SUVREMENE OPASNOSTI ZA PODUZETNIKA: PREVARE U BANKARSKOM KARTIČNOM POSLOVANJU I NEOVLAŠTENO POVLAČENJE SREDSTAVA

Toni Miljak, mag.oec., Visoka škola za menadžment i dizajn Aspira, Mike Tripala 6, 21 000 Split, tony.miljak@gmail.com, +38591/517-35-25
Maximilian Ivan Fechner, student Visoke škole za menadžment i dizajn Aspira, Mike Tripala 6, 21 000 Split, maximilianivan@hotmail.com, +38599/698-44-32

Sažetak

Zaštita identiteta i osobnih podataka u Republici Hrvatskoj definirana je Zakonom o zaštiti osobnih podataka. U suvremenom elektroničkom, gotovo savršenom svijetu, dolazi do novih oblika kriminala vezanih uz korištenje računala.
Posebno su zanimljive krađe identiteta i prevara u bankarskom poslovanju koje se koriste za neovlaštena povlačenja s poduzetnikovih računa. Zemlje Europske unije označile su 28. siječnja kao Dan zaštite podataka.
U ovom radu opisuju se najčešće vrste prevara kojima su izloženi poduzetnici, kao i načini kako se one mogu spriječiti. Također, pojasnit će se načini na koje poduzetnik treba reagirati u slučaju prevare te što učiniti u slučaju takvog oblika kriminala.

Ključne riječi: bankovna kartica, cyber kriminal, krađa identiteta, prevare u bankarskom poslovanju, skimming

1. Identitet

Identitet je individualna karakteristika odnosno osobina po kojoj je predmet ili osoba prepoznatljiva ili znana. Postoje razne vrste identiteta: nacionalni identitet, regionalni identitet, elektronički identitet itd. Elektronički identitet predstavlja skup podataka o pojedincu koji se koristi za potrebe provjere identiteta i prava pristupa (autorizacija). Pamti se u posebnoj bazi podataka i sadrži korisničku oznaku koja na jednoznačan način opisuje korisnika te zaporku koja je poznata isključivo korisniku (PBF, 2013.).

1.1. Zaštita identiteta i osobnih podataka

U općoj deklaraciji Ujedinjenih naroda o ljudskim pravima od 10. prosinca 1948. godine navodi se: "*Nikoga se nesmije uznemiravati samovoljnim miješanjem u njegov privatni život, njegovu obitelj, njegov stan, njegovo privatno dopisivanje niti napadom na njegovu čast i ugled.*"

Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda od 04. studenog 1950. godine u članku 8. navodi kako svatko ima pravo na štovanje svog osobnog i obiteljskog života, prebivališta i dopisivanja. Vlasti se neće uplitati u to pravo, osim u skladu sa zakonom i kad je to potrebno u interesu javne sigurnosti, sprječavanju kaznenih djela i sl.

Zaštita identiteta i osobnih podataka fizičkih i pravnih osoba u Republici Hrvatskoj osigurana je Zakonom o zaštiti osobnih podataka (Narodne novine, 2012.). U Članku 1. tog zakona navodi se "*Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka*." Sadržaj ovog zakona ujedno predstavlja Konvenciju koju su donijele i potpisale članice Vijeća sigurnosti u Strassbourgu 28. veljače 1981. godine. Potpisnica ove konvencije je i Republika Hrvatska kao članica Vijeća Europe (Alfa portal, 2013.).

Osim osobnih podataka štite se i javni podaci. Zaštita podataka također se koristi kod prijenosa podataka osjetljivog sadržaja (vladinih, korporacijskih, bankarskih, itd.). Potrebno je zaštiti i podatke na vlastitom računalu od neovlaštenih upada. Osobne podatke pojedinaca posjeduju poslodavci, državne institucije, mobilni operateri, banke i mnogi drugi.

1.2. Krađa identiteta

Krađa identiteta najneugodniji je oblik krađe podataka kako za pojedinca tako i za poduzetnika. Uobičajeno se definira kao oblik kriminalne radnje lažnog predstavljanja radi stjecanja materijalne ili druge koristi.

