UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Miloš Suša

Socialni inženiring na internetu

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Miloš Suša

Mentor: doc. dr. Franc Trček

Somentor: dr. Matej Kovačič

Socialni inženiring na internetu

Diplomsko delo

Ljubljana, 2009

Hvala obema mentorjema za trud in usmeritve pri nalogi!

Hvala vsem, ki ste me podpirali v času študija!

SOCIALNI INŽENIRING NA INTERNETU

Socialni inženiring je način prevare, kjer prevarant z izkoriščanjem človekovih lastnosti, ter s pomočjo manipulacije, prepriča žrtev v neko dejanje, ki ga sicer običajno ne bi storila. Pri svojem delu socialni inženir uporablja mimikrijo, najpogosteje pa se trudi priti do zasebnih informacij. Socialni inženiring lahko ločimo glede na uporabo tehnologije, in sicer na netehnični in tehnični socialni inženiring. Pri prvem se uporablja osebni pristop, medtem ko se drugi uporablja predvsem v navezi z računalniki in internetom. Trenutno najbolj pogoste prevare socialnega inženiringa na internetu predstavljajo ribarjenje (phishing), pharming, smishing in vishing napadi. Skupno vsem je prikrito zbiranje zasebnih informacij, kot so na primer uporabniška imena in gesla za dostop do spletnih bank, spletnih preprodajaln, strani socialnih omrežij, elektronskih poštnih predalov, ipd. Poleg omenjenih prevar pa so na internetu pogosta še elektronska sporočila o lažnem zadetku na loteriji, pisma lažnega prijatelja, nigerijska pisma, ipd. Omenjene ter ostale prevare socialnega inženiringa predstavljajo veliko grožnjo za ljudi. S pomočjo socialnega inženiringa prihaja ne le do kraje zasebnih informacij, pač pa tudi do kraje denarja ter identitet. Najboljšo obrambo proti socialnem inženiringu pa še vedno predstavljata previdnost in skeptičnost.

Ključne besede: socialni inženiring, spletne prevare, prevare, ribarjenje, phishing

SOCIAL ENGINEERING ON THE INTERNET

Social engineering is a method of deception where, by exploitation of human nature and by manipulation, a fraudulent person deceives their victim into doing something he/she usually would not do. Social engineers use mimicry in the process of their work. Usually, their main goal is accessing personal information. Social engineering can be classified according to the use of technology, namely into technical and non-technical social engineering. With the non-technical, personal approach is common, whereas with the technical, mostly computers and internet are used. At present, the most frequent types of fraud using social engineering on the internet are phishing, pharming, smishing and vishing attacks. Their common denominator is concealed acquiring of personal information, such as usernames and passwords for online banks, online shops, social networking sites, emails, etc. In addition to the types of fraud mentioned, other frequent types of fraud on the internet are also emails about (fictitious) winning the lottery, letters from fake friends, Nigerian letters, etc. In addition to the types of fraud mentioned, there are also other types which represent a serious threat to people. By way of social engineering, not only thefts of personal information are done but also thefts of money and identities. The best defenses against social engineering, however, still remain precaution and skepticism.

Keywords: social engineering, internet frauds, frauds, fishing, phishing

KAZALO

KAZALO SLIK

SEZNAM KRATIC

- OZN – Organizacija združenih narodov
- USB – Univerzalno serijsko vodilo (Universal serial bus)
- TAN – Avtentikacijska številka transakcije (transaction authentication number)
- iTAN – Indeksirana avtentikacijska številka transakcije (indexed transaction authentication number)
- mTAN – Mobilna avtentikacijska številka transakcije (mobile transaction authentication number)
- SMS – Kratka sporočila preko mobilnih telefonov (short message system)
- SI-CERT – Slovenski center za posredovanje pri internetnih incidentih (Slovenian computer emergency response team)
- DNS – Domenski strežnik ali sistem domenskih imen (domain name server/system)
- IP – Internetni protokol
- NLB – Nova ljubljanska banka
- MITM – Napad s posrednikom (man in the middle attack)
- VOIP – Telefonija preko internetnega protokola (voice over internet protocol)

UVOD

Nahajamo se v 21. stoletju oziroma informacijski dobi, kjer so informacije ključnega pomena. Pravijo, da kdor nadzira informacije, nadzira svet in tega se dobro zavedajo tudi socialni inženirji. Kaj pa sploh je socialni inženiring? Kratko povedano, gre za način prevare s pomočjo katere prevarant pride do zasebnih informacij ali drugega želenega cilja. Socialni inženir ima torej tehnično znanje in znanje človeške psihologije, medtem ko smo ljudje v skladu s človekovo naravo zelo predvidljivi in zaradi tega tudi ranljivi. Kljub svoji ranljivosti in dejstvu, da lahko prevaranti od nas dobijo informacije, ljudje vseeno prostovoljno razkrivamo svojo zasebnost in jo objavljamo na internetu. Tukaj bi izpostavil razne spletne strani namenjene druženju, kjer je celo leglo zasebnih podatkov. Na tak način ne le ustrežemo socialnim inženirjem, ko nas prosijo, pač pa nas celo prositi ni potrebno. Smo torej v obdobju deljenja informacij, kraj identitet in nasedanja spletnim prevaram, ki pa mu bo verjetno sledilo obdobje zavedanja, torej skrbnega čuvanja informacij in previdnosti.

Skozi nalogo bom natančneje opredelil fenomen socialnega inženiringa in čemu je ta uspešen. Vemo, da prevaranti pri svojem delu uporabljajo različne prepričevalne in manipulativne tehnike, zanimalo pa me bo, čemu ljudje navkljub vsem opozorilom še vedno podležemo njihovim »čarovniškim« trikom. Raziskati nameravam profil žrtve socialnega inženiringa, torej kdo so te osebe, ki so bolj podvržene tovrstnim prevaram. Podrobneje nameravam opredeliti različne vrste napadov oziroma prevar socialnega inženiringa, raziskati pristope prevarantov ter poiskati možne preventivne ukrepe zanje. Na podlagi vsega tega pa bom skušal napovedati smernice razvoja socialnega inženiringa, pri tem pa še posebej izpostavil Slovenijo, ki je bila do nedavnega oaza, kamor vsaj spletne prevare socialnega inženiringa niso segle.

Empirični del naloge vključuje sekundarno analizo podatkov, t.j. analizo obstoječih raziskav s tega področja, ter preučevanje strokovne literature. Socialni inženiring na internetu je, tako kot sam internet, relativno nov pojav in se prav tako zelo hitro razvija. Ravno zaradi tega, je večina izvedenih raziskav in napisane literature novejšega datuma. Znanje, pridobljeno iz

raziskav ter literature, bom podkrepil s primeri iz prakse. O vprašanjih, ki sem si jih zastavil zgoraj, pa bom za mnenje povprašal strokovnjaka s področja informacijske varnosti, gospoda Gorazda Božiča iz slovenskega centra za posredovanje pri internetnih incidentih.

Nalogo bom torej začel z opredelitvijo osnovnega pojma, razdelitvijo in opredelitvijo različnih tipov socialnega inženiringa. Nadaljeval bom z opredelitvijo mehanizmov socialnih inženirjev, ter zaključil z možnimi preventivnimi ukrepi.

1 SOCIALNI INŽENIRING

Socialni inženiring je, laično povedano, prevara s katero prevaranti pridejo do določenih zaupnih podatkov. Gre za »netehnični način vdora, ki se pretežno zanaša na človeške interakcije in pogosto vključuje prevare ljudi z namenom zaobiti varnostne postopke« (Searchsecurity.com 2006). Širša definicija izpostavlja socialni inženiring kot »tehniko, s katero ciljne osebe z uporabo poznavanja psihologije ljudi, delovanja računalniških sistemov in terminologije ter z uporabo majhnih in verjetnih laži pripravimo do tega, da ravnajo (ali pa opustijo neko ravnanje) tako, kakor v običajnih okoliščinah, ko imajo opravka s tujci oz. nepoznanimi osebami, ne bi nikoli« (Zveza potrošnikov Slovenije 2009). Socialni inženiring »uporablja vpliv in prepričljivost za prevaro ljudi tako, da jih prepriča, da je socialni inženir nekdo, ki to ni oziroma jih prevara z manipulacijo« (Mitnick in Simon 2002). To pretvarjanje, da je inženir nekdo drug, imenujemo mimikrija oziroma človeška mimkrija, ki predstavlja »pripodobljanje osebe/skupine A (mimika) pojavu/osebi/skupini B (modelu), kar osebo /skupino C (ali B) (operatorja) zavede oz. naj bi zavedlo v napačno prepoznavo ali neprepoznavo osebe/skupine A; s tem oseba/skupina A doseže (ali naj bi dosegla) določen obrambni ali napadalni cilj« (Smrke 2007).

Razlika med socialnim inženirjem in hekerjem je torej v tem, da socialni inženir ne potrebuje nujno vrhunskega računalniškega znanja, pač pa mora biti le prepričljiv in dobro poznati psihologijo ljudi. Tak način kraje podatkov in ostalih nelegalnih početij je mnogo hitrejši in cenejši od hekerskega vdiranja v sisteme. Za osebe oziroma podjetja, ki želijo svoje podatke zaščititi, pa mnogo bolj nevaren. Pri socialnem inženiringu nam namreč bolj malo pomaga zaščitna tehnologija kot so protivirusni programi, požarni zidovi, posodobljeni računalniški sistemi, ipd. Tukaj sta poglavitni zaščiti pazljivost in zdrava pamet vsakega posameznika. Da gre za resen varnostni problem pričajo tudi raziskave. Orgill in ostali so v svoji raziskavi ugotovili, da bi izmišljenemu podpornemu osebju kar 80% zaposlenih zaupalo uporabniško ime in kar 60% svoje geslo (Orgill v Bakhshi et all 2008, 54). Zastrašujoči so tudi izsledki raziskave v ameriških bolnišnicah, kjer naj bi kar 73% zaposlenih delilo svoje geslo (Medlin et all 2008, 71). O nevarnosti socialnega inženiringa pa opozarjajo tudi pri priznani protivirusni programski hiši Kaspersky, kjer ugotavljajo, da se premika trend napadov iz tradicionalnih tehničnih ranljivosti na socialni inženiring. Naraščajoč trend socialnega

inženiringa pa se pojavlja pri spletnih portalih, namenjenih druženju, kot so npr. Facebook, Twitter, ipd (Westervelt 2009).

Različnih možnih izvedb socialnega inženiringa je mnogo. V nadaljevanju naloge jih bom naštel in opisal, sicer pa bi jih lahko razdelil na več skupin. Peltier razdeli načine socialnega inženiringa na tiste, ki temeljijo na človekovi bazi in na tiste, ki temeljijo na bazi tehnologije (Peltier 2006, 15-17). To razdelitev na netehnični in tehnični socialni inženiring bom v nadaljevanju tudi sam uporabil. Sicer pa lahko ločimo socialni inženiring od nasprotnega (reverse) socialnega inženiringa. Tukaj socialni inženir nastavi past in ga žrtev sama poišče. V tem primeru gre lahko za sabotažo, oglaševanje ali pa pomoč (Granger 2001). Žrtev torej, misleča da je poiskala pravo pomoč ali pravi kontakt, pokliče samega prevaranta.

Napadi socialnega inženiringa so si od primera do primera različni. Vsi pa imajo podoben tok dogodkov. Raziskovalna družba Gartner deli napadalčev cikel na 4 dele: zbiranje informacij, razvijanje odnosa, izkoriščanje odnosa in izvršitev cilja (Gartner 2002). V naslednjem poglavju bom opisal načine zbiranja informacij, nato pa raziskal, na kakšen način napadalec razvije odnos z žrtvijo.

2 VRSTE SOCIALNEGA INŽENIRINGA

V nadaljevanju ločujem socialni inženiring na dva dela. Netehnični pristop socialnega inženiringa predstavlja bolj oseben pristop in temelji na človekovi bazi, medtem ko tehnični pristop temelji na bazi tehnologije, kjer imam v mislih predvsem internet. Tukaj bi opozoril, da razvrstitve niso stoodstotne, saj nekatere prevare niso popolnoma enega ali drugega tipa in vsebujejo metode obeh pristopov.

