UDK 339.13:004.738.5

Kako varno je nakupovanje na spletu

*Gorazd Žagar**

ONLINE SHOPPING SAFETY
In the past, banks were targeted by criminals because they stored a large amount of money in form of cash or gold. Nowadays access to money is made possible through online shops where merchants store their customer data alongside with credit card information and fundamentally neglect to take the necessary security precautions to prevent unauthorized access by hackers worldwide. Most breaches occur through the exploitation of web applications. Stolen data is then most likely sold on underground forums and IRC channels. Credit card fraud is a serious problem which can potentially affect every online shopper. This article addresses possible misuses and suggests guidelines for safer handling of payment data.

JEL L81 02

V 20. stoletju je veljalo, da so bile tarče roparjev banke, saj so hranile večje količine denarja v materialni obliki. V digitalni dobi večjih količin denarja ne hranijo zgolj banke, ampak posredno tudi vsi trgovci, ki ob nakupu shranijo podatke o uporabljenem plačilnem sredstvu. Zaradi neupoštevanja uveljavljenih standardov varovanja podatkov in slabih praks so mnogi trgovci pogosto tarča kriminalcev, ki se poskušajo na različne, mnogokrat povsem enostavne načine, dokopati do številk plačilnih kartic in magnetnih zapisov na njih.

1. Uvod

Od januarja leta 2005 so kiberkriminalci odtujili že več kot 510 milijonov občutljivih osebnih podatkov, katerih pretežni del predstavljajo plačilne kartice[1]. Podatki o plačilnih karticah, skupaj z osebnimi podatki lastnika, predstavljajo kiberkriminalcem orodje za zlorabo. Če kraja osebnih podatkov ni pravočasno ugotovljena in prijavljena ustreznim institucijam, obstaja verjetnost, da bomo hitro ostali brez denarja na svojem bančnem računu.

Članek prinaša pregled plačilnih instrumentov, ki so v uporabi na svetovnem spletu, pojasnil, kako se do njih dokopljejo kiberkriminalci in jih zlorabijo, in podatkov o tem, kaj na drugi strani zagotavljajo trgovci ter ponudniki informacijsko-komunikacijskih storitev, da bi nas obvarovali pred zlorabami. Uporabljajo morda kakšne posebne varovalne mehanizme, standarde, priporočila, ki tovrstne zlorabe omejujejo?

* Gorazd Žagar, dipl. inž. rač. in inf., je samostojni, neodvisni raziskovalec informacijske varnosti, ki se tematiki ljubiteljsko posveča že 15 let. Ob prostem času ureja priljubljeni blog Infosec (http://infosec.si) in ponuja svetovanje na področju vpeljave dobrih praks varovanja informacij.

Spoznali bomo, da lahko za varovanje svojih osebnih podatkov veliko storimo tudi sami tako, da se pravočasno seznanimo z grožnjami.

Plačilne metode, ki se uporabljajo na spletu

Kreditne kartice

Koncept kreditne kartice je bil prvič predstavljen že davnega leta 1887, takšne kot jih poznamo danes, z magnetnim zapisom, pa smo dobili v uporabo v 70-tih letih prejšnjega stoletja.[2] Kreditna kartica običajno vsebuje (vsaj):

- 13- do 16-mestno številko, ki sestoji iz šestmestne številke izdajatelja (ang. Issuer Identification Number), sledi številka računa imetnika, zadnja cifra predstavlja validacijsko kodo (ang. Validity Check Code),
- datum veljavnosti (ponekod tudi datum izdaje),
- ime in priimek lastnika,
- magnetni zapis,
- novejše kartice imajo tudi čip (ang. smartcard),
- nekatere celo čip RFID (ang. Radio Frequency Identification) in
- na zadnji strani kartice 3- do 4-mestno kodo CVC (ang. Card Verification Code, imenovano tudi CVV oz. CVV2) ter lastniški podpis.

Spletno nakupovanje z uporabo kreditne kartice je bilo prvič omogočeno leta 1994, ko nam je podjetje Intershop ponudilo prvo spletno prodajalno.[3] Danes je kreditna kartica na svetovnem spletu najbolj razširjeno plačilno sredstvo in posledično tudi najbolj izpostavljeno zlorabam.

Nakup na spletu opravimo tako, da vpišemo v spletni obrazec zahtevane podatke o svoji kartici in lastniku ter po potrebi tudi dodatne podatke, ki niso del kartice (npr. avtorizacijsko geslo). Najpogosteje se kartica bremeni v trenutku, ko trgovec odpremi naročeno blago ali izvede storitev. Poročilo o porabi sredstev na kreditni kartici lahko spremljamo prek spletnega bančništva ali z mesečnimi bančnimi izpiski.

Nakazilo na bančni račun

Nakazilo na bančni račun spletnega trgovca za nakup storitve ali blaga je varnejša alternativa za tiste, ki spletnemu mestu ne želijo zaupati svojih podatkov o kreditni kartici. Kupec pri svoji banki ali prek spletnega bančništva opravi nakazilo na bančni račun trgovca. Možnosti za zlorabo so v tem primeru zelo omejene. Tako plačevanje je pogodu tudi trgovcem, saj se izognejo plačilu provizije, ki običajno znaša od enega do treh odstotkov pri transakcijah s kreditnimi karticami.

Moneta

Moneta je priročna in varna storitev plačevanja z mobilnikom, ki jo lahko uporabimo tudi za spletno nakupovanje, a zaenkrat zgolj v slovenskih spletnih trgovinah. Moneto podpirajo operaterji Mobitel, Si.Mobil in Debitel.[4] Plačevanje poteka tako, da nakup v spletni trgovini potrdimo z vnosom štirimestne kode, ki jo prejmemo v obliki SMS na svoj mobilnik. Nakupe plačamo enkrat mesečno z računom pri svojem operaterju.

PayPal

PayPal je storitev, ki omogoča plačevanje in prejemanje denarja na lastnikov račun, ki je lahko povezan s kreditno ali debetno kartico. Lastnik računa PayPal lahko svoj spletni račun poveže direktno s plačilno kartico ali pa prek storitve MoneyPak (na voljo samo v ZDA) sredstva tudi nakaže. Vsak lastnik računa PayPal lahko prejme nakazila drugih imetnikov računa. Uporaba računa in izvedba transakcije zahtevata vnos elektronskega naslova in pripadajočega gesla. PayPal za vsako transakcijo odvzame nakazatelju provizijo za storitev, hkrati pa ponuja zavarovanje transakcij.

Bitcoin

Bitcoin je prva decentralizirana navidezna valuta, ki deluje na podlagi navideznih kovancev, s katerimi je že možno trgovanje na svetovnem spletu. Od drugih sorodnih sistemov se Bitcoin razlikuje v tem, da:

- se transakcije izvajajo brez posrednikov in tako rekoč brez provizij,
- valuta je veljavna povsod po svetu,
- računa ni mogoče zamrzniti in
- ni pogojev za imetnike računov ter ni limita.

Vse transakcije so anonimne in opremljene z elektronskim podpisom. Hranijo se trajno v omrežju. Z odprtjem računa ni povezanih stroškov, kovance lahko vsakdo prejema ali pošilja brez omejitev, kar je že privedlo do tega, da danes valuto močno uporabljajo za trgovanje z drogo in za vplačila pri igrah na srečo. Danes je valuta Bitcoin že sprejeta kot veljavno plačilno sredstvo v nekaterih spletnih trgovinah in ima trenutno vrednost okrog 1 bitcoin = $ 20[20].

Elektronske valute

Pričakovati je, da bodo postale elektronske valute, imenovane tudi elektronski oz. digitalni denar (krajše e-denar, ang. E-Cash)[5], vse pogosteje uporabljeno plačilno sredstvo za plačilo blaga ali storitev na svetovnem spletu. Centralizirani sistemi PayPal, WebMoney, cashU, ki so v uporabi že vrsto let, omogočajo prenos sredstev na t.i. digitalno denarnico, s katero plačujemo na spletu. Decentralizirani sistemi, kot so Bitcoin in Ripple monetary system, so še najbolj podobni pravemu papirnatemu denarju in si prizadevajo za zagotavljanje anonimnosti tako imetnika računa kot samih transakcij.[6] V nasprotju s centraliziranimi sistemi decentralizirani ne omogočajo vplačil ali izplačil v druge valute.

Zlorabe pod drobnogledom

O vdorih v spletne strežnike poročajo spletni mediji že skoraj vsak teden. Zadnji odmevnejši vdor se je zgodil v omrežje Sony PlayStation, od koder naj bi zaenkrat še neznani napadalci odtujili poleg podatkov o računih uporabnikov tudi podatke o plačilnih karticah. Čeprav Sony zatrjuje, da so bili podatki o kreditnih karticah v nasprotju z osebnimi podatki kodirani, je med uporabniki prisoten upravičen dvom.[7] Namreč, na spletnem forumu zloglasne skupine 4chan[8] se je pojavil prispevek nekoga, ki je trdil, da je bila v podatkovni bazi shranjena ob številki kreditne kartice tudi koda CVV2.[9] Poleg tega pa je Sony prosil svoje uporabnike, naj se pri svoji banki pozanimajo o postopku preklica kreditne kartice. Računov s podatki o kreditni kartici naj bi bilo po poročanju v podatkovni bazi več kot 2,2 milijona in zagotovo so podatki že naprodaj na podzemnih spletnih forumih in strežnikih IRC (ang. Internet Relay Chat). Leta 2009 so aretirali hekerja Rogelia Hacketta, ki je s prodajo več kot pol milijona kreditnih kartic in z njimi povezanimi zlorabami povzročil 36-milijonsko izgubo[1]. Izsledili so ga na podzemnih spletnih forumih in strežnikih IRC, na katerih je za ukradeno številko kreditne kartice zahteval med 20 in 25 ameriških dolarjev. Tako visoko ceno, ki več kot 10-krat višja od povprečne cene ukradene kreditne kartice na trgu[10], je lahko dosegel le zaradi zaupanja (stalnih) kupcev, ki so vedeli, da kartica še ni bila nikoli zlorabljena.

Podatki o plačilnih karticah predstavljajo kriminalcem orodje za zlorabo.

Med trgovci se je za tovrstne številke ukradenih kreditnih kartic uveljavil izraz »nedolžna kartica« (ang. virgin card).

Samo v Veliki Britaniji je letni strošek zlorab, povezan s krajo in preprodajo ukradenih plačilnih kartic, že presegel 30 milijard funtov in je iz leta v leto višji.[11] Kolikšen delež teh zlorab predstavljajo zlorabe, ki se zgodijo izključno na svetovnem spletu, mi ni znano. Na svetovnem spletu se dogajajo zlorabe vseh plačilnih sredstev, ki smo jih spoznali, razen decentraliziranih sistemov, ki naj bi jih bilo nemogoče zlorabiti. Za zlorabo kreditne kartice danes ne zadostuje več zgolj poznavanje njene številke na prednji strani skupaj z datumom poteka. Do podatkov o številkah ter drugih povezanih podatkov o lastniku se napadalci dokopljejo z

- vdorom v podatkovno bazo plačilnih kartic, ki ni kodirana,
- s prestrezanjem podatkov na transakcijskem strežniku,
- s prestrezanjem podatkov na domačih osebnih računalnikih kupcev,
- z nakupom na spletnih forumih in kanalih IRC ali
- drugače.

Spletni trgovec, ki podpira plačevanje s plačilnimi karticami, se lahko odloči, da bo kupcem omogočil vnovičen nakup, ne da bi bilo treba ponovno vnesti podatke o plačilnem sredstvu. Da je to mogoče, mora v svoji podatkovni bazi ob računu shraniti vse potrebne podatke, s katerimi je mogoče izvesti vnovično transakcijo. Spletna trgovina izvede transakcijo tako, da strežnik vzpostavi povezavo z banko ali pogosteje s transakcijskim strežnikom, ki igra vlogo posrednika. Del podatka plačilnega sredstva, katerega standard PCI-DSS (standard, ki ga bomo v prihodnosti še vzeli pod drobnogled) shranjevanje striktno prepoveduje, je koda CVV. Ta koda se uporabi za preverjanje istovetnosti lastnika kartice, saj je dostopna samo imetnikom fizične kartice. Ker spletne trgovine tega načela ne upoštevajo in kodo CVV shranijo ob številki kreditne kartice, ogrožajo svoje kupce. Največ vdorov v podatkovne baze se danes zgodi predvsem zaradi slabo zasnovane spletne aplikacije. Vrivanje SQL (ang. SQL injection) je že desetletje poznana tehnika, ki omogoča napadalcem izvajanje poljubnih poizvedb nad podatkovno bazo skozi vnosna polja spletnih aplikacij ali drugače in je najpogosteje uporabljena med napadalci dostopa do osebnih podatkov kupcev v spletnih trgovinah. Transakcijski strežniki podatkov ne hranijo in nastopajo le kot posredniki. Podatki se prenašajo v kodirani obliki, kar zahteva od napadalcev bistveno večji napor pri poskusu

prestrezanja. Nad kupce grozijo napadalci tudi z vdori v njihove osebne računalnike, pri čemer niso pametni telefoni in tablični računalniki nikakršna izjema. S pomočjo trojanskih konj, kot je Zeus, in z njihovo funkcionalnostjo prestrezanja podatkov ter beleženja pritiskov tipk se polastijo avtentikacijskih podatkov za dostop do spletnega bančništva. S pomočjo zbranih podatkov opravijo prenos sredstev na druge bančne račune, pogosto ravno tako odtujene, ki služijo kot vmesni člen pri nadaljnjemu prenosu.

Čeprav se zlorabe kreditnih kartic dogajajo pravzaprav v vsakem sistemu, ki omogoča plačevanje z njimi, se bomo omejili na zlorabe, ki se dogajajo na svetovnem spletu. Z uvedbo plačevanja s plačilnimi karticami na spletu so kriminalci dobili nov »teren« za zlorabe. Za spletno nakupovanje je značilno, da kupcu ni treba izročiti kartice niti nakupa avtorizirati na enak način, kot bi to storil osebno v nakupovalnem centru. Spletni trgovci so bili primorani pri vsakem nakupu predpostaviti, da je kupec dejansko tudi lastnik plačilne kartice. Sprva je plačevanje s kreditnimi karticami prek spleta potekalo tako, da je kupec prek spletnega vmesnika ali spletne pošte posredoval trgovcu podatke o kreditni kartici. Prenos podatkov je potekal v prosto čitljivi obliki. V tem času koda CVV še ni bila v uporabi, ravno tako se ni preverjalo lastnikovega naslova, zato je bilo treba trgovcu posredovati samo številko kartice in datum poteka. Trgovci so se s prodajo v svetovni splet sprva vključevali tako, da so enostavno razširili obstoječo prodajo še na splet. Za izvrševanje transakcij so uporabljali terminal POS (ang. Point Of Sale) v načinu CNP (ang. Card Not Present). Preverjanje veljavnosti plačilne kartice je bilo nezanesljivo in neučinkovito. Plačevanje je potekalo torej podobno kot naročanje prek telefona, kjer je kupec trgovcu posredoval plačilne podatke prek telefona. V tem času, med leti 1994–1998, so bili sila priljubljeni programi za generiranje številk kreditnih kartic, s pomočjo katerih je bilo mogoče generirati »veljavne« številke kreditnih kartic različnih izdajateljev, brez datuma poteka. Če je napadalec posedoval veljavno številko kreditne kartice, je lahko s pomočjo takšnih orodij izračunal sorodne številke kreditne kartice istega izdajatelja. Postopek se imenuje ekstrapolacija (ang. extrapolation). Sledil je korak v razvoju elektronskega poslovanja, kjer so se spletne prodajalne povezale s podjetji, ki opravljajo vlogo posrednika med njimi in bankami. Uvedli so transakcijske strežnike, ki lahko v realnem času preverijo veljavnost kreditne kartice ali celo opravijo transakcijo. V Sloveniji smo dobili prvi tak transakcijski strežnik, imenovan Kastor, leta 1999, uvedlo pa ga je podjetje EON v sklopu sistema Transact-EON[1]. Transakcijski strežniki, ki so povezani direktno z bankami, so postopoma pri preverjanju veljavnosti številke upoštevali čedalje več podatkov o lastniku. Sprva je bila to samo številka z datumom veljavnosti, nato je sledilo ime, kot je napisano na kartici, in naslov lastnika, konec prejšnjega stoletja pa se je postopoma začela uveljavljati koda CVV[13]. Dodatni koraki pri preverjanju veljavnosti so naredili programe za generiranje številk svesplošno neuporabne. Zlorabe se z uvedbo kode CVV niso končale. Kiberkriminalci so bili sedaj primorani dobiti v roke veljavne podatke. Povečalo se je število kraj plačilnih kartic, napadov s sleparjenjem in napadov z uporabo socialnega inženirstva, s pomočjo katerega bi se napadalci lahko dokopali še do drugih podatkov. Spletni trgovci so postali tarče napadalcev, ki so iskali zapise o preteklih transakcijah, skupaj z vsemi podatki o uporabljenih plačilnih sredstvih. Nekateri trgovci so izničili funkcionalnost kode CVV tako, da so to številko shranili v podatkovno bazo skupaj z drugimi podatki. Najnovejši poskus vpeljave zavarovanja pred zlorabami predstavljata dodatna nivoja, imenovana »Mastercard SecureCode« in »Verified by Visa«, ki bosta podrobneje predstavljena v naslednjem poglavju.

O vdorih v spletne strežnike poročajo spletni mediji že skoraj vsak teden.

Ko so podatki o kreditni kartici na svetovnem spletu odtujeni, je zanje zelo verjetno, da se bodo pojavili v bazah, s katerimi napadalci trgujejo na različnih podzemnih spletnih forumih in strežnikih IRC. Organiziran krog vključuje napadalce, ki podatke odtujijo s strežnikov, oškodovane trgovce in kupce ter osebe, ki opravijo zlorabo in prenesena sredstva prek nakazila Western Union ali drugače posredujejo nazaj.[1]. Preostali manjši delež zlorab predstavljajo zlorabe kreditnih kartic na spletu, kjer so te uporabljene za nakup izdelkov v različnih spletnih trgovinah.

Na hitro poglejmo možne zlorabe preostalih plačilnih sredstev. Da bi napadalec lahko Moneto zlorabil in opravil nakup na račun nekoga drugega, potrebuje dostop do avtorizacijske kode, ki se na zahtevo pošlje telefonsko s sporočilom SMS. Čeprav se v tem primeru zdi zloraba nemogoča, če napadalec nima dostopa do telefona, pa le ni povsem tako. Mobilni telefoni Nokia 1100, ki na spletni dražbi E-bay dosegajo

tudi vrtoglave cene prek $700, naj bi omogočali prestrezanje sporočil SMS na isti bazni postaji.[1]. Napadalec lahko s prestrezanjem sporočil SMS dostopa do avtorizacijskih kod, ki jih uporabniki prejmejo na svoj telefon GSM v primerih dvofaktorskih prijav v sisteme ali enofaktorskih, kot je Moneta.
Zloraba računa PayPal je mogoča, če napadalec posreduje uporabniško ime (spletni poštni naslov) in geslo. Opravi lahko neupravičen nakup blaga ali storitev, vendar je zaradi pravil poslovanja PayPala, ki v takšnih primerih oškodovance primerno varuje, povsem verjetno, da bodo ti dobili sredstva povrnjena na svoj račun.

Zavarovanje pred zlorabami

Zloraba plačilnega sredstva lahko posledično vodi k izgubi sredstev na povezanem bančnem računu. Da bi zlorabe omejili in spletne kupce pred njimi obvarovali, večinoma poskrbijo že trgovci sami, izdajatelji plačilnih instrumentov, zakonodaja, varnostni standardi, veliko pa lahko k varnosti prispevamo tudi sami. Zelo pomembno je, da se tudi sami seznanimo z grožnjami in vpeljemo v svoje življenje dobre prakse ravnanja z našimi plačilnimi sredstvi, predvsem pri transakcijah na spletu.
Če se najprej osredotočimo na spletne trgovce, ti poslujejo s partnerji, ki zanje opravljajo transakcije. Trgovcu se predajo uporabniški račun, certifikat ter druga navodila za vzpostavitev varne povezave s transakcijskim strežnikom. Trgovec lahko kupcem omogoča ustvarjanje računov, pod katerimi se hranijo podatki o plačilnemu sredstvu. Dostop do uporabniškega računa je navadno zavarovan z uporabniškim imenom in geslom. Zelo redko, če sploh, bo uporabniku na voljo prikaz celotne številke shranjene kreditne kartice, kar onemogoča krajo podatkov nekomu, ki nam račun odtuji. Lahko pa opravi neodobren nakup v našem imenu, morda tudi na drug naslov. Uporabnikom spletnih trgovin zato priporočam, da izberejo za spletne trgovine edinstveno geslo, ki ni v uporabi nikjer drugje.
Spletne trgovine, ki temeljijo na slabo zastavljeni ali slabo sprogramirani rešitvi, so lahko tarče napadalcev, ki z uporabo različnih metod poskušajo dostopati do podatkovne baze in iz nje pretočiti podatke o vseh kupcih, opravljenih nakupih ali

