Centar Informacijske Sigurnosti

Prijevare na socijalnim mrežama

ožujak 2012.

CIS-DOC-2012-03-043

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Socijalna mreža je usluga na Internetu odnosno platforma ili web stranica s ciljem izgradnje odraza mreža ili veza među ljudima koji, na primjer, imaju iste interese ili aktivnosti. Socijalnim mrežama danas se koristi cijeli svijet, a osim onih neutralnih (opće uporabe) postoje i servisi s određenom namjenom u odnosu na sadržaj i profil korisnika. Servis socijalne mreže sastoji se od prikaza pojedinog korisnika (korisnički profil), korisnikovih socijalnih veza te mnoštva dodatnih usluga i sadržaja. Većina socijalnih mreža zasniva se na webu te pruža sredstva za interakciju korisnika putem Interneta, kao što su elektronička pošta i izravne poruke. Putem socijalnih mreža korisnici mogu dijeliti svoje ideje, aktivnosti, događaje i interese s odabranom skupinom ljudi. Glavni tipovi servisa socijalnih mreža su oni koji sadrže kategorije kao što su završene škole ili školski kolege omogućuju njihovo međusobno povezivanje. Socijalne mreže na Internetu jedan su od najznačajnijih tehnoloških fenomena 21. Stoljeća, čiji broj korisnika jako brzo raste već nekoliko godina. Primjer je socijalna mreža MySpace koja je u lipnju 2007. godine bila najposjećenija web stranica u SAD-u s 114 milijuna svjetskih posjetitelja, a to je predstavljalo 72% porasta korisnika u odnosu na 2006. godinu.

Svojstva koje određuju socijalne mreže su navedena u nastavku:

- Na socijalnim mrežama postoje alati za postavljanje osobnih podataka na profil korisnika i sadržaji koje je napravio korisnik povezani s njegovim interesima i osobnim životom.
- Mreže sadrže alate za osobnije, društveno usmjerene interakcije koji se zasnivaju oko korisničkog profila (npr. preporuke, rasprave, blogovi, organizacija socijalnih događaja koji nisu na Internetu, izvješća događaja).
- Alati za opisivanje društvenih odnosa koji određuju tko ima pristup podacima dostupnima na socijalnim mrežama te tko s kim može komunicirati. Socijalne mreže mogu se promatrati kao neformalni, ali sveobuhvatni alati za upravljanje identitetom i oni određuju pristup sadržaju koji je napravio korisnik putem socijalnih odnosa. Osjećaj povezanosti i intimnosti koji inače postoji u zajednici, sada se nalazi i u zajednicama na Internetu. Postoji značajan društveni kapital povezan s korištenjem socijalne mreže Facebook među studentima u SAD-u, koji sugerira kako korištenje socijalnih mreža može doprinijeti povećanju samopouzdanja i zadovoljstva u životu.
- Alati koji omogućavaju pronalazak istomišljenika i interakciju između njih.
- Alati za upravljanje identitetom i kontrolom pristupa za sadržaj koji je stvorio korisnik, dozvoljava korisnicima kontrolu nad time tko može vidjeti njihove podatke, što nije općenito dopušteno na blogovima.
- Forum s novim načinom suradnje na Internetu, edukacija, dijeljenje iskustva i povjerljivih informacija, kao što su prikupljanje i razmjena reputacije za tvrtke i pojedince.

Uz pogodnosti koje donose članovima, socijalne mreže imaju značajnu poslovnu vrijednost zbog marketinških programa koje nude. Na njima se korisnici besplatno prikazuju i dobrovoljno otkrivaju detalje svojih društvenih odnosa. Brojke govore same za sebe: socijalna mreža MySpace prodana je 2005. godine za cijenu koja odgovara otprilike 35$ po korisničkom profilu. U 2006. godini socijalna mreža Facebook procijenjena je na 2 milijarde američkih dolara, što bi bilo 286$ po korisničkom profilu, a do rujna 2007. godine ova vrijednost je narasla puno više. Budući da uspjeh socijalnih mreža ovisi o broju korisnika koji privuče, nastaje pritisak na pružatelje ove usluge koji potiče razvoj za povećanjem broja korisnika i njihovih veza. Kao i kod svake brzo rastuće tehnologije, sigurnost i privatnost korisnika nisu bili na prvom mjestu u njihovom razvoju. Rezultat toga je, uz navedene prednosti, nastanak značajnog rizika sigurnosti i privatnosti. Korisnici često nisu svjesni koliko drugih korisnika pristupa njihovom korisničkom računu i privatnim podacima. Stvoren je osjećaj prisnosti između „digitalnih prijatelja“ te često dovodi do neprimjerenih ili štetnih objava. Općenito se sve svodi na to da što veći broj prijatelja korisnik tima to je popularniji i ima veći utjecaj. U usporedbi sa stvarnim životom, članovi socijalnih mreža dijele informacije s drugim korisnicima puno lakše, bilo po izboru ili greškom.