2.1 NETEHNIČNI PRISTOP

2.1.1 Osebni pristop

Najstarejši pristop socialnega inženiringa, ki ga lahko vidimo tudi v raznih vohunskih filmih, je osebni pristop. Socialni inženir se pretvarja, da je zaposleni, obiskovalec ali pa podporno osebje (Peltier 2006, 16) in se prosto sprehaja po podjetju ter zbira informacije, vdira v omrežje, ipd., skratka prosto opravlja svoj cilj. Tak način deluje predvsem v podjetjih, ki imajo veliko število zaposlenih, načinov kako priti notri, pa je več. Najbolj zanimiv način se mi zdi vstop socialnega inženirja, ki ima polne roke kozarčkov kave in se pretvarja, da ne more odpreti vhodnih vrat. Tukaj mu v pomoč priskočijo prijazni zaposleni in ga tako spustijo v svoje podjetje (Finders 2009, 10). Inovativne pristope uporabljajo tudi ti, ki se pretvarjajo da so obiskovalci ali podporno osebje. Pretvarjajo se lahko, da so serviserji alarmnih naprav, telefonskih central, fotokopirnih strojev, ipd. Najbolj primeren čas takih napadov pa je čas malic. Takrat se lahko vsiljivci mirno sprehajajo po pisarnah in iščejo vredne informacije. Nemalokrat imajo zaposleni celo shranjena gesla na listku pod tipkovnico ali v predalu. To geslo pa lahko ta socialni inženir uporablja še dlje časa, ne da bi uporabnik vedel za zlorabo. Najboljši način za zaščito tovrstnih vdorov v podjetje je spremljanje vsakega obiskovalca po celotnem podjetju, uporaba službenih kartic in neposojanje le teh, ter seveda skrb, da se zaupne informacije, kar seveda uporabniška imena so, hranijo na varnih mestih.

2.1.2 Brskanje po smeteh

Brskanje po smeteh v angleškem jeziku imenujemo dumster diving. V smeteh podjetij ali posameznikov je mnogo stvari in marsikatera predstavlja za napadalca pomemben košček v

sestavljanju mozaika. Napadalcu vredne »smeti« predstavljajo predvsem interni imeniki zaposlenih, listki z raznimi telefonskimi številkami ali celo gesli, seznami strank, ki so bili odvrženi zaradi posodobljenih seznamov, naslovi zaposlenih in njihovi zasebni podatki, itd (Wiles 2007, 10). Socialni inženir lahko te podatke uporabi pri klicu ali osebnem pristopu, kjer se lahko na primer predstavlja kot eden zaposlenih, katerega ime je prebral iz imenika. Take zaupne informacije morajo podjetja varno zavreči, kar pomeni, da jih morajo razrezati z uničevalci dokumentov (ang. shredder). Nevarnost pa ne predstavljajo le dokumenti na papirju, pač pa tudi na vseh spominskih medijih, ki jih zavržemo ali prodamo. Iz diskov in ostalih spominskih medijev je možno obnoviti podatke, čeprav smo podatke zbrisali. V zadnjem času nevarnost predstavljajo tudi t.i. pametni telefoni, kjer imamo, poleg telefonskega imenika, na njem še elektronsko pošto in shranjena gesla za razne internetne strani, ipd. Tudi s takih naprav se da podatke obnoviti, če jih ne zbrišemo pravilno. Pred takimi napadi se torej obvarujemo s skrbnim ravnanjem oziroma skrbnim uničevanjem zaupnih podatkov.

2.1.3 Gledanje čez ramo

Gledanje čez ramo ali shoulder surfing je tehnika direktnega opazovanja tarče pri vnosu njenega uporabniškega imena in/ali gesla, ki se običajno izvaja kadar je prisotna množica ljudi. Računalniki na javnih mestih, npr. na letališčih, v internet lokalih, hotelskih ložah, ipd., kjer je veliko ljudi in pa tudi bančni avtomati so pogoste lokacije tovrstnih pogledov (Long 2008, 33-38). Previdnost pri vnosu podatkov je torej primerna zaščita pred neželenimi gledalci.

2.1.4 Socialni inženiring preko telefona

Tovrstne prevare so zelo popularne, saj napadalcem omogočajo veliko stopnjo anonimnosti, še posebej v sodobnem času, ko napadalec klic lahko opravi preko internetne telefonije (VOIP). Napad poteka tako, da napadalec svojo tarčo pokliče, se izdaja za nekoga drugega in z manipulativnimi sredstvi prepriča zaposlenega, da le ta opravi določeno akcijo. Napadalci pogosto ponaredijo številko klicatelja, tako da le ta daje videz internega klica (Kee 2008, 24). Primer tovrstnega napada je klic izmišljene računalniške podpore, ki prosi uporabnika, naj mu zaupa svoje uporabniško ime in geslo, da bodo lahko posodobili računalnik, ipd. Variacij

prevar preko telefona je veliko, vse pa uporabljajo manipulativne tehnike, ki jih bom opisal v nadaljevanju.

Najbolj znan socialni inženir, ki se je posluževal predvsem s to tehniko je Kevin Mitnick. Bivši heker, ki je s pomočjo socialnega inženiringa vdrl v več mednarodnih korporacij kot npr. Motorola, Sun Microsystems, Nokia, Novell, itd. Čeprav je vdiral, kot pravi, zaradi radovednosti, naj bi povzročil podjetjem za okoli 300 milijonov dolarjev škode (Leung 2004). Leta 2000 je bil po 5 letih izpuščen iz zapora in od takrat naprej vodi svoje podjetje Mitnick Security Consulting, ki legalno opravlja penetracijske teste računalniških omrežij in ostala izobraževanja glede računalniške varnosti.

Zanimiv primer tovrstnega socialnega inženiringa prihaja iz Češke, kjer je leta 2003 19 letni Lukas Kohut pretental vlado in si na državne stroške privoščil lete na več eksotičnih destinacij. To mu je uspelo tako, da je ponaredil naročilo leta za takratnega zunanjega ministra in predsednika Generalne skupščine OZN Jana Kaviana, kasneje pa v njegovem imenu sporočil, da se leta ne more udeležiti, ter da ga bo nadomestil njegov tajnik – Lukas. Na ta način je obiskal Maldive, Peru, Južno Afriko,... ko pa je želel obiskati Šrilanko, se je zataknilo. Za prelet Indije namreč ni imel urejenega dovoljenja in takrat so ga razkrinkali. Na ta polet je s seboj vzel tudi svojo »delegacijo«, svojih 5 prijateljev (Velinger 2003).

Preventivo pred telefonskim socialnim inženiringom predstavlja predvsem določena mera skepticizma. Vsakomur in vsemu namreč ni verjeti. Osebo, ki nas kliče, je pametno povprašati za telefonsko številko, kamor jo lahko pokličemo nazaj, seveda pa se je pametno dogovoriti tudi, kako naj se v podjetju ravna z gesli in na kakšen način deluje podporna služba. Na primer, naj podporna služba nikoli ne zahteva gesla ali pa naj vedno pridejo osebno, ipd.

2.1.5 Zunanje spominske enote

Kaj naredimo, če najdemo USB spominski ključek? Po vsej verjetnosti ga preizkusimo, pa če je to zaradi radovednosti ali pa zato, ker bi radi našli lastnika. Tudi socialni inženirji se

zavedajo, da bo večina najden USB ključek preizkusila, zato je to dober način, kamor skriti škodljivo programsko opremo kot na primer trojanskega konja, ki iz računalnika izbrska gesla in druge zaupne informacije, ter jih pošlje na želen elektronski naslov. Tak scenarij so preizkusili v Ameriki, kjer so na parkirišču podjetja raztresli 20 USB ključkov od katerih jih je bilo uporabljenih kar 15 (Dark Reading 2006). Tak način socialnega inženiringa se lahko uporablja tudi s katerimkoli drugim spominskim medijem, kot na primer z zgoščenko, spominsko kartico, disketo, ipd.

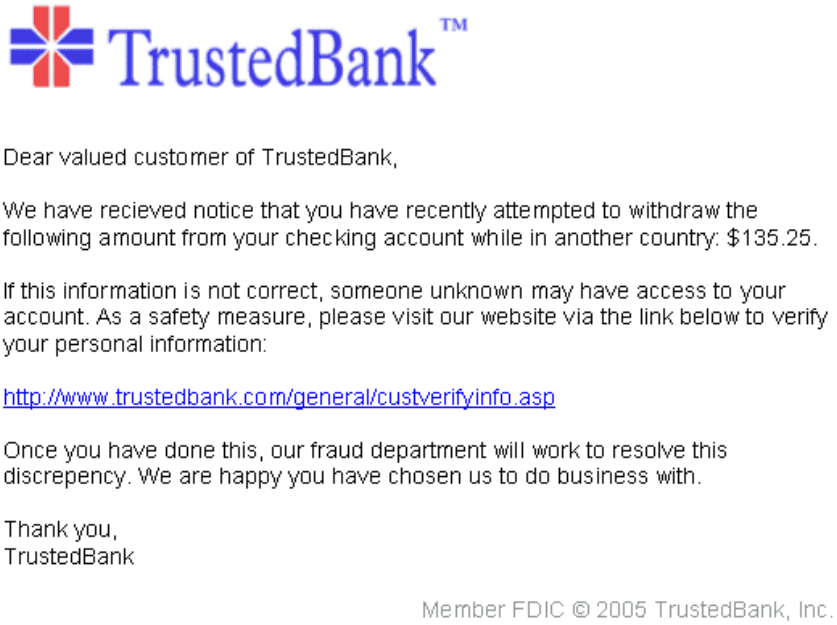
2.2 TEHNIČNI PRISTOP

2.2.1 Phishing

Phishing ali ribarjenje je najpogostejša vrsta socialnega inženiringa na internetu. Je kraja zasebnih podatkov s pomočjo ponarejenih elektronskih sporočil in spletnih strani. Najpogosteje ponarejene so strani finančnih organizacij, strani spletnih prodajaln oz. »oglasnikov« in ponudnikov internetnih storitev (Tipton in Krause 2008, 2856). Vse pogosteje po so tarča phishinga strani namenjene socialnemu omreževanju uporabnikov kot npr. Facebook, Myspace, ipd (Arthur 2009). O obsežnosti tovrstnih prevar priča tudi raziskava organizacije Gartner, ki ocenjuje povzročeno škodo v Združenih državah Amerike za leto 2007 na 3,2 milijarde dolarjev (Gartner 2007). Sama beseda phishing izvira iz besede fishing (ribarjenje), kjer sta črko »f« zamenjali »ph«. Ta zamenjava črk pa izvira iz začetkov računalniškega vdiranja v omrežja in sicer vdiranj v telefonska omrežja, ki so se imenovala phreaking. Le ta beseda pa izhaja iz phone freaking (Tipton in Krause 2008, 2854). Druga razlaga izvora beseda phishing je skovanka besed password (geslo) in fishing (ribarjenje), torej ribarjenje gesel (Skrt 2004).

Postopek phishinga, ki ga opisujeta Tipton in Krause poteka takole (Tipton in Krause 2008, 2856). Prevarant oziroma »ribič« najprej izbere organizacijo, za katero se bo pretvarjal, ter nato izdela podobno oziroma identično stran. Ko je stran izdelana, potrebuje uporabnike, ki bi tej strani nasedli. Le te privabi z elektronskimi sporočili, ki jih pošlje na milijone naslovov. Načinov, kako uporabnika privabijo, je veliko. Običajno uporabnika storitev obvestijo, da je prišlo do določenega zapleta, ter da je potrebno ponovno vnesti uporabnikove podatke, da bodo lahko nadaljevali z uporabo storitve. Spodaj je prikazan primer tovrstnega sporočila.

Slika 2.1: Primer phishing sporočila



Vir: Answers.com (2004).

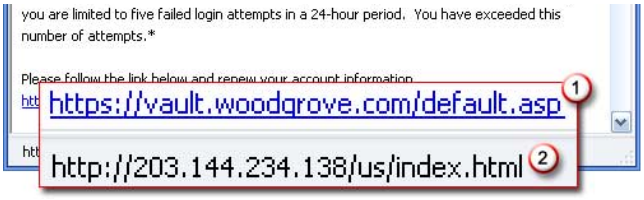
Izmed ogromnega števila poslanih sporočil se jih mnogo zaustavi že na prejemnikovih filtrih za neželeno pošto. Čeprav se le določen odstotek sporočil prebije do uporabnikov, je ta številka še vedno zelo velika. Nato pa se še tukaj izločijo še sporočila, ki jih uporabniki ignorirajo. Sporočilom podležejo tisti uporabniki, ki so v strahu, da bi izgubili določeno storitev in s tem izgubijo svoj denar ali pa identiteto (Tipton in Krause 2008, 2857).

Kako se torej zaščititi pred phishing napadi? Vedeti moramo, da so prevaranti velikokrat korak pred branilci. Ko se uporabniki naučimo prepoznavati določene prevare, se prevaranti prilagodijo in poiščejo nove načine. Spodaj je nekaj osnovnih pravil kako se ubraniti.

