PODVODY S BANKOVÝMI KARTAMI

Michal KORAUŠ

BANK CARD FRAUD

Abstrakt

Spôsoby zneužitia platobných kariet ktoré znižujú ich bezpečnosť sú jednou z negatívnych stránok používanie tohto platobného prostriedku. Dôležité je nachádzať a stále aktualizovať nástroje ako sa týmto podvodom brániť. V tomto kontexte je mimoriadne dôležitým aspektom ochrana a bezpečnosť platobných kariet.
Kľúčové slová: *Platobná karta, ochrana a bezpečnosť platobných kariet, podvod*

Abstract

Misuse of credit cards ways to reduce their security are one of the negative aspects of the use of the payment instrument. Important is to find and keep updated as tools to defend this fraud. In this context, an important aspect of safety and security cards.
Key words*: Payment card, protection and the security of payment card, fraud*

Úvod

V príspevku sa zaoberám podvodmi s platobnými kartami, konkrétne transakčným členením. Sú tu uvedené rôzne spôsoby zneužitia karty v určitých fázach manipulácie s kartou. Nasleduje technické členenie podvodov, kde sú popísané a vysvetlené najčastejšie techniky a postupy používané pri podvodoch s platobnými kartami, vrátane zneužitia karty na internete.

1. Podvody s platobnými kartami - Transakčné členenie

"Široké používanie platobných kariet vzbudilo záujem podvodníkov už v 60. rokoch a najmä od polovice 80. rokov."[1] Spolu s vývojom platobných kariet, predovšetkým ochranných prvkov a možnosťou používania, sa rozvíjajú nové spôsoby a technológie podvodov.

1.1. Zneužitie držiteľom karty

Majiteľ karty nahlási banke zneužitie platobnej karty, hoci tieto transakcie alebo výbery z bankomatu vykonal sám a následne ich popiera. Jedná sa o takzvanú fiktívnu krádež. Za zneužitie platobnej karty jeho držiteľom sa považuje aj jeho platobnú neschopnosť a následné nesplácanie využitých finančných prostriedkov. Banky sa snažia takýmto úverovým stratám vyhnúť dôsledným preverením bonity klienta[2] a tým znížiť riziko nesplácania úveru.

1.2. Zneužitie osobou blízkou

Platobnú kartu môžu zneužiť aj blízki príbuzní, priatelia alebo spolupracovníci držiteľa karty. Zneužitie karty je pre nich jednoduchšie, pretože sa pohybujú v blízkom okolí držiteľa a majú jednoduchšiu možnosť, pri nedostatočnej obozretnosti majiteľa karty, zistiť PIN.

1.3. Zneužitie cudzou osobou

K zneužitiu cudzou osobou dochádza kvôli strate alebo ukradnutiu platobnej karty a pre vydávateľa to znamená najväčšie straty. Majiteľ karty by mal stratu/ukradnutie čo najskôr nahlásiť svojej banke, čím na ňu prenáša zodpovednosť za prípadné zneužitie karty. Banka musí preplatiť klientovi časť škody spôsobenú podvodníkom pred nahlásením a následnou blokáciou. Majiteľ karty ponesie zodpovednosť za stratu do výšky 150 Eur a prípadnú vyššiu čiastku doplatí banka. Po nahlásení chýbajúcej karty nesie všetku zodpovednosť banka. Neplatí to však u autorizovaných transakcií, pri ktorých je nutné zadávať PIN. V tomto prípade stráca klient nárok na odškodnenie, pretože nevykonal dostatočné opatrenia preto, aby cudzia osoba nezistila PIN karty. To je označované ako hrubá nedbanlivosť. Neplatí to u organizovaných podvodov, napríklad skimmingu.

Ďalšou výraznou zmenou je zrušenie poplatku za blokáciu karty, ktorý by malo majiteľa kariet donútiť k včasnému nahlásenie chýbajúcej karty.

