Novodobni prodajalci megle ali kako priti do nezakonitega zaslužka preko kraje oziroma potvarjanja virtualne identitete

mag. David Modic, univ. dipl. soc. ped.

Kriminal preko medmrežja

Kriminal preko Medmrežja narašča. V zadnjih letih so se storilci preusmerili od želje po slavi, k želji po finančnem pridobitništvu (Lovet, 2007). Morda je eden od faktorjev, ki so k temu prispevali tudi relativno višja starost ljudi, ki so uporabljali računalnike od malih nog – če je bilo pri štirinajstih letih dovolj že to, da so vrstniki občudovali neznanega storilca, ki je na uradno šolsko spletno stran napisal »Matematika je bedna«, je pri petindvajsetih bolj pomembno to, kako bo nekdo plačal najemnino in pokril kredo, ki ga je naredil v lokalni piceriji. Medmrežje raste z nami in če je bilo na začetku te poti po eni strani lažje zlorabljati sisteme elektronskega poslovanja, ker so bili še v povojih (Gable, 2006), se je po drugi strani nadebudni heker srečeval bolj ali manj z ljudmi, ki so o Medmrežju nekaj vedeli in so bili iz tega razloga precej trši oreh. Z naraščanjem števila uporabnikov Medmrežja nujno naletimo tudi na vedno večje število ljudi, ki o orodju, ki ga uporabljajo ne vedo prav veliko.

Trženje preko Medmrežja je s seboj prineslo tudi velik priliv materialnih sredstev, kar pomeni, da je Medmrežje postalo aktualno tudi za organizacije, ki se ukvarjajo z organiziranim kriminalom (Williams, 2002). Tradicionalno so take organizacije zelo uspešne pri tržnih raziskavah in odkrivanju novih poslovnih priložnosti. Poleg tega so take organizacije velikokrat zelo spretne v novačenju članov, ki jim omogočajo izvedbo novega pristopa (prav tam) – preprosto povedano organiziranim kriminalcem ni potrebno postati računalniški eksperti, vse kar morajo narediti je najeti računalniške eksperte. Zelo znan primer (nikakor pa ne edini) takega početja je bil (sicer neuspešen) poskus pranja in preusmerjanja denarja preko lažnega portala *Banco di Silicia, oktobra 2000*, kjer so storilci poskušali prestreči namenska evropska sredstva za pomoč Siciliji in jih prenakazati na bančne račune več neprofitnih organizacij (prav tam). Poskus je bil sicer neuspešen, ker je eden od storilcev o dejanju predhodno obvestil oblasti.

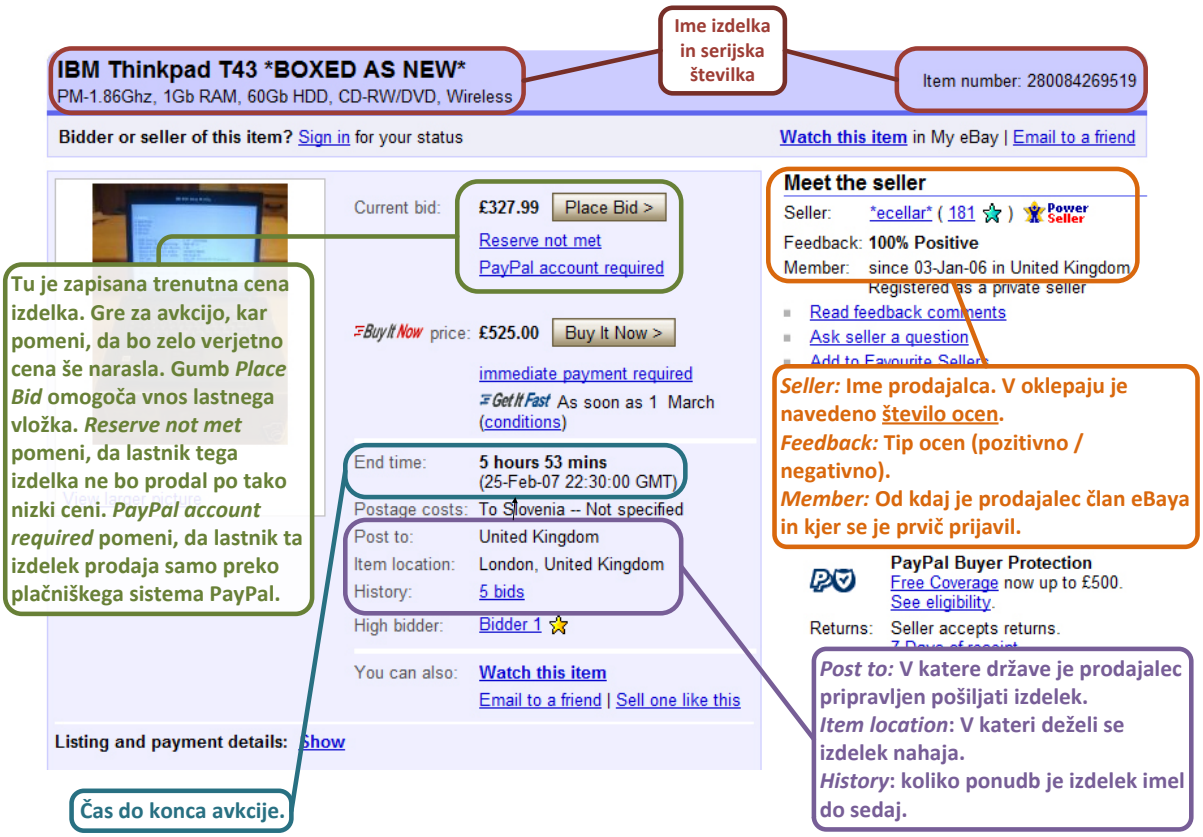
Na Medmrežju se s kiber-kriminalom srečujemo na več nivojih.

