B&B
VIŠJA STROKOVNA ŠOLA

Diplomsko delo višješolskega strokovnega študija
Program: Ekonomist
Modul: Asistent v podpori bančnega poslovanja

VARNOST KARTIČNEGA POSLOVANJA

Mentorica: mag. Romana Fišer
Lektorica: Ana Peklenik, prof.

Kandidat: Luka Klemenčič

Kranj, junij 2013

ZAHVALA

Zahvaljujem se mentorici mag. Romani Fišer, ki mi je nudila strokovno pomoč pri izdelavi diplomske naloge.

Zahvaljujem se lektorici Ani Peklenik, ki je mojo diplomsko nalogo jezikovno in slovnično pregledala.

IZJAVA

»Študent Luka Klemenčič izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom mag. Romane Fišer.«

»Skladno s 1. odstavkom 21. člena Zakona o avtorski in sorodnih pravicah dovoljujem objavo tega diplomskega dela na spletni strani šole.«

Dne 17. junija 2013 Podpis:

POVZETEK

Kartično poslovanje že vrsto let zamenjuje gotovinsko in je močno razširjeno po vsem svetu. Najbolj ključna za varnost kartičnega poslovanja je zaščita plačilne kartice s številko PIN (*Personal Identification Number*). Pomembne mednarodne plačilne kartice so zaščitene še z dodatnimi varnostnimi oznakami, kot so reliefni vtis podatkov o uporabniku, številka kartice, hologrami itd. Zlorabe plačilnih kartic so najpogostejše na bankomatih, kjer se uporabniki lahko srečamo s t. i. »skimming napravo«, »libanonsko zanko« ali zagozdo. Pozorni moramo biti tudi pri spletnem nakupovanju, kjer goljufi skušajo priti do podatkov o kartici na različne načine. Uporabniki se pred zlorabami delno lahko zaščitimo sami, kar pomeni predvsem varovanje številke PIN in primerno ravnanje s kartico. Vendar pa naše prizadevanje včasih ni dovolj, kaj hitro smo lahko tarča nezakonite kraje svojega imetja ali osebnih podatkov. Banke v ta namen ponujajo različna zavarovanja pred zlorabami plačilnih kartic, za varno spletno nakupovanje pa sta nam na voljo varnostna mehanizma *SecureCode* in *Verified by Visa*, ki ustvarita kodo za enkratno uporabo.

KLJUČNE BESEDE

- plačilna kartica
- kartično poslovanje
- varnost kartičnega poslovanja

SUMMARY

Card bussiness became well known replacement for cash bussiness and is now expended all over the world. The key to ensure the security of card bussiness is protection of pay card with PIN (Personal Identification Number). Important international pay cards are also protected with extra security code such as embossed user data entry, card number, holograms and so on. Misues with pay cards are usually on cash machines where as a user we can encounter with so called »skimming device«, »Lebanese loop« or chook. We should also be careful with internet shopping where abusers try to get information from pay cards on different kind of ways. Users can protect themselves, which means to secure PIN number and right handling with pay cards. It can happen that we become a target of illegal stealing of our property or personal data. Banks offer differnt ways of pay card security. For safe internet shopping there are two securtiy mechanisms: *SecureCode* and *Verifed by Visa* which can create a code for one time use only.

KEY WORDS

- pay card
- card bussiness
- security of card bussiness

KAZALO

1 UVOD

1.1 PREDSTAVITEV PROBLEMA

Plačilna kartica je vse pogostejši plačilni instrument brezgotovinskega poslovanja. Običajno takšne kartice omogočajo tudi dvig gotovine na bankomatih, zato jih lahko poimenujemo tudi gotovinske kartice. Zlorabe tovrstnih kartic, kot so »skimming«, »libanonska zanka«, »Cash Trapping« oz. zagozda so tako najbolj pogoste ravno na bankomatih. »Skimming naprava« prebere magnetni zapis na plačilni kartici in je nameščena na bankomatu. PIN (*Personal Identification Number*) se zajame vizualno, s kamero. Pri »libanonski zanki« bankomat ne vrne kartice in ne izda denarja. Pri t. i. »Cash Trappingu« pa se na bankomatu izpiše, da denar lahko prevzamemo, a ga ne moremo.

1.2 CILJI NALOGE

Opredelitev ciljev diplomske naloge:

- teoretično predstaviti kartično in POS-poslovanje (angl. *Point of Sale*),
- opredeliti vrste bančnih kartic,
- predstaviti najpogostejše zlorabe v zvezi s kartičnim poslovanjem,
- z anketo ugotoviti osveščenost uporabnikov o zlorabah in preučiti možnosti za zavarovanje pred zlorabami ter načine, kako za varnost kartičnega poslovanja poskrbimo sami.

Predvideni rezultati in ugotovitve v nalogi naj bi bili uporabni predvsem za vodilni kader v Banki X, za vse posameznike, ki uporabljajo bančne kartice, v pomoč pa bodo tudi vsem raziskovalcem kartičnega poslovanja pri nas in po svetu.

1.3 PREDSTAVITEV OKOLJA

Kartično poslovanje je danes najpogostejši način poslovanja. Kot komitent določene slovenske banke lahko plačujemo in dvigujemo denar kjerkoli po svetu. Zato je zelo pomembna varnost kartičnega poslovanja, osveščenost o vrstah in zaščiti pred zlorabami.

Raziskava o varnosti kartičnega poslovanja je sicer omejena na komitente Banke X, njene ugotovitve in rezultate pa lahko prenesemo na širše, svetovno okolje.

1.4 PREDPOSTAVKE IN OMEJITVE

Naša predpostavka pred pisanjem naloge je bila v prvi vrsti ta, da uporabniki bančnih kartic premalo poskrbijo za svojo varnost pri takšnem poslovanju. Vse več je tudi spletnega nakupovanja na neznanih spletnih straneh, za katere uporabniki ne morejo vedeti, ali so varne ali ne.

Zaradi varnosti osebnih in drugih podatkov banko v nalogi imenujemo Banka X; nanjo se raziskava nanaša. Pred pisanjem diplomske naloge je bilo treba pridobiti ustno dovoljenje nadrejenih za uporabo internega gradiva in izvajanje anketiranja.

1.5 METODE DELA

Naloga je sestavljena iz teoretičnega in empiričnega dela. V teoretičnem delu naloge smo uporabili več metod. Raziskovalni problem smo v prvi vrsti opisovali – uporabili smo torej metodo deskripcije. Pri tem smo si pomagali predvsem s strokovno literaturo, spletnimi viri in internimi viri Banke X. Črpali smo iz literature in virov različnih avtorjev, ki so se lotili raziskovanja sorodnega problema. Takšno metodo raziskovanja imenujemo metoda kompilacije.

Literaturo in vire smo iskali s pomočjo spleta in brskalnikov. Uporabljali smo COBISS (angl. *Cooperative Online Bibliographic System and Services*), ki je namenjen iskanju znanstvene in strokovne literature, ter iskalnika *Google* in *Google Scholar*.

Empirični del naloge je sestavljen iz analize delovnih hipotez in anketnega vprašalnika. Pred izvajanjem ankete smo si zastavili šest hipotez, ki smo jih po obdelavi odgovorov iz anketnega vprašalnika potrdili, delno potrdili ali ovrgli. Raziskovali smo mnenje petdesetih naključno izbranih anketirancev, ki so bile različno stare in različnega spola. Njihove odgovore smo opisali in jih ponazorili v tabelah ter grafih.

2 KARTIČNO IN POS-POSLOVANJE

Plastični denar že vrsto let zamenjuje gotovinsko in čekovno poslovanje. V poznih šestdesetih letih se je skupina ameriških poslovnežev v restavraciji znašla v neprijetni situaciji. Niso imeli denarja, da bi plačali kosilo s svojimi poslovnimi partnerji. Ta situacija jih je spodbudila, da so leta 1959 izdali prvo plačilno kartico *Diners* in ustanovili kartični sistem, ki se je razširil po celem svetu in pridobil veliko tekmecev. Tako je kmalu sledila izdaja kartice *American Express* v letu 1958, leta 1966 *MasterCard* in leta 1977 *Visa.* Prva slovenska kartica *Activa* je bila ustanovljena leta 1992, danes pa na slovenskem obstajajo še kartice, kot so *Activa Maestro*, *Activa Mastercard*, *Activa Visa* in *Activa Visa Electron* (Novak, 2009).

Kartično poslovanje lahko opišemo kot princip delovanja med štirimi strankami, tj. banko kot izdajateljico kartice, imetnikom kartice, banko kot lastnico prodajnega mesta ter prodajnim mestom. Takšen štiripartitni sistem omogoča, da je kartica sprejeta po celem svetu (Novak, 2009). Mejač Krassnigova (2008) pri uporabi plačilne kartice govori o naslednjih udeležencih:

- banki kot izdajateljici kartice,
- banki kot lastnici prodajnega mesta,
- procesnem denarju,
- mednarodnem kartičnem sistemu,
- imetniku kartice in
- prodajnem mestu.

2.1 PLAČILNE KARTICE

Plačilna kartica je plačilni instrument brezgotovinskega poslovanja, lahko pa je namenjena tudi dvigovanju gotovine ali plačilu računov, izstavljenih s strani trgovcev in storitvenih podjetij.

V grobem plačilne kartice delimo glede na dve značilnosti:

- glede na roke poravnanja obveznosti in
- možnosti koriščenja posojil.

Glede na roke poravnanja obveznosti delimo plačilne kartice na kartice:

- z zamikom plačila in
- kartice s takojšnjim plačilom.

Glede na možnosti koriščenja posojil pa jih delimo na:

- kreditne plačilne kartice in
- plačilne kartice brez možnosti koriščenja posojil.

Izdajatelji plačilnih kartic uporabnikom plačilnih kartic torej odobravajo tudi posojila. Posojilo je lahko vezano na nakupe s kartico ali pa ga uporabnik črpa na katerikoli drugi način. Plačilna kartica *Activa Maestro* je tako kartica s takojšnjim plačilom, plačilna kartica *Activa MasterCard* pa je po določenih kriterijih plačilno-kreditna in omogoča zamik plačila.

Plačilne kartice so običajno veljavne štiri leta, njihova veljavnost se avtomatično obnavlja. Za vse nakupe s plačilnimi karticami uporabniki plačujejo obveznosti s svojega osebnega računa. Tako so plačilne kartice vezane na osebne račune uporabnikov in so instrumenti za poslovanje s tovrstnimi računi. Uporabnik kartice odgovarja za vse neporavnane obveznosti, ki izhajajo iz poslovanja s kartico (Navodila za izdajanje plačilnih kartic, 2012).

Uporabnik kartice je dolžan zagotoviti kritje na osebnem računu za vse opravljene nakupe s kartico za vsa prejeta potrdila o nakupu. To je glavna razlika med to in kartico z odloženim plačilom, kot je npr. *Activa MasterCard*. Matični podatki, podatki o osebnem računu in prometu s plačilno kartico so poslovna tajnost banke. Navedene podatke bančni delavec lahko sporoči le na osnovi pisne zahteve sodišča in na osnovi ustne ali pisne zahteve uporabnika. V primeru nepravilno opravljenega nakupa bančni delavec ne sme sporočiti podatkov o uporabniku kartice prodajnemu mestu, kjer je bil nakup opravljen. Reklamacijo lahko rešuje le tako, da uporabnika kartice pokliče v banko (Navodila za izdajanje plačilnih kartic, 2012).

Plačilna kartica je identifikacijski dokument pri opravljanju bančnih storitev in plačilni instrument, namenjen uporabnikom osebnih računov ter njihovim pooblaščencem za plačilo blaga in storitev na prodajnih mestih v domači državi in tujini. Prodajna mesta morajo biti opremljena s POS-terminali. Lahko tudi dvigujejo gotovino, in sicer na bankah, bankomatih, poštah in prodajnih mestih, ki so označena z možnostjo za izplačilo gotovine.