Skrátenie doby prevodu peňazí medzi účtami klientov rôznych bánk by tiež malo prispieť k včasnému odhaleniu podvodných transakcií. Táto doba sa skracuje o jeden deň a prevod peňazí medzi účtami nesmie trvať dlhšie ako dva dni.

[1] Juřík, P.: Platební karty - Velká encyklopedie 1870-2006. 1. vyd. Praha : Grada Publishing, a.s., 2006. 201 s. ISBN 80-247-1381-0.
[2] Schopnosť splácať poskytnutý úver

1.4. Zneužitie nedoručenej karty

Banky zasielajú klientom platobné karty Slovenskou poštou, PIN v inej zásielke a v iný deň. Po doručení musí klient kartu najprv aktivovať, čo znižuje riziko zneužitia karty pred doručením zásielky pravému majiteľovi. Banky však ponúkajú osobné prevzatie karty a PINu na svojich pobočkách.

1.5. Platby na diaľku

Zneužitia platobnej karty pri platbe na diaľku (Mail order/Telephone order) je možné vďaka tomu, že k platbe nie je potrebná fyzická prítomnosť karty. Číslo karty a dátum expirácie sa oznamujú buď písomne, alebo ústne podľa toho, či je platba realizovaná pomocou telefónu, faxu alebo emailu.

Keďže je platba na diaľku neautorizovaná, tak pri strate/odcudzení banka nahrádza finančnú stratu od 150 Euro.

1.6. Podvodná žiadosť o kartu

Falošná žiadosť o platobnú kartu môže byť vykonaná po ukradnutí identity, čo znamená, že páchateľ zneužije stratený / ukradnutý občiansky preukaz či iné doklady totožnosti. V Slovenskej republike nejde o rozšírený podvod, pretože jednotlivé banky majú svoje opatrenia, ako predísť vydaniu platobnej karty neoprávnenému držiteľovi.

1.7. Zneužitie obchodníkom

Jedným z podvodov zo strany obchodníka je poznamenanie si údajov z platobnej karty, ktoré potom použije na platby na internete, pri ktorých stačí zadať len číslo platobnej karty, dátum platnosti a elektronický kód.

Obchodník môže tiež skopírovať údaje z magnetického prúžku karty. K tomu využíva zariadenie, ktorým "prejde" platobnú kartu, alebo špeciálne upravené platobné terminály. Táto nelegálna činnosť sa nazýva skimming.

Pri platbe embosovanou platobnou kartou (len ak je použitý imprinter) môže dôjsť k riziku viacnásobnej transakcie alebo upravovaniu predajných dokladov. Viacnásobnú transakciu môže vykonať vyhotovením bianko (nevyplnenej) kópie platobnej karty, kde potom vyplní sumu platby a sfalšovaný podpis. Obchodník musí vyhotoviť odtlačky na 3 predajné doklady, z ktorých je jeden odovzdaný zákazníkovi, jeden si obchodník necháva pre svoje vyúčtovanie a posledný zasiela na zúčtovanie banke. Obchodník môže upraviť finančnú čiastku na dokladoch, ktorý si ponecháva a odovzdáva banke. V prípade, že si zákazník uschoval predajný doklad, má jasný dôkaz o nezákonnej činnosti obchodníka, v opačnom prípade sa dostáva do situácie dôkaznej núdze a s reklamáciou môže mať značné problémy. Prevenciou proti zneužitiu platobnej karty obchodníkom je nestrácať kartu z dohľadu a sledovať priebeh transakcie.

2. Technické členenie podvodov

2.1. Skimming

Pri tzv. skimmingu dochádza ku kopírovaniu údajov z magnetického prúžku platobnej karty. Najčastejšie sú na to používané zariadenia, ktoré sú nainštalované priamo na bankomat. Kópiu dát z magnetického prúžku môže vykonať tiež obchodník (napríklad pri platbe v reštaurácii, hoteli). Názov je odvodený od slova "to skim", čo vo voľnom preklade znamená "zobrať smotanu", v tomto prípade dostať z platobnej karty to najlepšie pre falšovateľov.