- Medmrežje lahko zgolj sredstvo ne pa tudi lokacija izvedbe kaznivega dejanja – npr. po elektronski pošti poslano šifrirano usklajevanje pripadnikov terorističnih organizacij ali pa pošiljanje neželenih vabil na sodelovanje v piramidnih shemah.
- Medmrežje je lahko lokacija, vendar uporabniki Medmrežja niso žrtve – npr. pranje denarja preko spletnih aukcij, kjer nekdo samemu sebi proda neko fiktivno dobrino in tako nelegalen priliv denarja spremeni v legalnega.
- Medmrežje je lahko sredstvo, lokacija, žrtve pa so uporabniki ali podjetja. Ta vidik obsega vdore v in krajo zaupnih podatkov podjetjem, zlorabo uporabniških imen in goljufanje posameznikov.

Ta članek se osredotoča na tretji vidik kiber-kriminala. Kraja oz. varovanje identitete je v tem pogledu ključnega pomena. Po eni strani mora storilec zagotoviti da njegova spletna identiteta ni lahko povezljiva z njegovo konkretno, žrtev pa mora paziti, da prav njegova spletna identiteta ne postane tarča zlorabe. Osredotočili se bomo na konkretne študije primera prevar preko spletne avkcijske hiše eBay, ki je hvaležna tarča take analize. Zaradi ogromne dnevne količine transkacij in velikega pretoka denarja je eBay postal hvaležna tarča tudi za storilce.

eBay

Spletna avkcijska hiša je bila osnovana leta 1995 kot nekakšen spletni bolšji sejem. Sprva je delovala samo v Ameriki, kasneje pa se je razširila tudi po vseh ostalih celinah sveta. Postopek poslovanja je preprost – posameznik si ustvari uporabniško ime in poišče artikel, ki ga zanima. Ko željeni artikel najde, se osredotoči na naslednje postavke:



Slika 1: Tip iskanega artikla. Pridobljeno s svetovnega spleta 25.02.2007. Vir: http://cgi.ebay.co.uk/IBM-Thinkpad-T43-BOXED-AS-NEW_W0QQitemZ280084269519QQihZ018QQcategoryZ177QQrdZ1QQcmdZViewItem

Če so mu postavke po godu se odloči za ponudbo. Če je njegova ponudba najvišja, je zmagal na avkciji in proti plačilu dobi artikel.

eBay deluje po principu ocene (oz. povratne informacije[1]) - ob vsaki transakciji, bodisi nakupu, bodisi prodaji izvajalec transakcije pusti povratno informacijo ponudniku, ki služi kot ocena transakcije. Ta ocena je lahko pozitivna, nevtralna ali negativna. Posamezniki, ki imajo več kot eno ali dve negativni oceni ne morejo več poslovati na eBayu, ker jim člani skupnosti ne zaupajo in od njih ne kupujejo več, oz. jim več ne prodajajo. Ocena služi specifičnemu preverjanju identitete, ker je vezana na uporabniško ime. Posameznik tako sicer ne ve konkretno s kom posluje, lahko pa oceni s kakšno gotovostjo mu lahko zaupa.

[1] Feedback (ang.)

Virtualna identiteta

Telo in identiteta v virtualnem svetu nista več nerazdružljivo povezana in telo, ki sedi za tipkovnico in projecira sebe v eter, ni več omejeno samo s seboj. Postavlja se vprašanje: *Na kak način sta sebstvo in telo povezana?* Ne gre za filozofsko dilemo, ampak temo, ki se nas globoko dotika – na spletu se nek moški predstavlja kot ženska, nek osnovnošolec kot ekspert na določenem področju, razvije se odnos, osnovan na premisah, ki so morda povsem neresnične. Srednješolec ponudi lažno upanje osebam, okuženim z virusom HIV, ko se predstavi za vrhunskega mikrobiologa in napiše na svoji spletni strani, da je našel zdravilo. Moški se hoče poročiti z moškim, ki se v klepetalnici izdaja za žensko. Vprašanje identitete je temeljno vprašanje na Medmrežju in pomeni osnovni gradnik za izgradnjo skupnosti (Donath, 1999).

V vsaki skupini prihaja do zakrivanja identitete – razlogov za to je lahko več, ravno tako posledic. Če so prevare preveč pogoste in uspešne, potem izgubijo svoj smisel, saj ljudje ali živali a priori ne zaupajo več oddanemu signalu, ne glede na njegovo verodostojnost (Donath, 1999). Amotz Zahavi, eden najbolj priznanih znanstvenikov na področju komunikacijskih sistemov, je predstavil t. i. *princip hendikepa* (Coniff, 2001), ki klasificira signale, glede na vložek posameznika. Signali, ki imajo višjo ceno za posameznika, so bolj verodostojni – npr. nekdo, ki veliko zapravlja, bolj jasno sporoča, da je bogat, kot nekdo, ki pravi, da je bogat, pa nikoli ne zapravlja. Moč je bolj jasno izkazana s prenašanjem težkih bremen kot z majico, na kateri piše: »Redno obiskujem fitness«. Signalom, ki sledijo principu hendikepa, pravimo *opredelitveni signali*[2]. Zanje je značilno, da so vezani na specifično lastnost in da imajo za posameznika visoko ceno (Donath, 1999). Varnostnik v nočnem klubu ima mišičasto postavo, kar pomeni, da je moral vložiti veliko časa v dviganje uteži, vendar pa že njegova pojava sporoča, da nima smisla preverjati, ali je v resnici šibak. *Opredelitveni signali* so dokaj zanesljivi, saj zahtevajo, da ima posameznik v resnici lastnost, ki jo razglaša.

