VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

BEZPEČNOST A RIZIKA PLATEBNÍCH KARET V ČR

Autor práce: Lukáš Kyttler

Studijní obor: Management a marketing služeb – specializace finanční služby

Forma studia: Kombinovaná

Vedoucí práce: Ing. Jiří Dušek, Ph.D.

Katedra: Katedra managementu a marketingu služeb

2017

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce Ing. Jiřímu Duškovi, Ph.D. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

KYTTLER, L. *Bezpečnost a rizika platebních karet v ČR : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, z. ú., 2017. 78 s. Vedoucí bakalářské práce : Ing. Jiří Dušek, Ph.D.

Klíčová slova: analýza rizik, platební karty, podvody s platebními kartami, úroveň bezpečnosti, zneužití platebních karet

Bakalářská práce se zabývá platebními kartami a to jejich zabezpečením a také riziky, která jsou spojená s jejich používáním. Hlavním cílem je zanalyzovat současná rizika, které vznikají při používání platebních karet. Následně jsou zhodnoceny bezpečnostní prvky platebních karet.

Bakalářská práce obsahuje dvě části. První část je teoretická a zabývá se analýzou platebních karet. Zde jsou analyzovány nejčastější typy útoků na platební karty a jejich slabé stránky. Dále jsou popsány bezpečnostní opatření a další způsoby ochrany platebních karet. Druhá část obsahuje dotazníkové šetření, které hodnotí, jak lidé vnímají rizika spojená s používáním platebních karet a zda se brání proti případným rizikům.

ABSTRACT

KYTTLER, L. *Security and Risks of Payment Cards in the Czech Republic : Bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2017. 78 p. Supervisor : Ing. Jiří Dušek, Ph.D.

Key words: misuse of payment card, payment cards, payment card fraud, risk analysis, security level

The bachelor thesis deals with the security and risks of the payment cards, which are associated with their use. The main purpose is to analyse the current risks which occurs while using the payment cards. In addition, the security elements of the payment cards are assessed.

The bachelor thesis consists of the two parts. The first theoretical part deals with the analyses of the payment cards. Firstly, the most common types of attacks on the payment cards and their weaknesses are described. Secondly, security features and other ways of protecting of the payment cards are discussed. The second part contains the research which evaluates how people perceive the risks associated with using the payment cards and whether they make certain precautions to eliminate the potential risks.

Obsah

ÚVOD

Kdo by to byl řekl, že jedna večeře povede ke vzniku platebních karet. Ten večer si Frank McNamara zapomněl peněženku a nastalo nepříjemné zjištění, že nemá jak zaplatit. Tato situace vedla k tomu, že se McNamara rozhodl v následujících dnech založit se svými přáteli Diners Club International. Tímto se tato organizace stala prvotním vydavatelem a provozovatelem platebních karet.

Tyto platební karty se dostaly také k nám do České republiky. Nastal tedy postupný vývoj, a když banky u nás v devadesátých letech dvacátého století začaly vydávat první platební karty, tak měly veliké finanční náklady a také byly bez předchozích zkušeností. I tak jsou dnes platební karty jedním z nejpopulárnějších bankovních produktů, mají velice široké spektrum použití. Dnes už platební karty neslouží pouze pro placení v kamenných obchodech, ale můžeme si s jejich pomocí koupit např. jízdenku, platit telefonem nebo také mohou sloužit ke zprostředkování online plateb na internetu. Tento platební nástroj o ploše 46 cm^2 prošel za posledních 25 let velikým vývojem a stal se velice využívanou metodou pro běžné placení, které je součástí našeho každodenního života.

Platební karty ovšem nezůstaly bez povšimnutí a s jejich rozvojem se rozvíjela také kriminalita s nimi spojená. Vydavatelé platebních karet na rizika do určité míry zareagovali. Ovšem nenastaly takové změny, že by byl narušen určitý komfort platby. Protože, pokud by zde bylo příliš bezpečnostních prvků, které vyžadují aktivitu uživatele, tak bychom raději zaplatili hotově, než kartou. To ovšem vydavatelé platebních karet nechtějí.

Platební karty byly, jsou a nejspíše i stále budou vystaveny různým hrozbám ať už ze strany samotného uživatele, nebo cizích osob. Proti takovým hrozbám se můžeme bránit, nebo přinejmenším minimalizovat jejich dopady. Kvůli tomu, že jsou platební karty napojeny na běžný účet, mohou zde vzniknout značné finanční ztráty. Proto by se neměla bezpečnost podceňovat a rizika se snažit snížit na nejnižší možnou míru.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Hlavním cílem bakalářské práce je zanalyzovat současná rizika a identifikovat typy útoků na platební karty. Vedlejším cílem je zhodnotit bezpečnostní prvky, pojištění a další způsoby ochrany platebních karet.

Bakalářská práce je rozdělena do 5 kapitol. V teoretické části jsou analyzovány rizika a bezpečnost platebních karet. První kapitola se zabývá stanovením cíle a metodickými postupy. Druhá kapitola se zaměřuje na vývoj platebních karet v České republice a jejich druhy, náležitosti a používané technologie. Třetí kapitola analyzuje rizika a různé typy útoku na platební karty, se kterými se uživatelé mohou setkat. Čtvrtá kapitola se orientuje na úroveň zabezpečení platebních karet a další způsoby, jak například můžeme snížit rizika při jejich používání.

Poslední pátá kapitola vyhodnocuje dotazníkové šetření, které je zaměřené na držitele platebních karet. Šlo o zjištění, jak držitelé platebních karet vnímají rizika, která jsou s nimi spojená a jestli vědí, jak se proti nim mohou chránit nebo jim předcházet. Dotazník obsahoval 20 otázek a byl umístěn od 17. února 2017 do 3. března 2017 na webu https://www.vyplnto.cz/databaze-dotazniku/bezpecnost-a-rizika-platebni/. Zde byl dotazník vyplněn celkem 165 respondenty. Mohlo být tedy osloveno široké spektrum osob, ze všech možných regionů České republiky. Dotazník byl šířen pouze v elektronické podobě.

Bakalářská práce je zpracována na základě literárních a elektronických zdrojů. Literární zdroje byly čerpány především od JUŘÍKA[1] a SCHLOSSBERGERA[2]. Co se týká zdrojů elektronických, tak zde byly stěžejní informace a data byla získána z webových stránek www.ecb.europa.eu a www.bankovnikarty.cz. V bakalářské práci byly použity tyto metody: popisná a analyticko-statistická.

[1] JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. 248 s.
[2] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. 373 s.

2 PLATEBNÍ KARTY V ČESKÉ REPUBLICE

2.1 Historie platebních karet

V Československu se vývoj bankovních produktů zpomalil, ale ve vyspělých zemích došlo v šedesátých až osmdesátých letech dvacátého století k revolučnímu rozvoji. Téměř všichni občané dostávali výplaty na běžné účty v bankách a spořitelnách a k placení používali šeky a později i kreditní a debetní karty. Zvýšit komfort klientům umožnil koncem sedmdesátých let vynález bankomatu a postupně se tak začal snižovat počet pokladen na pobočkách peněžních ústavů. Od základu se změnil model obsluhy zákazníků, protože bankomaty byly levnější než pokladníci a mohly pracovat nepřetržitě 24 hodin denně.[3]

Od roku 1969 jsou v Československu přijímány mezinárodní platební karty. Mezi prvními byly karty Diners Club a American Express. Dále byly do roku 1990 akceptovány platební karty American Express, Diners Club, Eurocard/MasterCard, JCB, VISA a krátce i Air Plus a enRoute. Cestovní kancelář Čedok zajišťovala uzavírání smluv s obchodními místy, školení jejich personálu, autorizaci a zúčtování transakcí. V roce 1988 vydala Živnostenská banka první platební karty (i když s omezeným použitím). Jednalo se o tzv. dispoziční karty k tuzexovým účtům, které sloužily k výběru odběrních poukazů PZO Tuzex v pobočkách ČSOB, SBČS a k bezhotovostnímu placení v prodejnách Tuzex. V roce 1991 navázala Živnostenská banka na tento projekt vydáním karet VISA Classic a o rok později VISA Business (v roce 1995 i VISA Gold). Společnost American Express otevřela v Praze v roce 1990 svojí kancelář a převzala od Čedoku zajištění příjmu svých karet v obchodní síti. Čedok ukončil v červnu 1992 svoji zprostředkovatelskou činnost pro ostatní systémy – převzaly ji členské banky VISA a Eurocard/MasterCard.[4]

K širšímu využívání platebních karet bylo nutné překonat určitou nedůvěru veřejnosti, která měla k této nové technologii pochybnosti a v neposlední řadě vybudovat potřebnou infrastrukturu, která by umožňovala využívat rozšíření platebních karet jako plnohodnotného platebního nástroje. Ze začátku se platební karty využívaly spíše jako nástroj hotovostního platebního styku k výběrům z bankomatu. S příchodem mezinárodních obchodních řetězců do České republiky se začaly platební karty využívat ve větší míře a to díky tomu, že ve svých obchodních jednotkách zavedly platbu kartou, jako samozřejmou součást nabízených služeb. Okolo roku 2000 došlo k masivnímu

[3] JUŘÍK, P. *Historie bank a spořitelen v Čechách a na Moravě.* Praha : Libri, 2011. s. 163.
[4] JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. s. 203.

rozvoji využívání platebních terminálů. Objem bezhotovostních transakcí na platebních terminálech začal po roce 2010 přesahovat v hodnotovém vyjádření objem výběrů z bankomatů. Podíl platebních operací prostřednictvím platebních karet na celkovém počtu platebních operací se na konci první dekády tohoto století přibližuje průměru zemí eurozóny.[5]

2.2 Způsoby použití platebních karet

Nynější technologie umožňují podstatné rozšíření využití platební karet. Kromě nejužívanější aplikace – výběru hotovosti z bankomatu nebo u bankovní přepážky – je to zejména bezhotovostní platba v prodejních místech obchodu a služeb, která může nabývat celé řady forem:[6]

- **Výběr hotovosti z bankomatu**

  Při výběru hotovosti z bankomatu, která probíhá výhradně na elektronické bázi bez jakýchkoliv dokladů (kromě stvrzenky o provedení výběru), jde však stále o hotovostní transakci. Výběr peněz z bankomatu zvyšuje produktivitu výplaty hotovostí bankou a umožňuje svým klientům přístup k hotovosti 24 hodin denně. Bankomaty mohou pracovat v režimu online, tj. stálé propojení s autorizační centrálou, umožňující kontrolu zůstatku na účtu a dalších hodnot v reálném čase, nebo v režimu offline, kdy jsou kontroly prováděny proti hodnotám, jež jsou uloženy v paměti řídicího systému bankomatu a periodicky aktualizovány. V České republice pracují všechny bankomaty v režimu online.

- **Výběr hotovosti proti předložení karty (Cash Advance)**

  Hotovost lze obdržet po předložení karty, která tuto transakci dovoluje u bankovních pokladen nebo v některých vybraných obchodních místech (směnárny, mezinárodní hotely). Transakce musí být vždy, bez ohledu na výši částky autorizována, a to buď prostřednictvím elektronického terminálu, nebo telefonickým dotazem v „hlasovém“ autorizačním středisku.

- **Platba za zboží nebo služby v obchodním místě**

  Z pohledu účastníků (držitel karty, obchodník a zprostředkovatelská banka) jde o ideální způsob používání platebních karet. S hotovostí nemusejí manipulovat držitel ani obchodník, platba proběhne účetním převodem mezi účtem obchodníka a držitele karty a to prostřednictvím vnitřních účtů zpracovávající, případně i vydávající banky. Aby mohl obchodník přijímat platební karty

[5] POLOUČEK, S., et al. *Bankovnictví.* 2. vyd. Praha : C. H. Beck, 2013. s. 113.
[6] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 176.

jednotlivých značek k placení a platby mu byly uhrazeny, je potřeba, aby měl obchodník uzavřenou smlouvu se zpracovatelskou bankou tj. bankou, která má k této činnosti (tzv. acquiring) od příslušné asociace (EC/MC, VISA, American Express, JCB, Diners Club) licenční oprávnění.

- **Transakce MO/TO**

  Při rezervacích ubytování, v zásilkovém prodeji apod. lze použít způsob platby, spočívající v uvedení dat karty, potřebný k provedení platby (číslo karty, platnost) s podpisem držitele karty na objednávkovém formuláři, příp. v uvedení těchto dat při telefonické objednávce. Bance předá obchodní místo tato data ke zpracování obvyklým způsobem. Většina bank uzavírá smlouvy s obchodníky na tento typ transakcí jen výjimečně za zvlášť stanovených podmínek, jelikož tento způsob transakce nezaručuje dokonalou ochranu proti zneužití takto předávaných údajů.

- **Transakce prostřednictví veřejné datové sítě Internet**

  S rychlým rozvojem internetové sítě a stále větší objem nabízeného zboží a služeb v tomto virtuálním prostředí vzrostla také poptávka po zjednodušení plateb zde. Ze začátku řada tzv. virtuálních obchodů nabízela možnost uvedení čísla platnosti a platební karty přímo do objednávky. Ovšem zde bylo velké riziko zneužití, vzhledem k prakticky neomezené dostupnosti přenášených dat po síti. Rozvoj internetové sítě si vynutil i řešení toho problému. Největší kartové asociace – EC/MC a VISA spolu se společnostmi z oblasti IT vyvinuly a zveřejnily společný standard, umožňující bezpečný (šifrovaný) přenos dat pro platby platebními kartami v tomto prostředí. Standard známý pod zkratkou SET spočívá v přidělování tzv. certifikátů jednotlivým účastníkům sítě.

2.3 Rozdělení platebních karet

Platební karty můžeme členit podle určitých hledisek, které veřejnosti většinou splývají do názvů kreditní nebo úvěrová karta. V České republice se nejčastěji používá obecný název „platební karta“. Platební karty se postupem času vyvíjeli a rozšiřovali se jejich možnosti použití a fungování. Platební karty tedy nejsou stejné a můžeme je dělit do několika skupin podle řady kritérií:

Podle způsobu zúčtování transakcí:[7]

- **Charge Card** – na úplném začátku bylo záměrem vydavatele karty prodat více nebo i dražší zboží. Chtěl zjednodušit zákazníkovi placení tím, že bude hradit až na konci měsíce nebo ještě v pozdějším období. Tak vznikla Charge Card. Klient má obvykle stanovenou lhůtu 14 – 30 dnů od obdržení výpisu od vydavatele karty, během které svůj závazek musí vyrovnat. Na soukromých nebo služebních cestách karta slouží především jako jednoduchý, pohodlný a bezpečný platební prostředek.

  Karta umožňuje hradit bez problému nepředvídatelné výdaje nebo zakoupit zboží, které zákazník původně neplánoval, ale odstraňuje i nutnost obstarávat si například před služební cestou nebo nákupem hotovost nebo šeky a umožňuje tak hradit bez překážek tyto výdaje. Snižuje se riziko krádeže peněz, ztráty nebo jejich defraudace pracovníkem organizace. Mohou to být cestovní karty, virtuální, dárkové.
- **Úvěrová karta** – jedná se o spotřební úvěr čerpaný prostřednictvím revolvingového úvěrového účtu. Tento úvěr může být použit i splácen najednou nebo po částech. Splacením dlužné částky se úvěrový limit automaticky obnovuje. Poskytnutý úvěr nebývá zajištěn a banka proto nemá možnost realizovat nesplacený dluh pomocí zástavy. Po celou dobu platnosti karty zůstává relativně vysoké úvěrové riziko (v závislosti na druhu segmentu klientů), protože klient může kdykoliv opakovaně čerpat disponibilní limit, zatímco u jiných druhů spotřebních půjček se úvěrové riziko snižuje pravidelnými splátkami.
- **Debetní karta** – základem debetní karty je okamžité zatížení účtu klienta. Banka, která vydala kartu, se ihned dozví o transakci uskutečněné touto kartou. Znamená to tedy téměř okamžité placení všech transakcí.[8]
- **Předplacená karta** – nazývané také jako předplacená elektronická peněženka, transakce jsou zde ověřovány na úrovní čipová karta – platební terminál. Záměrem těchto karet je omezit používání drobných bankovek a mincí, nabíjení se provádí u provozovatele systému.[9]

[7] JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. s. 60.
[8] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 198.
[9] POLOUČEK, S., et al. *Bankovnictví.* 2. vyd. Praha : C. H. Beck, 2013. s. 114.

Podle druhu záznamu na kartě:[10]

První karty byly v zásadě dokladem, který potvrzoval nárok jejich držitelů na odklad placení. S postupným rozšiřováním těchto karet bylo třeba doložit, že klient kartu u obchodníka skutečně předložil a bylo také nutné zajistit správný přenos identifikačního čísla klienta. Karty z papíru pro tento účel nebylo možné použít, proto se vyráběly z kovu a později z plastu, který se používá dodnes.

- **Reliéfní záznam** – reliéfním písmem se do karty vyrazí identifikační údaje. Ty se pomocí kopírovacího papíru a přítlaku rukojeti s válečkem otiskují na účtenku. Tento způsob odstranil ruční přepisování identifikačních údajů z karty a doplňování identifikace obchodníka, při nichž docházelo k chybám a časovým ztrátám.
- **Magnetický záznam** – umožňuje u karet spustit službu výplaty hotovosti z bankomatů a později i elektronické placení. Na magnetickém proužku jsou údaje zakódovány. Použití karty v bankomatu nebo platebním terminálu je vázáno na znalost identifikačního kódu PIN.
- **Čipové karty** – k záznamu dat se využívá paměťový čip nebo mikroprocesor.
- **Laserové karty** – jsou založeny na principu záznamu dat na kompaktním disku. V bankovnictví se tyto karty nerozšířily a ani do budoucna se s nimi nepočítá.

Podle uživatele:[11]

- **Osobní karty** – tyto karty jsou určeny jen pro soukromé účely držitele karty (nákupy zboží a služeb pro jeho potřeby). Všechny osobní bankovní karty jsou vydány na jméno držitele, jsou nepřenosné a jsou vystaveny k jeho osobnímu účtu, příp. k účtu osoby, která souhlasila s vydáním karty pro jinou – zmocněnou osobu.
- **Služební karty** – jsou vyhrazeny převážně k úhradám výdajů spojených s plněním pracovních úkolů. Jsou vydávány pro majitele účtu a zmocněné pracovníky firem, podniků a vládních institucí. Nejsou určeny pro úhrady výdajů soukromého charakteru, vydávají se k firemnímu účtu.

[10] JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. s. 65.
[11] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 209.

Podle rozsahu služeb spojených s kartou:[12]

Rozsah služeb je jedním z hlavních faktorů, ke kterému klient při rozhodování o druhu zvolené karty přihlíží. Některé banky se zaměřují pouze na určitý segment trhu, jemuž přizpůsobují paletu nabízených karet. Na trhu jsou banky, které některé typy karet vůbec nenabízejí.

- **Doplňkové služby** – k některým kartám nejsou většinou nabízeny žádné doplňkové služby. Čím prestižnější typ karty, tím širší řada doplňkových služeb. Doplňkové služby jsou tím, co může poměrně výrazným způsobem odlišovat karty jednotlivých vydavatelů. Velmi důležitým prostředkem konkurenčního boje mezi vydavatelskými kartami se stává úroveň a rozsah těchto služeb. Mezi nejčastěji nabízené doplňkové služby patří zejména: pojištění léčebných výloh v zahraničí, úrazové a cestovní pojištění, členství v určitých společnostech, získání slev v řadě hotelů, autopůjčoven apod.

2.4 Náležitosti a technologie u platebních karet

Velkou podstatou rozšíření platebních karet jsou mezinárodní normy ISO a variabilní technologie schopná uskutečnit potřeby jednotlivých uživatelů. K těmto podmínkám je třeba přiřadit také úsporu nákladů, jednoduché použití a ekonomický provoz. Další technická a organizační zlepšení bylo potřeba vytvořit s rozšířením použitelnosti karet na celostátní i mezinárodní úrovni. V současné době tvoří moderní systém platebních karet následující prvky:[13]

- platební karta,
- platební terminál,
- bankomat,
- autorizační, clearingový a zúčtovací systém,
- systém řízení karet.

2.4.1 Rozměry a vlastnosti

První platební karty byly vyrobeny z plechu. Pak se zavedly plastové karty z PVC, aby se zjednodušilo placení a zvýšila ochrana karet proti padělání. Následně musely být vyvinuty nové technologie pro výrobu plastových karet. Pro potisk karet se

[12] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 211.
[13] JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. s. 37.

nejdříve zkoušel sítotisk, ale kvalita vyrobených karet nebyla vysoká. Každá karta byla v podstatě originálem. Od šedesátých let dvacátého století se pro potisk používá ofset.[14]

Rozměry a fyzikální vlastnosti plastiku platební karty stanoví mezinárodní norma ISO 3554. Plastik má pevně stanovený rozměr 85,6x54,0x0,76 mm. Většinou je vyroben z třívrstvého PVC s následujícími vlastnostmi:[15]

- odolnost proti mechanickému namáhání,
- nulový obsah toxických látek,
- strukturální stálost – odolnost vůči změnám teploty (rozmezí od -36 do 50°C),
- odolnost vůči chemickým vlivům při běžném používání.

