu platbu nejčastěji zaplatí částku do 1000 Kč. Z těchto dotázaných službu pojištění proti zneužití využívá 20 respondentů, kteří tvoří 16, 95 %.

8.2.2.2 Použití platební karty

7. Pro jaké účely kartu využíváte? (možno i více odpovědí)

Graf číslo 12: Účely využití platební karty (v osobách).

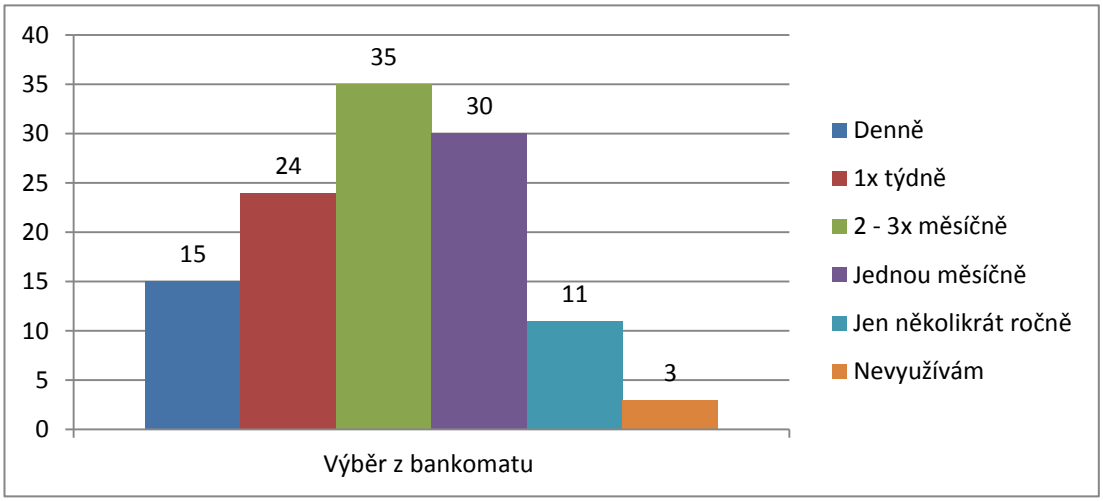


Zdroj: vlastní zpracování

Na tuto otázku mohli respondenti vybrat více odpovědí. Proto se nerovnají odpovědi s počtem zpracovávaných dotazníků, jichž je 118. Celkový počet odpovědí na tuto otázku je 283. Z nichž tedy 39,6% respondentů využívá platební kartu k platbám u obchodníka. 38,9% k výběrům z bankomatu, 19,8% k platbám přes internet a pouhých 1,8% k platbám přes mobilní telefon.

8. Jak často využíváte platební kartu k výběru z bankomatu?

Graf číslo 13: Výběr z bankomatu (v osobách).

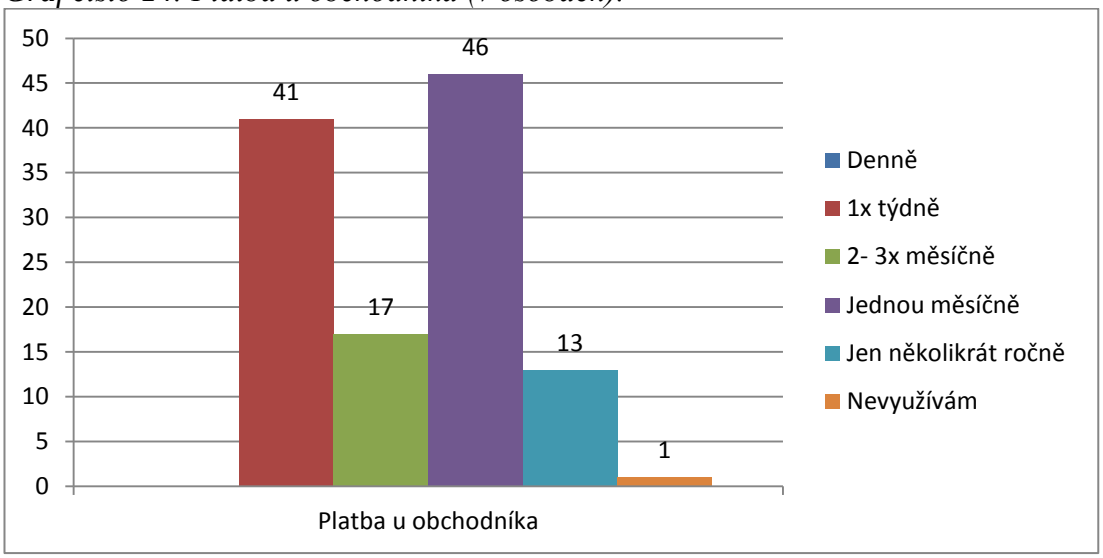


Zdroj: vlastní zpracování

Nejčastěji dotazovaní lidé vybírají peníze z bankomatu v rozpětí 2 – 3 měsíčně. Tuto kategorii tvoří 29,6% respondentů. Jednou měsíčně si vybírá z bankomatu 25,4%. Naopak jen 3 osoby, tedy 2,4% si z bankomatu vůbec nevybírá.

9. Jak často využíváte platební kartu k platbě u obchodníka?

Graf číslo 14: Platba u obchodníka (v osobách).

