CARNET

Sigurno korištenje i rizici bankovnih kartica

NCERT-PUBDOC-2018-2-353

CERT.hr

Sadržaj

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

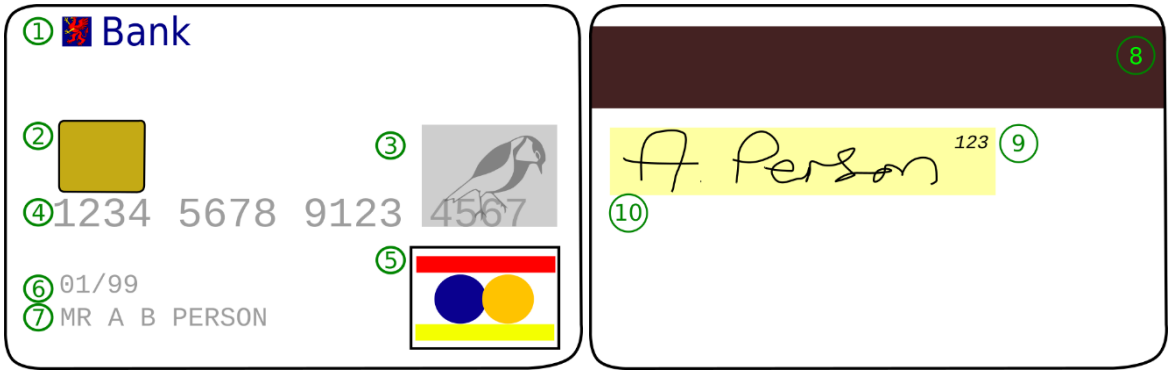
Bankovne kartice praktičan su način plaćanja. Debitne, kreditne, poklon i slične kartice moguće je koristiti umjesto gotovine na velikom broju prodajnih mjesta diljem svijeta te su glavni način plaćanja pri kupovini na Internetu. No, one su i česta meta kriminalaca zbog potencijalnog pristupa svim novcima na računu žrtve. Ovaj dokument opisat će česte rizike prilikom korištenja bankovnih kartica te kako se zaštititi od njih. Kako bi bilo moguće razumjeti te rizike, potrebno je prvo steći osnovno razumijevanje tehnologije bankovnih kartica.

1.1 Što se nalazi na kartici?

Glavni podaci koji se nalaze na bankovnoj kartici su:

- Ime i prezime vlasnika kartice
- Broj kartice
- Datum isteka kartice

To su podaci koji su u pravilu potrebni za provedbu transakcije, tj. za plaćanje bankovnom karticom. Ono što je zanimljivo je način kako su ti podaci zapravo zapisani na kartici. Kako bi sljedeća objašnjenja bila jasnija, slika 1 prikazuje primjer prednje (lijevo) i stražnje (desno) strane moderne bankovne kartice s označenim dijelovima. Dijelovi kartice su na slici označeni brojevima na koje će se tekst iz ovog poglavlja pozivati.



Slika 1 – Primjer prednje (lijevo) i stražnje (desno) strane moderne bankovne kartice s označenim dijelovima.

Navedeni glavni podaci su na današnjim bankovnim karticama zapisani na tri mjesta:

- Ispisani ili izbočeni na kartici (brojevi 4, 6 i 7)
- Zapisani na magnetskoj traci (broj 8)
- Zapisani na čipu (brojem 2 označeni su kontakti čipa)

Uz to, na kartici se još obično nalaze sigurnosni brojevi (CVV1 – zapisan na magnetskoj traci, broj 8, CVV2 – obično ispisan na poleđini kartice, broj 9), potpis (broj 10), hologram (broj 3), logotip marke kartice (broj 5), naziv i logotip banke (broj 1)…

U sljedećem poglavlju bit će opisana kratka povijest tehnologije bankovnih kartica. Kroz objašnjenje kako su se bankovne kartice koristile postat će jasno zašto su podaci na karticama zapisani na ovaj način.

1.2 Kratka povijest tehnologije

Do otprilike 70-tih godina prošlog stoljeća, najefikasniji način korištenja bankovnih kartica bilo je otiskivanje izbočenih podataka s kartice na papir. Podaci su otiskivani pomoću uređaja za otiskivanje (eng. *imprinter*) – primjer takvog uređaja prikazan je na slici 2. Za transakcije s većim iznosom trgovci bi zvali banku koja bi zatim odobrila odnosno odbila transakciju.

