HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Socijalni inženjering putem VoIP tehnologije

CCERT-PUBDOC-2008-03-221

CARNet CERT u suradnji s LS&S

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

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

CARNet 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 4

2. ŠTO JE VISHING? 5

2.1. VRIJEDNI PODACI 6

3. VEKTORI NAPADA 7

3.1. AUTOMATSKO PRIKUPLJANJE PODATAKA 7
3.2. PRIMJERI NAPADA 7
3.2.1. Slanje poruka elektroničke pošte 7
3.2.2. Slanje SMS poruka 9
3.2.3. Glasovna pošta 9
3.2.4. Telefonski poziv 10
3.3. NAPADI U BUDUĆNOSTI 10

4. ISKUSTVA S VISHING NAPADIMA 11

5. ZAKLJUČAK 12

6. REFERENCE 12

1. Uvod

U moderno doba napadači sve češće koriste socijalni inženjering. Ovaj pojam označava skup tehnika namijenjenih iskorištavanju ranjivosti sustava. On se od ostalih tehnika iste namjene razlikuje upravo po meti napada odnosno vrsti ranjivosti koje iskorištava. Dok se svi ostali pristupi bave zlouporabom tehničkih i tehnoloških nedostataka, ovaj se pristup temelji na iskorištavanju značajki ljudskog ponašanja.

Jedna od najčešće korištenih metoda socijalnog inženjeringa, čija je prijetnja preplavila Internet i njegove korisnike, je *phishing*. Ova metoda općenito podrazumijeva navođenje korisnika na određenu, napadaču korisnu radnju, predočenjem lažne obavijesti, svojevrsnog mamca. Obično se ovaj napad poistovjećuje s uporabom poruka elektroničke pošte i navođenjem korisnika na posjetu posebno oblikovanih lažnih web stranica. Kada korisnik posjeti web stranicu od njega se traži unos određenih povjerljivih podataka. Podaci mogu biti brojevi kreditnih kartica, PIN brojevi, zaporke itd.

Osim *phishinga*, još je jedna popularna metoda socijalnog inženjeringa, a to je *vishing*. *Vishing* je tehnika zlouporabe VoIP (eng. *Voice over Internet Protocol*) tehnologije korištenjem principa *phishing* tehnike napada.

Osim tehnika *phishinga* i *vishinga*, socijalni inženjering uključuje još i:

- *pharming* – manipulaciju DNS (eng. *Domain Name Server*) zapisima,
- *spear phishing* – metode ciljanih napada i
- *smishing* – zlouporaba SMS servisa na mobitelima.

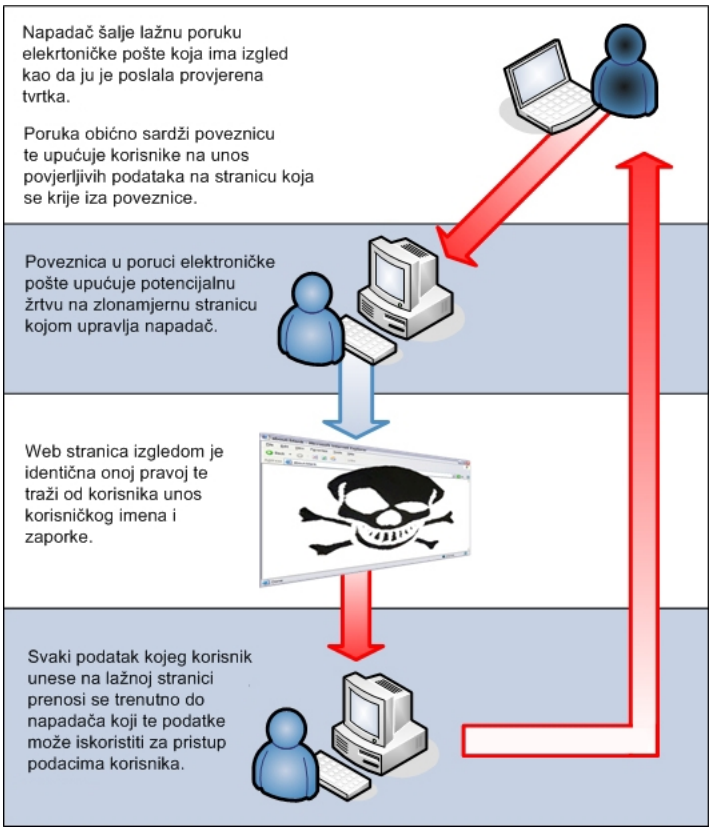
Ovaj dokument opisuje *vishing* metodu napada, u njoj korištene vektore napada te posljedice eventualno uspješne zlouporabe. Osim toga dokument nudi kratak pregled dosadašnjih iskustava u obrani od *vishing* napada.

2. Što je *vishing*?

Vishing je jedna od metoda socijalnog inženjeringa koja se temelji na zlouporabi VoIP tehnologije. Ona omogućuje prijenos glasovnih poruka putem Interneta. Tvrtke koje pružaju VoIP servise obično se nazivaju pružatelji usluga (eng. *providers*), a protokoli koji se koriste za prijenos zvučnog signala preko IP mreže se nazivaju VoIP (eng. *Voice over IP*) protokolima. Upotrebom računalne mreže ostvaruje se prijenos zvuka (glasa) i podataka. Troškovi pružanja telefonskih usluga su znatno smanjeni u odnosu na zemljanu telefonsku liniju te su telefonski pozivi s jednog VoIP telefona na drugi katkad besplatni. VoIP protokoli prenose telefonski signal kao komprimirani digitalni zvučni zapis enkapsuliran u tok podataka koji se prenosi putem IP protokola. Sljedeća slika prikazuje strukturu VoIP načina komuniciranja:

Slika 1. VoIP komunikacija

Napadač koristi socijalni inženjering putem VoIP tehnologije kako bi naveo korisnike na odavanje osobnih, financijskih ili nekih drugih povjerljivih podataka uz obećanje novčane ili neke druge nagrade. Pojam *vishing* je kovanica nastala kombinacijom pojmova *voice* i *phishing*.
Upotreba telefona kao sredstva za navođenje korisnika na odavanje povjerljivih informacija poznata je još od vremena kad je dizajniran prvi telefonski uređaj. Međutim, telefonske uređaje povezane zemnom linijom moguće je točno locirati do određenog korisnika, dok je mnogo teže otkriti lokaciju korisnika telefonskog uređaja koji koristi VoIP tehnologiju. Povećana je upotreba IP tehnologije za povezivanje telefonskih uređaja na telefonske servise. Činjenica da telefonski uređaj može biti bilo koje računalo pruža mnogo mogućnosti za zlouporabu te u mnogo slučajeva nije moguće odrediti točnu lokaciju napadača. Troškovi telefonskih poziva su se s vremenom smanjili toliko da su postali zanemarivi te to dodatno pogoduje ne samo korisnicima telefonskih usluga, već i napadačima.
Današnji uvjeti uporabe telefonskih servisa postali su financijski povoljni za *phishing* napade putem VoIP tehnologije. Sljedeća slika prikazuje metodu *phishing* napada u njenom uobičajenom obliku:



Slika 2. Prikaz *phishing* napada

Napadači mogu postići veći uspjeh *vishing* metodama napada nego uporabom bilo koje druge metode socijalnog inženjeringa, a situacija je takva jer:

- su telefonski sustavi temeljeni na Internet protokolima su manje pouzdani od zemnih telefonskih sustava,
- mnogo više ljudi posjeduje i koristi telefonski uređaj nego elektroničku poštu,
- neke dobne skupine lakše je kontaktirati putem telefona nego Interneta i jer
- telefon omogućuje veću personalizaciju poruka kreiranih metodama socijalnog inženjeringa.

2.1. Vrijedni podaci za napadača

Iako postoji mnogo metoda izvođenja *vishing* napada, važno je primjetiti do kojih podataka napadač najlakše može doći. Neki od tih podataka su:

- podaci o kreditnim karticama (kao i podaci o isteku valjanosti kartice te podaci o sigurnosnim kodovima),
- brojevi računa te korisnički osobni identifikacijski brojevi (PIN),
- datumi rođendana i
- brojevi putovnica.

Neki od najprofitabilnijih načina uporabe pobrojanih podataka su:

- kontrola bankovnih računa,
- kupovina luksuzne robe i usluga,
- krađa identiteta,
- prijave za pozajmice i kreditne kartice,
- prikrivanje kriminalnih aktivnosti, kao što je pranje novca,
- dobivanje putovnice i
- primanje vladinih povlastica.

3. Vektori napada

IP telefonija otvara mnoga vrata zlonamjernim osobama, ali najčešći napadi koji uključuju IP telefoniju su *phishing* napadi jer ih je moguće izvesti kombiniranjem socijalnih i tehnoloških metoda zlouporabe. Aspekti koji su privlačni napadačima su:

- mogućnost obavljanja poziva bilo kojem telefonskom broju sa bilo koje lokacije na svijetu,
- niska cijena poziva,
- mogućnost lažnog predstavljanja,
- automatizirani pozivi, kao što je *war-dialing* metoda uporabe modemskih uređaja za automatsko pretraživanje popisa telefonskih brojeva,
- kompleksnost filtriranja glasovnih poruka u smislu odbacivanja zabranjenih riječi ili fraza i
- pristup *bot* agentima (*zombie* računala postavljena za prosljeđivanje neželjene elektroničke pošte (eng. *spam*)).

3.1. Automatsko prikupljanje podataka

Napadači često koriste automatizirane sustave za *vishing* prijevare u svrhu prikupljanja korisničkih podataka. Vrste automatizirane tehnologije dostupne napadačima uključuju slijedeće:

- Automatsko prepoznavanje tonskog biranja – kada žrtva unese svoje podatke preko telefonskog uređaja, tonovi svake tipke se konvertiraju i pohranjuju u obliku brojeva.
- Automatsko prepoznavanje glasa – tehnologije su razvijene i moguće ih je nabaviti po povoljnoj cijeni.

Spomenute metode napadaču omogućuju prikupljanje različitih numeričkih podataka kao i drugih osobnih detalja (npr. adrese i imena) .

3.2. Primjeri napada

Napadač može koristiti različita sredstva za pokretanje *vishing* napada, od kojih je svako specifično za određeni objekt napada. Primarne metode dostavljanja i navođenja korisnika na otvaranje posebno oblikovanih poruka su:

- slanje poruka elektroničke pošte,
- slanje SMS poruka,
- upotreba glasovne pošte i
- upućivanje telefonskih poziva.

Potrebno je napomenuti da usluge telefaksa još nisu dostupne u VoIP okružju. Ipak, u bliskoj se budućnosti očekuje i njihova integracija, što će dovesti i do integracije u metode napada. Tada će napadači zasigurno osmisliti i metode izvođenja *phishing* napada upotrebom faksnih uređaja.

3.2.1. Slanje poruka elektroničke pošte

U nekim scenarijima napada, žrtve prime poruku elektroničke pošte koja ih poziva, nagovara ili mami na nazivanje podmetnutog telefonskog broja. Sadržaj poruka elektroničke pošte je gotovo jednak kao kod *phishing* napada, gdje se žrtvu poziva da slijedi poveznicu (eng. URL – *Uniform Resource Locator*) koja vodi do zlonamjerno oblikovane lažne web stranice. Korisnici koji su slijedili URL najvjerojatnije će upisati svoje podatke u obrazac, kao što su brojevi kreditnih kartica te PIN brojevi, te ih će ostaviti napadaču na korištenje.

U slučaju kada se korisnike navodi na zvanje podmetnutog telefonskog broja, automatska snimka propituje pozivatelja o autentikacijskim podacima.

Na primjer, potencijalna žrtva može primiti slijedeću poruku elektroničke pošte:

```
Poštovani korisniče,

Primijetili smo da je došlo do pojave tri uzastopna neuspješna
pokušaja prilikom pristupa vašem bankovnom računu u banci Free
Market Bank & Trust.

Kako bi vaš račun bio siguran te vaši privatni podaci bili
zaštićeni, banka Free Market Bank & Trust je zaključala vaš račun.
Obvezni smo osigurati vaše transakcije putem Interneta.

Molimo vas da nazovete broj 060-xxx-xxxx kako biste potvrdili vaš
račun i identitet.

Srdačan pozdrav,
Free Market Bank & Trust
Korisnička služba
```

U poruci se korisnika obavještava o trostrukom neuspješnom pristupu bankovnom računu te ga se poziva na zvanje određenog telefonskog broja kako bi potvrdio svoje podatke. Kada žrtva lažne elektroničke poruke nazove telefonski broj, javi se automatska snimka koja izgovara tekst sličan ovome:

```
Hvala što ste nazvali banku Free Market Bank i Trust. Vaš nam je
posao važan. Kako bismo vam pomogli da kontaktirate pravog
predstavnika te vam odgovorili na sva pitanja, pritisnite
prikladni broj na telefonskom uređaju.
```

Dakle, snimljena poruka navodi korisnika da odgovara na pitanja pritiskom određenih tipki na telefonskom uređaju. Poruka zvuči autentično i žrtva nije u mogućnosti naslutiti da se radi o prijevari. Zatim se korisniku nudi izbor:

- Pritisnite 1 ukoliko trebate provjeriti podatke za pristup bankovnom računu te stanje na računu.
- Pritisnite 2 ukoliko želite prenijeti novčana sredstva.
- Pritisnite 3 ukoliko želite otključati vaš Internet profil.
- Pritisnite 0 za neki drugi upit.

Bez obzira na to koju tipku korisnik pritisne, automatizirani sustav ga traži autentikaciju te mu kaže nešto slično sljedećem:

```
Sigurnost svakog korisnika nam je važna. Za daljnji nastavak
trebate autenticirati vaš identitet. Molim utipkajte broj
bankovnog računa.
```

Pozivatelj zatim upiše broj svog bankovnog računa. Nakon upisa slijedi upit:

```
Hvala. Sada molim unesite vaš broj jedinstveni matični broj.
```

Pozivatelj posluša automatsku poruku i upiše svoj JMBG. Interakcija s korisnikom se nastavlja te automatska snimka traži upis PIN broja:

```
Hvala. Sada unesite vaš PIN broj.
```

Nakon upisa PIN broja pozivatelj odsluša posljednju poruku:

```
Hvala. Sada ćemo vas spojiti s prikladnim predstavnikom.
```

U ovom trenutku telefonski poziv se prekida i žrtva misli da je nešto pošlo po krivu sa uslugom. Alternativno umjesto prekida veze žrtva se preusmjerava na stvarnu korisničku uslugu i pozivatelj nije ni svjestan da je svoje autentikacijske podatke ostavio napadaču.

3.2.2. Slanje SMS poruka

Inicijalni vektori napada usko su vezani uz metode slanja elektroničke pošte. Napadač može iskoristiti protokole mobilnih mreža, kao što su SMS ili MMS, za prosljeđivanje lažnih poruka koje pozivaju, navode ili mame korisnike da odgovore na primljenu poruku slanjem tekstualnih ili multimedijalnih poruka.
Na primjer, potencijalna žrtva primi SMS poruku sljedećeg sadržaja:

```
Automatska obavijest o novootvorenom kreditu! Uspostavljena je
nova vrsta kredita za vas u dućanu XXX [obično je napisan neki
poznati dućan]. Ukoliko smatrate da je ovakva primjena kredita
neovlaštena, nazovite 060-xxx-xxxx.
```

Također, potencijalna žrtva može zaprimiti SMS poruku koja izgleda kao da ju je poslao pružatelj mobilnih usluga. Takva poruka sadrži tekst koji potiče korisnika da na nju odgovori porukom s osobnim podacima. Jedan primjer takve poruke je ovaj:

```
Prekoračili ste mjesečni broj poruka koji smijete poslati. Od sada
će vam se tekstualne poruke naplaćivati po tarifi 50 lipa po
poruci. Ukoliko odgovorite na ovu poruku s vašim autorizacijskim
kodom moći ćete slati dodatnih 500 poruka za 2 kune.
```

Dakle, korisniku se u lažnoj poruci obećava mogućnost slanja dodatnih tekstualnih poruka ukoliko pošalje svoj autorizacijski kod.
Upotrebom multimedijalnih poruka, napadač može korisniku poslati slikovnu ili animiranu poruku s prikladnim logom tvrtke, kako bi ga dodatno potaknuo korisnika na suradnju.

3.2.3. Glasovna pošta

Upotrebom različitih metoda, napadač može brzo doći do popisa telefonskih brojeva i odrediti koji su brojevi još uvijek aktivni. Neke od metoda preuzimanja popisa telefonskih brojeva su *war-dialing* te zlouporaba SIP (eng. *Session Initiation Protocol*) protokola. *War-dialing* je metoda napada kod koje se koristi modemski uređaj za automatsko skeniranje popisa telefonskih brojeva, gdje se svaki telefonski broj naziva s lokalnim pozivnim brojem u svrhu pronalaska nepoznatih računala. SIP je protokol aplikacijske razine za stvaranje, izmjenu, i prekid sjednica u kojima sudjeluje jedan ili više korisnika. Moguće ga je iskoristiti za kreiranje višekorisničkih sjednica koje uključuju Internetske telefonske pozive te multimedijske konferencije.
Jednom kada napadač pobroji sve aktivne telefonske brojeve, može na lak način snimiti prikladnu poruku na svaki telefon s aktiviranom glasovnom poštom. Sustavi glasovne pošte su meta napada zbog lakoće izvođenja napada.
Poruke ostavljene na glasovnoj pošti obično su takve da potiču korisnika na akciju čim odslušaju poruku. Na primjer, potencijalna žrtva primi sljedeću poruku:

```
Pozdrav, ovdje Ana iz HEP-a. Trebam vas hitno kontaktirati glede
promjene vašeg prebivališta. Potrebno je potvrditi zatvaranje
vašeg računa i prestanak primanja usluge na vašem prethodnom
prebivalištu. Dostava električne energije bit će prekinuta sutra u
21:00. Molim vas da nazovete korisničku službu na broj 060-xxx-
xxxx, radi dogovora o plaćanju konačnog računa.
```

Kako potencijalna žrtva uopće nema namjeru promijeniti trenutno prebivalište i nikako ne želi da joj se isključi struja, nazvat će dani broj te će obaviti autentikaciju najvjerojatnije koristeći broj kreditne kartice i PIN broj.

Vektorom napada "ostavljanje snimljene poruke" napadačeva meta je repozitorij glasovne pošte te ostavljanje poruke potencijalnoj žrtvi. Poruka traži hitnu intervenciju korisnika te nazivanje ostavljenog telefonskog broja. Kada korisnik nazove broj, poziv se naplaćuje korisniku i novac od naplate ide napadaču. Upotrebom vektora napada "zlonamjerna poruka" napadač također ciljano ostavlja posebno oblikovanu poruku na korisnikovoj glasovnoj pošti. Tehnologija za primanje poruka glasovne pošte razlikuje se ovisno o uređaju koji će žrtva koristiti za preslušavanje snimljenih poruka. Napadač može iskoristiti tu razliku u tehnologijama za podmetanje posebno oblikovanih poruka. Kada se korisnik poveže na svoju glasovnu poštu i preuzme poruke kako bi ih preslušao, napadač može preuzeti kontrolu nad uređajem za preslušavanje te obavljati operacije za koje inače nema ovlasti.

3.2.4. Telefonski poziv

Mogućnost preuzimanja identiteta različitih korisnika telefonskih usluga je jedan od važnih aspekata za napadača kod izvođenja napada putem VoIP tehnologije. Promjenom identifikacijskog broja (eng. *caller ID*) pozivatelja napadač može korisniku telefonske usluge podmetnuti priču koja je vjerodostojna te na taj način otežati postupak pronalaženja izvora napada. Napadač, također može, kako bi poboljšao vjerojatnost uspješnosti napada, iskoristiti IP telefonske usluge koje koriste lokalni pozivni broj, tzv. *point of presence* (POP) izlazni broj (npr. telefonski broj unutar istog županijskog pozivnog broja).

Zbog mogućnosti koje pruža krađa identiteta, kao i zbog mogućnosti uspostavljanja poziva putem Interneta s bilo koje lokacije na svijetu, napadač može izvesti tzv. "napad u živo". Kod takvog napada napadač upućuje poziv potencijalnoj žrtvi koja na svojoj strani čuje glas generiran automatskim glasovnim sustavom. Taj glasovni sustav potiče korisnika na odavanje osobnih podataka. Kako bi napad polučio uspjeh, napadač oponaša dobro poznati entitet (npr. banku ili lanac robnih kuća, lokalnu radio stanicu, vladin ured, itd.) i koristi pripadan identifikacijski broj pozivatelja.

Troškovi poziva putem Interneta postaju s vremenom sve manji te postoji mogućnost da organizirani kriminalci izgrade svoj sustav telefonskih centara i provedu žrtvu kroz *vishing* lanac. To dakle znači da više neće postojati potreba za podmetanjem snimljenih poruka. Upotrebom ovog vektora napada postižu se najbolji rezultati.

Kod "napada u živo", napadač može kombinirati bilo koji aspekt socijalnog inženjeringa, ali napad će biti uspješniji ukoliko napadač koristi lokalni pristup koji je dobro vremenski isplaniran te sadrži interaktivne poruke. Slijede primjeri takvog pristupa:

- Plaćena anketa – nakon odgovaranja na anketna pitanja korisnika traži se unos detalja bankovnog računa tako da se novac odmah može prebaciti s žrtvinog računa.
- Porezno upozorenje – žrtvu se upozorava da, kao stanovnik određene države, može imati koristi od nedavne promjene poreza. Sve što treba učiniti jest navesti ime, prezime, adresu, broj socijalnog osiguranja.

3.3. Napadi u budućnosti

U budućnosti će se sigurno povećati raspon vektora napada u smislu kreiranja sofisticiranijih ciljanih napada. Sljedeće metode ulaze u obzir:

- Kopanje po smeću – napadač redovito prebire po smeću lokalnih prodavača te pronalazi račune i poništene transakcije. U računima se nalazi riznica informacija, kao što su imena vlasnika kreditnih kartica, potpuni ili djelomični brojevi kreditnih kartica, datumi transakcija, kupljeni proizvodi, troškovi, itd. Sve se nabrojane informacije mogu iskoristiti na jednostavan način prilikom izvođenja personaliziranog *vishing* napada.
- Validacija vlasnika kreditne kartice – potrošače se često pita za validaciju njihovog identiteta kod kupovine robe visoke vrijednosti. Blagajnik obično naziva broj određene banke kako bi dobio autorizacijski broj transakcije. No prvo banka treba razgovarati s korisnikom kreditne kartice kako bi se ustanovilo da je korisnik upravo onaj za kojeg se predstavlja da jest, vlasnik bankovnog računa. Organiziranim napadačima ne bi bio problem ubaciti ili oponašati opisani proces validacije, pogotovo u suradnji s blagajnikom. Imali bi mogućnost prikupiti dodatne osobne informacije o svojim žrtvama, kao što su datumi rođenja, brojevi socijalnog osiguranja, itd.

- Ucjena – napadač može uvjeriti korisnika telefonske usluge da instalira obnovljenu inačicu programskog paketa na telefonske uređaje. Nakon što korisnik instalira program, telefon se zaključava te može primati ili zvati isključivo brojeve koje je napadač postavio. Kako bi žrtva otključala telefon, mora nazvati točno određeni telefonski broj.
- Iskorištavanje podatkovnih paketa – napadač podmeće pakete koji uzrokuju automatsko biranje predbroja za sve telefonske brojeve koji koriste ISDN (eng. *Integrated Services Digital Network*). Napadač može automatski presresti, snimiti ili prepisati sadržaj telefonskih poziva žrtve te automatski identificirati povjerljive informacije.

4. Iskustva s *vishing* napadima

Prema izvještajima agencije *Javelin Strategy and Research* iz veljače 2008. godine, broj prijevara u Sjedinjenim Američkim Državama koje uključuju krađu identiteta se smanjuje, ali se zato znatno povećava broj prijevara putem telefona i elektroničke pošte. Utvrđeno je da su mladi ljudi podložniji *vishing* napadima te da je vjerojatnije da će upasti u zamke napadača. Stariji ljudi koji postanu žrtvama prijevara reagiraju prestankom plaćanja računa i slanja čekova putem nesigurnih poštanskih sandučića elektroničke pošte.

Padu broja prijevara mogu pridonijeti različiti faktori, a neki od njih su razvijena svijest, poboljšanje sustava i navika tvrtki koje upravljaju osobnim podacima, učestale provjere podataka osobnih računa te redovita obnova instaliranih programskih paketa, poput antivirusnih programa. Osim toga, očekuje se povećana, kako od korisnika usluga, tako i od tvrtki, odgovornost kod prihvaćanja Internet bankarstva i plaćanja računa putem takvih usluga.

Kako se povećala svijest korisnika o pojavama *vishing* prijevara, povećala se i upotreba sigurnih Internetskih prostora. Zbog toga napadači postaju sve kreativniji u upotrebi kako tradicionalnih, tako i bežičnih telefonskih usluga, u smislu izvođenja prijevara. Prevelik je broj potrošača koji ostavljaju svoje osobne i financijske podatke nepoznatim pozivateljima. Informacije kao što su matični brojevi, brojevi bankovnih računa i kreditnih kartica trebaju ostati povjerljivi te se ne bi trebali lako odavati putem javnih kanala.

5. Zaključak

Metode socijalnog inženjeringa, a među njima i *vishing* metoda pridonijele su postizanju velikog profita kod kriminalaca. Razvojem telefonskih usluga te upotrebom Interneta, kriminalne se djelatnosti šire te se u budućnosti može očekivati sve više napada. Napadači uvijek smišljaju nove načine napada, a u sljedećem vremenu očekuje se upravo povećanje broja napada uz primjenu različitih metoda socijalnog inženjeringa.

Vishing metoda, kao jedan oblik *phishing* napada, odnosno napada socijalnim inženjeringom, napadačima pruža mogućnost zlouporabe telefonskih usluga, tj., preciznije, telefonskih usluga temeljenih na VoIP tehnologiji. Ona je pogodna za zlouporabu jer pruža mnogo širi skup potencijalnih meta, tj. ljudi koje je moguće navesti na odavanje osjetljivih podataka putem telefona.

Sveprisutan razvoj tehnologije donosi mnogo korisnih usluga te omogućuje poboljšanu komunikaciju među ljudima. No svaku je tehnologiju moguće zlouporabiti, a uvijek će biti onih koji će tražiti zaradu na oportunističke načine te je zbog toga prijeko potreban oprez pri upotrebi svih novih tehnologija pa tako i tehnologije VoIP.

6. Reference

[1] O *vishing* metodama, http://www.technicalinfo.net/papers/Vishing.html , ožujak 2008.

[2] *IBM vishing guide*, http://www.iss.net/documents/whitepapers/IBM_ISS_vishing_guide.pdf , ožujak 2008

[3] *Vishing* metode, http://en.wikipedia.org/wiki/Vishing, ožujak 2008.

[4] Iskustva s *vishing* napadima, http://security.tekrati.com/research/10059/, veljača 2008.