- *Naučiti se moramo identificirati potencialne phishing prevare.*
  Kot omenjeno taka sporočila dajejo vtis avtentičnosti in sicer z logotipom, imenom in priimkom, telefonsko številko, internetnim naslovom banke.
- *Preveriti moramo vir prejetih sporočil.*
  Če smo negotovi glede pošiljatelja, pokličimo v banko in preverimo ali ta oseba res obstaja.
- *Nikoli ne dostopamo do strani banke preko povezav v elektronski pošti.*

Za povezavo, ki jo vidimo na prvi pogled, se lahko marsikaj skriva. Ko na tako povezavo kliknemo, se nam namreč odpre druga stran. Primer take povezave je prikazan na spodnji sliki.

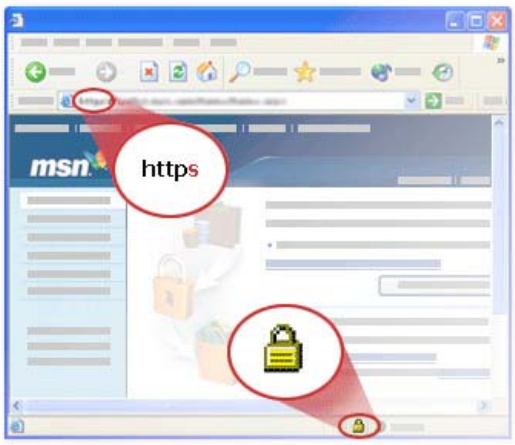
Slika 2.2: Zavajajoča internetna povezava v phishing sporočilu



Vir: Microsoft (2006).

- *Poskrbimo za varnost računalnika.*
  Za varnost poskrbimo tako, da imamo protivirusni program, požarni zid in program za odstranjevanje neželenih programov. Vsi ti programi pa morajo biti posodobljeni. Prav tako moramo skrbeti, da je posodobljen tudi naš operacijski sistem. Veliko virusov namreč izkorišča ravno te pomanjkljivosti oziroma varnostne luknje v programih.
- *Bodimo pozorni na uporabo varnih povezav.*
  Ko obiskujemo spletne strani bank in ostalih finančnih organizacij moramo biti previdni, da uporabljamo varno povezavo, ki je v brskalnikih razvidna na dveh mestih. V naslovni vrstici mora pisati https://, poleg tega pa mora v brskalniku viden simbol zaklenjene ključavnice. Simbol se običajno nahaja na dnu brskalnika, je pa lokacija simbola odvisna tudi od internetnega brskalnika.

Slika 2.3: Izgled varne povezave



Vir: Microsoft (2009).

- *Redno preverjajmo bančne izpiske.*
- *Bodimo pozorni tudi na prevare na drugih straneh in ne le na spletnih bankah.*
- *Phishing se uporablja v različnih jezikih.*

Čeprav je večina phishing sporočil v angleškem jeziku, se ta trend spreminja. Prevaranti zaradi večjega »ulova« sporočila in strani prevajajo v lokalne jezike, vendar pri tem prihaja do določenih slovničnih napak. Prevaranti namreč uporabljajo avtomatske prevajalnike, ki pa zaenkrat niso dovolj natančni. Phishinga pa se vedno ne bo dalo prepoznati po slovničnih napakah, saj bodo prevodi vedno boljši, s prevarami pa se bodo začeli ukvarjati tudi domačini. Spodaj je primer slabega poskusa phishinga, kjer so prevaranti uporabili avtomatski prevajalnik kot je na primer Google Translate.

Slika 2.4: Phishing sporočilo Siol.net

From: "SiOL INTERNET STORITEV"<info@siol.net>
Sent: Wednesday, March 04, 2009 12:30 AM
Subject: Dear SiOL imetnika računa,

Dear SiOL imetnika računa,

Za dokončanje vasega SiOL račun, morate odgovoriti na to sporočilo takoj in vpisite svoje geslo (). To sporočilo je od SiOL internetni naslov sporočila nadgradnja centra za vse SiOL e-postnega računa lastnikov. Trenutno poteka nadgradnja nase baze podatkov in e-postni račun klubi. Smo izbrisete vse neuporabljene in privzete SiOL e-postnih računov, da ustvarite več prostora za nove račune.

Ta proces bo tudi nam pomagajo v boju proti spam poste. Če zelite preprečiti, da vas račun ni zaključena, boste morali posodobiti zdaj takoj za potrditev, da je sedanja uporablja račun in za veljaven dokaz, če ste za lastnika tega računa.

Potrdite svoj e-naslov IDENTITETA SPODAJ ZA POSODOBITEV

E-mail Uporabnisko ime:
EMAIL Geslo:
Datum rojstva:
Drzava ali ozemlje:

Opozorilo! Račun lastnikov, ki noče, da posodobi svojo računa withinSeven dneh po prejemu tega opozorilo bo izgubila svojega računa stalno in samodejno.

OPOMBA: Če bo treba poslati sporočilo za ponastavitev gesla v naslednjih sedmih delovnih dneh potem, ko so v tem procesu.

Upam, da razumes.

Zahvaljujemo se vam za uporabo SiOL.

SiOL POSODOBLJENA CENTER.

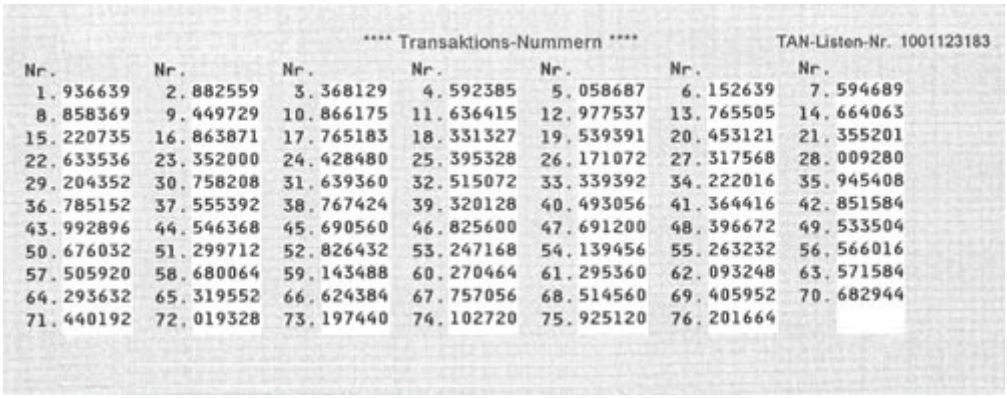
Vir: Monitor (2009).

- *Če si v dvomih, ne zaupaj nobenih zasebnih podatkov.*
- *Spremljaj novosti o novih tehnikah phishinga* (Panda security).

Vsi omenjeni nasveti so le osnovna zaščita. Zavedati se moramo namreč, da te ukrepe poznajo tudi prevaranti, ki vedno znova izumljajo poti kako se ogniti takim obrambnim ukrepom. Če se nasvet glasi, naj bomo pozorni na avtentičnost, bodo prevaranti izdelali take strani, ki se jih vsaj po videzu ne bo dalo prepoznati kot lažne. Eden izmed nasvetov je tudi preverjanje, če podpisana oseba v resnici obstaja. Prevarant lahko uporabi ime resnične zaposlene osebe in nam preverjanje osebe pri banki ne bo pomagalo odstraniti dvoma o prevari. Tudi pozornost na prisotnost varne povezave ne daje zagotovila, da gre za originalno stran. Certifikat, ki potrjuje, da gre za varno povezavo, se da namreč ponarediti (Kovačič 2008).

Zaščita, ki je kot kaže uspela celo malenkost zmanjšati phishing napade predvsem na spletne banke, je uporaba varnostnega sistema TAN (transaction authentication number) oziroma avtentikacijska številka transakcije (Heise.de 2009). TAN predstavlja avtentikacijsko informacijo, ki jo naključno določi na primer banka, ter posreduje uporabniku preko varnega komunikacijskega kanala. Lahko se uporablja za vstop na stran ali pa za posamezno transakcijo opravljeno na strani (Oppliger 2002, 115). To avetnikacijsko informacijo lahko dobimo preko SMS sporočila, kar se imenuje mTAN (mobilni TAN) ali pa preko seznama gesel, ki nam ga je po pošti posredovala banka in se imenuje iTAN (indeksirani TAN) (Enisa 2008, 9). Tudi tak varnostni mehanizem ni nepremagljiv, je pa z njegovo uporabo delo prevarantom zelo otežkočeno.

Slika 2.5: seznam TAN številk – iTAN



**** Transaktions-Nummern **** TAN-Listen-Nr. 1001123183

Nr.	Nr.	Nr.	Nr.	Nr.	Nr.	Nr.
1. 936639	2. 882559	3. 368129	4. 592385	5. 058687	6. 152639	7. 594689
8. 858369	9. 449729	10. 866175	11. 636415	12. 977537	13. 765505	14. 664063
15. 220735	16. 863871	17. 765183	18. 331327	19. 539391	20. 453121	21. 355201
22. 633536	23. 352000	24. 428480	25. 395328	26. 171072	27. 317568	28. 009280
29. 204352	30. 758208	31. 639360	32. 515072	33. 339392	34. 222016	35. 945408
36. 785152	37. 555392	38. 767424	39. 320128	40. 493056	41. 364416	42. 851584
43. 992896	44. 546368	45. 690560	46. 825600	47. 691200	48. 396672	49. 533504
50. 676032	51. 299712	52. 826432	53. 247168	54. 139456	55. 263232	56. 566016
57. 505920	58. 680064	59. 143488	60. 270464	61. 295360	62. 093248	63. 571584
64. 293632	65. 319552	66. 624384	67. 757056	68. 514560	69. 405952	70. 682944
71. 440192	72. 019328	73. 197440	74. 102720	75. 925120	76. 201664	

Vir: Sparkasse.

Vsekakor pa velja vedeti tudi, da vam banka ali kaka druga ustanova nikoli ne bo pošiljala elektronske pošte, v kateri bo zahtevala vpis vaših osebnih podatkov. Če bo potrebno, bo to storila na druge načine. Poleg lastne previdnosti pa je dobro na prevare opozoriti policijo in Si-Cert (Slovenian Computer Emergency Response Team). Slednji bodo poskušali stran čim prej locirati in jo odstraniti.

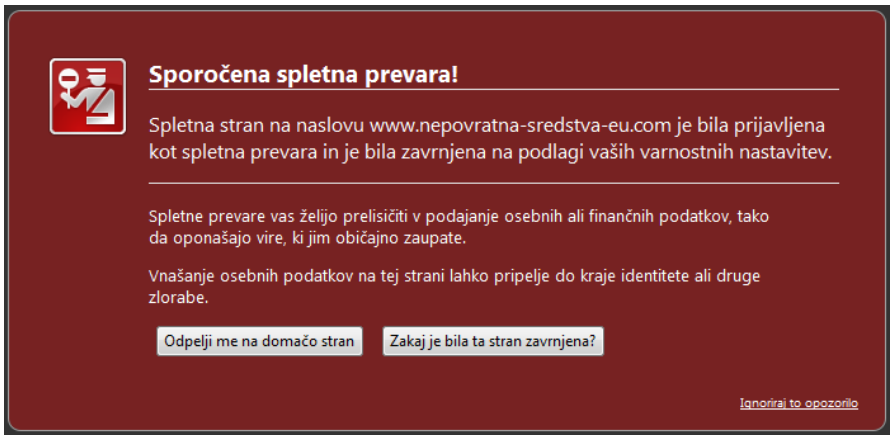
2.2.2 Pharming

Pharming je prevara zelo podobna phishingu, s to razliko, da se jo težje odkrije. Pharming predstavlja »preusmerjanje z legitimnih strani na nelegitimne z namenom pridobitve zasebnih podatkov« (Whitman in Mattord 2007, 72). Drugače ga imenujemo tudi »DNS poisoning« (Lininger in Vines 2005, 100) oziroma, če prevedemo, bi lahko rekli zastrupljanje DNS strežnika ali DNS preusmerjanje. Kako torej deluje? Domenski strežnik (DNS – domain name server) je strežnik, ki skrbi, da posamezniku za odprtje neke strani kot npr. www.fdv.uni-lj.si, ni potrebno vpisovati v brskalnik IP naslova te strani, ki je 193.2.106.66, pač pa le domeno, ki si jo je veliko lažje zapomniti kot številke. DNS strežnik torej usmerja internetne domene na pravi IP naslov. Pharming spremeni DNS strežnik in uporabi svoje, ter nas usmerja na svoj IP naslov. Torej ko vtipkamo želeno stran, se nam stran odpre, vendar je to stran, ki se nahaja drugje kot originalna. Vrst pharming napadov je več. Eden od načinov je sprememba hosts datoteke na posameznem računalniku, bolj pogoste pa so spremembe na routerjih oziroma usmerjevalnikih (Jakobsson in Myers 2006, 124-127). Spremembo DNS strežnikov oziroma tak napad izvede običajno trojanski konj, ki ga dobimo na računalnik (Whitman in Mattord 2007, 72). Ko se nam ponarejena stran odpre in ko vpišemo uporabniško ime in geslo (ali katerekoli druge zahtevane podatke) nas običajno ponarejena stran obvesti, da je prišlo do tehnične napake in naj geslo vpišemo še enkrat. Takrat pa se nam odpre originalna stran. Na ta način prevaranti pridejo do zasebnih podatkov, uporabnik pa nič sluteč normalno uporablja naprej storitev, ne vedoč, da je prišlo do vdora.