Prirodna je ljudska želja biti povezan s drugim ljudima i to u kombinaciji s tehnologijom socijalnih mreža dovodi do sklonosti prihvaćanja zahtjeva za prijateljstvom od osoba koje u stvarnom životu čovijek ne poznaje. Korisnici imaju sve manji prag za prihvaćanje zahtjeva za prijateljstvom. Ovo naravno nije točno za sve korisnike ili sve zajednice. Međutim to je dominantni pokretač, budući da teži brzom rastu mreže te neizbježno utječe na web stranice s najvećim brojem korisnika. Ovo

ugrožava obranu korisnikovih podataka na socijalnim mrežama i mogućnosti ograničavanja pristupa manjim skupinama kontakata te također doprinosi opasnosti od računalnih virusa i crvi. Takve mogućnosti zajedno s prijetnjama koje zadaju drugi podaci koji su otkriveni pružateljima usluge, ukazuju na to da je potrebno preispitati dosadašnju praksu na socijalnim mrežama s obzirom na zaštitu podataka. O sigurnosti socijalnih mreža i prijetnjama koje se na njima javljaju bit će više riječi u drugom poglavlju. U trećem poglavlju opisuju se vrste prijevara na socijalnim mrežama (nove prijevare, ali i stare prijevare koje su se raširile na socijalnim mrežama). Prijevarama koje se spominju stalno u medijima možete više pročitati u četvrtom poglavlju. Peto poglavlje govori o tome kako se korisnik može zaštiti na socijalnim mrežama. Zadnje poglavlje govori o budućnosti prijevara na socijalnim mrežama.

2. Sigurnost socijalnih mreža

Ovo poglavlje opisuje najvažnije prijetnje privatnosti i sigurnosti koje su povezane sa socijalnim mrežama. Cilj je usmjeriti se na prijetnje koje su specifične za socijalne mreže, umjesto na one koje su zajedničke svim web aplikacijama, osim ako ne postoji posebna inačica takvih prijetnji za socijalne mreže ili se prijetnja proširila nekom određenom značajkom socijalnih mreža.

2.1. Prijetnje povezane s narušavanjem privatnosti

Korisničke profile na socijalnim mrežama mogu drugi preuzeti na računalo i pohraniti tijekom vremena te stvoriti digitalni dosje s osobnim podacima. Informacije koje korisnici otkriju na socijalnim mrežama mogu se koristiti u druge svrhe i u kontekstu koji je različit od onog kojeg je vlasnik profila uzeo u obzir. Obzirom na znatno smanjeni trošak pohrane podataka na diskove i preuzimanje s Interneta, moguće je spremiti snimke cijele mreže i pohraniti profile članova na duže vrijeme. Informacije koje se nalaze u pojedinom profilu mogu se jednostavno skupiti kako bi se pratile i istaknule promjene. Sve je više privatnih svojstava kojima se može izravno pristupiti pregledavanjem profila do kojih se može doći pretraživanjem Interneta što čini zajedničku ranjivost socijalnih mreža. Upisivanjem korisnikovog imena u Internet tražilicu dostupan je profil korisnika i njegove fotografije na socijalnim mrežama MySpace**,** Facebook i drugima, osim ako zadane postavke privatnosti nisu promijenjene.

Pojavljuju se ranjivosti povezane s prepoznavanjem lica. Trenutna provjera privatnosti na fotografijama koje se postavljaju na socijalne mreže ne uzima u obzir mogućnost preuzimanje fotografija na temelju sadržaja (eng. *Content-based Image Retrieval* - CBIR), a to je izvorno napravljeno za digitalnu forenziku. Ova ranjivost detaljnije je opisana u poglavlju 3.1.

2.2. Socijalne prijetnje

Uhođenje obično uključuje prijeteće ponašanje u kojem počinitelj više puta traži fizički kontakt sa žrtvom ili njen telefonski broj. Događa se uhođenje i na Internetu kroz elektroničku poštu, izravne poruke i poruke na socijalnim mrežama. Ne postoji puno pouzdanih podataka o uhođenju, ali podaci koji su dostupni pokazuju povećanje pokušaja uhođena na socijalnim mrežama. One potiču objavljivanje osobnih informacija, uključujući podatke koji mogu otkriti lokaciju korisnika i njegov raspored (na primjer postoji mjesto gdje se može upisati adresa stanovanja, telefonski broj ili raspored predavanja i drugo). Pomoću aplikacija koje korisnik koristi na Internetu može se vidjeti kada je kod kuće, primjer toga je profil za izravne poruke koji može otkriti je li korisnik spojen na Internet. Računalno uznemiravanje (eng. cyberbullying) je naziv koji opisuje stalne i namjerne radnje u kojima se nanosi šteta korisniku, a provodi se korištenjem tehnologije, točnije mobilnih telefona i Interneta. Istraživanje u ovom području je u povojima zajedno s kvantitativnim istraživanjem drugih oblika zlostavljanja, a statistika varira od istraživanja do istraživanja. No, ono što je očito je kako prijavljeni slučajevi nasilja putem socijalnih mreža rastu.