Nekoliko najčešćih pojavnih oblika krađe identiteta su (Alfa portal, 2013.):

- spoofing (posebno opasan oblik prevare za usluge e-bankarstva) – podrazumijeva kreiranje lažne ili krivotvorene verzije nečega poput Web lokacije ili adrese elektronske pošte: korisnk se prijavljuje sa svojim korisničkim imenom i lozinkom koje tako dolaze u ruke kriminalaca, a oni ih zlorabe za pristup stvarnoj Web lokaciji;

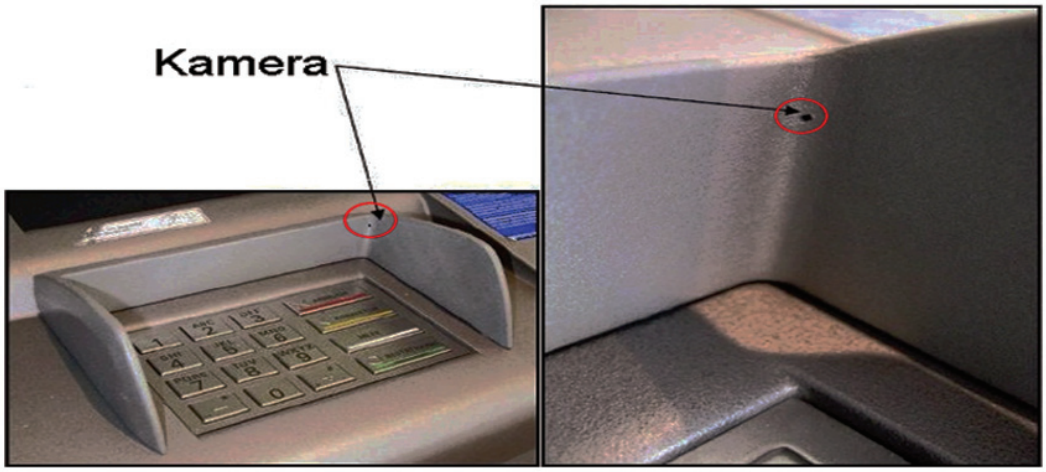
- phising – napadi predstavljaju najštetniji napad prevaranata: mnogi počinju e-mail porukom gdje se korisnika obavještava o problemu s računom te se traže podaci od istog kako bi se taj problem riješio; ponekad se samo stavi poveznica s internetskom stranicom koja je skoro ista kao originalna stranica banke preko koje korisnik posluje i uljudno zamole da se prijavite na stranicu s vašim podacima. Te se informacije prosljeđuju prevarantu, a on uzima s računa sav Vaš novac. Korisniku koji je žrtva "phising-a" može pomoći ako promijeni lozinku ili PIN na svojim računima ili kontaktira banku čije usluge koristi te čak zatvori račun;

- vishing – je slično kao i “phising”, ali se neovlašeno prikupljanje podataka obavlja putem telefonskog poziva;
- skimming (oblik neovlaštenog prikupljanja kartičnih podataka na prodajnim mjestima i bankomatima – kopiranje/krađa magnetskog zapisa) – najčešće se odvija na način da se u bankomat ugradi lažni čitač koji kopira podatke s magnetskog zapisa kartice te mini kamera koja snima utipkavanje PIN-a: novac nestane s računa, a da se kradljivac i poduzetnik ne nalaze ni na istom kontinentu.

Na slikama 1. i 2. prikazane su lažne tipkovnice, kao i kamere koje kradljivci ugrađuju na bankomate.

Slika 1. Lažna tipkovnica (The local portal, 2013.)

Slika 2.: Kamera na bankomatu (SGKB, 2013.)



Šteta nastala krađom podataka i povredama privatnosti na godinu premašuje dvostruku vrijednost svjetskog narkotržišta. Ovakve krađe spadaju u cyber kriminal koji sve više raste i pogađa sve veći broj fizičkih i pravnih osoba. Cyber kriminal je svaka kriminalna radnja koja podrazumijeva upotrebu umreženog računala.

2. Prevare u bankarskom poslovanju

Od osnivanja prve banke današnjeg tipa, Banco di San Giorgio, u Italiji u 15. stoljeću, (Moj bankar, 2013.) osnovna djelatnost banke je pružanje financijskih usluga. Tradicionalne usluge banke su primanje depozita, što ujedno predstavlja i izvor sredstava za davanje kredita te pružanje novčanih transkacije. Razvojem bankarstva dolazi i do razvoja raznih prevara u bankarskom poslovanju, kao npr. prevare i zlouporabe zaposlenika, krivotvorevine novčanica, kreditne prevare, prevare čekovima, menadžerske prevare, prevare u financijskim izvještajima, prevare unutar informatičkih sustava, kartične prevare, itd.