Slika 2 – Otiskivanje podataka izbočenih na bankovnoj kartici uređajem za otiskivanje (eng. *imprinter*). (izvor)

Uvođenje kartica s magnetskom trakom bio je veliki napredak po pitanju praktičnosti i sigurnosti. Kartice s magnetskom trakom bilo je moguće brzo očitati na POS (skraćenica za eng. *point of sale*) uređajima te su transakcije bile automatski i na relativno siguran način obrađene. Primjer POS uređaja i plaćanja karticom s magnetskom trakom prikazan je na slici 3.

Slika 3 – Očitanje podataka s magnetske trake bankovne kartice POS uređajem. (izvor)

Tehnologija magnetskih traka bila je revolucionarna te se i dan danas na nekim mjestima koristi kao primarna tehnologija plaćanja bankovnim karticama. No ona ima svoje sigurnosne probleme koji postaju ozbiljniji svakim danom. Konkretnije, kriminalcima je danas relativno lako uz odgovarajuće podatke napraviti lažnu kopiju kartice s

magnetskom trakom. S takvom lažnom kopijom oni zatim mogu plaćati kao i s originalnom karticom – i sve to na račun žrtve.

Odgovor na te sigurnosne probleme bilo je uvođenje pametnih kartica – kartica s čipom na sebi. Čip na kartici je zapravo malo računalo koje prilikom provođenja transakcije komunicira s POS uređajem. Podaci su zapisani u memoriju čipa na način da je kriminalcima izrazito teško izvaditi te podatke i napraviti kopiju kartice.

Uz to, prilikom komunikacije kartice s POS uređajem, podaci su u pravilu kriptografski zaštićeni. Drugim riječima, kriminalci ne mogu doći do povjerljivih podataka ni prisluškivanjem odnosno presretanjem komunikacije.

Primjer plaćanja pametnom bankovnom karticom prikazan je na slici 4. Za razliku od očitanja kartice s magnetskom trakom, pametna kartica se ne „provlači“ kroz POS uređaj, već se priključi (utakne) u njega.

Slika 4 – Komunikacija POS uređaja i čipa na bankovnoj kartici. (izvor)

Najnovija tehnologija plaćanja bankovnim karticama je beskontaktno plaćanje. Što se same tehnologije tiče, ona je u pravilu izrazito slična uobičajenom plaćanju pametnom karticom, samo što se u ovom slučaju komunikacija odvija bežično. Podaci su i dalje zapisani na istom čipu, no on sada ima i mogućnost bežične komunikacije s POS uređajem. Primjer plaćanja beskontaktnom karticom prikazan je na slici 5.

Slika 5 – Beskontaktna komunikacija POS uređaja i čipa na bankovnoj kartici. (izvor)

2 Rizici prilikom korištenja bankovnih kartica

Preduvjet za sigurnije korištenje bankovnih kartica je svijest o odgovarajućim rizicima i njihovo razumijevanje. Upravo zato, ovo poglavlje opisuje najčešće rizike u obliku koji je koristan krajnjim korisnicima.

2.1 Gubitak/krađa kartice

Rizik kojega su građani obično najviše svjesni je gubitak odnosno krađa bankovne kartice. O vrsti kartice i načinu autorizacije transakcije ovisi može li kriminalac zapravo zlouporabiti izgubljenu odnosno ukradenu karticu.

Ako je karticom moguće kupovati preko Interneta bez dodatnih autorizacijskih mehanizama, kriminalac će upravo tako moći i ukrasti novac s računa.

Što se tiče zlouporabe kartice u fizičkoj kupovini, najveći rizik predstavljaju kartice kojima je za autorizaciju transakcije dovoljan samo potpis. Kriminalac može vidjeti kako potpis izgleda na poleđini kartice te ga zatim prilikom kupovine može i lažirati. Često nije ni potrebno uvjerljivo lažiranje jer trgovci rijetko obraćaju pažnju pri usporedbi potpisa kupca s onim na poleđini kartice.

Nešto manju, ali i dalje značajnu količinu rizika u fizičkoj kupovini predstavljaju beskontaktne kartice. Njih je često moguće koristiti bez autorizacije PIN-om do neke granice. Primjerice, kriminalac ukradenom beskontaktnom karticom može napraviti 10 transakcija u vrijednosti do 100kn i tako sveukupno ukrasti do 1000kn. Nakon toga, sljedeća transakcija će zahtijevati autorizaciju PIN-om. Konkretna ograničenja (do 100kn po transakciji, maksimalno 10 transakcija) za transakcije bez autorizacije variraju, no u pravilu kriminalac će bez znanja PIN-a moći ukrasti određenu svotu novca.