2.2 VRSTE PLAČILNIH KARTIC SISTEMA ACTIVA

»*Sistem Activa združuje dvanajst bank, ki skrbijo za razvoj domačega in mednarodnega brezgotovinskega poslovanja. S svojimi storitvami in izdelki je dodobra osvojil slovenske uporabnike kartic. Odkar je sistem Activa postavil temelje za razvoj kartičnega poslovanja v Sloveniji, je njegova rast v nenehnem vzponu*« (http://www.activa.si/).

Slovenci imamo torej sistem *Activa*, ki izdaja domače in pomembne mednarodne kartice, kot so *Activa Maestro*, *Activa MasterCard*, *Visa* in *Visa Electron*. Na kratko bomo povzeli skupne lastnosti in razlike med karticama *Activa Maestro in Activa MasterCard*, ki sta najpogosteje uporabljeni.

Activa Maestro je plačilna kartica, namenjena imetnikom osebnih računov za plačilo blaga in storitev, omogoča pa tudi dvig gotovine v Sloveniji in tujih državah. *Activa Maestro* se uporablja izključno na POS-terminalih in bankomatih. Na površini je gladka in nima reliefnega vtisa podatkov o imenu in priimku uporabnika ter številki kartice. Uporabniki lahko opravljajo tudi nakupe preko spleta, vendar le pri tistih trgovcih, ki imajo svoje strani označene z logotipom Maestro. Za opravljene dvige in plačila je uporabnik takoj obremenjen na svojem osebnem računu (http://www.activa.si/).

V desnem zgornjem kotu vsebuje logotip Activa, desno spodaj pa logotip Maestro. Na sprednji strani zgoraj se nahaja naziv banke izdajateljice, v spodnji polovici kartice pa so navedeni ime in priimek uporabnika, SI56 in številka računa, številka kartice ter njena veljavnost. Na hrbtni strani je zapisana telefonska številka avtorizacijskega centra, magnetni zapis, prostor za podpis uporabnika, PAN (angl. *Primary Account Number*) kartice, oznaka OE (območna enota), logotipi sistemov, kjer se kartica lahko uporablja, in besedilo o lastništvu kartice (http://www.activa.si/).

Slika 1: Activa Maestro
(Vir: http://www.activa.si/)

Activa MasterCard je ravno tako namenjena plačevanju blaga in storitev v Sloveniji in tujih državah ter dvigovanju gotovine na bankomatih. Uporabnik lahko nakupuje tudi preko spleta s pomočjo uporabe kode CVC (angl. *Card Verification Code*). Za uporabo plačuje letno članarino, za dvig gotovine pa provizijo. Na plačilni kartici Activa MasterCard se levo zgoraj nahaja naziv banke izdajateljice, kjer je levo pod napisom vgrajen čip, v sredini pa je sklop šestnajstih števil, ki predstavljajo številko kartice (PAN). Levo pod PAN-om se nahaja šifra banke izdajateljice ali BIN (angl. *Bank Identification Number*), tj. štirimestna koda, ki se ujema s prvimi številkami kartice, desno pa se nahajata še datum veljavnosti in oznaka MC (MasterCard) –

dodatno vtisnjen varnostni znak. Na desni strani se nahaja tudi hologram – zaščitni tridimenzionalni znak za *MasterCard*. Na hrbtni strani je zapisana telefonska številka avtorizacijskega centra, magnetni zapis, prostor za podpis uporabnika in naziv lastnika – izdajatelja kartice. Na praznem prostoru za podpis se nahaja 4 + 3-mestna koda (CV2), zadnje tri številke te kode potrebujemo pri plačevanju preko spletnih strani (http://www.activa.si/).

Slika 2: Activa MasterCard
(Vir: http://www.activa.si/)

2.3 IZDAJANJE IN VROČANJE KARTIC UPORABNIKOM

Pri izdajanju in vročanju plačilnih kartic uporabnikom se zahteva poseben postopek, ki je določen s pravilniki o izdajanju plačilnih kartic že obstoječim in novim uporabnikom. Tako je posebej določen postopek pri prejemu kartic in PIN-a s strani izdelovalca, pri izročanju kartic že obstoječim in novim uporabnikom ter pri izročanju osebnih gesel (PIN-a) uporabnikom.

Najprej se izdelajo PIN-i, ki jih banka prejme v zaprtih kuvertah. Pooblaščeni delavec v banki te PIN-e potrdi in svojo potrditev posreduje Banki Koper preko elektronske pošte. Po potrditvi pooblaščenega delavca Banka Koper pošlje banki kartice. Pooblaščeni delavec jih nato prevzame, kar potrdi s svojim podpisom in posreduje po poslovalnicah banke še isti dan. Za novo izdelane kartice se vodijo določeni seznami, ki se morajo hraniti eno leto. Vodja poslovalnice je dolžan preveriti, če je prejel vse naročene kartice in svojo kontrolo tudi arhivirati. Do izročitve uporabniku se kartice hranijo v priročnih in zaklenjenih blagajnah. V času hranjenja je delavec v banki materialno odgovoren za izgubo ali zlorabo kartic. Po zaključku dela se mora priročna blagajna shraniti v trezor. Prejem kartice morajo uporabniki potrditi z lastnoročnim podpisom na določenem obrazcu (Navodila za izdajanje plačilnih kartic, 2012).

Plačilne kartice uporabnikom torej izročajo delavci v poslovalnici, kjer vodijo tudi njihov t. i. dosje osebnega računa. Pred izročitvijo je delavec dolžan ponovno preveriti, če imetnik osebnega računa še izpolnjuje pogoje za poslovanje s kartico,

in pravilnost dodeljenih limitov. Uporabnik prejem in seznanjenost s pogoji poslovanja potrdi s podpisom v za to namenjeni obrazec. Podpisani obrazec odgovorni delavec shrani v dosje osebnega računa. Če gre za izdajo prenovljene kartice, je uporabnik dolžan vrniti staro plačilno kartico. Vrnjeno kartico je delavec v banki dolžan uničiti takoj, pred očmi stranke. Lahko jo prereže ali preluknja in kasneje odda v razrez. Plačilna kartica je aktivna takoj po izročitvi uporabniku (Navodila za izdajanje plačilnih kartic, 2012).

Uporabniki plačilnih kartic ob prejemu kartic dobijo tudi svoje osebno geslo (PIN). PIN služi uporabnikom kartice za dvig gotovine na bankomatih in za nakup na tistih prodajnih mestih, ki so opremljena s POS-tehnologijo in zahtevajo vnos PIN-a. V tem primeru podpis ni potreben. Bančni delavci izročajo osebna gesla po posebnem postopku. Uporabnik, ki izgubi ali pozabi PIN, lahko dobi novega le z naročilom nove kartice (Navodila za izdajanje plačilnih kartic, 2012).

2.4 POS-TERMINALI

POS-tehnologija predstavlja avtomatski prenos in izmenjavo podatkov preko terminala, ki je nameščen na prodajnem mestu. Ob uporabi javnega omrežja se preko terminala podatki prenesejo do glavnega računalnika v banki. Takšne naprave so torej povezane z banko in avtomatsko zajemajo podatke o nakupu s plačilno kartico. POS-terminal pri vsaki transakciji preveri tudi veljavnost kartice ter potrdi ali zavrne nakup. Elektronski prodajni terminal oz. POS-terminal shranjuje vse podatke o nakupih in jih v določenih časovnih presledkih prenaša v glavni in centralni računalnik, kjer se transakcije poknjižijo. Terminal izdaja potrdila o nakupih (angl. *Slip*) in izdela zaključek ob koncu poslovnega dne (Črničovič Krofič, 1995).

Prodajno mesto je mesto, kjer stoji POS-terminal, najemnik pa sklene z banko najemno pogodbo. Znesek mesečne najemnine je odvisen od prometa na tem prodajnem mestu, pri čemer je običajna praksa, da prodajna mesta z večjim prometom plačujejo manjše najemnine (Novak, 2009).

Grubar (1998) navaja številne prednosti POS-tehnologije:

- avtomatska avtorizacija,
- izpisovanje potrdil o nakupu,
- terminal samodejno natisne potrdilo o nakupu,
- izvede se kontrola veljavnosti kartice,
- preveri se tudi, ali se kartica nahaja na t. i. »stop« listi,
- nadomestilo za podpis je PIN-koda,
- prodajna mesta lahko sprejemajo različne vrste kartic,
- enostaven zaključek poslovanja,
- ni potrebno seštevati potrdil o nakupu, ker terminal to opravi avtomatsko,

- terminali ločijo tudi zbirne vsote nakupov po različnih karticah.

Sama transakcija na POS-terminalu poteka tako, da stranka najprej vstavi svojo plačilno kartico v režo. Po vložitvi kartice se preko servisnega centra vzpostavi zveza z računalnikom na strani izdajatelja kartice. Opravi se identifikacija in ugotovi plačilno sposobnost kupca, preveri se veljavnost kartice ter podatki o zadostnih sredstvih na osebnem računu. Če so podatki skladni, POS-terminal izda potrdilo o nakupu, v nasprotnem primeru pa transakcijo zavrne (Bobek, 2003). Vse fizične povezave z banko tako odpadejo, nič več ni poti in pošiljanja dokumentov. Vse se prične in zaključi preko komunikacije s terminalom in centralnim računalnikom. Pri tem teče tudi obračun med trgovcem – lastnikom prodajnega mesta, banko in imetnikom plačilne kartice (Novak, 2009).

2.5 SERVISIRANJE POS-TERMINALOV

Banke vse postopke ravnanja s POS-terminali in odgovornosti svojih delavcev ob izvajanju servisiranja določajo s pravilniki o servisiranju POS-terminalov in ostale pripadajoče opreme.

Skrbniki POS-terminalov so pooblaščeni delavci, ki izvajajo naslednje naloge:

- organizirajo in izvajajo servisne dejavnosti, vodijo evidenco ter izdelajo poročilo s področja servisiranja POS-terminalov,
- izvajajo vse aktivnosti v skladu s sprejetimi pravilniki, ki veljajo v določeni banki.

Obveznosti servisiranja in vzdrževanja POS-terminalov so običajno opredeljene v pogodbah o najemu POS-terminalov z najemniki. Skrbnik POS terminalov mora popravilo POS-terminala organizirati v najkrajšem možnem času v skladu z vsemi veljavnimi akti določene banke. Organizacijo servisiranja torej v celoti vodi skrbnik POS-terminalov (Pravilnik o servisiranju POS terminalov in ostale pripadajoče opreme, 2008).

Skrbnik POS-terminalov mora voditi evidenco o prijavljenih napakah v njihovem delovanju, ki morajo vsebovati vsaj naslednje podatke (Pravilnik o servisiranju POS terminalov in ostale pripadajoče opreme, 2012):

- zaporedno številko napake,
- datum prijave,
- uro prijave,
- prijavno mesto,
- kontaktno osebo,
- telefonsko številko,

- opis okvare,
- razločen vpis (z velikimi črkami) imena in priimka tistega delavca, ki je prejel sporočilo o napaki,
- katerega dne se je opravil servis,
- razločen vpis (z velikimi črkami) imena in priimka osebe, ki je izvedla popravilo.

Najemniki POS-terminalov sporočajo napake v delovanju na sledeče načine (Pravilnik o servisiranju POS terminalov in ostale pripadajoče opreme, 2012):

- po telefonu za to odgovornim delavcem,
- po telefonu servisnemu centru Activa,
- po telefonu ali na mobilni telefon skrbniku POS-terminalov,
- po elektronski pošti na naslov odgovornih delavcev ali pa na dogovorjen naslov in
- po faksu.

Skrbniki POS-terminalov in njihovi namestniki so dolžni izvajati popravila POS-terminalov na podlagi prijav najemnikov tudi izven rednega delovnega časa.

