Revija za kriminalistiko in kriminologijo / Ljubljana 50 / 1999 / 3, s. 215–224

Zlorabe plačilnih kartic pri elektronskem poslovanju

Maja Zupančič*

Članek obravnava elektronsko poslovanje in uporabo plačilnih kartic v poslovnih sistemih, elektronsko trgovino in elektronsko bančništvo, predvsem pa se osredotoča na zlorabo plačilnih kartic pri elektronskem poslovanju. Opozarja na neizoblikovano zakonodajo in pravno varstvo elektronskega poslovanja. Opisane so zlorabe elektronskega poslovanja, ki nastajajo pri nakupih na daljavo, kazniva dejanja v povezavi z elektronskim poslovanjem in oblike zlorab plačilnih kartic, ki so se pri uporabi t. i. plastičnega denarja pridružile goljufijam, povezanim z zlorabo plačilnih sredstev. Avtorica skuša ugotoviti, zakaj sploh prihaja do zlorab plačilnih kartic, kakšne so posledice goljufij in kako se zavarovati pred tovrstnimi goljufijami. Prikazati skuša vlogo organov pregona pri tovrstni obliki kriminalitete. Na koncu so opisana priporočila za varno elektronsko poslovanje in naštete nekatere varnostne tehnike za učinkovitejše varovanje v elektronskem svetu.

Ključne besede: elektronsko poslovanje, plačilne kartice, kazniva dejanja, goljufije, preprečevanje

UDK: 343.53 + 343.72

1. Uvod

Na oblikovanje celotne družbene infrastrukture vplivajo telekomunikacije in informacijska tehnologija. V zadnjem času postaja internet medij komuniciranja in prodira v svetovno poslovno omrežje, kjer postaja vse bolj pomembno središče sodobne ponudbe in povpraševanja. Znotraj interneta se razvijajo raznovrstne dejavnosti, med drugimi tudi elektronsko poslovanje (opravljanje poslovnih procesov nekega podjetja ali organizacije s podporo različnih informacijskih tehnologij). Liberalizacija telekomunikacij v razvitih državah spodbuja razvoj elektronskega poslovanja, hkrati pa postaja internet okolje za informacijsko izmenjavo, ki naj bi potekala hitro, poceni in varno.

Elektronsko poslovanje stremi k temu, da olajša poslovanje (razvil se je nov sistem poslovanja z uporabo različnih plačilnih kartic[1]), ga naredi bolj učinkovitega, hkrati pa ne ruši, ampak nadgrajuje sedanje poslovanje. Elektronsko poslovanje pri tem potrebuje sodobno bančno ureditev, ki bo omogočala poslovanje tudi po javni računalniški mreži.

Z ekonomsko rastjo in razvojem rastejo tudi družbeni problemi, med njimi kriminal. Nakupi na 'daljavo' (tj. brez fizične navzočnosti stranke in kartice), ki potekajo brez ustreznih varnostnih mehanizmov, sodijo med nevarne transakcije in omogočajo organizirano zlorabo[2] plačilnih kartic. Goljufije, povezane z zlorabo plačilnih sredstev, poznamo že dolgo, pri uporabi t. i. 'plastičnega' denarja pa se razvijajo vedno nove oblike. Uporaba elektronskega medija omogoča, da se tehnike in že preverjeni načini izvajanja goljufij še izpopolnjujejo.

Po pričakovanem komercialnem učinku interneta se zato med strokovnjaki in uporabniki postavlja vprašanje, kako razvijati omrežje in uporabo njegovih storitev, ga pravno urediti in zavarovati pred možnimi zlorabami. Varstvo posameznikove zasebnosti tudi v elektronskem prostoru namreč zahteva, da kakršnokoli zbiranje in izmenjava podatkov spoštujeta in ščitita varstvo zasebnosti[3].

2. Opredelitev pojma elektronsko poslovanje

Elektronsko poslovanje pomeni elektronske poslovne transakcije, ki vplivajo na procese in oblike poslovanja. Elektronsko poslovanje vključuje v najširšem smislu uporabo vseh oblik informacijske in komunikacijske tehnologije v poslovnih odnosih med trgovskimi, proizvodnimi in storitvenimi organizacijami, ponudniki podatkov, potrošniki in državno upravo (Gričar, 1997). Je splet tehnologij, rešitev, procesov in poslovnih strategij.

Znane tehnologije elektronskega poslovanja so: elektronska pošta, računalniško izmenjavanje podatkov ('rip'[4]), svetovni

* Maja Zupančič, dipl. sociologinja, svetovalka v Ministrstvu za notranje zadeve RS, Štefanova 2, 1501 Ljubljana.

[1] Tako kot ček je tudi plačilna kartica (npr. American Express, Diners Club, Activa, EuroCard, Visa, MasterCard, AT&T) plačilni instrument, ki ga trgovci sprejemajo po lastni presoji oz. po vnaprej predvidenih neposrednih in posrednih koristih pri poslovanju z njimi.

[2] Po podatkih *Association for Payment Clearing Services* ima Velika Britanija zaradi zlorabe kreditnih kartic vsako leto izgube v višini nad 27 milijonov ECU. *Gesellschaft für Zahlungsysteme* navaja, da je zaradi uvedbe novega elektronskega varnostnega sistema v letu 1995 škoda zlorabe in kraje kreditnih kartic v Nemčiji v letu 1995 padla pod 15 milijonov ECU s prejšnjih 23 milijonov ECU.

[3] Internet je omogočil razvoj novih orodij za zbiranje osebnih podatkov. Nastali so programi, ki beležijo, katere naslove obiskuje posameznik, koliko časa porabi na posameznem strežniku ipd. Tudi uporaba kreditnih kartic pri elektronskem trgovanju omogoča oblikovanje zbirk, ki služijo t. i. osebnemu trženju prodajnih izdelkov. Na ministrski Bonnski deklaraciji so (tudi zato) ministri (držav članic Evropske unije, držav Evropskega združenja za svobodno trgovino in držav Srednje in Vzhodne Evrope ter Cipra) sklenili, da "se sme zbirati in obdelovati podatke o uporabnikih globalnih informacijskih omrežij le v primerih, ko so na podlagi predhodne informiranosti uporabniki za to dali svoj pristanek, ali ko sta takšno zbiranje in obdelava podatkov dovoljena z zakonom, pri tem pa je treba sprejeti takšne pravne varovalke in tehnična sredstva, ki bodo zagotavljale uporabnikovo pravico do zasebnosti".

[4] Rip nadomešča poslovne listine (npr. računi, plačilni nalogi, naročila) z računalniškim prenosom podatkov v standardizirani obliki in predstavlja predhodno obliko modernega elektronskega poslovanja.

splet strani na internetu, intranet in druge oblike (npr. mobilna telefonija, videokonference, elektronski denar) (Podlogar, 1997). Med oblike elektronskega poslovanja (največkrat povezane z omrežjem internet) sodi pošiljanje plačilnih nalogov po elektronski pošti, poslovanje z bankami, nakupovanje in prodajanje prek interneta, nameščanje predstavitvenih strani. Znotraj posameznih oblik potekajo dejavnosti (npr. naročanje knjig in glasbenih plošč, bančno poslovanje), ki pomenijo kompleksne rešitve posameznih oblik poslovanja.

Elektronsko poslovanje delimo v zaprto elektronsko poslovanje in odprto elektronsko poslovanje (Toplišek, 1996). **Zaprto** elektronsko poslovanje se uveljavlja pri poslovanju med podjetji ali znotraj podjetij in poteka po ločenih komunikacijskih poteh (npr. rip). **Odprto** elektronsko poslovanje pa se je uveljavilo in razširilo šele z uporabo omrežja internet, ki pa lahko poteka tudi po drugih odprtih omrežnih sistemih (Horwitt, 1997). Strokovnjaki pripisujejo odprtemu elektronskemu poslovanju velik pomen v prihodnjih letih. Prek tovrstnega poslovanja naj bi namreč potekala večina gospodarske dejavnosti in se pretakala ogromna količina kapitala.