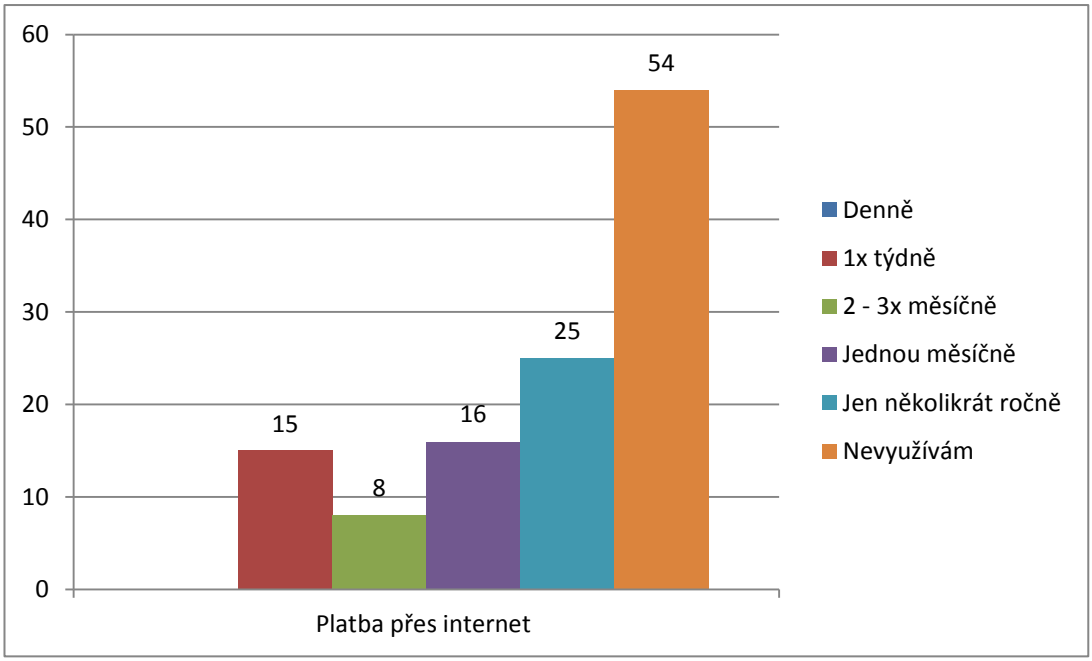


Zdroj: vlastní zpracování

Platební kartu k platbám u obchodníka využívá 39% jednou měsíčně. Jednou týdně ji pak využívá 34,7% dotázaných. Nikdo z dotazovaných nepoužívá k platbám u obchodníka denně. A tuto možnost nevyužívá 0,85% respondentů.

10. Jak často využíváte platební kartu k platbě na internetu?

Graf číslo 15: Platba přes internet (v osobách).

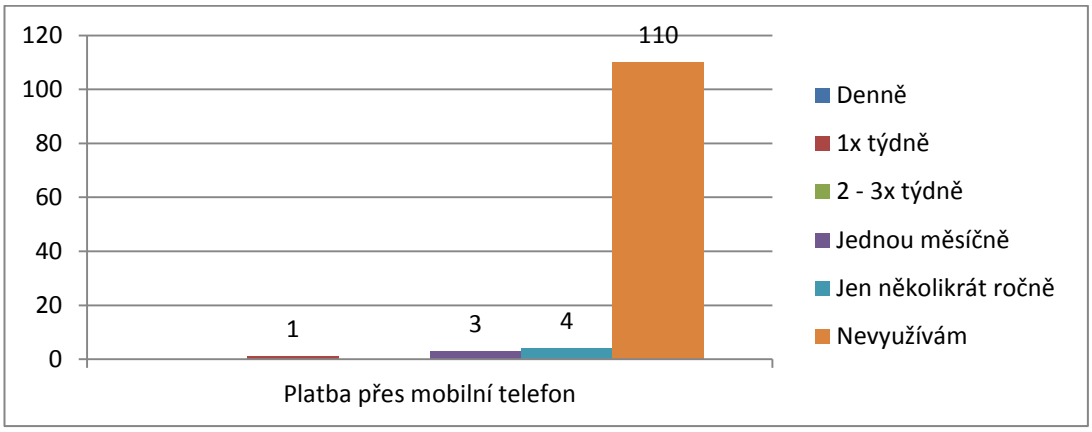


Zdroj: vlastní zpracování

Platbu přes internet nevyužívá 45,8%. 21,1 % pak tuto možnost využívá jen několikrát ročně. Jednou měsíčně takto platí 13,6% a jednou týdně jen 12,7%. Denně tyto platby nevyužívá nikdo z dotázaných.

11. Jak často využíváte platební kartu k platbě přes mobilní telefon?

Graf číslo 16: Platba přes mobilní telefon (v osobách).

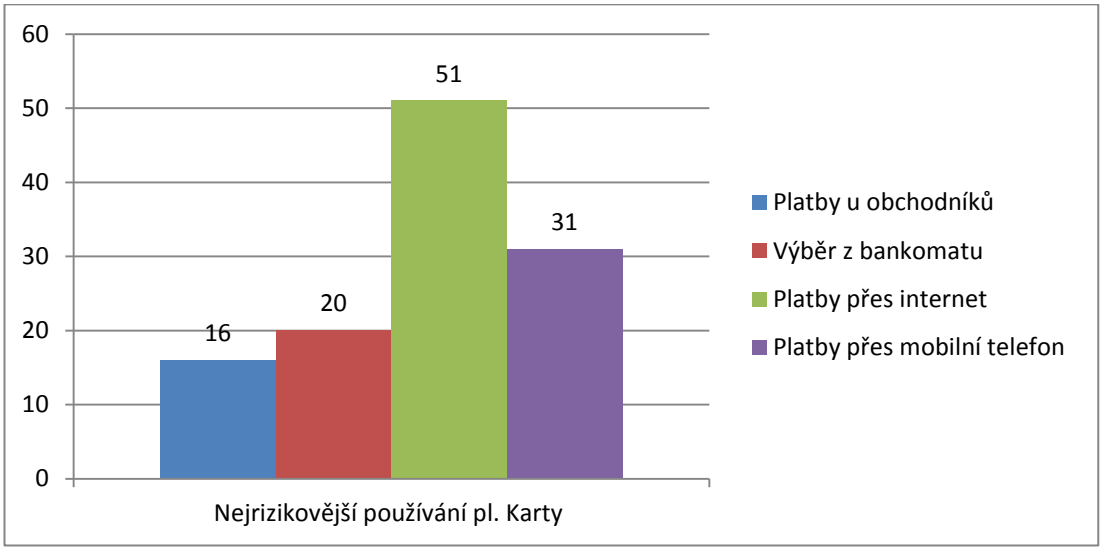


Zdroj: vlastní zpracování

Možnost platby přes mobilní telefon ze 118 dotázaných respondentů nevyužívá 110, což je 93,2%. Jen několikrát ročně ji pak využívá 3,4% jednou měsíčně 2,5% a jednou týdně pouhých 0,84%.

12. Který případ je podle vás nejrizikovější při používání platební karty?

Graf číslo 17: Nejrizikovější používání platební karty (v osobách).



Zdroj: vlastní zpracování

43,22% se jako nejrizikovější způsob používání platební karty jeví platby přes internet. Na druhém místě jsou platby přes mobilní telefon, který označilo 26,27%. Jako nejméně riziková byla označena platba u obchodníka s 13,56%.

