CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Napredne tehnike socijalnog inženjeringa

NCERT-PUBDOC-2010-02-292

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Postoje mnoge tehnike i ranjivosti koje zlonamjerni korisnici mogu iskoristiti za proboj informacijske sigurnosti neke organizacije. Jednu od njih predstavljaju i ljudske ranjivosti, koje je moguće iskoristiti preko raznih metoda socijalnog inženjeringa. Ove metode iskorištavaju ljudske pogreške ili slabosti kako bi se ostvarila prava pristupa sustavu bez obzira na razinu sigurnosti koju je organizacija uvela. Usredotočenost na ljudske osobine poput povjerenja, želje za pomoći ili nemarnosti osnovna je prednost ovih napada. Također, svaka osoba može postati socijalni inženjer i primijeniti neku od brojnih taktika napada. Socijalni inženjering uključuje razne tehnike, od jednostavne krađe zapisanih lozinki do stvaranja i izvođenja složenih scenarija. Jedna od najraširenijih i najpoznatijih, je izvođenje *phishing* napada. Riječ je o procesu prijevare u kojem se napadač predstavlja kao povjerljiva strana kako bi došao do osjetljivih podataka žrtve. Tijekom povijesti izvedeni su razni napadi socijalnog inženjeringa, a neki od njih su uzrokovali velike gubitke raznim organizacijama.

Ovaj dokument donosi kratki uvod u socijalni inženjering opisujući ciklus napada i socijalne inženjere. Također, dan je i uvid u način prikupljanja informacija te ciljeve ovih napada. Zatim su navedene napredne metode izvođenja napada socijalnog inženjeringa koje su popraćene stvarnim primjerima izvedenim u praksi. Dokument sadrži i statističke podatke o toj vrsti napada, kao i opis najpoznatijih socijalnih inženjera. Na kraju su dani savjeti za zaštitu, kako organizacija, tako i „običnih“ korisnika.

2. Socijalni inženjering

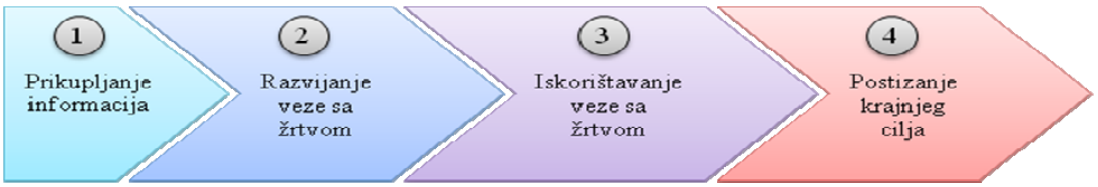
2.1. Osnove socijalnog inženjeringa

Socijalni inženjering je postupak manipulacije osobama kako bi se izvele nedozvoljene akcije ili otkrile povjerljive informacije bez izravnog proboja u sustav. Izraz obično označava prikupljanje informacija, prijevaru ili dobivanje pristupa računalnom sustavu tako da se korisnike nagovori da predaju vjerodostojnice.

Tehnike socijalnog inženjeringa moguće je klasificirati u dvije osnovne kategorije:

1. **Napadi usmjereni na osobe** – jednostavniji i popularniji oblik socijalnog inženjeringa koji se zasniva na međuljudskim vezama i prijevarama uz uporabu zastrašivanja, straha od autoriteta, laskanja i sl. Jedan od primjera ovih napada je lažno predstavljanje prilikom pozivanja službe za pomoć neke organizacije. Pri tome napadač može zatražiti izmjenu lozinke za koju tvrdi kako ju je zaboravio. U slučaju da službenik učini ono što od njega traži napadač te mu proslijedi novu lozinku, napadač ima mogućnost pristupa sustavu s ovlastima onog korisnika za kojeg se lažno predstavljao.
2. **Napadi preko računala/tehnologija** – zasnivaju se na tehnikama prijevare individualnih korisnika za otkrivanje informacija uporabom raznih tehnologija ili iskorištavanjem ranjivosti u sustavu. Moguće je, na primjer, iskoristiti *pop-up* prozore koji nose poruku o prekidu mrežne konekcije te zahtijevaju ponovni unos korisničkog imena i lozinke. Nakon što korisnik unese tražene podatke, oni se šalju napadaču koji je instalirao zlonamjerni program. Naravno, ovakav oblik napada zahtjeva postojanje određene razine pristupa sustavu kako bi napadač uspješno instalirao program.

Napadi socijalnog inženjeringa odvijaju se kroz četiri faze (Slika 1.). U prvoj fazi obavlja se prikupljanje informacija. U ovoj fazi napadač prati informacije o sustavu koje može iskoristiti za povećanje prava pristupa. Prikupljene informacije koristi u drugoj fazi napada kako bi uspostavio vezu sa žrtvom. Ova faza može trajati jako kratko (jednostavan telefonski poziv) ili može zahtijevati dugotrajan posao (stvaranje scenarija). Nakon uspostave veze sa žrtvom, napadač prelazi u treću fazu napada gdje iskorištava tu vezu kako bi dobio željene informacije sa sustava ili izveo neku drugu akciju. Ta faza zapravo otvara put sljedećoj i posljednjoj fazi napada u kojoj napadač postiže konačni cilj napada.



Slika 1. Ciklus napada socijalnog inženjeringa

2.2. Socijalni inženjeri

Socijalni inženjer je bilo koja osoba koja koristi tehnike socijalnog inženjeringa, a neke od kategorija opisane su u nastavku:

- **Hakeri** - često koriste tehnike socijalnog inženjeringa jer je puno jednostavnije iskoristiti ljudske ranjivosti nego ranjivosti na mreži/sustavu. Nakon otkrivanja povjerljivih informacija hakeri iskorištavaju takve podatke za pokretanje stvarnih napada na ciljane sustave.
- **Osobe koje izvode penetracijsko ispitivanje** (eng. *Penetration Testers*) - osobe koje ispituju ranjivosti sustava ili mogućnosti neautoriziranog pristupa sustavu. Pri tome, tehnike socijalnog inženjeringa (najčešće *phishing* napad) koriste kako bi povećali prava pristupa sustavu.
- **Špijuni** - osobe koje koriste razne tehnike (među kojima je i socijalni inženjering) kako bi naveli ljude da vjeruju da su oni netko tko zapravo nisu.
- **Osobe koje žele ukrasti identitet** (eng. *Identity Thieves*) - lopovi koji koriste osobne informacije druge osobe (poput imena, brojeva bankovnih računa, adresa, datuma rođenja i sl.) bez njihovog znanja. Tehnike socijalnog inženjeringa koje koriste sežu od lažnog predstavljanja do *phishing* napada.

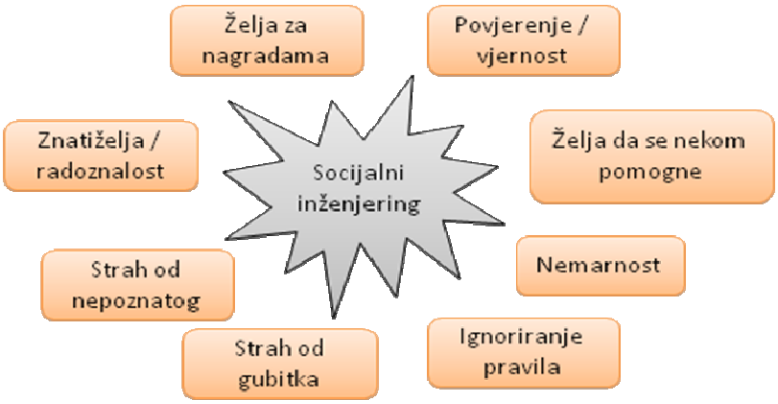
- **Nezadovoljni zaposlenici** - mogu se vrlo lako okrenuti protiv organizacije, a razlozi njihovog nezadovoljstva su razni (poput prenapornog posla, premale plaće i sl.). Takve osobe mogu iskoristiti socijalni inženjering kako bi dobili pristup zabranjenim podacima ili izveli neke nedopuštenje radnje.
- **Informacijski posrednici** (eng. *Information Brokers*) - osobe koje prikupljaju informacije za neku organizaciju (često vladine organizacije) pa obično posjeduju velike količine podataka o nekom poduzeću ili osobi. Postupci prikupljanja podataka često uključuju i socijalni inženjering kako vlasnik ne bi bio svjestan da su podaci došli u posjed nepovjerljive strane.
- **Prodavači** - često se koriste metodama socijalnog inženjeringa kako bi prikupili informacije o potrebama i željama korisnika. Često se usmjeravaju na poduzeća kako bi pristupili poslovnim informacijama i otkrili njihove potrebe i planove.
- **Vladini službenici** - koriste tehnike socijalnog inženjeringa kako bi otkrili mišljenje javnosti o podršci vladinih akcija. Često postoje posebne organizacije koje provode navedene postupke.
- **Obični ljudi** - svakodnevno koriste neke od jednostavnih, osnovnih metoda socijalnog inženjeringa. Iako su takvi postupci često namijenjeni postizanju željenog cilja, najčešće ne dovode do ozbiljnijih posljedica.

2.3. Prikupljanje informacija o žrtvama

Postoje različiti načini prikupljanja informacija o žrtvi, a sežu od korištenja telefona ili upada u organizaciju do uporabe Interneta. Socijalni inženjer može iskoristiti više malih dijelova informacija kako bi dobio koristan podatak. Prema tome, svaka informacija o organizaciji (bez obzira na izvor i važnost) može pomoći u kreiranju ranjivosti i ulaza u sustav za socijalnog inženjera.