2.4.2 Tištěné údaje na kartě

Nezbytné identifikační údaje (Embossing) se na kartu vyráží písmem OCR 7B velikosti 3,63 mm. Pro ně je určena dolní polovina přední části karty, kterou norma dělí na čtyři řádky:[16]

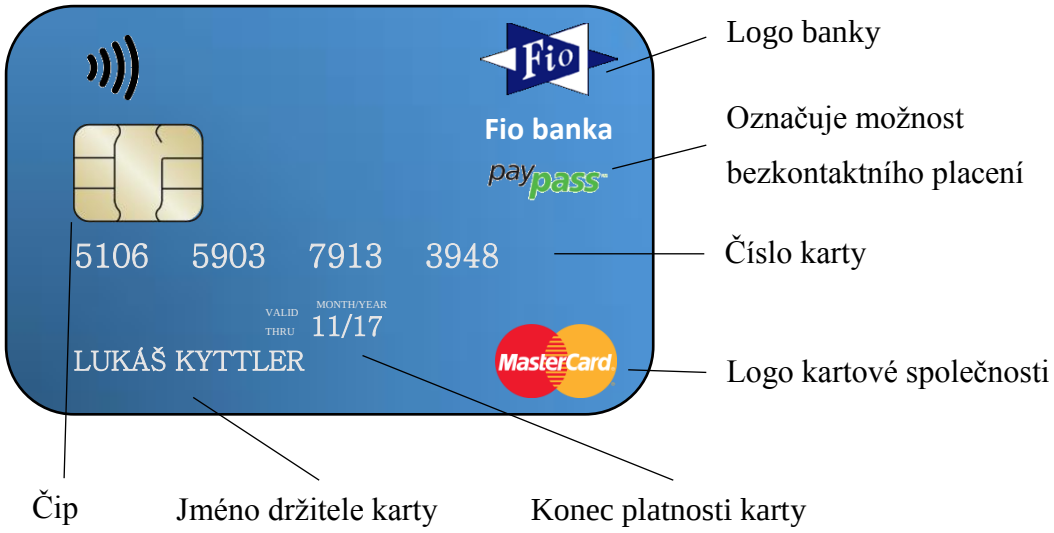
1. **Account Number Line** – obsahuje číslo karty. První číslice nebo dvojčíslí určují druh karty. Například MasterCard začínají vždy číslicí 5, VISA 4, číslice 4 a 5 také říká, že se jedná o bankovní sektor. Za nimi následuje identifikace vydavatele karty a identifikace konkrétního klienta.
2. **Valid Data Line** – uvádí se v ní období platnosti karty (měsíc a rok) a to buď v podobě uvádějícího začátek i konec platnosti nebo jen konec platnosti.
3. **Third Line** – je určena pro jméno držitele karty.
4. **Fourth Line** – obsahuje u služebních karet jméno společnosti, k jejímuž účtu je karta vydána.

Kromě výše uvedené identifikace musí karta dále obsahovat povinné bezpečnostní prvky a podkladový design. Rozmístění, tvar a velikost všech povinně užívaných prvků se řídí předpisy vydavatelských asociací a příslušnými ISO normami. Design platebních karet včetně rozmístění všech prvků je certifikován v sídle asociace vždy před realizací výroby plastiku platební karty, pod jejímž logem bude karta vydávána.[17]

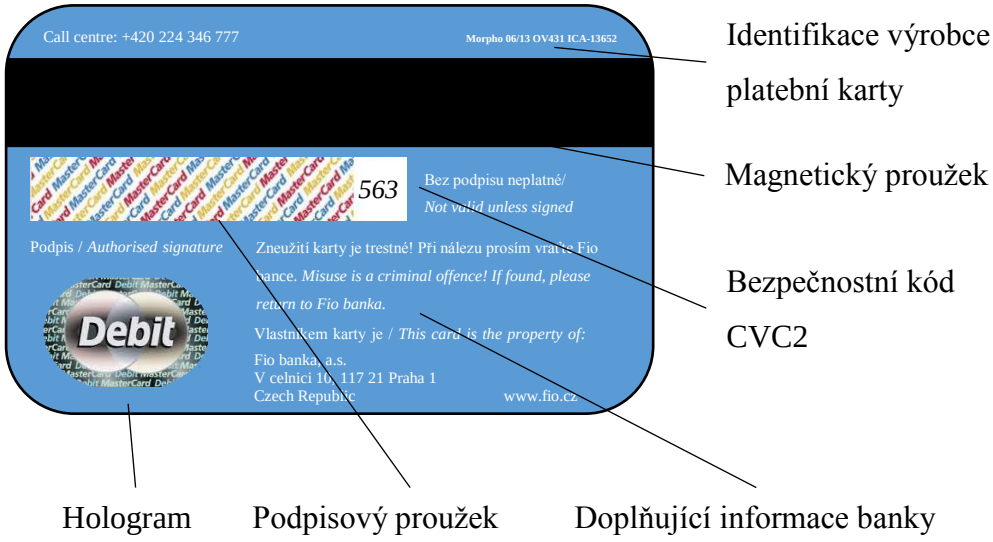
---

[14] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 72.
[15] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 229.
[16] JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. s. 38.
[17] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 231.

Obrázek č. 1: Přední strana platební karty[18]



Obrázek č. 2: Zadní strana platební karty[19]



2.4.3 Magnetický proužek

Zavedením platebních karet a magnetického záznamu, tzv. magnetického proužku se zjednodušilo a zrychlilo používání platebních karet v bankomatech a později i při placení. Magnetický proužek je definován normou ISO a to nejen pro bankovnictví, ale obecně pro všechny sektory. Norma ISO však ponechává dostatek prostoru pro to, aby např. bankovní platební systémy využívaly některá definovaná pole podle svých

[18] Vlastní zpracování.
[19] Vlastní zpracování

potřeb. Flexibilita standardu a snadná výroba umožnily, aby se magnetický proužek rychle rozšířil.[20]

Magnetický proužek obsahuje tři záznamové stopy:[21]

- **Stopa I** – je určena pouze pro čtení. Obsahuje identifikační údaje karty jako je platnost, jméno držitele a další bezpečností údaje. Obsahuje 79 znaků.
- **Stopa II** – je určena pouze pro čtení. Obsahuje podobné informace jako stopa první. Obsahuje 40 numerických znaků.
- **Stopa III** – je určena jak pro čtení, tak zápis dat. Slouží především pro off-line transakce. Na třetí stopě se nachází offset, podle kterého se ověřuje PIN, který je zde zašifrován. Obsahuje 109 numerických znaků.

2.4.4 Čipové karty

Čipová karta má obdobné fyzikální vlastnosti jako běžná platební karta. Čip je umístěn na přední straně pod povrchem plastiku v normalizované pozici. Pomocí normalizovaných kontaktních plošek je zajištěna komunikace mezi čipem a čtečkou v platebním terminálu nebo bankomatu. Samotný čip je v plastiku platební karty pevně zalepen a je chráněn právě kontaktními ploškami. Tyto karty nazýváme kontaktními.

Existují i čipové karty, které kontaktní plošky nemají. Čip je umístěn pod vrchní laminací plastiku karty. Prostřednictvím speciálních radiových snímačů je zajištěna komunikace s čipem. Nazýváme je bezkontaktními kartami a na rozdíl od kontaktních se vyznačují delší životností.

Bankovní čipové (popř. hybridní) karty jsou schopny bezpečně uchovávat informace sloužící k identifikaci držitele, o provedených transakcích, zůstatku, výši částky apod. Držitel může změnit osobní identifikační číslo PIN u těchto karet, což je z uživatelského hlediska pro něj velmi přijatelné.

Od roku 1999 začaly v České republice některé banky pracovat na vlastních projektech čipových karet dle standardu EMV verze 3.1.1. Na těchto velkých investicích se musejí podílet všechny banky zpracovávající transakce platebními kartami. Dle stanoviska asociace Europay International musejí od roku 2005 všechny členské banky vydávat platební karty založené výhradně na bázi čipové technologie.[22]

---

[20] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 75.

[21] *Magnetický proužek: přečíst ho je tak snadné* [online]. Praha : Economia, 2001 [cit. 2016-10-02]. Dostupné z WWW: <http://www.penize.cz/investice/14375-magneticky-prouzek-precist-ho-je-tak-snadne>.

[22] SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. s. 203.

2.4.5 Autorizační, clearingový a zúčtovací systém

Ověření transakce spočívá v kontrole samotné platební karty, zda není blokovaná nebo její platnost už vypršela. Autorizaci je možné provádět prostřednictvím dotazu telefonem a to u autorizačního střediska, které propojuje jednotlivé vydavatele karet. Ovšem dnes se ověřování provádí zpravidla prostřednictvím platebního terminálu, který ve většině případů pracuje online a je napojen na tuto síť. V tomto případě se ověřuje kód PIN držitele karty, který musí být zadán, autorizace probíhá zcela automaticky a trvá jen několik málo vteřin. Přenos je zajištěn prostřednictvím internetové sítě, na kterou jsou jednotlivé banky z celého světa napojeny. Systém provádí clearing veškerých plateb, které jsou uskutečněny prostřednictvím karet během jednoho dne. Do clearingového a zúčtovacího centra jsou tedy odeslány transakce provedené v České republice kartami vydanými v tuzemsku. Tyto vzájemné závazky jsou vyrovnány v českých korunách prostřednictvím komerčních bank a zúčtovacího centra České národní banky.[23]

[23] MÁČE, M. *Platební styk – klasický a elektronický.* Praha : Grada, 2006. s. 59.

3 RIZIKA PLATEBNÍCH KARET

Stejně jako všechny dosavadní druhy platebních prostředků (mince, bankovky, šeky) nebo cenin (známky, kolky), ani platební karty neunikly pozornosti pachatelů trestných činů. Proto se velmi brzy objevilo zneužití karet vlastními držiteli i cizími osobami (odcizené nebo ztracené karty), dokonce i padělky různé kvality.

Všechny tyto případy podvodů se v průběhu let odrazily v neustávajícím zdokonalování bezpečnostních technik ochrany karet i samotných platebních transakcí. Společnosti a asociace zabývající se provozem platebních systémů (včetně členských bank) dnes zaměstnávají rozsáhlé týmy odborníků, kteří se věnují vyšetřování a analýzám podvodných transakcí, přípravě nových ochranných technik a způsobu včasné detekce podvodných transakcí. Boj proti podvodníkům je veden na mezinárodní úrovni včetně spolupráce s Interpolem.

Žádný platební systém není dnes schopen absolutně zabránit vzniku škod vyplývajících ze zneužití platebních karet. Opatření pro zajištění úplné ochrany by byla tak nákladná a organizačně náročná, že by znesnadňovala (nebo i znemožňovala) jejich běžné používání. Proto je hlavním cílem dosažení kontroly nad trestnými činy v této oblasti a udržení jejich relativní úrovně v řádu promile z obratu.[24]

V České republice byly vždy lepší mezibankovní spolupráce než v ostatních zemích. V roce 1992 se do českého trestního zákona dostalo ustanovení o trestnosti padělání platebních karet, podvodů s nimi a neoprávněná držení.

V rámci sdružení pro bankovní karty byl v roce 1997 založen bezpečnostní výbor, který sdružoval pracovníky bank a dalších organizací, institucí, kteří se zabývali řešením podvodných transakcí. Tato spolupráce v boji proti organizovaným skupinám podvodníků má za následek snižování ztrát z podvodů. Jejich spolupráce s orgány činnými v trestním řízení v boji proti organizovaným nájezdům podvodníků nese užitek ve snižování ztrát z podvodů.[25]

[24] MARVANOVÁ, M., et al. *Platební styk*. 2. vyd. Praha : Bankovní institut, 1998. s. 311.
[25] *Bezpečnost karet* [online]. Praha : Sdružení pro bankovní karty, 2014 [cit. 2016-10-03]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_karty.html>.

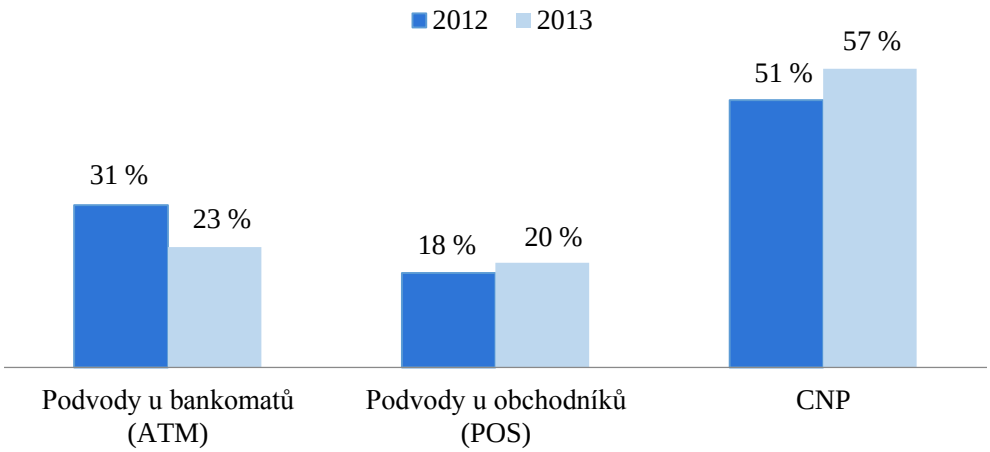
3.1 Podvody s platebními kartami v České republice

Co se týká rizik spojených s platebními kartami, tak je třeba rozlišit dvě situace. První situace je, když je karta fyzicky odcizena a následně je použita k neoprávněnému využití peněžních prostředků, například výběrem z bankomatu nebo platbou v POS terminálech.

Druhá situace nastane tehdy, když jsou získána důležitá data o platební kartě. Na základě těchto dat se může vytvořit padělaná karta a může být následně využita pro výběr z bankomatu nebo pro platbu v POS terminálech. Další způsob jak využít získaná data je, že pomocí CNP transakcí provedeme například platbu přes internet. Tento způsob je jeden z nejvyužívanějších jak můžeme vidět z grafu č. 1. Důvodem je jednak větší anonymita a větší možnost využití peněžních prostředků. K tomuto způsobu je ovšem potřeba CVV2/CVC2 kód, který se nachází na zadní straně platební karty a není obsažen v mikročipu nebo magnetickém proužku a není ho tedy možné získat např. pomocí skimmingu. Co se týká původu těchto dat, tak je velké množství způsobů jak je získat, a proto nelze přesně zjistit, kde k získaným datům došlo.

Z grafu č. 1 vyplývá, že CNP transakce jsou tedy jedny z nejčastějších podvodů. Nárůst ovšem zaznamenaly i podvody u obchodníků, to mohlo být způsobeno s rozvojem bezkontaktní technologie, která umožňuje placení bez nutnosti zadávání PIN kódu a to do částky nepřevyšující 500 Kč.

Graf č. 1: Rozložení podvodů s platebními kartami v ČR za rok 2012[26] a 2013[27] z pohledu vydavatele platebních karet



[26] *Third Report on card fraud: February 2014* [online]. Frankfurt nad Mohanem : European Central Bank, 2014 [cit. 2016-10-03]. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.
[27] *Fourth report on card fraud: July 2015* [online]. Frankfurt nad Mohanem : European Central Bank, 2015 [cit. 2016-10-03]. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.

Dále musíme rozlišovat, zda jsou útoky vedené na platební karty, které jsou vydané v dané zemi, tedy v ČR (issuing), nebo zda jsou vedené proti všem kartám v ČR, které jsou v dané zemi akceptovány (acquiring). Do statistik podvodů z pohledu issuingu jsou zahrnuty také podvody v zahraničí, které byly provedené kartami vydanými v ČR. Pro pachatele může být totiž jednodušší zneužít platební kartu v zahraničí.

Z hlediska acquiringu jsou do statistiky zahrnuty všechny zneužité platební karty, které se nacházely na území ČR za určité časové období. Jsou zde znatelné rozdíly, celkově v Evropě jsou nejrozšířenější podvody s CNP. Zatímco padělané karty, které se využívají k výběru z bankomatů nebo pro platby v POS terminálech jsou ve většině případů uskutečňovány mimo Evropu. Například v zemích Latinské Ameriky nebo Východní Asie.

V České republice bylo v roce 2013 vydaných 10 250 651[28] platebních karet. Celkový objem provedených transakcí byl 36 584 573 419 €. Z tabulky č. 1 můžeme tedy vypočítat, že na jednu platební kartu připadá ztráta 0,32 €. To je ovšem přepočet na všechny karty vydané v ČR, poškozených platebních karet bylo samozřejmě jen velmi málo. Celkový objem zneužitých finančních prostředků za rok 2013 byl 3 292 611 €.

Tabulka č. 1: Transakce a počet podvodů s platebními kartami[29]

	Hodnota (€)	**Počet transakcí**
Transakce na 1 kartu	3569	53
Transakce na 1 obyvatele	3529	53
Podvod za transakci	0,009 %	0,005 %
Podvod na 1000 karet	308	2,9
Podvod na 1000 obyvatel	305	2,8
Počet karet na obyvatele	1,0	

[28] *Souhrnné statistiky za rok 2013* [online]. Praha : Sdružení pro bankovní karty, 2013 [cit. 2016-10-08]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html>.

[29] *Fourth report on card fraud: July 2015* [online]. Frankfurt nad Mohanem : European Central Bank, 2015 [cit. 2016-10-08]. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.

3.2 Druhy rizik

S rostoucím počtem vydávaných platebních karet, se začaly také objevovat i rizika spojená s nimi. Platební systémy VISA, MC a další musely vyvíjet bezpečnostní systémy a zaváděly určité standardy. Se samotným rizikem ztráty se už v samotném obchodním modelu počítá, ale zpravidla by nemělo přesáhnout jedno promile z obratu.[30]

Při útocích na platební karty můžeme rozlišovat dvě situace. Zda je platební karta fyzicky odcizena nebo zda jsou odcizena „pouze" data o platební kartě. V případě kdy jsou odcizena pouze data o kartě, nemusí tato situace ihned znamenat peněžní ztrátu držitele platební karty. V těchto případech se pachatelé snaží nevzbudit u držitele karty podezření, že mu byla odcizena citlivá data a v následujícím určitém období mohou získaná data sami využit, například pro výrobu padělku platební karty nebo je prodat na černém trhu. Ve většině případů se jedná o útoky typu – skimming, krádež identity, phishing a získávání dat při online platbách na internetu.

Druhá situace nastane tehdy, když jsou odcizeny peněžní prostředky. Tato situace může nastat, když má pachatel přístup k datům o platební kartě a na základě těchto dat, vytvoří například padělek platební karty a následně jsou odcizeny finanční prostředky držitele karty. Další způsob odcizení peněžních prostředků a zároveň jeden z nejčastějších je prostá krádež nebo zneužití nalezené platební karty. Tyto útoky budou zcela jistě odhaleny, ať už samotným vlastníkem karty nebo bankou. Záleží zde na čase, po který bude moci pachatel zneužít platební kartu, než bude karta zablokována bankou.

3.2.1 Libanonská smyčka

Tato technika je nazývána podle Libanonců, kteří žili v Londýně a byli první, kteří tuto techniku používali a byli také následně zatčeni. Princip je takový, že na bankomat je nainstalované zařízení, které sice umožní vložení platební karty, ale jejímu vydání zpět držiteli už zabraňuje vytvořená smyčka. Držitel platební karty zadá do bankomatu svůj PIN a vybere si peníze. Bankomat mu ovšem kartu zpět nevydá. Po chvíli čekání zákazník obvykle odchází od bankomatu. V ten okamžik přistoupí k bankomatu pachatel, odstraní zábranu a vezme platební kartu, kterou bezprostředně využije k vybrání hotovosti z bankomatu nebo k placení. K tomuto úkonu bude ovšem potřebovat kód PIN, popřípadě by mohl pachatel využít získanou kartu k CNP transakcím.[31]

[30] *Budeme platit jen bankovními kartami?* [online]. Praha : RF Hobby, 2013 [cit. 2016-10-09]. Dostupné z WWW: <http://21stoleti.cz/2006/10/21/budeme-platit-jen-bankovnimi-kartami/>.
[31] JOSHI, M. *Black Cards Forensics.* 2. vyd. India : Indiaforensic, 2006. s. 14.

K získání kódu PIN má pachatel několik možností. Jedna s možností je, že k oběti přistoupí pachatel, který se bude snažit namluvit oběti, že bankomat je nejspíše rozbitý a poradí oběti, ať zkusí zadat opakovaně PIN, který následně odpozoruje. Poté doporučí oběti návštěvu pobočky banky. Následně pachatel odstraní mechanizmus zabraňující vysunutí platební karty a tu také bezprostředně zneužije.[32] Další způsoby získání PIN kódu mohou být za pomoci falešné klávesnice, kamery nebo může být odpozorován ať už v blízkosti bankomatu nebo ze vzdáleného místa, odkud má pachatel na bankomat dobrý výhled.

Tento druh útoku na platební karty se v České republice v současné době vyskytuje jen velmi vzácně. Většina českých bankomatů je na libanonskou smyčku odolná.[33]

Ochrana před tímto rizikem:[34]

- zkontrolovat bankomat před použitím, zda na něm nejsou stopy neoprávněného zásahu. Pokud do bankomatu nejde snadno vložit karta nebo se kolem bankomatu vyskytují podezřelé osoby, je lepší vyhledat jiný bankomat,
- kontrolu bankomatů provádějí také banky, instalují se kamery nebo modernější bankomaty, které dokážou detekovat umístění cizích předmětů,
- sledovat a řídit se pokyny na obrazovce bankomatu,
- pokud bankomat nesdělí oznámení o tom, že karta byla zadržena, neměli bychom předpokládat, že se banka dozvěděla o tom, že bankomat zadržel kartu,
- pokud bankomat nevydá platební kartu bez vysvětlení, měli bychom okamžitě zablokovat kartu u své banky.

3.2.2 Skimming

Ke skimmingu dochází nejčastěji u bankomatu, ale může být proveden i u obchodníka. Skimming je technika pomocí které jsou získávaná data z magnetického proužku nebo čipu na platební kartě, přičemž cílem pachatele je i získání příslušného kódu PIN. Následně pomocí těchto dat může být vytvořen padělek karty nebo mohou být data použita při CNP transakcích.

[32] *Když bankomat spolkne kartu* [online]. Praha : Economia, 2005 [cit. 2016-10-13]. Dostupné z WWW: <http://www.penize.cz/debetni-karty/17573-kdyz-bankomat-polyka>.
[33] *Podvody s kartami* [online]. Praha : Internet Info, 2010 [cit. 2016-10-13]. Dostupné z WWW: <http://www.mesec.cz/clanky/nejcastejsi-podvody-platebnimi-kartami>.
[34] *Zařízení na zachycení karty* [online]. Praha : Sdružení pro bankovní karty, 2016 [cit. 2016-10-13]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html>.

Skimming u bankomatu[35]

Pro tento účel je sestrojeno speciální technické zařízení, které většinou kombinuje dvě funkční části. První částí je skimmovací hrdlo, které je umístěné na bankomatu u vstupu pro platební kartu. Skimmovací hrdlo obsahuje čtecí magnetickou hlavu, datové úložiště a napájecí zdroj. Toto zařízení zaznamenává a ukládá data z magnetického proužku platební karty vložené do bankomatu.