2.6 BANKOMATI

Bankomate uporabljamo takrat, ko potrebujemo gotovino. Razvejana mreža samopostrežnih bankomatov nam omogoča, da nam je gotovina dostopna takrat, ko jo potrebujemo. Običajno so nameščeni na priročnih lokacijah, kot so trgovski centri, avtobusna postajališča, na ulicah, ki so namenjene pešcem, ob bančnih poslovalnicah ipd. Delujejo štiriindvajset ur na dan, vse dni v tednu, dvig pa je običajno mogoče opraviti z različnimi vrstami plačilnih kartic (http://www.gbkr.si/osebne-finance/bankomat-4216*).*

Slovensko podjetje Bankart upravlja in nadzoruje mrežo bančnih avtomatov za poslovne banke in hranilnice, ki so dejavne na področju Slovenije. Podjetje pokriva kar 95-odstotni delež na slovenskem trgu. V Bankartovi mreži so trenutno Abanka Vipa, d.d., Banka Celje, d.d., Banka Koper, d.d., Banka Sparkasse, d.d., Delavska hranilnica, Deželna banka Slovenije, d.d., Factor banka, d.d., Gorenjska banka, d.d., Hranilnica LON, Hypo Alpe-Adria-Bank, d.d., Nova Ljubljanska banka, d.d., Nova KBM, d.d., Poštna banka Slovenije, d.d., Probanka, d.d., Raiffeisen banka, d.d., Sberbank banka, d.d., SKB, d.d. in UniCredit Banka Slovenija, d.d. (http://www.bankart.si/si/ponudba/upravljanje_mreze_bankomatov/*,* 7. 5. 2013).

V mrežo bankomatov so vključeni bančni avtomati *Diebold*, *NCR (National cash Register)* in *Wincor Nixdorf*, ki sprejemajo kartice *BA Maestro* in *Activo Maestro* ter vse glavne mednarodne kartice, kot so *MasterCard*, *Visa* in *Diners*. Število

bankomatov se iz leta v leto povečuje, v letu 2012 so presegli število dva tisoč (http://www.bankart.si/si/ponudba/upravljanje_mreze_bankomatov/).

Storitve, ki jih bankomati omogočajo, so naslednje (http://www.bankart.si/si/ponudba/upravljanje_mreze_bankomatov/):

- prenos sredstev med računi,
- polog gotovine,
- plačilo univerzalnih plačilnih nalogov (UPN),
- dvig gotovine,
- izpis prometa po osebnem računu,
- vpogled v stanje na osebnem računu,
- sprememba PIN-številk,
- nakup GSM (franc. *Groupe Spécial Mobile*) kartic,
- vpogled v stanje na kreditnih karticah,
- naročilo za polog gotovine in
- naročilo za poravnavo plačilnih nalogov.

2.7 SKLEP

Kartično in POS-poslovanje že vrsto let zamenjuje gotovinsko in čekovno poslovanje. Uporabnik plačilne kartice je dolžan zagotoviti kritje na osebnem računu, na katerega je kartica vezana. V Sloveniji je temelje kartičnega poslovanja postavilo podjetje Activa, ki danes združuje dvanajst slovenskih bank in za katere izdaja domače in pomembne mednarodne plačilne kartice. Pri izdajanju in vročanju kartic uporabnikom morajo banke upoštevati posebne varnostne postopke, še posebej pri rokovanju s PIN-številkami. Kartice so torej zaščitene s PIN-i, mednarodne pa vsebujejo celo reliefni vtis podatkov o uporabniku ter številki kartice. Imajo hologram, dodatno pa imajo vtisnjeno še varnostno oznako MC. Uporabniki lahko z njimi poslujejo tudi na bankomatih in POS-terminalih. Naprave morajo delovati brezhibno, v primeru napake pri delovanju oz. kasnejšem servisiranju se morajo upoštevati točno določeni protokoli.

3 VARNOST KARTIČNEGA POSLOVANJA

Zlorabe plačilnih kartic so najpogostejše na bankomatih in pri spletnem nakupovanju, in sicer gre za izdelavo ponarejenih plačilnih kartic in zlorabo podatkov pri oddaljenih nakupih preko spleta. Goljufi ponarejene magnetne plačilne kartice uporabijo na prodajnih mestih ali bankomatih, pri oddaljenih nakupih pa jih uporabijo neposredno, pri tem pa včasih niti ne potrebujejo številke PIN.

3.1 VRSTE ZLORAB NA BANKOMATIH

Bankomat je naprava, ki je namenjena samopostrežnemu oskrbovanju strank z gotovino. Največ poskusov zlorab se zgodi na bankomatih in med najpogostejše spadajo tiste s t. i. »skimming napravo«, »libanonsko zanko« in zagozdo.

»Skimming« je nelegalen poizkus pridobivanja podatkov, ki so zapisani na magnetnem traku bančne kartice. Pogosto je povezan s snemanjem vnašanja PIN-kode. »Skimming naprava« je sestavljena iz čitalca magnetnega zapisa, ki kopira podatke iz bančne kartice na ustrezen medij. Na podlagi tega medija se bančne kartice kasneje klonirajo (naredijo identične kopije).

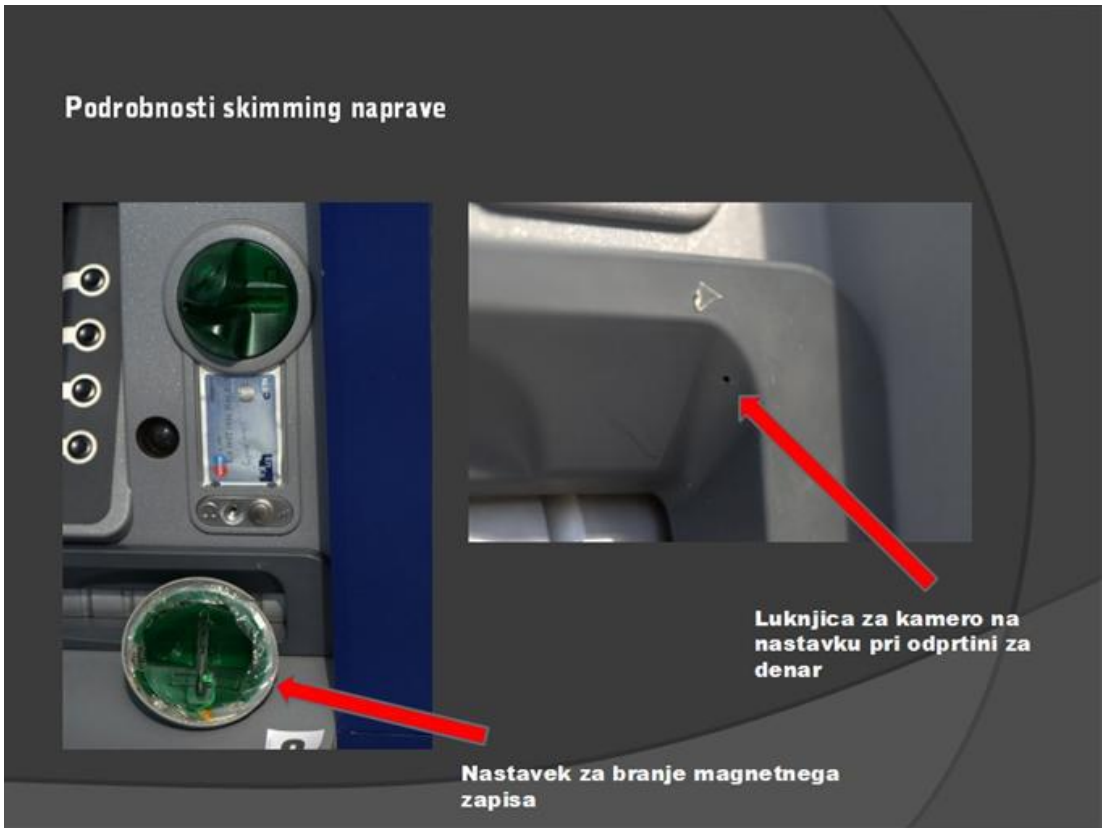
»Libanonska zanka« je tip zlorabe, pri kateri storilec zlorabe v čitalec bankomata namesti plastičen trak ali laks. S trakom ali laksom kartico zadrži v čitalcu, tako da je bankomat ne more več potisniti iz reže in s tem vrniti uporabniku. Ko stranka zapusti bankomat, storilec kartico potegne iz čitalca. Na enega od možnih načinov, kot je kamera, gledanje preko ramena, ogledala ali razgovora s stranko, pa pridobi še PIN.

Zagozda na reži za izplačilo gotovine je fizična ovira, ki jo namestijo storilci kaznivega dejanja in prepreči izplačilo gotovine. Po odhodu stranke, ki v tem primeru ne prejme gotovine, storilci kaznivega dejanja odstranijo nameščeno fizično oviro in protipravno vzamejo zagozdeno gotovino.

3.2 »SKIMMING NAPRAVA«

Naprava je običajno sestavljena iz dveh delov. Prvega sestavlja del, ki zajema podatke o magnetnem zapisu na bančni kartici. Gre za prenosni čitalec z vgrajenim pomnilnikom, ki lahko shrani več tisoč magnetnih zapisov, ne da bi ga bilo potrebno zamenjati. Ker odčitava magnetni zapis, je običajno nameščen nekje v bližini reže za vstavljanje kartic. Ponavadi se nahaja tik nad to odprtino, izdelan je tako, da se popolnoma prilega originani reži in ga je izredno težko opaziti. Je popolnoma enake barve in od originalne reže odstopa dva do tri milimetre (Walters, 2009).

Drugi del naprave je sestavljen iz dela, ki vizualno zajema PIN-številke bančnih kartic. Običajno gre za miniaturno kamero, ki je vgrajena nekje v bližini tipkovnice, na katero je seveda kamera usmerjena. Običajno je v tem delu izvrtana luknjica za mikro kamero, ki snema pritisnjene tipke ob vnosu PIN-številke (Walters, 2009).



Slika 3: »Skimming naprava«
(Vir: Gracer, 2011)

Gracer (2011) ugotavlja, da so bančne kartice vedno zlorabljene v tujini, kar kaže na to, da se s takšnimi dejanji ukvarjajo dobro organizirane in medsebojno povezane skupine posameznikov. Imajo dobro elektronsko opremo, ki jo uporabljajo za prenos podatkov in izdelavo ponarejenih kartic. Bančne kartice se običajno izdelajo v tujini, potem pa služijo za dvige na bančnih avtomatih in zlorabo na prodajnih mestih. Pri tem nastaja velika materialna škoda, ki doleti slovenske banke. Dejstvo je tudi, da mora takšna skupina delovati izredno hitro, predvsem od trenutka prve zlorabe naprej, saj slovenska družba Bankart d.d. pri spremljanju transakcij zelo hitro lahko ugotovi, da je bilo v tujini na določenem bankomatu ali POS-terminalu uporabljenih večje število slovenskih bančnih kartic. Bankart d.d. po ugotovitvi zlorabe takoj preveri, na katerih bankomatih v Sloveniji je dvigoval lastnik zlorabljene bančne kartice in prekliče vse bančne kartice, ki so bile v določenem času tam uporabljene.

3.3 »LIBANONSKA ZANKA«

Libanonska zanka je posebna naprava, ki jo zlikovec vstavi v režo bankomata in onemogoči, da bi bankomat vrnil plačilno kartico uporabniku. Uporabnik ne more do svoje kartice, kriminalec, ki je v bližini bankomata, pa mu ponudi pomoč, seveda z namenom, da bi izvedel številko PIN. Ko lastnik kartice po neuspelih poskusih, da bi prišel do kartice, odide, jo zlikovec izvleče in jo s pomočjo pridobljene številke PIN tudi enostavno uporabi. Sodobnejši bankomati praviloma zaznajo tovrstne naprave (Šavnik, 2008).

Ogorevčeva (2004) pojasnjuje, da je poskus tovrstne zlorabe precej nezahteven, saj storilci ne potrebujejo visoke tehnologije ali znanja. Kartico fizično ukradejo in ko izvedo še številko, v pičlih nekaj minutah pridejo do gotovine. Pri reži za čitalnik kartic je nameščena ovira oz. plastični vložek, ki bankomatu prepreči, da bi kartico vrnil. Kaj se zgodi, je odvisno od dolžine tega tujka. Bankomat se običajno zapre ali pa najprej opravi transakcijo, v vsakem primeru pa kartica ostane v njem. Običajno je na bankomatu nalepljeno obvestilo, domnevno od banke, naj uporabnik še večkrat odtipka PIN, včasih pa zraven stoji še nekdo, ki se predstavlja za bančnega delavca. Ta nič hudega slutečemu lastniku kartice predlaga, naj s kodo poskusi še večkrat, in seveda stoji zraven, da si lahko zapomni številke.