Signalom, ki ne sledijo principu hendikepa, pravimo *običajni signali*[3]. V tem primeru je signal povezan z nekim običajem ali socialnim ritualom. Posameznik nima nujno določene lastnosti, zato da lahko odda signal. Na motorističnem forumu se lahko nekdo podpiše kot *HondaHornet900*, pa to še ne pomeni, da je sploh motorist ali da v resnici ima Hondo Hornet. Če je posedovanje motorja nekaj, kar si mnogo ljudi želi, je logično, da bodo nosili majice z motorističnimi motivi, vendar ta signal ne bo zanesljiv. Če bo velika večina posameznikov nosila oblačila znamke Harley Davidson, ta signal ne bo imel več pomena, ki ga je imel prej[4].

Običajne signale uporabljamo zato, ker pomenijo manjši vložek kot opredelitveni signali, tako za tistega, ki signal odda, kot tudi za tistega, ki ga sprejema. Vzemimo za primer iskanje službe – nekdo lahko napiše v svoj življenjepis, kar hoče (*običajni signal*), ne glede na verodostojnost izjav, intervju s posameznikom pa razkrije natančen nivo njegove ekspertize na določenem področju (*opredelitveni signal*). Zaposlovalca stane precej manj časa in denarja, če preprosto pregleda prošnjo, vendar pa je možnost prevare mnogo večja. Večja ko je odgovornost pri opravljanju določenega posla, večja je verjetnost, da bo zaposlovalec zahteval *opredelitveni signal* – natakarjevega življenjepisa ne bo nihče

[2] Assessment signals (ang).

[3] Conventional signals (ang).

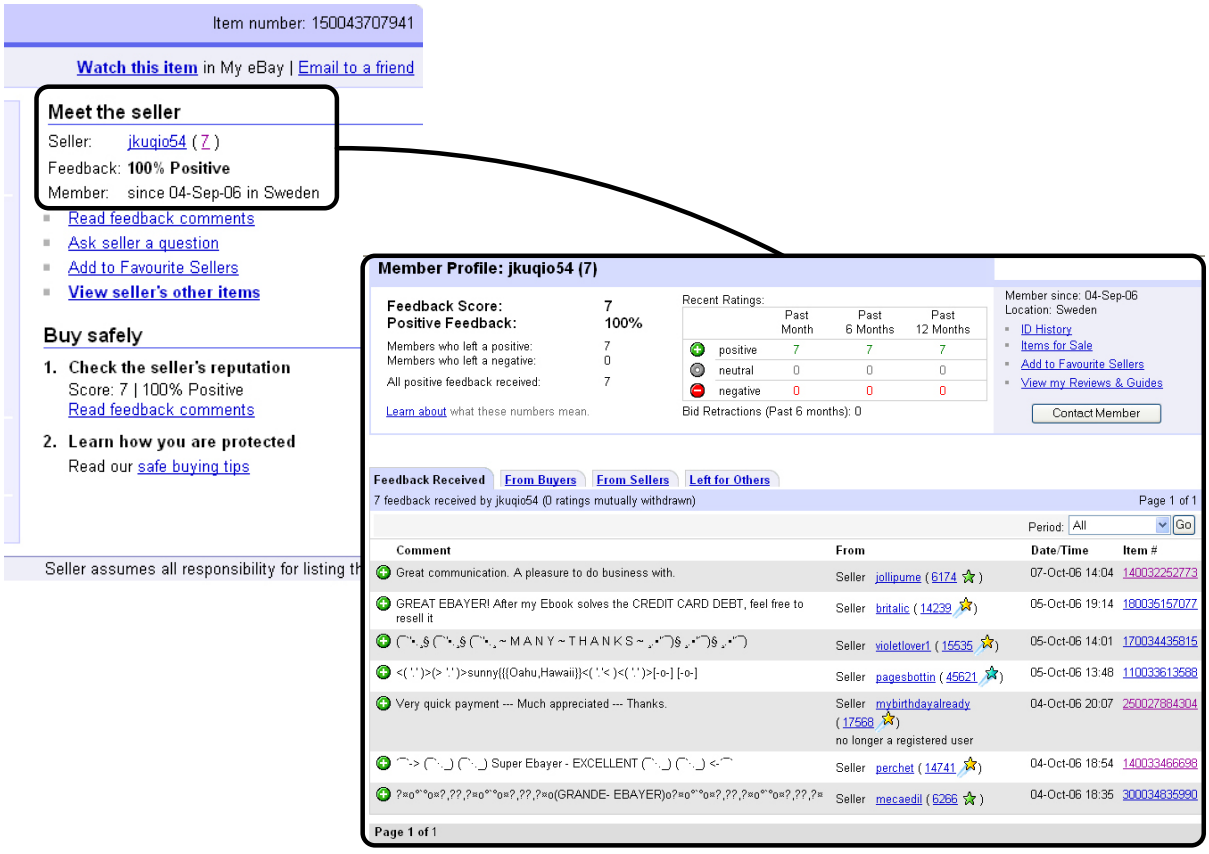
[4] Torej posameznik, ki bo imel Harley Davidson zippo vžigalnik, ne bo več veljal za ostudno bogatega podjetnika, ki je enkrat videl film Goli v sedlu, si kupil Harleyja zato, da je lahko utajil davke, in se z njim bolj ali manj v ravni črti pelje do najbližjega bara in nazaj, ampak bo tak posameznik veljal za nekoga, ki si želi, da bi bil tak kot zgoraj opisani osebek.

pregledal, srčni kirurg pa bo verjetno sprejet šele po razgovoru z zaposlovalcem. Z večanjem odgovornosti raste tudi kazen za prevaro – na ta način zagotovimo večjo verodostojnost *običajnih signalov*.

Kaznovanje lažnivih signalov je ravno tako drag proces (Donath, 1999). Nekdo mora vložiti sredstva v proces preverjanja, poleg tega je cena lahko še višja, če se izkaže, da je bil signal avtentičen – npr. raziskovalec izzove samozvanega karateista na dvoboj in v končni fazi se izkaže, da človek v resnici ima črni pas ...