Závěr druhé podčásti

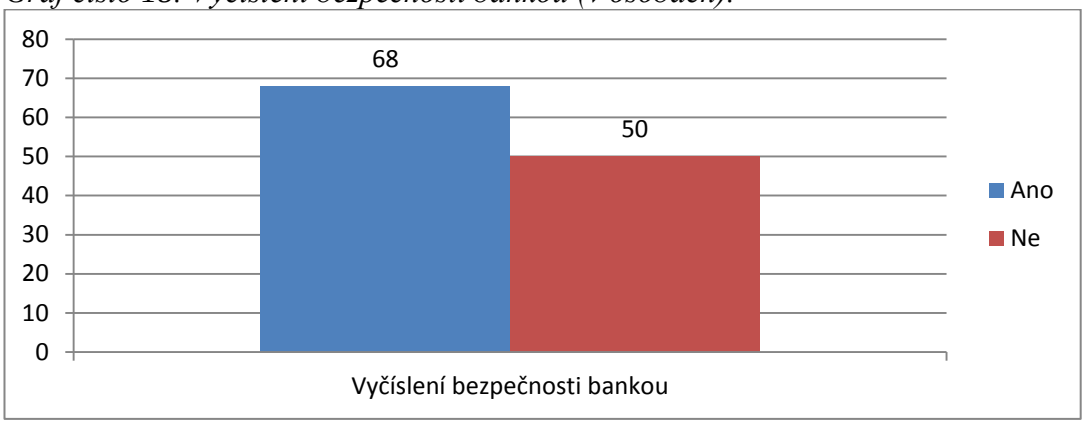
V této části se autorka zabývala použitím platební karty. Výsledkem výzkumu je, že nejvíce respondentů využívá platební kartu k platbám u obchodníka a k výběru hotovosti z bankomatu. Při otázkách na četnost použití platební karty k těmto účelům, byly zjištěny tyto výsledky. K výběru z bankomatu dotazovaní využívají svou kartu 2 – 3 do měsíce. K platbě u obchodníka je to jednou za měsíc. Nejvíce respondentů na platbu na internetu odpovědělo, že ji nevyužívají. A tutéž odpověď odpověděli respondenti i u plateb přes mobilní telefon. Tato odpověď byla očekávaná, jelikož platby přes mobilní telefon jsou u nás možné teprve od loňského roku.

Tvrzení, že nejvíce respondentů považuje za nejrizikovější používání platební karty, bylo tímto výzkumem potvrzeno. 59% dotázaných opravdu považuje platbu přes internet, jako nejrizikovější. Na druhém místě se umístila platba přes mobilní telefon a dále výběr z bankomatu.

8.2.2.3 PIN kód, vyčíslení bezpečnosti

13. Měl/a byste zájem o to, aby vám banka každý měsíc vyčíslila, kolik korun měsíčně utratíte za bezpečnost vaší platební karty?

Graf číslo 18: Vyčíslení bezpečnosti bankou (v osobách).

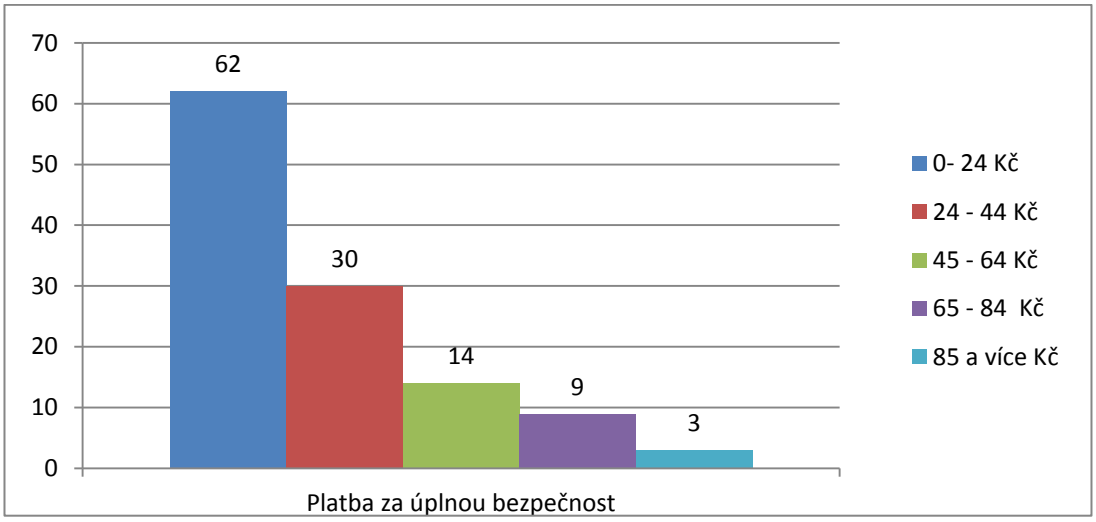


Zdroj: vlastní zpracování

Na otázku, zda by dotazovaní měli zájem o to, aby jim banka vyčíslila, kolik korun měsíčně utratí za bezpečnost platební karty, řeklo 57,63% ano a 42,37% ne.

14. Kolik byste byl/a ochoten/na měsíčně zaplatit, v případě, že by byla zajištěna úplná bezpečnost vaší platební karty z hlediska ztráty peněz?

Graf číslo 19: Platba za úplnou bezpečnost (v osobách).

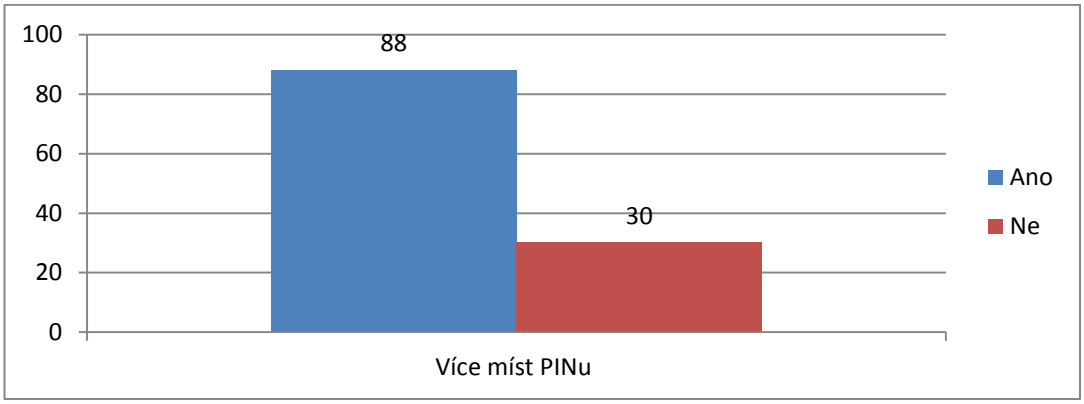


Zdroj: vlastní zpracování

V případě, že by majitelé platební karty měli zajištěnou úplnou bezpečnost platební karty z hlediska ztráty peněz, pak by 52,54% respondentů bylo ochotno zaplatit do 24Kč za měsíc. 25,42% do 44 Kč a 11,86% do 64 Kč. Pouhé 2,54% dotázaných by byli ochotni zaplatit více než 85 Kč. U této odpovědi měli dotazovaní specifikovat částku. Jako jednoznačnou částku všichni tři respondenti uvedli 100 Kč za měsíc.