Slika 4: »Libanonska zanka«
(Vir: http://www.rtvslo.si/crna-kronika/pazite-se-libanonske-zanke/20805*)*

3.4 »CASH TRAPPING« ALI ZAGOZDA

»Cash Trapping« ali zagozda je še ena oblika zlorabe na bančnih avtomatih. Pri tem gre za t. i. past za gotovino. Storilci na režo za izdajanje denarja namestijo posebno letev, na kateri je lepilo oz. obojestranski lepilni trak, ki ovira izdajo gotovine, ta se zagozdi v reži. Dvig gotovine sicer poteka nemoteno, saj bankomat pozove uporabnika, naj vzame gotovino. A ker te ni, se ljudem dozdeva, da izplačilo ni mogoče zaradi tehnične okvare bankomata, in nič hudega sluteč odidejo.

Nepridipravi postopek opazujejo z varne razdalje. Po odhodu stranke se vrnejo k bankomatu, odstranijo posebej nameščeno režo, na katero se je ujela gotovina, in jo nelegalno prevzamejo (Felc, 2012).

Policija strankam v takšnih primerih svetuje pozornost pred uporabo bankomata. Stranke naj preverijo, ali je reža za izdajanje gotovine dostopna, saj je letev mogoče preprosto odstraniti. Če bankomat gotovine ne izplača, naj stranka preveri stanje na svojem računu. Policija še svetuje, naj uporabniki v primeru nepravilnosti s stopijo v stik s skrbnikom, ne da bi se od bankomata oddaljili, poleg tega pa naj bodo pozorni še na morebitne neznance, ki bi jih pod pretvezo nudenja pomoči želeli zvabiti s kraja dogodka (http://www.rtvslo.si/crna-kronika/past-za-gotovino-pozor-pred-novo-vrsto-goljufije-na-bankomatih/277302). Tovrstne zlorabe so v Sloveniji poleg »skimming naprav« v zadnjem času zelo pogoste.

3.5 POSTOPEK V PRIMERU ZLORABE NA BANKOMATIH

Banke natančno določajo postopek v primeru zlorabe na bankomatu v svojih internih pravilnikih, ki sledijo *Priporočilom za ravnanje bank v primeru suma zlorab na bančnih avtomatih in POS terminalih* z dne 23. 2. 2005. V primeru, da bančni delavec odkrije nameščeno napravo za zlorabo kartic na bankomatu ali pa ga na to opozori stranka, je postopek ravnanja sledeč (Navodila preverjanja namestitve in ukrepanja v primeru nameščenih naprav za izvajanje zlorab na bankomatih, 2012):

- po telefonu je takoj treba obvestiti policijo na telefonsko številko 113,
- okolico bankomata je treba zavarovati, kolikor je le mogoče. Strankam je treba pojasniti, da bankomata trenutno ni mogoče uporabljati. Naprave se ne sme nihče dotikati, da se ne bi uničili morebitni prstni odtisi,
- poklicati je treba delavce banke, ki so za to odgovorni, tudi če je to izven njihovega delovnega časa,
- o sumu nameščene naprave za izvajanje zlorab na bankomatu je treba čim prej obvestiti tudi servisno službo in se z njo dogovoriti za takojšen pregled bankomata,
- obvestiti je treba tudi Servisni center Activa.

Predanič (2011) pojasnjuje, da »skimming naprave« storilci nameščajo bolj ali manj na bankomate, na katerih je visoka frekvenca ljudi. Gre torej za centre večjih mest, nakupovalna središča ipd. Skrbi, da bi bila naprava v našem domačem kraju, so skoraj odveč, čeprav previdnost pri uporabi ostaja. Ko se nesporno ugotovi, da je prišlo do zlorabe bančne kartice, banke svojim komitentom denar povrnejo, o tem pa obvestijo tudi policijo.

3.6 PREVENTIVA PRED ZLORABAMI NA BANKOMATIH

Skrbniki bankomatov oz. njihovi namestniki, ki se nahajajo v poslovalnicah, so dolžni ob vsakem prihodu na delo in nato najmanj na dve uri ter ob odhodu z dela preveriti zunanjost bankomata. V poslovalnicah, ki so opremljene z bankomatom, poslovalnica pa ni skrbnik bankomata, morajo delavci preverjati zunanjost bankomata ob prihodu in odhodu z dela.

S strani banke za varnost poskrbijo skrbniki bankomatov in njihovi namestniki. Za našo varnost pa moramo seveda poskrbeti sami. Šavnik (2008) podaja splošne napotke za izboljšanje naše varnosti kartičnega poslovanja:

- ko dobite novo kartico, jo takoj podpišite,
- ko plačujete, imejte plačilno kartico vedno pri sebi. Ne izročajte je nikomur, temveč jo sami vstavite v terminal POS oz. jo potegnite prek čitalnika magnetnega zapisa,
- redno pregledujte bančne izpiske in preverite zabeležene transakcije, o nepravilnostih pa takoj obvestite banko,
- plačilne kartice, bančne izpiske in drugo občutljivo dokumentacijo po uporabi varno uničite (z rezalnikom ali s sežiganjem),
- kartice, ki niso več veljavne, uničite tako, da jih prerežete prek čipa in magnetnega zapisa,
- lahko uporabljate tudi storitev, ko boste s pomočjo sporočil SMS obveščeni o uporabi kartice, seveda če izdajatelj to omogoča. To je še posebej primerno, ko potujete v države, kjer so zlorabe pogoste,
- dokumente v papirni ali digitalni obliki, ki vsebujejo vaše osebne ali finančne podatke in jih želite zavreči, morate uničiti. Nikakor jih ne smete preprosto odvreči v koš za smeti, saj lahko pridejo v roke nepoklicanim, ki jih lahko zlorabijo za tatvino identitete,
- pri vnosu številke PIN stopite bližje k napravi in prekrijte številčnico s prosto roko ali pa se nadnjo nagnite s telesom,
- številke PIN nikoli ne zapišite in je nikomur ne povejte (niti policiji niti bančnim uslužbencem),
- ko dobite novo številko PIN, jo spremenite, če vam kombinacija številk ne ustreza,
- če na bankomatu ali terminalu POS opazite karkoli nenavadnega (poškodbe, dodatke), prekinite postopek in o tem obvestite prodajalca, banko ali policijo,
- pri uporabi plačilne kartice nikoli ne sprejmite pomoči neznancev,
- po opravljeni transakciji takoj pospravite denar, potrdilo in kartico, šele nato odidite,
- če bankomat iz neznanega razloga zadrži kartico, o tem takoj obvestite banko, lahko pa tudi policijo,

- ne dovolite, da bi trgovec kartico prek terminala ali celo tipkovnice potegnil več kot enkrat. Če pa se to zgodi, za vsak neuspešen poskus zahtevajte potrdilo o neuspeli transakciji.

Gracer (2011) pojasnjuje, da je naprava za presnemavanje magnetnega zapisa bančnih, kreditnih in drugih kartic oz. t. i. »skimming naprava« na bankomat običajno nameščena na način, ki je za uporabnike praktično neopazen. Obstaja majhna možnost, da uporabnik prepozna napravo, kadar odtenek barve naprave ni identičen barvi bankomata. Če torej uporabnik opazi, da se barvi reže za bančno kartico in reže za izdajo bankovcev ne ujemata in ob dotiku omenjenih delov začuti, da niso trdno pritrjeni na bankomat, nemudoma pokliče policijo, naprave pa naj se čim manj dotika. Deli naprav na bankomat običajno niso pritrjeni zelo trdno in lahko uporabniku ostanejo v rokah že ob malo močnejšem prijemu. Zato je priporočljivo, da si človek pred uporabo bankomata vzame sekundo časa in malo močneje prime za del, na katerem je reža za vstavitev bančne kartice ali reža za izdajo bankovcev. Bankomati so narejeni tako, da se pri tem ne bi smelo nič premakniti, če je nanj nameščena »skimming naprava«, pa bo ob močnejšem prijemu uporabniku skoraj zagotovo ostala v rokah. Obenem še pojasnjuje, da storilci »skimming napravo« pogosto prekrijejo z nalepkami varnostnih služb, bank ipd. Precej očitno pri tem je, da je na bankomatu nalepka kakšne tuje varnostne službe ali banke, kar pa uporabniki bankomata pogosto spregledajo.

Saranow Schultzeva (2010) opozarja tudi na lego in namestitev miniaturne kamere. Naprava mora posneti vnos kode PIN. Pri tem se pričakuje, da bo uporabnik svoje tipkanje prekril z roko. Zato je v večini primerov kamera nameščena diagonalno, pod zelo ostrim kotom, ki bo kljub prekritju z roko posnela tipkanje PIN-številke. Običajno je nameščena kar na dodatnem okvirju za izdajanje bankovcev. Pri natančnem pregledu bankomata bomo opazili majhno luknjico premera največ enega milimetra. Poleg miniaturne kamere v luknjici je eden izmed možnih načinov namestitve tudi prirejena tipkovnica, ki bo nalepljena čez originalno tipkovnico. Ob močnejšem prijemu bi se morala odlepiti. O tem naj uporabnik takoj obvesti policijo.

3.7 VARNOST SPLETNEGA NAKUPOVANJA

Na področju varnosti spletnega nakupovanja s karticami deluje sodobni varnostni mehanizem *MasterCard SecureCode*. V spletnih trgovinah, ki so podprte s takšnim mehanizmom, je pri plačilu s kartico treba poleg številke kartice vpisati še osemmestno številko, ki jo ustvari prenosni čitalec. Prenosni čitalec ustvari geslo, ki je enkratno, in potrdi avtentičnost nakupa. Čitalec je po določeni ceni mogoče kupiti v banki in je prenosljiv (Pravilnik o izdajanju plačilnih kartic, 2012).

Varni spletni nakup s karticami *Activa Maestro* in *Activa Mastercard* tako poteka v naslednjih korakih (Pravilnik o izdajanju plačilnih kartic, 2012):

- v spletni trgovini najprej izberemo izdelek, ki ga želimo kupiti,
- v spletni obrazec vnesemo podatke s svoje kartice in potrdimo plačilo,
- na spletni strani se bo pojavilo sporočilo banke o zahtevi po vpisu osemmestne naključne številke sistema *SecureCode*, ki jo bomo ustvarili s pomočjo prenosnega čitalca in kartice. Kartico najprej vstavimo v režo čitalca, na zaslonu se nam bo izpisalo »ACTIVA«, kjer nato izberemo možnost »P« in v polje pri tej možnosti vpišemo številko, ki se prikaže na spletni strani. Ti podatki spletnemu trgovcu niso vidni,
- številko dvakrat preverimo in potrdimo z »OK«,
- v čitalec nato vnesemo še svojo PIN-številko,
- v tem trenutku bo čitalec ustvaril tudi osemmestno številko *SecureCode*, ki jo vpišemo v za to namenjeno polje,
- kodo potrdimo, opravljena je avtentikacija, nakup je zaključen.