2.1 Elektronsko trgovanje

Elektronsko trgovanje ali 'virtualna trgovina' pomeni plačevanje storitev ali blaga imetnika plačilne kartice po internetu. Najbolj je razvito v ZDA, vse bolj pa se uveljavlja tudi v Evropi[5], predvsem v Veliki Britaniji. Največkrat gre za komunikacije z neznano osebo, zato ga imenujejo tudi 'enostransko zaupanje'. Z omrežnim trgovanjem pridobijo podjetja časovno prednost pred konkurenco, kupci pa imajo zagotovljeno neposredno trženje, prodajo in dostavo.

Elektronsko trgovanje je odvisno od varnosti trgovskih transakcij in je v odprtem sistemu internet izpostavljeno različnim zlorabam. Poslovanje v virtualni trgovini ne poteka samo med pravnimi osebami, zato virtualne trgovine, ki zagotavljajo varnost transakcij in avtentičnost, uporabljajo kodirane podatke in varnostne mehanizme.

2.2 Elektronsko bančništvo

Elektronsko bančništvo[6] zajema bančne storitve, ki jih lahko opravimo zunaj banke (npr. doma, v podjetju) z uporabo elektronike oziroma elektronskega medija t.j. osebnega računalnika, telefona s tonskim oddajanjem, televizijo idr.

Za elektronsko bančništvo je pomembno, da so notranji podatki varovani z zaščitnim sistemom, da je komunikacija prek omrežja šifrirana, da je preverjanje uporabnikov izvedeno z identifikacijsko kartico in da je na strani banke postavljen varen strežnik omrežja. Pomembno je tudi, da zagotavlja tako delovanje, ki že velja v tradicionalnem bančnem poslovanju.

3. Zakonodaja in pravno varstvo elektronskega poslovanja

Elektronsko poslovanje zaradi prostora, v katerem deluje, imenujemo tudi mednarodno poslovanje. Strokovnjaki opozarjajo, da počasno reševanje pravnih vprašanj (o zaščiti, veljavni zakonodaji itd.) lahko povzroči gospodarsko škodo. Mednarodno poslovanje je z novim delovnim okoljem postalo eno izmed vse bolj zapletenih področij, ki mu mora mednarodno pravo posvetiti precejšnjo pozornost.

Pravna pravila elektronskega poslovanja so še neizoblikovana.[7] Zakonsko necelovito obravnavano je tudi samo poslovanje s kreditnimi karticami. Kaznovanje je po pravnih predpisih možno samo za tatvino kartice in še to v primeru, da je tatvina storjena v državi, ne pa v tujini.

OECD (Organizacija za ekonomsko sodelovanje in razvoj), ki se ukvarja tudi z varstvom podatkov, je pozvala številne vlade in gospodarske organizacije k odpravi ovir za razvoj poslovanja v kibernetskem prostoru in k zagotavljanju primerne zaščite, ki naj ohrani določeno zasebnost vsakega uporabnika. Neenotno razumevanje zasebnosti, oblikovano glede na raznovrstnost nacionalnih zakonodaj, onemogoča usklajeno reševanje vprašanja o nadzorstvu spoštovanja zasebnosti v internetu.

3.1 Slovenska zakonodaja

Zlorabe pri elektronskem poslovanju (najpogosteje kot zloraba ukradene ali drugače odvzete plačilne kartice in uporabe ponarejene kartice, v zadnjem času pa tudi zloraba številke kartice) niso ustrezno kazenskopravno sankcionirane. V kazenskem zakoniku ni omenjeno ponarejanje plačilnih kartic,

[5] Po nekaterih podatkih naj bi v Evropi v prihodnjih petnajstih letih kupovalo prek interneta sedem odstotkov vseh gospodinjstev in za te nakupe porabilo 3,2 milijarde dolarjev.

[6] Pojem elektronsko bančništvo pomeni opravljanje bančnih storitev za stranko prek elektronskih medijev (prikaz stanja na tekočem, žiro ali deviznem računu v realnem času, izpis prometa za poljubno preteklo obdobje, opravljanje plačil, naročilo čekov, prošnja za prekoračitev sredstev na tekočem računu in prenos sredstev). Ena od najbolj znanih oblik je 'internet elektronsko bančništvo'.

[7] Na področju elektronskega poslovanja Evropska unija če ni sprejela obvezujočih napotkov za svoje članice, strategijo elektronskega poslovanja pa opredeljujejo predvsem naslednji dokumenti: Ministrska Bonnska deklaracija, Evropska inicijativa o elektronskem poslovanju in Skupna izjava EU in ZDA o elektronskem poslovanju. Maja 1999 pa smo udeleženci SRC Foruma izvedeli, da je v pripravi predlog slovenskega zakona o elektronskem poslovanju

temveč le ponarejanje vrednotnic ali vrednostnih papirjev, vendar pa kreditnih in drugih plačilnih kartic ne moremo enačiti z vrednostnimi papirji (Tekavc, 1995).

253. člen KZ RS govori o zlorabi bančne ali kreditne kartice in sicer o uporabi lastne kartice brez kritja, ne pa o zlorabi kartice druge osebe.

Tatvino kartice lahko uvrstimo med kazniva dejanja tatvine po 211. členu ali velike tatvine po 212. členu KZ RS. Pri tem se postavlja vprašanje vrednosti. Kartica sama po sebi namreč nima posebne vrednosti. Tatvina kartice bi lahko sodila med pripravljalna dejanja, vendar samo takrat, če bi bila tatvina opravljena z namenom, da bo kartica kasneje uporabljena. Uporabo ukradene ali ponarejene kartice nekateri uvrščajo v kaznivo dejanje goljufije (217. člen KZ RS), ki v 1. točki določa, da "kdor z namenom, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist, spravi koga z lažnivim prikazovanjem ali prikrivanjem dejanskih okoliščin v zmoto ali ga pusti v zmoti in ga s tem zapelje, da ta v škodo svojega ali tujega premoženja kaj stori ali opusti, se kaznuje z zaporom do treh let" in v 2. točki dopolnjuje, "če je storilec z dejanjem povzročil veliko premoženjsko korist, se kaznuje z zaporom od enega do osmih let". V 3. točki še določa, da se storilec kaznuje z denarno kaznijo ali z zaporom do enega leta, če je bila povzročena majhna premoženjska škoda in pridobljena majhna premoženjska korist. Kartice se običajno uporabljajo za nižje zneske, zato se njihova zloraba pojasnjuje kot povzročitev majhne premoženjske koristi in škode (za kartice z večjimi zneski, npr. pri zlatih ali platinastih karticah, se namreč za višje obremenitve vedno zahteva avtorizacija). Tudi poskusa uporabe kartice za goljufijo zato ni smiselno kazensko preganjati.

Slovenska kazenska zakonodaja je na področju plačilnih kartic nedodelana, resna sankcija in grožnja vsem oblikam zlorab pa je le civilnopravna odškodnina (Tekavc, 1995).