Predpokladá sa, že skimming zameraný na čipové karty sa stane atraktívnym cieľom pre podvodníkov, ktorí sa budú snažiť prekonať bezpečnostné prekážky.

Na získanie bezpečnostného kódu PIN pripevnia podvodníci miniatúrne kamery nad klávesnicu a snímajú pohyby prstov. Ďalej môžu použiť dotykové klávesnice, ktoré sú umiestnené priamo na klávesnici bankomatu, prípadne PIN odpozorujú.

Odkopírované údaje z karty sú uložené buď priamo vo skimmovacom zariadení a následne prenesené napríklad do notebooku, alebo sú okamžite odosielané pomocou bezdrôtovej technológie prenosu dát. Nasleduje výroba falzifikátu karty, buď nahraním dát na akúkoľvek platobnú kartu, ktorá je použitá pri platbe v obchode, alebo na tzv. "biely plast"[3], pre výbery z bankomatov.

Držitelia karty pritom často vôbec netušia, že vložili kartu do bankomatu vybaveného skimmovacím zariadením. Jedinou ochranou je dobrá znalosť vzhľadu bankomatu, avšak skimmovacie nadstavce, ktoré používajú páchatelia, sú vyrobené presne podľa vzoru tých originálnych. Banky sa snažia ochrániť svojich klientov inštalovaním antiskimmovacích nadstavcov na vstupnej štrbiny, ktoré by mali zamedziť montáži kopírovacieho zariadenia, avšak ani táto ochrana nie je stopercentná. Proti prezradeniu PINu cez kamery na bankomatoch sa dá chrániť veľmi jednoducho - pri zadávaní PINu si zakryť ruku druhou rukou.

Prvé skimmovacie zariadenie bolo použité už v 90. rokoch, v Slovenskej republike sa objavilo v roku 2001. V roku 2005 a 2006 nebolo skimmovacie zariadenie tak ťažko rozpoznateľné ako dnes a práve tomu zodpovedá nízky počet vykonaných skimmovaní v Slovenskej republike najmä z dôvodu ich rýchleho odhalenia. V roku 2007 sa počet skimovaní výrazne zvýšil. Na tejto činnosti sa podieľali predovšetkým rumunské zločinecké gangy.[4] Pri útokoch v roku 2010 na bankomaty boli dáta zneužité okamžite, vyrobené falzifikáty, a tie potom boli použité k výberom finančných hotovostí, predovšetkým v mimoeurópskych krajinách (napr. Peru, Dominikánska republika, Keňa, Maroko, Austrália, Kanada a USA).

2.1.1. Libanonská slučka

Libanonská slučka je primitívny predchodca skimmingu. Táto trestná činnosť však nespočíva v kopírovaní údajov, ale páchateľ týmto spôsobom scudzí platobnú kartu. Do bankomatu zasunie a nenápadne zafixuje prúžok odstrihnutej magnetofónovej alebo podobnej pásky a tým spôsobí, že sa platobná karta nedostane do bankomatu a majiteľ ju nemá ani možnosť vytiahnuť. Páchatelia

[3] Biela platobná karta, opatrená magnetickým prúžkom. Je ju možné získať ako bežný spotrebný materiál

[4] Hradecký, M.: Skimming v ČR . Padělání peněz a skimming. Dostupné z www: <http://www.karty-penize.webgarden.name/thema/skimming-v-cr>.