Napadi socijalnog inženjeringa koji koriste socijalne mreže rastu te su često podcijenjeni rizik za IT (eng. *Information Technology*) infrastrukturu tvrtki. Ovo je sredstvo napada koje često koriste hakeri odnosno napadači kako bi zaobišli sigurnosni sustav i imali pristup osjetljivim informacijama poduzeća. Napadači ne koriste tehnologiju za ovu vrstu napada, iako i ona može biti uključena, nego koriste zaposlenike. Podaci se često stječu suptilno i prikupljaju dio po dio. Socijalne mreže mogu biti posebno važno oruđe u organiziranom napadu socijalnog inženjeringa na neko poduzeće. Neke informacije su potrebne kako bi se pristupilo zajednici na Internetu, no često su postavke privatnosti zanemarene te je zbog toga nizak prag za dobivanje informacija koje se koriste za socijalni inženjering. Nekoliko stručnih socijalnih mreža objavljuje informacije o popisima zaposlenih te se mogu vidjeti čak i veze među njima.

2.3. Sigurnosni rizici na socijalnim mrežama

Socijalne mreže na Internetu su jako dobro mjesta za upoznavanje i povezivanje s ljudima koji dijele slične interese, no mogu predstavljati i ozbiljnu prijetnju sigurnosti korisnika i njihovim tvrtkama. Mnoga poduzeća gledaju na socijalne mreže kao prijateljsko mjesto gdje mogu uspostaviti kontakte, pronaći kupce i prodavače te učiniti popularnijim osobni ili tvrtkin profil. Budući da većina korisnika pristupa socijalnim mrežama iz svojih udobnih i sigurnih domova, mogu dobiti lažni osjećaj sigurnosti i anonimnosti. Nedostatak fizičkog kontakta na socijalnim mrežama može smanjiti korisnikovu prirodnu obranu i dovesti pojedince do otkrivanja informacija koje nikad ne bi otkrili osobi koju su upravo sreli na ulici. Ostati siguran na socijalnim mrežama znači prepoznati određene prijetnje i rizike od kojih će neki biti navedeni u poglavlju 3.

Kako bi korisnik izbjegao prijevare na socijalnim mrežama trebao bi slijediti određena pravila. Prvo što korisnik treba napraviti je biti diskretan. Nikada ne treba pisati nešto na stranicu profila, oglasnu ploču, instant poruke ili neki drugi elektronički oblik za objavljivanje što može izložiti korisnika neželjenim posjetiteljima, mogućnosti krađe identiteta ili zlonamjernim prijetnjama. Ovo uključuje osobna imena, imena tvrtke, adrese, brojeve telefona, naslov posla, datum rođenja, detalji osobnog rasporeda, dnevnu rutinu te informacije o poslu ili obitelji. Puno bolje je komunicirati o općenitim stvarima nego otkriti informacije koje zlonamjerni pojedinci jednog dana mogu iskoristiti.

Treba biti skeptičan jer su stranice socijalnih mreža pune korisnih poslovnih informacija, kao i velike količine beskorisnih dezinformacija. Prema svemu što se vidi na Internetu, kao što su savjeti o dionicama, vijesti, osobni tračevi i druge stvari, treba pristupati s velikim stupnjem skepticizma. Neki korisnici mogu lagati kako bi poboljšali svoj profil, dok drugi mogu govoriti neutemeljene informacije iz šale ili iz neznanja.

Kao treće treba biti promišljen i nikada ne pisati na Internetu podatke koji se mogu iskoristiti za nanošenje štete uključujući uvredljive tvrdnje, klevetu i uvrede. Treba biti profesionalan te uvijek promisliti dva puta prije nego se nešto napiše.

Treba biti profesionalan ako se postavljaju slike ili video sadržaj na društvenu mrežu te se pobrinuti kako predstavljaju korisnike u najboljem svjetlu. Na slikama korisnici trebaju biti prikladno obučeni, jer se na taj način predstavljaju drugim korisnicima.

Četvrto što korisnik treba je biti oprezan. Ljudi na Internetu nisu uvijek oni za koje se predstavljaju. Dok se korisnik ne može samostalno uvjeriti u nečiji identitet nikada ne treba otkriti osobne, poslovne ili financijske informacije.

Posljednja, ali ne i manje važna, smjernica govori da treba provjeriti sigurnosne politike socijalnih mreža. Sve velike socijalne mreže imaju posebne smjernice privatnosti koje su objavljene na njihovim web stranicama. Treba uzeti vremena, pročitati i razumjeti te dokumente, budući da uključuju razne vrste informacija koje će otkriti drugim tvrtkama. Ako se korisniku ne sviđaju uvjeti korištenja, ne treba koristiti usluge jer njihovim korištenjem može postati žrtva prijevare.