Druhá část je skimmovací lišta, která je vyrobena nejčastěji z plastu a je osazena kamerou, datovým uložištěm a také napájecím zdrojem. Tato část se umísťuje na napadený bankomat a to tak, aby bylo možné pomocí kamery zaznamenávat zadávaný PIN držitelem platební karty. Tímto způsobem jsou získána data o platební kartě, která jsou následně pachateli zpracována a pomocí dalšího vybavení jsou využita nejčastěji k výrobě padělků platebních karet. Tyto platební karty jsou následně využity k výběru hotovosti a to většinou v zahraničí (padělky evropských karet, které jsou hybridní, mají tedy čip i magnetický proužek dohromady, lze využít jen v zemích, kde je podporována pouze technologie magnetických proužků).

Ochrana před tímto rizikem:[36]

- zkontrolovat bankomat před použitím, zda na něm nejsou stopy konstrukční změny nebo úpravy. Pokud do bankomatu nejde snadno vložit karta nebo se kolem bankomatu vyskytují podezřelé osoby, je lepší vyhledat jiný bankomat,
- pro výběr hotovosti je lepší zvolit bankomat, který je na frekventovaném a osvětleném místě,
- při zadávání kódu PIN zakryjeme klávesnici s čísly druhou rukou, tímto eliminujeme možné odpozorování číselné kombinace,
- pravidelná kontrola výpisu z účtu,
- dodržovaní diskrétní zóny u bankomatu, nenechat se ničím a nikým ovlivnit,
- výběr z bankomatu neprovedeme, pokud máme podezření, že není něco v pořádku,
- bankomaty, které jsou doplněné o antiskimmingové prvky, popř. bezkontaktní bankomaty, antiskimmovací hrdla.

[35] KLUFA, F. *Elektronické platební prostředky: Jak se vyhnout rizikům.* Praha : Sdružení českých spotřebitelů, 2013. s. 9.
[36] *Skimming* [online]. Praha : Národní centrála proti organizovanému zločinu, 2013 [cit. 2016-10-14]. Dostupné z WWW: <http://www.policie.cz/clanek/skimming-2013.aspx>.

Skimming u obchodníka[37]

Zde v roli nepoctivého pracovníka obchodní společnosti, který může během platby kartou použít zařízení ke zkopírování dat z magnetického proužku. Data jsou opět nejčastěji použita k výrobě padělku platební karty nebo k transakcím bez přítomnosti karty. K těmto transakcím dochází bez vědomí držitele platební karty.

Nejčastěji k takovým případům dochází v barech, hotelech, restauracích a čerpacích stanicích. Pracovník k provedenému skimmingu může používat různé manipulační triky, nátlaky nebo výmluvy. Jde mu především o odlákání pozornosti klienta, aby mohl zkopírovat údaje platební karty, toto může provést i za cenu, že nebude zaplaceno za zboží či službu, aby nevzbudil zbytečná podezření.

Pracovník se bude snažit získat kromě dat z magnetického proužku také PIN. Chování pracovníka se bude odlišovat od obvyklého chování personálu při platbě kartou. Nepoctivý pracovník může říci, že je nefunkční platební terminál nebo jeho klávesnice a následně požádá o sdělení kódu PIN s tím, že transakci provede sám po zprovoznění terminálu/klávesnice, nebo nám poskytne jiný platební terminál/klávesnici než na kterém jsme začali transakci poprvé provádět.

Ke skimmingu nemusí dojít přímo u obchodníka, v minulosti se objevil případ, kdy se podvodníci vydávali v převleku za policii a předstírali, že kontrolují pravost karet. Ve skutečnosti použili zařízení ke zkopírování dat na platební kartě a požádali ještě o PIN. Důvěřivější a nepoučení držitele platebních karet se mohou díky takovýmto způsobům nechat oklamat.

Ochrana před tímto rizikem:

- nikdy nikomu nesdělovat PIN a ani ho nezaznamenávat poblíž platební karty,
- nenechte nikdy personál odejít s platební kartou z Vašeho dohledu,
- při platbách za zboží či služby je potřeba mít stálý dohled nad platební kartou,
- při zadávání kódu PIN zakryjeme klávesnici s čísly druhou rukou, tímto eliminujeme možné odpozorování číselné kombinace,
- nenechat se nikým zmanipulovat,
- použití čistě čipových platebních karet namísto hybridních, které umožňují jednoduší okopírování karty díky magnetickému proužku,
- pravidelná kontrola výpisu z účtu.

[37] *Skimming u obchodníka* [online]. Praha : Sdružení pro bankovní karty, 2016 [cit. 2016-10-14]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Skimming>.

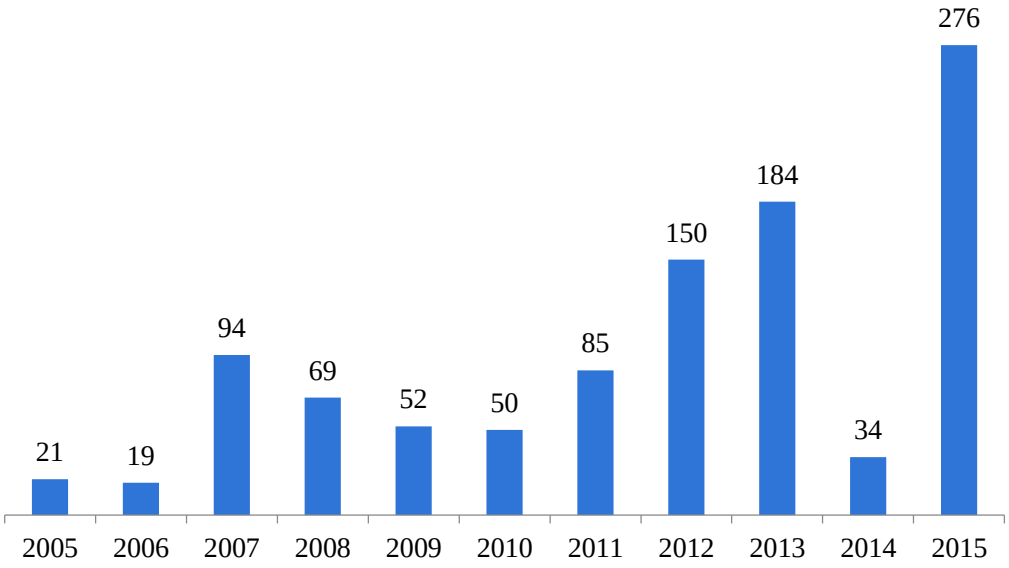
Skimming v České republice[38]

V roce 2015 bylo na území ČR evidováno 276 skimmingových útoků. Nejvíce skimmingových útoku bylo na území hlavního města Prahy a Středočeského kraje, tyto dvě oblasti tvořili 189 z celkových 276 skimmingových útoků. U 182 případů bylo přímo nasazeno skimmovací zařízení, u ostatních případů šlo o použití tzv. testovací karty, která se používá pro ověření funkčnosti skimmovacího zařízení. Za rok 2015 nebyl evidován žádný skimmovací útok u obchodníků.

Po odcizení dat z platební karty jsou data využita k vytvoření padělku platebních karet. S těmito kartami jsou prováděny výběry hotovosti v bankomatech mimoevropských zemí (Vietnam, Ekvádor, Salvador, USA). Jedná se o země, kde bankomaty a POS terminály nevyžadují k provedení transakce čtení z čipu platební karty.

Většinou se jedná o organizované skupiny, které se zaměřují na oblast platebních karet. V roce 2015 se jednalo o skupiny převážně z Bulharska, Moldávie a Rumunska. Pokles v roce 2014 je přisuzován k celkem vysoké objasněnosti této trestné činnosti a dále tím, že za ní české soudy ukládají poměrně vysoké tresty. V roce 2008 se začaly instalovat na bankomaty antiskimmovací hrdla, tudíž je zde znát mírný pokles skimmingových útoků.

Graf č. 2: Počet skimmingových útoků za určitá období[39]



[38] *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2015* [online]. Praha : Ministerstvo vnitra ČR, 2016 [cit. 2016-10-14]. Dostupné z WWW: <http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx>.

[39] *Skimming* [online]. Praha : Národní centrála proti organizovanému zločinu, 2015 [cit. 2016-10-14]. Dostupné z WWW: <http://www.policie.cz/clanek/skimming-2013.aspx>.

3.2.3 Riziko zneužití osobou blízkou

Přátelé, příbuzní a popřípadě další osoby, které se dostávají do častého kontaktu s držitelem platební karty, mohou být určitým rizikem. Zneužít platební kartu nebo získat potřebné údaje je pro ně snazší, protože mají většinou důvěru u držitele platební karty, tedy potencionální oběti. Z platební karty mohou být opsány údaje, které mohou být následně využity k platbám na internetu, nebo může pachatel vylákat z oběti PIN kód a platební karta může být využita k platbám v POS terminálech nebo k vybrání hotovosti v bankomatech.

Pokud ovšem i sám držitel platební karty poskytnul dobrovolně platební kartu třetí osobě, porušuje tím obchodní podmínky jak on tak osoba, která neoprávněně disponuje jeho platební kartou. Platební kartu může používat třetí osoba jen tehdy, pokud se jedná o zmocněnou osobu, která je uvedená ve smlouvě. Dále držitel nesmí nikomu sdělovat kód PIN.

Ochrana před tímto rizikem spočívá především v tom, aby držitel platební karty dodržoval určitá preventivní opatření, která jsou uvedená v obchodních podmínkách banky, která mu spravuje jeho účet a vydala mu platební kartu:[40]

- držitel platební karty je povinen zabránit prozrazení kódu PIN, čísla platební karty, platnost platební karty, CVC2 nebo CVV2 kód a jednorázových kódů zaslaných v rámci 3D Secure,
- je zakázáno zaznamenávat si kód PIN na platební kartu nebo na předmět, který se nachází v blízkosti platební karty,
- je zakázáno sdělovat PIN jakýmkoliv osobám,
- nikomu nepůjčovat platební kartu,
- držitel platební karty je povinen nahlásit bance jakékoli pochybnosti či podezření na zneužití platební karty,
- banka doporučuje mít nastavené limity pro internetové platby na minimální hodnotě.

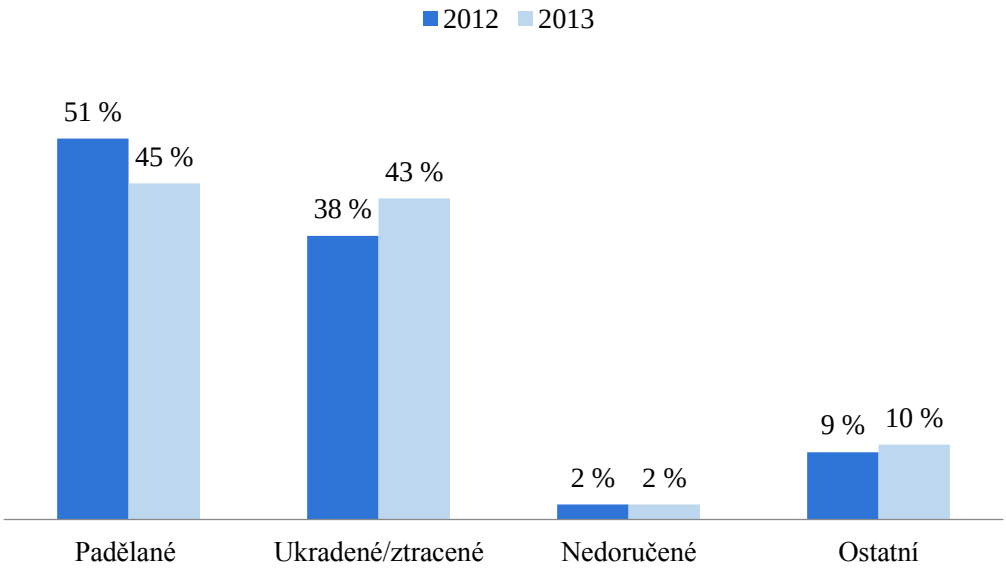
[40] *Obchodní podmínky pro vydávání a používání vlastních platebních karet* [online]. Praha : Fio banka, 2016 [cit. 2016-10-30]. Dostupné z WWW: <http://www.fio.cz/docs/cz/OP_Karty.pdf>.

3.2.4 Ztráta, odcizení a nedoručené platební karty

Jedním z největších rizik pro držitele platební karty je odcizení nebo ztráta platební karty a její následné zneužití. Z grafu č. 3 vyplývá, že v roce 2013 bylo z celkových podvodů s platebními kartami 43 % platebních karet odcizeno nebo ztraceno a následně zneužito a to v rámci card-present transakcí (card-present transakce v Evropě tvořily v roce 2013 34 % z celkových podvodů, 66 % byly CNP transakce, použity jsou data pro celou Evropu, jelikož žádná data v tomto směru pro ČR nejsou k dispozici). Zatímco padělání karet každým rokem klesá, u ztracených nebo odcizených karet toto pravidlo neplatí. Pokles padělání je způsobený rozšířením čipových karet a také bezkontaktních, kdy na bezkontaktní platby ještě nebylo evidováno skimmovací zařízení.[41]

Příčin růstu odcizených a ztracených platebních karet může být několik, například rozšíření bezkontaktních karet, díky kterým není potřeba zadávat do určité částky PIN. Toto je pro potencionální pachatele jeden z nejjednodušších způsobů jak zneužít nalezenou nebo odcizenou platební kartu.

Graf č. 3: Složení podvodů s platebními kartami v Evropě za rok 2012[42] a 2013[43] v rámci card-present transakcí



[41] *Fourth report on card fraud: July 2015* [online]. Frankfurt nad Mohanem : European Central Bank, 2015 [cit. 2016-10-30]. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.
[42] *Third Report on card fraud: February 2014* [online]. Frankfurt nad Mohanem : European Central Bank, 2014 [cit. 2016-10-03]. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.
[43] *Fourth report on card fraud: July 2015* [online]. Frankfurt nad Mohanem : European Central Bank, 2015 [cit. 2016-10-30]. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.

Držitel platební karty by měl kontrolovat, zda stále platební kartou disponuje. Pokud ji ztratil nebo mu byla odcizena, měl by urychleně zkontaktovat svou banku. Banka následně zablokuje veškeré elektronické transakce. Po zablokování platební karty může ale stále pachatel za jistých okolností provést neautorizovanou bezkontaktní platbu a to až do částky 500 Kč. A to u terminálů, které pracují v offline režimu, resp. nebudou vyžadovat okamžité potvrzení. Offline transakce jsou tedy ty, které nebyly autorizované online. Do vydavatelské banky jsou informace zaslány až po zpracování, které proběhne v jedné z karetních asociací (VISA, MC) a také v bance obchodníka, který platbu akceptuje. Muselo by se samozřejmě jednat o ztrátu/odcizení bezkontaktní platební karty. A zároveň platební karta také nesmí vyžadovat online potvrzení, některé platební karty to mají nastavené jako prioritu. Důvody offline transakcí jsou jasné, jsou zde nižší náklady na mezibankovní poplatky.[44]

Pokud nebude platební karta včas zablokována, pachatel může provést několik plateb u obchodníků a to do částky 500 Kč a to bez nutností zadání kódu PIN, musí se však jednat o bezkontaktní platební kartu. Přesný počet transakcí, které může pachatel provést má každá banka jinak nastavené, a z bezpečnostních důvodů se nesdělují (většinou se však jedná 3-5 transakcí, kdy se platba nemusí autorizovat, ale není to pravidlo). Po překročení těchto limitů je potřeba ověřit transakci za pomocí kódu PIN. Pokud bude mít pachatel k dispozici i kód PIN, mohou být ztráty na účtu majitele v řádech desetitisíců.

Pachatel takto získanou kartu může využít také k CNP transakcím, ovšem musí opět jednat velice rychle. Nicméně právoplatný držitel platební karty musí jednat také rychle a po zjištění, že postrádá platební kartu, ji musí co nejdříve zablokovat u své banky, která mu platební kartu vydala.

Ochrana před tímto rizikem:

- opatrovat platební kartu/y,
- kontrolovat pravidelně výpisy z účtu,
- nezaznamenávat si PIN poblíž platební karty,
- pří zjištění ztráty platební karty okamžitě tuto skutečnost nahlásit bance,
- využívání informačních e-mailů/SMS o realizovaných pohybech na účtu,
- nemít nastavené zbytečně vysoké limity.

[44] *Offline Transaction* [online]. Austin : InvestingAnswers, 2010 [cit. 2016-10-04]. Dostupné z WWW: <http://www.investinganswers.com/financial-dictionary/personal-finance/offline-transaction-2317>.

Nedoručené platební karty

Riziko nedoručené platební karty a její následné zneužití je v současnosti u nás v České republice téměř nulové. Potencionální hrozba, která může nastat je otevření poštovní zásilky třetí osobou a získání tak citlivých údajů o platební kartě, které mohou být následně zneužity. Platební karty se většině případů zasílají poštovní zásilkou, a i kdyby platební karta nedorazila, tak banky v České republice zasílají karty výhradně neaktivované, aby předešli podobným rizikům. Tudíž riziko nedoručené a následně zneužité platební karty je u nás v současné době nemožné. Platební karty se nejčastěji aktivují pomocí bankomatu, platby u obchodníka (musí to být online POS terminál), internetového bankovnictví nebo i telefonicky. Kód PIN je buďto zasílán zvlášť poštovní zásilkou, nikdy není zasílán společně s platební kartou. PIN si také můžeme sami zvolit prostřednictvím internetového bankovnictví, popřípadě může být zaslán SMS zprávou, každá banka má své způsoby.

Ochrana před tímto rizikem:

- při porušení poštovní zásilky, by měl držitel platební karty informovat banku,
- pokud ve stanové lhůtě nedorazí platební karta, tak také.

3.2.5 Phishing

Je snaha o získání citlivých dat klientů bank, většinou je to za pomocí e-mailových zpráv. Slovo phishing je odvozeno od anglického „fishing“, což v překladu znamená rybaření. Rybaření velice vystihuje tento způsob útoku, je rozesláno několik stovek e-mailových zpráv a jenom se čeká, kdo se „chytne“. Tyto nevyžádané e-mailové zprávy jsou zasílány ze zdánlivě důvěryhodného zdroje a jsou především zaměřeny na důvěřivé a neznalé klienty bank. Dále je zde velice proměnlivá kvalita těchto zpráv, některé jsou „amatérské“ a obsahují gramatické chyby a celkově jsou psány lámavou češtinou (viz příloha I).

Na druhé straně jsou zde phishingové zprávy, které jsou mnohem propracovanější a snaží se o co největší podobnost s bankou klienta (viz příloha II). Obsahují loga bank, jména zaměstnanců a většinou se jedná o zprávu, která obsahuje přímý odkaz na podvodné webové stránky, které se tváří jako stránky banky nebo na formulář do kterého se vyplní citlivá data např. o platební kartě. Cílem těchto útoků je tedy získání přihlašovacích údajů ke službě internetového bankovnictví nebo čísla platebních karet, jejich platností a CVV2/CVC2 kódů. Nejčastější phishingové útoky jsou na Českou spořitelnu, důvod je prostý, Česká spořitelna má nejvíce klientů v ČR.

Phishing nemusí mít nutně formu e-mailové zprávy, jsou zde i další způsoby. Poslední dobou se objevují phishingové útoky spojené se sociálními sítěmi, především Facebookem. Na Facebooku se objevil falešný profil, který nabádal k využívání nového internetového bankovnictví od České spořitelny. [45]

Další z útoků rovněž na Facebooku, kde pachatelé cílili na správce českých a slovenských facebookových profilů firem a dalších takovýchto stránek. Správci dostali varováni o tom, že jejich účet byl označen za podezřelý ostatními uživateli. Zpráva obsahovala odkaz na formulář, kde se měly vyplnit údaje o platební kartě a přihlašovací údaje na Facebook. Tímto mohl pachatel získat finanční prostředky a zároveň přístup na profily firem a dalších podobných fanouškovských stránek, díky kterým mohl například šířit reklamy, spam nebo podobné podvodné formuláře.[46]

Mezi další druhy phishingu patří smishing a vishing. U smishingu jde o textovou zprávu zaslanou na mobilní telefon, která příjemce nabádá k zaslání údajů o platební kartě nebo přihlašovacích údajů do internetového bankovnictví. Vishing je forma podvodu, který je zahájen telefonátem a nabádá klienta k přihlášení do internetového bankovnictví ze svého počítače. Tento počítač je ovšem napadnut virem a sleduje vše, co je zadáváno do přihlašovacího formuláře.[47]

Je třeba brát zřetel, že phishingové útoky se nemusejí týkat jen bank, ale i jiných společností jako jsou karetní asociace, či další internetové firmy například PayPal.

Ochrana před těmito riziky:

- především banka ani jiná instituce nebude po nás nikdy chtít jakékoli přihlašovací údaje nebo údaje o platební kartě, nikdy a nikomu nic nesdělujeme,
- neměli bychom se přihlašovat do internetového bankovnictví na neznámých Wi-Fi sítích a už vůbec ne na veřejných počítačích,
- klást důraz na ochranné mechanismy svého počítače i chytrého telefonu a pravidelně je aktualizovat, mít aktivní antivirový program,
- neotvírat přílohy a e-maily od neznámých nebo podezřelých odesílatelů,
- pravidelně měnit hesla a nepoužívat stejná pro přihlašování na různých webech,
- přihlašovat se pouze na ověřených webech.

[45] *Falešný profil na Facebooku nabízející „nový servis 24“* [online]. Praha : Česká spořitelna, 2016 [cit. 2016-10-04]. Dostupné z WWW: <http://www.csas.cz/banka/content/inet/internet/cs/sc_17573.xml?archivePage=phishing&navid=nav00156_phishing_aktuality>.

[46] *Útočníci na Facebooku kradou přihlašovací údaje administrátorů stránek a čísla platebních karet* [online]. Praha : ESET software, 2016 [cit. 2016-10-04]. Dostupné z WWW: <https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/article/utocnici-na-facebooku-kradou-prihlasovaci-udaje-administratoru-stranek/>.

[47] KALABIS, Z. *Základy bankovnictví.* Brno : Albatros, 2012. s. 153.