4. Pomen kartic v poslovnih sistemih

4.1 Vrste kartic

Najbolj razširjene kartice so:

a) magnetne kartice (pomnilne): zaradi potrebe po avtomatizaciji v bančništvu so plastični kartici dodali magnetni trak. Kasneje so magnetnim trakovom zaradi varnosti dodali funkcijo '*read-only*', ki omogoča, da podatke s take magnetne kartice lahko beremo, ni pa jih mogoče spreminjati. Zaradi preprostega posnemanja magnetnega traku lahko kartico ponaredimo, zato niso dovolj varne;

b) optične kartice (pomnilne): delujejo po načelu 'enkrat zapiši, večkrat preberi'. Vsebino kartice ne moremo izbrisati. Za branje in pisanje optične kartice uporabljajo laserje. Kartice imajo veliko pomnilno zmogljivost, zato jih uporabljajo v zdravstvu in netiskanih publikacijah (npr. CD-ROM) in

c) kartice *s čipom*, ki jih ločimo na: pomnilne kartice, ki izvajajo manjše logične operacije s pomočjo integriranih vezij in so namenjene splošni uporabi (npr. telekomunikacije, zdravstvo, šolstvo, vojska), in t. i. pametne kartice z vgrajenim čipom obsežnega pomnilnika.[8] Osnovne funkcije pametnih kartic so: prenašanje podatkov, prepoznavanje lastnika kartice, nadomestilo za denar in varno plačilno poslovanje. V prihodnosti bodo pomembne kot nadomestilo za denar in čeke, in sicer bo to t. i. elektronska denarnica[9], ki bo zagotavljala tudi kreditno sposobnost (Jurišić idr., 1997). Pametna kartica preprečuje lastniku prekoračiti limit in s procesorjem nadzira[10] vse interakcije.

4.2 Uporaba t. i. plastičnega denarja

Sodoben plačilni promet se razvija tudi v Sloveniji, saj po podatkih Banke Slovenije obseg poslovanja z uporabo sodobnih plačilnih inštrumentov nadpovprečno narašča, plačilna kartica pa vse bolj postaja plačilni instrument prihodnosti.

Ankete, s katerimi ugotavljajo uporabnost interneta, kažejo, da se nakupovanje prek omrežja internet v Sloveniji šele razvija. V raziskavi, ki so jo izvedli v okviru projekta RIS, so ugotovili, da slovenski uporabniki interneta ne poznajo vseh možnosti finančnih transakcij in nakupa v omrežju. Raziskovalci so z anketo (izvedena je bila na spletnih straneh omrežja) ugotovili, da je tretjina anketirancev menila, da je elektronsko

[8] Pametna kartica naj bi bila v prihodnje namenjena vsem vrstam transakcij. Omogočila naj bi preprostejše in za posameznika cenejše poslovanje, večjo varnost in združitev različnih tehnologij v eno (gre za modularno zasnovo, ki se lahko dograjuje). Pametna kartica služi uporabniku omrežja tudi kot nekakšen ključ za uporabo omrežnega računalnika, ki omogoča priključitev in delo v omrežju od koderkoli. Zagotavlja varnost, ki je potrebna za komunikacije v računalniških mrežah (združuje telekomunikacije in računalnike). Zaradi svoje tehnološke osnove (vsebuje eno ali več tiskanih vezij s funkcijami procesorja, pomnilnik in vhodno-izhodno enoto) združuje različne funkcije (npr. telefoniranje, uporaba avtomatov, zdravstvena kartica, idetifikacija itd.) (Jurišić idr., 1997). Glej tudi Blythe, I.: Smarter. More Secure Smartcards. Byte Magazine, št. 6, 1997 in Gueulle, P.: Smartcard reader/writer. Elector Electronics, št. 12, 1997, str. 38-43.

[9] V informacijsko najbolj razvitih državah že poznajo elektronske denarnice in jih množično uporabljajo. V Sloveniji za zdaj obstajajo le enonamenske čipne kartice, in sicer za plačilo telefona, cestnine ali storitev satelitske televizije. Prave elektronske denarnice oz. kartice s predplačilom se uporabljajo za poravnavo plačil v več dejavnostih.

[10] Pametna kartica lahko služi kot varnostna ključavnica za računalnike in diske. Če uporabnik vtipka napačno geslo ali poskuša vzpostaviti komunikacijo brez pametne kartice (tam kjer je to potrebno), se sistem 'zaklene'. Informacije na disku ali kakšnem drugem podatkovnem mediju lahko zakodiramo s ključem, ki je dodeljen lastniku. Na podoben način lahko zaščitimo tudi komunikacijo med različnimi računalniki (Jurišić idr., 1997).

nakupovanje boljše v primerjavi z drugimi oblikami nakupa[11]. Raziskava, poimenovana "Ljubljanska banka proti internetu"[12], je potrdila, da slovenski uporabniki interneta opravljajo malo nakupov prek omrežja. Zanimive so predvsem ugotovitve, da sta pri uporabi plačilne kartice na internetu utrpela škodo 2% anketirancev. Večinoma so bili ogoljufani tako, da so prejeli račun za blago ali storitev neznanega prodajalca, pri katerem niso ničesar naročili ali pa jim je prodajalec, pri katerem so že kupovali, izstavil račun, pri tem pa ni dostavil naročenega blaga.

5. Zloraba elektronskega poslovanja

V odprtih sistemih, kot je elektronsko poslovanje, imajo lahko tudi nepooblaščene osebe dostop do strežnika, prestrezajo lahko sporočila med prenosom podatkov, zanikajo udeležbo pri kateremkoli delu prenosa in podvajajo sporočila z namenom okoriščanja (Hudoklin idr., 1997).

Ob tovrstnih in podobnih nezaželenih dejanjih se postavljajo vprašanja o zlorabi zasebnih podatkov (npr. vpogled v finančno stanje posameznika), o zlorabi številk plačilnih kartic, o računalniških goljufijah z bančnimi računi itd. Med značilnimi problemi elektronskega poslovanja, ki odvračajo možne uporabnike, poznavalci navajajo izvor posameznih storitev, standarde kakovosti in nepopolno poznavanje varnega poslovanja s plačilnimi karticami v elektronskem svetu[13].

5.1 Kazniva dejanja v povezavi z elektronskim poslovanjem

V državah, ki sledijo informacijskemu razvoju, opozarjajo na obstoj in rast kaznivih dejanj, povezanih z elektronskim poslovanjem. Odprto omrežje, kot je internet, omogoča posameznikom anonimnost delovanja. Zaradi možnosti zakrivanja identitete, izogibanja davkom in 'premagovanja' pravnih predpisov, uporabljajo nekateri internet za opravljanje nedovoljenih dejavnosti. Najnovejši medij internet je zaradi organiziranih goljufij, povezanih s kreditnimi karticami, tatvin računalniške strojne in programske opreme in drugih oblik mednarodnega kriminala, postal priljubljen prostor 'modernih' kriminalcev (Barrett, 1997). Vsakršno manipulacijo v anonimnem svetu, kot je internet, je težko nadzorovati. Pri izvajanju kaznivih dejanj si storilci v virtualnem svetu interneta pogosto pomagajo z lažno identiteto in s ponarejeno elektronsko pošto.

Strokovnjaki z različnih področij omenjajo predvsem naslednje oblike zlorab:

a) manipuliranje z elektronskim prostorom

Kriminalne skupine uporabljajo elektronski prostor za zlorabo trgovinskega sistema, zlorabo elektronskih denarnih vrednosti (valut), finančne goljufije idr. Najpogosteje se dogaja, da goljufije potekajo prek omrežja internet. Večja možnost za goljufije je pri plačilu storitev, čeprav se pojavljajo tudi pri plačevanju blaga. Posebno nevarno manipuliranje v odprtem elektronskem prostoru pa je igralništvo[14].