15. Byl/a byste ochoten/na mít PIN delší než 4 místný pro vyšší bezpečnost?

Graf číslo 20: Více míst PINu (v osobách).

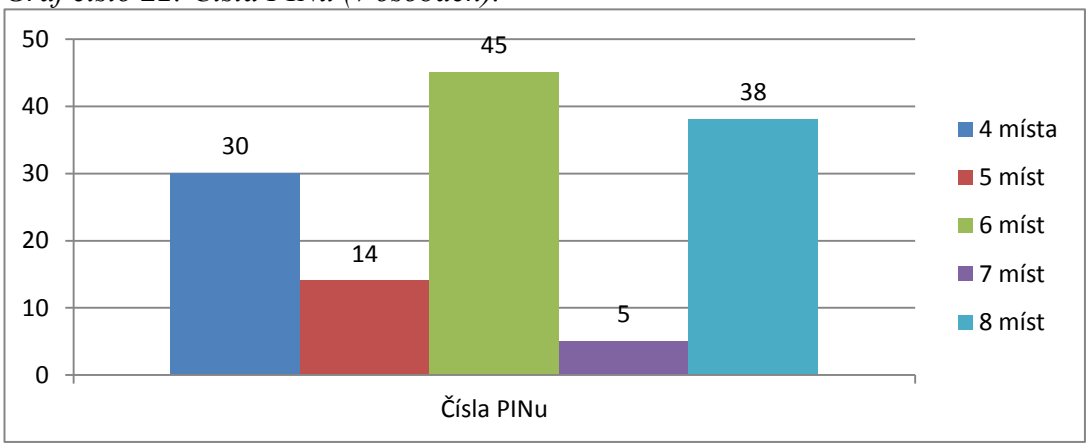


Zdroj: vlastní zpracování

Ochotno mít více místný PIN kód pro vyšší bezpečnost své platební karty je 74,58% respondentů. 25,42% dotazovaných to odmítá.

16. V případě, že ano. Kolik čísel PIN kódu, byste si byl/a schopen/na a ochoten/na zapamatovat? (možno i více odpovědí)

Graf číslo 21: Čísla PINu (v osobách).



Zdroj: vlastní zpracování

U této otázky mohli respondenti opět vybrat více odpovědí. Počet odpovědí je tedy 132 a dotazníků použitých ke zpracování 118. 4 místa PIN kódu jsou ochotni mít tedy jen ti, kteří odmítli pamatovat si více čísel pro vyšší bezpečnost své platební karty, jichž je tedy 22,72%. 34,1% lidí je ochotných si zapamatovat 6 čísel. 28,8% by bylo ochotno zapamatovat i 8 míst PIN kódu. Jednoznačně tedy vedou sudá čísla oproti lichým.

Závěr třetí podčásti:

V této třetí pod části se jednalo o otázky dotazující se především na PIN kód platební karty a na vyčíslení sumy bankou danou na bezpečnost platební karty. Tvrzení, které říká, že každý kdo vlastní platební kartu by chtěl, aby mu banka vyčíslovala, kolik korun zaplatí měsíčně za bezpečnost, taktéž není pravdivé. Pouze 57,63% dotazovaných má zájem o tuto službu.

Nejvíce respondentů uvedlo, že by byli ochotni zaplatit do 24Kč v případě úplného zajištění bezpečnost vaší platební karty z hlediska ztráty peněz. Tento výsledek má za následek vyvrácení prvního tvrzení pro tuto podčást výzkumu. Jímž

je nejvíce respondentů by bylo ochotno zaplatit za bezpečnost 25 – 44Kč měsíčně. Pouhé 2,54% dotázaných by byli ochotni zaplatit více než 85 Kč.

V případě zajištění bezpečnosti finančních prostředků pomocí více místného PIN kódu se setkalo s kladnou odezvou. 74,58% respondentů je ochotno mít více místný PIN kód. 34,1% lidí je ochotných si zapamatovat 6 čísel. 28,8% by bylo ochotno zapamatovat i 8 míst PIN kódu. Jednoznačně tedy vedou sudá čísla oproti lichým.

9 Závěr

Během necelých sto let své existence zcela ovládly platební karty svět bezhotovostního placení. Velmi rychle se rozšířily mezi všechny vrstvy a mnoho lidí ve vyspělých státech světa vyměnilo svou peněženku za platební kartu. Často hotovost už vůbec nenosí, popřípadě si ji vyberou z bankomatu pouze v ojedinělých situacích. V posledních třiceti letech pozorujeme přesun plateb od luxusních hotelů a restaurací k platbám běžné potřeby.

Moderní technologie nám dnes dovoluje zaplatit hodinkami, prstenem či mobilním telefonem. Ovšem platba bezkontaktní platební kartou v nejbližších letech zažije v České republice revoluci. Již v prvních dvou měsících, kdy banky ČSOB a Era začaly vydávat bezkontaktní platební karty, vydaly bezmála 25 000 kusů. Nejčastější průměrná částka placená touto kartou je 180Kč. Tato částka je placena bez zadání PIN kódu, může proto karta být snadněji zneužita. Z tohoto důvodu je potřeba zajistit především bezpečnost tohoto bankovního produktu.

Dnes je bezpečnost spojena s neustálým bojem o ochranu před důmyslnými zloději. Znepříjemnit a znesnadnit jim možnost během vteřiny vzít finanční prostředky. Zajištění karty pomocí nových a nových technologických zabezpečení, popřípadě přidáním nových ochranných prvků na platební kartu či osvětou klientů vlastnící platební kartu. Zabezpečení tedy závisí na karetní asociaci, která kartu vydává, na bance, která ji poskytuje klientovi a v neposlední řadě na klientovi, který ji využívá v běžném životě.

Pro omezení škody způsobené krádeží identity je důležité, aby si zákazníci pravidelně kontrolovali výpisy a jakoukoliv podezřelou transakci okamžitě hlásili bance. V průměru trvá 467 dní, než oběť přijde na to, že byla okradena. Po tak dlouhé době, už je téměř nemožné vystopovat pachatele.

Výsledky výzkumu provedeného v této práci jsou jak předvídatelné, tak překvapující. Tvrzení stanovená ve vlastní části byla potvrzena i vyvrácena. Tvrzení

číslo jedna, Respondenti, kteří utratí nejčastěji do 1000Kč, nevyužívají službu pojištění proti zneužití karty, bylo vyvráceno. Každý, kdo vlastní platební kartu by chtěl, aby mu banka vyčíslovala, kolik měsíčně zaplatí za bezpečnost, bylo také vyvráceno. Nejvíce respondentů by bylo ochotno zaplatit za bezpečnost 25 – 44Kč měsíčně, bylo vyvráceno. Nejvíce respondentů považuje za nejrizikovější způsob používání platební karty platbu přes internet, bylo potvrzeno.