Spletnih trgovin je zaradi nižjih stroškov pri njihovem poslovanju vedno več, uporabniki pa se tudi počasi privajajo nanje. Šavnik (2008) opozarja na več nevarnosti za uporabnike pri spletnem nakupovanju:

- Pri lažnem predstavljanju nepridipravi pošiljajo lažna e-poštna sporočila, s katerimi pozivajo, naj uporabnik obišče določeno spletno mesto neke banke, v sporočilo pa je vključena tudi spletna povezava do nje. To spletno mesto je seveda ponarejeno, čeprav na prvi pogled deluje pristno. Uporabnik tako nevede nepridipravom posreduje svoje podatke o plačilni kartici.
- Podobno lažnemu predstavljanju je zvabljanje. Napadalci uporabnika preusmerijo na lažno spletno mesto, ki je na prvi pogled seveda pristno. Tudi v tem primeru uporabniki nevede posredujejo podatke o svoji plačilni kartici, vključno z uporabniškimi imeni in gesli.
- Škodljiva programska oprema, kot so trojanski konji, orodja za prevzem dostopa in programi, ki snemajo vse pritiske na tipkovnici, omogoča nepridipravom, da pridobijo vse podatke o plačilni kartici, ki jih potrebujejo za oddaljene nakupe.
- Lažne spletne strani po ugodnih cenah ponujajo različne mikavne izdelke, do katerih uporabnik pride preko določenih spletnih povezav, ki mu jih kriminalci pošljejo v neželeni e-pošti.
- Lažne prodaje so tudi po telefonu, ko nas pokliče neznanec, ki opravlja lažno prodajo. Preko telefona skuša priti do naših podatkov, ki bi mu omogočili nadaljnje nakupe.
- »Hekersko« vdiranje v baze podatkov e-trgovcev je vse bolj popularno, saj nekateri trgovci zaradi svoje nepoučenosti in nestrokovnosti shranjujejo podatke o plačilnih karticah in s tem močno izpostavljajo svoje stranke. »Hekerji« uspejo prodreti v njihove baze podatkov o kupcih in prekopirati podatke o plačilnih karticah.

Šavnik (2008) podaja tudi nekaj nasvetov za zaščito pred zlorabo pri spletnem nakupovanju:

- zaupajte le tistim spletnim stranem in prodajalcem, ki od vas zahtevajo varnostno številko kartice,
- ne kupujte na spletnih straneh, do katerih ste prišli s pomočjo spletnih povezav, ki ste jih dobili v neželeni elektronski pošti ali pa so vas poklicali po telefonu,
- pri oddaljenih nakupih nikoli ne vpisujte PIN-številke, saj ta ni potrebna,
- natisnite spletno stran z oddanim naročilom in pogoji poslovanja in dostave ter prodajalčevimi kontaktnimi podatki,
- pri izbiri trgovca dajte prednost tistim, ki omogočajo uporabo varnostnih storitev (takšna sistema sta *SecureCode* na sliki 5 in varnostni sistem *Verified by Visa*),
- če pogosto opravljate oddaljene nakupe, je smiselno uporabljati le eno bančno kartico, ki je namenjena izključno temu.

Slika 5: Logotip SecureCode
(Vir*:* http://www.activa.si/)

3.8 ZAVAROVANJE ZLORABE IZGUBLJENE ALI ODVZETE KARTICE PRI BANKI X

Uporabniki plačilnih kartic se lahko odločijo za individualno zavarovanje v primeru zlorabe kartice. Zavarovanje se lahko ponudi vsem uporabnikom plačilnih kartic, ki so fizične osebe in izpolnjujejo interna pravila kartičnega poslovanja pri Banki X. Pri zavarovanju je zavarovanec oseba, katere premoženje oz. premoženjski interes je zavarovan.

V zavarovanje pri Banki X so vključeni naslednji riziki z določenimi limiti zavarovalnega kritja, skladno s *Posebnimi pogoji za zavarovanje imetnika kartice* (Navodila za izdajanje plačilnih kartic, 2012):

- Škoda, ki jo utrpi uporabnik plačilne kartice na osebnem računu zaradi zlorabe izgubljene ali protipravno odvzete kartice s strani tretje osebe, ko gre za tatvino, drzno tatvino, vlom, rop ali roparsko tatvino. Limit zavarovalnega

kritja po posamezni kartici in škodnem dogodku je 150 EUR, limit za vse kartice, ki jih uporabnik zavaruje, pa 1.000 EUR. 150 oz. 1.000 EUR je maksimalni znesek škode, ki ga krije zavarovalnica po pogodbi z Banko X, vendar le, če je uporabnik s kartico ravnal v skladu s pravili poslovanja.

- Protipravno odvzeta gotovina uporabniku kartice, če je do odvzema prišlo v eni uri po dvigu gotovine na banki ali bančnem avtomatu. Limit zavarovalnega kritja po škodnem dogodku in na leto je 200 EUR.
- Stroški zamenjave osebnih predmetov (dokumentov, ključev, torbice, denarnice), ki jih utrpi uporabnik kartice, če so bili hkrati s kartico odvzeti tudi njegovi osebni dokumenti. Limit zavarovalnega kritja za zamenjavo ključev in ključavnic je 200 EUR, za zamenjavo osebnih dokumentov 100 EUR, za nakup nove torbe ali denarnice pa je limit 100 EUR.
- Strošek klicev, ki jih opravi tretja oseba z uporabnikovega mobilnega telefona, če je hkrati s kartico odvzet tudi njegov mobilni telefon. Limit zavarovalnega kritja v tem škodnem dogodku pri Banki X je 100 EUR na leto.

Uporabnik plačilne kartice sklene zavarovanje tako, da podpiše računalniško (in ne ročno) izpolnjeno *Pristopno izjavo k zavarovanju imetnika kartice* in plača letno premijo na način direktne obremenitve s svojega računa. Obrazec se nato natisne v treh izvodih, in sicer en izvod za stranko, drugega hrani poslovalnica, tretji pa se pošlje zavarovalnemu posredniku. Na pristopno izjavo se mora podpisati tudi delavec, ki je zavarovanje sklepal. Pristopno izjavo lahko podpisujejo le delavci s pridobljenim dovoljenjem AZN (Agencije za zavarovalni nadzor) ter pri nazivu dopišejo še besedo »za«. Ob podpisu izjave mora bančni delavec uporabnika seznaniti o zavarovalnih pogojih, po katerih je zavarovanje sklenjeno (Navodila za izdajanje plačilnih kartic, 2012).

V pristopni izjavi so navedeni podatki o uporabniku kartice oz. zavarovancu in po potrebi tudi o zavarovalcu, če ni ta oseba hkrati zavarovanec, podatki o osebnem računu, limiti zavarovalnega kritja, letna zavarovalna premija ter način in datum plačila zavarovalne premije. Uporabnik kartice nato podpiše *Pooblastilo banki za odpiranje direktne obremenitve*, s katerim se bo znesek uporabniku odtegnil z računa (Navodila za izdajanje plačilnih kartic, 2012).

Zavarovanje uporabnika se sklene za dobo enega leta in se vsako leto avtomatično podaljšuje. Če je zavarovanje prenehalo zaradi odpovedi zavarovanja, odvzete kartice, zaprtega ali blokiranega računa ipd., banka to sporoči zavarovalnici, da se za to zavarovanje ne pošiljajo več direktne obremenitve.

Zavarovanec ima ob zavarovalnem primeru pri Banki X naslednje dolžnosti (Navodila za izdajanje plačilnih kartic, 2012):

- imetnik kartice je dolžan takoj po dogodku izgubo ali protipravni odvzem kartice prijaviti banki v času in na način, ki je naveden v bančnih pogojih poslovanja s kartico,
- v primeru protipravnega odvzema kartice ali osebnih predmetov je zavarovanec dolžan to takoj prijaviti tudi policiji. Iz njegove prijave mora biti razvidno, kateri osebni predmeti so bili imetniku odvzeti,
- v primeru protipravnega odvzema mobilnega telefona mora zavarovanec to takoj prijaviti tudi mobilnemu operaterju, da onemogoči vse klice,
- zavarovanec prijavi zavarovalni primer Banki X tudi pisno na obrazcu *Prijava zavarovalnega primera – zavarovanje imetnika kartice* z navedbo škodnega dogodka,
- zavarovanec je dolžan prijaviti zavarovalni primer najkasneje v tridesetih dneh od dneva, ko je banki prijavil izgubo ali protipravni odvzem kartice.

3.9 SKLEP

Zlorabe s plačilnimi karticami so najpogostejše na bankomatih in pri spletnem nakupovanju. »Skimming naprava«, »libanonska zanka« in zagozda so najbolj znani primeri zlorab na bankomatih. Banke imajo v takšnem primeru zlorabe natančno določene postopke kako ravnati, o tem morajo obvestiti policijo, servisno službo in Servisni center Activa. V primeru, ko je zloraba nesporno ugotovljena, banke svojim komitentom povrnejo denar. Skrbniki zato bankomate redno pregledujejo, za svojo varnost pri tovrstnem poslovanju pa moramo seveda poskrbeti tudi sami. Avtorji pri tem dajejo različne napotke.

Pri spletnem nakupovanju obstaja več vrst nevarnosti, kot so lažna spletna mesta, škodljiva programska oprema, lažne prodaje po telefonu in »hekerski« vdori, s katerimi zlikovci pridejo do podatkov o plačilnih karticah. Pred zlorabami se lahko zaščitimo z uporabo varnostnih sistemov, kot sta npr. *MasterCard SecureCode* in *Verified by Visa.*

Banke običajno ponujajo tudi zavarovanje zlorabe izgubljene ali protipravno odvzete kartice. Pri tem moramo biti pozorni na limite in posebne pogoje zavarovanja, ki jih določena banka ponuja.

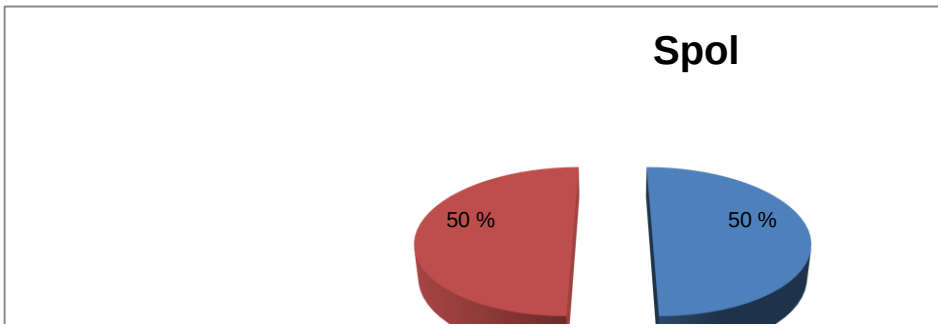
4 EMPIRIČNI DEL

4.1 VZOREC IN OBDELAVA ODGOVOROV

Z anketnim vprašalnikom (priloga 1) smo raziskali osveščenost uporabnikov o varni uporabi bančnih kartic. Anketirali smo petdeset komitentov Banke X. Anketni vprašalnik je kombinacija zaprtih, polodprtih in odprtih vprašanj, kjer so anketiranci odgovore obkrožili ali pa dopisali. Pred anketiranjem smo si zastavili šest delovnih hipotez, ki smo jih po obdelavi odgovorov potrdili, delno potrdili ali ovrgli. Odgovore smo predstavili v tabelah in grafih, kjer smo ponazorili deleže odgovorov v številu in odstotkih. Najprej sta nas zanimala spol in starost.

Spol	Število	Odstotek
ženski	25	50
moški	25	50
Skupaj	50	100

Tabela 1: Spol
(Vir: Lasten)

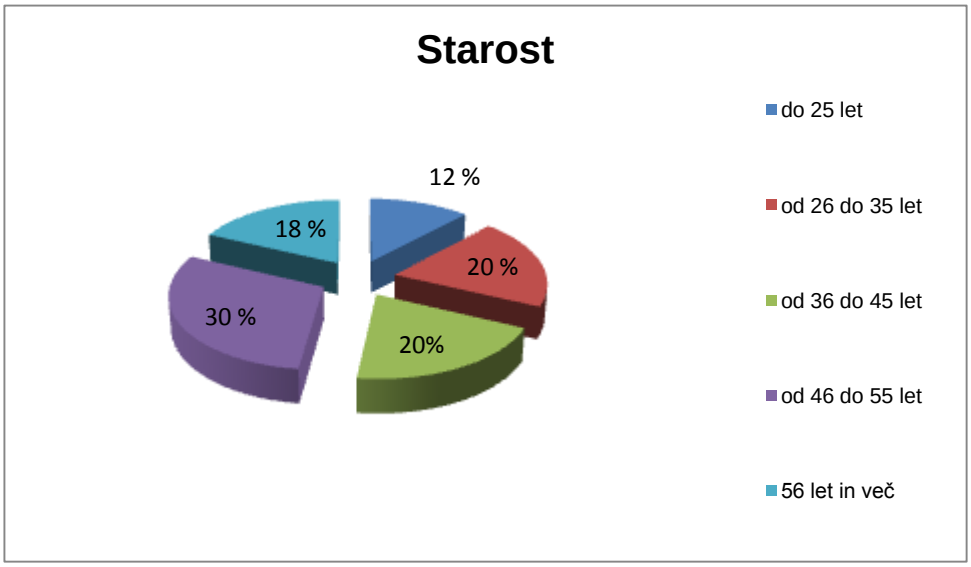


Graf 1: Spol
(Vir: Lasten)

Polovica anketirancev je ženskega in polovica moškega spola. Spola sta bila v naši anketi torej enako zastopana.