Spletni trgovci so postali tarče napadalcev, ki so iskali zapise o preteklih transakcijah.

transakcijah ter plačilnih sredstvih.
V primeru vdora v spletno trgovino smo kupci nemočni. Upamo lahko le, da je spletni trgovec uporabljal za zavarovanje podatkov v podatkovni bazi katero izmed ireverzibilnih kriptografskih metod, ki onemogočajo prosto berljivost in dešifriranje. Spletni trgovci lahko za boljšo varnost poskrbijo tudi tako, da svoje poslovanje standardizirajo po katerem izmed uveljavljenih standardov, npr. PCI-DSS. PCI-DSS strogo zapoveduje kriptiranje vseh ključnih podatkov o plačilnih karticah, prepoveduje hranjenja kode CVV2 ter zahteva kodiranje vse komunikacije s povezanimi strežniki.
Izdajatelji plačilnih kartic skrbijo za našo varnost preventivno z varovalnimi mehanizmi, ki temeljijo na analizi vzorcev uporabe. Tako lahko učinkovito izpostavljajo vse anomalije v prometu na računu. V primeru, da smo neupravičeno transakcijo prvi zaznali sami, moramo o tem nemudoma obvestiti banko, ki nam daje za to s pogodbo določen čas preklica. Ta čas je običajno 48 ur, kar pa morda ne zadostuje za uporabnike, ki ne uporabljajo spletnega bančništva in dnevno ne preverjajo vseh transakcij. A vse še ni izgubljeno, saj nas imetnike plačilnih kartic v takšnih primerih varuje tudi zakonodaja. Odgovornosti tako ponudnika plačilnih storitev kot uporabnika pri plačevanju s plačilnimi instrumenti v Sloveniji opredeljuje zakon o plačilnih storitvah in sistemih (ZPlaSS)[16]. Uporabniki kreditnih kartic naj se o svoji odgovornosti ob izgubi ali kraji kreditne kartice glede podrobnejših navodil vselej pozanimajo pri svoji banki. Koristno pa bo ob tem poznati tudi zakonodajo. 116. člen v splošnem zavezuje uporabnika k skrbnemu varovanju plačilnega instrumenta. 119. člen zavezuje ponudnika plačilnih storitev, da ta uporabniku povrne znesek neodobrene plačilne transakcije, razen v primerih nepredvidljivih ali neizogibnih okoliščin. 120. člen nas kot uporabnike seznani, da smo v primerih ukradenega ali izgubljenega plačilnega sredstva dolžni kriti izgube, ki nastanejo zaradi neodobrenih plačilnih transakcij, vendar le do največ 150 evrov na transakcijo.

Leta 2001 je korporacija Visa predstavila dodaten nivo varovanja z uvedbo storitve »Verified by Visa«, podprto s standardom 3D Secure[17]. Ideji se je kmalu pridružil Mastercard s standardom »Mastercard SecureCode«[18]. Sorodna sistema delujeta z istim tipom prenosnih čitalnikov, ki generirajo enkratno geslo (ang. one time password, OTP). V primeru, da čitalnika ne uporabljamo, to geslo ni generirano vnovič pred vsako