Pharming izhaja iz besede phishing, katerega izvor sem že pojasnil. Razlika med tema dvema napadoma je v tem, da pharming ne potrebuje vabe – elektronskih sporočil. S tem, ko ni sporočil, ki se nam bi lahko zdela sumljiva, je pharming mnogo težje odkriti. Odkrivanje pa nam otežuje tudi pravilen naslov spletne strani. Preventiva je torej potrebna že preden dobimo

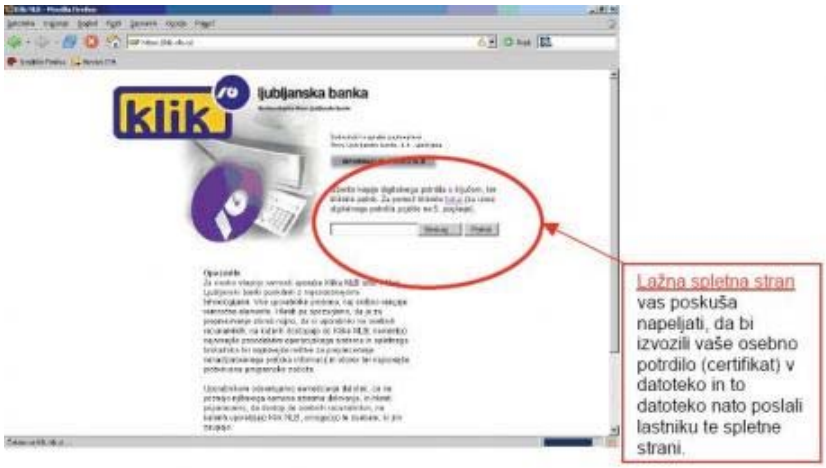
virus. Le tega se lahko obranimo z posodobljenimi protivirusnimi programi, požarnim zidom, posodobljenim brskalnikom in operacijskim sistemom. Če pa že slučajno dobimo tak virus, ki nam je spremenil DNS strežnike, se pharminga lahko obranimo z novejšimi brskalniki, ki preverjajo ime internetne strani in IP naslov z znanimi phishing stranmi (Jakobsson in Myers 2006, 125). Primer blokade take strani je prikazan na spodnji sliki.

Slika 2.6: Opozorilo brskalnika o spletni prevari



Primeri pharminga so vse pogostejši tudi v Sloveniji. Nekatere banke so že izkusile vdore ali poskuse vdora. Spodaj je primer ponarejene spletne banke NLB.

Slika 2.7: Pharming strani NLB Klik leta 2006



Vir: Računalniške novice (2006).

Cilj takratnega prevaranta je bil dobiti uporabnikov certifikat, ki je eden od varnostnih mehanizmov, potrebnih za vstop na spletno banko. Stran se je nahajala na istem naslovu https://klik.nlb.si, vendar pa se je od originalne ločila po tem, da kot prvo, na brskalniku ni

bilo simbola zaklenjene ključavnice, kot drugo pa na strani ni bilo zapisanega imena uporabnika (Računalniške novice 2006).

Pharming pri NLB spletni banki se je ponovil tudi v letošnjem letu, letu 2009. Tudi tokrat je bila stran na pravem naslovu https://klik.nlb.si in tudi tokrat v brskalniku ni bilo simbola zaklenjene ključavnice. Tokrat je bil cilj prevare pridobitev dodatnega gesla, ki je druga stopnja varnosti pri spletni banki (NLB 2009). To dodatno geslo temelji pri tej banki na sistemu iTAN, ki sem ga maloprej omenil. Edini problem pa je v tem, da je geslo sestavljeno le iz 8 znakov, medtem ko je prej omenjen iTAN primer sestavljen iz večih kombinacij po 6 znakov. Kar pomeni, da v primeru NLB dejansko lahko dodatno geslo zaupamo prevarantu, medtem ko v drugem primeru malo težje zaupamo vseh 70 kombinacij znakov. Verjetnost vdorov v spletne račune pa bi še dodatno zmanjšali z uporabo dveh različnih komunikacijskih kanalov, kjer drugi kanal ne vključuje interneta (Enisa 2008). Za vstop na stran bi na primer dobili sms na katerega bi morali odgovoriti in šele nato bi lahko z običajnim geslom vstopili na stran.

Slika 2.8: Pharming strani NLB Klik leta 2009

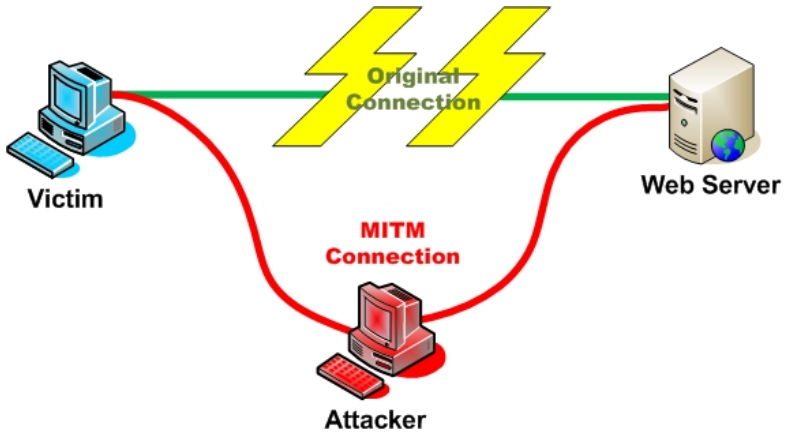
Vir: NLB (2009).

Kot sem omenil je pharming bolj tehnična verzija phishinga. Čeprav vsi viri vključujejo pharming v tehnike socialnega inženiringa pa se poraja vprašanje, če pharming to sploh je. Bistvo socialnega inženiringa je namreč izkoriščanje naivnosti posameznikov za dosego cilja. V tem primeru pa napad ne izkorišča ljudi pač pa napada DNS strežnike, torej računalnik ali usmerjevalnik. Uporabnika tako skoraj ne moremo kriviti za naivnost, saj je kriva kvečjemu zaščita računalnika. Vseeno pharming ne obstaja brez phishinga, ki sam po sebi je tehnika socialnega inženiringa.

2.2.3 Man in the middle attack (MITM)

Še bolj napredna izvedba napada od phaminga je napad »man in the middle« ali v slovenščini napad s posrednikom. Gre za napad, kjer napadalec prestreza komunikacijo med dvema sistemoma, kot na primer med uporabnikom in spletno banko (Wismer 2007). Tak način je še toliko težje prepoznati, saj vse strani delujejo normalno kot prej, ugotoviti, da nam nekdo »prisluškuje«, pa je zelo težko. Zaščita proti tem napadom je uporaba varnih povezav, torej certifikatov, za katere pa sem že omenil, da so ranljivi. Verjetno najboljša zaščita je torej uporaba dvofaktorske avtentikacije TAN in sicer preko drugega komunikacijskega kanala.

Slika 2.9: Napad s posrednikom (MITM)



Vir: Owasp (2009).

2.2.4 Smishing

Smishing je posebna oblika ribarjenja in sicer preko SMS sporočil. Prejemnik dobi sporočilo na mobilni telefon od banke, spletne prodajalne ali druge finančne institucije, kjer zahtevajo potrditev določenih podatkov, tako da kliknete na določeno povezavo ali pokličete na določeno telefonsko številko (Wall 2007, 229). Na ta način prevaranti pridobijo zasebne podatke. Smishing je prevara, ki naj bi bila v porastu, prevaranti pa se je poslužujejo predvsem zato, ker smo uporabniki postali sumničavi na zahteve banke po elektronski pošti, medtem ko smo manj previdni, če gre za sms sporočilo ali telefonski klic (Wall 2007, 74).

2.2.5 Vishing

Tudi vishing je novejša prevara, ki pa temelji na telefoniji preko interneta (VOIP – Voice over IP). Vishing napad je oblikovan tako, da na več tisoč telefonskih številk pošljejo posneto telefonsko sporočilo različnih organizacij, ki zahtevajo določeno akcijo. Tako na primer zahtevajo, naj uporabnik pokliče v klicni center, saj so zaznali, da je bila njihova kreditna kartica zlorabljena. Uporabnika nato v telefonskem pogovoru zaprosijo za številko kreditne kartice in kodo, da bi preverili, če je šlo res za napako, ter mu sporočijo na primer, da je vse v redu. Telefonska številka, uporabljena za klicni center, je v tem primeru ponarejena, kar je z internetno telefonijo (VOIP) mnogo lažje storiti (Wall 2007, 76).

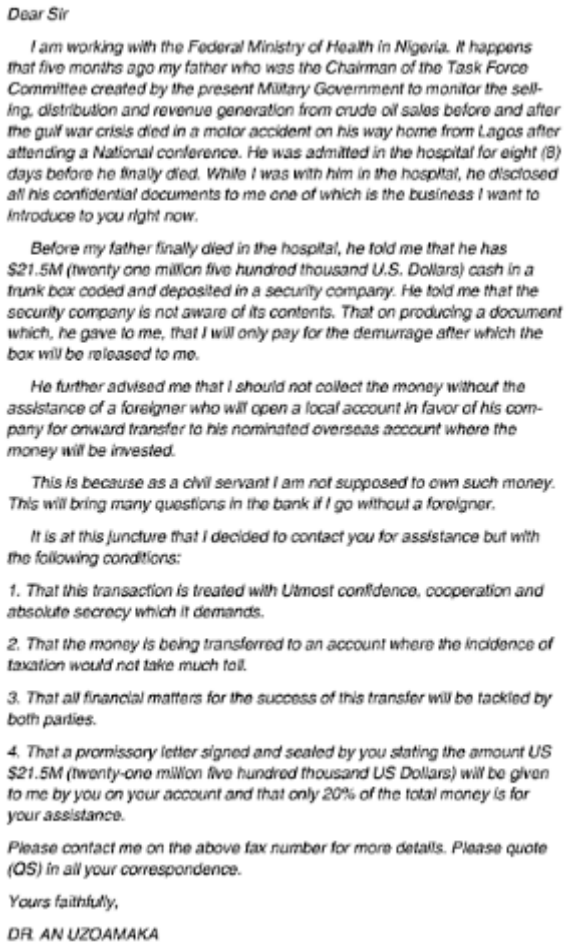
2.2.6 Nigerijska pisma – prevara 419

Nigerijske prevare so pisma, v katerih se prevarant pretvarja, da je npr. sin Nigerijskega predsednika, nigerijski uslužbenec, poslovnež, ipd. V pismu pojasni situacijo, da ima na računu večjo količino denarja, ki jo mora spraviti iz države. Za pomoč poprosi nas, v zameno pa nam obljubi določen odstotek nakazane vsote. Ko uporabnik izkaže voljo za sodelovanje, mu običajno naročijo, naj nakaže nekaj malega denarja za ureditev papirjev, ipd. Zadeva se ponovno zatakne in izmislijo si drug izgovor, zakaj denarja še ni na računu, kot na primer, da mora podkupiti bančnega uslužbenca, oblast, ipd. in da ponovno potrebuje denar. To se ponovi večkrat, dokler prevarani ne ugotovi, da denarja oziroma provizije nikoli ne bo dobil (Miller 2008, 123).

Prva tovrstna prevara se je pojavila že leta 1588 in se imenuje »prevara španski zapornik« (Weisman 2008, 42). V pismu je takrat namišljeni španski zapornik, sicer premožen aristokrat, prosil za denarno pomoč, ki jo potrebuje za izpustitev iz zapora, v zameno pa obljubljal večje vsote denarja, ko bo izpuščen. Sicer pa naj bi se nigerijska prevara, kot jo poznamo danes, razširila v letu 1980 preko faksa in teleksa, kasneje pa preko elektronske pošte, ki je danes najpogostejša oblika (Miller 2008, 123). Prevaro z nigerijskimi pismi imenujemo tudi prevara 419, ta način poimenovanja izvira pa iz 419. člena Nigerijskega kazenskega zakonika (Wang 2006, 172).