Starostna skupina	Število	Odstotek
do 25 let	6	12
od 26 do 35 let	10	20
od 36 do 45 let	10	20
od 46 do 55 let	15	30
56 let in več	9	18
Skupaj	50	100

Tabela 2: Starost
(Vir: Lasten)



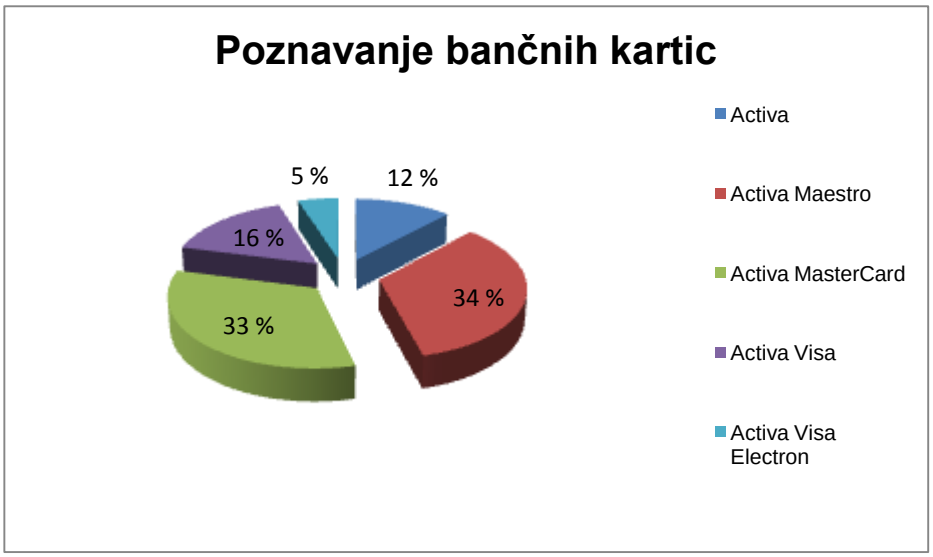
Graf 2: *Starost*
(Vir: Lasten)

Največ komitentov Banke X, ki smo jih anketirali, spada v starostno skupino od 46 do 55 let.

V anketi nas je v nadaljevanju zanimalo, koliko anketirani komitenti Banke X sploh poznajo vrste bančnih kartic. Pri tem so lahko obkrožili enega ali več odgovorov. Vseh obkroženih odgovorov je bilo 137, pri tem pa nas je zanimal predvsem delež poznavanja posamezne bančne kartice v odstotkih.

Vrsta bančne kartice	Število	Odstotek
Activa	17	12
Activa Maestro	46	34
Activa MasterCard	45	33
Activa Visa	22	16
Activa Visa Electron	7	5
Activa Obrtnik OZS	0	0
Skupaj	137	100

Tabela 3: *Poznavanje bančnih kartic*
(Vir: Lasten)



Graf 3: *Poznavanje bančnih kartic*
(Vir: Lasten)

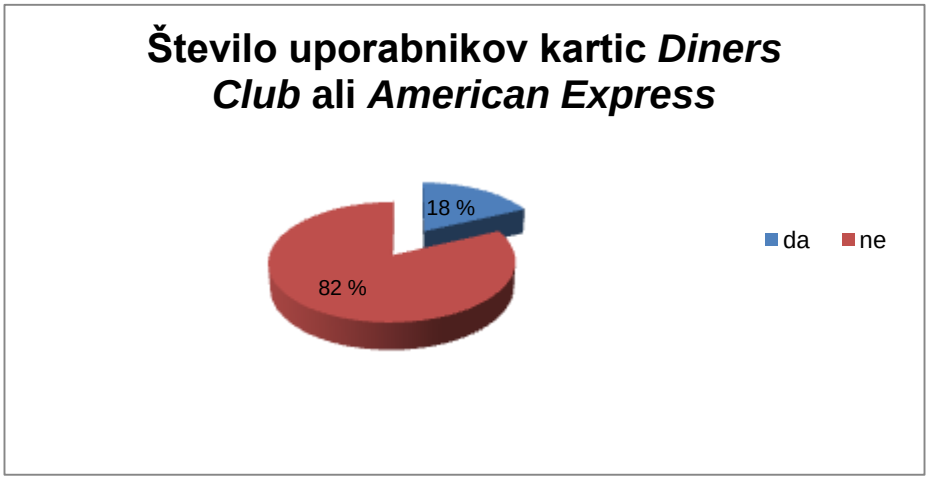
Anketirani komitenti Banke X najbolje poznajo plačilno kartico *Activo Maestro* in kreditno kartico *Activo MasterCard*. Komitenti ne poznajo dobro kreditne kartice *Activa Visa*, kar je presenetljivo, saj jo v plačilo sprejemajo vsa prodajna mesta, ki so opremljena s POS-terminali, z njo je možen dvig na bankomatih in je ena od

glavnih plačilnih sredstev tudi preko spleta. Razlog je verjetno treba iskati v ponudbi bančnih kartic Banke X, anketirali smo namreč samo njene komitente.

Naslednje vprašanje v anketi se je nanašalo na število uporabnikov kartic *Diners Club* ali *American Express*. Anketirance smo vprašali, ali uporabljajo tudi ti dve vrsti plačilnih kartic, lahko so obkrožili odgovor »da«, kar je pomenilo, da uporabljajo vsaj eno od teh dveh oz. »ne«, če ne uporabljajo nobene.

Število uporabnikov	Število	Odstotek
da	9	18
ne	41	82
Skupaj	50	100

Tabela 4: Število uporabnikov kartic Diners Club ali American Express
(Vir: Lasten)



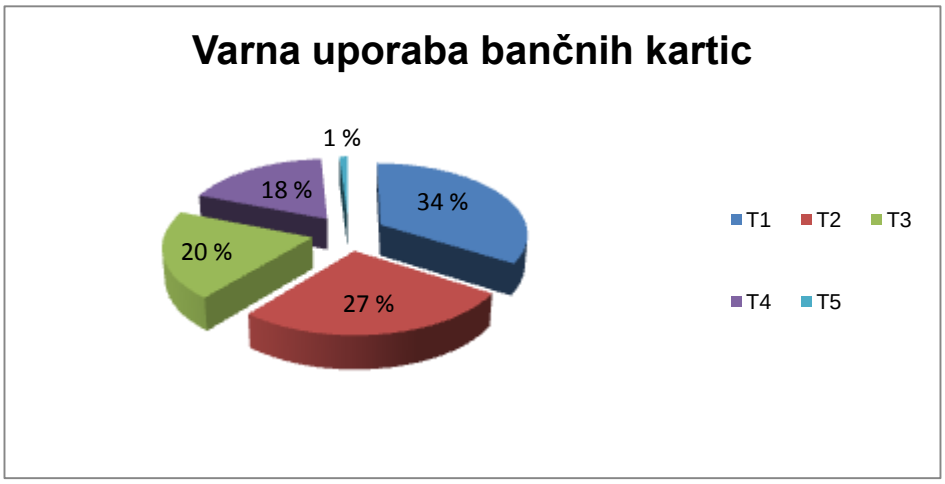
Graf 4: *Število uporabnikov kartic Diners Club ali American Express*
(Vir: Lasten)

Večina anketiranih komitentov Banke X ne uporablja plačilnih kartic, kot sta *Diners Club* ali *American Express*.

V petem vprašanju smo anketirane komitente Banke X vprašali, kaj pomeni varna uporaba bančnih kartic. Zopet so lahko obkrožili več odgovorov, ki so bili oblikovani kot trditve od T1 do T5, ali pa so sami dopisali tisto, kar se jim je zdelo pomembno za varno uporabo. Dobili smo 143 obkroženih odgovorov, od teh je le eden dopisal svoje mnenje o varni uporabi bančnih kartic.

Trditev	Število	Odstotek
T1: varovanje osebne identifikacijske številke kartice (PIN)	49	34
T2: pri dvigovanju gotovine na bankomatu z roko prekrijemo odtipkavanje PIN-a	39	27
T3: pred nakupovanjem na spletu se prepričamo o varnosti spletne strani	28	20
T4: svoje plačilne kartice ne posojamo drugim osebam	26	18
T5: drugo	1	1
Skupaj	143	100

Tabela 5: *Varna uporaba bančnih kartic*
(Vir: Lasten)



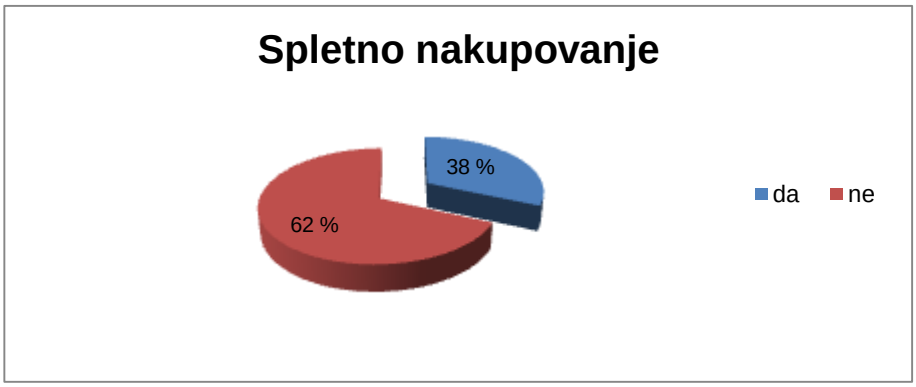
Graf 5: *Varna uporaba bančnih kartic*
(Vir: Lasten)

Uporabnikom bančnih kartic se zdi najpomembneje varovati identifikacijske številke svoje kartice. Pri tem so najbolj poudarili, da pri tipkanju svojega PIN-a z roko prekrijemo odtipkavanje. Le en anketirani je dopisal, da svojega PIN-a nikoli ne beležimo na manjši list papirja ali ga prenašamo v denarnici poleg bančne kartice.

Šesto vprašanje v anketi se je nanašalo na spletno nakupovanje. Zanimal nas je odstotek tistih, ki so že nakupovali preko spleta. Anketirani komitenti so obkrožili »da«, če so že kadarkoli nakupovali preko spleta, oz. »ne«, če niso še nikoli.

Spletno nakupovanje	Število	Odstotek
da	19	38
ne	31	62
Skupaj	50	100

Tabela 6: *Spletno nakupovanje*
(Vir: Lasten)



Graf 6: *Spletno nakupovanje*
(Vir: Lasten)

Nekaj več kot polovica anketiranih še ni nakupovala preko spleta, skoraj polovica pa je to že storila.

V sedmem vprašanju nas je zanimalo, ali anketirani komitenti poznajo zavarovanja pred zlorabami bančnih kartic, ki jih ponujajo različne banke. Zopet sta bila podana enostavna odgovora »da« in »ne«.