b) pranje denarja

Najdonosnejša in za storilce najmanj nevarna oblika kriminala, ki se z razvojem tehnologije, predvsem interneta in telebančništva širi v svetu in tudi pri nas je mednarodni posel – pranje denarja. Strokovnjaki ocenjujejo, da znaša vrednost tega denarja v svetu v povprečju približno 5% bruto domačega proizvoda razvite države. Opozarjajo na naglo spreminjajoče se načine pranja denarja, pri katerih zlorabljajo vse bolj izpopolnjeno tehnologijo. Eden od načinov pranja denarja je tudi prenos denarja v tujino z uporabo različnih finančnih instrumentov in medijev, med katerimi pogosto uporabljajo elektronske medbančne transferje, zlasti kreditne kartice. Sodobni 'pralci' denarja uporabljajo namerno zavajajoče načine zakrivanja izvora premoženja z opravljanjem resničnih in neresničnih transakcij. Pri tem jim pogosto pomagajo 'hekerji', ki z vdorom v bančne baze podatkov spreminjajo stanje na bančnem računu ali opravljajo nedovoljen prenos denarja. Banke in druge finančne ustanove nemalokrat niti ne vedo, da njihova omrežja izkoriščajo za pranje denarja in organizirani kriminal[15]. Izkupičke 'elektronskega' kriminala pa kriminalne združbe običajno vlagajo v donosnejše dejavnosti, predvsem v trgovino z mamili. Virtualni svet okolja internet, v katerem se poslovanje in prenos denarja preusmerja oziroma poteka v obliki elektronskega denarja, močno olajšuje tovrstno kriminalno dejavnost. Elektronski denar zagotavlja anonimnost, njegov prenos pa poteka po zaščitenih in šifriranih poteh, ki naj bi bile namenjene poslovnemu svetu kot varovalo elektronskih transakcij pred zlorabo.

[11] Med najbolj zanimivimi izdelki za elektronski nakup so anketiranci navedli: CD plošče, knjige, računalniško in programsko opremo, zabavno elektroniko, rezervacije pri potovanjih, že pripravljeno hrano idr. Več o tem in sami anketi glej URL: http://www.ris.org.

[12] Glej URL: http://www.ijs.si/anketa.

[13] Po mnenju strokovnjakov zloraba interneta ne pomeni, da nekdo z ukradeno kartico kupuje v elektronski trgovini, temveč da lahko nekdo ugotovi vsebino podatkov, ki so kodirani. Poudarjajo, da je nevarnost zlorabe kartice teoretično še vedno večja pri plačevanju računov v restavraciji ali trgovini kot pa v kibernetskem prostoru.

[14] Med nekaterimi preučevalci elektronskega medija je razširjeno celo prepričanje, da je igralništvo po internetu ena najbolj obetavnih dejavnosti.

[15] Notranji in pravosodni ministri držav iz skupine G8 (ZDA, Kanada, Japonska, Italija, Francija, Nemčija, Velika Britanija in Rusija) so tako na sestanku o kriminalu na internetu razpravljali med drugim tudi o pranju denarja kolumbijskih in mehiških kokainskih kartelov. Večino svojega denarja od prodanih mamil premeščajo po bančnih računih vsega sveta, pri tem pa uporabljajo svetovno omrežje internet za pranje denarja, saj so ugotovili, da jih pri tem nihče ne preganja (Stojanov: O kriminalu na internetu. Delo, 12. decembra 1997).

c) zloraba plačilnih kartic

Posebno nevarnost v elektronskem poslovanju pomeni zloraba plačilne kartice[16]. Obstaja vrsta znanih oblik zlorab plačilnih kartic, med najbolj nevarnimi pa je ponarejanje kreditnih kartic, ki prerašča v novo področje mednarodnega organiziranega kriminala. Kriminalne združbe pri tem ponarejajo potne listine, vozniška dovoljenja in druge osebne dokumente, s katerimi 'dokazujejo' upravičenost in veljavnost ponarejenih kartic.

5.2 Oblike zlorab plačilnih kartic

Nakupovanje in plačevanje blaga in storitev na daljavo (telefon, pošta, internet) dopuščata različne, nemalokrat množične[17] zlorabe, kot so: zloraba izgubljenih, ukradenih in neprejetih kartic, ponarejanje kartic, zloraba številk kartic, ponarejene pristopnice in zlorabe računov.

Poleg prekoračitev računa lastnika kartice se najpogosteje pojavljajo zlorabe **izgubljenih** in **ukradenih** plačilnih kartic (ponavadi v 24 urah od časa prijave pogrešane kartice)[18]. Prihaja pa tudi do zlorab 'nikoli prejetih' oz. **neprejetih** plačilnih kartic (kartice so se 'izgubile' na poti od izdajatelja do imetnika kartice).

Ponarejanje in **kopiranje** sta naslednji obliki zlorabe plastičnih kartic. Vse bolj se uveljavljajo različni načini elektronskega ponarejanja, pri katerih ponarejevalci uporabljajo izvrstno tehnološko opremo. Med ponarejenimi karticami se pojavljajo ponovno kodirane[19] kartice, t. i. 'bele' kartice in kartice, ki so popolna reprodukcija.

Hekerji, ki sodelujejo pri ponarejanju in kopiranju plačilnih kartic, so sposobni pretvoriti 'surove' bančne podatke v varnostne kode. Osnovni vir podatkov so zanje podatki, shranjeni na zapuščenih obrazcih zakonitih kartic (pozabljena potrdila ali pridobljena potrdila s podkupovanjem osebja v restavraciji, na bencinski črpalki itd.). Podatke pridobivajo še z vdorom v računalniške sisteme bank in družb, ki izdajajo kreditne kartice. Računalniški strokovnjaki, ki sodelujejo pri tovrstnem kriminalu, lahko na podlagi nekaterih, za imetnika kartice nepomembnih podrobnosti, izdelajo popolne ponaredke. Med imetniki ponarejenih kartic se pojavljajo imena otrok, umrlih oseb in (bivših) zapornikov (naslov zapora, kjer (je) prestaja(l) zaporno kazen). Pri distribuiranju in iskanju imen, primernih za kasnejše uporabnike belih kartic, si ponarejevalci pomagajo tudi z zbiranjem imen na poštnih nabiralnikih (Clough, 1997). Osnovne bančne podatke pretvorijo v varnostne kode, jih prenesejo na ponarejene kreditne kartice, narejene v ilegalnih tiskarnah, ali pa jih uporabijo pri različnih prenosih v omrežju internet.

Pri iskanju podatkov, ki omogočajo zlorabe kartic, si storilci pomagajo tudi z namestitvijo lažnih bankomatov (imetnik vstavi kartico v bankomat, odtipka svojo osebno identifikacijsko kodo, ki se zapiše v lažni bankomat, ta pa nato javi, da bančni avtomat trenutno ne deluje). Na ta način in z drugimi podobnimi metodami pridobijo ponarejevalci kartic pomembne informacije, s katerimi lahko kasneje zlorabijo podatke o imetniku kartice. Raziskovalci zlorab plačilnih kartic so ugotovili, da s ponarejevalci sodelujejo pri pridobivanju ključnih informacij tudi bančni uslužbenci (npr. pooblaščeni uslužbenci ali servisni inženirji), ki imajo dostop do zaupnih podatkov. Vdiralci v bančne sisteme si pomagajo tudi s posebnimi programi za odkrivanje vstopnih gesel, ki jih je mogoče dobiti na internetu[20].

Med zlorabe plačilnih kartic uvrščamo tudi **zlorabe številk kartic**, ponarejanje **pristopnic** in zlorabe **računov**. Povezane so z zlorabami s strani trgovcev (npr. kartico odnesejo iz vidnega polja imetnika) in zlorabami pri nakupih na daljavo (telefon, pošta idr.).

Do zlorab plačilnih kartic lahko prihaja zaradi nevarnosti, kot so:

- način uporabe kartice: zaradi zamika plačil pri kreditnih karticah ima imetnik kartice možnost reklamacije šele po prejemu izpisa; medtem pa je lahko kartica zlorabljena brez vednosti imetnika;

- lažne ('navidezne') storitve: zaradi navideznih loterij, iger na srečo, kazinojev, porno strani, oglaševalnih storitev, je poizvedovanje o zlorabi plačila nemogoče;

- lažne strani interneta: lažno predstavljanje različnih podjetij, ki npr. sprejemajo prednaročila za storitve ali blago;

[16] Na zlorabo plačilnih kartic je opozorilo tudi združenje ameriških bank (*American Banking Association*), ki je v letu 1996 zaznalo zlorabo kreditnih kartic kot enega od glavnih kriminalnih dejavnikov, povezanih z bančnim svetom (Dobeck, M.: Taking Advantage of the Internet. The Police Chief, št. 1, 1997, str. 35-38).