Předvídatelná a z jiných výzkumů už zjištěná fakta jsou, že za nejvíce obávanou transakci je platba přes internet. Nyní je ale tato platba zabezpečena a existuje už minimální riziko ztráty peněz. Banky poskytují virtuální platební karty, jež jsou určeny jen na platbu přes internet. Ovšem paradoxem k této odpovědi je, že 50 % dotázaných využívá doplňkovou službu platby přes bankomat. Dotazník ale nezjišťuje, zda k těmto platbám používají již zmíněnou virtuální kartu, či svou fyzickou platební kartu.

Nejvíce respondentů využívá platební kartu k platbě u obchodníka a k výběru hotovosti v bankomatu. Zajímavější odpovědi a tudíž méně předvídatelné jsou odpovědi na četnost používání platební karty k danému účelu. Výběr z bankomatu nevyužívá 2,4 % dotázaných. Kdežto 12,71 % dotázaných vybírá z bankomatu denně. Z toho plyne, že hotovost využívá stále velké množství lidí, ale někteří ji nevyužívají už vůbec. Platbu u obchodníka nevyužívá pouhé 0,85 %. Pravidelně dotázaní zaplatí platební kartou do 1000 Kč za jednu platbu. V porovnání s bankovními poplatky je platba u obchodníka výhodnější než výběr z bankomatu. Jelikož výběr z vlastního bankomatu u České spořitelny u „osobního účtu ČS“ stojí klienta 6Kč, v případě bankomatu jiné banky je to 40 Kč. Platba u obchodníka je zdarma.

Za zmínku stojí i nastavení denních limitů na platební kartě. Bezpochyby nepředvídatelnou částkou je limit 1 000 000 Kč, který mají nastaveni dva respondenti. Zajímavostí je, že oba jsou muži ve věku 20 – 24 let s bakalářským vzděláním.

Samotná otázka: Jaký druh doplňkových služeb využíváte k platební kartě? Má zajímavé odpovědi, 28,8 % dotázaných odpovědělo, že nepoužívá žádnou doplňkovou službu, přestože v nabídce odpovědí byly možnosti – cestovní pojištění, pojištění proti zneužití karty, pojištění ztráty platební karty. Ani výše uvedení dva respondenti s nastaveným limitem 1 000 000 Kč tyto služby nevyužívají.

Přes 70 % respondentů je ochotno mít vícemístný PIN kód pro zajištění bezpečnosti svých finančních prostředků. Respondenti preferují sudá čísla míst PINu – 6 míst, 8 míst. Velmi překvapivou odpověď má otázka číslo 13 (Měl/a byste zájem o to, aby vám banka každý měsíc vyčíslila, kolik korun měsíčně utratíte za bezpečnost vaší platební karty?). Kde s pouhým rozdílem 15,26 % byla nejčastěji vybrána odpověď, že by dotazující měli zájem o vyčíslení, kolik korun měsíčně utratí za bezpečnosti platební karty. V případě, že by měli klienti možnost zaplatit si úplné zajištění bezpečnosti platební karty z hlediska ztráty peněz, nejčastěji by si zaplatiti částku do 24 Kč. Nejvyšší částku, kterou by byli ochotni zaplatit je 100 Kč. Tak odpovědělo 2,54 % dotázaných.

Z těchto výsledků lze usuzovat, že zajištění bezpečnosti platební karty z pohledu klienta je malé. Na jednu stranu jsou ochotni zajistit bezpečnost platební karty prostřednictvím PIN kódu a zaplacení si úplné bezpečnosti. Ale na druhou stranu si kartu nechtějí zabezpečit pomocí pojištění platební karty, či v případě, dalších poplatků za zajištění finančních prostředků prostřednictvím doplňkový služeb na svém účtu, ke kterému mají platební kartu. Na tyto výsledky má bezpochybně vliv věk a vzdělání respondentů. Jsou to mladí lidé v rozmezí 20 – 29 let s vysokoškolským vzděláním (bakalářské i magisterské studium). Pouhých 5,6 % jsou lidi vyučení s maturitou nebo bez maturity. V tomto věku tito lidé studují a okolo 25 let nalézají svá první zaměstnání na plný úvazek, z čehož vyplývá, že nemají takové příjmy, aby mysleli na zabezpečení svých finančních prostředků. I tito lidé by si měli zabezpečovat své platební karty. Většina studentů si chodí přivydělávat či pracují na částečný úvazek, a pokud ne, tak jim rodiče posílají kapesné na účet. Studenti tedy mohou přestavovat nejlehčí oběti krádeží.

Doporučením pro tuto i jakoukoliv věkovou skupinu je neustále se informovat o nových zabezpečeních své katry. Zvážit zda by nebyl dobrý krok provést nějaké doplňkové služby – pojištění proti zneužití platební karty, pojištění ztráty platební karty. O podvodech, kterých je neustále větší množství, a jsou důmyslnější. Sledovat své bankovní výpisy a i malou chybějící či podezřelou částku konzultovat s bankou. To hlavně z důvodu toho, že v případě včasného zjištění zcizení finančních prostředků, lze přijmout různá opatření a je zde možnost nalézt zloděje v blízké době.

10 Seznam použitých zdrojů

[1]: JUŘÍK, Pavel. *Platební karty, velká encyklopedie 1870-2006*. vyd. 1 Praha: Grada Publishing, 2006. 296 s. ISBN 8024713810.

[2]: ELY PLISCHKE, Simona. *Penize.cz* [online]. 27. 04. 2007 [cit. 2012-02-23]. Jak došly platební karty do českých zemí aneb historie karet plná zajímavostí. Dostupné z WWW:http://www.penize.cz/platebni-karty/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti

[3]: ELY PLISCHKE, Simona. Čedok, Tuzex a český karetní boom. In: *Peníze.cz* [online]. 23. 12. 2003 [cit. 2012-08-29]. Dostupné z:http://www.penize.cz/platebni-karty/16363-cedok-tuzex-a-cesky-karetni-boom

[4]: *www.*Csa.cz [online]. 1998-2010 [cit. 2012-02-23]. OK Plus - věrnostní programy. Dostupné z WWW: <http://www.csa.cz/cs/portal/loyalty_programs/ffp_okplus/ffp_ homepage.htm>.

[5]: JUŘÍK, Pavel. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet.* 1. vyd. Praha: Grada, 2003. 312 s. ISBN 8024706857.