2.4. Statistički podaci

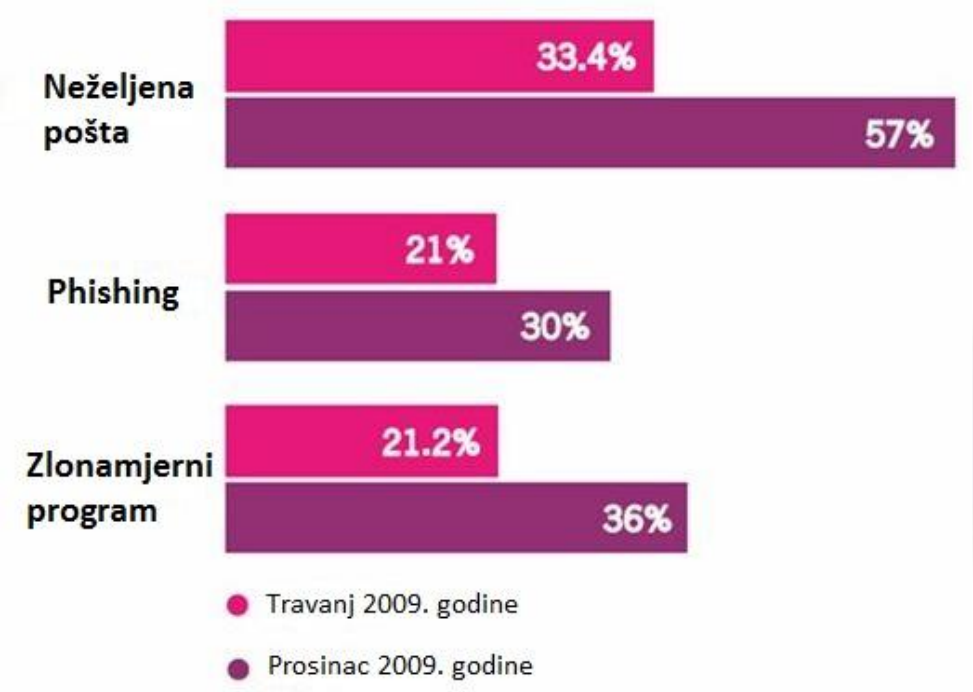
Broj korisnika na socijalnim mrežama svakim danom sve više raste. U Tabela 1. nalazi se prikaz broja korisnika u svijetu koji pripadaju pojedinim socijalnim mrežama. U početku su socijalnim mrežama pristupali mlađi korisnici Interneta koji imaju između 18 i 30 godina te je došlo do zasićenja. Nakon toga počeli su pristupati i stariji korisnici koji imaju više od 40 godina.

Tabela 1. Broj jedinstvenih korisnika na socijalnim mrežama do studenog 2011. Godine
Izvor: Wikipedia: Social networking service

Socijalne mreže u svijetu	Broj jedinstvenih	Postotak

	posjetitelja	
Facebook	792,999 milijuna	55,1%
Twitter	167,903 milijuna	11,7%
LinkedIn	94,823 milijuna	6,6%
Google+	66,756 milijuna	4,6%
MySpace	61,032 milijuna	4,2%
Ostale	255,539 milijuna	17,8%
Ukupno	1,438 877 milijuna	100%

Na Slika 1. nalazi se prikaz porasta prijetnji na socijalnim mrežama u 2009. Godini. Danas ima sve više i više prijetnji koje su sve učinkovitije. Prevaranti na sve načine pokušavaju prevariti korisnike te im je cilj smisliti što više novih prijetnji koje su korisnicima nepoznate.