Socijalni inženjeri prikupljaju informacije o žrtvama tako da iskorištavaju sljedeće ljudske osobine (Slika 2Slika 2. Prikupljanje informacija u socijalnom inženjeringu):

- povjerenje,
- želju osoba da nekom pomognu,
- želju besplatnog dobivanja stvari,
- znatiželju,
- strah od nepoznatog,
- strah od gubitka,
- nemarnost,
- ignoriranje pravila.



Slika 2. Prikupljanje informacija u socijalnom inženjeringu

Prema načinu prikupljanja informacija napade socijalnog inženjeringa moguće je podijeliti na dvije razine:

1. **Fizički pristup** – napadač se fokusira na fizička obilježja poput radnog mjesta, telefonskog broja ili prekopavanja smeća. Primjer ovih napada je dolazak na radno mjesto žrtve glumeći zaposlenika. Tada napadač može pregledati okolinu ili smeće kako bi otkrio lozinke.
2. **Psihologijski pristup** – napadač se fokusira na praćenje korisnikova ponašanja kako bi otkrio informacije za povećanje ovlasti na sustavu. Primjer je praćenje korisnika pri unosu lozinke za prijavu na osobno računalo.

2.4. Cilj socijalnog inženjeringa

Osnovni cilj socijalnog inženjeringa je povećati prava pristupa sustavu ili informacijama s mogućnošću:

1. izvođenja prijevara – dobivanje vjerodostojnica legitimnih korisnika najčešće se koristi za izvođenje prijevara koje nanose novčanu štetu.
2. upada u mrežu – poznavanje osjetljivih korisničkih podataka (korisničko ime i lozinka) omogućuje prijavu na sustav s jednakim pravima koja su dodijeljena legitimnom korisniku.
3. industrijskog špijuniranja – otkrivanje povjerljivih podataka neke organizacije moguće je iskoristiti za razne svrhe poput ostvarivanja konkurentnosti na tržištu ili prodaje ideja konkurentskim organizacijama.
4. krađe identiteta – dobivanjem korisničkih imena, lozinki ili drugih vjerodostojnica napadač se može predstaviti kao korisnik.
5. jednostavnog narušavanja sustava ili mreže – dobivanje pristupa sustavu omogućuje napadaču nanošenje štete te izvođenje svih akcija koje su dozvoljene korisniku čije je podatke otkrio. To može uključivati brisanje, izmjenu ili pregled datoteka, umetanje lažnih podataka, blokiranje mreže, stvaranje nepotrebnih konekcija i sl.

Tipične žrtve napada su:

- telefonske kompanije,
- tvrtke s uslugama oglašavanja,
- poznate organizacije,
- financijske institucije,
- vojne i vladine agencije,
- bolnice.

3. Napredne tehnike socijalnog inženjeringa

3.1. Phishing napad

Jedna od tehnika socijalnog inženjeringa je *phishing* napad, koji se koristi kako bi se prevarilo korisnike i iskoristilo lošu implementaciju i uporabu tehnologija za sigurnost web stranica. *Phishing* napad, prikazan na Slika 3, je proces prijevare u kojem se pokušava otkriti osjetljive podatke (poput korisničkih imena, lozinki, brojeva kreditnih kartica i sl.) predstavljanjem kao povjerljivi entitet u elektroničkoj komunikaciji. Napadači se obično usmjeravaju na komunikaciju preko popularnih socijalnih mreža te *web* stranica s aukcijama ili *online* naplatom.

Napad se najčešće provodi preko poruka elektroničke pošte ili poruka koje se prenose u stvarnom vremenu (eng. *instant messaging*), a cilj je usmjeriti korisnika na lažnu web stranicu koja izgleda identično kao i originalna, legitimna stranica. Često je vrlo teško uočiti razliku između lažne i originalne stranice čak i kada se koriste napredne tehnike autentikacije korisnika.

Slika 3. Tijek phishing napada

3.1.1. Izvođenje phishing napada

Većina metoda izvođenja *phishing* napada koristi tehnike obmana dizajnirane za umetanje poveznica (koje vode na lažirane web stranice) u poruke elektroničke pošte. Osnovni postupci koji se koriste za preusmjeravanje poveznica na lažirane web stranice spadaju u metode manipulacije poveznicama (eng. *link manipulation*), a mogu se provesti pogrešnim pisanjem URL (eng. *Uniform Resource Locator*) nizova (eng. *misspelled URL*) te uporabom poddomena.

Na primjer, URL niz:

http://www.banka.primjer.com/

korisniku izgleda kao da vodi do dijela „primjer“ na web stranici „banka“. Ipak, zadani niz zapravo vodi do dijela „banka“ na web stranici „primjer“. Još jedan od primjera prikazan je na Slika 4, gdje korisnik ima dojam da se nalazi na dijelu „*access-logins*“ stranice „*twitter*“, iako zapravo pregledava dio „*twitter*“ na stranici „*access-logins*“.

Slika 4. Manipulacija URL nizom
Izvor: helzerman

Još jedan od mogućih pokušaja zavaravanja korisnika je uporaba sidra (eng. *anchor*) za poveznicu koja vodi do lažne stranice.

Na primjer, poveznica:

http://en.wikipedia.org/wiki/Genuine

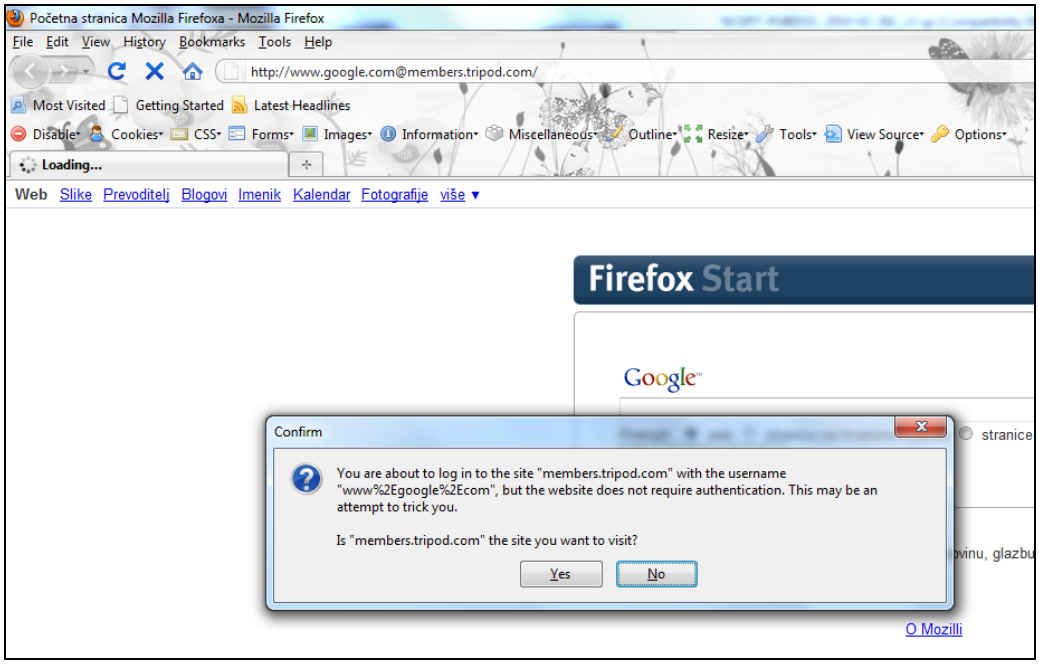
izgleda kao da vodi do članka „*Genuine*“, ali njenim posjećivanjem u pregledniku se zapravo prikazuje članak „*Deception*“.

Postoji još jedna metoda lažiranja poveznica koje sadrže simbol „@“, a originalno su nastale kako bi se omogućio prijenos korisničkog imena i lozinke.

Na primjer, poveznica:

http://www.google.com@members.tripod.com/

korisnika navodi na misao kako posjećuje stranicu „www.google.com“, dok je zapravo preglednik preusmjeren na stranicu „members.tripod.com“ koristeći korisničko ime „www.google.com“. Preglednik Internet Explorer blokira ovakve poveznice, dok preglednici Mozilla Firefox i Opera daju poruku upozorenja (Slika 5) te korisniku prepuštaju odluku o daljnjim radnjama.



Slika 5. Poruka s upozorenjem korisnicima

Daljnji problem s URL nizovima nalaze se kod rukovanja s IDN (eng. *Internationalized Domain Names*) imenima u *web* preglednicima. Njihovim korištenjem omogućuje se da vizualno identična *web* adresa vodi na drugu, moguće zlonamjernu *web* stranicu. Napadači najčešće koriste preusmjeravanje URL nizova na *web* stranicama kojima korisnik vjeruje.

Osim manipulacije URL nizovima, napadači se koriste raznim metodama kako bi zavarali filtre koji otkrivaju *phishing* poruke elektroničke pošte. Primjer je umetanje slikovnih datoteka u tekst kako bi filtri teže detektirali izraze koji se često koriste u takvim porukama.