[6]: CHARLES, Arthur. How ATM fraud nearly brought down British banking. *The register* [online]. 25. srpna 2005 [cit. 2012-03-07]. Dostupné z: http://www. Theregister.co.uk/2005/ 10/21/phantoms_and_rogues/

[7]: MÁČE, Jaroslav. Platební styk – klasický a elektronický. vyd. Praha - Grada Publishing, 2006. 220 s. ISBN 8024717255.

[8]: JUŘÍK, Pavel. *Svět platebních a identifikačních karet*. 2. přeprac. vyd.Praha: Grada Publishing, spol. s r. o., 2001, 210 s. ISBN 8024701952

[9]: DVOŘÁK, Petr. *Bankovnictví pro bankéře a klienty*. 3. přeprac. a rozšíř.

vyd. Praha: Linde Praha, a.s., 2005, s. 370 – 385. ISBN 807201515X.

[10]: Česká spořitelna. *Jak vyzrát na skimming.* [online]. 2010 [cit. 2012-04-02]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/jak-vyzrat-na-skimmingd00014291

[11]: *Česká spořitelna*: *Co je phishing?* [online]. 2010 [cit. 2012-04-02]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/strucne-o-phishingu-d00014563

[12]: SALMON, Michal. *Podvody s kartami: skimmovací zařízení koupíte snadno i s návodem*: *Libanonská smyčka*[online]. 30. 4. 2010 [cit. 2012-04-03]. Dostupné z: http://www.mesec.cz/clanky/nejcastejsi-podvody-platebnimi-kartami/

[13]: SAMUEL, Henry. *The telegraph*: *Chip and pin scam 'has netted millions from British shoppers'* [online]. 10 Oct 2008 [cit. 2012-04-03]. Dostupné z: http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html

[14]: *Bezpečný internet*: *spywere* [online]. 1999 [cit. 2012-04-04]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/spyware.aspx

[15]: BITTO, Ondřej. *Lupa.cz*: *Rhybaření střídá pharming* [online]. 31. 3. 2005 [cit. 2012-04-04]. Dostupné z: http://www.lupa.cz/clanky/rhybareni-strida-pharming/

[16]: CVV, CVC kód (CVV1, CVC1, CVV2, CVC2 kód). *Totalmoney.sk* [online]. 2009-2012 [cit. 2012-08-29]. Dostupné z: http://totalmoney.etrend.sk/slovnik/C /cvvcvc-kod-cvv1-cvc1-cvv2-cvc2-kod/

[17]: Desatero bezpečnosti. *Www.mojebanka.cz* [online]. 2012 [cit. 2012-08-31]. Dostupné z: http://www.mojebanka.cz/cs/desatero-bezpecnosti.shtmlrady_uk/ kriminalita/kradeze_s_identitou_mizi_i_penize

[18]: *Echomagazin.com*: *KRÁDEŽE: S identitou mizí i peníze* [online]. 2008-2010 [cit. 2012-04-04]. Dostupné z: http://www.echomagazin.com/clanky/prakticke_

[19]: *Financnivzdelavani.cz*: *Bezpečné zacházení s platební kartou* [online]. 2007 [cit. 2012-04-04]. Dostupné z: http://www.financnivzdelavani.cz/webmagazine/page .asp?idk=321

[20]: FRIŠAUFOVÁ, Alice. Vydání Vzorových obchodních podmínek pro vydávání a užívání elektronických platebních prostředků. *Cnb.cz* [online]. 29. 11. 2002 [cit.

2012-09-09]. Dostupné z: http://www.cnb.cz/cs/verejnost/pro_media/tiskove_zpravy_cnb/2002/tz2002_vzorove_podminky.html

[21]: GAJDUŠKOVÁ, Klára. *Mesec.cz*: *ČS odvrací napadení svého internetbankingu phishingem a pharmingem*[online]. 16. 3. 2007 [cit. 2012-04-04]. Dostupné z: http://www.mesec.cz/tiskove-zpravy/cs-odvraci-napadeni-sveho-internet bankingu-phishingem-a-pharmingem/

[22]: How ATM fraud nearly brought down British banking. *Http:// www.theregister.co.uk* [online]. 21st October 2005 [cit. 2012-08-31]. Dostupné z: http://www.theregister.co.uk/2005/10/21/phantoms_and_rogues/

[23]: HEARY, Jamey. Newest Attack on your Credit Card: Pin Pad Shims. *Networkworld* [online]. 07/11/10 [cit. 2012-09-28]. Dostupné z: http://www. networkworld.com/community/node/63544

[24]: JUŘÍK, Pavel. Historie platebních karet: podvody. *Idnes.cz/Finance* [online]. 22. října 2005 [cit. 2012-08-31]. Dostupné z: http://finance.idnes.cz/historie-platebnich-karet-podvody-d56-/bank.aspx?c=A051012_155215_fi_osobni_zal

[25]: Jaké (ne)výhody má platební karta. *Idnes.cz/Finance* [online]. 13. prosince 2006 [cit. 2012-08-29]. Dostupné z: http://finance.idnes.cz/jake-ne-vyhody-ma-platebni-karta-dnq-/bank.aspx?c=A061212_110349_fi_osobni_vra

[26]: INFORMACE PRO DRŽITELE PLATEBNÍCH KARET. *Kb.cz* [online]. 2013 [cit. 2013-02-24]. Dostupné z: http://www.kb.cz/file/cs/produktove-listy/kreditni-karta-visa-electron-p.products.16.2/kb-informace-pro-drzitele-platebnich-karet.Pdf ?e3d1c377b54cfba01b867f80159c9039

[27]: PUŽMANOVÁ, Rita. Biometrické systémy v praxi. *Systemonline.cz* [online]. 2001-2012 [cit. 2012-08-29]. Dostupné z: http://www.systemonline.cz/clanky /biometricke-systemy-v-praxi.htm

[28]: Používejte platební karty, ale dodržujte naše desatero zásad bezpečné manipulace. *Bankovnipoplatky.com* [online]. 04.06.2012 [cit. 2012-08-31]. Dostupné

z: http://www.bankovnipoplatky.com/dovolena-2012-pouzivejte-platebni-karty-ale-dodrzujte-nase-desatero-zasad-bezpecne-manipulace-14449.html

[29]: Podvod bez přítomnosti karty. *Bankovnikarty.cz* [online]. 2012 [cit. 2012-09-28]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Podvod_bez_přítomnosti_karty

[30]: Podvody padělanou kartou. *Bankovnikarty.cz* [online]. 2012 [cit. 2012-09-28]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html #Podvody_padělanou_kartou