[17] O množičnih zlorabah govorimo takrat, ko ne gre za posamezna dejanja računalniških hekerjev, ampak ko sodeluje organizirana veriga ponarejevalcev plačilnih kartic.

[18] Centri plačilnih kartic, kot je npr. licenčni lastnik Eurocarda (*Europay International*), posedujejo sezname številk kreditnih kartic, ki so jih imetniki kartice 'proglasili' za izgubljene, ukradene ali kako drugače zlorabljene. Sezname, imenovane tudi '*Hot Lists*', kar se da hitro ažurirajo, centralna baza podatkov pa se intenzivno dopoljuje.

[19] Največjo nevarnost je za banke prav 'razvozlanje' varnostnega ključa (dešifriranje), po katerem je sestavljena številka kartice. Ob takem odkritju lahko kdorkoli sestavi katerokoli številko.

[20] Poleg tovrstnih programov je na internetu mogoče dobiti tudi informacije o načinih vdiranja v različne sisteme oz. o t. i. razbitju varnostnih ključev. Nekateri menijo, da je treba takšna navodila izbrisati s spletnih strani (prihaja do zlorabe tovrstnih orodij), drugi pa, da si s takimi informacijami razvijalci programov pomagajo pri izdelavi varnih programskih paketov. Vsaka zloraba namreč povzroči iskanje novega (boljšega) načina zaščite (npr. preverijo svoj program in nivo zaščite prav s tovrstnimi orodji).

• na internetu dostopni programi o generiranju številk kartic in navodila o načinu izvedbe zlorabe kartic (programi, ki naključno generirajo številke[21], ponujajo izbiro številk obstoječih plačilnih kartic);

• problematično preverjanje tujih imetnikov plačilnih kartic;

• nedorečena zakonodaja: med zakonodajalci, izdajatelji kartic in ponudniki elektronskih storitev še ni celovitega sodelovanja (Lasbaher, 1997).

Pri zlorabah plačilnih kartic gre pogosto za organizirane oblike kriminala (posebne skupine so specializirane za določena področja, npr. ponarejanje, distribuiranje). Za tovrstni kriminal[22] so značilne povezave med podzemljem in finančnimi ustanovami, dobro poznavanje tehnoloških novosti in varnostnih mehanizmov. Kriminalci uporabljajo raznovrstno tehnologijo in izkoriščajo slabosti razvijajočega se svetovnega komunikacijskega omrežja.

5.3 Posledice goljufij, povezanih s plačilnimi karticami

Sistemi plačilnih kartic omogočajo poslovanje tudi zunaj državnih meja. Vzroki, zaradi katerih sploh prihaja do možnih zlorab v mrežnih sistemih plačilnih kartic, so povezani s tehničnimi pomanjkljivostmi (slabi varnostni mehanizmi) in človekovo nepazljivostjo (brezbrižno ravnanje s plačilnimi karticami). Vse finančne izgube, ki nastanejo zaradi različnih tovrstnih zlorab, je težko natančno ugotoviti.

Vodilne organizacije, ki izdajajo plačilne kartice (VISA International, MasterCard International, American Express), natančno spremljajo delovanje plačilnega sistema. Ugotovile so, da se večina vseh zlorab plačilnih kartic zgodi na območju ZDA (40%) in v Evropi (22%). Med drugimi geografskimi območji izstopa azijska regija.

Čeprav so finančne izgube, ki jih povzročijo zlorabe plačilnih kartic, v primerjavi s celotnim dobičkom tovrstnega poslovanja skoraj zanemarljive (med 0,1 in 0,2%) pa vsota nikakor ni nepomembna.

5.3.1 Slovenija

Poskuse goljufij, povezanih z zlorabo plačilnih kartic, so v Sloveniji zaznali leta 1996, ko so bančne ustanove zasledile prvi organizirani napad na bančne sisteme.

V slovenskih bankah ugotavljajo, da pri nas prevladujejo mednarodne zlorabe (v državah z bolj razvitim in daljšim časovnim obdobjem poslovanja s plačilnimi karticami prevladujejo 'domače' zlorabe (70%) pred mednarodnimi (30%)), primerov 'domačih' zlorab pa je v primerjavi s številom transakcij zelo malo.

6. Preprečevanje zlorab pri elektronskem poslovanju

Elektronsko poslovanje, še posebej finančno, zahteva: varnost prenosa podatkov po javnem omrežju, zanesljivost delovanja kljub nezanesljivim in tehnično nepopolnim komunikacijam, standardizacijo programske opreme in uporabljenih protokolov, ter varnostni mehanizem, ki tudi s podpisom zagotavlja istovetnost pošiljatelja in neokrnjenost vsebine sporočila.

6.1 Varnostni mehanizmi

Eden izmed najbolj kompleksnih problemov v času globalnih računalniških mrež je varovanje podatkov. Lastniki t. i. občutljivih sistemov (npr. policija, vojska, diplomatske službe, banke) zaradi varnosti fizično ločijo računalniško mrežo na interni sistem (zaupni podatki) in javni sistem (dostop na omrežje internet). Varovanje zaupnih podatkov v odprtih sistemih je globalni informacijski problem, ki ga ne more rešiti samo ena v razvoju informacijske tehnologije vodilna država. Strokovnjaki razvijajo mehanizme za varovanje podatkov, ki so podprti z ustreznimi standardi in bi veljali za vladne ustanove, podjetja in posameznike.

Med pomembne varnostne tehnike strokovnjaki uvrščajo:

a) **Varnostne tehnike v elektronskem bančništvu,** kot so kriptografija, usmerjevalniki, 'požarni zid', interna kontrola, preverjanje uporabnika z identifikacijsko številko, identifikacijska kartica[23] in preverjanje navzočnosti kupca, t.j. naslova

[21] Računalniški program za generiranje številk kreditnih kartic uporablja isti algoritem, kot ga je uporabila banka. Deluje tako, da lahko izbiramo vrsto kreditne kartice, banko, pri kateri naj bo kartica izdana, ter število številk, ki naj jih program generira. Program nudi še možnost izbire imena in priimka enega izmed komitentov izbrane banke, s katerim se kasneje uporabnik ob navedeni številki generirane in na ta način 'izdelane' kreditne kartice predstavlja (za nakup preko omrežja tako niti ne potrebuje fizične plastične kartice).

[22] Izvedbe goljufij potekajo v petih značilnih korakih: pridobivanje informacij o kreditni kartici (predvsem podatka o številki kreditne kartice); prepoznavanje podatkov, zapisanih na kopiji transakcije; testiranje veljavnosti bančnega računa in odloga plačila; izbira naslova za dostavo blaga (nenaseljena hiša, kratek najem stanovanja, naslovi znancev); izpeljava transakcije (uporaba katalogov, naročanje po pošti).