Kartice koje za svaku transakciju zahtijevaju PIN predstavljaju najmanji rizik zlouporabe u fizičkoj kupovini. No u tom slučaju ključna je tajnost PIN-a – ako žrtva koristi PIN koji je jednostavan za pogoditi (npr. 1234, neki značajni datum ili godina…), kriminalcima on neće predstavljati veliku prepreku pri krađi. Alternativno, ako žrtva ima PIN zapisan negdje, kriminalci također potencijalno mogu doći do njega. U konačnici, kriminalci znaju biti izrazito dosjetljivi u načinima krađe PIN-a. Znaju koristiti skrivene kamere, lažne tipkovnice na bankomatima, prijenosne toplinske kamere, no često im je dovoljno i jednostavno gledanje preko ramena dok žrtva upisuje PIN.

2.2 Kompromitirano računalo/pametni telefon korisnika

Prilikom plaćanja karticom preko Interneta ili korištenja internetskog bankarstva, najveći rizik je kompromitirano računalo odnosno pametni telefon korisnika.

Drugim riječima, ako je korisnikov uređaj zaražen zlonamjernim softverom (eng. *malware*), kriminalac koji stoji iza napada može vidjeti sve što korisnik upisuje. To uključuje i broj kartice, sigurnosni broj te čak i lozinke za internetsko bankarstvo.

Konkretno, ako žrtva plaća karticom preko Interneta na zaraženom uređaju, kriminalac može vidjeti te podatke te zatim i ukrasti novce s te kartice.

Ako žrtva koristi internetsko bankarstvo na zaraženom uređaju, rizik je još i veći. Tada, kriminalac preko zlonamjernog softvera može dobiti pristup cijelom žrtvinom internetskom bankarstvu. U pravilu to znači da kriminalac onda može i ukrasti novce sa svih žrtvinih računa i štednji.

Zaraza uređaja zlonamjernim softverom obično se događa zbog:

- Neažurnog softvera (Web preglednika, dodataka Web pregledniku, programa za čitanje elektroničke pošte, operacijskog sustava…)
- Preuzimanja i pokretanja zaraženih programa
- Preuzimanja i otvaranja zaraženih dokumenata

2.3 Kompromitiran bankomat – *skimmer* uređaji

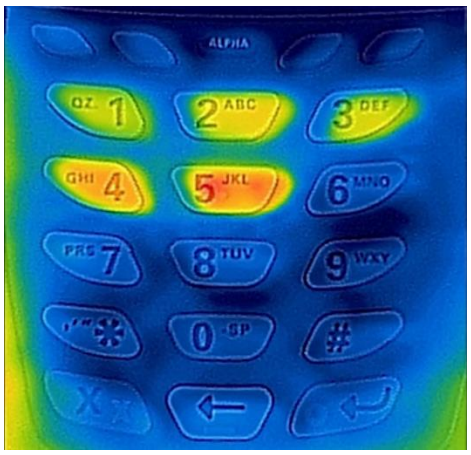
Jedan od načina krađe novaca preko bankovnih kartica je i kompromitacija bankomata takozvanim *skimmer* uređajima. To su uređaji koje kriminalci obično skriveno ugrade na bankomat kako bi prikupljali podatke s bankovnih kartica bez znanja žrtve. Slika 6 prikazuje dva primjera *skimmer* uređaja skriveno ugrađenih na bankomat.

Slika 6 – Primjeri skriveno ugrađenih *skimmer* uređaja (izvor)

Uz *skimmer* uređaje, kriminalci gotovo uvijek ugrade i uređaj za skriveno prikupljanje odgovarajućih PIN-ova. Na slici 7 prikazana su dva primjera takvih uređaja – lijevo je prikazana lažna tipkovnica, a desno skrivena kamera.

Slika 7 – Primjeri uređaja za skriveno prikupljanje PIN-ova – lažna tipkovnica (lijevo) i skrivena kamera (desno) (izvor)

PIN je moguće saznati i tako da se infracrvenom kamerom snimi tipkovnica POS-a ili bankomata neposredno nakon što ju je koristio legitimni korisnik. Korištene tipke su toplije, što se vidi na snimci. Čak je moguće prepoznati koja je tipka pritisnuta ranije, a koja kasnije. Slika 8 prikazuje POS uređaj snimljen infracrvenom kamerom nakon utipkavanja broja „12345“. Neki mobiteli već tvornički mogu snimiti infracrveni dio spektra, a za neke je moguće lagano dodati nastavak.



Slika 8 – POS uređaj snimljen infracrvenom kamerom nakon utipkavanja broja „12345“

Jednom kada prikupe navedene podatke, kriminalci mogu napraviti fizičku kopiju kartice ili ju koristiti preko Interneta – u oba slučaja za plaćanje na žrtvin račun.