Poznavanje zavarovanj	Število	Odstotek
da	18	36
ne	32	64
Skupaj	50	100

Tabela 7: *Poznavanje zavarovanj pred zlorabami bančnih kartic*
(Vir: Lasten)

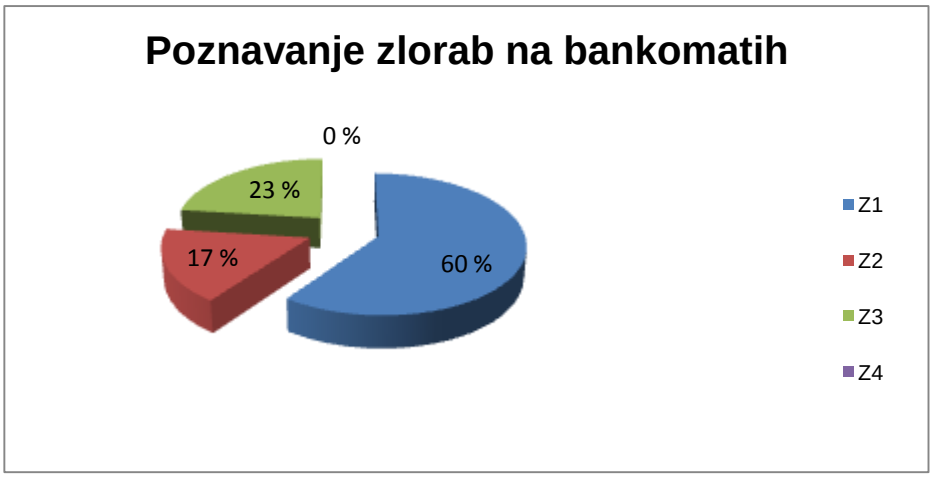
Graf 7: *Poznavanje zavarovanj pred zlorabami bančnih kartic*
(Vir: Lasten)

Komitenti Banke X, ki smo jih anketirali, po večini še ne poznajo zavarovanj pred zlorabami bančnih kartic. Vendar odstotek tistih, ki ta zavarovanja poznajo, ni zanemarljiv, kar nam pove, da so anketirani dokaj osveščeni o zlorabah.

Najpogostejše so seveda zlorabe na bankomatih, zato smo anketirane v osmem vprašanju povprašali, katere vrste zlorab na bankomatih poznajo. Obkrožili so lahko več odgovorov, kar je pomenilo, da poznajo več vrst zlorab. Med odgovore smo zapisali tri vrste zlorab (od Z1 do Z3), četrti odgovor (Z4) pa je dopuščal možnost, da sami na kratko opišejo vrsto zlorabe. Dobili smo 70 obkroženih odgovorov, nihče pa ni dopisal kakšne druge vrste zlorabe.

Vrsta zlorabe	Število	Odstotek
Z1: »skimming naprava« prebere magnetni zapis na kartici in vizualno zajame PIN številko	42	60
Z2: pri »libanonski zanki« bankomat ne vrne kartice in ne izda denarja	12	17
Z3: »Cash Trapping« ali zagozda, kjer se na bankomatu izpiše, da denar lahko vzamete, a ga ne morete	16	23
Z4: drugo	0	0
Skupaj	70	100

Tabela 8: Poznavanje zlorab na bankomatih
(Vir: Lasten)



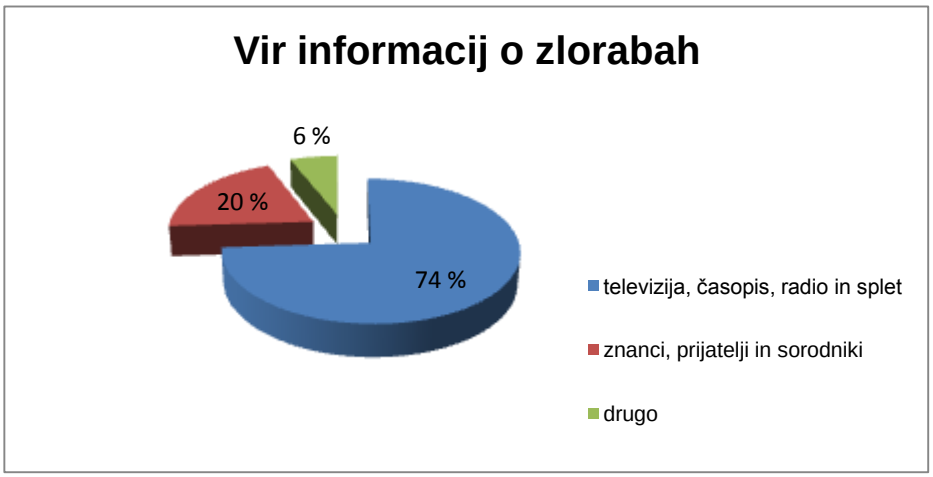
Graf 8: *Poznavanje zlorab na bankomatih*
(Vir: Lasten)

Anketirani zelo dobro poznajo »skimming napravo«, ki prebere magnetni zapis na kartici, PIN-številko pri tej zlorabi pa zlikovci zajamejo preko miniaturne kamere. Verjetno lahko sklepamo, da je to ena najpogostejših zlorab na bankomatih in jo anketirani zato tudi dobro poznajo.

V devetem vprašanju nas je zanimalo še, iz katerega medija so najpogosteje seznanjeni o zlorabah z bančnimi karticami. Podali smo tri možne odgovore, obkrožili pa so lahko le enega. Tretji odgovor je predstavljala možnost, da dopišejo vir, ki ga mi sami nismo zavedli med odgovore.

Vrsta medija	Število	Odstotek
televizija, časopis, radio in splet	37	74
znanci, prijatelji in sorodniki	10	20
drugo	3	6
Skupaj	50	100

Tabela 9: *Vir informacij o zlorabah*
(Vir: Lasten)



Graf 9: Vir informacij o zlorabah
(Vir: Lasten)

Mediji, kot so televizija, radio, časopis in splet so najpogostejši viri, preko katerih anketirani izvedo za informacije o zlorabah bančnih kartic. Dva anketirana sta kot vir informacij o zlorabah navedla svojo službo, eden pa je izpostavil svojo lastno izkušnjo.

Zadnje, deseto vprašanje, je bilo odprtega tipa. Zanimalo nas je, če so anketirani že doživeli zlorabo svoje bančne kartice. Če so zlorabo že doživeli, smo jih prosili, naj svojo izkušnjo opišejo. Dva anketirana sta svojo izkušnjo opisala. Prva je zapisala »*plačilno kartico so mi posneli na bankomatu pred Mercatorjem v Kranju – kartico so mi blokirali, vendar ni bila zlorabljena*« (Anketni vprašalnik, 10. vpr., 2013). Anketirana oseba je še dopisala »*Eurocard so mi zlorabili na ta način, da so z njo na Novi Zelandiji dvignili 2.500,00 EUR, čeprav tam še nikoli nisem bila*« (Anketni vprašalnik, 10. vpr., 2013).

Druga anketirana oseba je zapisala »*Mislim, da ne. Sem pa večkrat v dilemi, kako varno je vse skupaj, predvsem plačilo preko spleta in v tujini*« (Anketni vprašalnik, 10. vpr., 2013).

4.2 HIPOTEZE

Pri raziskovanju varnosti kartičnega poslovanja smo se osredotočili tudi na to, koliko uporabniki za varnost poskrbijo sami. Zastavili smo si naslednjih šest hipotez, ki smo jih potrdili, delno potrdili ali ovrgli.

- **H1**: Stranke dobro poznajo vrste bančnih kartic.
- **H2**: Stranke poznajo varno uporabo bančnih kartic.
- **H3**: Po večini so že vsi anketirani kupovali preko spleta.

- **H4**: Stranke poznajo možnosti zavarovanja pred zlorabo bančnih kartic v Banki X.
- **H5**: Stranke poznajo primere zlorab z bančnimi karticami.
- **H6**: Za zlorabo z bančnimi karticami so najpogosteje seznanjeni iz medijev.

***H1**: Stranke dobro poznajo vrste plačilnih kartic.*

Stranke Banke X zelo dobro poznajo plačilno kartico *Activa Maestro* in kreditno kartico *Activa MasterCard*, ne poznajo pa dobro kreditne kartice *Activa Visa*, še manj *Viso Electron*, nihče pa ne pozna *Active Obrtnik OZS*. Le 18 % vprašanih uporablja plačilno kartico *Diners Club* ali *American Express*. Hipoteze zato ne potrjujemo, stranke namreč ne poznajo dobro vseh vrst bančnih kartic, ki so na voljo v slovenskem prostoru.

***H2**: Stranke poznajo varno uporabo plačilnih kartic.*

Anketirane stranke Banke X so najbolj poudarile varovanje osebne identidikacijske številke PIN, kar je seveda pri varnosti kartičnega poslovanja eden najpomembnejših dejavnikov. Pri dvigovanju gotovine na bankomatih so poudarile, da je tipkanje PIN-številke na tipkovnici potrebno prekriti s svojo roko. Hipotezo zato potrjujemo, saj je varovanje PIN-številke ključnega pomena za varnost kartičnega poslovanja.

***H3**: Povečini so že vsi anketirani nakupovali preko spleta.*

Rezultat ankete je pokazal, da je le 38 % vprašanih že nakupovalo preko spleta. Hipoteze zato ne potrjujemo, vendar moramo pri tem poudariti, da so vprašani komitenti spadali povečini v starostno skupino od 46 do 55 let, ki verjetno ne uporablja pogosto takšnega načina nakupovanja.

***H4**: Stranke poznajo možnosti zavarovanja pred zlorabo bančnih kartic v Banki X.*

Večina anketiranih komitentov Banke X ne pozna tovrstnih zavarovanj, zato hipoteze ne potrjujemo. Na tem mestu obenem poudarjamo, da bi bilo komitente Banke X smiselno obveščati o vrstah in možnostih zavarovanj pred takšnimi zlorabami.

***H5**: Stranke poznajo primere zlorab z bančnimi karticami.*

Stranke zelo dobro poznajo »skimming napravo«, slabo pa poznajo t. i. libanonsko zanko in zagozdo. Zadnji dve metodi prevare sta že dokaj zastareli, zelo pogosto zlorabo v zadnjem času, t. i. zlorabo s »skimming napravo«, pa stranke poznajo dobro. Zato hipotezo vseeno delno potrjujemo.

***H6**: Za zlorabo z bančnimi karticami so najpogosteje seznanjeni iz medijev.*

Hipotezo v celoti potrjujemo, saj so komitenti Banke X najpogosteje seznanjeni o zlorabah iz medijskih virov, kot so televizija, časopis, radio in splet. Le majhen del vprašanih je navedlo za glavni vir informacij o zlorabah znance, prijatelje, sorodnike ali svojo službo.

4.3 SKLEP

Komitenti Banke X zelo dobro poznajo plačilno kartico *Activo Maestro* in kreditno kartico *Activo MasterCard*, ostale vrste bančnih kartic poznajo zelo slabo. Razlog za to je treba verjetno iskati v sami ponudbi bančnih kartic, ki jih ponuja Banka X.

Anketirane stranke so poudarile, da je previdnost pri uporabi tovrstnih kartic ključnega pomena za varnost kartičnega poslovanja. Zlorabe, ki so v zadnjem času najpogostejše, zelo dobro poznajo. O njih se seznanjajo predvsem iz medijev, kot so časopis, radio, televizija in splet. Naš predlog Banki X na tem mestu je, da se osredotoči na obveščanje svojih komitentov o možnostih zavarovanj pred takšnimi zlorabami. Za to ima na voljo več medijev, izbere naj tistega, ki ga trenutno pogosto uporablja za namene obveščanja (mobilni telefoni, tiskana sporočila, objave na svojih spletnih straneh ipd.).

5 ZAKLJUČKI

Temelje kartičnega poslovanja v Sloveniji je postavilo podjetje Activa, ki danes združuje dvanajst slovenskih bank, za katere izdaja domače in pomembne mednarodne bančne kartice. Uporabniki lahko z njimi poslujejo v bankah, na bankomatih in POS-terminalih. PIN-številka je bistvena za varnost kartičnega poslovanja med uporabniki, mednarodne bančne kartice pa so še dodatno zaščitene z reliefnim vtisom podatkov o uporabniku, hologramom, kreditna kartica *MasterCard* vsebuje celo varnostno oznako MC.

Zlorabe bančnih kartic so najpogostejše na bankomatih in pri spletnem nakupovanju, na bankomatih v zadnjem času nelegalno nameščena »skimming naprava«, med zlorabami na spletu pa so najpogostejše lažno spletno mesto, škodljiva programska oprema, lažna prodaja po telefonu in »hekerski« vdor. Bistvo vseh teh prevar je nezakonita pridobitev podatkov o uporabniku kartice, s pomočnjo katerih se mu kasneje protipravno odvzame denar z njegovega bančnega računa.