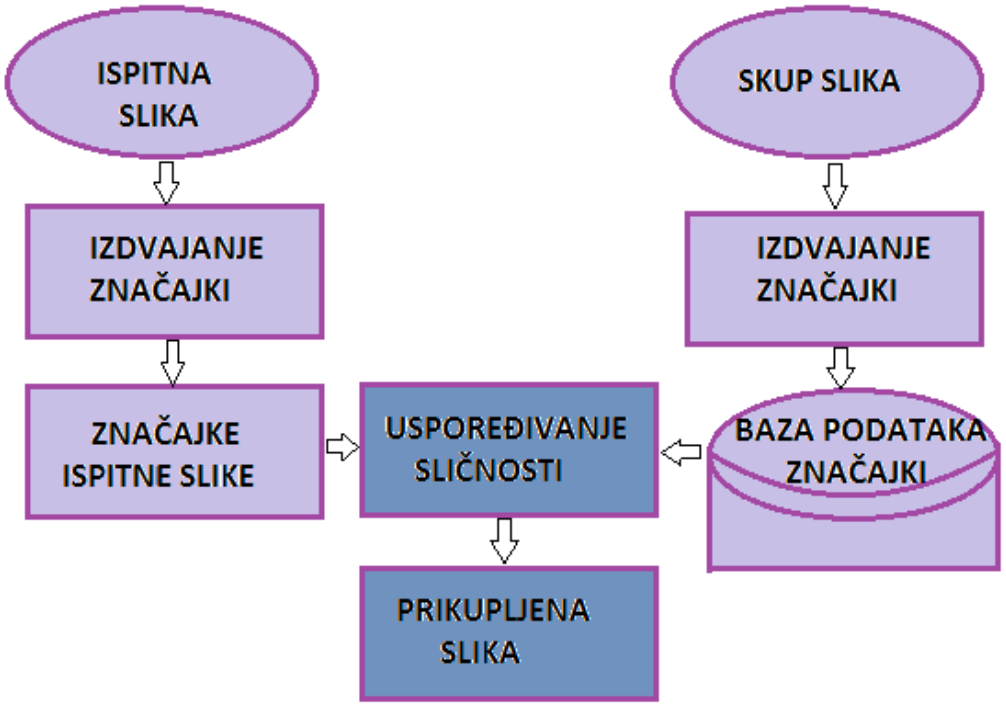
Slika 1. Rast prijetnji na socijanim mrežama u 2009. Godini
Izvor: Social Media Malware, Spam Up 70%

3. Vrste prijevara na socijalnim mrežama

Stručnjaci za sigurnost na Internetu sve su više zabrinuti zbog velikog i brzog rasta prijevara na socijalnim mrežama i napada na članove zajednica na Internetu, kao što su socijalne mreže Facebook**,** MySpace**,** Flickr i LinkedIn. Više od 70 milijuna korisnika Interneta pripada jednoj ili više virtualnih skupina, ali stvarni broj je značajno veći te i dalje brzo raste iz dana u dan. Na konferenciji hakera Black Hat u Las Vegasu govorilo se kako članstvo u nekoj socijalnoj mreži nužno ne daje zaštitu od prijevara na socijalnim mrežama. Bilo tko može otvoriti profil na ime nekog drugog korisnika. Neke od prijevara koje se javljaju na socijalnim mrežama opisane su u nastavku poglavlja.

3.1. Dohvat fotografije na temelju sadržaja

Dohvat fotografija socijalnih mreža na temelju sadržaja moguć je uz pomoć tehnologije CBIR te se zbog toga javlja ranjivost prepoznavanja lica. Trenutne postavke privatnosti za fotografije koje su postavljene na socijalnu mrežu ne uzimaju u obzir CBIR tehnologije i vrlo je malo ljudi svjesno posljedica objavljivanja fotografija zajedno s lokacijama. Dok prepoznavanje lica omogućuje povezivanje podataka profila s fizičkom osobom, CBIR tehnologija dopušta povezivanje podataka lokacije preko prepoznavanja zajedničkih objekata u slikama. CBIR tehnologija ima mogućnost izdvojiti podatke o lokaciji iz naizgled anonimnih profila korisnika koji sadrže fotografije korisnikovih domova. Ovo može dovesti do uhođenja, neželjenog marketinga, ucjenjivanja te drugih prijetnji koje su povezane s neželjenim objavljivanjem podataka o lokaciji.Na **Error! Reference source not found.**. nalazi se prikaz rada CBIR tehnologije.



Slika 2. Prikaz CBIR tehnologije
Izvor: Benchmarking Visual Information Indexing and Retrieval Systems

3.2. Povezanost metapodataka slike, označavanja i unakrsnih fotografija profila

Mnoge socijalne mreže dopuštaju korisnicima označavanje fotografija s metapodacima kao što su ime osobe koja se nalazi na fotografiji te poveznica na profil ili čak adresu elektroničke pošte. Primjer je socijalna mreža Facebook koja dopušta označavanje fotografija s podacima korisničkih profila i adresama elektroničke pošte. Ako određeni korisnik pazi na to koje slike objavljuje o sebi i svojoj lokaciji, njegova privatnost može biti ugrožena slikama koje drugi korisnici stavljaju o njemu. Vrlo malo alata za privatnost na socijalnim mrežama dopušta korisnicima kontrolu nad označavanjem fotografija koje su povezane s njihovim profilima.

3.3. Poteškoće potpunog brisanja računa

Korisnici koji žele obrisati svoj račun sa socijalne mreže, vidjet će kako je najčešće lako obrisati osnovne stranice, ali informacije kao što su javni komentari koje su ostavili će ostati. Osim toga, općenito je nejasno hoće li informacije biti obrisane nakon što se zatvori račun. Primjer su sigurnosna pravila socijalne mreže Facebook u kojima piše kako će korisnik nakon deaktivacije korisničkog računa dobiti elektroničku poruku u kojoj je objašnjeno kako može ponovno aktivirati svoj račun, što znači da se čuva kopija osobnih podataka. Nadalje, osobni podaci ne mogu biti u potpunosti izbrisani, osim ako korisnik ručno ne izbriše sve javne bilješke i komentare na drugim korisničkim profilima. Rizik je u tome što su korisnici izgubili kontrolu nad svojim identitetom i ne mogu ostvariti svoje temeljno pravo na kontrolu svojih osobnih informacija.