Variacij te prevare je mnogo, saj se prevaranti, v želji po čim večjem številu žrtev, prilagajajo oziroma svoja pisma prilagajajo razmeram. Spodnja slika je prikaz povprečnega pisma, sicer pa si mi zdi zelo zanimiv primer pisma, ki se je razvil v času ameriške vojaške operacije v Iraku. V pismu ameriški vojak navaja, da je odkril večjo količino denarja in jo želi prikrito spraviti v Ameriko. Da bi to storil pa potrebuje tuj bančni račun in tako se zgodba odvija naprej, podobno kot v ostalih primerih te prevare.

Slika 2.10: Primer nigerijskega pisma



Dear Sir

I am working with the Federal Ministry of Health in Nigeria. It happens that five months ago my father who was the Chairman of the Task Force Committee created by the present Military Government to monitor the selling, distribution and revenue generation from crude oil sales before and after the gulf war crisis died in a motor accident on his way home from Lagos after attending a National conference. He was admitted in the hospital for eight (8) days before he finally died. While I was with him in the hospital, he disclosed all his confidential documents to me one of which is the business I want to introduce to you right now.

Before my father finally died in the hospital, he told me that he has $21.5M (twenty one million five hundred thousand U.S. Dollars) cash in a trunk box coded and deposited in a security company. He told me that the security company is not aware of its contents. That on producing a document which, he gave to me, that I will only pay for the demurrage after which the box will be released to me.

He further advised me that I should not collect the money without the assistance of a foreigner who will open a local account in favor of his company for onward transfer to his nominated overseas account where the money will be invested.

This is because as a civil servant I am not supposed to own such money. This will bring many questions in the bank if I go without a foreigner.

It is at this juncture that I decided to contact you for assistance but with the following conditions:

1. That this transaction is treated with Utmost confidence, cooperation and absolute secrecy which it demands.

2. That the money is being transferred to an account where the incidence of taxation would not take much toll.

3. That all financial matters for the success of this transfer will be tackled by both parties.

4. That a promissory letter signed and sealed by you stating the amount US $21.5M (twenty-one million five hundred thousand US Dollars) will be given to me by you on your account and that only 20% of the total money is for your assistance.

Please contact me on the above fax number for more details. Please quote (OS) in all your correspondence.

Yours faithfully,

DR. AN UZOAMAKA

Vir: Wang (2006, 173).

Prevarane s to prevaro lahko primerjamo z zasvojenci z igralništvom. Tudi če so opozorjeni, so v zanikanju, saj so zaradi želje po nenadnem zaslužku močno čustveno vpleteni (Moses 2008). Ljudi, ki so nasedli tem prevaram je mnogo, v Sloveniji pa jih bo verjetno še več, ko bodo nigerijska pisma dobro prevedena v slovenščino. Dobro pa mislim zato, ker so zaenkrat prevedena le s prevajalskimi orodji, kjer je takoj vidnih več napak. Razsežnost teh prevar kaže tudi podatek, da le te predstavljajo tretjo industrijsko panogo v Nigeriji (Wang 2006, 172).

Najboljša obramba pred nigerijskimi prevarami je prav gotovo skeptičnost in ne nasedanje obljubam o denarju.

2.2.7 Ostala pisma

Prevar s pismi, kjer se nekdo pretvarja za nekoga drugega, je več vrst. V zadnjem času so aktualne prevare v Sloveniji prošnje za denarno pomoč. Prijatelj, ki so mu sicer vdrli v poštni predal, nam pošlje sporočilo, da je bil na primer v Afriki, kjer so mu ukradli denar, ter nas prosi za pomoč, da se bo lahko vrnil v domovino (Arnes 2009).

Slika 2.11: Pismo prijatelja za pomoč

I am sorry nisem vas obvestim o mojem potovanju v Afriko za program, imenovan "Usposabljanje Mladi v boju proti rasizmu, HIV / AIDS, revščina in pomanjkanje izobrazbe, program poteka v Gani. To je bil zelo žalosten in slab trenutek zame, sedanje stanje, da sem našel samega sebe je zelo težko za mene, da razložim.
Jaz sem res nasedle v Gani, ker sem pozabil mojo vrečo v taksi, če mi moj denar, potni list, dokumente in druge dragocene stvari so se hrani na moji poti do hotela sem ostal, sem se sooča s trdo časa tukaj, ker nimam denarja za mene. Zdaj sem jaz, ki je lastnica hotela obračun $ 650 $ in se mi hotel plačati račun, ko ostali bodo morali izkoristiti moja torba in roke nad mano, da je Hotel Management, rabim to pomoč od vas nujno, da bi me domov , želim, da mi pomagaš s hotela zakona in bom tudi potrebo $ 750 $ za krmo in pomagajo sebi domov, tako si lahko prosim pomagaj mi z vsoto $ $ 1450 za rešila moje težave tukaj? Rabim to pomoč toliko ter na čas, ker sem grozna in težkem položaju tukaj, ne pa ima denar za krmo sam za en dan, kar pomeni, sem bila tako Stradam prosim razumeti, kako nujno rabim vašo help.i so se odločili, ne povej moji družini tako, da ne bodo worried.when I zameno bom jim povedati in bodo razumeli.
Jaz sem si to pošiljanje e-pošte iz mesta knjižnice in imam samo 45min, jaz cenim, kar tako kdaj si ga lahko privoščite za pošiljanje mene za zdaj in obljubim, da plača svoj denar nazaj, kakor hitro i vrnitvi home.You potrebno prenos denarja prek Money Gram ali Western Union za naslov below.Pls odgovor nazaj na mojo alternativno e-mail naslov na [redacted] @ hotmail.com gmail storitev, saj je zelo slabo tukaj v Gani Hope slišati od vas kmalu.

Tukaj je naslov o tem, kako poslati denar, ime spodaj, da plačilo je ime hotela upravitelj zaradi moje izgubljenem dokumentu z njo ne morem zbrati denar.

Ime: ofori Afrifa Louis
Mesto: Akra
Poštna številka: 00233
Država: Gana
S spoštovanjem,
krep
Prosimo, kakor hitro imaš moj mail pošlji mi podatke od denarja do nadomestnega email sem res čakajo, da je ....

Vir: Arnes (2009).

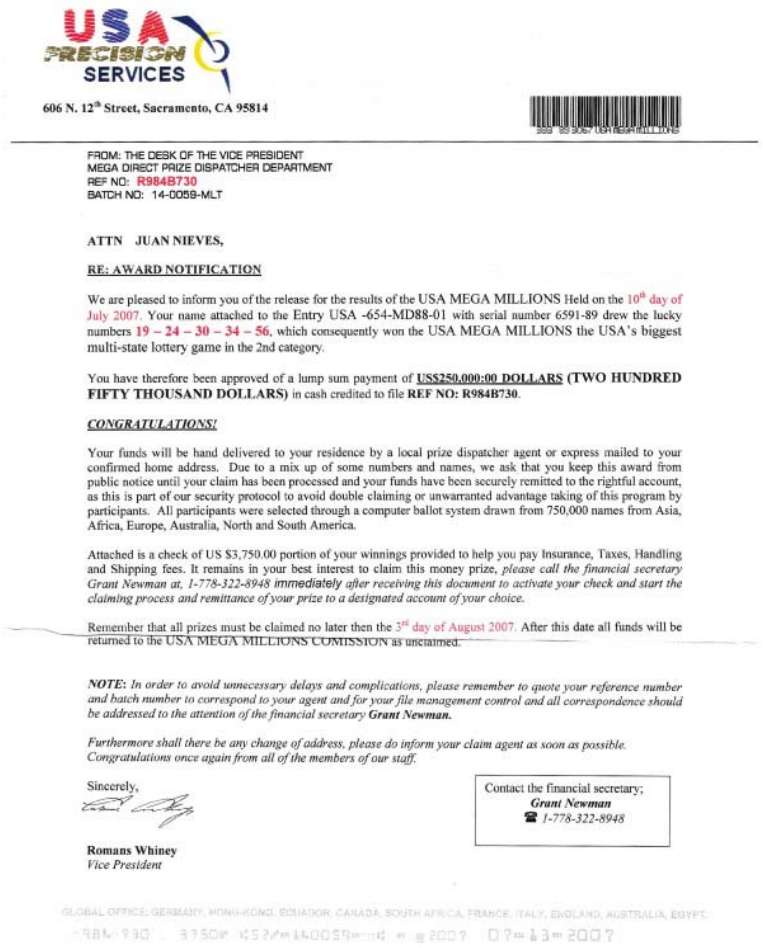
Paziti moramo torej tudi na pošto, ki nam jo pošljejo prijatelji in znanci. Če smo v dvomih, je vedno najbolje zadevo prej preveriti. Tokrat nas je na prevaro ponovno opozorila slaba slovenščina, a temu ne bo vedno tako.

2.2.8 Loterijske prevare

Konstantno prisotne prevare na spletu so loterijske prevare. Prevaranti uporabnika obvestijo, da je zadel večjo vsoto denarja, ta pa mora za prevzem nagrade poslati določeno vsoto, ki predstavlja stroške zavarovanja, davke ali pa mora navesti osebne podatke, med drugim

podatke o bančnem računu, ipd. Obstaja možnost, da prevaranti pošljejo uporabniku tudi ček, ki pa je brez kritja, vendar v vmesnem času uporabnik že nakaže zahtevano provizijo (Emarketer.si 2009). Obvestila o loterijskih zadetkih pošiljajo preko elektronske pošte in navadne pošte, preko pojavnih oken (pop-up) v internetnem brskalniku, v zadnjem času pa tudi preko sms sporočil (Livenews.com.au 2009).

Slika 2.12: Pismo loterijske prevare



USA PRECISION SERVICES

606 N. 12th Street, Sacramento, CA 95814

FROM: THE DESK OF THE VICE PRESIDENT
MEGA DIRECT PRIZE DISPATCHER DEPARTMENT
REF NO: R984B730
BATCH NO: 14-0059-MLT

ATTN JUAN NIEVES,

RE: AWARD NOTIFICATION

We are pleased to inform you of the release for the results of the USA MEGA MILLIONS Held on the 10th day of July 2007. Your name attached to the Entry USA -654-MD88-01 with serial number 6591-89 drew the lucky numbers 19 – 24 – 30 – 34 – 56, which consequently won the USA MEGA MILLIONS the USA's biggest multi-state lottery game in the 2nd category.

You have therefore been approved of a lump sum payment of US$250,000:00 DOLLARS (TWO HUNDRED FIFTY THOUSAND DOLLARS) in cash credited to file REF NO: R984B730.

CONGRATULATIONS!

Your funds will be hand delivered to your residence by a local prize dispatcher agent or express mailed to your confirmed home address. Due to a mix up of some numbers and names, we ask that you keep this award from public notice until your claim has been processed and your funds have been securely remitted to the rightful account, as this is part of our security protocol to avoid double claiming or unwarranted advantage taking of this program by participants. All participants were selected through a computer ballot system drawn from 750,000 names from Asia, Africa, Europe, Australia, North and South America.

Attached is a check of US $3,750.00 portion of your winnings provided to help you pay Insurance, Taxes, Handling and Shipping fees. It remains in your best interest to claim this money prize, *please call the financial secretary Grant Newman at, 1-778-322-8948 immediately after receiving this document to activate your check and start the claiming process and remittance of your prize to a designated account of your choice.*

Remember that all prizes must be claimed no later then the 3rd day of August 2007. After this date all funds will be returned to the USA MEGA MILLIONS COMISSION as unclaimed.

NOTE: *In order to avoid unnecessary delays and complications, please remember to quote your reference number and batch number to correspond to your agent and for your file management control and all correspondence should be addressed to the attention of the financial secretary* ***Grant Newman.***

Furthermore shall there be any change of address, please do inform your claim agent as soon as possible. Congratulations once again from all of the members of our staff.

Sincerely,

Romans Whiney
Vice President

Contact the financial secretary;
Grant Newman
☎ *1-778-322-8948*

GLOBAL OFFICE: GERMANY, HONG-KONG, ECUADOR, CANADA, SOUTH AFRICA, FRANCE, ITALY, ENGLAND, AUSTRALIA, EGYPT.