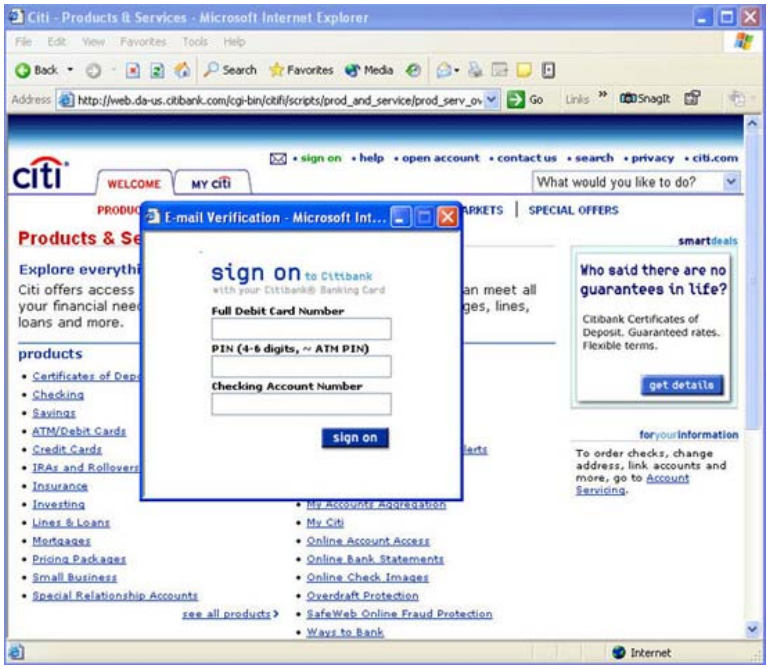
Kada žrtva posjeti lažnu, zlonamjernu web stranicu, napadači moraju zadržati povjerenje korisnika kako se radi o legitimnoj stranici. Zbog toga često koriste JavaScript naredbe kako bi izmijenili zapis u polju za adresu (eng. *address bar*). Neke od mogućnosti uključuju smještanje slike legitimnog URL niza ili zatvaranjem originalnog polja te stvaranje novog s legitimnim URL nizom. Znači, napadač kreira takvu stranicu koja nakon učitavanja u pregledniku prikazuje lažni URL niz kako korisnik ne bi posumnjao u njenu legitimnost.

Napadač, također, može iskoristiti XSS (eng. *cross-site scripting*) ranjivosti kod kojih se korisnika preusmjerava na stranicu sa svim indikatorima sigurnosti (*web* adresa, certifikat) identičnim onima na legitimnoj stranici.

Postoje *phishing* napadi koji ne zahtijevaju stvaranje lažnih *web* stranica. Primjer su poruke koje korisnika upućuju da nazove određeni telefonski broj zbog problema s njegovim računom u banci.

Nakon pozivanja telefonskog broja, od korisnika se zahtjeva unos njihovog računa i PIN broja. Ovakve metode se jednim imenom nazivaj *vishing* (eng. *voice phishing*).

Osim toga, moguće je korisnika uputiti na legitimnu web stranicu te iskoristiti *pop-up* prozore koji zahtijevaju unos korisničkog imena i lozinke. Jedan od takvih primjera napada dan je na Slika 6. Budući da je na povjerljivoj stranici, korisnik vjeruje kako te povjerljive podatke zahtjeva legitimna organizacija (npr. banka).



Slika 6. Phishing napad preko „pop-up" prozora
Izvor: fraudwatchinternational

3.1.2. Primjeri phishing napada

Phishing napadi su vrlo rašireni pa postoje brojni primjeri njihova izvođenja u praksi, a u nastavku su opisani nedavni napadi na poznatije organizacije.

Jedan od čestih ciljeva ovih napada je društvena mreža Facebook. Značajniji napad zabilježen je u svibnju 2009. godine kada je ugroženo 200 milijuna korisnika. Nakon ugrožavanja jednog korisničkog računa, napadači su ga koristili za slanje lažnih poruka i poveznica svim kontaktima što je omogućilo brzo širenje.

U rujnu 2009. godine, izveden je *phishing* napad na korisnike Gmail korisničkih računa. Napadači su stvorili poruku elektroničke pošte koja je izgledala kao da dolazi od Gmail tima. Poruka je korisnika obavještavala o ukidanju njegova računa u roku od 7 dana te mogućnosti da to spriječi posjećivanjem poveznice „*Cancel remove*". Navedena poveznica vodila je do zlonamjernog programa.

Sličan napad dogodio se u listopadu iste godine, kada su hakeri kreirali lažne *web* stranice kako bi došli do vjerodostojnica za prijavu na razne korisniče račune za razmjenu poruka elektroničke pošte. Napad je bio usmjeren na korisnike Gmail, Comcast, Earthlink, Hotmail, Yahoo i AOL računa. Popisi prikupljenih podataka objavljeni su javno, a uključivali su preko 30 tisuća korisničkih imena i lozinki.

Nedavno, početkom veljače 2010., dogodio se *phishing* napad na socijalnu mrežu Twitter. Korisnicima je poslana lažna poruka elektroničke pošte koja je upozoravala na mogući *phishing* napad te navodila korisnike da obnove svoje lozinke.

3.2. Stvaranje scenarija

Stvaranje scenarija (eng. *pretexting*) je postupak kreiranja ili uporabe scenarija (eng. *pretext*) za navođenje žrtve na otkrivanje informacija ili izvođenje neke radnje. Obično se provodi preko telefona, a uključuje prethodno istraživanje te slaganje dijelova informacija za uspostavljanje povjerenja kod žrtve.

Informacije koje se pri tome koriste su datumi rođenja, osobni identifikacijski brojevi i sl. Ova se tehnika često koristi za prijevaru poslodavaca u otkrivanju informacija o kupcima, telefonskih zapisa, bankovnih ispisa i drugih informacija.

Može se također iskoristiti kao priprema za oponašanje djelatnika ili nekih drugih osoba koje imaju neke veze s ciljanom žrtvom. Razlog tome je što stvaranje scenarija ima cilj pripremanja odgovora na pitanja koja može postaviti žrtva.

Osnovni principi napada su:

- više istraživanja donosi veću mogućnost uspjeha,
- ako stvaranje scenarija uključuje aktivnosti ili interese napadača, veća je vjerojatnost uspjeha,
- potrebno je pažljivo planiranje,
- napadač mora uvježbati razgovor sa žrtvom,
- jednostavniji scenarij (s manje koraka i dobro strukturiranim sadržajem) donosi veće šanse za uspjeh,
- scenarij treba izgledati spontano, ali mora biti točan,
- napadač mora upoznati tip osobe s kojom će razgovarati,
- treba paziti na lokalne zakone (kako se ne bi izazvala sumnja kod žrtve ili da žrtva ne bi odbila izvršiti neku radnju),
- scenarij mora uključivati logičan zaključak.

Stvaranje scenarija poznato je kao jedna od najbržih metoda otkrivanja informacija ukoliko se on ispravno kreira. Pri kreiranju scenarija napadač treba voditi računa o sljedećem:

1. koji problem treba riješiti,
2. na koja pitanja treba znati odgovore,
3. koje informacije želi dobiti i
4. s kakvim osobama dolazi u kontakt.

Socijalni inženjer koji koristi ovaj napad mora paziti na naglasak, fraze i izraze koje koristi pa se sam proces stvaranja scenarija često naziva stvaranjem karaktera. Pri tome, scenarij može biti vrlo jednostavan, poput ugodnog razgovora sa žrtvom, ali i jako složen što znači da uključuje uporabu podataka o korisniku (osobnih identifikacijskih podataka i dr.).

Jedan od primjera ovog tipa napada izveo je Mati Aharoni, koji je uvjerio zaposlenika ciljane organizacije da posjeti njegovu web stranicu s časopisima i novinama preko scenarija kako ima vrlo rijetke brojeve časopisa na prodaju. Pri tome je iskoristio informacije o navikama zaposlenika koje je pronašao na Internetu. Lažna web stranica sadržavala je zlonamjerni sadržaj, ali žrtva je napadaču povjerovala.

3.3. Trikovi vezani uz povjerenje

Trikovi vezani uz povjerenje (eng. *confidence trick* ili *confidence game*) su pokušaji prijevare jedne ili više osoba pridobivanjem njenog povjerenja. Napad se temelji na iskorištavanju ljudskih karakteristika poput (ne)iskrenosti, pohlepe i naivnosti, a osnovno je obilježje da žrtva potpuno vjeruje napadaču. Ne postoji općeniti profil za napadače ili žrtve pa teorijski, bilo koja osoba može izvesti napad ili postati žrtva. Cilj je navesti žrtvu kako će dobiti neku nagradu, novac ili drugu vrijednost kako bi bila voljna obaviti traženu radnju.

3.3.1. Metode napada

Postoje brojne metode izvođenja navedenog napada, a poznatije su:

1. shema brzog bogaćenja (eng. *Get-rich-quick scheme*) – uključuje prodaju beskorisnih proizvoda za koje se tvrdi kako sadrže razne funkcionalnosti. Neki od poznatijih postupaka koji spadaju u ovu metodu su:
    a. prijevare kod informiranja preko televizije - lažna svjedočenja „zadovoljnih“ kupaca;
    b. „*wire game*“ – trgovanje znanjem o pobjeđivanju na kladionicama, trgovanju dionicama i sl.
    c. „*salting*“ il „*salt the mine*“ – prijevara u kojoj se naruši ugled tvrtke kako bi se ostvarila kupnja dionica u vrijeme kad je tvrtka bezvrijedna.

   d. prijevara španjolskog zatvorenika – iskorištavanje žrtvine pohlepe prodavanjem informacije o mjestu na kojem je skriven novac ili neko drugo dobro.