Specifične tehnike prevar

Kot vidimo je vprašanje identitete ključnega pomena, za zadovoljivo izpeljano prevaro. Na avkcijski hiši eBay velja povratna informacija za opredelitveni signal – za vsako mora posameznik vložiti nekaj časa in večinoma tudi denarja (potencialni kupci ne marajo kupovati od prodajalcev, ki nimajo visoke ocene. Za dobro izpeljano prevaro mora torej posameznik vsaj na videz pridobiti zaupanje skupnosti. Najbolj preprosto bi bilo, če bi posameznik na hitro kupil nekaj deset predmetov manjše vrednosti, ter si tako hitro pridobil več pozitivnih ocen. Problem, ki bi ga še vedno imel pa bi bil problem staža – kot je vidno na sliki 1, je staž tudi del opredelitvenega signala. Potencialni kupci ne kupujejo radi od prodajalcev s kratkim stažem.



Slika 2: tipičen primer na hitro pridobljene pozitivne ocene. Sliki sta bili pridobljeni s svetovnega spleta 7.10.2006. Vira: http://cgi.ebay.co.uk/NEW-Apple-iPod-Video-60-GB-60GB-Black-Music-MP3-Player_W0QQitemZ150043707941QQihZ005QQcategoryZ90964QQrdZ1QQcmdZViewItem in http://feedback.ebay.co.uk/ws/eBayISAPI.dll?ViewFeedback&userid=jkuqio54&iid=150043707941&ssPageName=VIP:feedback:2:uk

Konkretni uporabnik konec decembra že ni bil več član eBay skupnosti. Opredelitveni signal tega konkretnega primer je sumljiv iz več razlogov:

- Ocen ni prav veliko.
- Ocene so bile pridobljene v zelo kratkem času.
- Posameznik ima zelo kratek staž (par dni več kot en mesec).
- Ob pregledu predmetov, ki jih je posameznik kupoval bi videli, da je šlo za predmete, ki ne stanejo praktično nič – recepti za en penny in podobno.
- Eden od sedmih ocenjevalcev ni več član eBaya, kar lahko pomeni, da je uporabnik bodisi sam, bodisi v navezi z drugimi ustvaril uporabniško ime samo z namenom dajanja pozitivnih ocen.
- Poleg tega uporabnika so se na isti dan prijavili še trije uporabniki, ki imajo pozitivne ocene od istih uporabnikov...

Očitno torej posameznik rabi več pozitivnih ocen in daljši staž. Tak proces je predolgotrajen, da bi se izplačal izpeljati na legitimen način. Najbolj pogosta zloraba v teh primerih je t.i. phishing – beseda je izpeljanka iz angleške besede za ribarjenje[5]. Phishing je tehnika pošiljanja lažnih elektronskih sporočil ki se izdajajo legitimne zahteve bank ali drugih spletnih organizacij (v našem primeru eBay). V teh sporočilih storilec običajno zahteva da mu žrtev razkrije zasebne informacije, kot npr. uporabniška imena, gesla, številko kreditne kartice ipd. (Watson, 2005). Sporočilo bo večinoma preusmerilo žrtev na spletno stran storilca, ki bo na prvi pogled videti identična kot prava spletna stran. Tam naj bi uporabnik npr. vpisal svoje uporabniško ime in geslo, ki pa se bo tako znašlo v rokah storilca. Tiste bolj napredne phishing strani v uporabnika še preusmerijo na avtentično spletno stran in ga prijavijo z njegovim uporabniškim imenom in geslom, ter tako zagotovijo, da se posamezniku še sanja ne, da je nekomu ravnokar izdal svoje osebne podatke. Študije so pokazale, da 90% posameznikov ne prepozna dobro izvedenega phishing napada (Dhamija, 2006).

V našem primeru bi storilec lahko poslal elektronsko sporočilo, kjer bi se predstavil ko uslužbenec Ebay-a in prosil žrtev, da se prijavi na njihovo spletno stran, ter preveri, če je z njena spletna identiteta zlorabljena. Sporočilo bi bilo videti pristno. Oblikovano bi bilo po grafični podobi eBaya, povezava v sporočilu bi navidez peljala na spletno stran avkcijske hiše. Žrtev bi potrdila povezavo. Prikazala bi se spletna stran identična tisti z eBaya, žrtev bi vpisala svoje uporabniško ime in geslo, storilec pa bi jo prijazno prijavil na avtentično stran eBay, pred tem pa bi si prisvojil uporabnikove podatke. Storilec bi poslal več tisoč takih elektronskih sporočil in si tako naredil bazo uporabniških imen in gesel.

Storilec bodisi z lažnim ali pravim uporabniškim imenom in geslom ne eBayu pripravi lažno ponudbo. Zato, da goljufija uspe, mora žrtev pristaviti svoj lonček – biti mora dovolj pohlepna, da se prepriča v legitimnost ponudbe. Storilec ponavadi ponuja artikel za smešno ceno, kot npr. MP3 predvajalnik Apple iPod za 70£, kljub temu, da je redna cena 300£. Ukradeno uporabniško ime za prevaro ni nujno, služi le kot eden od opredelitvenih signalov. Nizka cena ponavadi spodbudi žrtev, da ne razmišlja o drugih indicih prevare:

[5] Fishing (ang.)