však potrebujú poznať aj PIN, preto využívajú dôverčivosť postihnutého a ten na radu páchateľa zadá PIN. Potom majiteľ karty odchádza nahlásiť poruchu bankomatu, alebo je iným spôsobom odlákaný od bankomatu a páchateľ má možnosť kartu vytiahnuť.
Ochrana zo strany majiteľa karty je v tomto prípade jednoduchá. Dostatočná obozretnosť - nezadávať pred cudzím človekom PIN a neopúšťať bankomat so zaseknutou platobnou kartou. Tento spôsob krádeže platobných kariet sa už v Slovenskej republike nevyskytuje, pretože banky zaviedli dostatočnú ochranu (ochranné adaptéry).
Hradecká lišta je ďalší zo spôsobov nezákonných manipulácií s bankomatmi. Na rozdiel od Libanonskej slučky neukradne páchateľ platobnú kartu, ale priamo hotovosť vydanú bankomatom. Používa k tomu lištu alebo nadstavec, ktorý je z druhej strany opatrený samolepkou, a tú upevní na otvor pre výdaj hotovosti. Potom čaká, kým sa daný človek od bankomatu vzdiali a lištu odnesie aj s peniazmi. Tento spôsob krádeže je pomenovaný podľa prípadu v Hradci Králové z roku 2008.
Ďalšie možnosti odcudzenia platobnej karty sa vyskytujú veľmi zriedka. Jedná sa napríklad o upevnenie falošného predného krytu bankomatu na originálny kryt. Medzi nimi sa platobná karta zasekne. Ďalším veľmi nepravdepodobným, finančne náročným spôsobom je inštalácia falošného bankomatu, ktorý je vernou kópiou pravých bankomatov. Vydáva hotovosť, uskutočňuje požadované aplikácie, ale zaznamenáva údaje z platobných kariet a PIN.

2.2. Zneužitie karty na internete

Medzi podvodmi dnes ale prevláda zneužitie platobných kariet na internete, a to ako kvôli počítačovým vírusom alebo podvodným e-mailom, tak aj na základe použitia platobnej karty na pochybných internetových stránkach a e - shopoch. Pri platení po internete odporúčame klientom starostlivo vyberať obchodníka, u ktorého sa bude transakcia realizovať. Mal by byť dôveryhodný a mal by mať zabezpečený prenos dát o platobnej karte. Bezpečný internetový obchodník má na svojich stránkach inštalovaný certifikát potvrdzujúci SSL zabezpečenia, ktorý je graficky znázornený vo forme zlatého zámočku; zároveň sa v prehliadači zmení stránka obchodníka na https://www .... , ".
K bezpečným internetovým stránkam patria aj tie, ktoré ponúkajú platby kartou na platforme 3D - Secure a sú označené logami Verified by Visa a MasterCard SecureCode. Pri transakcii so zabezpečením 3D - Secure sa totiž údaje z karty odosielajú v zašifrovanej podobe priamo do banky, teda nie obchodníkovi, u ktorého človek nakupuje. Tým sa výrazne zníži možnosť zneužitia platobnej karty pri transakciách a takisto úplne znemožní prípadné zneužitie karty obchodníkom.
Platby prostredníctvom tejto platformy je navyše možné nakombinovať s ďalšími bezpečnostnými prvkami. Banky spustili pre klientov službu 3D - Secure, ktorá zvyšuje bezpečnosť platby na internete, podmieňuje vykonanie platby u obchodníka, využívajúceho ochrany 3D - Secure, vyplnením bezpečnostného autorizačného kódu, ktorý klient dostane SMS správou na svoj mobilný telefón. Značná časť klientov používajúcich internetové platby už túto službu využíva. Týmto sa nezlepšujú len metódy podvodníkov, ale aj bezpečnostné systémy bankových domov a vydavateľov platobných kariet. Bežnou praxou bánk je, že priebežne a detailne monitorujú transakcie na platobných kartách a zároveň dostávajú upozornenia od kartových asociácií, ak asociácia zistí čokoľvek podozrivé.
Vydavateľská banka potom kontaktuje klienta, aby overila, či skutočne chcel za niečo platiť. Bežným postupom sú tiež preventívne blokácie, kedy banka zablokuje karty, u ktorých má podozrenie, že by mohli byť potenciálne zneužité. Banky používajú systém, ktorý vyhodnocuje podozrivé transakcie. V niektorých prípadoch potom pracovníci banky telefonicky overujú, či sú transakcie realizované skutočne majiteľom karty.
Aj napriek tomu, že sú už niekoľko rokov internetové platby zabezpečené systémom 3-D Secure a inými, stále veľa ľudí tomuto spôsobu platby nedôveruje. Avšak vďaka 3-D Secure je zneužitie údajov z karty obchodníkom, či hackerom vylúčené, pretože platba prebieha iba medzi majiteľom karty a bankou a stránky, na ktorých je nutné zadať informácie z karty, sú dostatočne zabezpečené. Strate dát na internete sa dá jednoducho vyhnúť používaním takto zabezpečených stránok.
Určité riziko je však pri platení u internetových obchodníkov z USA, Ázie aj iných. Svoje stránky nemajú často dostatočne zabezpečené a skúsení hackeri sa môžu nabúrať do databáz ich klientov[5] a získať tak potrebné dáta. Dosvedčuje to aj veľký prípad hromadnej krádeže dát zo zákazníckych účtov v internetovej hernej sieti PlayStation Network. Spoločnosť odporúčala klientom zablokovanie svojich platobných kariet.