[23] Identifikacijska kartica je varnostni instrument, ki zagotavlja avtentičnost uporabnika storitev elektronskega bančništva. Velika je kot kreditna kartica, ima numerično tipkovnico in zaslon s tekočimi kristali. Na zahtevo stranke generira časovno spremenljivo varnostno geslo, ki omogoča varno identifikacijo uporabnika. Je neprenosljiva in zaščitena z osebnim geslom.

kupca oz. uporabnika storitev z naslovom imetnika plačilne kartice.

b) Eden izmed varovalnih mehanizmov, ki preprečujejo elektronsko ponarejanje kartic, je uvedba posebne **varnostne številke**, t. i. CVC (*Card Verification Code*) ali CVV[24] (*Card Verification Value*), ki ne more biti povzeta ali izračunana iz katerekoli vidne informacije na kartici.

c) **Standard SET (Secure Electronic Transaction)**[25] skrbi za (tehnično) varnost elektronskih transakcij, omejuje možnost zlorabe plačilnih kartic, olajšuje uporabnikovo nakupovanje in pospešuje postopek transakcije.[26]

d) Pojem **elektronski podpis**[27] je izraz za vse možne oblike podpisovanja elektronskih sporočil. Gre za nov način sporočanja, ki tudi pravno zagotavlja verodostojnost udeležencev v komunikaciji. Ni samo nadomestilo lastnoročnega podpisa, temveč prispeva k zmanjševanju nekaterih tveganj v elektronskem poslovanju (npr. digitalni podpis[28], ki preprečuje spreminjanje in zlorabljanje sporočil).

e) **Elektronski denar** je digitalni nadomestek za gotovino in zagotavlja anonimnost. Uporabnik z bančnega računa dviguje elektronske bankovce, njegova elektronska denarnica pa upravlja poslovanje z elektronskim denarjem in preprečuje, da bi uporabnik večkrat porabil iste bankovce.

6.2 Vloga organov pregona

Zlorabe in goljufije, povezane s plačilnimi karticami, so pri nas in v tujini slabo raziskane. Tako kot velja za večino novih oblik računalniške kriminalitete, je tudi odkrivanje, preiskovanje in preprečevanje goljufij s plačilnimi karticami, še posebej organiziranega ponarejanja kreditnih kartic, težavna naloga, ki je povezana z ogromnimi denarnimi sredstvi in močno odvisna od sodelovanja organov pregona z bančnimi ustanovami, ki odkrijejo[29] večino tovrstnih zlorab.

Izvajanje nalog policije pri preprečevanju, odkrivanju in preiskovanju finančnih zlorab v elektronskem prostoru je povezano s številnimi nepojasnjenimi okoliščinami, ki so jih povzročile nove tehnologije sodobnega trgovanja in poslovanja, kot so:

• **Šifriranja** sporočil, ki olajšujejo izvajanje kaznivih dejanj, povzročajo pri organih pregona dvom o njihovi upravičeni uporabi. Šifrirni mehanizmi namreč na eni strani omogočajo varno poslovanje, na drugi strani pa močno ovirajo preiskovalno delo policije. Šifriranja (zaenkrat) ni mogoče zakonito nadzorovati (v zvezi s tem je treba sprejeti zakon o elektronskem poslovanju in zakon o digitalnem podpisu, ki bosta določala, kdaj smejo organi pregona dešifrirati neko šifrirano sporočilo oziroma se seznaniti z vsebino sporočila). V elektronskem prostoru zato nastajajo konflikti med interesi države in posameznikov. Uporabniki omrežja želijo anonimnost in zasebnost svojega delovanja, interes države pa je nadzirati elektronsko pošto in druge prenose podatkov ter imeti vpogled v posamezna dejanja, še posebno, če gre za kazniva dejanja[30].

---

[24] Elektronska varnostna številka CVV je od leta 1992 obvezna na vseh zlatih in platinastih karticah, v zadnjem času pa jo vgrajujejo tudi na klasične kartice. Eden od dodatnih elementov pri prepoznavanju imetnika je tudi vgrajena fotografija imetnika na kartici. Fotografija je vgrajena s posebno računalniško tehniko, ki onemogoča poneverbe fotografij. Tako je zagotovljena večja varnost imetnika kartice (v primeru izgube) in tudi prejemniku plačila s kartico, da ta ni ponarejena ali ukradena.

[25] Standardi SET temeljijo na najnovejši kriptografski tehnologiji, uporabljajo digitalni niz za potrditev identitete sodelujočih in imajo dodan pomemben varnostni element, tj. posebno številko (osebno kodo), ki pa na kartici ni vidna. Več o standardu SET in njegovem delovanju glej Carroll, M: Internet-Commerce Security. Byte Magazine, št. 5, 1997 in Lange, B.: Blizableiter, Secure Electronic Transaction: Kreditkarten im Internet. Ix, št. 10, 1997, str. 120-124.

[26] Za prenos podatkov po omrežju se uporablja tudi standard SSL (*Secure Sockets Layer*), ki podpira zaupnost podatkov, verodostojnost udeležencev v komunikaciji in celovitost sporočil, varno komunikacijo med kupcem in trgovcem pa omogoča tudi protokol S-HTTP (*Secure Hyper Text Transfer Protocol*).

[27] Elektronski podpis omogoča verifikacijo pošiljatelja. Za kodiranje podatkov se praviloma uporablja sistem javnega ključa (RSA algoritem). Več o elektronskem podpisu in njegovi tehnološki izvedbi glej Toplišek (1996).

[28] V Nemčiji je v letu 1997 digitalni podpis pravno postal enakovreden tradicionalnemu podpisu. Nemški parlament je prvi v Evropi sprejel zakon o digitalnem podpisu (Gaertner, 1997). Da je tak zakon pomemben, kažejo tudi prizadevanja evropskega parlamenta, da bi čim prej sprejel smernice razvoja elektronske trgovine in s tem postavil temelje za sprejem podobne zakonodaje tudi v drugih evropskih državah. V svetu že uporabljajo sistem digitalnega podpisovanja v splošnem komercialnem poslovanju, pri elektronskem plačevanju, pri poslovanju davčnih organov in davčnih zavezancev, v zdravstvu in pri drugih oblikah poslovanja, ko je treba vsebino elektronskega sporočila zakriti. Kot poseben primer sistema vsakokratnega preverjanja pristnosti posameznika se v nekaterih tehnološko najbolj razvitih državah uporablja tudi digitalizacija podpisa, t.j. podpisovanje z digitalnim peresom. Več o sistemu javnih in zasebnih ključev glej še Karvé (1997), o digitalizaciji podpisa pa Toplišek (1996).

[29] Zlorabe kreditnih kartic je težko odkrivati, verjetnost odkritja storilca pa je razmeroma nizka. Da gre lahko za sum zlorabe kreditne kartice pa nakazujejo nekatera logična dejstva, kot so: počasno podpisovanje računa, razlika v podpisih, poškodovan ali uničen magnetni trak, neselekcionirano in hitro nakupovanje, nenavadna kombinacija izbranih dobrin in njihovih vrednosti, podpisano ime imetnika kartice se ne ujema z lastnostmi osebe, ki je račun podpisala in neujemanje spola ali naziva ob imenu (Levi idr., 1991:30).

[30] Edward Allen, zaposlen na informacijskem oddelku FBI, je v razpravi o spremembi amandmaja in uvedbi zakona o uporabi šifrirnih mehanizmov poudaril, da "želi imeti policija zagotovljeno pravico do dostopa šifriranih podatkov, v primeru, da so povezani s kaznivim dejanjem" (Mitchell, R.: Is the FBI reading your E-mail? U.S. News & World Report, št. 14, 1997, str. 49). Gre za spremembe o pravni ureditvi šifrirnih mehanizmov, še posebej o izvozu tovrstnih mehanizmov iz ZDA (omejitev izvoza t. i. 'močnih' kriptografij, ki je v ameriški zakonodaji uvrščena med vojaško opremo). Sprememba se nanaša na amandamaje k Ustavi ZDA, ki urejajo svoboščine in

• **Globalizacija** množičnih zlorab in goljufij je pripeljala do tega, da tudi preiskovanje kaznivega dejanja lokalnega izvora pogosto zahteva sodelovanje drugih (nelokalnih) sodnih oblasti. Dodatne težave povzroča še hitrost elektronskih transakcij. Določitev fizične lokacije kriminalnega dejanja, ki je pomembna pri ugotavljanju storilca, je zapletena in otežuje določitev sodne pristojnosti.