Komitenti Banke X, ki smo jih anketirali, zelo dobro poznajo plačilno kartico *Activo Maestro* in *Activo MasterCard*. Zavedajo se, da je za varnost kartičnega poslovanja varovanje PIN-številke ključnega pomena. Pri dvigovanju gotovine na bankomatih

običajno tipkanje PIN-a prekrijejo z roko, pred nakupovanjem na spletu se prepričajo o varnosti spletne strani. Svoje bančne kartice ne posojajo drugim osebam, PIN številke pa ne nosijo napisane na manjšem listu papirja v denarnici. Dobro so seznanjeni z najpogostejšo zlorabo na bankomatih, tj. napravo, ki prebere magnetni zapis na kartici. Večina jih še ni nakupovala preko spleta. Razlogi za to so sicer lahko različni, eden je zagotovo ta, da je bila povprečna starost anketirancev razmeroma visoka, drugi razlog pa je lahko tudi nezaupanje v spletno nakupovanje, kar pa je sicer izrecno poudaril le en anketiranec. Glavni vir informacij o zlorabah so mediji, kot so televizija, radio, časopis in splet. Možnosti zavarovanj pred zlorabami nikakor ne poznajo dobro, zato se bo naš predlog za nadaljnji razvoj Banke X vsekakor nanašal na osveščanje uporabnikov o možnostih takšnega zavarovanja.

5.1 MOŽNOSTI NADALJNEGA RAZVOJA

Stranke Banke X se torej dobro zavedajo, da so zlorabe v kartičnem poslovanju vse pogostejše, poznajo sicer načine, kako se pri ravnanju z bančnimi karticami lahko zaščitijo, vendar tudi njihovo prizadevanje včasih ni dovolj. Stranke Banke X bi bilo zato potrebno intenzivneje obveščati o možnostih zavarovanj, ki jih Banka X ponuja.

Uporabnik plačilne kartice *Activa Maestro* ali *Activa MasterCard* se torej v Banki X lahko odloči za individualno zavarovanje za primer zlorabe kartice. Banka X ima v ta namen sklenjeno pogodbo z določeno zavarovalnico. S takšnim zavarovanjem so krita vsa plačila ali dvigi gotovine s strani tretjih oseb, ki nastanejo v času, ko zavarovanec nosi riziko zlorabe skladno z bančnimi pogoji poslovanja s kartico. Banka X krije nastalo škodo največ štirinajst dni pred prijavo izgube ali protipravnega odvzema kartice. V zavarovalno kritje so vključena kritja, kot so zloraba kartice s strani tretjih oseb, protipravni odvzem gotovine, stroški zamenjave osebnih predmetov in stroški klicev z mobilnega telefona. Za vsako vrsto kritja se določi najvišji limit, ki ga banka še pokrije. Stranke morajo tovrstna zavarovanja dobro preučiti, zato bi bilo smiselno zgolj obveščanje komitentov o možnostih tovrstnih zavarovanj.

Presenetil nas je tudi rezultat ankete o spletnem nakupovanju. Stranke povečini še niso nakupovale preko spleta, razlogov za to je lahko veliko. Število spletnih kupcev narašča, to postaja vse bolj vsakdanji način nakupovanja med uporabniki plačilnih kartic, zato predlagamo, da se komitente intenzivno obvešča tudi o možnostih varnega spletnega nakupovanja. Pri izbiri trgovca naj dajo prednost tistim, ki omogočajo uporabo varnostnih storitev, kot je *SecureCode*, ki ga podpira kartični sistem *MasterCard*.

LITERATURA IN VIRI

Literatura

Gracer, D. (2011). *Skimming naprave v Sloveniji*. Maribor: Fakulteta za varnostne vede.

Kodrič, T. (2010). *Načrtovanje in uvajanje elektronskega poslovanja s poudarkm na internetnem bančništvu.* Diplomsko delo, Maribor: Univerza v Mariboru, Ekonomsko-poslovna fakulteta.

Mejač Krassnig, A. (2008). *Kartično poslovanje.* Izobraževalni center Združenje bank Slovenije, str. 1–20.

Novak, P. (2009). *Elektronsko bančništvo in kartično poslovanje.* Diplomsko delo, Maribor: Univerza v Mariboru, Ekonomsko-poslovna fakulteta.

Šavnik, J. (2008). *Varnost brezgotovinskega poslovanja.* Ljubljana: Zveza potrošnikov Slovenije.

Članki

Črničovič Krofič, V. (1995). Sodobni načini poravnavanja obveznosti v prometu blaga in storitev. *Pravna praksa* 332, stran 15.

Spletni viri

Activa. Pridobljeno 19. 4. 2013 z naslova *http://www.activa.si/*.

Bankart.si. Pridobljeno 7. 5. 2013 z naslova *http:/www.bankart.si/si/ponudba/upravljanje_mreze_bankomatov/.*

Bobek, S. (2003). *Informatika v bankah.* Pridobljeno 10. 5. 2013 z naslova *http://epf-oi.uni.mb.si/clani/bobek/FI/ISStoritve.pdf.*

Felc, M. (26. 2. 2012). Goljufi stalno iščejo pomankljivosti. *Dnevnik.* Pridobljeno 25. 4. 2013 z naslova *http://www.delo.si/novice/slovenija/goljufi-stalno-iscejo-pomanjkljivosti.html*.

Gorenjska banka, d.d., Kranj. Pridobljeno 8. 5. 2013 z naslova *http://www.gbkr.si/osebne-finance/bankomat-4216/.*

Ogorevc, M. (8. 7. 2004). »Libanonska zanka« tudi v Sloveniji. *Dnevnik*. Pridobljeno 20. 5. 2013 z naslova *http://www.dnevnik.si/kronika/88437*.

Past za gotovino – pozor pred novo vrsto goljufije na bankomatih. (21. 2. 2012). Ljubljana: MMC RTV SLO. Pridobljeno 19. 5. 2013 z naslova *http://www.rtvslo.si/crna-kronika/past-za-gotovino-pozor-pred-novo-vrsto-goljufije-na-bankomatih/277302*.

Pazite se libanonske zanke. (8. 7. 2004). Ljubljana: MMC RTV SLO. Pridobljeno 20. 5. 2013 z naslova *http://www.rtvslo.si/crna-kronika/pazite-se-libanonske-zanke/20805*.

Predanič, J. (12. 8. 2010). Banka žrtvam povrne denar. *Delo, kronika.* Pridobljeno 2. 5. 2013 z naslova *http://www.delo.si/gospodarstvo/makromonitor/banka-zrtvam-povrne-denar.html*.

Saranow Schultz, J. (7. 12. 2011). How to spot an A. T. M. Skimmer. *New York Times*. Pridobljeno z naslova *http://bucks.blogs.nytimes.com/2010/08/12how-to-spot-an-a-t-m-skimmer/.*

Walters, C. (2011). *How ATM card skimming works.* Pridobljeno 17. 4. 2013 z naslova *http://www.crikey.com.au/2009/03/30/how-atm-card-skimming-works/*.

Interni viri

Banka X (2008). Interno gradivo: *Pravilnik o servisiranju POS terminalov in ostale pripadajoče opreme,* 26. 5. 2008.

Banka X (2012). Interno gradivo: *Navodila preverjanja namestitve in ukrepanja v primeru nameščenih naprav za izvajanje zlorab na bankomatih*, 1. 7. 2012.

Banka X (2012). Interno gradivo: *Navodila za izdajanje plačilnih kartic,* 8. 6. 2012.

Banka X (2013). Interno gradivo: *Pravilnik o izdajanju plačilnih kartic,* 10. 1. 2013.

KAZALO SLIK

KAZALO GRAFOV

KAZALO TABEL

POJMOVNIK

»Cash Trapping«: past za denar

»Skimming«: posnemanje

KRATICE IN AKRONIMI

AZN: Agencija za zavarovalni nadzor

BIN: Bank Identification Number: identifikacijska številka banke

COBISS: Cooperative Online Bibliographic System and Services: Kooperativni online bibliografski sistem in servisi

CVC: Card Verification Code: koda za preverjanje kartice

GSM: Groupe Spécial Mobile: globalni sistem mobilnih komunikacij

MC: MasterCard

NCR: National Cash Register

OE: območna enota

PAN: Primary Account Number: primarna številka računa

PIN: Personal Identification Number: osebna identifikacijska številka

POS: Point of Sale: točka prodaje

UPN: univerzalni plačilni nalog

B&B, izobraževanje in usposabljanje d.o.o. - Kranj
Cesta Staneta Žagarja 27a
4000 Kranj
T: 04 280 83 00
F: 04 280 83 22
E: info@bb-kranj.si
www.promet.info

PRILOGA 1: ANKETNI VPRAŠALNIK

Pozdravljeni!

Moje ime je Luka Klemenčič in sem študent na Višji strokovni šoli B&B izobraževanje in usposabljanje d.o.o. v Kranju. Za svojo diplomsko nalogo z naslovom »*Varnost kartičnega poslovanja*« potrebujem Vaše sodelovanje. Anketa je anonimna, zato Vas prosim, da si vzamete čas in pri vsakem vprašanju obkrožite odgovor ali pa ga dopišite. Pri nekaterih vprašanjih je mogoče obkrožiti več odgovorov, na kar vas vprašanje posebej opomni.

1. Spol:

a) moški,
b) ženski.

2. Starost:

a) do 25 let,
b) 26–35 let,
c) 36–45 let,
d) 46–55 let,
e) 56 let ali več.

3. Katere vrste bančnih kartic poznate (obkrožite lahko več odgovorov)?

a) *Activa*,
b) *Activa Maestro*,
c) *Activa MasterCard*,
d) *Activa Visa*,
e) *Activa Visa Electron*,
f) *Activa Obrtnik OZS*.

4. Uporabljate tudi plačilne kartice, kot so *Diners Club* ali *American Express*? Če uporabljate samo eno, lahko obkrožite »da«.

a) da,
b) ne.

5. Varna uporaba bančnih kartic pomeni (obkrožite lahko več odgovorov):

a) varovanje osebne identifikacijske številke kartice (PIN),
b) pri dvigovanju gotovine na bankomatu z roko prekrijemo odtipkavanje PIN-a,
c) pred nakupovanjem na spletu se prepričamo o varnosti spletne strani,
d) svoje plačilne kartice nikoli ne posojamo drugim osebam,
e) drugo_____.

(opišite, kar se vam zdi pomembno za varno uporabo plačilnih kartic)

6. Ali ste z bančno kartico že nakupovali preko spleta?

a) da,
b) ne.

7. Banke ponujajo različne vrste zavarovanj pred zlorabami bančnih kartic. Poznate tovrstna zavarovanja?

a) da,
b) ne.

8. Katere primere zlorab na bankomatih poznate (obkrožite lahko več odgovorov)?

a) »Skimming naprava« prebere magnetni zapis na kartici in vizualno zajame PIN številko,
b) pri »libanonski zanki« bankomat ne vrne kartice in ne izda denarja,
c) »Cash Trapping« ali zagozda, kjer se na bankomatu izpiše, da denar lahko vzamete, a ga ne morete,
d) drugo _____.

(na kratko opišite vrsto zlorabe)

9. Preko katerega vira ste najpogosteje seznanjeni o zlorabah z bančnimi karticami?

a) preko medijev, kot so televizija, časopis, radio in splet,
b) preko znancev, prijateljev in sorodnikov,
c) drugo _____.

(dopišite vir, iz katerega ste najpogosteje seznanjeni o zlorabah)

B&B, izobraževanje in usposabljanje d.o.o. - Kranj
Cesta Staneta Žagarja 27a
4000 Kranj
T: 04 280 83 00
F: 04 280 83 22
E: info@bb-kranj.si
www.promet.info

10. Ali ste že doživeli zlorabo svoje bančne kartice? Če ste jo, svojo izkušnjo na kratko opišite.

_____

_____

_____

_____.

Hvala za Vaš čas!