2. Prijevare vezane uz romantiku – napadač iskorištava osobe kako bi došao do njihovih novčanih sredstava. U današnje vrijeme većinom se javlja u obliku *web* stranica za stvaranje romantičnih veza preko Interneta. Napadači obično traže neke novčane iznose od žrtve kako bi financirali putovanje i sl.
3. Prijevare *„gold brick"* – pokušaj prodaje proizvoda za puno veću vrijednost od stvarne:
   a. skupljanje novčića – usmjerenost na kolekcionare.
   b. *„pig-in-a-poke"* – skrivanje stvarnog proizvoda njegovim pakiranjem te prodaja za znatno veće novčane iznose.
   c. kupnja za piratske programe – skrivanje nedozvoljenog sadržaja od prijave.
4. Prijevare s lažnim nagradama – navođenje žrtve da vjeruje kako će dobiti nagradu nakon što je slučajno odabrana. Prije preuzimanja nagrade zahtjeva se potpisivanje određenih dokumenata ili uplata određenih novčanih iznosa.
5. *„Online"* prijevare – temeljene na uporabi Internet-a:
   a. Prijevara klikom (eng. *click fraud*) – osoba ili program oponaša legitimnog korisnika posjećivanjem poveznice kako bi se izvela naplata po kliku.
   b. Napadi lažiranjem (eng. *spoofing attacks*) – lažiranje adresa, DNS zapisa i sl. kako bi napadač uvjerio žrtvu da komunicira s povjerljivom stranom.
   c. Prijevare s prethodnim traženjem naknade (eng. *advance-fee fraud*)– žrtva uplaćuje traženu naknadu kako bi ostvarila željenu radnju.
   d. Pucanje domena (eng. *domain slamming*) – prijevara u kojoj jedan ISP (eng. *Internet Service Provider*) navodi korisnika druge tvrtke na uporabu usluga tog ISP-a.
   e. Guranje *web* stranica (eng. *web-cramming*) – nastaje kada kriminalci razviju novu web stranicu za neku grupu ili poslovanje te ju oglašavaju kao besplatnu.

3.3.2. Primjeri napada

Jedan primjer prijevara brzim bogaćenjem izveo je Charles Ponzi koji je 26. prosinca 1919. godine osnovao tvrtku pod nazivom „The Security Exchange Company". Tvrdio je kako može vratiti 150% uloga u 90 dana. Ubrzo su mnogobrojni ulagači željeli uložiti u navedenu tvrtku što je omogućilo prikupljanje oko milijun dolara za tjedan dana. Prikupljeni novac je koristio kako bi isplatio 50% uloga prijašnjih ulagača te privukao nove. Nakon nekoliko krugova uloga i isplata, Ponzi više nije mogao plaćati svojim ulagačima.

Sličan, ali poboljšan postupak primijenio je Bernard Madoff koji je poznat po krađi više milijuna dolara od nekoliko tisuća osoba. On se poslužio taktikom isplate velikih novčanih povrata za male uloge kako bi privukao puno ulagača.

Prijevaru lažnim nagradama izveo je Victor Lustig koji je prodao Eiffelov toranj te uvjerio glumca Al Caponea da uloži 50 000 dolara u njegov nepostojeći projekt. Sličan je potez napravio George Parker koji je htio prodati Brooklyn most.

3.4. Izmamljivanje

Izmamljivanje (eng. *elicitation*) je proces „izvlačenja" informacija iz nečega ili nekoga. Cilj je dobiti informacije koje imaju određeno značenje za povećanje ovlasti pristupa na ciljanom sustavu.

Poznavanje procesa napada može pomoći kod ovog postupka izmamljivanja informacija od žrtve. Jednostavni proces vođenja razgovora, dijeljenja informacija te postavljanja ispravnih pitanja može imati dvojaki utjecaj na žrtve (pozitivan ili negativan). Napadač ima mogućnost prikupljanja informacija koje mu omogućuju dolaženje do specifičnih podataka koje treba.

Ovo ispitivanje je analogno sa skeniranjem priključaka (eng. *port scaning*) ciljanog računala kako bi se otkrili otvoreni priključci. Informacije o priključcima omogućuju napadaču usmjeravanje na područja koja su značajna žrtvi. Sličnost s izmamljivanjem je u tome što žrtva u oba slučaja nije svjesna napada, a napadač dobije informacije koje mu omogućuju danje zlonamjerno djelovanje.

Uspješan napadač mora:

- biti vješt u komunikaciji s ljudima,
- biti adaptivan, tj. komunicirati na način da razgovor odgovara okolini i situaciji,

- razviti vezu sa žrtvom,
- postavljati pitanja koja zahtijevaju jasan odgovor (poput pitanja na koje je moguće odgovoriti sa „da“ ili „ne“),
- upoznati žrtvu i područja njenog rada i zanimanja.

3.5. Oponašanje dostavljača

Jedan od osnovnih napada je oponašanje dostavljača što predstavlja vrlo efektivan i jednostavan napad. Najteži dio je prikupljanje potvrda o ovlasti (eng. *credential*) i isprava kako bi napadač uvjerio zaposlenike da je upravo onaj za kojeg se predstavlja.

Na primjer, osoba se obuče u uniformu neke organizacije te automatski dobije povjerenje zaposlenika drugih organizacije. Problem se posebno ističe kod oponašanja vladinih organizacija jer napadač dobije potpuno povjerenje te može pristupiti vlasništvu ciljane organizacije.

Kako bi uspješno izveo napad, napadač mora:

- saznati tko i kada dostavlja u ciljanu organizaciju;
- nabaviti uniformu dostavljača;
- pripremiti lažne iskaznice i ostale papire;
- odrediti vrijeme napada kako ne bi došlo do susreta sa stvarnim dostavljačem;
- pridobiti povjerenje zaposlenika.

Jednom kada je napadač uspio ući u organizaciju pod krinkom dostavljača, on ima mogućnost pregleda okoline kako bi pronašao osjetljive podatke.

Jedan od primjera napada ovog tipa dogodio se 2007. godine, kada se jedna osoba predstavila kao dostavljač te opljačkala milijunaša Ernest-a Radya u gradu San Diego. Radi se o osnivaču najveće svjetske organizacije za financiranje automobila Westcorp.

Još jedan poznati slučaj dogodio se s ATM karticama kada se jedna osoba lažno predstavila kako bi ukrala kreditne kartice. Napadač je odglumio dostavljača te ukrao pisma s kreditnim karticama oko pedesetak osoba.

3.6. Tehnička podrška

Osoba koja uspije zavarati zaposlenika u tehničkoj podršci neke organizacije može uzrokovati jako velike štete na sustavu i mreži. Napadač može dobiti pristup mrežnim resursima i računalima.

Moguće je ostvariti pristup na tri načina:

1. telefonski poziv – napadač se pretvara kako radi u tehničkoj podršci organizacije te dozna povjerljive informacije stvarnih zaposlenika. Osim toga, može dogovoriti posjet te ostvariti fizički pristup kako bi preuzeo datoteke s računala, instalirao viruse ili druge zlonamjerne programe. Jednom kada je napadač instalirao program na računalu, on može povećati prava pristupa kada god poželi (ovaj se pristup naziva i „*quid pro quo*“).
2. fizički kontakt– dobivanje fizičkog pristupa za napadača predstavlja najpogodniji scenarij. Obično se napadači koriste USB uređajima kako bi prenijeli zlonamjerne programe na ciljana računala.
3. poruke elektroničke pošte – napad se izvodi slično kao *phishing* napad, stvaranjem lažnih poruka elektroničke pošte te navođenjem korisnika da pomisli kako dolaze od povjerljive strane (u ovom slučaju tehničke podrške). Razlika je u tome što napadač zahtjeva izravno slanje korisničkog imena i lozinke.

3.6.1. Primjeri napada

Godine 2004. studenti i osoblje sveučilišta u Kaliforniji primili su lažirane poruke elektroničke pošte. Poruke su nosile privitke sa zlonamjernim programom virusnog podrijetla, a dolazile su od tima za tehničku podršku. Nakon njihova pregleda, zlonamjerni kod bi ugrozio računalo s MyDoom virusom.

Također, zabilježen je jedan pokušaj krađe informacija o korisničkim računima zaposlenika tvrtke Google. Napad je izveden slanjem poruka koje su izgledale kao da dolaze od Gmail tima za podršku. Od korisnika su tražile da odgovore s vjerodostojnicama za prijavu kako bi spriječili ukidanje ili brisanje korisničkog računa.

Još jedna od prijevara koja je uključivala tehničku podršku izvedena je na štetu tvrtke Microsoft. Napadači su iskoristili telefonske pozive kako bi obavijestili korisnike da im je računalo ugroženo zlonamjernim virusom. Kako bi otklonili problem, korisnike se navodilo na preuzimanje programa koji je zapravo bio virus. Instaliranje virusa napadaču je omogućivalo udaljeno spajanje na korisničko računalo kako bi „ispravili problem". Jednom instaliran program ostao bi na računalu i nakon kraja poziva što je napadaču omogućilo proizvoljno pristupanje računalu. Drugi grupa napadača izvela je sličan napad, nazivajući korisnike operacijskog sustava Microsoft Windows te navodeći kako je njihova inačica operacijskog sustava ilegalna. Napadači su zahtijevali da korisnici plate korištenje sustava ili će biti prijavljeni policiji.

3.7. Uporaba alata za socijalni inženjering

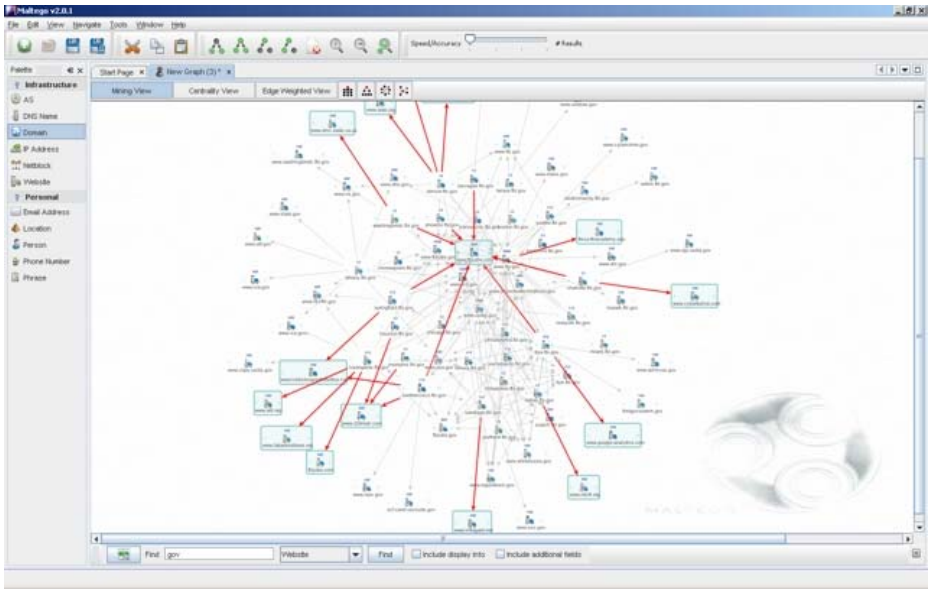
3.7.1. Maltego

Maltego je aplikacija otvorenog koda za forenzičke radnje koja pruža sučelje za prikupljanje informacija za prikaz u jednostavno razumljivom obliku. Zahvaljujući grafičkim bibliotekama, aplikacija omogućuje identificiranje ključnih veza između informacija i identificiranje nepoznatih veza među njima.

Može identificirati veze među:

- osobama,
- grupama osoba,
- organizacijama,
- *web* stranicama,
- Internet infrastrukturom (poput domena, DNS imena, IP adresa i sl),
- izrazima,
- dokumentima i datotekama.

Aplikaciju je jednostavno instalirati, a dostupna je za operacijske sustave Microsoft Windows, Mac i Linux. Sučelje opisanog alata prikazano je na Slika 7.



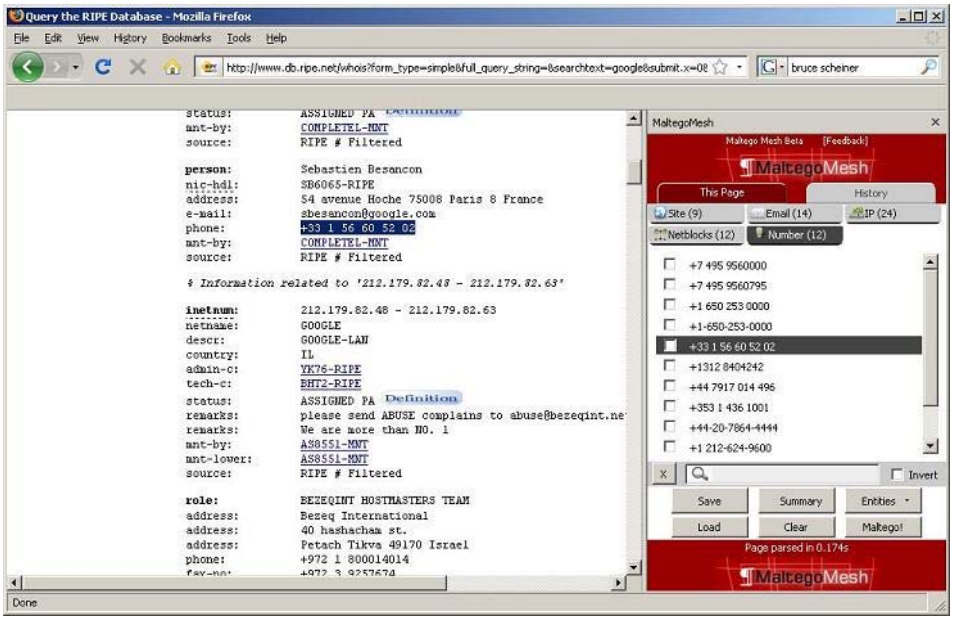
Slika 7. Alat Maltego
Izvor: Paterva

3.7.2. Maltego Mesh

Maltego Mesh (Slika 8) je dodatak za preglednik Firefox koji pomaže analizirati i pronaći korisne informacije unutar stranica. Rad temelji na pronalaženju teksta koji odgovaraju određenim regularnim izrazima.

Pretražuje:

- IP adrese,
- adrese elektroničke pošte,
- telefonske brojeve,
- web stranice,
- datume.



Slika 8. Alat Maltego Mesh
Izvor: social-engineer

Dobra obilježja programa:

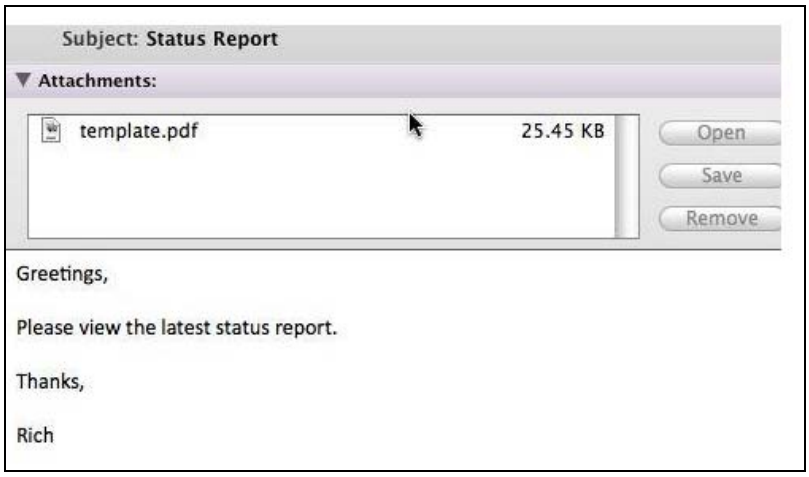
- uporaba je besplatna,
- omogućuje brzo pretraživanje velikih stranica,
- postojanje opcija za pretraživanje,
- mogućnost dodavanja vlastitih izraza za pretraživanje.

3.7.3. Social Engineer Toolkit

Social Engineering Toolkit je alat koji se fokusira na napadanje ljudskog elementa sigurnosti informacijskih sustava. Osnovna svrha je simuliranje napada socijalnog inženjeringa i omogućavanje ispitivanja uspješnosti istih. Cilj je osvijestiti korisnike o često zaboravljenim rizicima koje donosi socijalni inženjering.

Provode se dvije metode napada:

1. postavljanje zlonamjernih web stranica – stvara se lažna web stranica sa zlonamjernim java *applet*-om. Nakon posjete web stranice, žrtvi se prikazuje prozor za pokretanje programa koji najčešće ima potpis tvrtke Microsoft te je imenovan kao nadogradnja.
2. slanje *phishing* poruka elektroničke pošte – pri uporabi poruka elektroničke pošte moguće je odabrati opcije slanja poruka na jednu adresu ili na odabranu grupu korisnika. Također, postoji i mogućnost lažiranja adrese pošiljatelja. Primjer slanja opisanih poruka dan je na Slika 9.



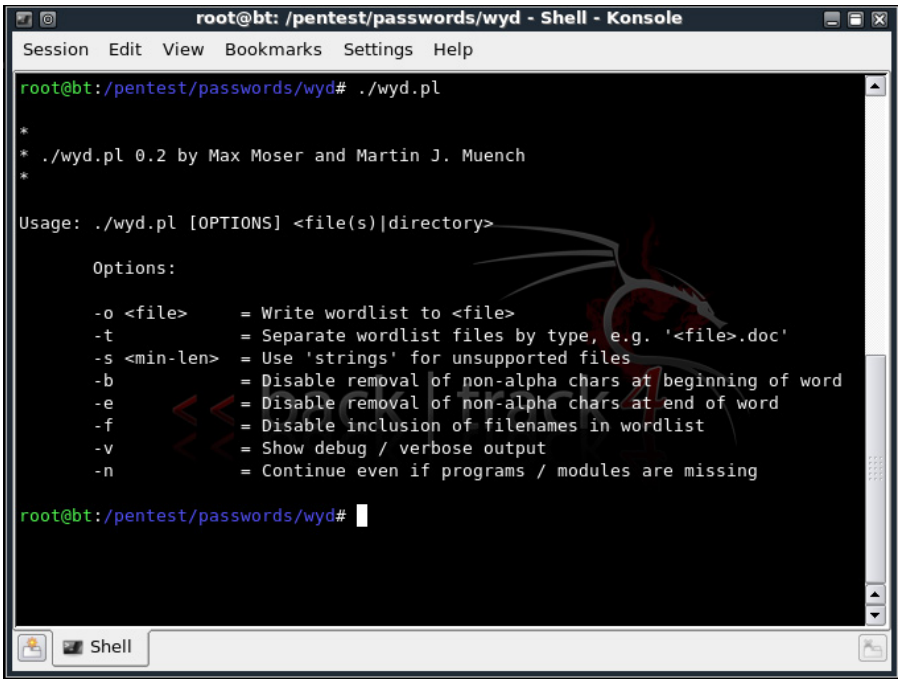
Slika 9. Uporaba alata Social-Engineering Toolkit
Izvor: social-engineer

3.7.4. Alati CUPP i WYD

Postoje dva vrlo korisna alata koja se mogu koristiti za penetracijsko ispitivanje ili forenzičku analizu, a to su:

1. CUPP (eng. *Common User Passwords Profiler*) – omogućuje prikupljanje riječi koje se mogu iskoristiti za pogađanje lozinki, napade rječnikom ili „*brute force*" napade.
2. WYD (eng. *Who's your daddy*) – omogućuje određivanje riječi mogućih lozinki prema profilu osobe ili sustava. Sučelje alata prikazuje Slika 10.

Radi se o besplatnim, relativno novim alatima sa slabo razvijenim opcijama i sučeljima.



Slika 10. Alat WYD
Izvor: social-engineer

3.7.5. Alati za lažiranje identiteta pozivatelja

Osnovna zamisao kod lažiranja ID-a pozivatelja je izmjena informacija o ID-u koje se prikazuju na zaslonu. Ovakva metoda se može iskoristiti za lažnu autorizaciju i preuzimanje identiteta osoba.

Kod socijalnog inženjeringa napadači mogu prikazati žrtvi da poziv dolazi iz udaljenog ureda, dijela organizacije, partnerske organizacije, dostavljačke organizacije, nadležnih uprava i sl.

Jedan od načina lažiranja ID-a pozivatelja je uporaba *SpoofCard* kartica koje omogućuju proizvoljni izbor ID-a. Prednosti uporabe ovih kartica su jednostavnost, nema potrebe za dodatnim sklopovljem ili programima te efikasnost. Ipak, ovakve tehnologije obično su vrlo skupe što ih u konačnici čini poprilično nepraktičnima.

Osim uporabe specijaliziranih kartica, postoji i programsko rješenje za lažiranje ID-a pozivatelja pod nazivom „Asterisk". Riječ je o besplatnom programu koji implementira PBX (eng. *private branch exchange*) telefonsku razmjenu, a dostupan je za operacijske sustave Linux, NetBSD, OpenBSD, FreeBSD, Mac OS X, Solaris te Microsoft Windows (AsteriskWin32).

Osnovna obilježja spomenutog programa su:

- glasovna pošta – centralizirani sustav za upravljanje telefonskim porukama za veliku grupu korisnika,
- konferencijski pozivi – pozivi u kojima sudjeluje više od 2 osobe, a svaka može proizvoljno pristupiti i napustiti poziv bez prekidanja sjednice,
- IVR (eng. *Interactive Voice Response*) – tehnologija koja omogućuje računalima da detektiraju glasovne signale, kao i da ih unose preko tipkovnice,
- ACD (eng. *Automatic Call Distributor*) – distribucija poziva na posebnu grupu terminala.

4. Statistika

4.1. Svjetski poznati socijalni inženjeri

4.1.1. Kevin David Mitnick

Jedan od najpoznatijih socijalnih inženjera je Kevin David Mitnick (Slika 11), konzultant za računalnu sigurnost koji je optužen za razne zločine povezane s računarstvom. Prvi zabilježeni napad socijalnog inženjeringa izveo je već s dvanaest godina kada je zaobišao naplatni sustav u autobusu u gradu Los Angeles. Nakon toga, tehnike socijalnog inženjeringa postale su njegova osnovna metoda u prikupljanju informacija (uključujući korisnička imena, lozinke, brojeve modema i sl.). U srednjoj školi upoznao se s metodom manipulacije telefonima koju je koristio za izbjegavanje skupe naplate razgovora na velikim udaljenostima. Također, počeo je upotrebljavati amaterski radio za dobivanje neautoriziranog pristupa sustavu u restoranima brze hrane.

Slika 11 Kevin David Mitnick
Izvor: s9

Godine 1979. uspio je prvi put neautorizirano pristupiti računalnoj mreži kada mu je prijatelj otkrio lozinku za Ark, računalni DEC (eng. Digital Equipment Corporation) sustav. Nakon proboja u računalnu mrežu, Mitnick je napravio kopije DEC programa, zbog čega je osuđen na godinu dana zatvora te tri godine uvjetne kazne.

Pri kraju njegovog uvjetnog služenja kazne, provalio je u Pacific Bell računala za govorne poruke elektroničke pošte. Za taj prekršaj osuđen je na dvije i pol godine zatvora.

Mitnick je uspio dobiti prava pristupa tisućama računalnih mreža, a koristio je mobilne telefone kako bi skrio svoju lokaciju. Također, napravio je kopije programa koji su u vlasništvu velikih telefonskih i računalnih organizacija.

Osim opisanih prekršaja, izveo je sljedeće napade:

- dobivanje administrativnog pristupa IBM računalu udruge „*Computer Learning Center*“,
- hakiranje Motorola, NEC, Mokia, Sun Microsystems i Fujitsu Siemens sustava,
- pregled poruka elektorničke pošte sigurnosnih službenika u organizacijama MCI Communications i Digital Wiretapped,
- hakiranje SCO, PacBell, FBI, Pentagon, Novell, CA DMV, USC i Los Angeles Unified School District sustava.

Organizacija FBI uhitila je Mitnicka u veljači 1995. godine, a četiri godine kasnije osuđen je za četiri prijevare, dvije računalne prijevare te niz ilegalnih prijevara preko telefona. Proveo je pet godina u zatvoru te je na slobodu pušten 2000. godine. Tijekom zatvorske i uvjetne kazne imao je zabranu uporabe bilo kakve komunikacijske tehnologije, a oduzet mu je i profit od filmova i knjiga temeljenih na njegovim kriminalnim radnjama. Danas, Mitnick vodi konzultantsku organizaciju za sigurnost računala pod nazivom „Mitnick Security Consulting LLC“.

4.1.2. Ramy, Muzher i Shadde Badir

Tri brata, Ramy, Muzher i Shadde Badir (Slika 12), jedni su od najpoznatijih socijalnih inženjera. Osim što su sva trojica slijepi od rođenja, zajedničko im je zanimanje za računala. Postali su popularni nakon izvođenja telefonskih i računalnih prijevara u Izraelu 90-ih godina prošlog stoljeća uporabom socijalnog inženjeringa, metoda oponašanja govora i posebnih računala. Njihov cilj je bio dokazati kako su sposobni misliti i djelovati poput svakog čovjeka.

Slika 12 Braća Badir
Izvor: Wired

Optuženi su za 44 prijevare koje uključuju:

- telekomunikacijske prijevare,
- krađu računalnih podataka,
- proboj u izraelski vojni telefonski sustav,
- krađu brojeva kreditnih kartica,
- oponašanje policijskih službenika.

Jedan od najozbiljnijih napada bio je proboj u izraelski telefonski sustav kako bi postavili lažnu telefonsku kompaniju. Time su od korisnika naplaćivali velike novčane iznose za lažne telefonske pozive na velike udaljenosti, a prijevarom su zaradili oko dva milijuna dolara.

Braća Badir koristila su mnoge tehnike socijalnog inženjeringa poput sposobnosti oponašanja osoba i izmamljivanja informacija. Godine 1999. osuđeni su za svoje zločine s tim da je samo Ramy (koji je bio i vođa svih prijevara) dobio zatvorsku kaznu, dok su ostala braća osuđena samo uvjetno.

4.1.3. Drugi poznati socijalni inženjeri

Steven Jay Russell je američki socijalni inženjer koji se koristio trikovima zasnovanim na povjerenju i oponašanju, a poznat je po brojnim bježanjima iz zatvora. Također, poznat je po nadimcima „Houdini" i „King Con". U svojim ranim danima, Russell je uvjerio voditelje nekoliko velikih tvrtki za proizvodnju prehrambenih proizvoda kako ima potrebne kvalifikacije za upravljanje istim tvrtkama. Često je koristio vještine oponašanja sudaca, liječnika i policijskih službenika. Godine 1994. pobjegao je iz zatvora noseći civilnu odjeću, nakon čega se zaposlio kao financijski upravitelj organizacije „North American Medical Management" gdje je pronevjerio velike iznose novca. Ponovno je pritvoren te je 1996. godine iskoristio vještine oponašanja suca kako bi smanjio vlastitu jamčevinu. Nakon plaćanja jamčevine, pušten je iz zatvora, ali i ponovno uhićen nakon samo 10 dana. Sljedeći pokušaj bijega izveo je bojanjem svoje uniforme u zelenu boju kakvu posjeduje medicinsko osoblje. Uhićen je 1998. godine nakon krađe 800 tisuća dolara iz organizacije koja upravlja financiranjem doktora. Nakon ponovnog uhićenja isplanirao je novi bijeg pretvarajući se kako boluje od HIV virusa. Koristio se lažnim liječničkim nalazima kako bi dobio premještaj u bolnicu, gdje je, glumeći doktora, dojavio zatvorskom liječniku kako je Russell umro. U ožujku 1998. godine predstavio se kao milijunaš iz Virginije te zatražio kredit u iznosu od 75 000 dolara u banci u gradu Dallas. Službenici su ga prijavili policiji, a Russell je nakon uhićenja odglumio srčani udar te je premješten u bolnicu pod stalnim nadzorom. Tada je odglumio FBI službenika te naredio osoblju koje ga nadzire da odstupe sa dužnosti kako bi otišao iz bolnice. Konačno je uhićen u travnju iste godine kada je dobio kaznu od 144 godine zatvora.

Frank William Abagnale, Jr. je američki sigurnosni konzultant poznat po izvođenju raznih prijevara uporabom socijalnog inženjeringa poput trikova temeljenih na povjerenju, falsificiranja, vještina oponašanja i izbjegavanja uhićenja. Postao je poznat u 60-im godinama prošlog stoljeća kada je izdao lažne čekove u vrijednosti od 2.5 milijuna dolara kroz 26 država tijekom četiri godine. Pri tome se koristio s osam lažnih identiteta oponašajući pilota, doktora, inspektora u zatvoru i odvjetnika. Također, uspio je dva puta pobjeći iz policijskog pritvora. Trenutno je zaposlen kao konzultant i predavač za organizaciju „Federal Bureau of Investigation" te vodi kompaniju za savjetovanje protiv financijskih prijevara pod nazivom „Abagnale & Associates".

David Buchwald, nekada poznat kao Bill From RNOC bio je haker i vođa grupe LOD (eng. Legion of Doom). Koristio se tehnikama socijalnog inženjeringa sa sposobnostima manipulacije zaposlenicima telefonskih kompanija diljem SAD-a. Također, koristio se hakerskim sposobnostima kako bi povećao prava pristupa telefonskim linijama Bell i AT&T sustava. Time je dobio mogućnost upravljanja komunikacijama diljem države. Trenutno radi kao filmski montažer i fotograf u gradu New York.

David „Race" Bannon je pseudonim za Davida Waynea Dilleya, američkog prevaranta koji se predstavljao kao bivši agent organizacije Interpol. Izdao je knjigu (Race Against Evil: The Secret Missions of the Interpol Agent Who Tracked the World's Most Sinister Criminals) u kojoj opisuje svoj rad kao tajni agent. Organizacija Interpol negirala je bilo kakvu povezanost s Dilleyem koji je uhićen u siječnju 2006. godine, a u travnju je priznao krivnju za optužbe.

Peter Clarence Foster je australski poduzetnik koji je poznat po izvođenju socijalnih napada preko trikova povezanih s povjerenjem. Predstavljao se kao pomoćnik žene američkog premijera Cherie Blair te navodio kako bi kupio posjede u gradu Bristol. Osuđen je za provođenje radnji koje su smanjile vrijednost posjeda. Trenutno radi kao filmski producent.

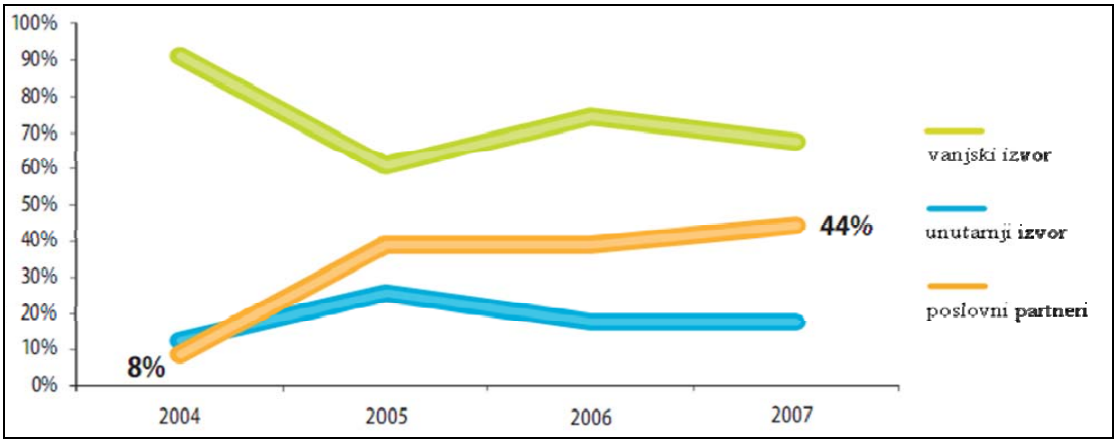
Stanley Mark Rifkin je socijalni inženjer koji je počinio prijevare u SAD-u u obliku krađe oko 10.2 milijuna dolara preko sustava za telefonske transakcije. Radeći za organizaciju koja je razvijala sustav za stvaranje sigurnosnih kopija za banku „Security Pacific National Bank", Rifkin je upoznao postupak prijenosa novca. Otkrio je kako agenti stalno zapisuju kodove za dnevne prijenose te je jedan dan zapamtio takav kod. Koristeći tehnike socijalnog inženjeringa, preko telefonskih poziva, prebacio je 10.2 milijuna dolara na vlastiti račun u švicarsku banku. Ukradenim novcem kupio je dijamante vrijedne 8.1 milijuna dolara koje je namjeravao prodati u SAD-u, ali organizacija FBI je otkrila njegove namjere.

4.2. Statistički podaci

Prema izvješću sigurnosnog tima organizacije Verzion o gubicima podataka vidljivo je kako najviše prijetnji dolazi iz vanjskih izvora (73 %) te od poslovnih partnera (39 %). Najveći broj gubitka podataka posljedica je pogrešaka (62 %), ali također veliki dio dolazi od hakiranja i proboja u sustav (59 %). Ostali podaci dani su na Slika 13, a ukazuju na značaj prijetnji koje donosi socijalni inženjering. Vidljivo je da najveći broj gubitaka podataka uzrokuju vanjski izvori te osobe od povjerenja (što čini glavne grupe u koje spadaju socijalni inženjeri).

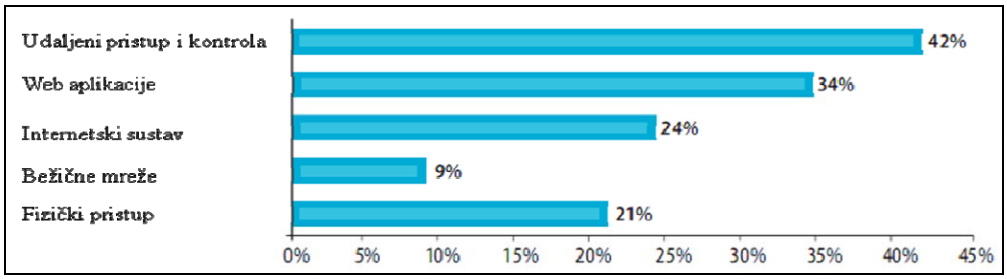
Slika 13 Izvori i vrste uzroka gubitka podataka
Izvor: Verizon

Ukoliko se pogleda postotak napada koji dolaze iz vanjskih i unutarnjih izvora te partnera prikazan na Slika 14, vidljivo je kako rizik koji donose osobe od povjerenja konstantno raste. Godine 2004. napadi koji su dolazili iz takvih izvora činili su 8 % ukupnog broja napada što je do 2007. godine poraslo na čak 44 %.



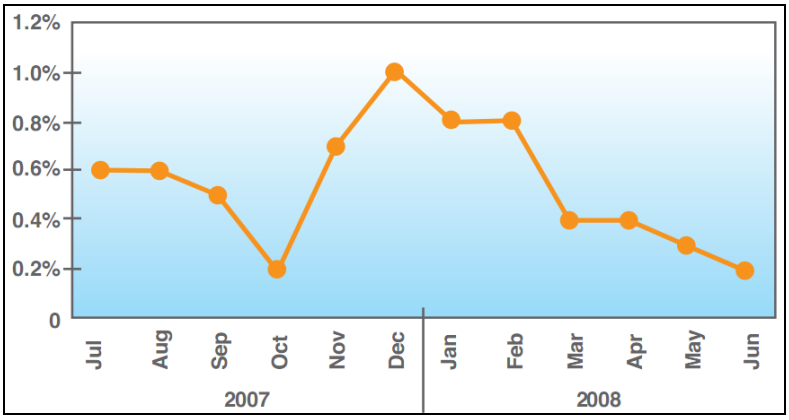
Slika 14 Promjena udjela izvora gubitaka podataka
Izvor: Verizon

Analiza načina proboja u sustav pokazuje kako najveći broj upada dolazi preko stjecanja udaljenog pristupa i kontrole što predstavlja jedan od glavnih ciljeva socijalnog inženjeringa. Postotak takvih napada, kojima prethodi stjecanje prava pristupa, je oko 42 % ukupnog broja napada. Ostali podaci prikazani su na Slika 15.



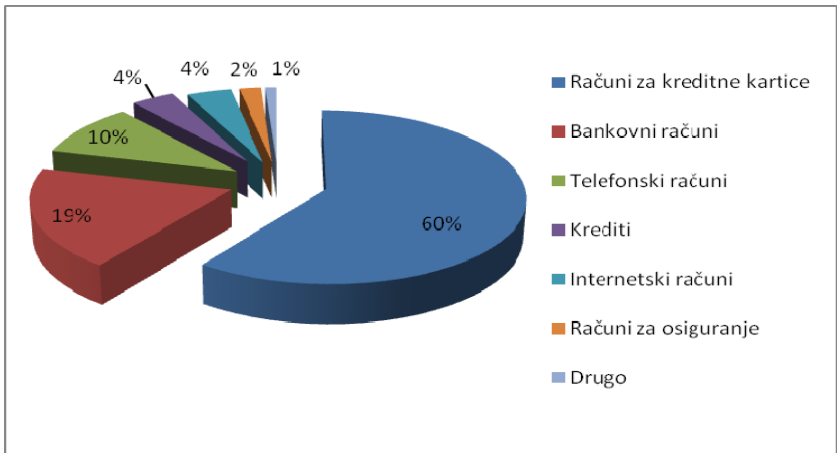
Slika 15 Način upada napadača
Izvor: Verizon

Organizacija X-Force izdala je vlastito izvješće o sigurnosnim prijetnjama na prijelazu iz 2007. u 2008. godinu. Slika 16. predstavlja udio *phishing* poruka elektroničke pošte, kao jednog od osnovnih metoda napada socijalnog inženjeringa u ukupnom broju lažnih poruka elektroničke pošte. Vidljivo je kako je udio takvih poruka znatan, što dovodi do zaključka da *phishing* napad nosi velike rizike sigurnosti računalnim sustavima. Također, može se primijetiti kako se broj *phishing* poruka povećava pri kraju godine jer napadači pokušavaju iskoristiti blagdane kako bi izveli napad.



Slika 16 Udio phishing napada u neželjenim porukama elektoničke pošte
Izvor: X-Force

Ukradene informacije napadači najčešće koriste za oponašanje legitimnih korisnika i lažno predstavljanje. Prema izvješću organizacije HIPAA, čak u 20 % slučajeva napadač koristi podatke za stvaranje lažnih korisničkih računa u ime žrtve. Lažne korisničke račune najčešće koriste kod prijevara s kreditnim karticama (60 %) te lažnim bankovnim računima (19 %) kako je prikazano na Slika 17.



Slika 17 Uporaba ukradenih podataka
Izvor: FraudWatch International

5. Metode zaštite

5.1. Zaštita organizacije

5.1.1. Sigurnosna politika i standardi

Dobro dokumentirana i pristupačna sigurnosna politika i standardi ključ su dobre sigurnosne strategije neke organizacije. Politika treba jasno definirati svoj opseg i sadržaj za svako područje na koje se odnosi. Zajedno sa svakom politikom potrebno je specificirati standarde koje treba uvesti kako bi se provele odredbe politike.

Neki od uobičajenih dijelova sigurnosne politike u borbi protiv socijalnog inženjeringa su:

- uporaba računalnog sustava – upravljanje korištenjem sustava, uporabom sklopovlja i programa koji nisu u vlasništvu organizacije i sl.,
- klasifikacija i rukovanje informacijama – osigurati pravilnu klasifikaciju povjerljivih informacija kako bi one bile zaštićene od neovlaštenog pristupa,
- osobna sigurnost – provjera novih zaposlenika kako bi se osiguralo da ne predstavljaju sigurnosnu prijetnju,
- fizička sigurnost – osigurati objekte znakovima, nadglednim i sigurnosnim uređajima i sl.,
- pristup informacijama – procesi za generiranje sigurnih lozinki, udaljeni pristup i sl.,
- zaštita od virusa – provesti mjere zaštite sustava od virusa i drugih zlonamjernih prijetnji,
- treninzi za podizanje svijesti zaposlenika o informacijskoj sigurnosti – informirati zaposlenike o prijetnjama i mjerama,
- upravljanje sukladnošću – osiguravanje sukladnosti sa zakonima i standardima,
- politika o lozinkama – definiranje standarda za osiguravanje lozinki,
- reagiranje na incident – definiranje postupka reakcije i prijave incidenta,
- distribuiranje dokumentacije – rukovanje s povjerljivim podacima.

Jednom definirana politika mora biti lako dostupna svim zaposlenicima. Također, potrebno je provoditi stalno ažuriranje i provjeravanje sigurnosne politike kako bi se načinile nužne promjene u skladu s novim odredbama ili prijetnjama.

5.1.2. Edukacija zaposlenika i osoblja

Kako bi sigurnosna politika bila efikasna potrebno je provesti postupke edukacije. Neke organizacije zahtijevaju da se svi zaposlenici upoznaju sa sigurnosnom politikom svake godine. Stvaranje svijesti o prijetnjama, ponašanju koje napadači iskorištavaju te metodologijama čini važan dio strategije zaštite od istih prijetnji. Najbolji način za postizanje toga je predstavljanjem stvarnih primjera hakiranja organizacija putem metoda socijalnog inženjeringa.

Postoje mnogi alati koji se mogu iskoristiti pri edukaciji poput video zapisa, brošura, znakova (natpisa na radnom mjestu, zaslonu računala, podsjetnika i dr.) i slično. Programi edukacije imaju ulogu:

- upoznavanja zaposlenika sa sigurnosnom politikom,
- stvaranje svijesti o rizicima i mogućim gubicima,
- treniranja s ciljem prepoznavanja tehnika socijalnog inženjeringa.

Znači, nije dovoljno zaposlenicima ukazati što i kako, činiti nego ih je potrebno upoznati s posljedicama koje donose prijetnje socijalnog inženjeringa.

Budući da educiranje zaposlenika o rizicima socijalnog inženjeringa predstavlja jednu od osnovnih metoda zaštite, to je vrlo zahtjevan zadatak. Dobar program poduke mora biti raznolik što znači da je potrebno iskoristiti svaku mogućnost i alat kako bi se postiglo povećanje svijesti i razumijevanje prijetnja koje donose socijalni inženjeri.

5.1.3. Drugi postupci zaštite

Jedan od ključnih postupaka zaštite od socijalnog inženjeringa je pravilno upravljanje lozinkama. Organizacija mora imati jedinstveni identifikator za svakog zaposlenika koji će biti povezana s pravima pristupa tog zaposlenika. Znači, identifikatorom se zaposleniku određuju prava pristupa informacijama na sustavu. U tome se vidi prednost korištenja posebnog identifikatora za svakog zaposlenika. U slučaju da napadač sazna identifikator nekog korisnika, on ima pravo pristupa samo onim informacijama koje su dodijeljene tom korisniku dok su ostali dijelovi sustava zaštićeni.

Definiranje operativnih postupaka također ima važnu ulogu u zaštiti organizacije od napada socijalnih inženjera. Pri tome se prvenstveno misli na procedure povezane s odobravanjem pristupa i izdavanjem dozvola. Takvi postupci zahtijevaju višestruku provjeru točnosti i vjerodostojnosti podataka. Osnovna svrha je smanjiti rizike napada oponašanjem zaposlenika.

5.2. Zaštita običnih korisnika

Svaki korisnik Interneta može provesti određene mjere zaštite od napada socijalnim inženjeringom poput:

- upoznavanja s vrijednostima podataka – napadači se obično usmjeravaju na korisnička imena i lozinke te brojeve kreditnih kartica pa je potrebno posebno oprezno rukovanje s tim podacima,
- provjeravanja identiteta sugovornika – socijalni inženjeri obično se usmjeravaju na stjecanje povjerenja korisnika uvjeravajući ih kako se radi o njima poznatim osobama, suradnicima, nadležnim osobama, vladinim službenicima i sl.
- zadržavanja lozinki tajnim – lozinke treba čuvati u tajnosti te izbjegavati njihovo zapisivanje ili dijeljenje s drugim osobama,
- provjeravanja poruka elektroničke pošte – provjeriti izvor poruke, provesti skeniranje antivirusnim alatom i sl.,
- izbjegavanja upisivanja vjerodostojnica u nesigurne stranice – provjeriti valjanost web stranica prije upisa lozinke preko URL niza i drugih indikatora sigurnosti,
- ne otkrivanja puno informacija o sebi – saznavanjem informacija o nekom korisniku socijalni inženjer se može fokusirati na njegove navike i hobije kako bi ga naveo na posjećivanje lažnih *web* stranica,
- korištenja *anti-phishing* zaštite – postoje alati koji provjeravaju poruke elektroničke pošte kako bi otkrili izraze koji su karakteristični za *phishing* poruke.

6. Zaključak

Napadi socijalnim inženjeringom već su desetljećima prisutni u probijanju sigurnosti računalnih i telekomunikacijskih sustava. Tijekom tog vremena razvijene su razne metode kojima je moguće zaobići definirane sigurnosne mjere iskorištavanjem ljudskih ranjivosti. Njihova uspješnost temelji se upravo na usmjerenosti na onaj faktor sigurnosti koji je često zaboravljen ili zapostavljen, a to su ljudi. Budući da korisnici često nisu svjesni rizika koje uzrokuju svojom nepažnjom, nemarom ili povjerenjem, oni lako podliježu napadima socijalnog inženjeringa. Osim toga, socijalni inženjeri mogu izvoditi napade na računalne sustave bez ikakvog ili s vrlo malo znanja o vještinama hakiranja. Ipak, uspješno izveden napad može napadaču pružiti informacije za nanošenje velikih gubitaka (npr. financijskih) nekoj organizaciji ili krađu identiteta nekog korisnika.

Metode socijalnog inženjeringa se brzo razvijaju i koriste na sve sofisticiranije načine što dovodi do potrebe za uvođenjem sigurnosnih politika o rukovanju informacijama, lozinkama, računalima i dr. Međutim, osnovni princip zaštite uključuje i programe edukacije o rizicima te mogućim posljedicama uspješno izvedenog napada socijalnog inženjeringa. Svaki korisnik Interneta treba provesti mjere vlastite zaštite od napada socijalnog inženjeringa.

7. Reference

[1] Socijalni inženjering, http://en.wikipedia.org/wiki/Social_engineering_%28security%29, veljača, 2010.

[2] Socijalni inženjering, http://www.social-engineer.org/, veljača, 2010.

[3] Phishing, http://en.wikipedia.org/wiki/Phishing, veljača, 2010.

[4] Phishing Gmail, http://www.social-engineer.org/wiki/archives/Phishing/Phishing-Gmail.html, rujan, 2009.

[5] Webmail phising, http://www.theregister.co.uk/2009/10/06/gmail_webmail_phish/, listopad, 2009.

[6] Facebook phishing, http://www.reuters.com/article/idUSTRE54D6BN20090514, svibanj, 2009.

[7] Twitter phising, http://status.twitter.com/post/367671822/reason-4132-for-changing-your-password, veljača, 2010.

[8] Stvaranje scenarija, http://www.pretexting.net/, veljača, 2010.

[9] Confidence trick, http://en.wikipedia.org/wiki/Confidence_trick, veljača, 2010.

[10] Popis confidence trick metoda, http://en.wikipedia.org/wiki/List_of_confidence_tricks, veljača, 2010.

[11] SET, http://www.social-engineer.org/newsletter/SocialEngineerNewsletterV01I01.html, veljača, 2010.

[12] Kevin David Mitnick, http://en.wikipedia.org/wiki/Kevin_Mitnick, veljača, 2010.

[13] Braća Badir, http://www.wired.com/wired/archive/12.02/phreaks_pr.html, veljača, 2010.

[14] 2008 DATA BREACH INVESTIGATIONS REPORT, Verizon business, http://www.verizonbusiness.com/resources/security/databreachreport.pdf, 2008.

[15] The Threat of Social Engineering and Your Defense Against It, SANS Institute, http://www.sans.org/reading_room/whitepapers/engineering/the_threat_of_social_engineering_and_your_defense_against_it_1232, veljača, 2010.