2.3. Phishing

Pri phishingu dochádza k zneužitiu emailovej pošty a predovšetkým dôverčivosti a neznalosti klientov bánk. Phishing je jeden z variantov sociálneho inžinierstva, ktoré je postavené na manipuláciu s ľuďmi. Názov je odvodený z anglického slova "fishing" čiže rybárčenie. Toto výstižné označenie zodpovedá aj podstate phishingu. Podvodníci hromadne rozošlú emaily klientom finančných inštitúcií, ktorých zoznam sa im podarilo nejakým spôsobom získať, a čakajú, kto sa na podvodné emaily "chytí". Emaily aj formuláre pre vyplnenie údajov sú vytvorené tak, aby na prvý pohľad vyzerali ako oficiálne správy a stránky banky, alebo aj niektoré z kartových asociácií, ktorá sa na nich obracia s určitou výzvou. Podnetov, ako z klientov vylákať citlivé údaje, môže byť veľa. Napríklad v emaile je uvedené, že banka potrebuje overiť správnosť heslá do internetového bankovníctva, potvrdiť príjem určitej finančnej čiastky na účet a takto podvodník vyláka od postihnutého číslo karty, prihlasovacie údaje alebo aj PIN. Zistené údaje sa najčastejšie predávajú na čiernych trhoch na internete. Ochrana je proti tomuto nelegálnemu postupu jednoduchá - na také emaily nereagovať, pretože banka či kartové asociácie nikdy nebudú požadovať potvrdzovanie bezpečnostných údajov cez email.
V roku 2006 sa v Slovenskej republike objavil prvý phishingový email, ktorý bol rozoslaný klientom bánk. Obeťami phishingu sa stávali stovky klientov, ktorí prezradili údaje k svojim platobným kartám, mnohí vrátane čísla PIN. Pri 10 % kariet došlo k

[5] Označované ako Database hacking

reálnym podvodným transakciám v zahraničí. Podvodníci mnohokrát rozosielajú emaily náhodne, takže sa môže aj stať, že email od určitej banky príde človeku, ktorý jej klientom vôbec nie je. Vhishing je forma phishingu, avšak prevádzkovaná cez telefón.

2.3.1. Phishingový email

Tento email z 2008 využíva to, že klienti bánk už o phishingu získali nejaké informácie a snaží sa pôsobiť vierohodne. Podvodný email možno odhaliť podľa toho, že je uvedený odkaz, ktorý má webovú adresu zhodnú so stránkami banky, ale v skutočnosti sa pri kliknutí otvorí podvrhnutá stránka. Slovenské phishingové emaily v rokoch 2006 - 2009 mali veľa gramatických a štylistických chýb a boli preložené automatickým prekladačom z angličtiny či ruštiny. Tieto emaily však ďalej prichádzajú do počítačov ale je už lepšie spracované.