3.4. Neželjena pošta

Mnogi pošiljatelji neželjene pošte nastoje iskoristiti eksponencijalni rast socijalnih mreža i slobodni promet koji one pružaju. Ovo je vrlo ozbiljan problem budući da statistika pokazuje kako socijalne mreže zamjenjuju elektroničku poštu u nekim krugovima. Problemi koji su utjecali na elektroničku poštu uskoro bi mogli utjecati na socijalne mreže.

Često korištene tehnike koje koriste pošiljatelji neželjene pošte:

- Korištenje posebnog programa za slanje neželjene pošte na socijalnim mrežama, kao što su FriendBot koji automatizira pozivnice za prijatelje te postavljanje bilješki i komentara.
- Slanje bilješki koje uključuju dodatne poveznice na pornografske ili druge proizvode koji su napravljeni kako bi prodali nešto.
- Pozivnice za prijateljstvom ili korištenjem atraktivnih profila kojima napadači mogu lako navesti nekoga da prihvati pozivnicu. Profil ili pozivnica sadrže poveznice na vanjske web stranice koje oglašavaju proizvode ili navode korisnike na phishing napad. Pomoću phishing napada napadači skupljaju korisničke osjetljive informacije.
- Postavljanje neželjenih komentara na javnim bilješkama ili komentarima. Obično će pošiljatelji neželjene pošte stvoriti što je više prijatelja moguće i usmjeriti se na one korisnike koji imaju javne bilješke, područja za komentiranje ili poruke te se uklapaju u određeni demografski profil. Nakon toga će početi sa slanjem neželjenih poruka.
- Krađa lozinki članovima kako bi umetnuli i promovirali svoje ponude na profilima drugih korisnika. Do nedavno nisu bili dostupni nikakvi filtri za bilješke ili zahtjeve za prijateljstvom. Najbolje što je korisnik mogao učiniti je blokirati bilješke s pošiljateljeve adrese elektroničke pošte. Socijalna mreža MySpace sada uključuje mogućnost za korisnike kojom mogu prijaviti adrese elektroničke pošte zbog slanja neželjenih poruka ili zloupotrebe. No, pošiljatelji neželjene pošte često mijenjaju svoje adrese. Pružatelji usluga socijalnih mreža već su ugradili filtre koji će usporiti korištenje robota (za slanje neželjene pošte) te brisati profile ako otkriju da šalju neželjenu poštu. Rizici su kao i kod drugih vrsta neželjene pošte: opterećenje prometa, gubitak povjerenja, *phishing* i

preusmjeravanje na pornografske stranice. Profili koji su napravljeni isključivo za slanje neželjene pošte i poruka predstavljaju rizik koji je specifičan za socijalne mreže.

3.5. XSS napadi te virusi i crvi

U nekim socijalnim mrežama korisnici mogu postavljati HTML (eng. *HyperText Markup Language*) kod i forume unutar svojih profila. Socijalne mreže su posebno ranjive na XXS (eng. *Cross Site Scripting*) napade jer se puno koriste takozvani dodaci (eng. *widget*) koje su napravili drugi proizvođači. Osim toga, oslanjanje na objavljivanje poruka i virusnog marketinga znači da se virusi na socijalnim mrežama šire jako brzo. Virus SAMY koji je zarazio profile na socijalnoj mreži MySpace proširio se na više od milijun korisnika u samo 20 sati, što ga je učinilo jednim od najbrže raširenih virusa svih vremena. Rezultati ovih ranjivosti su:

- ugroženi korisnički računi,
- uskraćivanje usluge (virus SAMY prisilio je socijalnu mrežu MySpace na privremeno isključenje) i gubitak ugleda,
- preusmjeravanje na *phishing* napad,
- širenje neželjenog sadržaja putem poruka elektroničke pošte.