Slika 3: Indici o lažnosti avkcije. Pridobljeno 7.10.2006 s svetovnega spleta. Vir: http://feedback.ebay.co.uk/ws/eBayISAPI.dll?ViewFeedback&userid=stephen55690&iid=330036733853&frm=284&ssPageName=VIP:feedback:1:uk

Kot je že omenjeno je cena daleč prenizka. Realno bi artikel stal 300£. V tej točki storilec računa na žrtvin pohlep in nepoštenost, ki sta osnovi večini goljufij (Kaminski, 2004 in Ball, 1982). Majhna razlika med začetno in končno ceno artikla sta zastavljeni tako, da si žrtev misli, da mora reagirati takoj, ker sicer nekdo drug dobil artikel za tako nizko ceno. To, da je cena nerealna si ponavadi razloži z mislijo, da je artikel mogoče »padel s tovornjaka« ali pa se je prodajalec zmotil, ko je navajal ceno. V tem primeru mora reagirati še hitreje, ker bo prodajalec hitro opazil svojo zmoto in ceno morda popravil. V prvem primeru je nelegalnost ponudbe ne moti, v drugem računa, da bo ogoljufala goljufa. V vsakem primeru si zatiska oči pred drugimi pokazatelji prevare:

- Cena poštnine je nerealna. Če je storilec res iz Evropske unije, potem je cena v Veliko Britanijo previsoka. Večina storilcev, ki artikle pošilja iz Hong Konga navaja možnost pošiljanja povsod po svetu. Artikli iz Hong Konga ali Kitajske na splošno sicer niso nujno vprašljivi, vendar mora potencialni kupec vračunati še dodatne stroške carine in DDV-ja. V našem primeru bi artikel torej stal[6] 250€ in nič več 150€, kot je sprva kazalo. Kitajski izdelki so sicer znani po tem, da so na prvi pogled identični kot originali, vendar so velikokrat ponarejeni (kot je avtor tega članka izkusil na lastni koži ob nakupu mobilnega telefona Nokia, ki ga je slovenski zastopnik prepoznal kot ponaredek v okroglih 30-ih sekundah).
- Lokacija artikla je navedena kot mesto »b.j.« na Švedskem. To mesto ne obstaja. Zakaj prodajalec noče izdati mesta iz katerega izhaja? Podoben primer lahko vidimo na sliki 5.
- Izdelka noče nihče kupiti. Le zakaj? Morda večina uporabnikov ve, da nakup ne bi bil smiseln.
- Staž in število ocen sta problematična.

[6] 70£ + 30£ = 100£. Carina, ki jo carinska služba zaračuna na skupno vrednost celotne pošiljke skupaj s poštnino znaša 25%, torej ja naš znesek 125£, DDV znaša 20% na celoten znesek, kar pomeni, da je naša cena že 150£. K temu dodatmo še stroške carinjenja in obdelave, ki znašajo približno 10%, kar pomeni, da je končna cena artikla, ko pride v naše roke 165£, kar je približno 250€.

Slika 4: Kaže, da se je Peking preselil na Švedsko. Pridobljeno s svetovnega spleta 7.10.2006. Vir: http://cgi.ebay.co.uk/NEW-Apple-iPod-Video-60-GB-60GB-Black-Music-MP3-Player_W0QQitemZ320035924411QQihZ011QQcategoryZ73839QQrdZ1QQcmdZViewItem

V primeru, da je storilec ukradel tujo identiteto se goljufija ponavadi razpleta drugače – storilec na oglasni strani milo zaprosi žrtev naj mu ne pošilja elektronske pošte preko eBaya, temveč na nek drug naslov (to naredi zato, ker bi pravi lastnik identitete naenkrat ugotovil, da prodaja traktor, podmornico in originalnega Rembrandta takoj, ko bi mu potencialni kupci poslali kako vprašanje preko eBaya – storilec je ukradel uporabniško ime za dostop do eBaya, ne pa tudi za dostop do uporabnikove elektronske pošte). V oglasu storilec navede neko dokaj nizko ceno za kakšen večji artikel[7], ki je ponavadi nekje na drugem koncu sveta. Žrtvi pove, da ne dovoli kar komurkoli, da bi se potegoval za to dobrino, najprej ga mora osebno kontaktirati (če bi pustil da vsakdo sodeluje v avkciji, bi resnični lastnik uporabniškega imena dobil obvestilo ob vsaki ponudbi). Storilec ponudi še malo popusta in pove, da naj mu žrtev nakaže polovico denarja vnaprej, tako, za stroške poštnine, ki je nizka, ker njegov sorodnik dela v transportu, polovico denarja pa naj žrtev nakaže potem, ko bo artikel dobila. Vse je povsem legalno storilec v ovčji preobleki pa je očitno vreden zaupanja – saj je že 70.000 ljudi kaj kupilo od njega, pa so bili vsi zadovoljni. Ko žrtev denar nakaže (ponavadi preko Western Uniona, ki mu je skoraj nemogoče slediti, potem, ko je znesek vnovčen), storilec izgine kot kafra. Vsi poskusi kontaktiranja se končajo tako, da v končni fazi žrtev pride do resničnega lastnika uporabniškega imena, ki o goljufiji nima pojma.

Razpletov prevar je torej dejansko več – storilec lahko samo pobere denar žrtvi, vendar je to tudi najbolj riskantno, saj gre za očitno goljufijo, ki jo tudi oblasti najbolj preganjajo. Dosti bolj elegantne so prevare s skritimi stroški (kot npr. tista opisana zgoraj) ali pa prevare, kjer posameznik dejansko dobi nek artikel, vendar ta ni tisto, kar je žrtev mislila, da je (npr. prenosnik, ki ima čez celo ohišje ogromno prasko ali pa manjkajoče tipke na tipkovnici. Če se žrtev pritoži, jo storilec obvesti, da je v besedilu oglasa lepo pisalo, da je računalnik rabljen in da so na ohišju praske ki so se pojavile ob normalni uporabi) .