2.4. Pharming

Pharming je obdobou phishingu, ale jeho cieľom je presmerovanie z oficiálnych stránok banky na falošné webové stránky. Existujú dva spôsoby Pharming. Jeden spôsob spočíva v napadnutí DNS[6] servera a jeho hierarchickej štruktúry. Potom, čo klient zadá webovú adresu, sa mu nezobrazí požadovaná stránka, ale je presmerovaný na stránku vytvorenú podvodníkom, ktorá však vyzerá úplne rovnako.
Druhý variant Pharmingu spočíva v napadnutí jednotlivých počítačov vírusom (napríklad trójskym koňom) a ten zmení súbor hosts, ktorý obsahuje IP adresy a výsledný efekt je rovnaký ako v prvom prípade. Vírus môže byť naprogramovaný aj tak, že vyčkáva, až obeť vykoná nejakú platbu platobnou kartou a takto podvodník získa všetky údaje pre zneužívanie karty cez internet. Pharmingu môžu zabrániť rôzne antivírusové programy, ktoré ho včas odhalia.

Záver

Polícia Slovenskej republiky rieši ročne tisíce prípadov zneužitia platobných kariet. K veľkej časti podvodov dochádza úplne zbytočne, ľudia skrátka často vôbec nedodržiavajú bežné zásady obozretnosti. Na tom sa zhodujú aj zástupcovia slovenských bankových domov. Znížiť riziko toho, že sa staneme obeťou podvodníkov a necháme si vysať peniaze z účtu , pritom nie je vôbec ťažké.
Počet zneužití platobných kariet v posledných rokoch zostáva takmer rovnaký, metódy podvodníkov sa ale stále vyvíjajú a ich odhaľovanie je dnes výrazne ťažšie. Okrem obvyklých typov zneužitia, ako je napríklad, „zapožičanie“ si karty člena rodiny, sa vyvíjajú predovšetkým spôsoby získavania dát o kartách, ktoré sú oveľa sofistikovanejšie ako predtým. Ide napríklad o skimming čiže podvodné načítanie údajov z magnetického prúžku platobných kariet v bankomate. Pri skimmingu zariadenie pripojené k bankomatu načíta a skopíruje kartové údaje, vyrobiť na ich základe kópiu karty už potom nie je pre podvodníkov žiadny problém. Stačí im už len získať PIN - a to väčšinou dokážu zároveň s kopírovaním údajov, prostredníctvom miniatúrnej kamery, ktorá sníma klávesnicu bankomatu, alebo priamo nainštalovaním falošnej klávesnice, ktorá zaznamená naťukaný PIN. S falošnou kópiou platobnej karty potom vyberajú peniaze tam, kde ešte nie sú čipové zariadenia, teda predovšetkým v určitých oblastiach USA, v juhovýchodnej Ázii a v štátoch strednej a Latinskej Ameriky (Mexiko, Kolumbia či Peru). V Európe došlo k nelegálnym výberom napríklad na Ukrajine a v Bulharsku .

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] Belás, J.: Kvalita vkladových produktov a služieb. In: BIATEC, roč. 6, 1998, č. 8, s. 6–8. ISSN 1335-0900
[2] Belás, J. a kol. Manažment komerčných bánk, bankových obchodov a operácií. Žilina: Georg, 2010. 471 s. ISBN: 978-80-89401-18-5
[3] Hradecký, M.: Skimming v ČR . Padělání peněz a skimming. - [on-line] Available on - URL: <http://www.karty-penize.webgarden.name/thema/skimming-v-cr>
[4] Juřík, P.: Platební karty - Velká encyklopedie 1870-2006. 1. vyd. Praha : Grada Publishing, a.s., 2006. 201 s. ISBN 80-247-1381-0
[5] Korauš, A.: Marketing v bankovníctve a poisťovníctve. Bratislava: Sprint, 2000, s. 297. ISBN 80-88848- 52-0
[6] Korauš, A.: Financial marketing. - Bratislava: Sprint dva, 2012. ISBN 978-80-89393-57-2

ADRESA AUTORA

Ing. Michal KORAUŠ, MBA, AT Computer, s.r.o., Framborská 253, 010 01 Žilina, Slovenská republika, e:Mail: koraus@atcomp.sk

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.

[6] DNS (Domain Name System) je hierarchická databáza, ktorá udržuje zoznam internetových domén a príslušných DNS adries