3.6. Spear phishing

*Spear phishing je inačica phishing napada koja je usmjerena na jednog korisnika.*Postojanje lako dostupnih samostalno stvorenih profila te samostalno proglašenog kruga prijatelja na socijalnim mrežama dopušta napadaču prikupljanje velike količine pouzdanih informacija koje se mogu upotrijebiti za vrlo osobne *phishing* napade. Povezana prijetnja je korištenje socijalnih mreža za *phishing* napade na same socijalne mreže, umjesto skupljanja podataka kako bi se drugdje koristili. Crv JS/Quickspace.A napravljen je kako bi se proširio na stranicama profila socijalne mreže MySpace. Stranice su bile zaražene s poveznicom na *phishing* web stranicu koja je tražila korisničke podatke za prijavu te ih je potom koristila za ugradnju poveznice na *phishing* web stranicu ukradenog profila. Iako je ovo novi način već postojeće prijetnje, dodatno povjerenje koje donosi krug prijatelja na socijalnim mrežama može ovo učiniti izrazito učinkovitim načinom *phishing* napada. Širenje ovakvih vrsta napada povećava se zbog ranjivosti socijalnih mreža na tehnike socijalnog inženjeringa koje se temelje na prodiranju u socijalne mreže s niskim ulaznim pragovima. *Spear phishing* na socijalnim mrežama nosi jednaku količinu rizika kao i druge vrste *phishing* napada uključujući: ugroženo prijavljivanje koje može povećati brzinu širenja *phishing* napada, krađu identiteta, financijsku štetu i narušavanje ugleda.

3.7. Infiltracija u socijalne mreže

Neke informaciju su dostupne samo prijateljima ili članovima ograničene skupine te je ovo prva linija obrane u zaštiti privatnosti na socijalnim mrežama. Budući da je često vrlo lako postati nečiji prijatelj, a ako se netko lažno predstavlja, ovaj mehanizam nije jako učinkovit. Trenutno je čak moguće koristiti skripte kako bi se pozvali prijatelji na socijalnoj mreži MySpace, a raste i količina specijaliziranih komercijalnih programa kao što su Friendbot i FriendBlasterPro. Neke socijalne mreže imaju vrlo široke kriterije za članstvo u mreži te pristup podacima. Primjerice, trenutno se bilo tko s odgovarajućom adresom elektroničke pošte može pridružiti bilo kojoj geografskoj skupini na socijalnoj mreži Facebook te dobiti pristup javim korisničkim profilima ove skupine. Socijalni i komercijalni pritisak je imati što više prijatelja, a to često znači kako će takav korisnik prihvatiti zahtjev za prijateljstvom bez provjere vjerodostojnosti ili prikladnosti korisničkog profila. U jednom istraživanju, antivirusna tvrtka Sophos napravila je stranicu profila za korisnika „Freddi Staur“ (što je anagram od „ID Fraudster“), zelene plastične žabe s jako malo osobnih informacija na svom profilu. Poslali su 200 zahtjeva za prijateljstvom kako bi vidjeli koliko će ljudi odgovoriti na zahtjev te koliko osobnih informacija mogu prikupiti. Rezultati koje su dobili su bili poražavajući. Osamdeset sedam od dvjesto korisnika je prihvatilo zahtjev za prijateljstvom, 72% ispitanika otkriva jednu ili više adresa elektroničke pošte, a 84% ima napisan puni datum rođenja.

Iako ova ranjivost ne stvara puno izravne štete osim što onečišćuje socijalne mreže s nevažnim ili varljivim profilima i smanjuje njihovu korisnost, napadačima omogućuje pristup privatnim informacijama, *phishing* napade te slanje neželjene pošte.

3.8. Krađa profila i narušavanje reputacije

Lažni korisnički profili često su napravljeni na ime poznatih osoba, robnih marki ili kako bi ogovarali ljude koji su poznati unutar određene mreže prijatelja. Ne bi svi profili trebali biti točan prikaz pojedinca koji postavlja profil. Postoje profili mnogih mrtvih slavnih osoba, koji mogu imati veliku edukacijsku vrijednost. Primjerice Galileo ima profil na socijalnoj mreži MySpace i više od 3000 prijatelja. Međutim, kada se lažni profili koriste za zlonamjerne svrhe kao što je kleveta, može biti nanesena velika šteta. Iako je ovo moguće napraviti korištenjem konvencionalnih web stranica, socijalne mreže pružaju dodatnu dimenziju jer:

- povezanost na socijalnim mrežama omogućava lakše uznemiravanjeljudi koji će to najvjerojatnije primijetiti,
- glavna svrha profila na socijalnim mrežama je opisivanje osoba koje predstavljaju, stoga se općenito pretpostavlja kako postoji jedan profil za jednu stvarnu osobu te se pretpostavlja kako je informacije na profilu izradio pojedinac kojeg on predstavlja,
- korisnik koji je cilj napada možda neće moći pristupiti profilu,
- većina socijalnih mreža nudi samo slabu provjeru autentičnosti za registrirane korisnike, slabiju nego za registraciju domene gdje je potrebno dati broj kreditne kartice.