[31]: Podvody kartou ztracenou v poště. *Bankovnikarty.cz* [online]. 2012 [cit. 2012-09-28]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Podvody_kartou_ztracenou_v_poště

[32]: Podvody se zcizenou identitou. *Bankovnikarty.cz* [online]. 2012 [cit. 2012-09-28]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html #Podvody_se_zcizenou_identitou

[33]: SADOVSKÝ, DALIBOR a JAROSLAV SUCHÁNEK. Platební karty a možnosti jejich zneužití. *Kriminalistika - Čtvrtletník pro kriminalistickou teorii a praxi* [online]. 2004, 1/2004 [cit. 2012-08-29]. Dostupné z: http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html

[34]: Trestní zákon. In: *Zákon č. 140/1961 Sb., trestní zákon*. 2012. Dostupné z: http://business.center.cz/business/pravo/zakony/trestni_zakon/

[35]: Virtuální karty. *Visa.cz* [online]. 2013 [cit. 2013-02-24]. Dostupné z: http://www.visa.cz/cz/osobni_karty/vyberte_si_vasi_visa_kartu/predplacene_visa_karty/virtualni_karty.aspx

[36]: Zákon o platebním styku. In: *Zákon č. 284/2009 Sb., o platebním styku*. 2012. Dostupné z: http://business.center.cz/business/pravo/zakony/platebni-styk/

[37]: A PIN-Entry Method Resilient Against Shoulder Surfing. *Http://volkerroth.com*[online]. 2013 [cit. 2013-02-24]. Dostupné z: http://nvolkerroth.com/download/Roth2004c.pdf

[38]: DVOŘÁK, Jakub. Nejlepší antispywarové nástroje zavřou špiónům dveře před nosem. *Technet.cz* [online]. 18. ledna 2011 [cit. 2013-02-24]. Dostupné z: http://technet.idnes.cz/nejlepsi-antispywarove-nastroje-zavrou-spionum-dvere-pred-nosem-1c2-/software.aspx?c=A101221_124009_software_dvr

11 Seznam vyobrazení

11.1.1 Grafy

11.1.2 Obrázky

12 Slovníček pojmů

- ✓ Adware - je označení pro produkty znepříjemňující práci nějakou reklamní aplikací.
- ✓ Akceptace – potvrzení platby kartou
- ✓ American Expres – společnost vydávající karty
- ✓ Antispamovací software - je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). Je účinnější než antivirový software
- ✓ Antivirový software - je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware).
- ✓ Autorizace plateb – ověření si zákazníka při platbě
- ✓ BIN – 4 místný identifikační znak banky
- ✓ CVC kód – 3 místné číslo u podpisového proužku
- ✓ Data mining – hledání průniku transakcí klientů, kteří nahlásili podezřelé transakce svých karet způsobené zřejmě kopií platební karty.
- ✓ Dinners club – společnost vydávající platební karty
- ✓ Dislokace – porucha, rozložení
- ✓ DNS server - je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace
- ✓ Elektronická karta – je karta s magnetickým proužkem
- ✓ Embosovaná karta – karta, na které jsou jméno majitele a číslo karty vytlačeny nad povrch
- ✓ Firewal - je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení.
- ✓ Hologram – trojrozměrný obraz na kartě, bezpečnostní prvek na kartě

- ✓ IP adresa – je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol).
- ✓ Karetní asociace – Společnost, krerá vydává platení karty
- ✓ Logo – nápis s názvem a značkou firmy
- ✓ PIN – 4 místné číslo pro identifikaci karty
- ✓ Platební terminál – přenosné nebo pevné zařízení pro platbu kartou u obchodníka
- ✓ Phishing – podpovdný e-mail nebo telefonát, podpod při používání platební karty
- ✓ Shimming – podvod pomocí bankomatu
- ✓ Shoulder surfing – „koukání přes rameno“ podvod při používání platební karty
- ✓ Skimovací zařízení – zařízení pro kopírování platebních karet prostřednictvím bankomatů
- ✓ Sniffovací programy – program, který zaznamenává každé kliknutí na klávesnici.
- ✓ Spywere - je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele.
- ✓ Scoring – výběr vhodného klienta bankou
- ✓ VISA – společnost vydávající karty
- ✓ Western Union – společnost v USA

13 Seznam příloh

Příloha číslo 1 - Biometrické systémy založené na fyziologických charakteristikách

Příloha číslo 2 - Jak poznat napadený bankomat při skimmingu.

Příloha číslo 3 - Dotazník – Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta

Příloha číslo 1 - Biometrické systémy založené na fyziologických charakteristikách

typ biometrie	rozhraní s uživatelem	výhody	nevýhody	přesnost	objem dat (B)
Biometrické systémy založené na fyziologických charakteristikách					
otisk prstu	uživatel položí prst na plochu snímače snímače optické, termální nebo odporové	stálá a přesná (otisky se liší u jednotlivců a v průběhu života se nemění) a zavedená technologie – dnes přijatelná cena a velikost snímačů (používaných už i na mobilních telefonech); značný rozsah použitelnosti (i malá přenosná zařízení)	uživatelům může vadit fyzický kontakt a logické spojení odebírání otisků s kriminalitou; náchylné na útoky	1:1000 (někdy se uvádí až 1:1 miliónu)	240 – 1000 B
geometrie ruky	uživatel položí ruku na plochu optického snímače	středně přesná technologie (přesnost roste s trojrozměrnými snímanými obrazy); celkem přijatelné pro uživatele	uživatelům může vadit fyzický kontakt se snímačem	1:1000 (pouze v dostatečně malé databázi)	9-20 B
sítnice	uživatel se zaměří na specifikovaný bod optického	vysoká přesnost (struktura žilek se liší u jednotlivců a v průběhu života se	nepříjemné pocity pro uživatele (fyzický kontakt) – potřeba snímat brýle, přiblížit se	1:1.000.000+	35 B