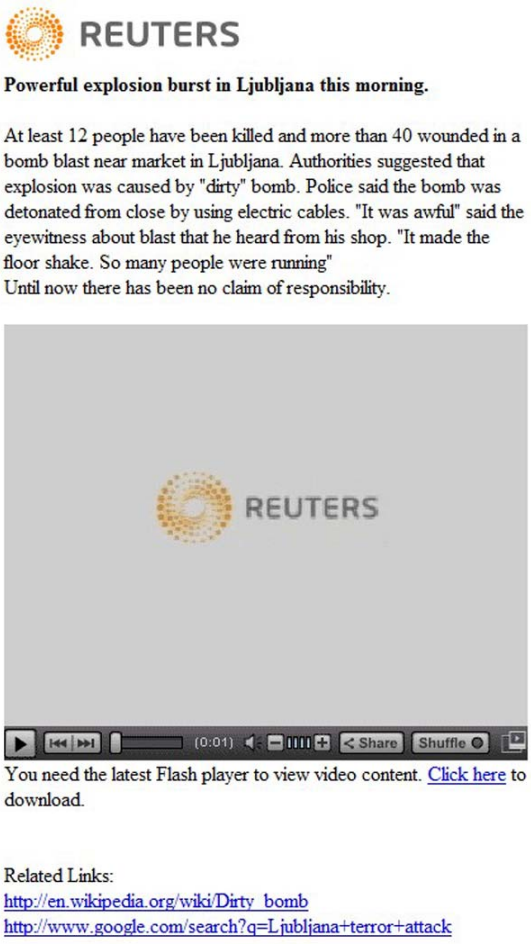
Vir: USA Mega.

2.2.9 Ostalo

Phishing napadi se ne osredotočajo le na finančne institucije, ipd., kjer je njihov namen kraja identitete, pač pa se phishinga poslužujejo tudi pri izdelovalcih škodljivih programov oz. virusov. Nedavno se je tudi v Sloveniji pojavil phishing v obliki novice, ki sporoča, da je na ljubljanski tržnici prišlo do eksplozije. Pod novico je video posnetek, kjer pa ob kliku nanj dobimo opozorilo, da je potrebno za ogled videa posodobiti predvajalnik. Z namestitvijo tega

programa smo dejansko namestili virus. Ta phishing se je posluževal geografske lokacije IP naslova in na podlagi tega izpisoval kraj, kjer naj bi prišlo do eksplozije. Tako, smo Ljubljančani avtomatsko videli Ljubljano, drugod po svetu pa so videli svojo lokacijo (Vest 2009).

Slika 2.13: novica eksplozije v lokalnem mestu

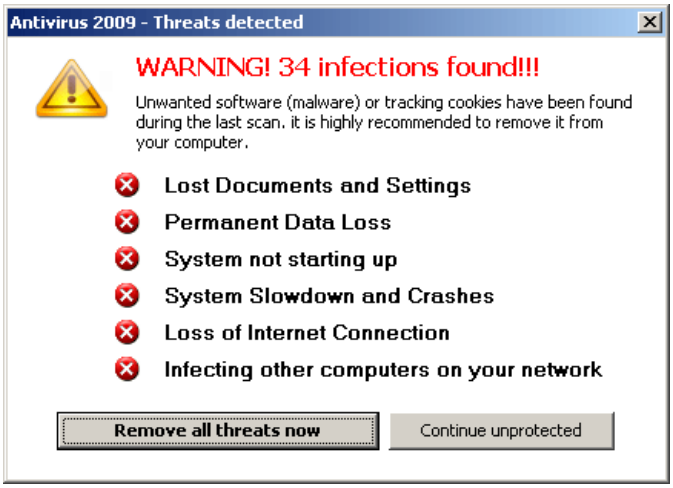


Vir: Vest (2009).

Primer prevare, kjer cilj ni pridobitev zasebnih podatkov, je tudi prevara z lažnimi protivirusnimi programi. Ljudje v želji po brezplačni protivirusni zaščiti nameščajo na svoje računalnike različne, nepriznane programe. Ti programi pa so lahko le krinka za razne računalniške viruse ali vohunska orodja. Torej, ko namestimo protivirusni program, dejansko namestimo virus. Nadaljuje se celo tako daleč, da ta lažni protivirusni program opozarja, da smo okuženi z virusom, ter da je potrebna nadgradnja programa, da ga odstranimo. Z

nadgradnjo pa dejansko spustimo v svoj računalnik še več škodljivih programov (Trend Micro 2008).

Slika 2.14: lažna opozorila za protivirusno zaščito



Vir: Trend Micro (2008).

Tudi tukaj težko govorimo o socialnem inženiringu, kjer človek z manipulativnimi postopki prepriča nekoga v neko akcijo. Vseeno pa so nasveti za boj pred tako prevaro podobni kot prvi večini primerov socialnega inženiringa in sicer previdnost ter skeptičnost. Na internetu ima pregovor »ni vse zlato, kar se sveti« še toliko večji pomen.

3 MEHANIZMI DELOVANJA

Socialni inženir, kot omenjeno, uporablja manipulativne prijeme za svoj cilj. Velja mnenje, da je človek najšibkejši člen v računalniški varnosti. Zakaj je temu tako in kako lahko uspe prevarant prepričati povprečnega uporabnika? Če sem v predhodnih poglavjih govoril o orodjih ali poteh bom sedaj govoril o načinih ali mehanizmih za predor človekovega varnostnega zidu.

Načini se med seboj, glede na tip prevare, razlikujejo. Raziskovalna hiša Gartner je opisala 6 tipov vedenjskih vzorcev, ki pomagajo prevarantu pri svojem delu (Gartner 2002). Ti so:

- *Vzajemnost.*
  Ko nam nekdo naredi uslugo, se čutimo obvezane, da bi mu jo vrnili. Tak primer predstavljajo degustacije, ko se kupcu ponudi zastonj poizkus izdelka, ta pa se čuti dolžnega, da ta izdelek potem kupi.
- *Doslednost.*
  Ljudje se držimo določenih vzorcev obnašanj in s tem postajamo predvidljivi. Na primer vedno kupujemo iste izdelke.
- *Družbena veljavnost.*
  Ljudje počnemo to kar je družbeno sprejemljivo. Počnemo to, kar počnejo drugi. Če vsi kupujejo neko blagovno znamko, jo kupujemo še mi.
- *Všečnost.*
  Pogosteje se pozitivno odzovemo, če nam je nekdo všeč. Zato so v oglasih pogosto prisotni/e manekeni/ke.
- *Avtoriteta.*
  Smo bolj poslušni, ko gre za ljudi na višjih položajih. Tak primer bi bil uporaba avtoritete strokovnjaka za prepričevanje kupcev.
- *Redkost.*
  Če je neka zadeva v omejeni količini, se nam zdi bolj privlačna.

Omenjeni načini so marketinški pristopi oziroma »manipulativni« pristopi, ki se uporabljajo v marketingu, jih pa lahko apliciramo tudi na manipulativne pristope socialnega inženiringa. Ljudje izdajamo zasebne podatke za npr. brezplačno igro na spletu (vzajemnost); iz

predvidljivega strahu pred ukinitvijo neke storitve (doslednost); ker naj bi naš sodelavec zaupal podatke, mi pa jih naj ne bi hoteli (družbena veljavnost); nas prijazen glas naprosi za pomoč (všečnost); se sklicuje na šefa, ki naj bi potreboval te podatke (avtoriteta) ali ker se redko zgodi, da zadenemo na lotu in slepo verjamemo obvestilu o zadetku (redkost).

Socialni inženirji prežijo na različne lastnosti človekove narave. Zanašajo se na *človekovo željo po prijaznosti in ustrežljivosti*. Veliko podjetij se namreč trudi, da bi bili prijazni do strank, ter tako včasih zaupajo več podatkov kot bi jih smeli. Prevaranti računajo tudi *na težnjo po zaupanju v ljudi*. Ljudje smo namreč po naravi zaupljivi, dokler se ne pokaže nasprotno. Vplivati se da tudi na *strah, da bi zabredli v težave v primeru nesodelovanja.* Ljudje v strahu, da bi na nas gledali čudno, da bi postopek preverjanja predolgo trajal ali da bi morda koga užalili, storimo kar nas prosijo. Prevaranti računajo tudi na človekovo lenobo oziroma *željo ljudi po bližnjicah*. Velikokrat smo ljudje površni in gesla shranjujemo na listkih, ki jih pospravimo v predal, pod tipkovnico ali pa jih nalepimo kar na monitor (Peltier 2006, 13-14). Prijaznost in ustrežljivost je poklicna dolžnost zaposlenih v službah za pomoč uporabnikom ter v tajništvu, zatorej socialni inženirji še toliko raje kontaktirajo njih. Ti se morajo naučiti ločiti prave stranke od prevarantov.

Workman v svoji raziskavi ugotavlja, da na uspešnost socialnega inženiringa vpliva (Workman 2007, 317-322):

- *Resnost grožnje in ranljivost.*
  Ljudje, kot pravi Workman, živimo v iluziji neranljivosti. Zavedamo se, da obstaja kriminal oziroma prevare, a vseeno imamo občutek, da se kaj takega ne more zgoditi nam. Bolj, ko smo takega mišljenja, se pravi prevare ne jemljemo za resne grožnje, večja je verjetnost, da podležemo prevaram. Podvrženost prevaram pa je odvisna tudi od občutka ranljivosti. Znano je namreč, da so ljudje, ki so že bili žrtve socialnega inženiringa, bolj previdni in pozorni na take napade (Dorn in Brown v Workman 2007, 318).
- *Vzajemnost oziroma obveza.*
  Ko nam nekdo ponudi nekaj za nas vrednega, se počutimo dolžne, da bi uslugo vrnili. Pri tem gre lahko za informacije lahko pa tudi za denar. Nigerijska pisma računajo

ravno na to. Najprej nam ponudijo denar oziroma provizijo, v zameno pa prosijo, če lahko skrijejo denar na naš račun (Mitnick in Simon v Workman 2007, 319).

- *Všečnost in zaupanje.*

  Všečnost lahko na kratko opišemo kot atraktivnost, karizmo, šarm in splošno popularnost (Cialdini v Workman 2007, 320), vendar pa pri različnih vrstah prevar ne morejo uporabiti vseh oblik. Večino teh lahko uporabijo pri osebnem pristopu socialnega inženiringa, ki pa ni tako pogost. Za neosebne pristope mora torej prevarant ubrati druge pristope, da bi se prikupil žrtvi in sicer tako, da pridobi njeno zaupanje s prijateljskim odnosom (Gendall v Workman 2007, 321).

- *Strah in avtoriteta.*

  Zelo pogosta metoda, ki se jo uporablja pri večini tipov socialnega inženiringa, je vplivanje na strah. Pri elektronski pošti je zelo pogosto uporabljen naslov »urgentno« ali »nujno posodobite informacije«, ipd (Workman 2007 321). Ljudje naredimo največ napak, ko se nam mudi. Strah pa se uporablja tudi pri telefonskih napadih.

Nekatere že omenjene, podobne in tudi nove smeri kako izkoristiti človeško naravo in prepričati ljudi v sodelovanje omenja tudi Manske. Ena izmed poti je *razpršitev odgovornosti*, kjer uporabnika prevarat prepriča, da ni možnosti, da bi zaradi želenega dejanja prišel v težave. Obljuba *lepe besede nadrejenemu* o uslužbencu, ki mu je pomagal, je lahko ena izmed taktik ki jo izbere prevarant. Socialni inženir lahko skuša vzbuditi pri žrtvi *občutek moralne dolžnosti*. S prošnjo, v kateri omeni, da bo brez njegove pomoči imel veliko težav, se žrtvi zasmili, ter tako pride do želenih informacij. Pot do informacij je tudi *vzbujanje občutka kontrole* pri tarči, ki lahko na primer v primeru dvoma pokliče svojega šefa in se prepriča. Za uspešen napad je priporočljiv *povečan občutek realnosti*. Dosti bolj pristen izpade napadalec, ki zna hitro navesti osebe iz organizacije, govori o organizaciji kot bi že dlje časa delal tam, skratka, se spozna na situacijo. Za tak napad mora torej napadalec prej opraviti raziskavo oziroma že prej s pomočjo socialnega inženiringa priti do teh podatkov. Kot zadnje pa navaja Manske *zastraševanje*, kjer se prevarant predstavlja za nekoga pomembnega in pompoznega, ter tako pride do želenega (Manske 2000, 57-58).

Poti, smeri, mehanizmov ali načinov kako zmanipulirati ljudi in priti do podatkov je, kot je videti, veliko. Opisani so samo osnovni koncepti, ki pa jih napadalci izvajajo na različne

načine. Gre za neke vrste čarovniške trike, kjer smo ljudje pozorni na eno stran, čarovnik pa nas po drugi strani prevara. V nadaljevanju naloge bom opisal osnovne načine obrambe, ki pa niso stoodstotni. Prevaranti so namreč znani po svoji iznajdljivosti in prilagodljivosti obrambnim mehanizmom.