3.2.6 Pharming

Pharming je o něco vyspělejší verzí phishingu akorát není v podobě e-mailu. Úmyslem je získat důležitá data a to bez jakéhokoli podezření klienta banky. Můžeme rozlišovat dva způsoby pharmingu. První způsob pharmingu je méně obtížný a jde o přesměrování z jednoho webu na web jiný pomocí souboru hosts. Soubor hosts slouží pro lokální mapování domén a IP adres a říká, jaká IP adresa se přiřadí k určité doméně. Tento způsob je pro pachatele o něco jednoduší, nejčastěji se do počítače dostane pomoci viru nebo otevřením přílohy v e-mailové zprávě. Druhý způsob je o něco složitější, ale za to více efektivní. V tomto případě je napadán DNS a může postihnout více potencionálních obětí, než v případě prvního způsobu, který změní soubor hosts pouze v konkrétním počítači a je tedy spíše zaměřen na jednotlivce.[48] DNS (Domain Name Sever) je prostředník mezi IP adresou počítače a webem na který se chceme připojit. Každý počítač má svou definovanou IP adresu a není možné ukládat všechny tyto adresy počítačů, které jsme navštívili nebo je plánujeme navštívit. Proto máme DNS, který má uložené databáze jmen a k nim přiřazené IP adresy.

V obou případech, když se uživatel pokusí jít na webové stránky své banky je následně přesměrován na jiné vizuálně podobné. Takže pachatel vytvoří falešné webové stránky banky X2, které budou vypadat co nejpodobněji jako originál X1. Klienti bank se budou chtít přihlásit například do internetového bankovnictví prostřednictvím formuláře, ovšem se nenacházejí na pravých webových stránkách banky, ale na stránkách, které jsou jim pouze podobné X2. Jakmile si banka uvědomí, že její stránky jsou přesměrovány na X2 (většinou se jedná o web, který má velmi podobnou adresu, jako např. sezvis24.cz versus servis24.cz), okamžitě sjednají nápravu a přesunují je zpět na X1. Ačkoliv jsou teď stránky X2 uzavřené, pachatelé byli schopni shromažďovat veškeré údaje během celé délky trvaní přesměrovaní, které mohly trvat několik minut, ale i dnů.[49]

V současné době pharming v České republice není již moc častý a vyskytuje se jen zřídka, pachatelé se spíše zaměřují na jednodušší metodu a to phishing.

Ochrana před tímto rizikem:[50]

- používat internet od prověřeného poskytovatele, nepoužívat veřejné Wi-Fi sítě,

[48] *Podvody v oblasti bezhotovostních plateb v ČR* [online]. Praha : Sdružení českých spotřebitelů, 2009 [cit. 2016-11-07]. Dostupné z WWW: <http://www.finarbitr.cz/download/137_cs_a5_bezhotovostni_podvody.pdf>.

[49] DULANEY, E., EASTTOM, CH. *CompTIA Security+ Certification Study Guide.* 6. vyd. Indianapolis : Wiley, 2014. s. 322.

[50] *Prevent Pharming - Protect Your Identity* [online]. San Jose : Symantec, 2009 [cit. 2016-11-08]. Dostupné z WWW: <http://securityresponse.symantec.com/norton/clubsymantec/library/article.jsp?aid=cs_prevent_pharming>.

- kontrolovat adresu webu, na který se připojujeme a také kontrolovat protokol http zda obsahuje „s“ tedy https, písmenko „s“ značí secure tedy zabezpečený protokol,
- kontrolovat certifikát webu, zda je platný a má legitimního majitele,
- prověřit zda se jedná o zašifrované připojení, to označuje klíč a visací zámek,
- mít aktivní antivirový program a udržovat ho aktualizovaný,
- mít nainstalované nejnovější aktualizace pro webový prohlížeč a operační systém.

3.2.7 Internetové platby

Obchod v rámci e-commerce je stále rostoucí a v České republice bylo na internetových obchodech utraceno za rok 2015 více než 81 miliard korun. Trend nakupování online a placení online v obchodech se stává stále běžnější záležitostí. Pro letošní rok se očekává opět nárůst objemu transakcí.[51]

Tento rostoucí trend s sebou nese určitá rizika, pokud budeme platit online pomocí platební brány a pomineme rizika typu - nedodání zboží u platby předem nebo třeba zaslání pytlíku rýže místo mobilního telefonu, tak nám zde hrozí zneužití údajů platební karty. Když se vyvíjely platební karty, tak se nepočítalo s online platbami, to měl změnit příchod CVV2/CVC2 autorizační kód, který měl přispět k bezpečnosti a v poslední době u nás poslední dobou stálé rozšířenější 3D Secure.

Údaje o platební kartě může zcizit například sám internetový obchod nebo pouze jeho zaměstnanec. Při platbách na internetu totiž nikdy nevíme, kdo další má přístup k našim datům, i když zde platí mezinárodní pravidla PCI DSS, která stanovují určité bezpečnostní prvky, které musí obchodník splnit, pokud přijímá platební karty.

Další z možností jak získat údaje platební karty je odcizení přímo od zprostředkovatele platby, tedy platební brány. V České republice není zatím evidován podobný útok. Nicméně nedávno byla napadena Bostonská společnost BlueSnap, která je provozovatelem platební brány a bylo jí odcizeno přes 324 tis. údajů o platebních kartách.[52]

---

[51] *Česká e-komerce v roce 2015 předčila očekávání, růst se nezastaví ani v roce 2016* [online]. Praha : Asociace pro elektronickou komerci, 2016 [cit. 2016-11-08]. Dostupné z WWW: <https://www.apek.cz/clanky/ceska-e-komerce-v-roce-2015-predcila-ocekavani-ru>.

[52] *324K Regpack users' info compromised when decrypted files placed on public-facing server* [online]. New York : Haymarket Media, 2016 [cit. 2016-11-13]. Dostupné z WWW: <https://www.scmagazine.com/324k-regpack-users-info-compromised-when-decrypted-files-placed-on-public-facing-server/article/529780/>.

Ochrana před tímto rizikem:

- nakupovat pouze u prověřených obchodníků nebo u obchodníků, kteří mají zavedenou službu 3D Secure, když má obchodník tuto službu, tak jsou zadávány všechny údaje o platební kartě mimo jeho webové stránky,
- mít nastavené minimální limity pro internetové platby nebo je mít ideálně vždy na 0 a pouze při plánovaném nákupu je změnit,
- používat internet od prověřeného poskytovatele a nepoužívat veřejné Wi-Fi sítě,
- mít aktivní a aktualizovaný antivirový program,
- udržovat aktualizovaný webový prohlížeč a operační systém.

3.2.8 Platby pomocí chytrého telefonu

Platby chytrým telefonem jsou v České republice stále více a více populárnější. Platby bez nutnosti nošení platební karty, nutností je ovšem telefon s technologii NFC, platba totiž probíhá pomocí této technologie, kde data jsou uložena v telefonu a pomocí NFC telefon komunikuje s platebním terminálem. Na úplném začátku banky spolupracovaly s mobilními operátory a vydávali speciální SIM kartu, která obsahovala NFC technologii, od toho se však upustilo, protože mobilní operátoři chtěli určitý podíl a tak banky přestoupili na HCE platby. Tyto HCE platby probíhají za pomoci nainstalované aplikace od banky nebo i kartové společnosti (VISA, MC) a umožňují tak platby telefonem bez nutnosti mobilních operátorů. Využít se dá také NFC nálepka, které některé banky vydávají, informace o kartě jsou nahrány do čipu.[53]

Jak už to tak bývá, tak s novou formou placení se zde objevili i nová rizika. Chytré telefony se sice v současné době prodávají více než počítače, ale s jejich bezpečností to není o moc lepší než u počítačů. S jejich rozšířením se rozšiřují i útoky na ně, a jelikož některé chytré telefony většinou postrádají prvky jako je firewall, antivir, šifrování a mobilní operační systémy nejsou tak často aktualizované, tak jako počítače. Bohužel jedno z rizik je také samotný uživatel, který si tyto bezpečnostní nedostatky neuvědomuje a ze své neznalosti nebo nedbalosti nainstaluje například neověřenou aplikací, která může v nejhorším případě přeposílat citlivá data nebo dokonce ověřovací SMS zprávy.

[53] *Revoluce v placení: Chytrým mobilem platí v obchodech už tisíce Čechů* [online]. Praha : Mafra, 2016 [cit. 2016-11-15]. Dostupné z WWW: <http://finance.idnes.cz/novy-trend-bezkontaktni-platby-mobilem-fc8-/bank.aspx?c=A161020_073627_bank_sov>.

Podobných případů už se v České republice několik objevilo, kdy klient banky byl vybídnut pachatelem, aby si nainstaloval aplikaci, která měla být prezentována jako „nová verze smartbankingu“, klient bohužel tak učinil. Tato aplikace následně přeposílala veškerá nutná data pro potvrzování plateb. Toto všechno bylo skryté, aniž by o tom klient banky věděl, takto vybavený útočník měl otevřenou cestu k jeho penězům.[54]

Společnost Kaspersky Lab[55] upozornila na vir, který se ukrýval v GoogleAdSense. Tento trojský kůň napadl více než 300 tis. telefonů s operačním systémem Android a byl zaměřen na získání údajů o platebních kartách. Pachatelé využili bezpečností chybu v prohlížecí Google Chrome, vir se tvářil jako aktualizace prohlížeče, nebo jiné populární aplikace a vybízel tak uživatele ke stažení. Jakmile se vir spustil, požádal o práva k řízení telefonního zařízení a tímto se stal ještě složitěji detekovatelným.

Riziko ztráty nebo krádeže chytrého telefonu, který obsahuje aplikaci pro platby telefonem, by nemělo znamenat okamžité zneužití finančních prostředků. Proti takovýmto „nahodilým“ situacím, musí být zaplá příslušná aplikace banky nebo karetní asociace a ty jsou většinou chráněny heslem nebo se platba provede až po prověření pomocí čtečky otisku prstu oprávněného majitele telefonu. Chytré telefony má dále většina lidí zabezpečených pomocí hesla, pinu nebo podobných ochranných opatření.

Ochrana před tímto rizikem:

- dbát na zabezpečení svého mobilního zařízení, být opatrný u instalování některých aplikací – nejprve si je trochu prověřit, např. jaká chtějí povolení k využívání určitých funkcí telefonu,
- vyhnout se připojování na veřejné Wi-Fi sítě, nemít zbytečně zapnuté funkce jako je Bluetooth, infraport, NFC pokud je nepotřebujeme,
- udržovat chytrý telefon aktualizovaný, včetně všech aplikací, používat antivirový program,
- neklikat na odkazy zaslaných z podezřelých e-mailů.

[54] *Setkává se s útoky na bankovní účty lidí. Češi jsou nepoučitelní,* říká [online]. Praha : Mafra, 2016 [cit. 2016-11-15]. Dostupné z WWW: <http://finance.idnes.cz/internetova-bezpecnost-a-utoky-na-bankovni-ucty-fux-/bank.aspx?c=A160608_154955_bank_sov>.

[55] *Kaspersky Lab Reveals How Mobile Banking Trojan Hit Nearly 330,000 Android Users via Google AdSense* [online]. Dubai : Kaspersky Lab, 2016 [cit. 2016-11-17]. Dostupné z WWW: <http://newsroom.kaspersky.eu/en/texts/detail/article/kaspersky-lab-reveals-how-mobile-banking-trojan-hit-nearly-330000-android-users-via-google-adsense/?no_cache=1&cHash=bfe4c8cb022ad94a970a484153bca2e8>.

Relay útoky

Tyto útoky jsou vedené na bezkontaktní karty. Bezkontaktní karty mají v sobě zabudovaný NFC čip, díky kterému komunikuji s platebním terminálem. Útok spočívá v tom, že je platební karta „virtuálně přenesena“ a to rovnou k platebnímu terminálu. K útoku jsou zapotřebí dvě osoby a většinou dva chytré telefony a spolehlivé propojení těchto mobilních zařízení. Modelová situace, jeden pachatel přiloží svůj mobilní telefon ke kabelce oběti například v MHD a druhý pachatel bude platit u platebního terminálu za zboží. Telefony budou připojeny na společný server, který je vzájemně propojí a vytvoří tak kopii bezkontaktní karty v telefonu. Telefony si budou přeposílat jednotlivé příkazy, které budou zapotřebí k dokončení platby. Ochrana proti takovému je, že by měl platební terminál mít schopnost rozeznat delší odezvu, která by při přenosu přes internet měla být vyšší. Z pohledu držitele karty spočívá ochrana v nošení speciálního pouzdra nebo nošení více podobných bezkontaktních karet, které se budou navzájem překrývat vydávaným signálem.[56]

3.2.9 Krádež identity

Prvotním cílem není získání platební karty, ale pouze údaje o jejím držitelovi. Při krádeži identity nám nejdříve pachatel odcizí naše osobní údaje a tyto získané údaje mu zajistí neoprávněnou identitu, ze které bude mít nějaký finanční prospěch. Tyto údaje mohou pachateli například umožnit změnu adresy držitele platební karty a na základě změny adresy si nechat vydat novou platební kartu a získat tak kontrolu nad jeho účtem, nebo si pachatel může sjednat úvěr apod. Způsoby jak získat cizí identitu je několik, pokud nebudeme brát v potaz již výše zmíněné možnosti, jako byl phishing, pharming atd.

Jeden ze způsobů, jak získat údaje může být i prohledávání odpadu, v tomto případě se předpokládá, že většina lidí nezničí, neskartuje různé dokumenty, jako jsou výpisy z bank a různá oznámení. Další může být vybírání poštovních schránek, dále s častějším používáním sociálních, kde uživatelé umisťují citlivé informace i zde se mohou najít údaje, které by mohl pachatel využít. I pokud zahodíme účtenku, kde bylo za zboží zaplaceno platební kartou nebo vyplňování různých dotazníků. Způsobů je opravdu několik a měli bychom tedy chránit naše osobní údaje.[57]

[56] *Analýza NFC relay útoku* [online]. Petr Holubec, 2016 [cit. 2016-11-15]. Dostupné z WWW: <http://excel.fit.vutbr.cz/submissions/2016/020/20.pdf>.

[57] *Ztráta identity* [online]. Praha : Národní centrála proti organizovanému zločinu, 2010 [cit. 2016-10-14]. Dostupné z WWW: <http://www.policie.cz/clanek/ztrata-identity.aspx>.

Ochrana před tímto rizikem:

- být obezřetní při sdělování našich osobních údajů,
- chránit své doklady a kontrolovat, jestli máme všechny a v případě ztráty nahlásit tuto skutečnost příslušnému orgánu,
- pokud nám nedochází pravidelná korespondence od banky, je třeba to nahlásit,
- nevyhazovat neskartované dokumenty, účtenky a písemnost, na kterých jsou citlivé údaje,
- kontrolovat pravidelně výpisy z účtů.

3.3 Zhodnocení rizik

Rozšíření čipových karet vedlo ke klesajícímu počtu podvodů u padělaných platebních karet. Na druhé straně zde máme rozšíření bezkontaktních karet, které také přinášejí určitá rizika. Pokud bude odcizena bezkontaktní karta a nedostane se pachateli do rukou kód PIN, tak budou ztráty maximálně v řádech tisíců a některé banky v České republice jsou většinou shovívavé a tyto transakce jsou bez jakékoli spoluúčasti vráceny klientovi. Ovšem pokud se dostane pachatel i ke kódu PIN, tak nejen že ztráty mohou být i několika násobně vyšší, ale zároveň mu ani banky ve většině případů tyto transakce nevyreklamují.

U skimmingových útoků nebo útoků kde jsou získány citlivé údaje o platební kartě bez vědomí držitele je nejhorší, že mohou být ztráty velké a klidně i po několika minutách může být vytvořen padělek karty a může být s kartou zaplaceno někde v zahraničí. Nebo mohou být postupně odčerpávány nižší částky, což může nějakou dobu trvat, než to majitel účtu zaregistruje. Může zde tedy vzniknout určitá prodleva mezi odcizením dat a zneužitím finančních prostředků, proto je také velice těžké zjistit, kde byly data získány. Jak jsme mohli vidět z grafu č. 1, tak skimmingové útoky stále rostou a to zejména díky jejich jednoduchosti.

Objemy transakcí v rámci CNP jsou čím dále větší a s tím roste i počet možných útoků. Co se týká vzniklých škod, tak pokud budou odcizeny údaje pro CNP transakce tedy číslo karty, platnost, jméno držitele a CVV2/CVC2 kód, tak mohou vzniknout ztráty pouze do výše limitu, které jsou nastavené na platební kartě. Většina bank v České republice dnes umožňuje individuální nastavení těchto limitů v internetovém bankovnictví. Výchozí nastavení těchto plateb je většinou v rozmezí mezi 5 až 10 tisíc. Zabránit podvodům v CNP prostředí by měl systém 3D Secure, který jednak vyžaduje ověření pomocí zaslaného SMS kódu a platba proběhne až po jeho zadání, dále platba probíhá mezi nakupujícím a bankou, obchodník nemá žádné data o kartě k dispozici.

3.4 Řízení rizik

Při ztrátě platební karty nebo při podezření, že někdo získal citlivá data o platební kartě, musíme včas zareagovat a učinit tak potřebné kroky, aby se zamezilo finančním ztrátám. Tři základní předpoklady úspěšného řízení rizik jsou:[58]

- **Lidé** – důležité je vytváření útvarů, které se budou zabývat bezpečností a budou spolupracovat na celostátní úrovni a s dalšími peněžními ústavy. V nejlepším případě je spolupráce na mezinárodní úrovni mezi bezpečnostními centrálami platebních systémů. Tyto centrály mají informace ze všech regionů, zemí a bank a tak mohou, poskytnou know-how a nejširší pohled na tuto problematiku.
- **Technologie** – podmínkou pro úspěch veškerých bezpečnostní opatření je práce s online autorizacemi transakcí a následným monitoringem veškerých provedených autorizací a zúčtovaných transakcí a to jak ze strany vydavatele, tak i zúčtovací banky.
- **Spolupráce bank** – kriminalita spojená s platebními kartami je globálním problémem. Globálně zavádějí nová opatření jednotlivé karetní asociace (VISA, MC). Na úrovni států je spolupráce bank řešena součinností bank, obchodníků a policejních útvarů. Existují „migrační vlny" podvodníků mezi zeměmi a právě díky takovéto spolupráci se tyto organizované skupiny pomáhá brzdit nebo zablokovat.

Při ztrátě nebo odcizení ztráty platební karty je nutné co nejdříve nahlásit tuto skutečnost vydavateli a podle okolností popřípadě i policii. Většina podvodných transakcí je prováděna do 20 minut až dvou hodin, kdy ještě stále není platební karta zablokována. Pokud ztratíme hotovost, tak se většinou dostáváme do nesnází a to zejména v zahraničí. U platebních karet tomu tak být nemusí, vydavatelé platebních karet nabízejí vydání náhradní nouzové platební karty a to ve většině zemí. Tato platební karta je omezena kratší dobou platnosti a není opatřena čipem a nelze ji tudíž použít v bankomatech a elektronických platebních terminálů, kde jsou transakce ověřovány pomocí PIN. Karta je použitelná pouze v zahraničí a to po omezenou dobu.[59]

[58] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 245.
[59] PŘÁDKA, M., KALA, J. *Elektronické bankovnictví.* Praha : Computer Press, 2000, s. 26.

4 ZABEZPEČENÍ PLATEBNÍCH KARET

Z právního hlediska platí v České republice *zákon č. 284/2009 Sb., o platebním styku*, který byl schválen parlamentem 22. 7. 2009 a nabyl účinnosti 1. 11. 2009, se zabývá platebními službami, ochranou peněžních prostředků, platebními systémy, pokutami, dohledem nad platebním stykem a dalšími záležitostmi. Další *zákon č. 229/2002 Sb., o finančním arbitrovi*, který také souvisí s touto problematikou, se zabývá mimosoudním řešením sporů, které řeší mezi spotřebiteli a finančními institucemi.[60]

Pokud bude platební karta zneužita, tak dle *§ 209 a § 234 zákona č. 40/2009 Sb., trestního zákoníku* může být pachatel potrestán odnětím svobody na dvě léta až dvanáct let, záleží na okolnostech a vzniklé škodě.[61]

Zabezpečení platebních karet je jejich nezbytnou součástí, mělo by být především zabráněno padělání a neoprávněnému použití. Během vývoje platebních karet byla vynalezena řada bezpečnostních a preventivních opatření. Můžeme je rozdělit na fyzické bezpečnostní prvky, které obsahuje přímo platební karta a měly by zabraňovat padělání a na systémové prvky, které by měly zajistit bezpečné používání platební karty a zabránit neoprávněnému použití. Další způsoby ochrany jsou chápany jako různá připojištění nebo alternativy pro placení na internetu, která nabízejí banky nebo jiné společnosti. Ovšem žádná zabezpečení nikdy nezamezí všem rizikům a tak je snaha alespoň rizika minimalizovat.

4.1 Ochranné systémy platebních karet

4.1.1 Mezinárodní bezpečnostní standardy

Jedním z mezinárodních bezpečnostních standardů je PCI DSS, který byl vyvinut za účelem zvýšení bezpečnosti držitelů platebních karet, respektive údajů o platební kartě. Tyto standardy platí pro všechny subjekty, které se podílejí na zpracování platebních karet a uchovávají, zpracovávají a přenášejí tak citlivá data držitelů platebních karet. Mezi data, která je možné ukládat a to za dodržení standardů PCI DSS patří číslo karty, platnost a jméno držitele. CVV2/CVC2, PIN a data z magnetického proužku nesmí být za žádných okolností ukládána. Ochranou dat se

[60] *Zákon o platebním styku* [online]. Praha : Ministerstvo vnitra ČR, 2017 [cit. 2017-01-15]. Dostupné z WWW:<http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=69225&nr=284~2F2009&rpp=15>.
[61] *Trestní zákoník* [online]. Praha : Ministerstvo vnitra ČR, 2017 [cit. 2017-01-15]. Dostupné z WWW: <https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68040&nr=40~2F2009&rpp=15>.

tedy nezabývají jen vydavatelé platebních karet, ale i třeba jednotliví obchodníci. PCI DSS se skládá z 12 bezpečnostních požadavků:

1. Instalovat a udržovat konfiguraci firewallu za účelem ochrany dat držitelů karet.
2. Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry.
3. Chránit uchovávaná data držitelů karet.
4. Zašifrovat přenos dat držitelů karet po otevřených veřejných sítích.
5. Chránit všechny systémy proti malware a pravidelně aktualizovat antivirový software nebo programy.
6. Vyvíjet a udržovat bezpečné systémy a aplikace.
7. Omezit přístup k datům držitelů karet jen podle oprávněné potřeby.
8. Identifikovat a autentizovat přístup k systémovým komponentám.
9. Omezit fyzický přístup k datům držitelů karet.
10. Sledovat a monitorovat všechny přístupy k síťovým zdrojům a datům držitelů karet.
11. Pravidelně testovat bezpečnostní systémy a procesy.
12. Udržovat politiku zaměřenou na bezpečnost informací pro všechny pracovníky.