V tej točki žrtev ugotovi, da je ogoljufana in začne iskati pravno pomoč. Najprej ugotovi, da praktično ni načina kako bi odkrila pravo identiteto storilca. Večina služb, ki se ukvarja z goljufijami preko Medmrežja ponuja načine kako se zavarovati pred ali po dejanju, odkrivanje in pregon storilca pa prepustijo državnim službam. Če stopimo izven situacije, vidimo srčiko problema – neizrečeno vero, da storilca ni mogoče ustaviti ali odkriti. Vse kar lahko naredimo je preventiva. Kljub temu, da avtorji tega ne napišejo naravnost je iz njihovega pisanja očitno, da so se na nek način že vdali v usodo. Tudi

[7] Zelo znan primer so traktorji znamke Kubota. Več o tem na: http://reviews.ebay.com/FRAUD-Auctions-WARNING_W0QQugidZ10000000001625942

inštitucije, ki so najbolj pogoste tarče prevar, bolj pogosto iščejo načine kako povrniti ali zmanjšati škodo, ne pa kako goljufije preprečiti (Cox, 2003). American Express, MasterCard in druge organizacije povrnejo nastalo škodo (Freeman, 2002), spletna podjetja eBay, Amazon.com in drugi so v svoj model poslovanja vključili tudi možnost oškodovanja zaradi goljufij in te stroške preprosto vključili v ceno poslovanja. To pomeni, da je žrtev relativno varna – njen denar prej ali slej pride nazaj do nje, kar pomeni, da so transakcije preko Medmrežja relativno neboleče. Kljub temu pa storilca zelo redko ujamejo. Večinoma se pojavi problem jurisdikcije, zneski so običajno premajhni, da bi vladne službe hotele ukvarjati z njimi, včasih so zneski celo tako majhni, da se tudi žrtve nočejo ukvarjati z birokracijo in vse kar preostane je, da nekdo napiše nov članek o tem kako se zaščititi pred goljufijo preko Medmrežja.

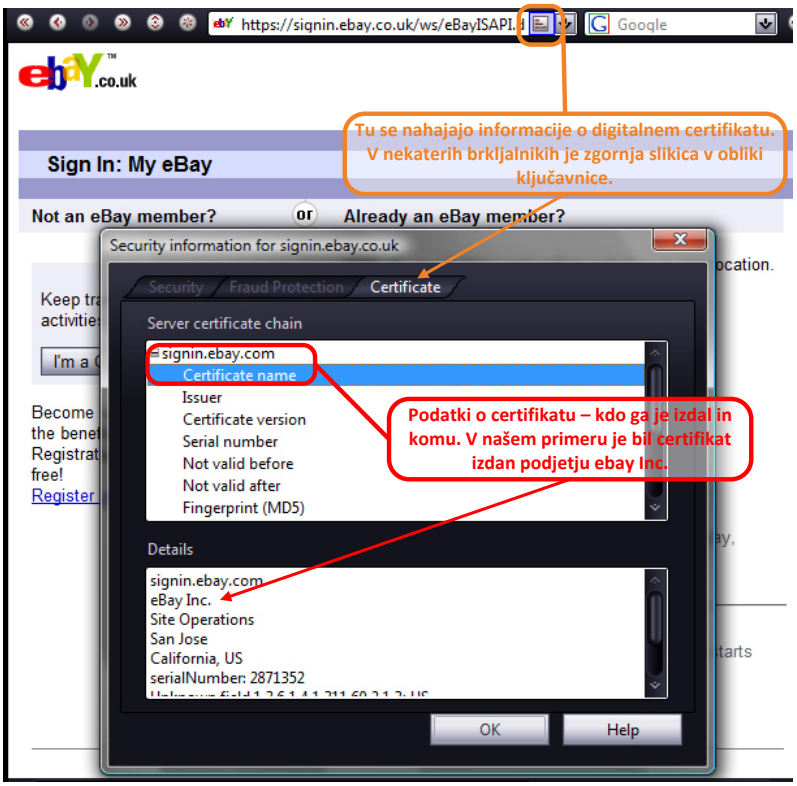
Preventiva: Postopki varovanja identitete

Prvi korak v varovanju virtualne identitete je, da uporabnik privzame paranoiden stav. V svetu, kjer je kraja identitete in osebnih podatkov priznano ekonomsko dejstvo, ni nenormalno računati na to, da obstajajo storilci, ki bi to radi naredili tudi nam. Preprosto povedano: vsakič, ko se v virtualnem svetu pojavi situacija, kjer obstaja možnost kraje identitete ali osebnih podatkov, lahko privzamemo, da se to tudi zares dogaja – če npr. dobimo pošto, kjer nas prosijo za geslo ali uporabniško ime neke storitve, najprej preverimo opredelitvene signale. Zelo preprosto je ponarediti elektronsko pošto, malo težje spletno stran, skoraj nemogoče digitalni certifikat.

Digitalni certifikati

Digitalni certifikati delujejo po principu zaupanja vredne avtoritete[8]. V situacijah, kjer poslujemo ali si izmenjujemo informacije z ljudmi ali pravnimi osebami, ki jih ne poznamo in v virtualnem svetu z njimi (običajno) tudi nimamo fizičnega kontakta, je težko preverjati njihovo istovetnost. Če npr. Francija pokliče npr. prijatelj Toni, ga prvi prepozna po glasu in prepozna njegovo telefonsko številko. Tako ve, da na drugi strani telefonske žice zares govori Toni. Če pa Francijunekdo pošlje elektronsko pošto z naslova vroca_najstnica@email.si in se v njej podpiše kot Toni, tu ni nobenega opredelitvenega signala. Kdor koli se lahko izdaja za Tonija. Ena možnost za potrjevanje istovetnosti je, da bi Toni v sporočilu navedel informacijo, ki jo poznata samo Franci in Toni, npr. »*Včeraj si mi rekel po telefonu naj omenim geslo shishkebab, ko ti pišem, tako, da boš vedel, da ti v resnici pišem jaz.*« Tako sporočilo vsebuje opredelitveni signal, vendar identiteta poššiljatelja še vedno ni popolnoma potrjena. Elektronska pošta po Medmrežju potuje nekriptirano, kar pomeni, da jo lahko nekdo z dovolj volje in nekaj znanja prestreže, prebere geslo, ki sta ga Franci in Toni uskladila, ter originalno pošto ustavi in namesto nje pošlje lažno, ki vseeno vsebuje dogovorjeno geslo. V primeru, da oba uporabnika poznata nekoga, ki mu implicitno zaupata, da bo jamčil za avtentičnost njunih sporočil, je dovolj, da vsakič prosita to *zaupanja vredno avtoriteto*, naj potrdi istovetnost sporočila. Ko v takem primeru Franci dobi elektronsko pošto z naslova vroca_najstnica@email.si zraven dobi še digitalno potrdilo, ki ga je podpisala zaupanja vredna avtoriteta, ki jamči, da mu je sporočilo res poslal Toni. Tak postopek ima prednost tudi v tem, da uporabniku v resnici ni treba poznati avtorja sporočila, dovolj je, da oba zaupata isti avtoriteti, ki je podpisala njuna digitalna certifikata in jamči za njuno istovetnost. Ko poslujemo preko Medmrežja, lahko vedno preverimo digitalni certifikat ponudnika storitve. Primer na sliki 5:

[8]Ang. - Trusted Authority.



Slika 5: Digitalni certifikat. Slika pridobljena 10. 05. 2007 s svetovnega spleta. Vir: https://signin.ebay.co.uk/ws/eBayISAPI.dll?SignIn&UsingSSL=1&pUserId=&co_partnerId=2&siteid=3&ru=http%3A%2F%2Fmy.ebay.co.uk%3A80%2Fws%2FeBayISAPI.dll%3FMyeBay%26MyeBay%3D%26guest%3D1&pageType=1883

Ta postopek zagotavlja uporabniku, da se v resnici nahaja na spletni strani eBay, v primeru seveda, da zaupa podpisniku eBayevega certifikata. V tem konkretnem primeru je to Verisign, podjetje z dolgoletno tradicijo in nedotaknjeno integriteto.

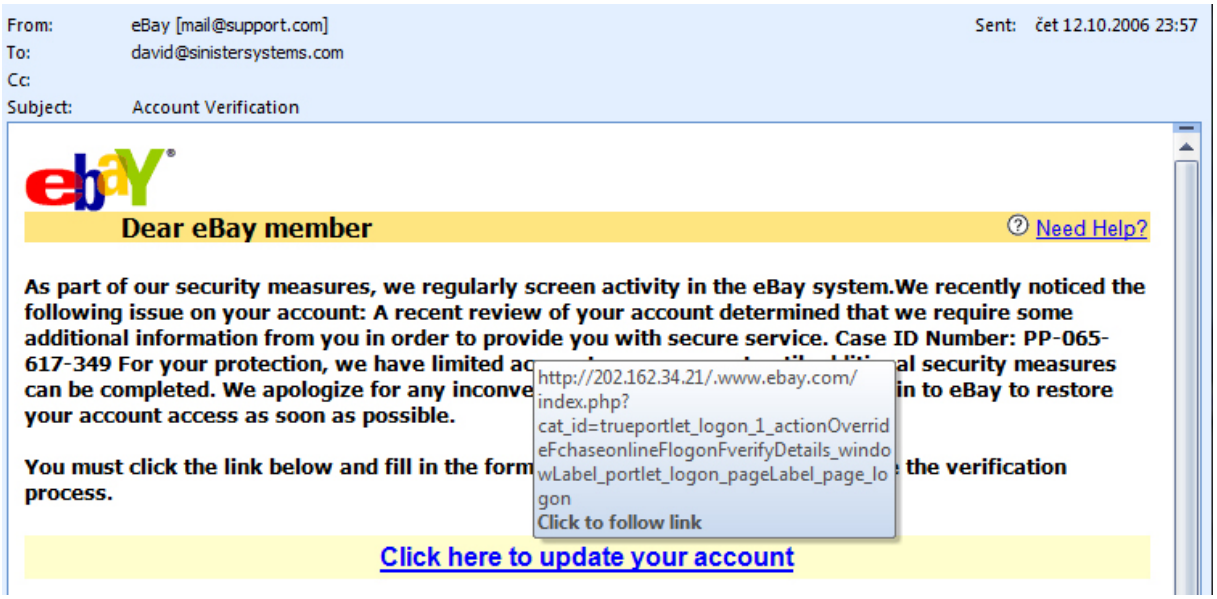
Postopki varovanja pred prevaro

Najbolj preprosto povedano, bi bil postopek samovarovanja tak:

- Ko posameznik dobi neko zahtevo po osebnih podatkih preko elektronske pošte (ali telefona), bi se najprej moral vprašati, kakšne so lahko posledice razkrivanja teh podatkov. Če gre za situacijo, kjer je posameznik lahko močno oškodovan (npr. zloraba kreditne kartice ali intimnosti), bi moral biti skrajno skeptičen do razkrivanja takih podatkov.
- Če gre za elektronsko pošto, naj posameznik najprej preveri naslov, ki naj vsebuje domeno pošiljatelja. Ko govorimo o eBayu, bi moral naslov vsebovati [neko uporabniško ime]@ebay.com. Ob tem velja še omeniti, da podjetje eBay **nikoli** ne pošilja elektronske pošte, v kateri bi spraševali po zasebnih podatkih. Pozor: support@ebay.com, support@e_bay.com, administrator@support.ebay.com in ebay@support.cn so štirje različni naslovi. Zadnji trije so namenjeni prevari. Če uporabnika kličejo po telefonu, naj zaprosi za ime klicatelja in podjetje, iz katerega ga oseba kliče, odloži, poišče telefonsko številko podjetja v imeniku in pokliče nazaj ter zaprosi za klicatelja po imenu. V primeru, da gre za krajo kreditnih kartic, goljuf ne potrebuje celotne številke kartice. Prvih osem številk na kreditini kartici označuje državo in banko, ki je kartico izdala. Podjetni goljuf lahko tako izbere