4 ZAŠČITA PRED SOCIALNIM INŽENIRINGOM

Ultimativne zaščite proti socialnem inženiringu ni. Lahko le zmanjšamo možnosti ali omilimo posledice. In, če je človek najšibkejši člen v sistemu obrambe, saj se ga da zlahka prevarati, si lahko predstavljamo, da je ključni faktor obrambe izobrazba ljudi v smislu zavedanja tovrstnih prevar. V organizacijah tak problem najlažje rešimo z *informativnimi varnostnimi tečaji* (Manske 2000, 58). Zaposlene moramo naučiti postopkov in standardov, kako v takih primerih ukrepati, te pa je priporočljivo obnavljati vsake pol leta. Zavedanje in pozornost je dobro okrepiti z rednim preverjanjem in lastnim preizkušanjem varnosti (Peltier 2006, 20). V organizacijah je potrebno poskrbeti tudi za sistem obveščanja v primeru, da posameznik odkrije prevaro ali poskus prevare (Manske 2000, 58).

Izobrazba ali poznavanje problema je osnovna potrebna zaščita. Z različnimi tipi prevar socialnega inženiringa se tudi obramba razlikuje od primera do primera. Nekatere načine sem pri posameznih tipih že opisal, vseeno pa bom naštel generalne preventivne ukrepe za posamezne tipe.

Pri osebnem pristopu socialnega inženiringa je ključna obramba spremljanje obiskovalcev v organizaciji od vhoda do izhoda organizacije. Prevaranti se pogosto pretvarjajo, da so eni izmed zaposlenih, ter se hitro postavijo v vrsto za vstop takoj za nekom, ki ima kontrolno kartico. Takemu načinu sledenja se po angleško reče »Tailgating«, sam izraz pa bi težko prevedli v slovenski jezik (Brandel 2008). Poleg pravila o nespuščanju neznancev, je potrebna skrb za identifikacijo zaposlenih, če pa se že kdo izmuzne ter mu uspe brez nadzora priti do pisarn, je potrebno poskrbeti, da zaupni podatki niso na vidnih mestih. Sem sodijo poleg zaupnih dokumentov predvsem gesla (Peltier 2006, 19).

Pri telefonskih pogovorih se je potrebno v organizacijah dogovoriti, da se gesel in zaupnih podatkov ne posreduje po telefonu (Peltier 2006 19). Gre namreč za to, da tako osebi, ki se pretvarja za nekoga, kot tudi številki klicočega, ki daje videz internega klica, ni mogoče zagotovo zaupati (Kee 2008, 24).

O zaščiti na internetu sem že marsikaj napisal. Naj izpostavim, da so najpogostejše žrtve prevar ljudje, ki niso prav pogosto na internetu in nimajo takega znanja kot vsakodnevni uporabniki interneta. Na tem mestu velja še priporočilo, naj ne odpiramo elektronske pošte, če ne poznamo pošiljatelja oziroma že po naslovu razberemo, da pošta nima vidne povezave z nami (Kee 2008, 25-26).

Na tem mestu bi izpostavil tudi problematiko z gesli. Opravljene raziskave namreč kažejo, da lahko večino uporabniških gesel razvrstimo v 4 skupine. Te so družina, kamor spadajo imena, vzdevki, ime otroka, partnerja, domače živali ali rojstni datumi. Drugo skupino predstavljajo idoli, kamor se uvrščajo na primer imena atletov, glasbenikov, igralcev, ipd. V tretjo skupino spadajo fantazijska gesla in v zadnjo, četrto skupino skrivnostna ali nejasna gesla, ki so sestavljena iz različnih znakov, številk ali simbolov. Najbolj preseneča to, da skoraj polovica gesel od 1200 anketiranih spada v prvo kategorijo (Medlin et all 2008, 74). Z malo spretnosti se do teh družinskih podatkov prikoplje socialni inženir, preizkusi nekaj kombinacij in že ima naše geslo.

Poleg vseh omenjenih nasvetov, kako se ogniti socialnem inženiringu, ne smemo pozabiti na osnovno zaščito. Svoje imetje, naj si bo fizično ali elektronsko, moramo skrbno varovati. Tako kot moramo pri svojih domovih ali pisarniških prostorih poskrbeti za osnovno varnost (npr. ključavnico, video nadzor, ipd.), tako moramo tudi na internetu poskrbeti za varnost (požarni zid, protivirusni program, posodobljena programska oprema, ipd.).

5 INTERVJU

Da bi dobil še širši in bolj aktualen pogled na prevare, izvedene s socialnim inženiringom, sem se odločil pogovoriti z g. Gorazdom Božičem, vodjo varnostnega centra SI-CERT (Slovenian computer emergency response team).

Na začetku me je predvsem zanimalo, kako bi sam opisal profil žrtve oziroma kdo po njegovem mnenju najpogosteje naseda prevaram socialnega inženiringa. Kot pravi, enotnega profila ne moremo določiti, saj prevaranti ciljajo na različne lastnosti človekove narave. Te so lahko pozitivne ali negativne lastnosti, torej na primer plemenitost in želja pomagati ljudem ali pa pohlep. V Sloveniji, pravi Božič, beležijo v zadnjem letu povečano število prevar socialnega inženiringa na spletnih preprodajalnah, kot npr. na strani bolha.com. Kot trdi, se kar pogosto dogaja, da nas kontaktira kupec, ki bi rad predmet kupil za svojega nečaka v Nigeriji. Obramba po njegovem mnenju predstavlja predvsem pomislek, preden reagiramo na neko sporočilo. Priporoča skeptičnost in zastavljanje vprašanj, kot na primer zakaj nekdo želi denar preko sistema Western Union in ne preko bančnega nakazila ali zakaj ne gre prijatelj, ki so ga okradli v Afriki, raje na ambasado, kot, da piše meni, ipd. Svetuje, da se zadeve prespi, premisli, priporočljivo pa je biti tudi malo skeptičen.

Pred kratkim je nigerijski diplomat izjavil, da bi morali ljudi, ki nasedajo nigerijskim prevaram, kaznovati ravno tako kot same prevarante. Ti namreč mečejo slabo luč na Nigerijo (Moses 2008), poleg tega pa bi se lahko reklo, da prevaranti ne bi imeli kaj delati, če se ljudje ne bi pustili prevarati. Božič se s tako izjavo absolutno ne strinja. Pravi, bi bilo sankcioniranje žrtev, ki so si želele hitrega načina zaslužka, napačno. Še posebej pa je napačno, če bi kaznovali žrtev zato, ker je želela iskreno pomagati nekomu v težavah. S tem bi si, kot pravi, »odžagali že tako rahlo vejo, na kateri sloni naša družba« (Božič 2009).

V primerjavi nevarnosti računalniških virusov ali socialnega inženiringa, bi Božič dal prednost socialnem inženiringu, s katerim lahko dosežemo več. Računalniški virusi so, kot omenja, omejeni in delujejo le na opremi, kjer so nameščeni.

SKLEP

Skoraj vsak se je že srečal s socialnim inženiringom. Še posebej uporabniki spleta, kjer skoraj ni uporabnika, ki še ne bi dobil sporočila z raznimi ponudbami, prošnjami, ipd. Z eno besedo bi rekel, da socialni inženiring sestavlja kombinacijo manipulacije, izkoriščanja človekove narave in predvsem naivnosti, marketinga ter »čarovniških« trikov. Bolj ko prevarant to kombinacijo pozna in obvlada, slabše je za nas. Profila žrtve ravno zaradi različnih prijemov socialnega inženirja, se pravi vplivov na različne lastnosti ljudi, ne moremo določiti. Kot ugotovljeno, socialni inženirji vplivajo na strah, avtoriteto, všečnost, vzajemnost, pohlep, itd. Vse te lastnosti pa so porazdeljene med vse ljudi. Vseeno pa bi lahko rekel, da so, tako kot so pri splošnih prevarah bolj ranljivi starejši ljudje, za spletne prevare bolj dovzetni nevešči uporabniki interneta.

Tu bi bil prav primeren pregovor, ki se glasi »You can always find free cheese in a mousetrap«, prevedeno: »Vedno lahko dobimo zastonj sir v mišelovki«. In če se nam zdijo miši ali ribe neumne, ker vedno znova nasedajo našim vabam, pomislimo, kako smo naivni mi ljudje, ki se imamo za razvito vrsto. Ponudijo nam denar in že grabimo za vabo. Pohlep, pa kot omenjeno, ni edina vaba, na katero se da loviti ljudi.

O preventivi sem veliko napisal, če pa skušam vse na kratko strniti, bi rekel, da je glavna obramba posameznikova previdnost in skeptičnost. K temu pa seveda pripomore osveščenost oziroma zavedanje nevarnosti. Kaj pa nas čaka v prihodnosti? Prevare socialnega inženiringa se bodo po mojem mnenju nadaljevale in še naprej sproti prilagajale razmeram. Dokler bodo ljudje nasedali in dokler bodo prevaranti plenili velike vsote denarja, bo socialni inženiring aktualen. Njihov motiv za nadaljevanje početja je torej velik. Motiv držav in meddržavnih organizacij, za boj proti njim, pa se, ravno zaradi vse večjih izgub denarja, povečuje. Vedno več je izobraževanj in osveščevalnih akcij. In če zaključim z vprašanjem, ki sem ga zastavil g. Božiču, t.j. v čem vidi večjo nevarnost, v računalniških virusih ali socialnemu inženiringu, bi rekel, da se z njegovim odgovorom strinjam. Socialni inženiring je bolj nevaren, vendar se lahko situacija v prihodnosti spremeni. Menim, da bo tudi socialni inženiring, vsaj kar se tiče interneta, nekoč dosegel svoj vrh in nato začel upadati. Zavedati se moramo namreč, da je

internet relativno nov pojav v svetu komunikacij in ga dodobra še nismo spoznali, kaj šele spoznali vse njegove pasti. Ko bo enkrat stopnja poznavanja interneta in socialnega inženiringa na internetu visoka, bo socialni inženiring na internetu upadel. Takrat bodo imeli prednost virusi, kjer človeški faktor nima vloge. Gre za neke vrste cikel socialnega inženiringa, kjer se sedaj po mojem mnenju šele vzpenjamo proti vrhu. Tokratni vrh bo socialni inženiring dosegel na internetu, predhodni je bil osebne narave, kakšen pa bo v prihodnosti bomo pa še videli.

Slovenijo bi na tej lestvici socialnega inženiringa sam uvrstil nižje kot ostale države. Sami še nismo imeli toliko prevar kot jih imajo drugje. V uvodu sem omenil, da smo bili do sedaj neke vrste oaza za socialni inženiring na internetu. K temu je pripomogla naša majhnost. Marsikdo namreč ni nasedel prevari, na primer lažnega prijatelja, ki je prosil za pomoč, ker je bila napisana v angleščini. Marsikomu se je že zaradi samega jezika zdelo sporočilo sumljivo. Na vrhuncu prevar socialnega inženiringa bomo po mojem mnenju takrat, ko bodo sporočila pisana v slovenskem jeziku. Do takrat pa so vse prevare, ki jih srečujemo za nas vaja in priprave na ta čas.

LITERATURA

- Answers.com. 2004. *Phish*. Dostopno prek: http://www.answers.com/topic/phishing (13. avgust 2009).
- Arnes. 2009. *SI-CERT 2009-04: Porast spletnih goljufij*. Dostopno prek: http://www.arnes.si/si-cert/obvestila/2009-04.html (31. avgust 2009).
- Arthur, Charles. 2009. *Facebook hit by phishing attack*. Dostopno prek: http://www.guardian.co.uk/technology/2009/apr/30/facebook-phishing-scam (13. avgust 2009).
- Bakhshi, Taimur, Maria Papadaki in Steven Furnell. 2009. Social engineering: assessing vulnerabilities in practice. *Information management & computer security* 17 (1). Dostopno prek: http://www.emeraldinsight.com/0968-5227.htm (13. avgust 2009).
- Božič, Gorazd. 2009. Intervju z avtorjem. Ljubljana, 4. september.
- Brandel, Mary. 2008. How to spot a spy. *Computerworld*, 14. april. Dostopno prek: http://proquest.umi.com.nukweb.nuk.uni-lj.si/pqdweb?index=39&did=1466277331&SrchMode=1&sid=1&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1246380606&clientId=65784&cfc=1 (3. september 2009).
- Dark Reading. 2006. *Social engineering, the USB way*. Dostopno prek: http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634 (5. september 2009).
- Emarketer.si. 2009. *Loterijske in nagradne prevare*. Dostopno prek: http://emarketer.si/2009/03/loterijske-in-nagradne-prevare/ (31. avgust 2009).
- Enisa. 2008. *Security issues in the context of authentication using mobile devices (Mobile eIP)*. Dostopno prek: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf (6. september 2009).
- Finders, Karl. 2009. How social engineering cracked a FTSE company. *Computer weekly,* 19. maj. Dostopno prek: http://proquest.umi.com.nukweb.nuk.uni-lj.si/pqdweb?index=6&did=1737891131&SrchMode=1&sid=2&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1246376918&clientId=65784 (13. avgust 2009).