• **Anonimnost** delovanja je ena izmed številnih lastnosti, zaradi katere se je priljubljenost elektronskega omrežja množično razširila. Anonimni elektronski prostor zato tudi zlorabljajo za izvajanje kaznivih dejanj, saj je storilca skoraj nemogoče identificirati in ni oprijemljivih dokazov, ki bi bili v pomoč preiskovalcem goljufij in zlorab in bi služili kot dokazno gradivo pri obravnavi na sodišču.

Organi pregona si zato prizadevajo za sprejetje ukrepov, s katerimi bi bilo mogoče omejiti naraščanje tovrstnega kriminala in ublažiti njegove posledice. Za uspešno preiskovanje v globalnem okolju je pomembno multidisciplinarno in mednarodno sodelovanje (Palmer, 1996). O potrebi po skupnem sodelovanju v boju proti elektronskemu kriminalu, v katerem se prepletajo gospodarska, organizirana in računalniška kriminaliteta, so razpravljali tudi predstavniki osmih držav (G8). Menili so, da je potrebno razviti orodja in načine, ki bodo pripomogli k hitrejšemu in bolj učinkovitemu odkrivanju kaznivih dejanj, nastajajočih v računalniških omrežjih. Zavzeli so se za usposobitev organov pregona za boj proti t. i. 'high-tech' kriminalu in za dopolnitev obstoječe zakonodaje, ki naj bi uredila področje računalniške kriminalitete.

7. Zaključek

Razvoj informacijske tehnologije izrabljajo tudi storilci kaznivih dejanj, ki jim ta tehnologija služi kot sredstvo za lažje, hitrejše, bolj učinkovito in bolj anonimno izvajanje svoje dejavnosti. Število primerov zlorab, povezanih s plačilnimi sredstvi, ki jih obravnava policija, je zanemarljivo, preiskovanje tovrstne kriminalitete pa je izredno zahtevno in povezano z ogromnimi finančnimi sredstvi. Z vidika posledic, ki jih povzročijo, pa zlorabe niso nepomembne. Preiskani primeri kažejo, da so te zlorabe povezane tudi z drugimi oblikami kriminala, kot so npr. ropi, vlomi, tatvine avtomobilov (tuje policijske enote so poročale, da so žrtev celo umorili, da so prišli do njene plačilne kartice) (Newton, 1995).

Ob vse bolj raznovrstnih oblikah kaznivih dejanj, povezanih z računalniki in elektronskim poslovanjem, opozarjajo strokovnjaki tudi na prestrezanje in zlorabljanje informacij (seznami kupcev, ki pogosto uporabljajo '*on-line*' prejemanja uslug ali blaga) in na vključevanje organiziranih kriminalnih skupin v tovrstno kriminaliteto. Organizirani kriminal sistematično izrablja pridobitve informacijske tehnologije, ki mu omogočajo nove načine pridobivanja dobička.

Zloraba plačilnih kartic v elektronskem prostoru je samo ena izmed številnih novih oblik globalne kriminalitete. Po podatkih ustanov, ki odkrivajo ali preiskujejo kazniva dejanja, povezana s plačilnimi karticami, so posledice, povzročene z uporabo računalnikov, razmeroma majhne v primerjavi z vsemi ostalimi klasičnimi oblikami finančnih goljufij.

Strokovnjaki za omrežje poudarjajo, da internet kot medij ni nevaren za elektronsko poslovanje[31], nevarna je predvsem neprevidnost pri njegovi uporabi, ki dopušča možnosti za zlorabe in goljufije (npr. razkrivanje gesel, nešifrirano pošiljanje številk kartic, nepreverjanje oziroma neustrezni sistemi preverjanja identitete imetnikov kartice, neupoštevanje pravil o postopku pri sprejemu kartic na strani trgovcev, zanemarjanje varnostnih mehanizmov in zahtev kupca po varnih elektronskih transakcijah).

Priporočila za varno elektronsko poslovanje:

- Izobraževanje in preventivna vzgoja uporabnikov (npr. komunikacijski protokol za elektronsko poslovanje naj bo predstavljen tudi 'on-line' kupcu).
- Sprotno preverjanje pravilno opravljenega nakazila (možnost zlorabe kartice se zmanjša ob avtorizaciji 'on-line' na prodajnem mestu v realnem času in pri pazljivem spremljanju imetnikovega poslovanja s karticami).
- Varno shranjevanje kode in potrdil o nakupu; varno shranjevanje informacij (npr. fotokopije številk) o plačilnih karticah (v primeru zlorabe tovrstni podatki bistveno olajšajo delo preiskovalcem).
- Poizvedba o uporabi šifrirnih mehanizmov[32] pri pošiljanju številk plačilnih kartic.
- Omejitev zneska za elektronsko poslovanje, natančno preverjanje prihodkov in odhodkov na računu.
- Izogibanje shranjevanju programov neznanega izvora na osebni računalnik (možnost podtaknjenega programa za odkrivanje osebnih podatkov).

pravice ameriških državljanov in so še posebej pomembne z vidika kazenskega procesnega prava (vsebujejo garancije, pomembne za status obdolženca v predkazenskem in kazenskem postopku in za varstvo njegovih pravic).

[31] Ameriška banka Citibank, ki izdaja vrsto kreditnih, debetnih in plačilnih kartic celo uradno izjavlja, da je število zlorab pri poslovanju po internetu zanemarljivo. Opozarjajo, da največ zlorab kartic povzročita telefonska prodaja in protizakonito kopiranje kartic v trgovinah.

[32] Obstaja vrsta varovalnih mehanizmov, s katerimi izdajatelji lahko preprečijo zlorabo kartic: standardi SSL, SET, t. i. požarni zid, laserski podpis, fotografija imetnika, CVV, tiskani BIN, digitalni podpis, idetifikacijske kartice, idr.

- Izogibanje poslovanja z neznanimi trgovci, usmerjenost poslovanja k preverjenim trgovcem.
- Pazljivo ravnanje z listinami, ki vsebujejo informacije o identifikacijskih podatkih (prestrezanje informacij in 'tatvina identitete' olajša zlorabo plačilnih kartic).

Priporočila za boj proti 'elektronski' kriminaliteti:

- Najučinkovitejše sredstvo je preprečevanje tovrstne kriminalitete, kar je predvsem naloga bank in drugih finančnih ustanov.
- K odkrivanju storilcev pripomore natančno in celovito zbiranje informacij, pri čemer je pri mednarodnem sodelovanju pomembna vloga mednarodnih organizacij (Svet Evrope, Interpol itd.).
- Potrebno je sodelovanje med izdelovalci oziroma pooblaščenimi ustanovami za izdajanje plačilnih kartic, organi pregona in potrošniki (imetniki plačilnih kartic).
- Pomembna je usklajenost nacionalnih zakonodaj in tesno sodelovanje med policijo, tožilstvom in drugimi organi odkrivanja in preganjanja storilcev kaznivih dejanj.
- Uspešnega zatiranja 'elektronskega' kriminala ni mogoče pričakovati brez dodatnega izobraževanja in finančnih sredstev, ki so za to potrebna.

Elektronsko trgovanje danes še poteka z uporabo kreditnih kartic, v prihodnosti pa naj bi imeli bolj zavarovane in za zlorabo manj občutljive oblike plačilnih sredstev, kot so npr. pametna kartica, digitalni denar in elektronska denarnica (prednosti sodobnejših oblik se kažejo v poenostavljanju administracije, zmanjšanju zlorab in onemogočanju kriminalnih dejanj). Pri razvoju elektronskega poslovanja, ki bo razširil praktično uporabo elektronske kartice, ima svojo pomembno vlogo tudi država, ki naj zagotovi vsebinsko opredeljen, razumljiv in predvidljiv pravni sistem in ustrezno varstvo javnega interesa (zasebnost, intelektualna lastnina, preprečevanje goljufij, zaščita uporabnikov, javna varnost idr.) z zanesljivim načinom poslovanja (digitalni podpis, varni elektronski plačilni mehanizmi idr.).

Dodatek: Primeri zlorab elektronskega poslovanja

♦ V ZDA so obtožili računalniškega hekerja kraje 40.000 številk plačilnih kartic, ki jih je prestregel s strežnikov družbe Netcom.

♦ V Kaliforniji so prijeli osumljenca, ki je z internetnih strežnikov ukradel več kot 100.000 številk plačilnih kartic. Pri tem si je pomagal s posebnim računalniškim programom 'packet snifer', ki beleži plačilni promet prek interneta na določenem strežniku. S tem programom je storilec vdrl v strežnik družbe, ki je sprejemala naročila s plačilnimi karticami, pri tem pa ni šifrirala shranjenih številk. Ukradene številke plačilnih kartic je osumljeni ponudil v prodajo neznancu v omrežju, ki je o njegovi ponudbi obvestil upravljalca strežnika, kasneje pa je s FBI sodeloval pri njegovem prijetju. Agenti FBI so pri navideznem odkupu številk plačilnih kartic dobili pomemben dokaz (vsota 260.000 ameriških dolarjev za 100.000 ukradenih plačilnih kartic). Za krajo številk kreditnih kartic je v ZDA zagrožena kazen petnajst let zapora in denarna kazen 5.000.000 dolarjev.

♦ Na spletni strani interneta se je anonimnež predstavil kot zastopnik trgovskega podjetja. Zbiral je naročila za določeno blago, pri tem pa skrbno beležil številke kreditnih kartic. V času, ko naj bi dostavil blago, je nepooblaščeno kupoval z zbranimi številkami kartic, nato pa se je pravočasno umaknil z interneta.

♦ Štirje najstniki v San Franciscu, stari med 14 in 16 let, so se prek interneta vključili v poslovanje avkcijske hiše, ukradli številke kreditnih kartic in z njimi nakupili računalniško opremo v vrednosti okoli 20.000 ameriških dolarjev.

♦ Slovenski kriminalisti so podali prvo kazensko ovadbo zaradi zlorabe kreditih kartic na internetu maja 1998. 24-letni študent je obiskoval stran Interlotta v Leichteinsteinu, kjer Interlotto Leischeinstein Gouverment prireja igre na srečo. Z uporabo številk kreditnih kartic s 'Stop liste' avtorizacijskega centra Republike Slovenije je z namenom, da bi si pridobil protipravno premoženjsko korist oziroma plačilo uslug iger na srečo, opravil 103 transakcije. Pri tem je na škodo poslovnih bank iz sistema Eurocard izvršil plačilo uslug iger na srečo v višini 263.718,00 SIT in poskušal izvršiti plačilo uslug v višini 2.391.948,00 SIT. Poslane čeke je prejemal in prevzemal po pošti na naslov začasnega bivališča, vnovčeval pa jih je v tujini, pri čemer je uporabljal bančništvo na daljavo. Goljufijo je prijavila banka, ki je prva zaznala zlorabe.

VIRI IN LITERATURA:

1. Barrett, N. (1997). **Digital Crime; Policing the Cybernation.** London: Kogan Page.
2. Bela knjiga – Elektronsko poslovanje v malih in srednje velikih podjetjih. **Uporabna informatika**, posebna številka, 1997.
3. Birch, D. (1997). Real electronic commerce – smart cards on the superhighway. **Internet Research: Electronic Networking Applications and Policy**, št. 2, 1997, str. 116–119.
4. Clough, B. (1997). Plastic Fraud. **Intersec**, št. 7, 1997, str. 289–292.

5. Drol Novak, Ž. (1997). Bančno pravo s stališča potrošnika. **Podjetje in delo**, št. 6, 1997.
6. Evropa (1994). Evropa in globalna informacijska družba. Priporočila Svetu Evrope, maj 1994. **Uporabna informatika**, št. 4, 1994, str. 5–20.
7. Gaertner, R. (1997). A Matter of Trust. **Byte Magazine**, št. 6, 1997.
8. Gričar, J. (1997). Elektronsko poslovanje: priložnost za gospodarske družbe, državno upravo in potrošnike. **Uporabna informatika**, št. 2, 1997, str. 7–12.
9. Horwitt, E. (1997). Global Warming to the 'net. **Computerworld The Network** , št. 25, 1997, str. 17–22.
10. Hudoklin, A., Stadler, A. (1997). Varno elektronsko trgovanje s pomočjo kreditnih kartic. **Organizacija**, št. 5, 1997, str. 288–293.
11. Jurišic, A., Trojar, A. (1997). Pametna kartica. **Uporabna informatika**, št. 1, 1997, str. 37–45.
12. Karvé, A. (1997). Public Key Infrastructure. **Network Magazine**, št. 12, 1997, str. 69–73.
13. Lasbaher, A. (1997). Nasveti izdajateljev. **Kapital**, št. 164, 1997, str. 48–50.
14. Levi, M., Bissell, P., Richardson, T. (1991). **The Prevention of Checque and Credit Card Fraud**. Crime Prevention Unit; Paper No. 26. London: Home Office.
15. Ministrska deklaracija. Ministrska konferenca o globalnih informacijskih omrežjih Bonn, 6. do 8. julij 1997. **Uporabna informatika**, št. 3, 1997, str. 5–11.
16. Newton, J. (1995). **Organised Plastic Counterfeiting**. London: HMSO.
17. Palmer, M. (1996). The art of deception. **Policing Today**, št. 4, 1996, str. 30–33.
18. Podlogar, M. (1997). Elektronsko poslovanje. **Sistem** (priloga revije Monitor), št. 10/11, 1997, str. 6–9.
19. Smith, R. E. (1997). **Internet Cryptography**. Massachusetts: Addison Wesley Longman.
20. Tekavc, J. (1995). Zloraba kreditnih kartic. **Pravna praksa**, št. 337, 1995, str. 11–12.
21. Toplišek, J. (1996). Elektronski podpis – usklajevanje tehnoloških in pravnih rešitev pri elektronskem poslovanju. **Organizacija**, št. 5, 1996, str. 291–300.
22. Toplišek, J. (1997). Vprašanje jurisdikcije v odprtih elektronskih sistemih. **Podjetje in delo**, št. 6, 1997, str. 1050–1057.
23. Vidmar, T. (1997). **Računalniška omrežja in storitve**. Ljubljana: Atlantis.
24. Windolph, J. (1997). Scheckbetrug mittels Homebanking-Software. **Kriminalistik**, št. 2, 1997, str. 114–115.
25. **Zakon o kazenskem postopku.** (1994). Ljubljana, Ministrstvo za notranje zadeve RS.

Abuse of payment cards in electronic commerce

Maja Zupančič, Graduated Sociologist, Counsellor, Ministry of the Interior, Štefanova 2, 1000 Ljubljana, Slovenia

The paper deals with electronic commerce and the use of payment cards in business systems, electronic trade and electronic banking, and pays special attention to the abuse of payment cards in electronic commerce. It points to the unelaborated legislation and legal protection of electronic commerce. It describes various abuses of electronic commerce which take place in purchases at a distance, criminal offences related to electronic commerce and forms of abuse of payment cards, which, with the use of the so-called plastic money, have joined the frauds related to the abuse of payment instruments. The author tries to find out, why abuse of payment cards occurs, what are the consequences of frauds and how to be protected against this type of fraud. She tries to present the role of law enforcement agencies in this kind of crime. The paper concludes with recommendations for safe electronic commerce and provides some security techniques for more efficient protection in the electronic world.

Key words: electronic commerce, payment cards, criminal offences, prevention

UDC: 343.53 + 343.72