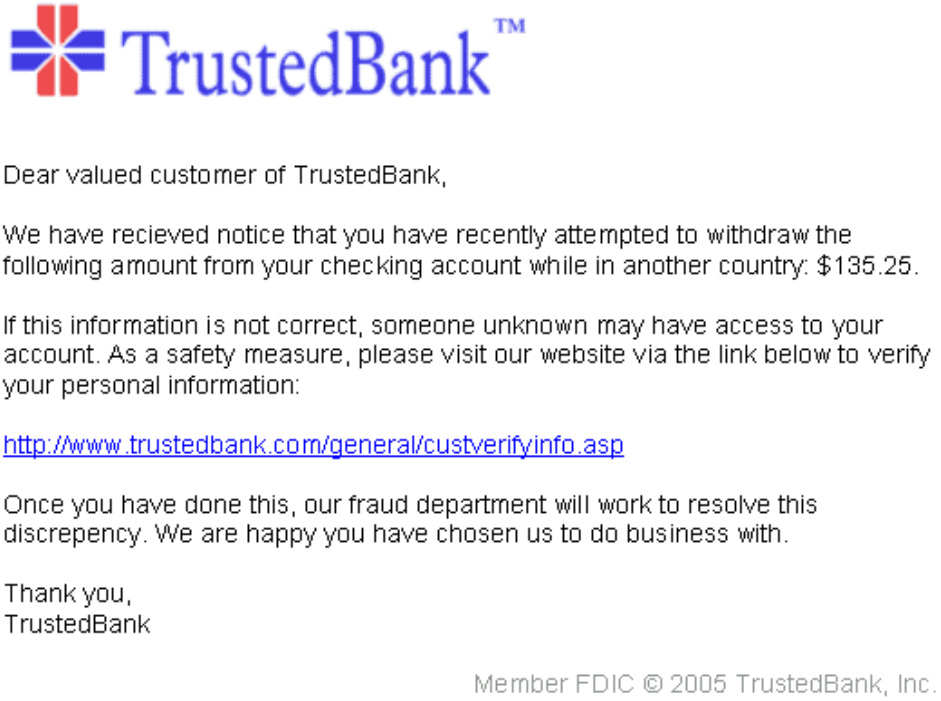
2.4 Prevara/socijalni inženjering

Jedna od najčešćih prijetnji u ovom kontekstu ne uključuje tehničku kompromitaciju uređaja ili fizičku krađu. Ta prijetnja se u kontekstu informacijske sigurnosti naziva socijalni inženjering, a pojednostavljeno, ona se može opisati kao prevara. Prevara je jedna od najčešćih prijetnji upravo zato jer je često lakše obmanuti žrtvu nego fizički joj ukrasti karticu odnosno kompromitirati uređaj.

Primjer jedne česte prevare vezane za bankovne kartice počinje tako da žrtva, na primjer gost hotela, dobije poziv usred noći. Pozivatelj se duboko ispričava i kaže kako zove s recepcije hotela. U nastavku objašnjava kako su izgubili podatke o žrtvinoj kartici te su im oni upravo sada potrebni jer moraju pod hitno završiti neku poslovnu obvezu i konačno, traži žrtvu da mu izdiktira podatke sa svoje bankovne kartice preko telefona. Kao što je

moguće i pretpostaviti – pozivatelj je zapravo napadač koji obmanom pokušava prikupiti podatke o karticama žrtava.

Danas je izrazito česta prevara putem elektroničke komunikacije (elektronička pošta, društvene mreže, *instant messaging/chat* aplikacije), u kontekstu informacijske sigurnosti zvana *phishing*. Većina ljudi susrela se s nekim oblikom takve prevare. Uobičajeni primjer bila bi poruka elektroničke pošte koja naizgled dolazi od žrtvine banke. U poruci se žrtvu traži da otvori poveznicu iz poruke te tamo upiše podatke o svojoj bankovnoj kartici. Otvaranjem poveznice i popunjavanjem podataka žrtva zapravo predaje svoje podatke napadaču. Jedan primjer takvog *phishing* napada kroz elektroničku poštu prikazan je na slici 9.



Slika 9 – Primjer *phishing* napada kroz elektroničku poštu

Prevara ne mora nužno biti takva da napadač kontaktira korisnika. Primjerice, postoje brojne usluge koje su naizgled besplatne, no traže podatke o kartici za njihovo korištenje. Jednom upisani podaci zatim se ilegalno koriste odnosno preprodaju. U blažim slučajevima takve prevare, podaci čak neće biti ni ilegalno korišteni već će na nekom manje vidljivom mjestu biti naznačeno da se korisnik zapravo prijavljuje za plaćenu uslugu, a samo je, primjerice, prvih mjesec dana besplatno.

Ove se prevare temelje na obmani krajnjih korisnika i postoji velik broj različitih tehnika prevare koji svakim danom raste. Zato nije moguće ovdje popisati sve takve tehnike, ali je važno biti svjestan da su prevare raširene i da su često najčešćih oblik ugroza sigurnosti – i u kontekstu bankovnih kartica, ali i šire.

2.5 Rizici izvan žrtvine kontrole

Za neke od prethodno navedenih rizika, primjerice dobro sakriveni *skimmer* uređaj ili složenu prevaru, nije realno očekivati da će bilo tko osim najopreznijih korisnika ostati siguran. Uz njih, još brojni rizici su velikim dijelom izvan žrtvine kontrole – drugim riječima, žrtva ne može gotovo ništa učiniti da spriječi napad.

S tehničke strane, za uspješnu krađu dovoljno je da napadač kompromitira bilo koju točku u procesu obrade transakcije: POS uređaj, Web stranicu trgovca ili posredničku tvrtku koja obrađuje transakcije. Na taj način, napadač može doći do podataka o kartici osobe koja zapravo sama nije ništa nesigurno napravila.

U drugu ruku, ne postoji nužno ni potreba za tehničkim napadom. Prilikom svakog korištenja kartice, korisnik povjerava svoju karticu odnosno njene podatke nekome – blagajniku u dućanu, recepcioneru hotela, konobaru u restoranu, Web stranici internetske trgovine i slično. Bilo tko od njih može zlouporabiti to povjerenje. Primjerice, zabilježeni su slučajevi u kojima su konobari u restoranu prilikom plaćanja provlačili kartice žrtava kroz ručne *skimmer* uređaje te su zatim te podatke preprodavali.

3 Sigurno korištenje bankovnih kartica

Razumijevanje rizika prilikom korištenja bankovnih kartica dobar je prvi korak za zaštitu od napada. Uz dodatne mjere opreza, moguće je značajno smanjiti vjerojatnost uspješnog napada i u konačnici – krađe.

Nažalost, neovisno o oprezu krajnjeg korisnika, potpunu sigurnost prilikom korištenja bankovnih kartica nije moguće postići. Kao što je navedeno u prošlom poglavlju, postoji niz rizika koji su velikim dijelom izvan žrtvine kontrole. Iako neke napade nije moguće spriječiti, moguće je poduzeti mjere ograničavanja potencijalne štete.

Uzimajući navedeno u obzir, mjere sigurnog korištenja bankovnih kartica u ovom dokumentu podijeljene su u dvije kategorije:

1. Minimizacija vjerojatnosti uspješne krađe
2. Ograničavanje štete potencijalne krađe

3.1 Minimizacija vjerojatnosti uspješne krađe

3.1.1 Fizička zaštita kartice

Izrazito je bitno nikada ne ostavljati karticu bez nadzora, čak niti za vrijeme transakcije. Kao što je opisano u prethodnom poglavlju, nije potrebno ukrasti karticu kako bi se ukrali novci – za uspješnu krađu dovoljno je da, primjerice, zlonamjerni blagajnik ili konobar provuče karticu kroz ručni *skimmer* uređaj.

Uz to, ključno je ne davati drugima da koriste karticu. Druga osoba ne mora nužno biti zlonamjerna da bi se dogodila krađa – dovoljno je samo da bude neoprezna.

Od dobro sakrivenog *skimmer* uređaja na bankomatu ili čak POS uređaju teško se zaštititi. No, moguće je izbjegavati korištenje bankomata ili POS uređaja ako oni izgledaju sumnjivo, primjerice ako imaju dijelove koji se ne čine kao da su zaista dio uređaja. Sumnjive bankomate, POS uređaje, osobe i slično najbolje je smjesta prijaviti banci ili policiji.

3.1.2 Zaštita prilikom kupovine na Internetu

Prilikom kupovine na Internetu ili korištenja internetskog bankarstva, ključne su dvije stvari:

1. Zaštita računala/pametnog telefona koji se koristi za plaćanje ili korištenje internetskog bankarstva
2. Zaštita mrežnog prometa

Računalo odnosno pametni telefon moguće je zaštititi od većine prijetnji tako da se:

- Redovito ažurira softver
- Koristi antivirusni softver (eng. *anti-virus/anti-malware software*)

- Ne preuzimaju niti otvaraju sumnjive aplikacije odnosno datoteke

Bitno je imati na umu da iako korisnik možda održava svoj vlastiti uređaj sigurnim, to ne znači da su javna ili zajednička računala sigurna. Primjerice, neovisno o tome koliko je korisnik oprezan, računalo u knjižnici ili računalo koje korisnik dijeli s obitelji može biti zaraženo tuđom krivicom. Upravo zato, takva računala treba izbjegavati kada je u pitanju kupovina preko Interneta ili internetsko bankarstvo.

Uz sigurnost uređaja, potrebno je osigurati i mrežni promet. Prilikom kupovine preko Interneta i internetskog bankarstva, zaštita mrežnog prometa se većinom svodi na korištenje HTTPS protokola. Drugim riječima, kako bi korisnik ostao siguran, nužno je unositi podatke isključivo na HTTPS Web stranicama. Konkretno, prilikom unosa podataka potrebno je obratiti pozornost na to da adresa Web stranice započinje s „https://" te da se u Web pregledniku pored adrese nalazi slika zelenog lokota.

3.1.3 Zaštita tajnosti PIN-a

Nakon kompromitacije kartice, tajnost PIN-a često predstavlja zadnju liniju obrane te je zato potrebno obratiti posebnu pažnju na odgovarajuće mjere zaštite.

To znači da isključivo vlasnik kartice smije znati svoj PIN. Često korisnici ne znaju da svoj PIN ne moraju reći ni policiji ni banci, nikome. Ako bilo koja osoba ili Web stranica traži PIN od vlasnika kartice, gotovo je sigurno da se radi o prevari – u takvim slučajevima najbolje je smjesta prijaviti incident banci.

Jednom kada vlasnik kartice dobije ili postavi novi PIN, potrebno ga je zapamtiti i nigdje ne zapisivati. Izrazito je bitno da PIN nigdje ne bude zapisan te da bilo koji zapisi gdje PIN možda i je zapisan, primjerice pismo od banke u kojemu je dostavljena kartica i PIN, budu sigurno uništeni. Na bankomatima nekih banaka moguće je promijeniti dobiveni PIN u neki drugi po vlastitoj volji.

Uz prevaru, kriminalci pokušavaju saznati tuđe PIN-ove skrivenim kamerama postavljenim oko bankomata i prodajnih mjesta ili jednostavnim gledanjem preko ramena. U takvim slučajevima, prekrivanje PIN-a prilikom unosa, kao što je prikazano na slici 10, značajno smanjuje rizike.

Slika 10 – Primjer pravilnog prikrivanja PIN-a prilikom unosa.

Konačno, nikakve mjere zaštite ne mogu zaštititi PIN koji je lako pogoditi. PIN-ovi kao što su „1234", datum rođenja i slični kriminalcima ne predstavljaju gotovo nikakvu prepreku. Ljudi su iznenađujuće slični i predvidljivi pri smišljanju lozinki i PIN-ova, tako da je najsigurnije koristiti nasumično generirani PIN.

3.2 Ograničavanje štete potencijalne krađe

Kako bi se šteta od potencijalne krađe svela na minimum, potrebno je:

1. Redovito pratiti promet na računima i pravovremeno primijetiti krađu

2. Izravno ograničiti količinu ukradenog novca

Danas je lako redovito provjeravati promet na računima putem internetskog bankarstva. Treba obratiti pažnju na bilo kakav sumnjivi promet te ga smjesta prijaviti banci. Za lakše uočavanje sumnjivog prometa, korisno je za usporedbu sačuvati račune i potvrde transakcija nakon svake kupovine i korištenja bankomata.

Kako bi prijava bila pravovremena, potrebno je unaprijed zapisati broj za prijavu ukradene kartice odnosno kartične prevare. No, čak i brza prijava krađe odnosno prevare nije uvijek dovoljna – kriminalci u kratkom roku mogu napraviti veliku štetu. Zato je važno i izravno ograničiti novčanu štetu potencijalnog napada.

U dogovoru s bankom obično je moguće postaviti ograničenja na dnevni promet kartice. Primjerice, moguće je ograničiti promet kartice na maksimalno 1.000kn dnevno. Ako korisnik u nekoj situaciji treba platiti veći iznos od dogovorenog ograničenja, moguće je pozivom banci kratkotrajno povisiti to ograničenje.

Alternativni ili dodatni način ograničavanja štete je držanje samo manje, ograničene količine novaca na računu povezanom s karticom. Neke banke nude mogućnost držanja novca u štednjama s mogućnošću uplate i isplate preko internetskog bankarstva. Na taj način moguće je neprekidno držati većinu novca na štednji koja nije povezana s nikakvom karticom. Taj novac onda ne može ni ukrasti preko kartice.

4 Zaključak

Od krađe kartice, preko kompromitacije korisničkih uređaja, bankomata, Web stranica pa do prevare – rizici prilikom korištenja bankovnih kartica su brojni. Prvi korak sigurnijeg korištenja bankovnih kartica uključuje svijest i razumijevanje odgovarajućih rizika.

Uz to, bitno je pravovremeno primijetiti potencijalnu prevaru. Danas je to relativno lako kroz redovito praćenje prometa internetskim bankarstvom. Ključno je bilo kakvu sumnjivu transakciju što prije prijaviti banci.

Neovisno o vrsti napada, uvijek je dobro i ograničiti potencijalnu štetu. To je moguće učiniti kroz ograničenja na karticama i držanje određene količine novca na računu povezanom s karticom.

Konačno, bitno je upoznati se s konkretnim mjerama zaštite prilikom korištenja bankovnih kartica kako bi se rizik od uspješnog napada sveo na minimum.

Oblici prevara razvijaju se svakodnevno. Stoga je važno redovito pratiti informacije o novim oblicima napada prevara i zloupotreba. Banke, udruženja banaka, policija i CERT promptno objavljuju upozorenja i upute.

5 Literatura

1. **Sigurnost na Internetu.** Sigurna uporaba kartica. [Mrežno] [Citirano: 27. prosinac 2017.] http://www.sigurnostnainternetu.hr/index.php/kako-se-zastititi/savjeti-za-gradane/item/49-sigurna-uporaba-kartica.
2. **Krebs, Brian.** All About Skimmers. *Krebs on Security.* [Mrežno] [Citirano: 8. prosinac 2017.] https://krebsonsecurity.com/all-about-skimmers/.
3. **Tomić, Dražen.** ZABA: Korisnici trebaju biti proaktivni kada je riječ o sigurnosti. *ICT Business.* [Mrežno] 10. ožujak 2017. [Citirano: 8. prosinac 2017.] http://www.ictbusiness.info/poslovanje/zaba-korisnici-trebaju-biti-proakitvni-kada-je-rijec-o-sigurnosti-2.
4. **Sigurnost na Internetu.** Sigurnosni mehanizmi banaka i preporuke za zaštitu. [Mrežno] [Citirano: 27. prosinac 2017.] http://www.sigurnostnainternetu.hr/index.php/novosti/item/3-sigurnosni-mehanizmi-banaka-i-preporuke-za-zastitu.
5. **Krebs, Brian.** Banking on a Live CD. *Krebs on Security.* [Mrežno] 12. srpanj 2012. [Citirano: 8. prosinac 2017.] https://krebsonsecurity.com/2012/07/banking-on-a-live-cd/.
6. —. Online Banking Best Practices for Businesses. *Krebs on Security.* [Mrežno] [Citirano: 8. prosinac 2017.] https://krebsonsecurity.com/online-banking-best-practices-for-businesses/.
7. —. Using Windows for a Day Cost Mac User $100,000. *Krebs on Security.* [Mrežno] 2. lipanj 2010. [Citirano: 8. prosinac 2017.] https://krebsonsecurity.com/2010/06/using-windows-for-a-day-cost-mac-user-100000/.
8. —. How Was Your Credit Card Stolen? *Krebs on Security.* [Mrežno] 19. siječanj 2015. [Citirano: 8. prosinac 2017.] https://krebsonsecurity.com/2015/01/how-was-your-credit-card-stolen/.
9. —. Peek Inside a Professional Carding Shop. *Krebs on Security.* [Mrežno] 4. lipanj 2014. [Citirano: 8. prosinac 2017.] https://krebsonsecurity.com/2014/06/peek-inside-a-professional-carding-shop/.
10. **Paya, Cem.** CVV1, CVV2, CVV3: Demystifying credit card data (1/2). *Random Oracle.* [Mrežno] 25. kolovoz 2012. [Citirano: 27. prosinac 2017.] https://randomoracle.wordpress.com/2012/08/25/cvv1-cvv2-cvv3-demystifying-credit-card-data-12/.
11. —. CVV3: Demystifying credit card verification (part 2). *Random Oracle.* [Mrežno] 11. rujan 2012. [Citirano: 27. prosinac 2017.] https://randomoracle.wordpress.com/2012/09/11/cvv3-demystifying-credit-card-verification-part-2/.
12. **Stross, Randall.** $9 Here, 20 Cents There and a Credit-Card Lawsuit. *The New York Times.* [Mrežno] 21. kolovoz 2010. [Citirano: 7. prosinac 2012.] https://www.nytimes.com/2010/08/22/business/22digi.html.
13. **IBM.** 2.4.2 "z/OS V1R3.0 ICSF Application Programmer's Guide" IBM Library Server. [Mrežno] [Citirano: 7. prosinac 2017.] http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/CSFB4Z20/2.4.2?SHELF=&DT=20020114105428.
14. **Hannah, Felicity.** Are contactless cards putting your cash at risk? *The Independent.* [Mrežno] 18. siječanj 2017. [Citirano: 12. prosinac 2017.] http://www.independent.co.uk/money/are-contactless-cards-putting-your-cash-at-risk-a7533091.html.

15. **Hoffmann, Allen i JD.** Before DarkNetMarkets Were Mainstream. *Deep Dot Web.* [Mrežno] 5. siječanj 2015. [Citirano: 8. prosinac 2017.] https://www.deepdotweb.com/2015/01/05/darknetmarkets-mainstream/.
16. **Consumer Action.** Questions and Answers About Credit Card Fraud. [Mrežno] 2009. [Citirano: 8. prosinac 2017.] https://www.consumer-action.org/downloads/english/Chase_CC_Fraud_Leaders.pdf.
17. **Square.** Chip Card Security: Why Is EMV More Secure? [Mrežno] [Citirano: 8. prosinac 2017.] https://squareup.com/townsquare/why-are-chip-cards-more-secure-than-magnetic-stripe-cards.
18. **Millward, David.** Don't bank on credit card security in the USA. *The Telegraph.* [Mrežno] 3. svibanj 2016. [Citirano: 8. prosinac 2017.] http://www.telegraph.co.uk/expat/money/dont-bank-on-credit-card-security-in-the-usa/.
19. **European Central Bank.** ECB releases final Recommendations for the security of internet payments and starts public consultation on payment account access services. [Mrežno] 31. siječanj 2013. [Citirano: 8. prosinac 2017.] https://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html.
20. **McMillan, Robert.** FTC Says Scammers Stole Millions, Using Virtual Companies. *PCWorld.* [Mrežno] 27. lipanj 2010. [Citirano: 7. prosinac 2017.] https://www.pcworld.com/article/199952/ftc_says_scammers_stole_millions_using_virtual_companies.html.
21. **BI Intelligence.** Here's why US EMV could be poised to rise in 2017. *Business Insider.* [Mrežno] 3. siječanj 2017. [Citirano: 8. prosinac 2017.] http://www.businessinsider.com/heres-why-us-emv-could-be-poised-to-rise-in-2017-2017-1.
22. **Wilson, Michael.** Pizza Orders Reveal Credit Card Scheme, and a Secondhand Market. *The New York Times.* [Mrežno] 5. prosinac 2014. [Citirano: 8. prosinac 2017.] https://www.nytimes.com/2014/12/06/nyregion/pizza-orders-reveal-credit-card-scheme-and-a-secondhand-market.html.
23. **Kessem, Limor.** The shifting panorama of global financial cybercrime. [Mrežno] [Citirano: 11. prosinac 2017.] https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03126usen/SEL03126USEN.PDF.
24. **Weisbaum, Herb.** Summer travel alert: Scammers target hotel guests. *NBC News.* [Mrežno] [Citirano: 8. prosinac 2017.] http://www.nbcnews.com/id/43662080/ns/business-consumer_news/t/summer-travel-alert-scammers-target-hotel-guests/.
25. **Abrams, Rachel.** Target to Pay $18.5 Million to 47 States in Security Breach Settlement. *The New York Times.* [Mrežno] 23. svibanj 2017. [Citirano: 8. prosinac 2017.] https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.
26. **Demos, Telis.** The evolution of the swipe - Manual imprint (1960) (1). *Fortune.* [Mrežno] 23. listopad 2008. [Citirano: 8. prosinac 2017.] http://archive.fortune.com/galleries/2008/fortune/0810/gallery.mastercard.fortune/.
27. **Square.** The State of the U.S. EMV Migration: When Will Everyone Have Chip Cards? [Mrežno] [Citirano: 8. prosinac 2017.] https://squareup.com/townsquare/the-state-of-the-u-s-emv-migration-when-will-everyone-have-chip-cards.
28. **IBM.** IBM100 - Magnetic Stripe Technology. [Mrežno] [Citirano: 28. prosinac 2017.] https://www-03.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/.

29. **Chamlee, Virginia.** How Restaurants and Diners Fall Victim to Credit Card Fraud. *Eater.* [Mrežno] 27. prosinac 2017. [Citirano: 8. siječanj 2018.] https://www.eater.com/2017/12/27/13676606/credit-card-fraud-restaurant-how-to-protect-yourself.