	snímače a infračervený paprsek snímá strukturu sítnice; vzdálenost musí být kolem 2 cm	nemění, pouze vlivem nemoci nebo úrazu) – vhodné pro identifikaci	ke snímači hodně blízko a nechat si svítit do oka		
duhovka	uživatel se dívá do kamery ve vzdálenosti až 1-2 m	vysoká přesnost; uživatelsky přátelské, žádný fyzický kontakt, brýle nevadí	vysoká cena systému – vhodné pro vysoce bezpečné zóny	1:6.000.000	256-500 B
obličejové znaky	uživatel se dívá do kamery	přijatelné pro uživatele – žádný fyzický kontakt (někdy i pasivní monitorování bez vědomí uživatele); nízká cena	nepříliš přesná metoda, ale vylepšuje se např. termografií; přepokládaná využitelnost např. v bankomatech		1 KB (100 B po kompresi)
DNA	řada možností získání DNA (krev, sliny, sperma)	vysoká přesnost	nepoužívá se komerčně; drahé; možnost obelhání systému cizím vzorkem		
tvar ucha	uživatel nastaví snímači ucho k jeho obrazovému sejmutí	není potřeba fyzický kontakt	zatím se zkoumá		
rozprostření žil na zápěstí	uživatel přiloží zápěstí na snímač	fyzický kontakt	přijatelnost obdobná jako u snímání otisků prstů		
Biometrické systémy založené na charakteristikách chování ***(společná vlastnost – malá přesnost)***					
charakteristiky hlasu	uživatel hovoří do mikrofonu	přijatelné pro uživatele; vhodné i pro vzdálenou autentizaci po telefonu; střední cena	méně přesné – vliv prostředí (hluky na pozadí) a vliv fyzického/psychického stavu uživatele (nemoc, stres, únava)	1:50	
podpisové charakteristiky (dynamika)	uživatel se podepíše speciálním	naprosto přijatelné pro uživatele – podpis jako takový	méně přesné – může mít vliv únava nebo stres, uživatelé se nemusí	1:50	

	perem na speciální podložku zařízení	je nejčastější verifikací uživatele	podepisovat stále stejně; při zranění ruky je tato metoda prakticky vyloučená; zatím málo rozšířené, ale s potenciálem u bezdrátových zařízení jako PDA		
charakteristiky psaní na klávesnici	uživatel píše vzorový text na klávesnici (měří se tlak a rychlost)	přijatelné pro uživatele; cenově dostupné, protože se maximálně využívá stávající hardware	méně přesné - může mít vliv únava nebo stres; při zranění ruky je tato metoda prakticky vyloučená; zatím málo rozšířené		

Zdroj: www.systemonline.cz

Příloha číslo 2 - Jak poznat napadený bankomat při skimmingu.

Zdroj: www.csas.cz

Příloha číslo 3 - Dotazník – Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta

Dobrý den,

jsem studentkou České zemědělské univerzity v Praze, obor Provoz a ekonomika. Tento dotazník je součástí mé diplomové práce na téma Ekonomické aspekty bezpečnosti platebních karet z pohledu klienta. Cílem práce vymezení ekonomických aspektů bezpečnosti platebních karet z pohledu klienta, proto vás prosím o vyplnění dotazníku a odevzdání autorce. V dotazníku vyberte vždy jednu odpověď. Tam, kde je napsáno, můžete zakroužkovat i více odpovědí.

Děkuji za vyplnění Bc. Naděžda Gasiorková

Vaše pohlaví

- žena
- muž

Váš věk

- 15 - 19 let
- 20 - 24 let
- 25 - 29 let
- 30 – 34 let
- 35 – 39 let
- 40 – 44 let
- 45 – 49 let
- 50 – 54 let
- 55 – 59 let
- 60 a více let

Vzdělání

- základní
- výuční bez maturity
- výuční s maturitou
- středoškolské
- bakalářské
- vysokoškolské

1. **Vlastníte platební kartu?**
   - ano
   - ne (dále dotazník už nevyplňujte a vraťte jen zpracovateli)

2. **Zajímáte se o bezpečnost své platební karty?**
    - ano
    - ne
    -
3. **Jak často využíváte platební kartu?**
    - denně
    - 1x týdně
    - 2 – 3x týdně
    - jednou měsíčně
    - jednou za dva měsíce
    - málo – jen několikrát ročně

4. **Při platbě kartou nejčastěji utratíte (za jednu platbu):**
    - Do 200Kč
    - 201 - 500 Kč
    - 510 – 1000Kč
    - 1100 – 3000Kč
    - 3100 – 5000 Kč
    - Více než 5000Kč – pokud více, specifikujte …….

5. **Jakou denní výši limitu máte nastavenou?**
    - 0 – 1000 Kč
    - 1 001 – 3 000 Kč
    - 3 001– 5 000 Kč
    - 5 001 – 7 000 Kč
    - 7 001 – 10 000 Kč
    - 10 001 a více Kč – pokud více, specifikujte …….
    - nemám nastaveno

6. **Jaký druh doplňkových služeb využíváte k platební kartě. (možno i více odpovědí)**
    - pojištění cestovní
    - pojištění proti zneužití karty
    - pojištění ztráty platební karty
    - platba přes internet
    - platba přes mobil
    - žádnou

7. **Pro jaké účely kartu využíváte? (možno i více odpovědí)**
    - platby u obchodníků

- výběr z bankomatu
- platby přes internet
- platby přes mobilní telefon

8. Jak často využíváte platební kartu k platbě u obchodníka?

- denně
- 1x týdně
- 2-3x měsíčně
- jednou měsíčně
- jen několikrát ročně
- nevyužívám

9. Jak často využíváte platební kartu k výběru z bankomatu?

- denně
- 1x týdně
- 2-3x měsíčně
- jednou měsíčně
- jen několikrát ročně
- nevyužívám

10. Jak často využíváte platební kartu k platbě na internetu?

- denně
- 1x týdně
- 2-3x měsíčně
- jednou měsíčně
- jen několikrát ročně
- nevyužívám

11. Jak často využíváte platební kartu k platbě přes mobilní telefon?

- denně
- 1x týdně
- 2-3x měsíčně
- jednou měsíčně
- jen několikrát ročně
- nevyužívám

12. Který případ je podle vás nejrizikovější při používání platební karty.

- platby u obchodníků
- výběr z bankomatu
- platby přes internet
- platby přes mobilní telefon

13. **Měl/a byste zájem o to, aby vám banka každý měsíc vyčíslila, kolik korun měsíčně utratíte za bezpečnost vaší platební karty?**
    - ano
    - ne

14. **Kolik byste byl/a ochoten/na měsíčně zaplatit, v případě, že by byla zajištěna úplná bezpečnost vaší platební karty z hlediska ztráty peněz?**
    - 0 - 24Kč
    - 25 - 44Kč
    - 45 - 64Kč
    - 65 - 84Kč
    - 85 a více korun – pokud více, specifikujte částku……..

15. **Byl/a byste ochoten/na mít PIN delší než 4 místný pro vyšší bezpečnost?**
    - ano
    - ne

16. **Kolik čísel PIN kódu, byste si byl/a schopen/na a ochoten/na zapamatovat? (možno i více odpovědí)**
    - 4 místa
    - 5 místný
    - 6 místný
    - 7 místný
    - 8 místný

Děkuji vám za trpělivost při vyplnění dotazníku a přeji pěkný den.