potrditvijo transakcije, temveč je stalno. Ob prvi uporabi sistem od nas zahteva vnos davčne številke in datum rojstva, morebiti še v kombinaciji s številko TTR. Po uspešni potrditvi identitete si izberemo geslo, ki ga nato uporabljamo pri vsakem nakupu skupaj še s preostalimi podatki. Z uvedbo tega dodatnega nivoja varovanja smo prišli do stopnje, ko napadalec samo s podatki o kreditni kartici in njenem lastniku le-te ne more zlorabiti. Izbrano geslo, ki ga za razliko od kode CVV2 prodajalec ne more shraniti, se uporabi za preverjanje istovetnosti uporabnika ob vsaki transakciji. Kupec, ki izbere geslo enako kateremu izmed njegovih preostalih gesel, posebno pa, če je to geslo enako geslu za dostop do računa pri isti spletni trgovini, skorajda izniči pomen varnostnega mehanizma. Povsem racionalno je predpostaviti, da ima napadalec pri dostopu do podatkovne baze s podatki o številkah kreditnih kartic ravno tako tudi dostop do avtentikacijskih podatkov za dostop do spletnega računa kupcev, vključno z gesli.
Eden izmed sistemov, ki ga uporabljam tudi sam za osebno varovanje pred zlorabami, je uporaba kreditne oz. debetne kartice samo za namen spletnega nakupovanja. Sam za nakupovanje na spletu uporabljam debetno kartico Visa Electron. Poseben bančni račun, vezan na kartico, nima pogojev za limit in je načeloma brez razpoložljivih sredstev. Pred spletnim nakupom opravim na povezani TTR nakazilo prek spletnega bančništva le v višini zneska, ki je izpisan na (pred) računu. Tako se izognem temu, da bi mi trgovec zaračunal preveč, hkrati pa se zavarujem tudi pred neupravičenimi nakupi, ki lahko nastopijo kot rezultat morebitne kraje podatkov o kartici. Moramo se zavedati, da se kriminalci, ki želijo zlorabiti našo kartico, a jim to zaradi nerazpoložljivih sredstev na njej ne uspe, k vnovičnemu poskusu nekoč kasneje ne vračajo ravno zaradi ogromnega števila razpoložljivih kartic v odtujenih podatkovnih bazah.

Želim vam prijetno in predvsem varno nakupovanje na svetovnem spletu!

LITERATURA IN VIRI / REFERENCES:

1. PCI SSC Quick Reference Guide, str. 4; dostopno na: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

2. The History of Credit Cards; dostopno na: http://www.creditorweb.com/articles/the-history-of-credit-cards.html

3. E-Commerce Success and Innovation Right From the Start : History; dostopno na http://www.intershop.com/history.html

4. Moneta/Predstavitev; dostopno na: http://moneta.si/predstavitev

5. Electronic Money, or E-Money, and Digital Cash; dostopno na: http://projects.exeter.ac.uk/RDavies/arian/emoney.html

6. E-money mini-FAQ (release 2.0); dostopno na: http://projects.exeter.ac.uk/RDavies/arian/emoneyfaq.html

7. Naked Security: PlayStation Network hacked: five days and counting..; dostopno na: http://nakedsecurity.sophos.com/2011/04/25/playstation-network-hacked/

8. 4chan; dostopno na: http://www.4chan.org/faq

9. The New York Times Blog: Hackers Claim to Have PlayStation Users' Card Data; dostopno na: http://bits.blogs.nytimes.com/2011/04/28/hackers-claim-to-have-playstation-users-card-data/

10. Krebs on Security: I'll Take 2 MasterCards and a Visa, Please; dostopno na: http://krebsonsecurity.com/2010/09/ill-take-2-mastercards-and-a-visa-please/

11. Treasury&Risk: UK report doubles estimates of fraud loss; dostopno na: http://www.treasuryandrisk.com/2011/02/01/press-release-uk-report-doubles-estimates-of-fraud-loss

12. Gorazd Žagar, Metode in tehnike napadov na komunikacijsko-informacijske sisteme, diplomsko delo, 2006; dostopno na: http://infosec.si/diploma.pdf

13. How to Find your CVV - Credit Card Code; dostopno na: http://www.torrid-tech.com/pcCardCode.html

14. Rolling Stone: Hackers Gone Wild, 10. junij, 2010, str.64-71 in 90

15. SecPoint: Nokia 1100 Can Be Used For Hacking Banks; dostopno na: http://www.secpoint.com/Nokia-1100-Can-Be-Used-For-Hacking-Banks.html

16. Zakon o plačilnih storitvah in sistemih (ZPlaSS); dostopno na: http://www.uradni-list.si/1/objava.jsp?urlid=200958&stevilka=2864

17. Activia: Verified by Visa; dostopno na: http://www.activa.si/pametnaKartica/vbv.asp

18. Activia: MasterCard SecureCode; dostopno na: http://www.activa.si/pametnakartica/securecode.asp

19. Wired: Carder Pleads Guilty to Fraud Involving $36 Million in Losses; dostopno na: http://www.wired.com/threatlevel/2011/04/rogelio-hackett-guilty/

20. BitcoinMe; dostopno na: http://bitcoinme.com/