naključno ime v telefonskem imeniku, kjer dobi ime, naslov in telefonsko številko uporabnika. Zavrti telefon in reče: »Pozdravljeni, sem Lovro Božič iz Mastercard Slovenija, obstaja sum zlorabe vaše kreditne kartice. Ste v zadnjem tednu kupili kaj v vrednosti 1500 evrov preko kreditne kartice?« Uporabnik je v tej točki paničen. *Kako 1500 evrov. Seveda ne. To je treba takoj urediti.* »Da lahko preverim, ali je šlo za zlorabo, potrebujem samo zadnjih osem številk vaše kartice in varnostno kodo, ki je napisana na hrbtni strani, da potrdim, ali sem res poklical lastnika naše kartice. Nikar mi ne povejte celotne številke kartice po telefonu, tako bi vas lahko kdo ogoljufal.« Uporabnik hvaležno pove še zadnje podatke, ki jih fiktivni Lovro Božič potrebuje za zlorabo kartice, obenem pa je prepričan, da je varen. Fiktivni Lovro Božič v tem primeru na noben način ne zagotavlja, da res kliče iz Mastercard Slovenija. Če previdni uporabnik prosi njega za telefonsko številko, na katero ga lahko pokliče nazaj, mu Lovro poda telefonsko iz najetega stanovanja, ki ga je najel s ponarejenimi papirji. Ob morebitnem klicu uporabnika dvigne telefon Lovrotova prijateljica, ki reče: »*Mastercard Slovenija, prosim?*« in prevara je popolna. Zato mora uporabnik nujno sam poiskati telefonsko številko v javnem imeniku, da bi odkril morebitno prevaro

- Če elektronska pošta vsebuje spletni naslov, ki naj bi ga uporabnik obiskal, mora nujno preveriti, kam ta naslov kaže. Podčrtani naslov v sporočilu ni nujno resnični naslov, kamor se uporabnik odpravi. Glej sliko 6.



Slika 6: primer phishing elektronske pošte. Naslov vodi na stran (http://202.162.34.21), ki zagotovo ni v domeni eBay. Naslov preverite tako, da z miško za hip lebdite nad mastno podčrtanim besedilom v sporočilu. Vir: lastni arhiv avtorja.

- Če elektronska pošta vsebuje pravilno uporabniško ime in povezave v njej kažejo na na prvi pogled avtentično spletno stran, uporabnik na koncu preveri še digitalni certifikat. V primeru, da so vsi zgoraj navedeni podatki pravilni, je zelo verjetno, da uporabnik ne bo predal zasebnih informacij nekomu, ki jih bo kasneje zlorabil.

Zaključek

Zelo verjetno je, da nekdo, ki je pravkar spoznal vse navedene možnosti zlorab, ne bo hotel nikoli več poslovati preko Medmrežja, vendar to ni cilj tega članka. Ob upoštevanju zgoraj navedenih napotkov in kančku zdrave pameti je namreč možnost zlorabe kreditne kartice ali kraje identitete zelo majhna. Raziskava, izvedena v Sloveniji leta 2006 je pokazala, da v testnem vzorcu uporabnikov Medmrežja

kar 98,8% udeležencev ni utrpelo zlorabe kreditne kartice preko Medmrežja, 88% pa jih ni nikoli utrpelo kraje identitete (Modic, 2006). Ti izsledki nam povejo, da lahko dokaj brez skrbi poslujemo preko Medmrežja, če skrbimo za lastno varnost, v tem pogledu pa se virtualno poslovanje ne razlikuje od tistega, ki poteka v konkretnem svetu.

Literatura

Ball, J. B. (1982). *Cheating and Deception.* London: Transaction Publishers.

Connif, R. (2001). *Why We Take Risks.* V S. L. Petranek (ur.), DISCOVER 22(12). Pridobljeno 14.2.2002 s svetovnega spleta: http://www.discover.com/issues/dec-01/features/featrisks/.

Cox, B. (2003). *And the Online Fraud Goes On...* V e-commerce Guide. Pridobljeno 1.2.2007 s svetovnega spleta: http://www.ecommerce-guide.com/news/news/article.php/11825_1584531_2

Dhamija, R. et. al. (2006). *Why Phishing Works*. V: the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), Harvard University: Cambridge, MA. Pridobljeno 5.1.2007 s svetovnega spleta: http://www.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

Donath, J. (1999). *Identity and deception in the virtual community*. V P. Kollock (ur.), Communities in cyberspace. (s. 29–60). London: Routledge.

Freeman, J. (2002). *Should you use your credit card online?* V USA Today.com. Gannett Co. Inc.: ZDA. Pridobljeno 12.01.2007 s svetovnega spleta: http://www.usatoday.com/news/opinion/columnists/freeman/ncjf64.htm

Gable, E. (2006). *A Short Synopsis Of Cybercrime*. V EzineArticles. Pridobljeno 23. 01.2007 s svetovnega spleta: http://ezinearticles.com/?A-Short-Synopsis-Of-Cybercrime&id=391574

Kaminski, M. (2004). *Games Prisoners Play*. Princeton: Princeton University Press.

Lovet, G. (2007). *How cybercrime operations work – and why they make money*. V OUT-LAW news. Pridobljeno 22.02.2007 s svetovnega spleta: http://www.out-law.com/page-7791

Modic, D. (2006). *Odklonskost v virtualnih skupnostih*. Magistrsko delo. Univerza v Ljubljani: Pedagoška fakulteta.

Watson, D. (2005). *Know your Enemy: Phishing*. The Honeynet Project & Research Alliance. Pridobljeno 12.12.2006 s svetovnega spleta: http://www.honeynet.org/papers/phishing/

Wiliams, P. (2002). *Organized Crime and Cybercrime: Synergies, Trends, and Responses*.V Williams, P. (ur.): Global Issues. Pridobljeno 10.10.2007 s svetovnega spleta: http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm