CARNET

Phishing

NCERT-PUBDOC-2018-5-361

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Socijalnim inženjeringom nazivamo skupinu metoda i tehnika napada na sigurnost informacijskih sustava koji su usmjereni na čovjeka, a ne na tehniku. Zapravo se radi o različitim načinima obmane mete (osobe koju se izravno napada) ili žrtve (osobe koja je krajnji cilj napada) da učini nešto ili oda neku informaciju što ne bi učinila da je svjesna da je to napad ili da se može iskoristiti za napad.

Izrazito česta metoda skupini socijalnog inženjeringa naziva se *phishing* (od eng. *fishing* – pecanje). Naziv podsjeća na bacanje „elektroničkog mamca" u nadi da će netko „zagristi" i, nesvjestan opasnosti, napraviti nešto što nije u interesu njegove sigurnost ili sigurnosti drugih.

Na primjer, napadač pošalje poruku elektroničkom poštom koja naizgled dolazi od banke i koja traži od mete da preda broj svoje kreditne kartice. To može tražiti očigledno, sugerirajući u tekstu poruke da meta uzvrati odgovorom i u njemu dade željeni podatak ili prikriveno, tražeći da meta posjeti Web stranicu, čija je poveznica u poruci, a na toj stranici se među ostalim traži i željeni osjetljivi podatak. Na slici 1 nalazi se ilustracija Federalne Trgovačke Komisije SAD-a (eng. *Federal Trade Commision*) koja analogijom s pecanjem prikazuje upravo ovaj primjer.

Slika 1 – ilustracija Federalne Trgovačke Komisije SAD-a (eng. *Federal Trade Commision*) koja analogijom s pecanjem prikazuje primjer *phishing* napada (izvor)

Osjetljivi je podatak svaki koji omogućava napadaču da sebi priskrbi materijalnu ili nematerijalnu dobit, čak i ako pri tome žrtva nije oštećena ili svaki podatak kojim napadač može nauditi meti ili nekoj drugoj žrtvi. Osjetljivi se podaci ne moraju odnositi samo na ljude (osobni podaci), već se oni mogu odnositi i na sustave (IP adrese, lozinke…) i organizacije (njihov ustroj, plaće, tehničke mjere zaštite, poslovni planovi, klijenti…).

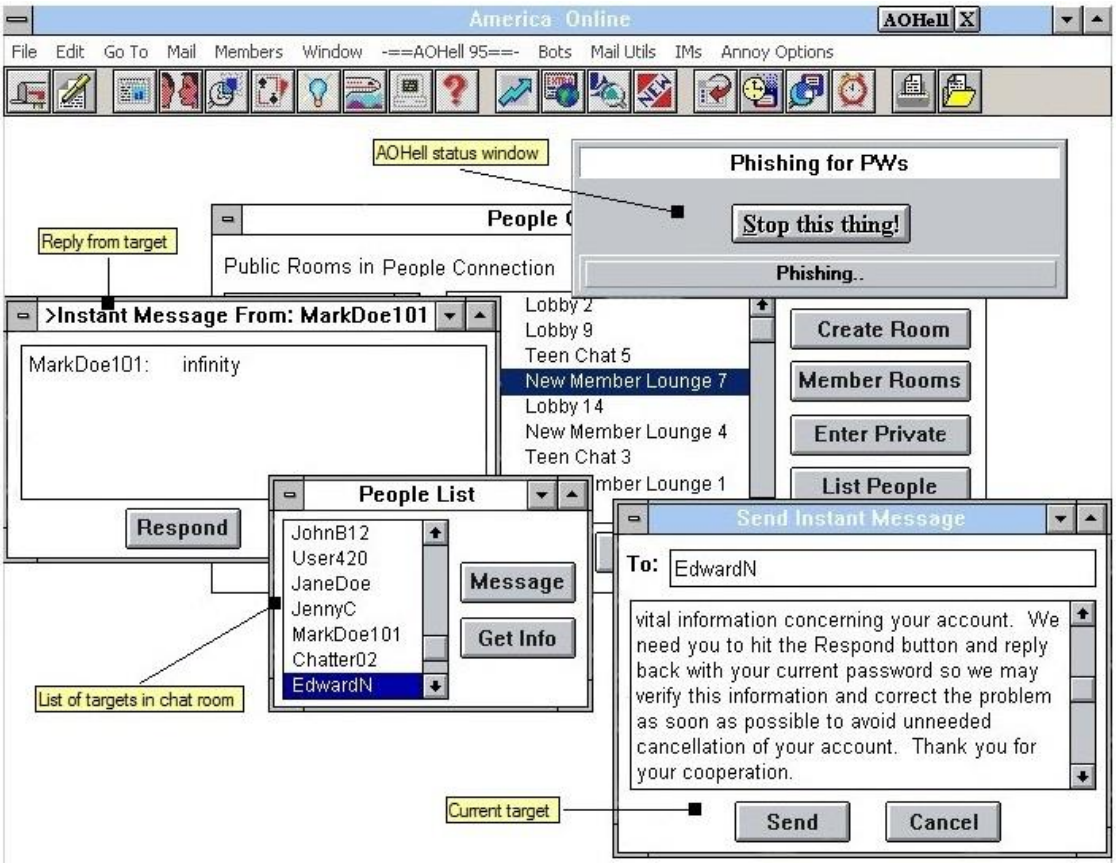
Iako se *phishing* poruke najčešće šalju putem elektroničke pošte, sve su češći slučajevi da se koriste *instant messaging/chat* aplikacije (WhatsApp, Viber, SnapChat…) te SMS (*Short Message Service* u mobilnoj telefoniji).

Jedni od prvih, ako ne i prvi *phishing* napadi odvijali su se na AOL mreži 90-tih godina (1). Jedna od poruka koja se tada navodno koristila za *phishing* bila je sljedeća:

> *ATTENTION: AOL NEWS*
>
> **********************************
>
> *Hi, I'm with the America Online billing department.*
>
> *Due to a problem we our experiencing with our records, we have lost vital information concerning your account.*
>
> *We need you to hit the Respond button and reply back with your current password so we may verify this information and correct the problem as soon as possible to avoid unneeded cancellation of your account.*
>
> *Thank you for your cooperation.*

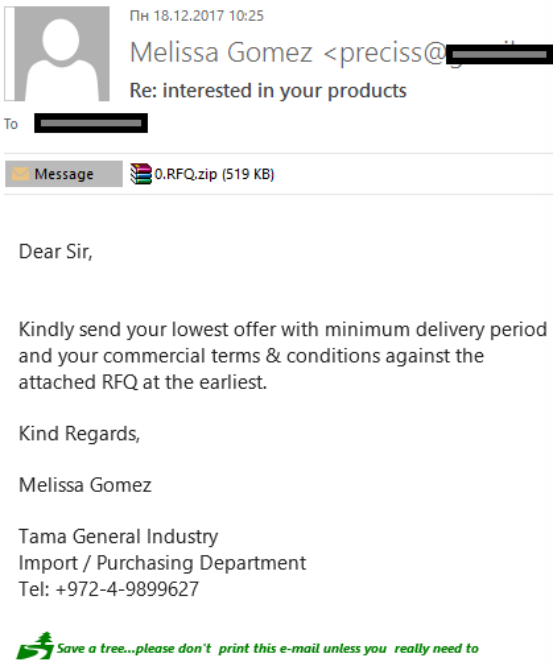
Uz takve poruke i mijenjanje imena svog korisničkog računa u ime koje naizgled pripada AOL osoblju (npr. *BillingDept*), tadašnji napadači su navodno izvodili jedne od prvih *phishing* napada. Slika 2 prikazuje konfiguracijsko sučelje alata *AOHell*, jednog od prvih alata za *phishing* napade kojim su se ovakve poruke automatski slale velikom broju meta. Slika 3 prikazuje napadačevu perspektivu prilikom izvođenja napada istim programom.

Slika 2 – konfiguracijsko sučelje alata *AOHell*, jednog od prvih alata za *phishing* napade (1)



Slika 3 – napadačeva perspektiva prilikom izvođenja napada programom *AOHell* (1)

Phishing danas izgleda nešto drugačije – u pravilu uključuje poruke elektroničke pošte te obmanjivanje mete da preuzme i pokrene zlonamjerni softver (primjer prikazan na slici 4) ili usmjeravanje mete na napadačevu Web stranicu (primjer prikazan na slici 5).



Slika 4 – primjer *phishing* poruke koja pokušava obmanuti metu da preuzme i pokrene zlonamjerni softver (izvor)

> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

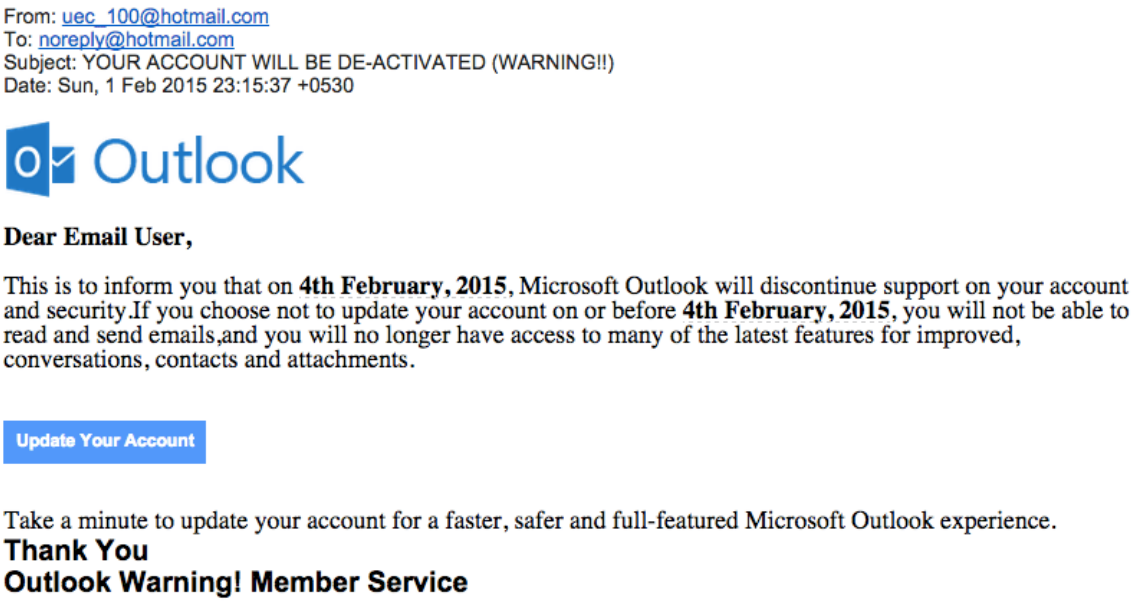
Slika 5 – primjer *phishing* poruke koja pokušava usmjeriti metu na napadačevu Web stranicu (izvor)

1.1 Spearphishing

Posebna vrsta *phishinga* je tzv. *spearphishing* (od eng. *spearfishing* – lov riba kopljem).

„Obične“ *phishing* poruke su generičke i šalju se velikom broju meta u nadi da će barem jedan dio nasjesti na prevaru. Takve poruke često su jednostavne i mnogima sumnjive već na prvi pogled. No i dalje, ako je poruka poslana na tisuće adresa, moguće je da će netko tko zaista slabo poznaje sigurnost, ili je tek počeo koristiti računala ili je jednostavno u žurbi i nepažljiv, dati podatak ili pokrenuti zlonamjerni program. Na slici 6 nalazi se primjer uobičajene, generičke *phishing* poruke. Ta poruka je iz niza razloga već na prvi pogled sumnjiva, između ostaloga i zato jer se korisniku obrača s „Dear Email User“.

Za razliku od takvog uobičajenog *phishinga*, tj. slanja poruke velikom broju meta, ali s niskom efikasnošću, *spearphishing* je ciljani napad u kojemu se napada točno određena osoba ili organizacija. U analogiji s lovom riba, *spearphishing* je „lov kopljem” za razliku od običnog *phishinga* koji je „bacanje udice u more riba”. Na slici 7 nalazi se primjer *spearphishing* poruke. U kontekstu mete, takva poruka vjerojatno se ne ističe značajno od brojnih drugih poruka koje je meta primila.



From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530

Outlook

Dear Email User,

This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support on your account and security.If you choose not to update your account on or before **4th February, 2015**, you will not be able to read and send emails,and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

Update Your Account

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service

Slika 6 – primjer uobičajene, generičke *phishing* poruke (izvor)

[redacted]
13 July 2016 at 9:38 AM
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

Slika 7 – primjer *spearphishing* poruke (izvor)

Ključna karakteristika *spearphishing* napada je to da su oni prilagođeni meti – prividni pošiljatelj i sadržaj poruke su relevantni kontekstu mete. Primjerice, pošiljatelj je netko s kim meta i inače komunicira ili bi mogla komunicirati, a sadržaj je nešto što se odnosi na posao, nadležnost ili interese mete.

Adresa s koje je poslana *spearphishing* poruka je često naizgled poznata, a sadržaj poruke ima smisla i koristi žargon koji odgovara kontekstu. Pored toga, i razni drugi detalji su ispravni: drugi sporedni ljudi, projekti, postupci, događaji koji se spominju u poruci itd.

Osim prilagođenosti meti, *spearphishing* napadi često su i prilično sofisticirani. Uobičajeno je da oni koriste napredne tehnike koje zahtijevaju više resursa, prikupljanje podataka o meti, dobru pripremu, poznavanje konteksta mete te svime time povećavaju vjerojatnost uspjeha napada.

Zbog svoje visoke efikasnosti i gotovo potpunog zaobilaženja tehničkih zaštita, *spearphishing* je jedna od glavnih metoda napada naprednih prijetnji/napadača (eng. *advanced persistent threat*) (2). Sve u svemu, ključno je znati da je *spearphishing* jedna od najvećih prijetnja sigurnosti organizacija danas!

2 Tehnike *phishing* napada

Tehnike korištene u *phishing* napadima uključuju tehnike obmane (tehnike socijalnog inženjeringa) i općenite tehnike napada na računalnu sigurnost (npr. iskorištavanje ranjivosti softvera). Kod nekih tehnika je čak teško odvojiti komponentu koja iskorištava ljudsku psihologiju od komponente koja iskorištava ranjivosti računalnih sustava.

Kako se mijenjaju ljudske navike, socijalne norme i slično, tako se mijenjaju i tehnike *phishing* napada te tehnike socijalnog inženjeringa općenito. Upravo zato ne postoji jasna kategorizacija ovakvih tehnika napada. U ovom dokumentu, pregled i kategorizacija tehnika *phishing* napada napravljeni su na temelju onoga kako *phishing* napadi izgledaju danas.

Daljnji pregled tehnika *phishing* napada bit će podijeljen u sljedeće kategorije:

1. Uvjerljivost *phishing* poruke
2. Napadi kroz Web stranice
3. Napadi zlonamjernim softverom
4. Ostali napadi

2.1 Uvjerljivost poruke

Kako bi *phishing* napad uspio, tj. obmana uspjela, poruka koju napadač pošalje mora biti u većoj ili manjoj mjeri uvjerljiva. Postoji niz tehnika koje napadači koriste kako bi učinili *phishing* poruku uvjerljivijom.

2.1.1 Lažno predstavljanje

Kako bi *phishing* poruka bila uvjerljiva, i time cijeli *phishing* napad uspio, prvi korak je da prividni pošiljatelj bude uvjerljiv.

Phishing napad uvijek uključuje lažno predstavljanje:

- ili se napadač predstavlja kao neka druga, postojeća osoba/organizacija,
    - npr. kao metina banka koja želi potvrditi njene podatke,
- ili se predstavlja kao nepostojeća, ali i dalje relevantna osoba/organizacija,
    - npr. kao izmišljena tvrtka koja želi poslovati s tvrtkom mete.

Napadač nikada neće jasno dati do znanja da poruka zapravo dolazi od njega – u slučajevima gdje je jasno da napadač kontaktira metu (npr. ucjena), to više nije *phishing* niti socijalni inženjering.

Osim sadržaja poruke koji odgovara lažnom identitetu pošiljatelja, moguće je i s tehničke strane učiniti lažno predstavljanje uvjerljivijim.

Kada je medij komunikacije elektronička pošta, moguće je prilično jednostavno lažirati adresu pošiljatelja. Primjerice, lako je poslati poruku da izgleda kao da je došla s adrese „support@paypal.com". No, takva poruka će kod primatelja često završiti u mapi s neželjenom poštom (eng. *spam*).

U kontekstu elektroničke pošte i ostalih medija komunikacije gdje je ključni dio identiteta domena, moguće je i registrirati sličnu domenu u svrhe obmane. Tada je moguće, primjerice, s registrirane domene poslati potpuno (tehnički) legitimnu poruku e-pošte. Ako je ciljna domena *paypal.com*, primjeri sličnih domena su: *paypa1.com*, *poypal.com*, *paypal-com.hr*…

Jedan alat povezan s ovom tehnikom je *dnstwist*. Njime je moguće za određenu domenu automatski provjeriti koje slične domene postoje te jesu li registrirane. Slika 8 prikazuje dio ispisa alata *dnstwist* za ciljnu domenu *carnet.hr*.

```
$ ./dnstwist.py carnet.hr
     _           _            _     _
  __| |_ __  ___| |___      _(_)___| |_
 / _` | '_ \/ __| __\ \ /\ / / / __| __|
| (_| | | | \__ \ |_ \ V  V /| \__ \ |_
 \__,_|_| |_|___/\__| \_/\_/ |_|___/\__| {1.04b}

Processing 210 domain variants ..78%......... 4 hits (1%)

Original*       carnet.hr          161.53.160.25 NS:dns1.carnet.hr MX:mail.carnet.hr
Addition        carneta.hr         -
Addition        carnetb.hr         -
Addition        carnetc.hr         -
Addition        carnetd.hr         -
Addition        carnete.hr         -
Addition        carnetf.hr         -
Addition        carnetg.hr         -
Addition        carneth.hr         -
Addition        carneti.hr         -
Addition        carnetj.hr         -
Addition        carnetk.hr         -
Addition        carnetl.hr         -
Addition        carnetm.hr         -
Addition        carnetn.hr         -
Addition        carneto.hr         -
Addition        carnetp.hr         -
Addition        carnetq.hr         -
Addition        carnetr.hr         -
Addition        carnets.hr         -
Addition        carnett.hr         -
Addition        carnetu.hr         -
Addition        carnetv.hr         -
Addition        carnetw.hr         -
Addition        carnetx.hr         -
Addition        carnety.hr         -
Addition        carnetz.hr         -
Bitsquatting    barnet.hr          -
Bitsquatting    aarnet.hr          -
Bitsquatting    garnet.hr          NS:bery1.studio4web.com
Bitsquatting    karnet.hr          -
Bitsquatting    sarnet.hr          -
Bitsquatting    ccrnet.hr          -
Bitsquatting    cernet.hr          -
Bitsquatting    cirnet.hr          -
Bitsquatting    carnet.hr          -
```

Slika 8 – dio ispisa alata *dnstwist* za ciljnu domenu *carnet.hr*

U kontekstu elektroničke pošte, napadači ponekada šalju poruke i s drugih, ali i dalje djelomično uvjerljivih adresa. Primjerice, ako se napadač lažno predstavlja kao tvrtka *Paypal*, može poslati poruku s adresa kao što su *paypal@gmail.com*,

support@paypal.<napadačeva domena>.com i slično. Već i slanje s takvih adresa može uspješno obmanuti žrtve, pogotovo ako je uvjerljivo prividno ime pošiljatelja, sadržaj poruke i ostalo.

Već u 90-ima, u *phishing* napadima na AOL mreži, napadači su mijenjali imena svojih računa u lažna imena AOL osoblja (npr. *BillingDept*) te tako slali poruke. Slično je moguće učiniti i danas na društvenim mrežama, *instant messaging*/*chat* aplikacijama te brojnim drugim načinima komunikacije na internetu.

U komunikaciji SMS porukama, moguće je lažirati telefonski broj s kojeg dolazi poruka. To nije moguće napraviti tako lako kao za elektroničku poštu, no danas su dostupni servisi preko kojih je moguće slati SMS-ove s lažnim brojem za izrazito niske cijene (manje od 1€ po SMS-u – čak i značajno jeftinije za veći broj poruka).

U nekim slučajevima, moguće je i klonirati SIM karticu (neke druge mete) te zatim slati SMS-ove (ili zvati) metu s broja povezanog s originalnom SIM karticom. Tada je moguće i primiti SMS-ove na broj povezan s originalnom SIM karticom, te na temelju njega napraviti lažni korisnički račun na servisima kao što su WhatsApp, Viber i slično.

Što se tiče predstavljanja kao izmišljena osoba/organizacija, to u pravilu ne zahtjeva neko posebno tehničko znanje, već je samo pitanje koliko će napadač uložiti resursa. Primjerice, u slučaju predstavljanja kao izmišljena tvrtka, u svrhu povećanja uvjerljivosti moguće je:

- kupiti domenu s imenom tvrtke,
- napraviti Web stranice tvrtke,
- napraviti profil tvrtke na relevantnim društvenim mrežama (*LinkedIn*, *Facebook*…),
- postaviti poslužitelje za elektroničku poštu,
    - te konfigurirati dodatne mehanizme kao što su SPF, DKIM i DMARC kako bi se e-pošta s tehničke strane činila legitimnom,
- itd.

2.1.2 Općenite tehnike obmane/socijalnog inženjeringa

Što se tiče samog sadržaja poruke, općenite tehnike obmane/socijalnog inženjeringa su većinom primjenjive i na *phishing*. Te tehnike uključuju:

- pripremu uvjerljive lažne priče (eng. *pretext*),
- spominjanje relevantnih informacija, npr.
    - spominjanje relevantnih imena (eng. *name dropping*) iz organizacije ili društvenog kruga mete,
    - korištenje relevantnog žargona,

- obećanje nagrade ili prijetnju kaznom (problemima s računalom …).

Više informacija o općenitim tehnikama obmane/socijalnog inženjeringa nalazi se u prethodnom dokumentu NCERT-a: „Uvod u socijalni inženjering".

2.2 Napadi kroz Web stranice

U kontekstu *phishinga*, česti su napadi u kojima napadač pokušava obmanuti žrtvu da klikne napadačevu poveznicu/URL, odnosno da posjeti napadačevu Web stranicu.

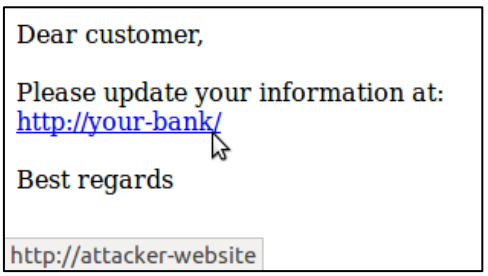
2.2.1 Lažiranje odredišta poveznice

Kako bi napadač uspješno obmanuo žrtvu, obično će nekako pokušati prikriti stvarno odredište poveznice.

Jedna od najjednostavnijih tehnika je prikrivanje odredišta poveznice u HTML-u. Primjer HTML koda bi bio:

prividno odredište

gdje umjesto stvarnog odredišta piše URL napadačeve Web stranice, a umjesto prividnog odredišta piše URL koji žrtvi izgleda bezopasno. Slika 9 prikazuje kako lažiranje odredišta poveznice u HTML-u može izgledati iz metine perspektive: u tekstu poruke se naizgled nalazi poveznica na Web stranicu banke, dok se u statusnoj traci prikazuje stvarno odredište poveznice – napadačeva Web stranica.



Slika 9 – primjer lažiranje odredišta poveznice u HTML-u iz perspektive mete

To znači da prije slijeđenja poveznice u bilo kojoj elektroničkoj poruci („klikanje na link") treba postaviti pokazivač iznad poveznice i u statusnoj traci provjeriti kamo ta poveznica zaista vodi.

Prethodno je spomenuto registriranje slične domene u kontekstu lažiranja izvora poruke – ista tehnika je korisna i u svrhe lažiranja odredišta poveznice.

Za prikrivanje stvarnog odredišta poveznice često se koriste i servisi skraćivanja URL-a, kao što su *bit.ly*, *tinyurl.com* i slični. Kratka, nekima i poznata domena dobivena takvim servisom metama može uliti povjerenje te ih potaknuti da posjete napadačev URL.

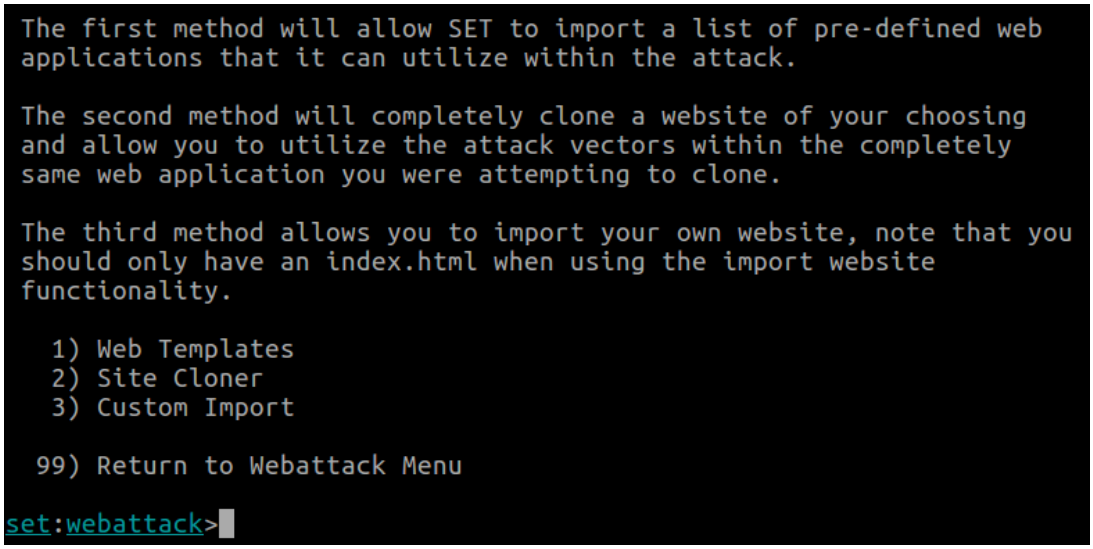
Jedna posebno opasna prijetnja u ovom kontekstu je tzv. ranjivost otvorenog preusmjeravanja (eng. *open redirect*). To je ranjivost na Web stranicama koja omogućava napadaču da izrazito uvjerljivo prikrije stvarno odredište URL-a. U praksi, ta ranjivost izgleda tako da napadač usmjeri žrtvu na poveznicu oblika:

http://example.com/?redirect=<*napadačev URL*>

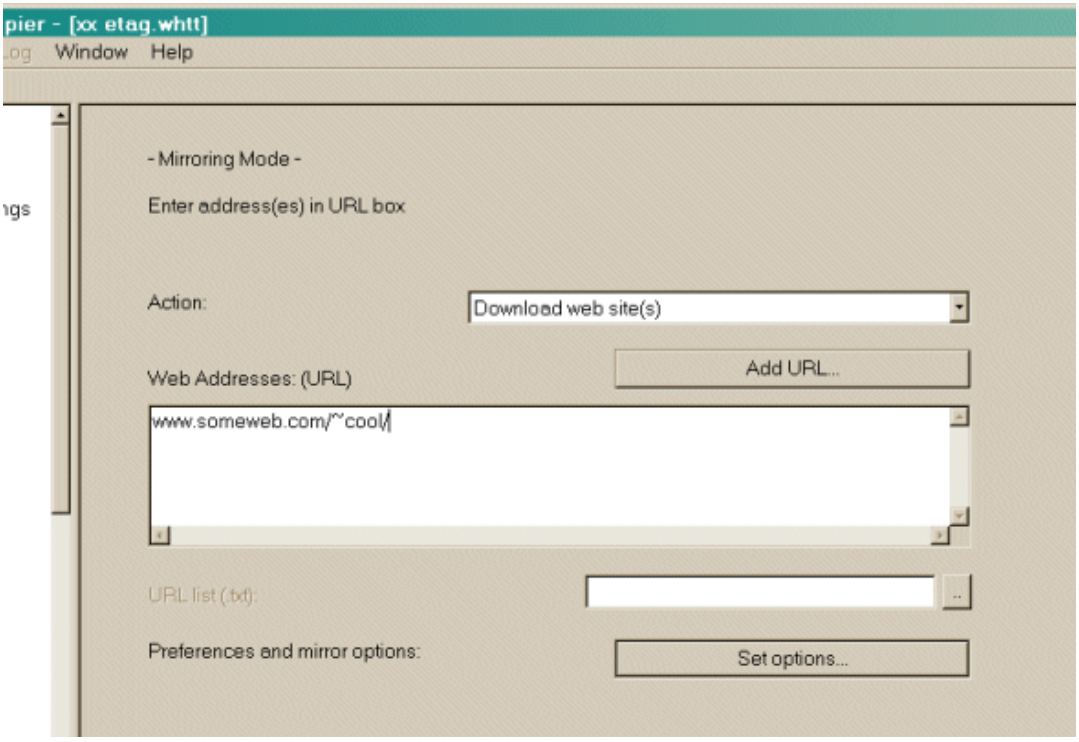
Ta poveznica izgleda kao da vodi na stranicu na domeni *example.com*, no ona zapravo u konačnici preusmjerava posjetitelja na napadačev URL.

2.2.2 Lažne kopije Web stranica

S tehničke strane, jednostavno je napraviti kopiju Web stranice koja vizualno izgleda isto kao original. Široko su dostupni alati koji automatiziraju proces „kloniranja" Web stranice – primjeri takvih alata su *Social-Engineer Toolkit* i *HTTrack*. Slika 10 prikazuje izbornik u alatu *Social-Engineer Toolkit* gdje je moguće vidjeti neke od izbora vezanih za napad lažnom kopijom Web stranice. Slika 11 prikazuje sučelje alata *HTTrack* u procesu kloniranja Web stranice.



Slika 10 – izbornik u alatu *Social-Engineer Toolkit* gdje je moguće vidjeti neke od izbora vezanih za napad lažnom kopijom Web stranice



Slika 11 – sučelje alata *HTTrack* u procesu kloniranja Web stranice (izvor)

Kako bi ovako napravljena lažna stranica bila uvjerljivija, prilikom postavljanja stranice koristi se i sličan URL/domena te HTTPS.

2.2.3 Socijalni inženjering i Web sigurnost općenito

Postoji niz sigurnosnih ranjivosti i napada u kontekstu Web sigurnosti koji se u pravilu oslanjaju na obmanu/socijalni inženjering žrtve, a koriste se i u *phishing* napadima. Primjeri kategorija takvih ranjivosti/napada uključuju:

- *cross-site scripting* (XSS) ranjivosti,
- *cross-site request forgery* (CSRF) ranjivosti,
- *clickjacking* napade,
- *tabnabbing* napade,
- itd.

Presjek socijalnog inženjeringa i Web sigurnosti je cijela tema za sebe te će kao takva biti obrađena u budućnosti, u zasebnom dokumentu.

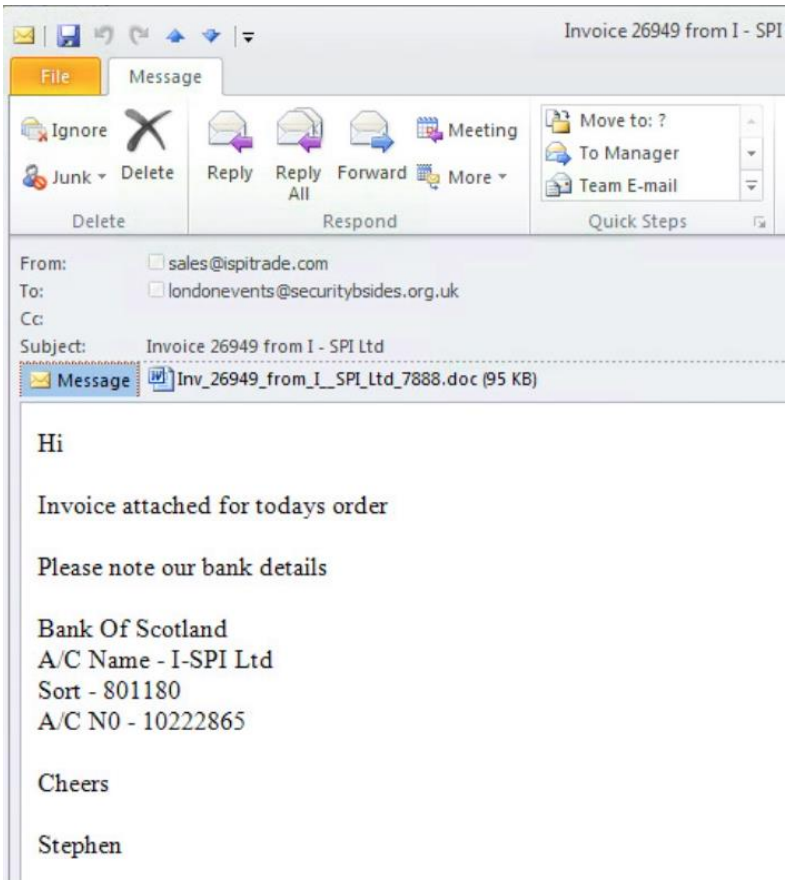
2.3 Napadi zlonamjernim softverom

Napadač *phishing* porukom često pokušava inficirati metu zlonamjernim softverom (eng. *malware*). U takvom napadu, napadač u pravilu manipulira žrtvu:

1. da preuzme zlonamjerni softver

2. te da ga pokrene.

Zlonamjerni softver obično je lažno predstavljen kao račun, ugovor, slika, program za pregledavanje poruke i slično, a obično se nalazi u privitku ili na URL-u iz poruke. Primjer *phishing* poruke sa zlonamjernim softverom prikazan je na slici 12. U tekstu poruke napadač piše kako se račun za današnju narudžbu nalazi u privitku, dok je u privitku zapravo dokument koji u sebi sadrži zlonamjerni kod.



Slika 12 – primjer *phishing* poruke sa zlonamjernim softverom (izvor)

U ovom kontekstu, tehnike napada u pravilu imaju cilj upakirati zlonamjerni kod u datoteku koja će se meti činiti bezopasnom.

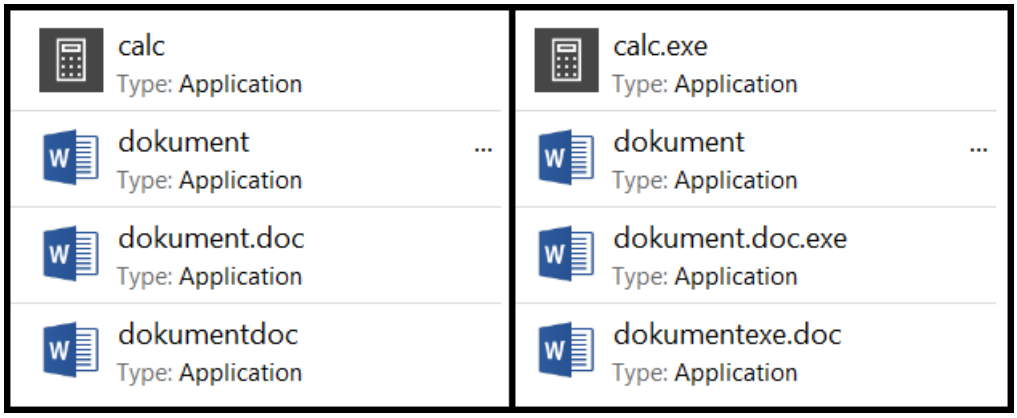
2.3.1 Prikrivanje vrste datoteke

Jedan od prvih načina po kojemu će meta procijeniti sadrži li datoteka zlonamjerni softver je vrsta datoteke specificirana njenim nastavkom. Veliki će broj krajnjih korisnika izvršnu (*.exe*) datoteku u privitku smatrati u najmanju ruku sumnjivom te ju često neće pokrenuti. No, ako im nije jasno da je datoteka zapravo izvršna, već im se primjerice čini da je ona zapravo dokument, tada takav oprez može pasti u vodu.

U ovom poglavlju koristit će se Windows izvršne (*.exe*) datoteke kao primjer zlonamjernog softvera, no slične tehnike primjenjive su i za druge vrste datoteka te na drugim operacijskim sustavima.

Kako bi napadač prikrio stvarnu vrstu Windows izvršne (*.exe*) datoteke, može koristiti sljedeće tehnike (sve tehnike popraćene su primjerima na slici 13 na kojoj je izvršna datoteka *calc.exe* na razne načine maskirana kao dokument):

- Izvršne datoteke mogu imati proizvoljnu ikonu, tako da izvršna datoteka koja se „pretvara" da je dokument može imati ikonu dokumenta (slika 13 drugi, treći i četvrti red)
- Gomila razmaka u imenu datoteke nakon „imena", a prije nastavka, može prikriti nastavak datoteke (slika 13 drugi red)
- Dvostruki nastavci mogu zavarati neke mete – npr. *slika.jpg.exe*, *dokument.doc.exe* (slika 13 treći red)
- *Right-To-Left Override* Unicode znak (U+202E) napravljen je za jezike koji se pišu s desna na lijevo, no koristi se i kod *phishinga* za prikrivanje stvarnog nastavka datoteke (slika 13 četvrti red)



Slika 13 – primjeri u kojima je izvršna datoteka *calc.exe* na razne načine maskirana kao dokument (lijeva strana prikazuje perspektivu korisnika s isključenim prikazom nastavaka, dok desna strana prikazuje perspektivu s uključenim prikazom nastavaka)

2.3.2 Zlonamjerni kod u datotekama

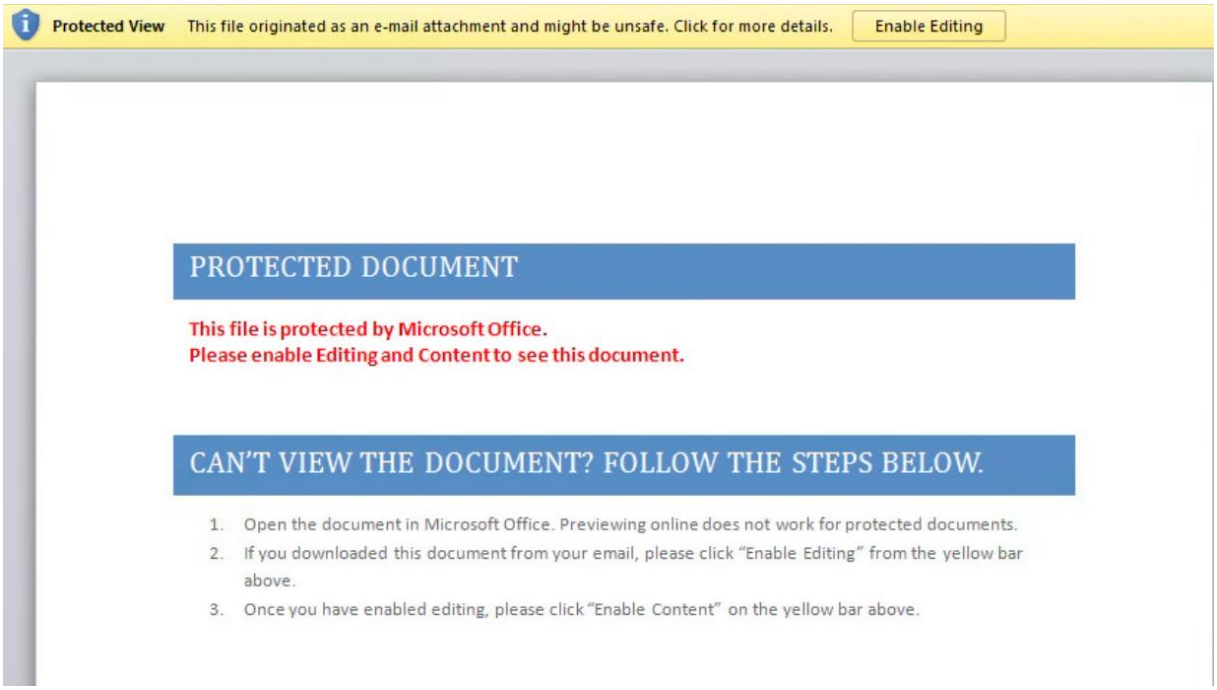
Kada se spominje zlonamjerni softver, prva vrsta datoteke koja većini korisnika pada napamet su upravo izvršne (*.exe*) datoteke. Osim što izvršne datoteke poslane u privitku često naiđu na sumnju kod meta, takve datoteke obično blokiraju i razni sigurnosni mehanizmi. Upravo zbog te rasprostranjenosti izvršnih datoteka u napadima, napadači su se morali prilagoditi.

Velik dio datoteka sa zlonamjernim softverom danas uopće nisu izvršne datoteke. Datoteke s neobičnim, naizgled bezopasni nastavcima kao što su *.js*, *.hta*, *.wsf*, *.lnk* i slično mogu sadržavati zlonamjerni kod te biti jednako opasne kao *.exe* datoteke, bez prethodno spomenutih negativnih strana iz perspektive napadača. Napadači redovito otkrivaju nove vrste datoteka čiju opasnost zanemaruju mete i sigurnosni mehanizmi te onda koriste te vrste datoteka kao „prijevozno sredstvo" za zlonamjerni kod.

Izrazito česti medij za zlonamjerni softver danas je VBA (*Visual Basic for Applications*) kod unutar *Microsoft Office* dokumenata. Takvi dokumenti svakodnevno se razmjenjuju u

poslovnim okruženjima te veliki broj korisnika neće uopće posumnjati da neki od njih može predstavljati i opasnost.

U takvim dokumentima, ugrađeni sigurnosni mehanizam ne dozvoljava automatsko aktiviranje takvog koda već od mete traži da mora kliknuti na „Omogući uređivanje" kako bi se pokrenuo zlonamjerni kod. Napadači pokušavaju manipulirati mete na razne načine kako bi ih naveli da pritisnu tu tipku i inficiraju svoje računalo zlonamjernim softverom. Jedan primjer takvog dokumenta dan je na slici 14. U njemu je napadač sadržaj dokumenta pokušao prikazati kao dio korisničkog sučelja koje kaže kako je dokument zaštićen te je potrebno pritisnuti na „Omogući uređivanje" da prikaže sadržaj dokumenta.



Slika 14 – primjer dokumenta s zlonamjernim VBA kodom (izvor)

U kontekstu datoteka sa zlonamjernim softverom, vjerojatno najopasnije datoteke su one koje sadržavaju *exploit*. Drugim riječima, to su posebno konstruirane datoteke (npr. slika, dokument…) koje već samim otvaranjem mogu iskoristiti ranjivost u programu i automatski pokrenuti napadačev zlonamjerni kod.

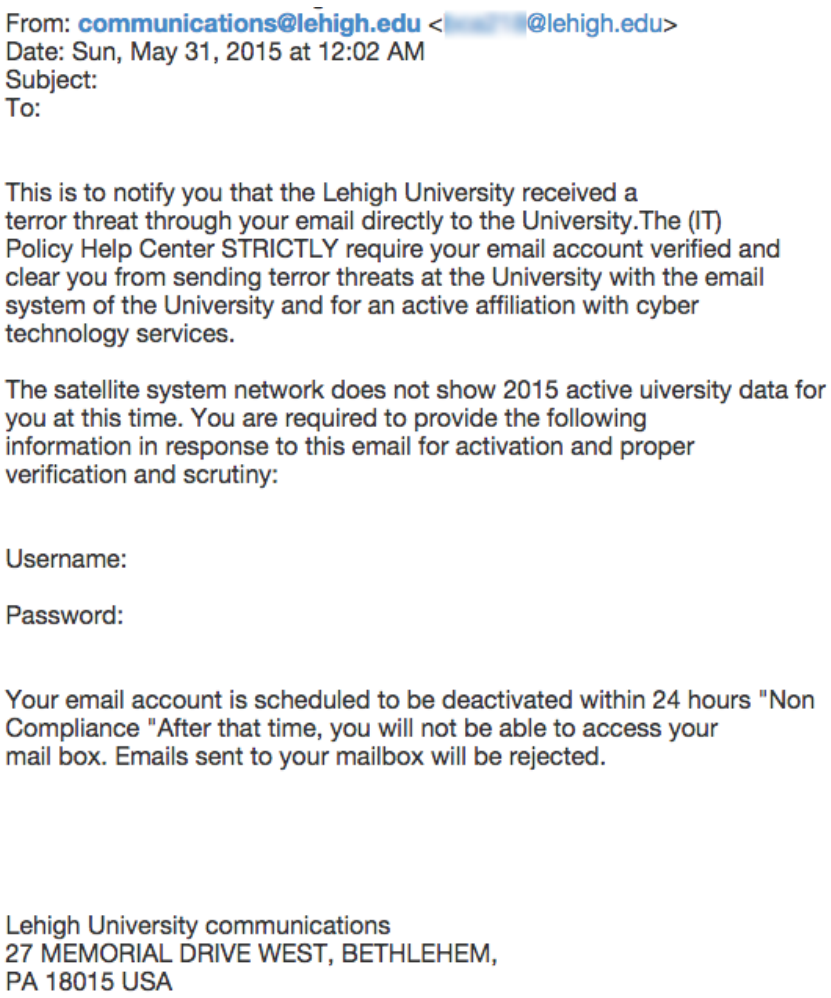
2.4 Ostali napadi

Phishing napadi ne moraju uključivati ni Web stranicu, ni zlonamjerni softver niti nešto sličnog karaktera. Primjerice, u *phishing* napadima na AOL mreži u 90-ima napadači su se lažno predstavljali kao AOL osoblje te izravno tražili žrtve da im pošalju svoju lozinku.

I danas se slični napadi uspješno odvijaju. U takvim napadima napadač izravno:

- traži od žrtve da mu preda osjetljive informacije (npr. lozinku)
- ili da učini nešto (npr. izvrši neku uplatu).

Primjer takve *phishing* poruke prikazan je na slici 15 – u njoj napadač izravno traži metu da mu preda korisničko ime i lozinku.



From: communications@lehigh.edu <[redacted]@lehigh.edu>
Date: Sun, May 31, 2015 at 12:02 AM
Subject:
To:

This is to notify you that the Lehigh University received a terror threat through your email directly to the University.The (IT) Policy Help Center STRICTLY require your email account verified and clear you from sending terror threats at the University with the email system of the University and for an active affiliation with cyber technology services.

The satellite system network does not show 2015 active uiversity data for you at this time. You are required to provide the following information in response to this email for activation and proper verification and scrutiny:

Username:

Password:

Your email account is scheduled to be deactivated within 24 hours "Non Compliance "After that time, you will not be able to access your mail box. Emails sent to your mailbox will be rejected.

Lehigh University communications
27 MEMORIAL DRIVE WEST, BETHLEHEM,
PA 18015 USA

Slika 15 – primjer *phishing* poruke u kojoj napadač izravno traži metu da mu preda korisničko ime i lozinku (izvor)

3 Zaštita od *phishinga*

U svojem blogu, sigurnosna tvrtka Kaspersky piše sljedeće po pitanju zaštite od *phishing* napada: „Nažalost, ne postoji pravi lijek za phishing napade osim opreza korisnika, na paranoičnoj razini." (3)

Kao i sigurnost općenito, nije se moguće u potpunosti zaštititi, no moguće je otežati uspješan napad i time smanjiti rizik. Mjere zaštite od *phishing* napada velikim dijelom se svode na općenite mjere zaštite od socijalnog inženjeringa. Više informacija o takvim mjerama nalazi se u prethodnom dokumentu NCERT-a: „Uvod u socijalni inženjering".

Po pitanju mjera zaštite za krajnjeg korisnika, preduvjet za zaštitu je da se krajnji korisnik upoznat s prijetnjama. Tek tada on može obratiti pažnju na potencijalne znakove *phishing* napada, posebice kada:

- poruka sadržava poveznicu
    - kamo ta poveznica zaista vodi?
- poruka sadržava datoteku kao privitak
    - ima li znakova da datoteka sadržava zlonamjerni softver?
- pošiljatelj traži povjerljive informacije ili izvršavanje osjetljive radnje (npr. uplata novca)

Ako postoji sumnja u legitimitet poruke, korisno je drugim komunikacijskim kanalom (telefonom, SMS porukom…) uspostaviti kontakt s pošiljateljem, provjeriti njegovu vjerodostojnost i legitimnost toga što traži. Ponekad je tu legitimnost potrebno provjeriti i s nadležnim službama: IT odjelom u organizaciji, računovodstvom, pravnim odjelom, povjerenikom za zaštitu osobnih podataka, a ponekad i policijom, agencijom za zaštitu osobnih podataka ili nacionalnim CERT-om.

Mjere zaštite na razini organizacije uključuju sljedeće:

- Upoznavanje zaposlenika s prijetnjama
    - Zaposlenike treba i pri zapošljavanju i kasnije, periodički, ali redovito upoznati s (novim) prijetnjama i tehnikama napada.
    - Posebice treba osvijestiti i obrazovati ključno osoblje koje ima najveći rizik za izloženost napadu: one koji rukuju osjetljivim informacijama ili osjetljivim sustavima te imaju važne ovlasti.
- Uklanjanje ljudske procjene iz procesa odlučivanja što je više moguće
    - Korisno je označiti tajnosti podataka: jesu li određeni podaci javni, tajni, za internu uporabu?
    - Potrebno je uspostaviti jasna pravila te provjeravati njihovo poznavanje, razumijevanje i primjenu.

Iako je srž socijalnog inženjeringa upravo obmana ljudi, tj. napad na ljudsku komponentu, napad socijalnog inženjeringa može imati i tehničku komponentu, *phishing* napadi često imaju i značajnu tehničku komponentu („manipulacije" URL-ovima, lažne i zlonamjerne Web stranice, zlonamjerni softver…). Upravo zato, u kontekstu zaštite od *phishing* napada bitno je spomenuti i zaštitu s tehničke strane.

Bitno je razumjeti da tehničkim rješenjima nikada neće biti moguće zaustaviti sve *phishing* napade, no njima je moguće značajan dio njih sasjeći u korijenu. Tehnička rješenja mogu biti izrazito efikasna protiv prethodno poznatih, raširenih napada, no često su bespomoćna protiv ciljanih (*spearphishing*) i sofisticiranih napada.

Postoji niz tehničkih zaštita predstavljenih kao *anti-phishing* rješenja. To je obično softver ugrađen u Web preglednik, u sustav obrade e-pošte ili slično koji prepoznaje i blokira *phishing* Web stranice ili poruke na temelju prethodno popunjene baze podataka i/ili heuristika.

Drugo značajno tehničko rješenje u obrani od *phishinga* je *anti-virus*/*anti-malware* softver. Takav softver ne sprječava *phishing* izravno, no izrazito je važna komponenta u sprječavanju napada koji uključuju zlonamjerni softver.

Brojni drugi općeniti sigurnosni mehanizmi korisni su i u zašiti protiv *phishing* napada. Primjerice, vatrozid na razini organizacije koji blokira pristup poznatim zlonamjernim domenama i IP adresama može jednako pomoći u zaustavljanju *phishing* napada kao i u zaustavljanju ostalih prijetnji.

U konačnici, bitno je spomenuti kako se tehnike *phishing* napada stalno mijenjaju, tako da se redovito mijenjaju i specifični savjeti za zaštitu od *phishinga*. Jedan primjer toga je sljedeći – HTTPS je često spominjan, te se i danas često spominje, kao znak da je Web stranica „sigurna". Neko vrijeme je to bio i praktičan savjet, jer osim što HTTPS štiti od posredničkih (*Man in the Middle* - MITM) napada, *phishing* Web stranice gotovo nikada nisu koristile HTTPS. No u posljednjih nekoliko godina, *phishing* Web stranice sve više koriste HTTPS te upravo zbog te kombinacije neopreznog savjeta i prilagodbe napadača neke žrtve sada podliježu prevari. (4)

4 Zaključak

Phishing, a posebice *spearphishing*, jedna je od najvećih prijetnji organizacijama danas.

Današnji *phishing* napadi često navode žrtvu na napadačevu zlonamjernu Web stranicu ili da preuzme zlonamjerni program te je korisno to imati na umu prilikom razmišljanja o zaštiti.

Pored ispravno podešenog i redovito osvježenog *anti-virus/anti-malware* softvera i vatrozida, glavne mjere zaštite većinom su iste kao i za socijalni inženjering općenito.

Ključno je da se krajnji korisnici računalnih sustava dobro upoznaju s prijetnjama te da na temelju tog znanja budu oprezni i rano prepoznaju znakove napada. Kad nisu sigurni predstavlja li neka poruka napad, trebaju imati dostupne stručnjake kojima se mogu javiti za savjet.

Na razini organizacije, pored uspostave tehničkih mjera zaštite, važno je redovito osvještavati i obrazovati zaposlenike, označiti tajnost podataka, uspostaviti jasna pravila te provjeravati njihovo poznavanje, razumijevanje i primjenu.

Pored toga, važno je uspostaviti atmosferu u kojoj se zaposlenici neće bojati pokazati svoje neznanje ili nepovjerljivost te redovito informirati sve zaposlene o eventualnim napadima, njihovom tijeku i posljedicama.

5 Literatura

1. **Rekouche, Koceilah.** Early Phishing. [Mrežno] 2011. http://arxiv.org/abs/1106.4692.
2. **Trend Micro.** Spear-Phishing Email: Most Favored APT Attack Bait. [Mrežno] 2012. [Citirano: 30. ožujak 2018.] https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.
3. **Kochetkova, Kate.** 10 Tips to protect yourself from phishing. *Kaspersky Lab.* [Mrežno] 13. studeni 2015. [Citirano: 5. svibanj 2018.] https://www.kaspersky.com/blog/phishing-ten-tips/10550/.
4. **Hassold, Crane.** A Quarter of Phishing Attacks are Now Hosted on HTTPS Domains: Why? *The PhishLabs Blog.* [Mrežno] 5. prosinac 2017. [Citirano: 3. svibanj 2018.] https://info.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains.
5. **Qualys.** How Open Redirection Threatens Your Web Applications. [Mrežno] 7. siječanj 2016. [Citirano: 28. ožujak 2018.] https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerability-threatens-your-web-applications.
6. **Ansari, MD Wasil.** How to clone SIM card under 15 minutes. *Tech2Hack.* [Mrežno] 12. siječanj 2018. [Citirano: 30. ožujak 2018.] https://www.tech2hack.com/how-to-clone-sim-card-easily/.
7. **Moramarco, Stephen.** Link Manipulation. *InfoSec Resources.* [Mrežno] [Citirano: 28. ožujak 2018.] http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-tools-techniques/link-manipulation/.
8. **Ramzan, Zulfikar.** A Brief History of Phishing: Part I. *Symantec Official Blog.* [Mrežno] 10. kolovoz 2007. [Citirano: 28. ožujak 2018.] http://www.symantec.com/connect/blogs/brief-history-phishing-part-i.
9. —. A Brief History of Phishing: Part II. *Symantec Official Blog.* [Mrežno] 13. kolovoz 2007. [Citirano: 28. ožujak 2018.] http://www.symantec.com/connect/blogs/brief-history-phishing-part-ii.
10. **Fischer, Thomas.** A Good Phishing Attack is Worth a Million Zero-Days. *Digital Guardian.* [Mrežno] 28. veljača 2017. [Citirano: 6. travanj 2018.] https://digitalguardian.com/blog/good-phishing-attack-worth-million-zero-days.
11. **Legon, Jeordan.** 'Phishing' scams reel in your identity. *CNN.com.* [Mrežno] 26. siječanj 2004. [Citirano: 27. ožujak 2018.] http://edition.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html.
12. **Abrams, Lawrence.** Dnstwist Helps You Find Phishing Sites Based on Your Domain. *BleepingComputer.* [Mrežno] 7. studeni 2017. [Citirano: 29. ožujak 2018.] https://www.bleepingcomputer.com/news/security/dnstwist-helps-you-find-phishing-sites-based-on-your-domain/.
13. **InfoSec.** Protecting Against Phishing Attacks. [Mrežno] [Citirano: 3. svibanj 2018.] https://www.infosec.gov.hk/english/anti/protect_org.html.
14. **Microsoft Secure.** Nemucod dot dot..WSF. [Mrežno] 23. srpanj 2016. [Citirano: 29. ožujak 2018.] https://cloudblogs.microsoft.com/microsoftsecure/2016/07/23/nemucod/.
15. **Kaspersky Lab.** Nigerian phishing: Industrial companies under attack. *Securelist - Kaspersky Lab's cyberthreat research and reports.* [Mrežno] 15. lipanj 2017. [Citirano: 2.

ožujak 2018.] https://securelist.com/nigerian-phishing-industrial-companies-under-attack/78565/.
16. **Cranor, Lorrie, i dr.** Phinding Phish: An Evaluation of Anti-Phishing Toolbars. [Mrežno] 13. studeni 2006. [Citirano: 3. svibanj 2018.] https://www.cylab.cmu.edu/_files/pdfs/tech_reports/cmucylab06018.pdf.
17. **Zheng, Xudong.** Phishing with Unicode Domains. [Mrežno] 14. travanj 2017. [Citirano: 26. ožujak 2018.] https://www.xudongz.com/blog/2017/idn-phishing/.
18. **Ducklin, Paul.** Ransomware in your inbox: the rise of malicious JavaScript attachments. *Naked Security.* [Mrežno] 26. travanj 2016. [Citirano: 29. ožujak 2018.] https://nakedsecurity.sophos.com/2016/04/26/ransomware-in-your-inbox-the-rise-of-malicious-javascript-attachments/.
19. **Arntz, Pieter.** File extensions. *Malwarebytes Labs.* [Mrežno] 30. ožujak 2016. [Citirano: 6. travanj 2018.] https://blog.malwarebytes.com/cybercrime/2013/12/file-extensions-2/.
20. —. The RTLO method. *Malwarebytes Labs.* [Mrežno] 9. siječanj 2014. [Citirano: 6. travanj 2018.] https://blog.malwarebytes.com/cybercrime/2014/01/the-rtlo-method/.
21. **Carlisle, Gordon.** Understanding Email Phishing. *BrightWire Networks.* [Mrežno] [Citirano: 6. travanj 2018.] https://www.brightwirenetworks.com/understanding-it/understanding-email-phishing.
22. **Fruhlinger, Josh.** What is phishing? How this cyber attack works and how to prevent it. *CSO Online.* [Mrežno] 8. prosinac 2017. [Citirano: 2. ožujak 2018.] https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
23. **Alsharnouby, Mohamed, Alaca, Furkan i Chiasson, Sonia.** Why phishing still works: User strategies for combating phishing attacks. [Mrežno] 2015. https://www.sciencedirect.com/science/article/pii/S1071581915000993?via%3Dihub.
24. **van Duijn, Rik.** Shortcuts: another neat phishing trick. *d.uijn.nl.* [Mrežno] 28. prosinac 2016. [Citirano: 29. ožujak 2018.] https://d.uijn.nl/2016/12/28/shortcuts-another-neat-phishing-trick/.
25. **Gudkova, Darya, i dr.** Spam and phishing in 2017. *Securelist - Kaspersky Lab's cyberthreat research and reports.* [Mrežno] 15. veljača 2018. [Citirano: 2. ožujak 2018.] https://securelist.com/spam-and-phishing-in-2017/83833/.
26. **Arntz, Pieter.** Surfacing HTA infections. *Malwarebytes Labs.* [Mrežno] 13. rujan 2016. [Citirano: 29. ožujak 2018.] https://blog.malwarebytes.com/cybercrime/2016/09/surfacing-hta-infections/.
27. **Narang, Rishi.** The infamous issue of target _blank code. *Cyber Sins Security Blog.* [Mrežno] 8. rujan 2016. [Citirano: 29. ožujak 2018.] https://cybersins.com/target-blank-vulnerability-phishing/.
28. **Microsoft Secure.** The new .LNK between spam and Locky infection. [Mrežno] 19. listopad 2016. [Citirano: 29. ožujak 2018.] https://cloudblogs.microsoft.com/microsoftsecure/2016/10/19/the-new-lnk-between-spam-and-locky-infection/.
29. **CBS News.** The phishing email that hacked the account of John Podesta. [Mrežno] 28. listopad 2016. [Citirano: 2. ožujak 2018.] https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/.
30. **Mitnick, Kevin D. i Simon, William L.** *The art of deception: Controlling the human element of security.* s.l. : John Wiley & Sons, 2011.