- Gartner. 2002. *There are no secrets: Social engineering and privacy.* Dostopno prek: http://www.gartner.com/gc/webletter/security/issue1/index.html (13. avgust 2009).
- --- 2007. *Gartner survey shows phishing attacks escalated in 2007; More than $3 billion lost to these attacks.* Dostopno prek: http://www.gartner.com/it/page.jsp?id=565125 (13. avgust 2009).
- Granger, Sarah. 2001. *Social engineering fundamentals: Part 1 – Hacker tactics*. Dostopno prek: http://www.securityfocus.com/infocus/1527 (13. avgust 2009).
- Heise.de. 2009. *Bericht: Phishing kommt aus der Mode*. Dostopno prek: http://www.heise.de/security/Bericht-Phishing-kommt-aus-der-Mode--/news/meldung/144444 (6. september 2009).
- Jakobsson, Markus in Steven Myers. 2006. ***Phishing and countermeasures: Understanding the increasing problem of electronic identity theft***. New Jersey: John Wiley & Sons. Dostopno prek: Google books.
- Kee, Jared. 2008. *Social engineering: Manipulating the source*. Dostopno prek: http://www.sans.org/reading_room/whitepapers/engineering/social_engineering_manipulating_the_source_32914 (3. september 2009).
- Kovačič, Matej. 2008. *Izdajanje ponarejenih CA certifikatov*. Dostopno prek: http://slo-tech.com/forum/t338308#crta (5. september 2009).
- Leung, Rebecca. 2004. *Kevin Mitnick: Cyberthief*. Dostopno prek: http://www.cbsnews.com/stories/2004/10/20/60II/main650428.shtml (13. avgust 2009).
- Lininger, Rachael in Russel Dean Vines. 2005. ***Phishing: cutting the identity theft line***. Indianapolis: Wiley Publishing. Dostopno prek: Google books.
- Livenews.com.au. 2009. *Phone owners warned of SMS lottery scam*. Dostopno prek: http://livenews.com.au/news/phone-owners-warned-of-sms-lottery-scam-/2009/9/4/218352 (4. september 2009).
- Long, Johnny. 2008. ***No tech hacking: A guide to social engineering, dumpster diving and shoulder surfing***. Burlington: Syngress Publishing. Dostopno prek: Google books.
- Manske, Kurt. 2000. *An introduction to social engineering.* Dostopno prek: http://web.ebscohost.com.nukweb.nuk.uni-lj.si/ehost/pdf?vid=1&hid=102&sid=c025b477-e23d-49b6-a7ac-1300da98865d%40sessionmgr108 (13. avgust 2009).
- Medlin, B., Joseph A. Cazier in Daniel P. Foulk. 2008. Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of Your Employees Would

Share Their Password? *International Journal of Information Security and Privacy* 2 (3): 71-83. Dostopno prek: http://proquest.umi.com.nukweb.nuk.uni-lj.si/pqdweb?did=1531612011&sid=1&Fmt=6&clientId=65784&RQT=309& (13. avgust 2009).

- Microsoft. 2006. *Recognize phishing scams and fraudulent e-mail*. Dostopno prek: http://www.microsoft.com/protect/yourself/phishing/identify.mspx (13. avgust 2009).
- --- 2009. *How to reduce the risk of online fraud*. Dostopno prek: http://www.microsoft.com/protect/fraud/phishing/onlinefraud_us.mspx (13. avgust 2009).
- Miller, Michael. 2008. ***Is it safe? Protecting your computer, your business and yourself online***. Indianapolis: Que Publishing. Dostopno prek: Google books.
- Mitnick, Kevin David in William L. Simon, 2002. *The art of deception*. Indianapolis: Willey Publishing.
- Monitor. 2009. *Nova potegavščina z Google Translate*. Dostopno prek: http://www.monitor.si/novica/nova-potegavscina-z-google-translate/ (13. avgust 2009).
- Moses, Asher. 2008. *Jail the »greedy« scam victims, says Nigerian diplomat*. Dostopno prek: http://www.smh.com.au/news/web/jail-the-greedy-scam-victims-says-nigeria/2008/08/21/1219262473059.html/ (5. september 2009).
- NLB. 2009. *Nlb Klik – Lažne strani*. Dostopno prek: http://www.nlb.si/cgi-bin/nlbweb.exe?doc=16038 (13. avgust 2009).
- Oppliger, Rolf. 2002. ***Internet and intranet security***. Norwood: Artech House. Dostopno prek: Google books.
- Owasp. 2009. *Man-in-the-middle attack.* Dostopno prek: http://www.owasp.org/index.php/Man-in-the-middle_attack (7. september 2009).
- Panda security. *Phishing: Personal data theft*. Dostopno prek: http://www.pandasecurity.com/homeusers/security-info/cybercrime/phishing/ (13. avgust 2009).
- Peltier, Thomas R. 2006. *Social engineering: Concepts and solutions*. Dostopno prek: http://web.ebscohost.com.nukweb.nuk.uni-lj.si/ehost/pdf?vid=1&hid=102&sid=fdbb1681-a9ca-4f13-9a7d-d6794288e314%40sessionmgr108 (1. julij 2009).
- Računalniške novice. 2006. *Ogrožen tudi Klik NLB*. Dostopno prek: http://www.racunalniske-novice.com/novice/programska-oprema/ogrozen-tudi-klik-nlb.html (13. avgust 2009).

- Searchsecurity.com. *Definitions: Social Engineering.* 2006. Dostopno prek: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html (13. avgust 2009).
- Skrt, Radoš. 2004. *Phishing napadi – internetna ribičija*. Dostopno prek: http://www.nasvet.com/phishing/ (13. avgust 2009).
- Smrke, Marjan. 2007. *Družbena mimikrija*. Ljubljana: Fakulteta za družbene vede.
- Sparkasse. *Sicherheit im internet: Online-banking mit indizierter TAN-liste*. Dostopno prek: https://sicherheit.sparkasse-weserbergland.de/anzeigen.php?tpl=privatkunden/konten_karten/sicherheit/details11.html&IFLBSERVERID=IF@@014@@IF&PHPSESSID=5285425b82813df619ae67f55f3238e5 (7. september 2009).
- Tipton, Harold F. in Micki Krause. 2008. ***Information security management handbook***. Boca Raton: Auerbach Publications. Dostopno prek: Google books.
- Trend Micro. *Fake antivirus trojans ramping up*. Dostopno prek: http://blog.trendmicro.com/fake-antivirus-trojans-ramping-up/ (31. avgust 2009).
- USA Mega. *Did you get a letter claiming that you won a big prize?* Dostopno prek: http://www.usamega.com/lottery-scams.asp (31. avgust 2009).
- Velinger, Jan. 2003. *»High Flyer« takes parliament for a ride*. Dostopno prek: http://new.radio.cz/en/article/37771 (13. avgust 2009).
- Vest. 2009. *Bomba na tržnici*. Dostopno prek: http://www.vest.si/2009/03/24/bomba-na-trznici/ (25. avgust 2009).
- Wall, David. 2007. ***Cybercrime: The transformation of crime in the information age***. Cambridge: Polity Press. Dostopno prek: Google books.
- Wang, Wallace. 2006. ***Steal this computer book 4.0: What they tell won't tell you about the internet***. San Francisco: No starch press. Dostopno prek: Google books.
- Weisman, Steve. 2008. ***The truth about avoiding scams***. New Jersey: FT Press. Dostopno prek: Google books.
- Westervelt, Robert. 2009. *Trust eroding as social engineering attacks climb in 2009, says Kaspersky expert.* Dostopno prek: http://usa.kaspersky.com/about-us/media-coverage.php?smnr_id=900000236 (13. avgust 2009).
- Whitman, Michael E. in Herbert J. Mattord,. 2007. ***Principles of information security***. Boston: Cengage Learning EMEA. Dostopno prek: Google books.

- Wiles, Jack. 2007. *Social engineering: Risks, Threats, Vulnerabilities and Countermeasures*. Dostopno prek: http://www.sciencedirect.com.nukweb.nuk.uni-lj.si/science?_ob=MiamiImageURL&_imagekey=B8K5S-4PPX21P-2-1&_cdi=44210&_user=4769578&_check=y&_orig=search&_coverDate=09%2F15%2F2007&view=c&wchp=dGLbVzbzSkWb&md5=b9b5e22fdf087cf1d4a255eb4fe2beb3&ie=/sdarticle.pdf (13. avgust 2009).
- Wismer, Kurt. 2007. *What is man-in-the-middle attack?* Dostopno prek: http://anti-virus-rants.blogspot.com/2007/03/what-is-man-in-middle-attack.html (7. september 2009).
- Workman, Michael. 2007. *Gaining access with social engineering: An empirical study of the threat*. Dostopno prek: http://web.ebscohost.com.nukweb.nuk.uni-lj.si/ehost/pdf?vid=2&hid=102&sid=5428dfc4-4327-44fb-9c02-b8853bfe6441%40sessionmgr108 (13. avgust 2009).
- Zveza potrošnikov Slovenije. 2009. *Socialni inženiring*. Dostopno prek: http://www.zps.si/racunalnik-in-telefon/internet/socialni-inzeniring.html?Itemid=311 (13. avgust 2009).

PRILOGE

Priloga A: Intervju z Gorazdom Božičem

Miloš: Socialni inženiring predstavlja vedno večjo nevarnost spleta. Kako bi opisali profil žrtve socialnega inženiringa?

Gorazd Božič: Enotnega profila sigurno ni, saj tehnike socialnega inženiringa ciljajo na ranljivosti človeške narave in obnašanja, ki so lastne vsem. Ene so pozitivne, denimo plemenitost in pripravljenost pomagati, druge pa negativne, recimo pohlep.

Miloš: Kako pogoste so prevare med slovenskimi uporabniki spleta?

Gorazd Božič: Predvsem v zadnjem letu beležimo veliko prevar na spletu, kjer se uporabljajo tehnike socialnega inženiringa z namenom zvabiti od prodajalca artikel, oz. ga prevarati da kupi nek artikel zelo ugodno. Poskusite lahko dati oglas na bolha.com za kakšen boljši telefon in hitro vas bo kontaktiral "kupec", ki bi rad predmet kupil za svojega nečaka v Nigeriji ...

Miloš: Nekateri so mnenja, da je potrebno te kaznovati te, ki nasedajo prevaram, saj le ti spodbujajo početje prevarantov. Če ljudje ne bi nasedali, tudi prevar ne bi bilo. Kakšno je vaše mnenje o tem?
Gorazd Božič: Zelo sem proti temu. Sankcionirati žrtev prevare ne glede na to, da je želela na hiter način priti do zaslužka, je narobe. Če pa kaznujemo nekoga, ki je postal žrtev prevare zato, ker je iskreno hotel nekomu pomagati, pa si žagamo že tako trhlo vejo, na kateri sloni naša družba.

Miloš: Kako se lahko zaščitimo pred socialnim inženiringom?

Gorazd Božič: S tem, da ne reagiramo takoj, ko prejmemo neko sporočilo. Vprašajmo se, kako nas je "ponudnik" našel, zakaj izbral ravno nas in ali je običajno, da se neke posle opravlja na tak način. Če recimo nekdo želi plačilo preko Western Uniona, se vprašajmo, zakaj ne preko navadnega bančnega računa podjetja. Če nam znanec sporoča, da so ga okradli v Afriki in potrebuje 2000 € za pot domov, se vprašajmo, zakaj ni šel do policijo in ambasado

naše ali kakšne druge EU države. Vprašajmo in zahtevajmo pojasnilo. Nekaj skepse torej ne škodi in če res ni nujno, stvar prespimo.

Miloš: Virusi ali socialni inženiring? Kaj je po vašem mnenju bolj nevarno?

Gorazd Božič: Virusi so omejeni, ker delujejo na opremi, na kateri so nameščeni. S pomočjo socialnega inženiringa pa lahko dosežemo več.

Miloš: Se spomnite kakega »zanimivega« ali pa prebrisanega primera socialnega inženiringa?

Gorazd Božič: Seveda. Zmaga slovenskega "računalniškega prvaka", ki mu je nasedlo tudi Ministrstvo za šolstvo in šport. (Glej recimo http://www.dnevnik.si/novice/kronika/8286).