Standard PCI DSS stanovuje základní provozní a technické požadavky, které jsou vytvořené pro ochranu dat o platebních kartách. Můžeme tedy říci, že jde o vybudování monitorované bezpečnostní sítě s velmi omezeným přístupem, která bude chránit data držitelů platebních karet.[62]

Další z mezinárodních standardů je EMV, který byl vyvinut především pro boj s rostoucími podvody, padělky a ztracenými nebo ukradenými platebními kartami. Je to celosvětově propojený systém pro čipové karty, který byl ve větší míře postupně zaváděn od roku 2005. Tento standard slouží převážně k boji proti podvodům, ale je využíván bankami ke zlepšování a modernizování jejich platebních produktů a služeb. Díky rozšíření a propojenosti EMV, banky také snížili ztráty, které byly způsobeny tím, že klienti chtěli mít platební karty od jiných kartových společností.[63]

[62] *Odvětví platebních karet, standard bezpečnosti dat* [online]. Praha : Sdružení pro bankovní karty, 2015 [cit. 2017-01-28]. Dostupné z WWW:<http://pcistandard.cz/admin/uploads/PCI_DSS_v3-1_CZ.pdf>.
[63] HADDAD, A. *A New Way To Pay: Creating Competitive Advantage Through The EMV Smart Card Standard.* 2. vyd. Burlington : Gower Pub Co, 2005, s. 2.

4.1.2 Kryptografie

U platebních karet nejde jen o zabezpečení proti padělání nebo pozměňování údajů, ale je třeba také zajistit zabezpečení dat, která se nacházejí v čipu platební karty a zabezpečenou komunikaci, která musí proběhnout, aby mohla být například ověřena pravost platební karty. Tyto komunikační kanály, které zajišťují přenos dat mezi klientem, POS terminálem, bankou, bankomatem a autorizačními centrálami musí probíhat v zabezpečené formě. V předchozí kapitole je zmíněný mezinárodní standard PCI DSS, který také pamatuje na tuto problematiku a to v bodech 3 a 4. Jeden z prvních šifrovacích algoritmů byl DES, který zavedla společnost VISA a velmi rychle toto šifrování začal používat i MasterCard a další kartové společnosti. DES také umožňoval pomocí jeho technologie uživatelskou změnu PIN, který následně zaznamenal na magnetický proužek. S rostoucím výpočetním výkonem počítačů, rostly také nároky na šifrovací metody, ať už ve formě délky nebo jiného algoritmu.[64]

U čipových platebních karet můžeme rozlišovat symetrické a asymetrické metody šifrování. Symetrické šifrování je takové, u kterého se používá pro zašifrování a dešifrování pouze jeden stejný klíč. U asymetrického šifrování jsou použity dva klíče, jeden „veřejný“ a jeden „soukromý“. Soukromý klíč se nikomu nesděluje a nechává si ho osoba nebo organizace, která tuto dvojici klíčů vytvořila. Jedním z těchto klíčů se zpráva zašifruje a druhým, který k němu patří, se dešifruje.[65]

Jedním se současných symetrických šifrovacích sytému je 3DES, který šifruje informací 3x po sobě, třemi různými klíči. 3DES je asi bilionkrát bezpečnější než obyčejný DES. Zařízení, která má k dispozici klíč k dešifrování (platební karty, bankomaty, POS terminály) jsou schopná ověřit platnost kódu PIN přibližně za 100 μsec. RSA je jedním z asymetrických šifrovacích sytému, fungování této metody je založeno na nevratném matematickém vzorci, který umožňuje druhým klíčem dešifrovat zprávu a zároveň neexistuje způsob jak zjistit původní šifrovací klíč. Klíčová jsou zde prvočísla, protože ze součinu prvočísel nelze zjistit, jaká prvočísla byla použita, a potencionální pachatel by musel počítat jedno prvočíslo za druhým.[66] Za zmínku, také stojí, že komunikace mezi terminálem a bezkontaktní kartou probíhá z velké části v nešifrované podobě. U webového rozhraní se používá zabezpečený protokol HTTPS, který zajišťuje asymetrickou šifrovanou komunikaci mezi klientem a serverem.

---

[64] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 234.

[65] *Symmetric vs Asymmetric Encryption* [online]. Florida : JSCAPE, 2015 [cit. 2016-01-30]. Dostupné z WWW: <http://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption>.

[66] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 235.

4.1.3 PIN

Jedna z prvních a nejvíce používaných metod pro ověření právoplatného držitele platební karty byl podpis. S rozvojem čipových karet se stále více začal využívat kód PIN, který měl oproti podpisu několik výhod. Ověření u kódu PIN probíhá automaticky přes autorizační centrum, oproti podpisu, který musel být ověřen prodavačem. Kód PIN přinesl tedy rychlejší platební proces, a také zvýšil jeho bezpečnost. PIN je v zašifrované podobě a oproti podpisu, který se dá do určité míry okopírovat a zfalšovat, aniž by to běžný obchodník poznal, je kód PIN bezpečnější. Kód PIN bychom si určitě neměli nikam zaznamenávat a už vůbec ne v oblasti platební karty, a nikomu jej ani sdělovat. Pokud je platební karta odcizena a pachatel bude zkoušet zadávat kód PIN, tak u většiny českých bank se po třech neúspěšných pokusech karta zablokuje, to dává čas pravoplatnému držiteli platební karty podniknout potřebné kroky. Některé banky zablokují kartu na jeden den a některé do doby, než držitel kontaktuje příslušnou banku. Platební karta může být i zadržena bankomatem po sérii špatných zadání kódu PIN.

Ověření držitele platební karty pomocí kódu PIN probíhá v šifrované podobě a používají se zde veřejné a soukromé klíče. Při vložení platební karty do platebního terminálu se terminál dotazuje na kód PIN, aby ověřil právoplatného držitele. Karta následně vygeneruje náhodně číslo a pošle ho společně se svým veřejným klíčem do terminálu. Terminál následně zašifruje pomocí přijatého veřejného klíče zadaný PIN a přijaté náhodně vygenerované číslo. Platební karta posléze dešifruje pomocí svého soukromého klíče přijatý kód PIN i náhodné číslo a porovná to s bezpečně uloženým kódem PIN a dříve vygenerovaným náhodným číslem. Pokud vše proběhne v pořádku, transakce je potvrzena a úspěšně provedena.[67]

4.1.4 CVV2/CVC2

CVV2 a CVC2 jsou třímístné kódy, které používají karetní asociace VISA a MasterCard a jsou vytištěné na zadní straně platební karty vedle podpisového proužku. Na platební karty byly přidány z důvodu zvýšení bezpečnosti při platbách na internetu. Tyto kódy slouží tedy k CNP transakcím a hlavní úlohou je chránit právoplatného držitele karty před zneužitím platební karty na internetu a to v případech, kdy pachatel nezíská fyzicky platební kartu, ale jen informace o ní. Pokud je platební karta fyzicky odcizena jsou kódy CVV2 a CVC2 k ničemu.

[67] VYCHODIL, J. *Princip a zabezpečení platebních karet*. [online]. Brno : VUT, 2015 [cit. 2016-01-30]. Dostupné z WWW: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/20/princip-a-zabezpeceni-platebnich-karet-1-1-1/>.

4.1.5 3D Secure

Zabezpečení 3D Secure můžeme znát také jako systémy Verified by Visa a MasterCard SecureCode. Jde o zabezpečení internetových plateb a mělo by být zabráněno úniku informací o platební kartě. Podmínkou pro správné používání 3D Secure je, že jí musí využívat jak zákazník, tak i obchodník. Při nákupu zboží nebo služeb prostřednictvím internetu budeme přesměrováni na platební bránu banky, která má smlouvu s e-shopem, na kterém právě nakupujeme a zde zadáme údaje o platební kartě. Vše probíhá v šifrované podobě a jen banka může zadané údaje dešifrovat a přečíst. Po zadání údajů o platební kartě budeme vyzváni k zadání jednorázového kódu, který je zaslán prostřednictvím SMS.

Mezi výhody 3D Secure patří vyšší bezpečnost placení na internetu a to především díky tomu, že údaje o platební kartě má k dispozici pouze banka a ne obchodník. Ovšem jedna ze zásadních nevýhod je nerozšířenost 3D Secure mezi obchodníky. Pokud nám bude odcizena platební karta nebo údaje o platební kartě, tak to, že máme aktivovanou službu 3D Secure nám v současné době nezabezpečí naše finanční prostředky na účtu, protože stačí, když někdo provede nákup u obchodníka, který 3D Secure nevyužívá a dvoufázové zabezpečení je tím pádem k ničemu. Další z nevýhod může být prodloužení platební transakce, které může být na obtíž, zejména u drobných plateb, které potřebujeme rychle zaplatit – např. platba za jízdenku apod.

4.1.6 Biometrické prvky

Pro ověření identity držitele platební karty nemusí sloužit nutně jenom kód PIN. Už i v segmentu platebních karet se můžeme nějaký čas setkat s formou biometrického ověřování. Mezi nejrozšířenější ověřovací biometrickou metodu v oblasti platebních karet patří otisk prstu, jako první tuto metodu ověření spustil MasterCard s platební kartou Zwipe.[68] V České republice se sice s platební kartou MasterCard Zwipe zatím setkat nemůžeme. Pokud ale vlastníme chytrý telefon, který má čtečku otisku prstů a používáme aplikaci MasterPass od MasterCard, díky které můžeme platit namísto platební karty, tak můžeme místo kódu PIN, potvrdit platbu právě přiložením prstu na čtečku. Jedna z výhod ověření pomocí otisku prstu je nezaměnitelnost, otisk prstu je jedinečný a máme ho vždy u sebe a tak nehrozí, že ho zapomeneme, jak se může stát u kódu PIN.

[68] *MasterCard And Zwipe Announce The Launch Of The World's First Biometric Contactless Payment Card With Integrated Fingerprint Sensor* [online]. London, 2014 [cit. 2016-01-31]. Dostupné z WWW: <http://newsroom.mastercard.com/press-releases/mastercard-zwipe-announce-launch-worlds-first-biometric-contactless-payment-card-integrated-fingerprint-sensor/>.

4.2 Fyzická ochrana platebních karet

4.2.1 Hologram

Hologram jako ochranný prvek u platebních karet implementoval jako první MasterCard a to v roce 1983, později se přidaly i další kartové společnosti. Hologramy se postupem času zdokonalovaly a měnily se i vzory. Cílem hologramů je zvýšit zabezpečení platebních karet, ztížit výrobu jejich padělku a umožnit veřejnosti, aby mohla padělky lépe odhalit. Hologramy pro kartové společnosti VISA a MasterCard vyrábí vždy jedna tiskárna cenin. Hologramy se vyrábějí na pásech a každý má své evidenční číslo. Pásy jsou poté dopravovány do několika tiskáren cenin a jsou na platební karty připevňovány metodou Hot Stamping, kdy je speciální polymerní fólie s hologramem zalisovaná na povrch platební karty. Hologram se může nacházet i na magnetickém proužku. Typickým hologramem pro kartovou společnost VISA je letící holubice a pro MasterCard jsou typické dvě propojené zeměkoule a v pozadí nápisy MasterCard.[69]

Obrázek č. 3: Příklady hologramů MasterCard[70]

4.2.2 Podpisový proužek

Podpisový proužek se nachází na zadní straně platebních karet. Slouží, neboli spíše sloužil pro ověřování transakcí, které se prováděly na základě shody podpisového vzoru a podpisu na účtence. V současné době je to v České republice již minulost, ale stále se na platebních kartách nachází a nepodepsaná platební karta je považována za neplatnou. Podpisový proužek je na zvláštním proužku papíru, který je chráněn proti dodatečné změně podtiskem nebo giloší, provedeným barvami, která jsou viditelná v ultrafialovém světle. Tento speciální proužek papíru je velice citlivý na chemikálie, gumování a těmito i dalšími zásahy do struktury papíru má za důsledek vystoupení textu „VOID“, což znamená neplatný. Další ochranný prvek pro ztížení padělání z originální

[69] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 229.

[70] *Card Security Features* [online]. London, 2008 [cit. 2016-02-01]. Dostupné z WWW: <https://www.mastercard.com/ca/wce/PDF/Final_May_27_08_Lay_By_Card.pdf>.

platební karty je tisk části čísla platební karty na podpisový proužek, při padělání bude muset být pozměněno jak číslo karty, tak i jeho část na podpisovém proužku.[71]

4.2.3 Bezpečnostní tisk

Jako další ochrana platebních karet je bezpečnostní tisk. Tisk do povrchu karty a plnobarevný ofset patří mezi nejpoužívanější techniky ceninového bezpečnostního tisku. Mikrotext, ultrafialové prvky, embosování a tisk identifikátoru BIN na platební kartu jsou další kombinace bezpečnostního opatření. Mikrotext je tisk velmi malého textu na vybraných místech a je velmi obtížné ho napodobit, pod mikroskopem nebo lupou je možné spolehlivě ověřit jeho pravost. Ultrafialové prvky a jejich chemické složení zajišťuje světélkování pod ultrafialovými paprsky. V České republice je stále možné se setkat s nově vydanými platebními kartami, které jsou embosované, i když se na českém území setkáme s imprinterem jen těžko. Můžeme to také chápat jako bezpečnostní prvek, u prvně vydávaných platebních karet od kartových společností VISA a MasterCard, obsahovaly karty zvláštní embosovaný znak „M“ u MasterCard a „V“ u VISA. Identifikátor BIN je vytištěn při výrobě karty v tiskárně cenin a díky tomu může banka vydávat jen vlastní karty se svým předčíslím a slouží také jako ochrana před paděláním originální karty. Bezpečnostní tisk ovšem nezabrání padělání, ale spíše ztíží a zvýší náklady na výrobu padělku. To především díky technologiím, které jsou veřejně dostupné.[72]

4.2.4 Číslo karty

Číslo platební karty je jeden ze základních identifikačních prvků. Číslo platební karty tedy není generováno náhodně a má určitý řád a je definováno podle normy ISO/IEC 7812. Všechna čísla platebních karet procházejí přes Luhnův algoritmus, který detekuje náhodné chyby. Číslo může být na platební kartě ve dvou podobách, embosované nebo pouze vytištěné. Platební karty od Mastercard a VISA mají šestnáctimístnou kombinaci čísel. První číslice říká, o jaký sektor se jedná, u číslic 4 a 5 se jedná o bankovní sektor. Prvních šest čísel identifikuje vydavatele platební karty a můžeme podle nich zjistit, o jakou kartovou společnost se jedná a v jaké zemi byla karta vydána. Sedmé až patnácté číslo identifikuje vydavatelskou banku a majitele účtu. Poslední šestnácté číslo je kontrolní číslice.[73]

---

[71] RAK, R., et al. *Biometrie a identita člověka*. Praha : Grada, 2008. s. 82.
[72] RAK, R., et al. *Biometrie a identita člověka*. Praha : Grada, 2008. s. 79.
[73] *Credit Cards* [online]. Seattle : DataGenetics, 2013 [cit. 2016-02-05]. Dostupné z WWW: <http://datagenetics.com/blog/july42013/index.html>.

4.2.5 Čip

Už samotné zavedení čipových karet zvýšilo bezpečnost platebních karet oproti kartám, které měly pouze magnetický proužek. Data na magnetickém proužku totiž nejsou žádným způsobem chráněna, magnetický proužek slouží pouze jako záznamové médium. Pachateli tak stačí získat kopii magnetického proužku, kód PIN a může si vytvořit duplicitní platební kartu. Čip na platebních karetách už ale neslouží pouze jako záznamové médium, ale obsahuje mikropočítač, který má vlastní operační a souborový systém a veškerá komunikace probíhá v zašifrované podobě. V České republice většina bank vydává tzv. hybridní karty, ty mají jak čip, tak i magnetický proužek.[74]

4.2.6 CVV/CVC

CVV/CVC se používá jako ověřovací parametr pro card-present transakce. Oproti CVV2/CVC2 kódům jsou tyto data implementovány do magnetického proužku nebo čipu. Jsou to zašifrovaná data, která jsou vygenerována z čísla platební karty, doby platnosti a servisního kódu karty. Autorizační centrum si tyto data vygeneruje také a ověřuje je v reálném čase při platbě u obchodníka. Pokud jsou shodná, platba probíhá bez problému, pokud odlišná, je platba zamítnuta. Tím, že jsou porovnávány v reálném čase, znamená, že nemusejí být nikde ukládána a zamezí se tak případnému odcizení.[75]

4.3 Další způsoby ochrany platebních karet

4.3.1 Virtuální platební karty

Pro zvýšenou bezpečnost při platbách na internetu můžeme využít virtuální platební karty. Virtuální platební karta může být buďto jednorázově vygenerované číslo nebo může být klientovi vytvořena speciální plastová karta určena pouze pro CNP transakce. Spolu s jednorázově vygenerovaným číslem platební karty je klientovi přidělen také bezpečnostní CVV2/CVC2 kód a expirace, to vše probíhá přes internetové bankovnictví. U vytvořených plastových karet, které jsou určené především pro častější nákupy na internetu, může mít tato karta i vlastní výpis nebo mohou být transakce převáděny na účet hlavní karty. Podobně mohou také posloužit předplacené platební karty nebo platební služby PayPal.[76]

---

[74] VYCHODIL, J. *Princip a zabezpečení platebních karet*. [online]. Brno : VUT, 2015, [cit. 2016-01-30]. Dostupné z WWW: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/20/princip-a-zabezpeceni-platebnich-karet-1-1-1/>.

[75] BHARGAV, A. *PCI Compilance: The Definitive Guide.* Boca Raton : CRC Press, 2015.

[76] JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. s. 240.

4.3.2 Připojištění

Ze zákona o Fondu pojištění vkladů jsou finanční prostředky ve všech bankách pojištěny do výše 100 000 € na jednoho klienta bez jakékoli spoluúčasti v případě zkrachování banky. Dále z právních předpisů vyplývá, že pokud klient neoznámí včas ztrátu nebo odcizení platební karty, tak nese odpovědnost za tyto neautorizované transakce a to do výše 150 €. Za neautorizovanou transakci se považuje transakce, která není provedena oprávněným uživatelem. Pokud vznikne klientovi finanční škoda po oznámení ztráty nebo odcizení, nese odpovědnost poskytovatel. Plnou odpovědnost nese klient tehdy, pokud úmyslně nebo z hrubé nedbalosti porušil některou ze svých povinností, které jsou stanovené poskytovatelem (např. zaznamenání PIN kódu na platební kartu).[77]

Jednotlivé banky nabízí různé druhy připojištění k platebním kartám. Mezi nejčastěji nabízená pojištění patří: cestovní pojištění, pojištění právní ochrany řidičů a pojištění ztráty a krádeže platební karty. Pro příklad pojištění ztráty a krádeže platební karty u Fio banky, a.s. má zpravidla několik variant a liší se především rozsahem pojistné ochrany. U těchto pojištění bychom se měli seznámit se smlouvou, abychom se potom nedivili, že nám banka nechce vyplatit příslušnou částku. Například pojištění se vztahuje i na krádež mobilního telefonu nebo klíčů, ale současně s těmito věcmi musí být odcizena také platební karta. Pokud platební karta odcizena nebude, nemá pojištěný nárok na finanční odškodnění.[78]

4.3.3 Bezpečnostní zásady

Bezpečností zásady můžeme u platebních karet rozdělit do dvou částí. Do první části můžeme zařadit bezpečné využívání internetového bankovnictví a bezpečnost u online plateb. První část je tedy spíše zaměřena na ochranu počítače a telefonu. Druhá část se zabývá bezpečným používáním platební karty.

Bezpečnostní zásady u online nákupů a internetového bankovnictví:[79]

- chránit své přístupové údaje do internetového bankovnictví, nikam si je nezaznamenávat ani je nikomu nesdělovat, nepoužívat jednoduchá hesla,
- nereagovat a neotvírat e-maily od neznámých adresátů,

[77] SCHLOSSBERGER, O. *Platební služby*. Praha : Management Press, 2012. s. 215.
[78] *Pojištění k platebním kartám* [online]. Praha : Fio banka, 2017 [cit. 2016-02-06]. Dostupné z WWW: <https://www.fio.cz/docs/cz/Informace_o_pojisteni_CP_ZDRAVI.pdf>.
[79] KLUFA, F. *Elektronické platební prostředky: Jak se vyhnout rizikům.* Praha : Sdružení českých spotřebitelů, 2013. s. 12.

- chránit svůj mobilní telefon, pokud si necháváme zasílat autorizační SMS, u chytrých telefonů neinstalovat neověřené aplikace, nepůjčovat telefon cizím osobám,
- nepřihlašovat se pomocí prohlížeče na chytrém telefonu do internetového bankovnictví,
- chránit svůj počítač a udržovat aktualizovaný operační systém i prohlížeč, být obezřetný u přihlašování na stránkách internetového bankovnictví,
- u telefonu a notebooků se k internetu přihlašovat jen na nám známých Wi-Fi sítích, v žádném případě se nepřihlašovat na veřejných Wi-Fi sítích,
- nestahovat z internetu neznámé soubory, navštěvovat pouze důvěryhodné a známé webové stránky,
- pro zvýšení bezpečnosti si můžeme nastavit, abychom byli informováni o pohybech na účtu a to formou SMS nebo e-mailem,
- při online nákupech a při přihlašování do internetového bankovnictví používat počítače, které známe a víme, že jsou aktualizované a zabezpečené,
- při nákupech na internetu preferovat prodejce, kteří mají službu 3D Secure,
- nakupovat u ověřených prodejců, velmi snížená cena produktu může znamenat podvodný e-shop,
- pokud nám to banka umožnuje, tak pracovat s peněžními limity na platební kartě, při plánovaném nákupu na internetu limity navýšit a poté snížit na nulu.

Bezpečnostní zásady při používání platební karty:[80]

- mít přehled o platební kartě a používat ji v souladu s podmínkami vydavatele,
- pravidelně kontrolovat výpisy z účtu,
- při zadávání kódu PIN si zakrýt klávesnici,
- nikdy nikomu nepůjčovat platební kartu ani nesdělovat kód PIN,
- nikdy nezaznamenávat PIN kód v blízkosti platební karty,
- ztrátu platební karty oznámit co nejdříve,
- být maximálně obezřetní u obchodníka, u kterého nakupujeme, zejména pak v zahraničí,
- být obezřetný při výběru z bankomatu,
- platební karty poškozují nejen mechanické vlivy, ale také velmi nízká nebo vysoká teplota, elektromagnetická pole.

[80] KLUFA, F. *Elektronické platební prostředky: Jak se vyhnout rizikům.* Praha : Sdružení českých spotřebitelů, 2013. s. 14.

5 VYHODNOCENÍ DOTAZNÍKOVÉHO ŠETŘENÍ

Hlavním cílem bylo na základě dotazníkového šetření zjistit, jak lidé, kteří jsou držiteli platebních karet, vnímají rizika, která jsou s nimi spojená a jestli vědí, jak se proti nim chránit nebo jak jim předcházet. Dotazník obsahoval celkem 20 otázek, z toho 4 polouzavřené. Dotazník byl umístěn na webový portál https://www.vyplnto.cz/databaze-dotazniku/bezpecnost-a-rizika-platebni/ od 17. února 2017 do 3. března 2017. Dotazník vyplnilo celkem 165 respondentů (blíže viz kapitola 1).

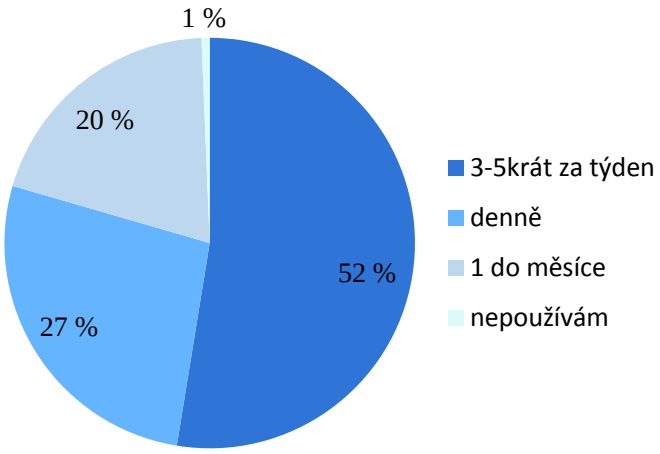
Otázka č. 1: Jste držitelem platební karty?

Bankovní služby a produkty využívá drtivá většina obyvatel ČR, nejčastěji využívaným bankovním produktem je běžný účet. Platební karty jsou až na druhém místě. Převážná většina dotázaných, tj. 95 %, jsou držiteli platební karty. Důvod je jednoduchý, bezhotovostní platební styk přináší značné urychlení a je pohodlný. Platebních terminálů je v České republice velké množství a tak není problém uskutečňovat bezhotovostní platební styk. Ti, kteří odpověděli, že nepoužívají platební karty, už dále dotazník nevyplňovali – 9 (5 %) respondentů. Ve zbylém vyhodnocení dotazníkové šetření bude bráno v potaz pouze oněch 95 %, tj. 156 respondentů.

Otázka č. 2: Jak často platební kartu používáte?

Zhruba polovina dotázaných používá platební kartu 3-5 krát za týden. 27 % používá platební kartu alespoň každý den a 20 % ji používá pouze jednou do měsíce. Pouze 1 z respondentů označil odpověď – nepoužívám platební kartu. Jak bylo zmíněno výše, platebních terminálů je dostatek a tak není důvod nevyužívat platební karty. Platební karty se staly nástrojem pro běžný platební styk. Platit můžeme za jízdenky v autobusech, u obchodníků, v restauračních zařízeních, na internetu. Způsobů jak využít platební kartu je v dnešní době opravdu několik, ovšem je potřeba abychom byly při platbách a při manipulaci s kartou obezřetní.

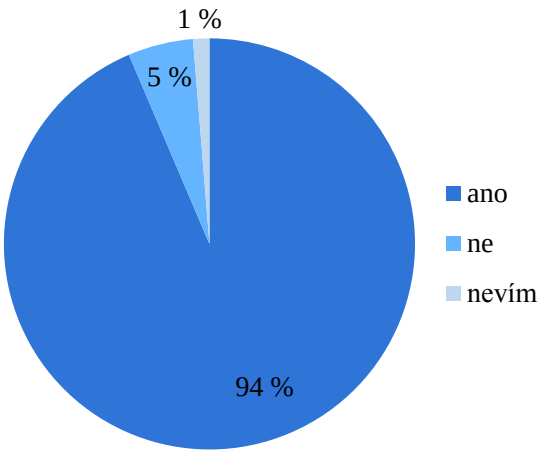
Graf č. 4: Jak často používáte platební kartu[81]



Otázka č. 3: Je vaše platební karta bezkontaktní?

Pouze 5 % respondentů uvedlo, že nemají bezkontaktní platební kartu. Bezkontaktní kartou disponuje 94 % dotázaných, zbytek uvedl, že neví, jestli mají bezkontaktní platební kartu. Banky v České republice za nátlaku karetních asociací vydávají v drtivé většině pouze bezkontaktní platební karty. Důvod je jednoduchý – vyrábět pouze jeden druh karet je snazší a levnější. Spousta platebních terminálu v ČR podporuje bezkontaktní platby a tak není důvod proč je neupřednostňovat. Na druhou stranu by měl mít klient banky možnost volby, ať už například z toho důvodu, že je možné provést neautorizované transakce.

Graf č. 5: Je vše platební karta bezkontaktní[82]



[81] Vlastní zpracování.
[82] Vlastní zpracování.

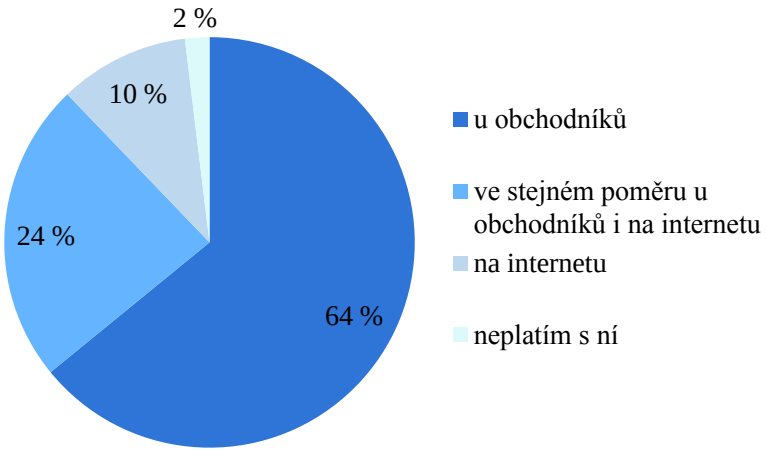
Otázka č. 4: Víte, jaké máte nastavené limity na platební kartě?

Většina bank v České republice umožňuje změnit limity na platební kartě pomocí internetového bankovnictví. Každá banka má určité základní limity, které nastavuje u svých nově vydaných platebních karet. Na platební kartě je několik limitů, které by měl její držitel znát – limit pro platbu u obchodníka, limit pro výběr z bankomatu, limit u MO/TO plateb a limit pro platby na internetu. Tyto limity mohou také být buďto denní nebo týdenní. 13 % respondentů nevědělo, jaké mají nastavené limity. Pokud někdo neví, jaké má nastavené limity na platební kartě, tak se dá předpokládat, že s limity ani nemanipuluje. A to je veliká škoda, protože je to jedno ze základních preventivních opatření proti zneužití platební karty. Pokud neplatíme na internetu, tak je zbytečné mít nastavený vysoký limit pro platbu na internetu, můžeme tak zamezit případnému zneužití našich finančních prostředků. V ideálním případě je nejlepší operovat s limity pokaždé, když budeme například chtít nakoupit na internetu. Nejdříve zvýšit limit a poté zase stáhnout na nulu. To samé platí i pro platby u obchodníků, je zbytečné mít nastavený denní limit čtyřicet tisíc, když platíme pouze malé částky. Zbytek dotázaných tj. 87 % odpovědělo, že znají své limity na platební karty. To ovšem neznamená, že pracují s limity na platební kartě, ale je zde větší předpoklad, že ano.

Otázka č. 5: Kde s platební kartou převážně platíte?

Platební karty se stále nejvíce používají k platbám u obchodníků, to dokazuje fakt, že takto odpovědělo 64 % respondentů. 24 % dotázaných uvedlo, že platí stejně na internetu i u obchodníků, 10 % platí převážně na internetu a zbylé 2 % uvedli, že s platební kartou neplatí vůbec. Na internetu se každým rokem v České republice utratí stále více peněz, a tak je pravděpodobné, že lidé budou využívat postupem času převážně platby na internetu. V dnešní době je možné nakoupit na internetu opravdu nepřeberné množství produktů a služeb. Existují i „online supermarkety“, ve kterých můžeme zakoupit potraviny, a nemusíme tak trávit hodiny v obchodních jednotkách. Tyto „online supermarkety“ nemusejí mít žádnou prodejnu, ale stačí jim pouze výdejní místo, takto mohou ušetřit náklady. Problémem je, že zatím tyto online obchody fungují pouze ve velkých městech. Na druhé straně někdo může mít nakupování v obchodních jednotkách jako zálibu, někteří si zase chtějí zboží před nákupem vyzkoušet, to platí zejména u oblečení, atd.

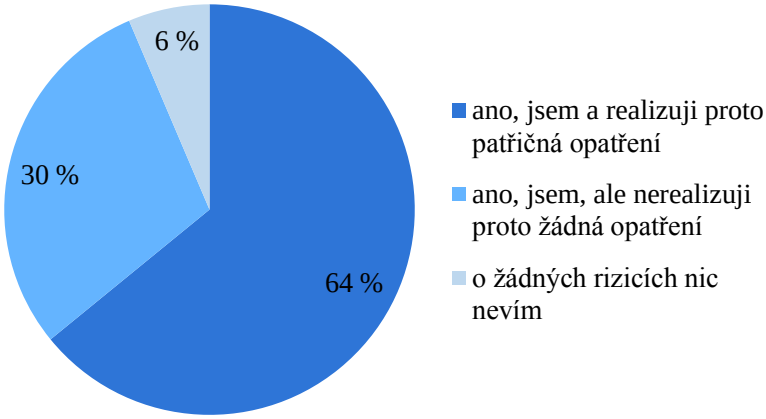
Graf č. 6: Kde s platební kartou převážně platíte[83]



Otázka č. 6: Jste si vědom/a rizik, která jsou spojena s používáním platební karty?

Většina dotázaných si uvědomuje rizika spojená s používáním platební karty, ale pouze 64 % z nich realizuje patřičná opatření. 30 % respondentů si je vědomo rizik, ale žádná opatření nerealizují a 6 % o žádných rizicích nic neví. Banky by měly své klienty více podněcovat, aby se chránili proti případným rizikům a snažit se je stále informovat o nových rizicích, která jsou spojená s používáním platebních karet. Je to samozřejmě v zájmu bank, aby se jejich klienti snažili předcházet případným rizikům. Ovšem někteří klienti nedbají těchto výzev a mohou si tak zbytečné způsobit vlastní nedbalostí finanční ztrátu.

Graf č. 7: Jste si vědom/a rizik, která jsou spojena s používáním platební karty[84]

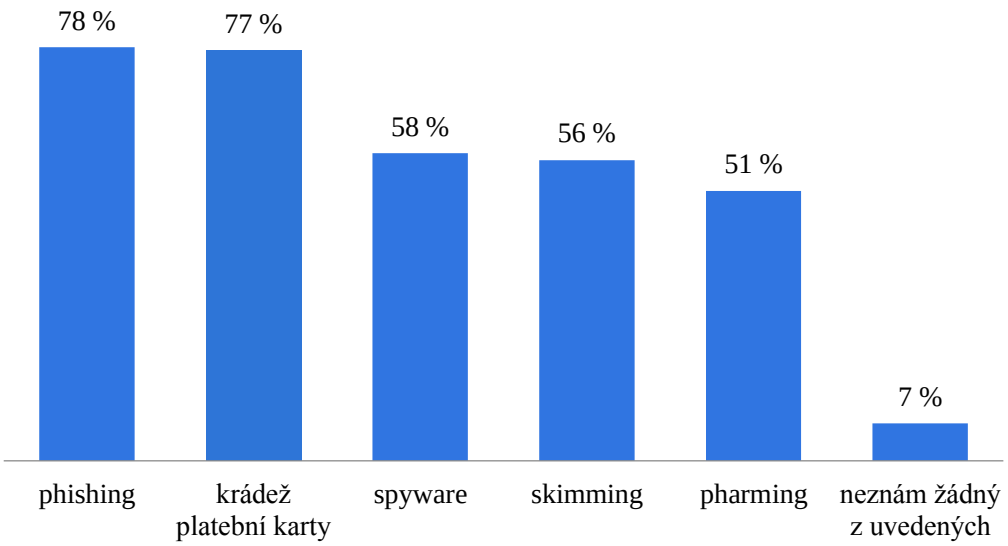


[83] Vlastní zpracování.
[84] Vlastní zpracování.

Otázka č. 7: Zaškrtněte typ/y útoků, které znáte nebo jste se s nimi setkal/a:

U této otázky bylo možné zaškrtnout více odpovědí, mezi nejznámější typy útoků patří podle respondentů phishing a krádež platební karty. Na třetím a čtvrtém místě se s podobným počtem odpovědí umístili spyware a skimming. Pátou pozici obsadil pharming. Pouze 11 respondentů tj. 7 % uvedlo, že neznají žádný z uvedených. To, že lidé nejvíce znají phishing je dáno nejspíše tím, že v posledních letech banky velice intenzivně upozorňují na tento útok a je to také jeden z nejčastějších útoků na klienty bank. Krádež platební karty je logicky domyslitelné riziko platební karty, tak není divu, že je to také jedna z nejčastějších odpovědí.

Graf č. 8: Zaškrtněte typ/y útoků, které znáte nebo jste se s nimi setkal/a[85]

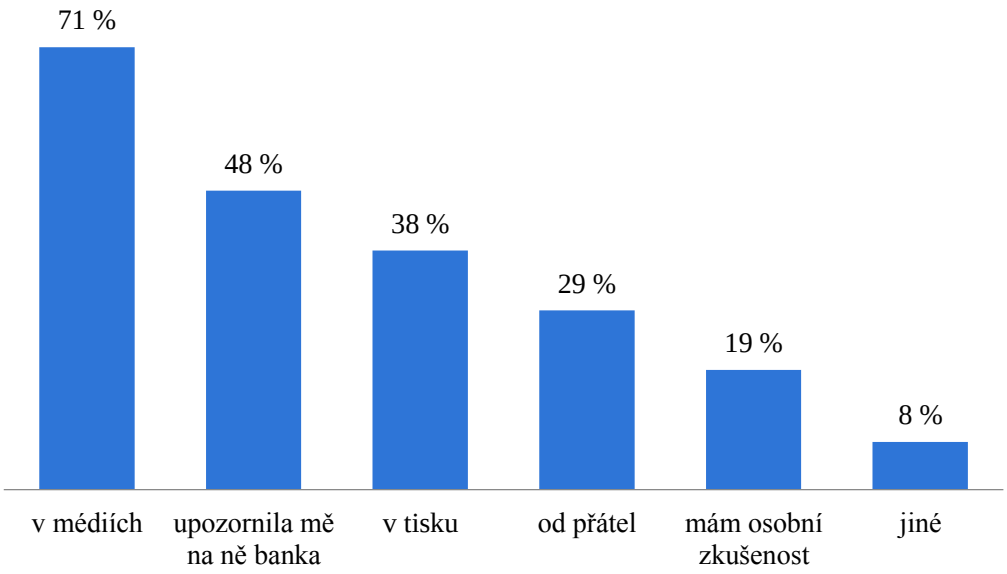


Otázka č. 8: Odkud znáte tyto útoky nebo kde jste se s nimi setkali?

V této otázce bylo opět možné označit více odpovědí. Nejčastěji se respondenti dozvěděli o útocích v médiích, tuto odpověď označilo 71 % z nich. Jako další důležitý zdroj informací byla banka, tu uvedlo 48 % respondentů. Tisk označilo 38 % respondentů a 29 % se o útocích na platební karty dozvědělo od přátel. Osobní zkušenost má 19 % dotázaných. Toto byla jedna z polouzavřených otázek a mohl zde být uveden i jiný zdroj informací, tuto možnost zvolilo 8 % respondentů, nejčastějšími odpověďmi byly, že se o útocích dozvěděli z internetu, ze školy a ze zaměstnání.

[85] Vlastní zpracování.

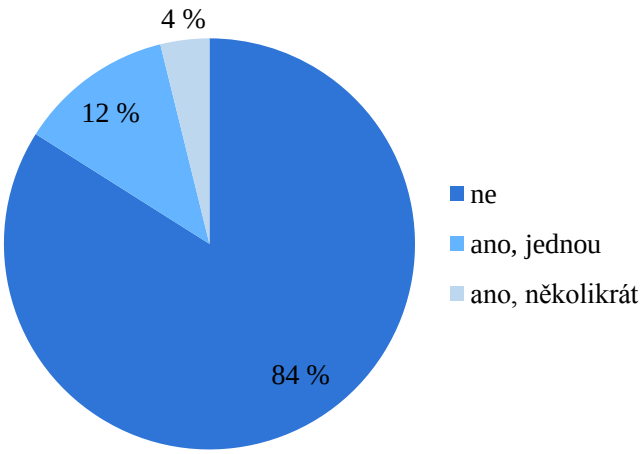
Graf č. 9: Odkud znáte tyto útoky nebo kde jste se s nimi setkali[86]



Otázka č. 9: Byla Vaše platební karta nebo ve vašem blízkém okolí někdy zneužita?

Se zneužitím platební karty se setkalo celkem 12 % dotázaných a z toho 4 % více než jednou. Více než tři čtvrtiny tj. 84 % dotázaných se nikdy nesetkala se zneužitím platební karty. 16 % je celkem vysoké číslo v této oblasti a poukazuje to na to, že bychom měli být při používání platebních karet obezřetní. Banky by se měli v této oblasti stále více angažovat a varovat tak své klienty. Není to ovšem jen o bankách, ale také samotných klientech, nicméně nikdy nebude nulové procento zneužití.

Graf č. 10: Byla Vaše platební karta nebo ve vašem blízkém okolí někdy zneužita[87]



[86] Vlastní zpracování.
[87] Vlastní zpracování.

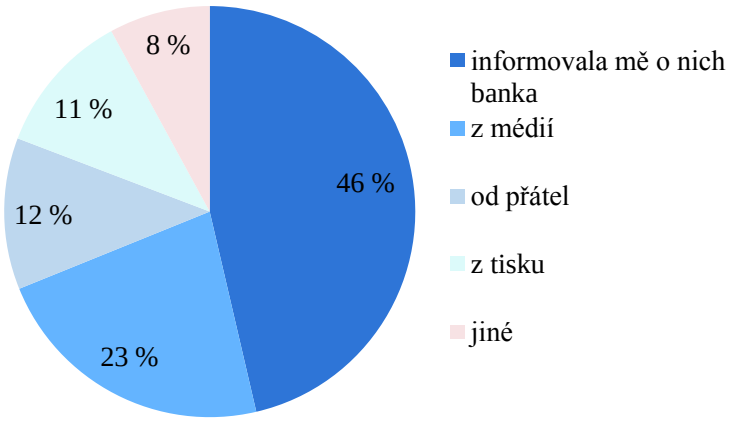
Otázka č. 10: Máte dostatek informací o možnostech ochrany platebních karet?

Více než polovina respondentů – 59 % odpověděla, že mají dostatečné informace o ochranně platebních karet. 41 % dotázaných uvedlo, že nemají dostatečné informace. Informace o ochranně platebních karet by měly přicházet zejména ze strany banky. Banka by měla průběžně informovat o možnostech, které může svému klientovi nabídnout. Ten kdo uvedl, že nemá dostatečné informace, tak to nutně neznamená, že informace od banky nedostal. Někteří klienti nemusejí informacím od banky přikládat velkou váhu anebo je také možné, že tyto informace ani nečtou, nepřikládají jim pozornost.

Otázka č. 11: Odkud máte tyto informace?

Na tuto otázku odpovídali pouze ti, kteří v předchozí otázce odpověděli ano. Celkem se jednalo o 92 respondentů. Téměř polovina z nich (46 %) má informace o možnostech ochrany platební karty přímo od banky, 23 % má informace z médií a 12 % od svých přátel. 11 % dotázaných má tyto informace z tisku. Jelikož toto byla druhá ze čtyř polouzavřených otázek, respondenti zde mohli dopsat i jiný zdroj informací. Mezi jinými zdroji informací respondenti uváděli zdroje jako internet, literatura, vlastní zkušenost. To že většina respondentů má informace primárně od banky je dobrou zprávou. Hlavně z toho důvodu, že informace, které poskytují banky, můžeme považovat jako spolehlivý zdroj informací, kterému můžeme důvěřovat. Informace z jiných zdrojů nemusí být tak přesné jako ty od banky, mohou být zkreslené nebo i nepravdivé.

Graf č. 11: Odkud máte tyto informace[88]

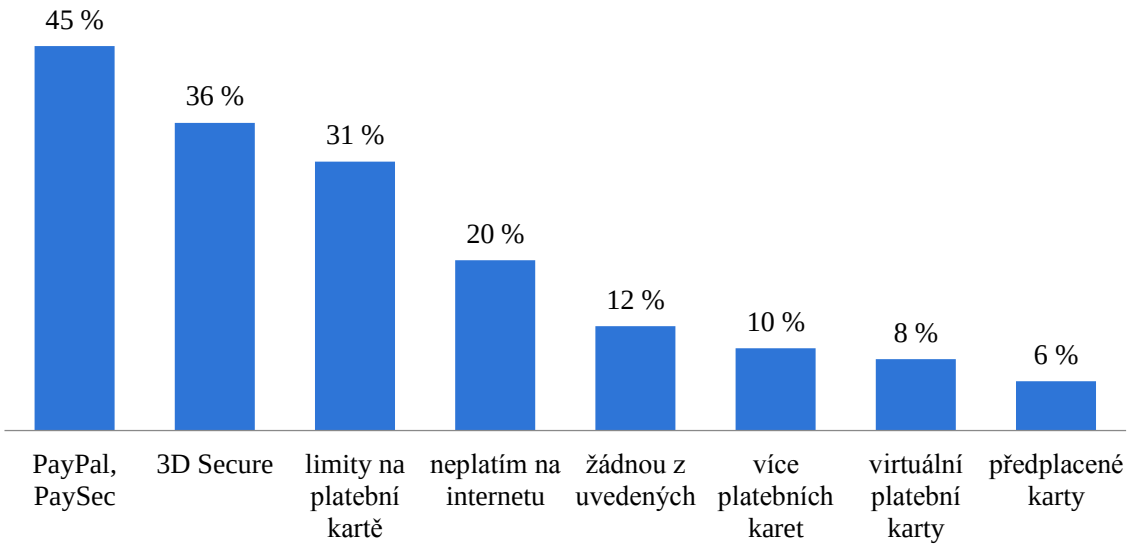


[88] Vlastní zpracování.

Otázka č. 12: Využíváte při platbách na internetu některé z těchto ochran?

U této otázky bylo možné zaškrtnout více odpovědí, to z důvodu, že je možné některé ochranné prvky kombinovat. Nejvíce používanou ochranou pro platby na internetu je zprostředkování platby pomocí – PayPal nebo PaySec, tu označilo 45 % respondentů. Zprostředkování pomocí těchto služeb funguje tak, že si u nich založíme účet a posíláme si na něj peněžní prostředky z našeho účtu. Následně můžeme platit u obchodníků z tohoto účtu a nemusíme tak nikde vkládat naše údaje o platební kartě. Ovšem všichni prodejci tuto službu nemusí podporovat, jeden z důvodu může být výše poplatků, které si např. PayPal nárokuje z částky. 36 % respondentů preferuje obchodníka, který používá službu 3D Secure. Největším problémem 3D Secure je jeho nerozšířenost mezi obchodníky. Třetí nejpoužívanější metoda je práce s limity na platební kartě, označilo ji 31 % respondentů. Jedná se vlastně o jednu ze základních ochran, kterou může držitel platební karty realizovat. Část respondentů (20 %) nevyužívá vůbec internetové platby. 12 % dotázaných nevyužívá žádnou z uvedených ochran při platbách na internetu. Je možné, že využívají nějaké jiné možnosti, jak se chránit anebo nepoužívají vůbec žádná bezpečnostní opatření. Pokud někdo nevyužívá žádná opatření, vystavuje se tak zbytečnému riziku. Více platebních karet využívá 10 % dotázaných, virtuální platební karty využívá 8 % respondentů a předplacené karty 6 %. Problém virtuálních platebních karet je ten, že některé banky nemají tento produkt v nabídce. Předplacené platební karty jsou jako běžné platební karty, ale nejsou vázány na žádný účet. Na kartě je jen tolik finančních prostředků, kolik si tam její držitel pošle.

Graf č. 12: Využíváte při platbách na internetu některé z těchto ochran[89]

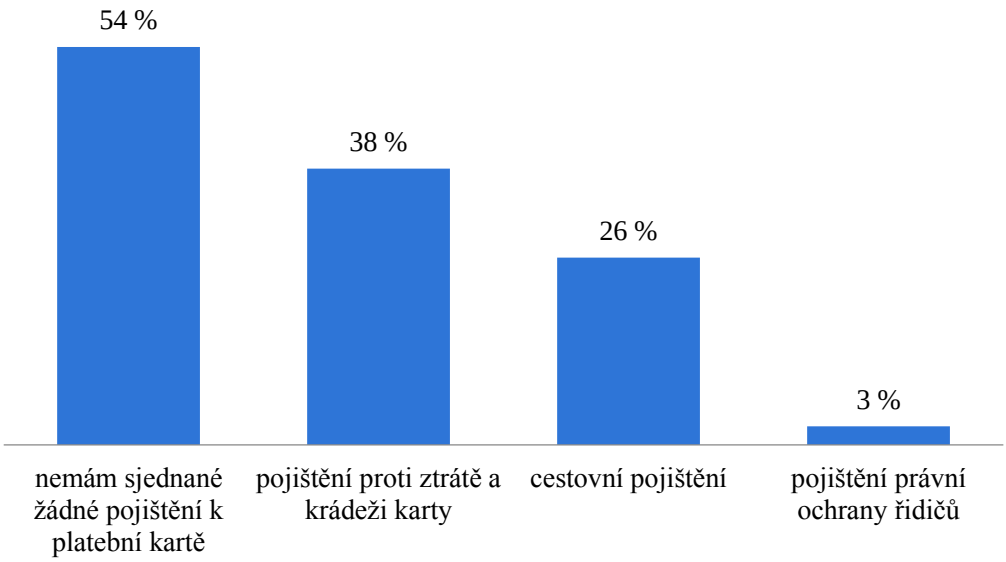


[89] Vlastní zpracování.

Otázka č. 13: Zaškrtněte pojištění, která máte sjednaná k platební kartě…

K platební kartě je možné si sjednat zpravidla tři druhy pojištění. V této otázce bylo opět možné označit více odpovědí. Nejčastěji sjednané pojištění je proti ztrátě a krádeži platební karty, tuto odpověď označilo 38 % dotazovaných. Cestovní pojištění označilo 26 % respondentů a 3 % označilo pojištění právní ochrany řidičů. 54 % dotázaných tedy nemá sjednané žádné pojištění. Důvodů může být několik, buďto neinformovanost o tom, že banky nějaké pojištění nabízí, druhý důvod může být nízké limity plnění nebo se pojištění nemusí vztahovat na vše, například u cestovního pojištění.

Graf č. 13: Zaškrtněte pojištění, která máte sjednaná k platební kartě[90]



Otázka č. 14: Používáte internetové bankovnictví?

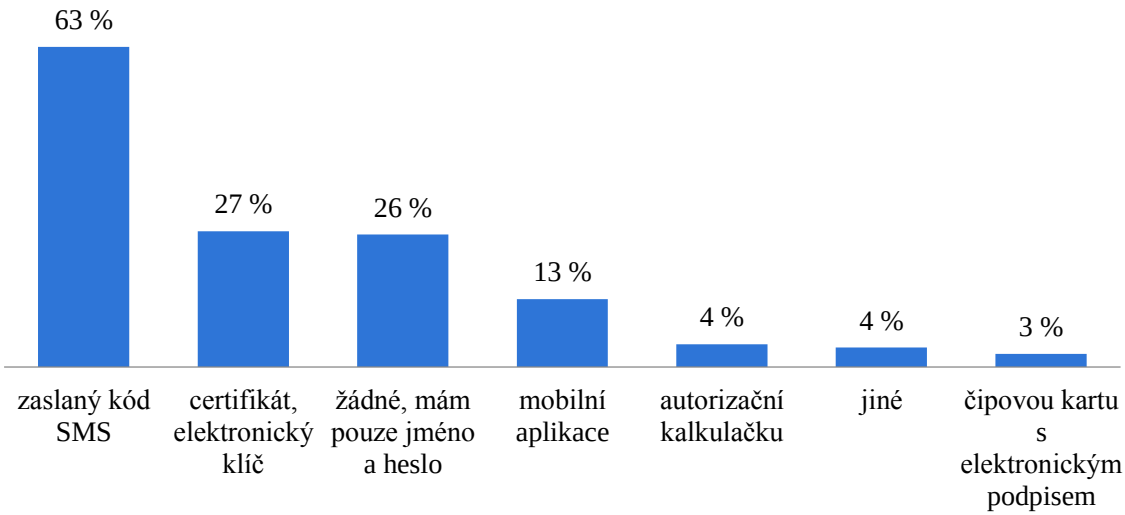
Internetové bankovnictví využívá 95 % respondentů. Používání internetového bankovnictví je dáno především jeho dostupností a snadného ovládání. Je to nejjednodušší způsob jak může klient banky spravovat své bankovní účty a kontrolovat své finance. 5 % respondentů odpovědělo, že nevyužívá internetové bankovnictví. Můžeme jen předpokládat proč tomu tak je, důvodů může být několik. Někdo může raději upřednostňovat osobní kontakt, někdo může používat jiné způsoby komunikace se svou bankou a někdo může mít nedůvěru v internetové bankovnictví, z hlediska jeho zabezpečenosti.

[90] Vlastní zpracování.

Otázka č. 15: Jaké používáte při přihlašování autorizační metody?

Na tuto otázku odpovídali pouze respondenti, kteří v minulé otázce potvrdili, že používají internetové bankovnictví. U této otázky bylo možné označit více odpovědí, jelikož je možné využívat kombinaci autorizačních metod. Nejčastější autorizační metodou je zaslaný kód pomocí SMS, dalo se to předpokládat, jelikož je to jedna z nečastějších metod, které banky nabízejí. Druhá, nejvíce označená odpověď respondenty byla, že využívají certifikát nebo elektronický klič. Certifikát je soubor, který slouží jako ověření totožnosti a klient se s ním prokazuje při elektronické komunikaci s bankou, elektronický klíč funguje na podobném principu. 26 % dotazovaných nepoužívá žádné autorizační metody. Pokud má někdo dostatečné silné heslo, tak je to dostačující metoda, ale dvoufaktorové ověření bude vždy bezpečnější. S rozvojem chytrých mobilních telefonů mohly také banky začít vyvíjet své bankovní aplikace. Pomocí těchto aplikací nám může být zaslán ověřovací kód, který zadáme při přihlašování do internetového bankovnictví, tuto metodu využívá 13 % dotázaných. Zbylé autorizační metody nejsou mezi klienty příliš rozšířené a tak není divu, že je používá pouze zlomek dotázaných. Tyto autorizační metody jako je autorizační kalkulačka a čipová karta s elektronickým podpisem nabízejí pouze některé banky v České republice. Tyto autorizační metody také většinou vyžadují ze strany klienta banky finanční náklady na pořízení těchto přístrojů. Ten kdo používá jiné metody autorizace, je zde mohl dopsat, toto byla jedna z polouzavřených otázek. 4 % respondentů využilo tuto možnost a nejčastější odpověď byla, že požívají jako autorizační metodu otisk prstu.

Graf č. 14: Jaké používáte při přihlašování autorizační metody[91]

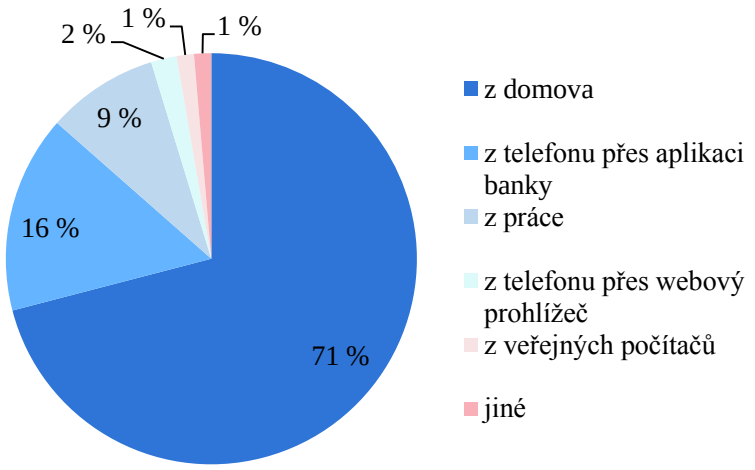


[91] Vlastní zpracování.

Otázka č. 16: Odkud se převážně přihlašujete do internetového bankovnictví?

Tato otázka byla také určena pro respondenty, kteří používají internetové bankovnictví. Většina z nich, tj. 71 %, se do internetového bankovnictví přihlašuje z domova. Z hlediska bezpečnosti je toto nejlepší volbou, to ovšem platí za předpokladu, pokud máme aktualizovaný prohlížeč, operační systém a používáme kvalitní antivirový program. Druhá, ale už ne tak početná část 16 % respondentů, se přihlašuje pomocí aplikace vydané bankou. Tyto aplikace jsou poměrně novou záležitostí oproti klasickému přihlašování do internetového bankovnictví na počítači a zatím nejsou tak rozšířené. 9 % se přihlašuje z práce a zbylí respondenti využívají k přihlášení veřejné počítače a webový prohlížeč v telefonu. Naštěstí z veřejných počítačů a přes webový prohlížeč v telefonu se přihlašuje pouze minimum z dotázaných, při tomto způsobu přihlašování se vystavují zbytečné velkému riziku.

Graf č. 15: Odkud se převážně přihlašujete do internetového bankovnictví[92]



Otázka č. 17: Máte nastavené notifikace o pohybech na účtu, SMS zprávou nebo e-mailem?

Pouze 37 % respondentů má nastavené notifikace o pohybech na účtu. Tato jednoduchá notifikace dokáže zabránit případnému zneužití finančních prostředků. Díky tomu můžeme například včas stornovat podezřelou platbu u banky. SMS zpráva bývá zpoplatněna a tak je možné, že právě díky tomu spousta klientů tuto službu nevyužívá. 63 % dotazovaných uvedlo, že nevyužívá tyto notifikace, nicméně zasílání pomocí e-mailu není nijak zpoplatněno a je možné, že někteří klienti o této službě vůbec nevědí.

[92] Vlastní zpracování.

Otázka č. 18: Platíte mobilním telefonem (NFC)?

Jen 8 % z respondentů používá mobilní telefon jako platební kartu. Banky nabízejí v současnosti také NFC štítky, pomocí kterých se dá také platit. Placení mobilním telefonem přináší určité výhody, může přinést jednak další způsob ověřování majitele pomocí otisku prstu, telefon musí samozřejmě mít senzor otisku prstu. Další výhoda může být ta, že platební kartu nemusíme mít u sebe a odpadá tak riziko způsobené ztrátou nebo krádeži platební karty. Většina respondentů – 92 % tuto možnost placení nevyužívá. Je možné, že je to způsobeno tím, že je to relativně nová metoda placení a nedostala se tak do povědomí všech. Může to být také tím, že ne každý má mobilní telefon s NFC technologií.

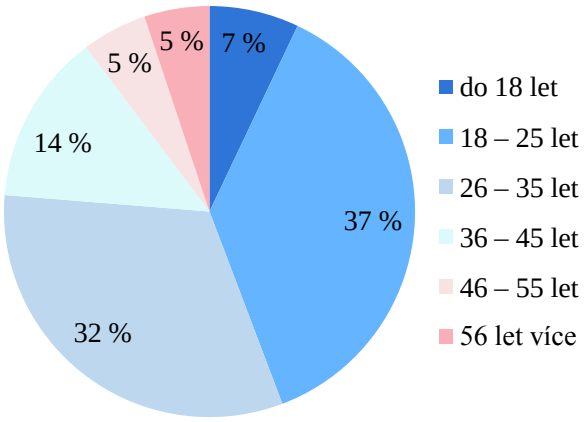
Otázka č. 19: Jaké je Vaše pohlaví?

Předposlední otázka byla zaměřena na demografický výzkum. Složení bylo následovné – 56 % byly ženy a 44 % byli muži. Můžeme tedy říci, že zastoupení žen a mužů, bylo vcelku vyrovnané.

Otázka č. 20: Do jaké věkové kategorie patříte?

Nejvíce respondentů (37 %) bylo ve věku mezi 18 – 25 lety. Druhá nejvíce zastoupená věková skupina byla mezi 26 – 35 lety, ta tvořila 32 % podíl ze všech respondentů. 14 % dotázaných bylo ve věku 36 – 45 let, 7 % ve věku do 18 let. Po 5 % procentech byli zastoupeni věkové kategorie 46 – 55 let a 56 let a více.

Graf č. 16: Do jaké věkové kategorie patříte[93]



[93] Vlastní zpracování.

ZÁVĚR

Hlavním cílem bakalářské práce je zanalyzovat současná rizika a identifikovat typy útoků na platební karty. V rámci vedlejšího cíle bylo provedeno zhodnocení bezpečnostních prvků, pojištění a další způsobů ochrany platebních karet.

Platební karty se od samého počátků jejich existence potýkají s riziky, stejně jako bankovky, mince a další ceniny. Karetní asociace se snaží tyto rizika eliminovat a vynakládají na to nemalé peněžní prostředky. Ovšem pachatelé jsou mnohdy o krok napřed a není to tak jednoduchý boj. Samozřejmě, že by bylo možné vymyslet taková opatření, aby bylo minimum zneužitých platebních karet, jenomže to by používání platebních kartě bylo natolik složité a zdlouhavé, že by lidé raději platili hotově. To samozřejmě karetní asociace a banky nechtějí a tak se musí smířit s určitým procentem zneužitých platebních karet. Odkud pachatelé získávají potřebná data, je také velice těžké určit. Způsobu je několik a většinou se jedná o organizované zločinecké skupiny.

Nejvíce se zneužité platební karty využívají v CNP prostředí, a to především díky větší anonymitě a jednoduchosti pro pachatele. Tomu by měl ovšem zabránit systém 3D Secure. Tento systém, ale spíše chrání jen samotné obchodníky, aby nepřijali platby kradenou platební kartou. Zákazníka to chrání jen ve smyslu, že daný obchodník by neměl mít přístup k údajům o platební kartě, a je zde tedy snížené riziko podvodu ze strany obchodníka. Ovšem pokud se bude jednat o podvodný internetový obchod, tak ten určitě nebude využívat službu 3D Secure. Aby byl tedy tento systém 3D Secure plně použitelný, museli by ho používat povinně všichni internetoví obchodníci anebo by musel mít držitel platební karty možnost nastavit, že lze s platební kartou platit pouze u obchodníků se službou 3D Secure. V současné době tento systém nic neřeší a vyvolává spíše falešný pocit bezpečí. Další bezpečnostní prvek, který měl více ochránit platební karty v CNP prostředí je CVV2/CVC2 kód. Ten se začal používat na přelomu tisíciletí a má jednu zásadní chybu. Při ztrátě nebo krádeži platební karty má pachatel tento kód automaticky také k dispozici. Podle názoru autora by tento kód splnil lépe svůj účel, kdyby nebyl umístěn přímo na platební kartě. Jediný důvod, který autora napadá, proč je tento kód umístěn na platební kartě, je ten, aby věděli držitelé platebních karet kde tento kód hledat. Jako jeden z dalších bezpečnostních prvků současné doby, můžeme považovat bezkontaktní platební karty. Zde je hlavního výhoda v tom, že není nutný přímý kontakt s platebním terminálem nebo bankomatem a vše probíhá

v bezkontaktní podobě. Tímto způsobem můžeme eliminovat různá skimmovací zařízení. Ovšem tento způsob plateb s sebou přinesl i další možná rizika. Zatímco se vyřadila možnost současných skimmovacích útoků, objevili se nové druhy útoků, např. relay útoky nebo zachycení přenosu dat, kdy za pomocí různých zesilovačů a dalších zařízení je možné prodloužit komunikační vzdálenost mezi kartou a platebním terminálem a zachytit tak potřebná data (ve své podstatě je to skimming, ale v modernější podobě). Dalším současným trendem v bezpečnosti je využívání biometrických údajů. Například ověření držitele pomocí otisku prstu je velice spolehlivá metoda autorizace. Tento způsob autorizace by mohl v budoucnosti úplně nahradit zadávání kódu PIN, je zde také velký potenciál, propojení platební karty s chytrým telefonem, který má čtečku otisku prstů. Mimochodem platební karty s biometrickým ověřením již existují, ale jsou jen ve fázi testování. Dalším trendem a asi v současné době nejpoužívanějším způsobem ochrany platebních karet je používání zprostředkovatelských služeb pro platby na internetu např. PayPal. To nicméně potvrdil i samotný výzkum, kdy se tato metoda ochrany platebních karet umístila na prvním místě. Výhodou je, že obchodník, u kterého nakupujeme, nemá žádné informace o naší platební kartě a riziko zneužití obchodníkem je tedy nulové. Problém nastane tehdy, pokud někdo získá přihlašovací údaje do našeho PayPal účtu. Pokud se tak stane, může vesele platit na internetu a pokud je PayPal propojený s platební kartou, můžou zde vzniknout značné finanční škody. PayPal také není v českých internetových obchodech příliš rozšířený, oblibě se těší zejména v zahraničí.

Způsobu jak chránit platební karty je opravdu několik, ovšem každá z metod má většinou nějaké nedostatky. Každý držitel platební si musí vybrat sám, co bude preferovat, nejlepší je ovšem kombinovat více ochranných metod. Nicméně když karetní asociace zavádějí nebo vymýšlejí nové bezpečnostní prvky, musejí brát v potaz určitou zpětnou kompatibilitu se současným zařízením. Jen těžko si lze představit, že by každý rok museli obchodníci nahrazovat své platební terminály za nové. I to může být jeden z důvodů „nedokonalých“ bezpečnostních prvků.

Z realizovaného dotazníkové šetření vyplývá, že velká část respondentů používá platební karty, ty jsou v dnešní době velice dostupné a získat je není problém. Dále z dotazníku vyplynulo, že 94 % dotázaných si uvědomuje rizika spojená s používáním platebních karet. Ovšem jen 68 % z těchto dotázaných realizuje alespoň nějaká opatření, aby zabránili těmto rizikům. Pokud někdo nevnímá rizika nebo nerealizuje alespoň nějaká opatření, vystavuje se zbytečnému riziku. Vzhledem k tomu, že se v dnešní době komunikuje s bankou především v elektronické formě, mají útočníci spousty příležitostí

a metod k tomu jak získat od takovéhoto držitele platební karty jeho údaje. Na to navazuje fakt, že 78 % z dotázaných se setkalo nebo zná phishing – tedy podvodný e-mail, který má snahu vylákat veškeré informace uvedené na platební kartě. Je šokující, že stále velká část lidí těmto e-mailům věří. 58 % respondentů označilo spyware, tedy různé druhy virů, které mohou napadnout jak počítat tak i mobilní telefon. Tyto viry mohou např. přeposílat informace o přihlašovacích údajích bez vědomí uživatele. Tyto viry se dostávají na tato zařízení neopatrným používáním – otevírání příloh neznámých e-mailů, stahovaní souborů z P2P sítí a warez webech apod., infikovaní pomocí USB zařízení a další. Způsobu je opravdu několik, a jelikož 95 % dotázaných využívá internetové bankovnictví, jsou potencionálně vystavení těmto typům útoků. Z výsledků dále vyplynulo, že se platební karty stále nejčastěji využívají u obchodníků, tedy card-present transakce. Ovšem každým rokem se v České republice utrácí na internetu stále více peněz a tak je jen otázkou času, než budou převažovat právě CNP transakce. Je to dáno především tím, že tento způsob placení je poměrně novou záležitostí a je využíván především mladší generací. Co se týká zabezpečení platebních karet tak více než třetina dotázaných (38 %) má sjednané pojištění proti ztrátě a krádeži platební karty. Pojištění je většinou spjato i na pojištění osobních věcí a hlavně rozšiřuje ochranu klienta pro uskutečněné transakce před oznámením ztráty. Pojištění může také vyřešit různé sporné situace, aniž bychom se museli ohánět soudem nebo finančním arbitrem. Ovšem ani pojištění nezaručí vždy vrácení finančních prostředků. Pro výhodnější pojištění s vyššími limity si je potřeba připlácet, pojištění se vztahuje pouze na první ztrátu – poté si musíme sjednat nové, spoluúčast na finanční ztrátě, územní platnost jen na Českou republiku – všechny tyto faktory mohou ovlivňovat klienty, zda si sjednají toto pojištění k platebním kartám. Dále z výsledků vyplývá, že 36 % respondentů vyhledává při online nákupech obchodníky, kteří mají službu 3D Secure. Jak je zmíněno výše, v současné době tento systém přináší pouze falešný pocit bezpečí a spíše zdržení platby.

Platební karty se stále vyvíjejí a používají se stále nové technologie a zabezpečovací systémy, které by měly zvýšit bezpečnost platebních karet. Důležitá je však především prevence. Nikdo by neměl nikdy poskytovat své údaje o svých bankovních produktech a být velice obezřetný ve všech směrech. Důležitým prvkem je tedy samotný držitel platební karty, ten by měl dbát bezpečnostních opatření, jak u výběru z bankomatu, platbách u obchodníků tak i při platbách na internetu. Jelikož většina lidí má na svých běžných účtech uložené veškeré své úspory a při neopatrném používání platební karty o ně můžou rázem nenávratně přijít.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. BHARGAV, A. *PCI Compilance: The Definitive Guide.* Boca Raton : CRC Press, 2015. 351 s. ISBN 978-1-4987-5999-1.
2. DULANEY, E., EASTTOM, CH. *CompTIA Security+ Certification Study Guide*. 6. vyd. Indianapolis : Wiley, 2014. 505 s. ISBN 978-1-118-87547-6.
3. HADDAD, A. *A New Way To Pay: Creating Competitive Advantage Through The EMV Smart Card Standard*. 2. vyd. Burlington : Gower Pub Co, 2005. 143 s. ISBN 978-0566086885.
4. JOSHI, M. *Black Cards Forensics*. 2. vyd. India : Indiaforensic, 2006. 175 s. ISBN 81-903759-0-3.
5. JUŘÍK, P. *Encyklopedie platebních karet: Historie, současnost a budoucnost peněz a platebních karet.* Praha : Grada, 2003. 312 s. ISBN 80-247-0685-7.
6. JUŘÍK, P. *Historie bank a spořitelen v Čechách a na Moravě*. Praha : Libri, 2011. 190 s. ISBN 978-80-7277-488-3.
7. JUŘÍK, P. *Svět platebních a identifikačních karet.* Praha : Grada, 1999. 248 s. ISBN 80-7169-759-1.
8. KALABIS, Z. *Základy bankovnictví.* Brno : Albatros, 2012. 168 s. ISBN 978-80-265-0001-8.
9. KLUFA, F. *Elektronické platební prostředky: Jak se vyhnout rizikům.* Praha : Sdružení českých spotřebitelů, 2013. 15 s. ISBN 978-80-87719-07-7.
10. MÁČE, M. *Platební styk – klasický a elektronický.* Praha : Grada, 2006. 220 s. ISBN 80-247-1725-5.
11. POLOUČEK, S., et al. *Bankovnictví.* 2. vyd. Praha : C. H. Beck, 2013. 480 s. ISBN 978-80-7400-491-9.
12. PŘÁDKA, M., KALA, J. *Elektronické bankovnictví.* Praha : Computer Press, 2000. 166 s. ISBN 80-7226-328-5.
13. RAK, R., et al. *Biometrie a identita člověka.* Praha : Grada, 2008. 664 s. ISBN 978-80-247-2365-5.
14. SCHLOSSBERGER, O., et al. *Platební styk.* 3. vyd. Praha : Bankovní institut vysoká škola, 2000. 373 s. ISBN 80-7265-036-X.
15. SCHLOSSBERGER, O. *Platební služby*. Praha : Management Press, 2012. 325 s. ISBN 978-80-7261-238-3.

16. MARVANOVÁ, M., et al. *Platební styk.* 2. vyd. Praha : Bankovní institut, 1998. 376 s.

Elektronické zdroje

1. *324K Regpack users' info compromised when decrypted files placed on public-facing server* [online]. New York : Haymarket Media, 2016 [cit. 2016-11-13]. Dostupné z WWW: <https://www.scmagazine.com/324k-regpack-users-info-compromised-when-decryptedfilesplacedonpublicfacingserver/article/529780/>.
2. *Analýza NFC relay útoku* [online]. Petr Holubec, 2016 [cit. 2016-11-15]. Dostupné z WWW: <http://excel.fit.vutbr.cz/submissions/2016/020/20.pdf>.
3. *Bezpečnost karet* [online]. Praha : Sdružení pro bankovní karty, 2014 [cit. 2016-10-03]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_karty.html>.
4. *Budeme platit jen bankovními kartami?* [online]. Praha : RF Hobby, 2013 [cit. 2016-10-09]. Dostupné z WWW: <http://21stoleti.cz/2006/10/21/budeme-platit-jen-bankovnimi-kartami/>.
5. *Card Security Features* [online]. London, 2008 [cit. 2016-02-01]. Dostupné z WWW: <https://www.mastercard.com/ca/wce/PDF/Final_May_27_08_Lay_By_Card.pdf>.
6. *Credit Cards* [online]. Seattle : DataGenetics, 2013 [cit. 2016-02-05]. Dostupné z WWW: <http://datagenetics.com/blog/july42013/index.html>.
7. *Česká e-komerce v roce 2015 předčila očekávání, růst se nezastaví ani v roce 2016* [online]. Praha : Asociace pro elektronickou komerci, 2016 [cit. 2016-11-08]. Dostupné z WWW: <https://www.apek.cz/clanky/ceska-e-komerce-v-roce-2015-predcila-ocekavani-ru>.
8. *Falešný profil na Facebooku nabízející „nový servis 24“* [online]. Praha : Česká spořitelna, 2016 [cit. 2016-10-04]. Dostupné z WWW: <http://www.csas.cz/banka/content/inet/internet/cs/sc_17573.xml?archivePage=phishing&navid=nav00156_phishing_aktuality>.
9. *Fourth report on card fraud: July 2015* [online]. Frankfurt nad Mohanem : European Central Bank, 2015 [cit. 2016-10-03]. ISSN 2315-0033. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.

10. *Kaspersky Lab Reveals How Mobile Banking Trojan Hit Nearly 330,000 Android Users via Google AdSense* [online]. Dubai : Kaspersky Lab, 2016 [cit. 2016-11-17]. Dostupné z WWW: <http://newsroom.kaspersky.eu/en/texts/detail/article/kaspersky-lab-reveals-how-mobile-banking-trojan-hit-nearly-330000-android-users-via-google-adsense/?no_cache=1&cHash=bfe4c8cb022ad94a970a484153bca2e8>.
11. *Když bankomat spolkne kartu* [online]. Praha : Economia, 2005 [cit. 2016-10-13]. Dostupné z WWW: <http://www.penize.cz/debetni-karty/17573-kdyz-bankomat-polyka>.
12. *MasterCard And Zwipe Announce The Launch Of The World's First Biometric Contactless Payment Card With Integrated Fingerprint Sensor* [online]. London, 2014 [cit. 2016-01-31]. Dostupné z WWW: <http://newsroom.mastercard.com/press-releases/mastercard-zwipe-announce-launch-worlds-first-biometric-contactless-payment-card-integrated-fingerprint-sensor/>.
13. *Obchodní podmínky pro vydávání a používání vlastních platebních karet* [online]. Praha : Fio banka, 2016 [cit. 2016-10-30]. Dostupné z WWW: <http://www.fio.cz/docs/cz/OP_Karty_161222.pdf>.
14. *Odvětví platebních karet, standard bezpečnosti dat* [online]. Praha : Sdružení pro bankovní karty, 2015 [cit. 2017-01-28]. Dostupné z WWW: <http://pcistandard.cz/admin/uploads/PCI_DSS_v3-1_CZ.pdf>.
15. *Offline Transaction* [online]. Austin : InvestingAnswers, 2010 [cit. 2016-10-04]. Dostupné z WWW: <http://www.investinganswers.com/financial-dictionary/personal-finance/offline-transaction-2317>.
16. *Phishing - drahoušek zákazník* [online]. Josef Džubák, 2008 [cit. 2016-11-06]. Dostupné z WWW: <http://www.hoax.cz/cze/index.php?action=news_detail&id=158>.
17. *Podvody s kartami* [online]. Praha : Internet Info, 2010 [cit. 2016-10-13]. Dostupné z WWW: <http://www.mesec.cz/clanky/nejcastejsi-podvody-platebnimi-kartami/>.
18. *Podvody v oblasti bezhotovostních plateb v ČR* [online]. Praha : Sdružení českých spotřebitelů, 2009 [cit. 2016-11-07]. Dostupné z WWW: <http://www.finarbitr.cz/download/137_cs_a5_bezhotovostni_podvody.pdf>.

19. *Pojištění k platebním kartám* [online]. Praha : Fio banka, 2017 [cit. 2016-02-06]. Dostupné z WWW: <https://www.fio.cz/docs/cz/Informace_o_pojisteni_CP_ZDRAVI.pdf>.
20. *Prevent Pharming - Protect Your Identity* [online]. San Jose : Symantec, 2009 [cit. 2016-11-08]. Dostupné z WWW: <http://securityresponse.symantec.com/norton/clubsymantec/library/article.jsp?aid=cs_prevent_pharming>.
21. *Revoluce v placení: Chytrým mobilem platí v obchodech už tisíce Čechů* [online]. Praha : Mafra, 2016 [cit. 2016-11-15]. Dostupné z WWW: <http://finance.idnes.cz/novy-trend-bezkontaktni-platby-mobilem-fc8-/bank.aspx?c=A161020_073627_bank_sov>.
22. *Skimming* [online]. Praha : Národní centrála proti organizovanému zločinu, 2013 [cit. 2016-10-14]. Dostupné z WWW: <http://www.policie.cz/clanek/skimming-2013.aspx>.
23. *Setkává se s útoky na bankovní účty lidí. Češi jsou nepoučitelní, říká* [online]. Praha : Mafra, 2016 [cit. 2016-11-15]. Dostupné z WWW: <http://finance.idnes.cz/internetova-bezpecnost-a-utoky-na-bankovni-ucty-fux-/bank.aspx?c=A160608_154955_bank_sov>.
24. *Skimming u bankomatu* [online]. Praha : Sdružení pro bankovní karty, 2016 [cit. 2016-10-14]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Skimming_u _bankomatu>.
25. *Skimming u obchodníka* [online]. Praha : Sdružení pro bankovní karty, 2016 [cit. 2016-10-14]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html#Skimming>.
26. *Souhrnné statistiky za rok 2013* [online]. Praha : Sdružení pro bankovní karty, 2013 [cit. 2016-10-08]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html>.
27. *Symmetric vs Asymmetric Encryption* [online]. Florida : JSCAPE, 2015 [cit. 2016-01-30]. Dostupné z WWW: <http://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption>.
28. *Third Report on card fraud: February 2014* [online]. Frankfurt nad Mohanem : European Central Bank, 2014 [cit. 2016-10-03]. ISSN 2315-0033. Dostupné z WWW: <https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html>.
29. *Trestní zákoník* [online]. Praha : Ministerstvo vnitra ČR, 2017 [cit. 2017-01-15]. Dostupné z WWW: <https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68040&nr=40~2F2009&rpp=15>.

30. *Útočníci na Facebooku kradou přihlašovací údaje administrátorů stránek a čísla platebních karet* [online]. Praha : ESET software, 2016 [cit. 2016-10-04]. Dostupné z WWW: <https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/article/utocnici-na-facebooku-kradou-prihlasovaci-udaje-administratoru-stranek/>.
31. *Varujeme před novou verzí phishingu* [online]. Praha : Česká spořitelna, 2014 [cit. 2016-11-06]. Dostupné z WWW: <https://www.csas.cz/banka/content/inet/internet/cs/news_ie_2309.xml?archivePage=pishing&navid=nav00156_phishing_aktuality>.
32. VYCHODIL, J. *Princip a zabezpečení platebních karet*. [online]. Brno : VUT, 2015 [cit. 2016-01-30]. ISSN 1213-1539. Dostupné z WWW: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/20/princip-a-zabezpeceni-platebnich-karet-1-1-1/>.
33. *Zařízení na zachycení karty* [online]. Praha : Sdružení pro bankovní karty, 2016 [cit. 2016-10-13]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html>.
34. *Zákon o platebním styku* [online]. Praha : Ministerstvo vnitra ČR, 2017 [cit. 2017-01-15]. Dostupné z WWW:<http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=69225&nr=284~2F2009&rpp=15>.
35. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2015* [online]. Praha : Ministerstvo vnitra ČR, 2015 [cit. 2016-10-14]. Dostupné z WWW: <http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx>.
36. *Ztráta identity* [online]. Praha : Národní centrála proti organizovanému zločinu, 2010 [cit. 2016-10-14]. Dostupné z WWW: <http://www.policie.cz/clanek/ztrata-identity.aspx>.

SEZNAM ZKRATEK

BIN – Bank Identification Number

CNP – Card Not Present

CVC – Card Verification Code (MasterCard)

CVV – Card Verification Value (VISA)

ČSOB – Československá obchodní banka

DES – Data Encryption Standard

EC/MC – EuroCard/MasterCard

EMV – Europay, MasterCard, VISA

GPE – Global Payments Europe

HCE – Host Card Emulation

HTTPS – Hypertext Transfer Protocol Secure

ISO – International Standard Organization

JCB – Japan Credit Bureau

MO/TO – Mail Order/Telephone Order

NFC – Near Filed Communication

OCR – Optical Character Recognition

PCI DSS – Payment Card Industry Data Security Standard

PIN – Personal Identification Number

POS – Point-of-Sale

RVHP – Rada vzájemné hospodářské pomoci

SBČS – Státní banka československá

SET – Secure Electronic Transaction

VISA – Visa International Service Association

VÚB – Všeobecná úvěrová banka

SEZNAM TABULEK, OBRÁZKŮ A GRAFŮ

Seznam tabulek

Seznam obrázků

Seznam grafů

PŘÍLOHY

Příloha č. I: Lehce rozeznatelný phishing[94]

Drahoušek Zákazník,

Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostrední.

Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet.

Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit.

Obnovit se Ted tvuj SERVIS 24 Internetbanking.

SERVIZ: SERVIS 24 Internetbanking
SKONANI: Leden, 11 2008

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k sloužit tebe.

Ceská Sporitelna Služba úcastníkum

****
DULEŽITÝ Služba úcastníkum HLÁŠENÍ
****

Být príjemný cinit ne namítat až k tato poselstvi. Do jakýkoliv bádat , dotyk Služba úcastníkum

© Ceská Sporitelna.

Všechna práva vyhrazena.

[94] *Phishing - drahoušek zákazník* [online]. Josef Džubák, 2008 [cit. 2016-11-06]. Dostupné z WWW: <http://www.hoax.cz/cze/index.php?action=news_detail&id=158>.

Příloha č. II: Propracovanější verze phishingu[95]

----- Original Message -----
From: Česká spořitelna
To: [redacted]
Sent: Tuesday, December 02, 2014 7:33 AM
Subject: Naléhavý Naléhavé od Česká spořitelna !!

Aktualizace Aktivace účtu Česká spořitelna

Vážený zákazníku

Chtěli bychom zdůraznit, že přístup do vašeho internetového bankovnictví je brzy skončí. Aby bylo možné i nadále využívat on-line bankovnictví, žádáme vás o potvrzení své údaje pomocí odkazu níže.

Aktualizujte svůj on-line bankovní účet: klikněte zde

Budeme automaticky obnovovat on-line bankovní účet, a budete kontaktováni jedním z našich zaměstnanců. Internetové bankovnictví umožňuje rychlý a snadný přístup k vašemu účtu. Můžete snadno převést peníze pomocí jediného kliknutí.

S pozdravem,

Klára Pačesová

Agent Zákaznický servis.

[95] *Varujeme před novou verzí phishingu* [online]. Praha : Česká spořitelna, 2014 [cit. 2016-11-06]. Dostupné z WWW: <https://www.csas.cz/banka/content/inet/internet/cs/news_ie_2309.xml?archivePage=pishing&navid=nav00156_phishing_aktuality>.

Příloha č. III: Vzor dotazníku

Dotazník „Bezpečnost a rizika platebních karet“

Dobrý den, jsem studentem Vysoké školy evropských a regionálních studií, z. ú. Chtěl bych Vás požádat o vyplnění toho dotazníku, který je zaměřený na rizika spojená s používáním platebních karet a na jejich možnou ochranu. Zjištěné informace budou použity ke zpracování bakalářské práce.

1. **Jste držitelem platební karty?**
   - ☐ ano
   - ☐ ne
2. **Jak často platební kartu používáte?**
   - ☐ denně
   - ☐ 3-5krát za týden
   - ☐ 1 do měsíce
   - ☐ nepoužívám
3. **Je vaše platební karta bezkontaktní?**
   - ☐ ano
   - ☐ ne
   - ☐ nevím
4. **Víte, jaké máte nastavené limity na platební kartě?**
   - ☐ ano
   - ☐ ne
5. **Kde s platební kartou převážně platíte?**
   - ☐ na internetu
   - ☐ u obchodníků
   - ☐ ve stejném poměru u obchodníků i na internetu
   - ☐ neplatím s ní
6. **Jste si vědom/a rizik, která jsou spojena s používáním platební karty?**
   - ☐ ano, jsem a realizuji proto patřičná opatření
   - ☐ ano, jsem, ale nerealizuji proto žádná opatření
   - ☐ o žádných rizicích nic nevím

7. Zaškrtněte typ/y útoků, které znáte nebo jste se s nimi setkal/a:

☐ skimming (odcizení údajů o platební kartě)

☐ phishing (podvodné e-maily)

☐ pharming (podvodné stránky banky)

☐ spyware (trojský kůň, viry)

☐ krádež platební karty

☐ neznám žádný z uvedených

8. Odkud znáte tyto útoky nebo kde jste se s nimi setkali?

☐ mám osobní zkušenost

☐ v médiích

☐ v tisku

☐ upozornila mě na ně banka

☐ od přátel

☐ jinde, uveďte……

9. Byla Vaše platební karta nebo ve vašem blízkém okolí někdy zneužita?

☐ ano, jednou

☐ ano, několikrát

☐ ne

10. Máte dostatek informací o možnostech ochrany platebních karet?

☐ ano

☐ ne

11. Odkud máte tyto informace?

☐ z médií

☐ z tisku

☐ informovala mě o nich banka

☐ od přátel

☐ odjinud, uveďte……

12. Využíváte při platbách na internetu některé z těchto ochran?

- ☐ virtuální platební karty
- ☐ předplacené karty
- ☐ více platebních karet
- ☐ zprostředkování platby pomocí - PayPal, PaySec
- ☐ manipulace s limity na platební kartě
- ☐ preferování obchodníka se službou 3D Secure
- ☐ žádnou z uvedených
- ☐ neplatím na internetu

13. Zaškrtněte pojištění, která máte sjednaná k platební kartě:

- ☐ cestovní pojištění
- ☐ pojištění proti ztrátě a krádeži karty
- ☐ pojištění právní ochrany řidičů
- ☐ nemám sjednané žádné pojištění k platební kartě

14. Používáte internetové bankovnictví?

- ☐ ano
- ☐ ne

15. Jaké používáte při přihlašování autorizační metody?

- ☐ zaslaný kód SMS
- ☐ certifikát, elektronický klíč
- ☐ vygenerovaný kód přes mobilní aplikaci, potvrzení pomocí mobilní aplikace
- ☐ čipovou kartu s elektronickým podpisem
- ☐ autorizační kalkulačku
- ☐ žádné, mám pouze jméno a heslo
- ☐ používám jinou metodu autorizace, uveďte……

16. Odkud se převážně přihlašujete do internetového bankovnictví?

☐ z domova

☐ z práce

☐ z veřejných počítačů

☐ z telefonu přes webový prohlížeč

☐ z telefonu přes aplikaci banky

☐ odjinud, uveďte……

17. Máte nastavené notifikace o pohybech na účtu, SMS zprávou nebo e-mailem?

☐ ano

☐ ne

18. Platíte mobilním telefonem (NFC)?

☐ ano

☐ ne

19. Jaké je Vaše pohlaví?

☐ muž

☐ žena

20. Do jaké věkové kategorie patříte?

☐ do 18 let

☐ 18 – 25 let

☐ 26 – 35 let

☐ 36 – 45 let

☐ 46 – 55 let

☐ 56 let více

Děkuji za Váš čas, který jste strávili u vyplňování dotazníku.