Kartica ili bankovna kartica je plastična kartica s magnetnom trakom koja sadrži čitljiv identifikacijski broj i koja je izdana od strane banke ili kartičarske kuće. Najčešće se koriste na POS terminalima, internetu ili bankomatima. Vlasnici takvih kartica su fizičke i pravne osobe odnosno poduzetnici.

U tablici 1. prikazan je broj poslovnih jedinica banaka te bankomata i POS (EFTPOS) uređaja u Republici Hrvatskoj na dan 30.09.2012. godine (HNB, 2013.).

Tablica 1. Poslovne jedinice banaka, bankomati prema funkcijama i POS (EFTPOS) uređaji / ukupno/

Prikaz poslovnih jedinica banaka, bankomata prema funkcijama i POS (EFTPOS) uređaja na dan 30.09.2012. godine	
	UKUPNO
1. Poslovne jedinice	**1.263**
2. Bankomati ukupno	**4.082**
2.1. Bankomati u vlasništvu banaka*	3.419
- isplatni	3.413
- uplatno/isplatni	228
- transakcijski	0
- za punjenje e-novca	0
- s videonadzorom	1.067
- u osiguranom prostoru	738
2.2. Bankomati u vlasništvu druge pravne osobe	663
- isplatni	663
- uplatno/isplatni	31
- transakcijski	0
- za punjenje e-novca	0
- s videonadzorom	207
Prikaz poslovnih jedinica banaka, bankomata prema funkcijama i POS (EFTPOS) uređaja na dan 30.09.2012. godine	
	UKUPNO
- u osiguranom prostoru	33
3. POS (EFTPOS) uređaji ukupno	**90.294**
3.1. POS (EFTPOS) uređaji u vlasništvu banaka	51.748
3.2. POS (EFTPOS) uređaji u vlasništvu druge pravne osobe	38.546
*** Jedan bankomat može imati više funkcija.**	

Kartica, za koju je najčešće rabljeni naziv plastični novac, instrument je plaćanja koji se razvija sredinom 20. stoljeća. Prva bankovna kartica predstavljena je 1958. godine što ujedno predstavlja početak nove ere s obzirom da gotovina gubi dominaciju na tržištu. Iako se i gotovina krivotvori, kartice su ipak daleko više na meti prevara, pogotovo u današnje vrijeme visokih tehnologija u kojem se „kreativnost“ u prevarama svakodnevno gotovo eksponencijalno širi.

Stoga banke svake sekunde moraju imati oči širom otvorene kako bi svoje klijente i korisnike zaštitili od prevara i krađa (Moj bankar, 2013.).

Činjenica je da netko uvijek nađe način da se „provuče" kroz sigurnosni sustav kartičara. Prema Visinim podacima taj je trend u Europi u stalnom opadanju, više zbog uvođenja čipa na kartice, što predstavlja sigurnije kartično poslovanje. Kartice i dalje imaju jedinstven elektronički kod, ali taj kod kod kartica s čipom se mijenja i predstavlja veću sigurnost u poslovanju.

Zemlje članice EU-a 28. siječnja obilježavaju Europski dan zaštite podataka kojim se ističe važnost zaštite privatnosti europskih građana i poduzetnika, a ponajprije njihovih osobnih podataka.

Temeljem ispitivanja koje je provela Europska komisija pokazalo se da tek nešto više ispitanika, 52 posto, smatra da su njihovi osobni podaci u njihovoj zemlji dostatno zaštičeni, a većina, 82 posto, smatra da je svijest ljudi o zaštiti osobnih podataka u njihovoj zemlji niska. Gotovo 75 posto ispitanika reklo je da se boje ostaviti svoje podatke na internetu, a što se tiče kreditnih kartica s praćenjem se slaže gotovo 70 posto ispitanika.

Prema informacijama predstavnika hrvatskih banaka, u Republici Hrvatskoj kartičnih prevara ima manje nego u zemljama Europske unije. U Hrvatskoj je postavljeno oko 4.000 bankomata i oko 90.000 POS uređaja. U prometu se nalazi 8,5 milijuna kartica, odnosno 2,2 kartice po stanovniku. Prva krađa PIN-a na bankomatima u Hrvatskoj je zabilježena 2004. godine dok je taj oblik prevare u svijetu poznat i ranije.

2.1. Nastanak prevare

Prevare u kartičnom poslovanju nastaju pojedinačno ili u sklopu međunarodno organiziranog kriminala, a vezane su uz:

- gubitak/krađu kartica
- otuđenje kartica na bankomatima
- krivotvorenje kartica
- neovlaštenog prikupljanja kartičnih podataka na prodajnim mjestima i bankomatima (skimming)
- neovlaštene (hakerske) upade u sustave prodajnih mjesta, banaka ili procesora s ciljem pribavljanja kartičnih podataka
- neovlašteno prikupljanje kartičnih podataka putem e-maila (phising), telefonskog poziva (vishing)
- zlouporabe prodajnih mjesta (npr. svjesni prihvat krivotvorenih kartica/izgubljenih/ukradenih kartica, propust zaposlenika prodajnih mjesta zbog neprovjeravanja sigurnosnih karakteristika kartice prilikom provođenja transakcija i slično)

- neovlašteno korištenje kartičnih podataka iniciranjem transakcija putem kataloške prodaje (poštom ili telefonom) i putem E-commerce-a (internet prodaja).

- Osnovne prevare na bankomatu koriste nepažnju vlasnika kartice dok se razrađenije metode zasnivaju na upotrebi različitih uređaja kojima se kopiraju osjetljivi podaci s kartice i/ili PIN. Na bankomatu se kriminal čini na nekoliko načina:

- promatranjem - metoda prevare tokom koje kriminalci posmatraju za vrijeme unošenja PIN-a pokušavajući uočiti i zapamtiti PIN, a potom kradu karticu koristeći se džeparenjem ili odvlačenjem pozornosti;

- upotrebom kartične petlje - vrlo jednostavna i djelotvorna metoda koja koristi "uređaj" (često je dovoljna samo gumica ili plastična vrpca) koji se umetne u utor čitača kartica na bankomatu sa ciljem da zadrži umetnutu karticu u bankomatu; zbog umetnute plastične vrpce ("libanonska petlja"), čitač karticu ne može uvući i obraditi je, a kartica ostaje zadržana u plastičnoj vrpci i nedostupna korisniku; nakon što korisnik bankomata odustane od transakcije i napusti bankomat ostavljajući karticu u njemu, kriminalci uklone petlju i karticu: ukoliko nekom od metoda otkriju i broj PIN-a (npr. praćenjem unosa PIN-a, korištenjem skrivene kamere i slično) daljnja zloupotreba kartice je jednostavna i praktično bez rizika za kriminalca;

- skimming - skimming uređaj kriminalci priključuju na utor čitača kartice radi kopiranja podataka s magnetne staze kartice; pripadajući PIN kod se dobavi posmatranjem njegovog unosa ili putem skrivene mikrokamere; kopirani podaci s originalne kartice prenose se na novu, krivotvorenu karticu; korištenjem krivotvorene kartice kriminalci mogu podizati novac na bankomatu (ukoliko su otkrili i PIN) ili iskoristiti krivotvorenu karticu za plaćanje preko interneta i slično.

Metoda motrenja preko ramena je najprimitivnija metoda usmjerena na neoprezne i pojedinačne vlasnike kartica. S druge strane, kartična petlja i skimming koriste se od organiziranih kriminalnih grupa koje za posljedicu imaju masovniju štetu. Također, u slučaju zadržavanja kartice vlasnik kartice svjestan je da je ostao bez kartice (mada ne zna pravi razlog). Skimming je sofisticiranija metoda obzirom da vlasnik kartice nije svjestan da su podaci s kartice kompromitirani sve dok se neovlaštena transakcija ne obavi.

2.2. Načini otkrivanja prevare

Prevara se najčešće otkriva:

- reklamacijom samih korisnika kartičnog poslovanja
- banke, odnosno kartične kuće, u postupcima uslijed dnevnih praćenja autorizacija i transakcija za kartice koje su izdale
- banke, odnosno kartične kuće, otkrivaju prevare uslijed dnevnih praćenja prodajno – isplate mreže
- temeljem informacija dobivenih od drugih banaka, kartičnih kuća ili MUP-a.

2.3. Sankcioniranje prevare

U slučaju kartične prevare sumnjive kartice se u najkraćem mogućem roku blokiraju, a klijenti, odnosno poduzetnici, dobivaju nove kartice u roku od nekoliko dana. Ukoliko se utvrdi prevara, banke, odnosno kartične kuće, u potpunosti namiruju oštećenima izgubljenu financijske imovinu i učinjene troškove te potom u daljnjim postupcima one potražuju sredstva od osiguravajuće kuće ili od treće strane koja je odgovorna za štetni događaj.

Kartična prevara podliježe prema Zakonu o Platnom prometu (Zakon portal, 2013.) kaznenoj prijavi, a da bi pokrenuo postupak poduzetnik treba priložiti sljedeću dokumentaciju (ovisno o vrsti prevare):

- pisanu izjavu da vlasnik kartice (poduzetnik) nije učinio transakcije za koje ga se tereti
- obavijest o učinjenim troškovima
- potpisanu Izjavu o krađi / gubitku / zlouporabi kartice
- kopije transakcijskih slipova (ako su dostupni)
- dokumentaciju dobivenu od prodajnog mjesta (npr. ukoliko hotel ima kopije osobnih iskaznica)
- drugu raspoloživu dokumentaciju.

Važno je da poduzetnik u izjavama navede ukupan iznos štete u kunama i originalnoj valuti ako se radi o zloupotrebi u inozemstvu. Banke i kartičarske kuće obavezno trebaju obavijestiti MUP te podnijeti kaznenu prijavu.

Bitno je naglasiti da 0,3% ukupnih transakcija jesu zlouporabe kartica. Upotrebom kartica na način predviđen ugovorom, korisnik je 100% siguran od moguće zlouporabe. Štetu kod slučajeva zlouporabe pokriva banka ili kartična kuća (Gregurek, M., Vidaković, N., 2011.).

Zaključak

Osim brojnih prednosti moderne tehnologije imaju i određene nedostatke. Kod bankarskog poslovanja to se prije svega odnosi na krađe identiteta zbog kojih poduzetnik može doživjeti neugodnosti jer kratkoročno može ostati bez financijskih sredstava dok ih banka, odnosno kartična kuća, ne isplati. Naime, financijske institucije u potpunosti poduzetnicima namiruju izgubljenu financijsku imovinu i učinjene troškove.

Poduzetnici moraju biti upoznati sa svim oblicima krađe identiteta kako bi spriječili njhove eventualne nastanke, a samim time i poteškoće u svakodnevnom poslovanju.

Posljednjih godina banke u Republici Hrvatskoj uspješno su se nosile s kriminalcima koji su nastojali biti uvijek korak ispred. I kod nas i u svijetu s razvojem tehnologije sigurnost kartičnog poslovanja postaje gotovo besprijekorna iz čega proizlazi da je od ukupno svih obavljenih transakcija bankovnim karticama samo njih 0,3% predstavljalo zloupotrebu kartica.

MODERN THREATS TO BUSINESSES: FRAUDS IN THE BANKING CARD BUSINESS AND UNAUTHORIZED WITHDRAWAL OF THE PROCEEDS

Abstract

Protection of identity and personal data in the Republic of Croatia is provided by the Law on the Protection of Personal Data. In the modern, electronic almost perfect, world comes to new forms of crime associated with computer use.

Especially interesting are the identity theft and fraud in the banking business which are used to unauthorized withdrawals from entrepreneur's account. The EU countries mark 28th January as European Data Protection Day. This paper will outline most common types of fraud that have been exposed as entrepreneurs and how these can be prevented. Also, it will clarify the ways that an entrepreneur needs to react and what to do in case of such forms of crime.

Key words: bank card, cyber criminal, fraud in the banking business, identity theft, skimming

Literatura

- Gregurek, M., Vidaković, N. (2011.) Bankarsko poslovanje, Zagreb:RRIF-plus, str.62.
- http://www.alfa-portal.com/obrazovanje-2/life-long-learning/europski-dan-zastite-podataka (sačuvano 18.06.2013.)
- http://www.hnb.hr/platni-promet/h-statisticki-podaci (sačuvano 19.06.2013.)
- http://www.pbf.unizg.hr/hr/sluzbe/informaticka_sluzba/elektronicki_identitet (sačuvano 18.06.2013.)
- http://www.moj-bankar.hr/Kazalo/K/Kartice- (sačuvano 17.06.2013.)
- http://www.zakon.hr/z/86/Zakon-o-platnom-prometu (sačuvano 18.06.2013.)
- Zakon o zaštiti osobnih podataka, NN 106/12, Zagreb