Krađa profila može dovesti do:

- uvreda i osobne štete za korisnika. Lažni profili se koriste za narušavanje reputacije ili ismijavanje nekoga u javnosti iz osvete ili kako bi nekoga ucjenjivali. Ovo nije problem samo za slavne ličnosti. Primjerice, zabilježen je niz incidenata gdje se profili koriste za ismijavanje profesora ili učenika u školama.
- korištenja profila za *phishing* napade kao mamca za naivne korisnike kako bi otkrili informacije. Na primjer, lažni profili se mogu zamaskirati kao korisnikovi prijatelji koji trenutno nije na Internetu te ga je onda lako navesti na otkrivanje osjetljivih informacija,
- korištenje lažnih profila za oglašavanje proizvoda dok se lažni korisnici pretvaraju da su prijatelj ciljanog korisnika,
- pravnog postupaka protiv počinitelja koji nema zlonamjerne motive. Postavljanje lažnog profila može biti zabavna aktivnost koja može imati i edukacijsku vrijednost.

3.9. Računalno nasilje

Cyber nasilje opisano je u poglavlju 2.2., a ovdje će biti opisano kako se nasilje na Internetu provodi na socijalnim mrežama.

Oblici cyber nasilja koji se mogu provesti na socijalnim mrežama su:

- svađe na Internetu s elektroničkim porukama ljutitim i vulgarnim jezikom,
- uznemiravanje, odnosno neprestano slanje štetnih, okrutnih i uvredljivih poruka. Zlonamjerni korisnici se koriste tuđim korisničkim imenom i lozinkom kako bi mogli slati neprikladne poruke prijateljima,
- klevetanje korisnika uspostavljanjem novog računa kako bi se lažno predstavljali te na taj način ponizili određene korisnike, slanjem ili objavljivanjem tračeva i glasina kako bi naškodili ugledu ili prijateljstvu korisnika. Primjerice, objavljivanje šala, stripova, tračeva i glasina koji su svi usmjereni na jednu osobu. Također uključuje, objavljivanje štetnih, neistinitih i okrutnih izjava ili fotografija te pozivanje ostalih korisnika na isto,
- lažno predstavljanje i slanje ili objavljivanje informacije kako bi se ta osoba dovela u neprilike, opasnost i narušavanje ugleda ili prijateljstva,
- dijeljenje nečije tajne ili neugodne informacije ili slike na Internetu,
- nagovaranje određenog korisnika na otkrivanje svojih tajni ili sramotnih informacija, a zatim dijeljenje te informacije na Internetu,

- namjerno i okrutno isključivanje određene osobe iz skupine na Internetu. Primjerice skupina prijatelja odlučuje ignorirati određenog pojedinca,
- uhođenje tipično povezano s problematičnom intimnom vezom, uznemiravanjem i klevetanjem koje uključuje prijetnje te stvara značajan strah,
- prijeteće ponašanje koje može biti izravno ili neizravno,

3.10. Špijunaža tvrtki

Ova ranjivost je opisana u poglavlju 2.2. Glavni rizik koji se javlja zbog ove ranjivosti je gubitak intelektualnog vlasništva poduzeća. No, dobivanje pristupa može biti komponenta za široki raspon drugih zločina, kao što je napadanje tvrtke poduzeća kako bi se nanijela šteta, ucjenjivanje zaposlenika kako bi otkrili osjetljive informacija i drugo.

4. Stvarne prijevare na socijalnim mrežama

U ovom poglavlju bit će opisane neke od prijevara na socijalnim mrežama koje su odjeknule u medijima.

Kako je socijalna mreža Facebook dobivala popularnost, tako je postala glavna meta za napadače i pošiljatelje neželjene pošte. Sve veći broj korisnika ima ugrožen korisnički račun. Svaki novi ugroženi korisnički račun koriste napadači kako bi proširili svoje prijevare. Neke od prijevara na socijalnim mrežama s naglasnom na socijalnu mrežu Facebook opisane su u nastavku.

4.1. Reklame za IQ kviz

Tijekom prošle godine socijalna mreža Facebook pokušavala je smanjiti broj pogrešnih reklama na svojim web stranicama. No, činjenica je kako mali postotak korisnika još uvijek vjeruje ovim pogrešnim reklamama te kupuje proizvode koje zapravo ne žele. Prijevara IQ kviz postala je sveprisutna na socijalnoj mreži Facebook i oni korisnici koji instaliraju ovu aplikaciju onda mogu vidjeti reklamu za „IQ Quiz Scam“. U prosincu 2009. godine uhvaćen je jedan razvojni programer aplikacija koji je koristio tehnike slanja neželjene pošte kako bi pridobio nove korisnike koji bi instalirali aplikaciju te na kraju odabrali reklamu za IQ kviz.

Čim korisnik klikne na jednu od reklama, bit će preusmjeren na web stranicu gdje će mu biti postavljeno 10 pitanja na koja je relativno lako odgovoriti. Nakon toga od korisnika će se tražiti unos njegovog broja telefona kako bi mogao vidjeti rezultate. Ako korisnik unese svoj broj telefona to će mu se skupo naplatiti. Izgled aplikacije za IQ kviz nalazi se na Slika 3. Ukoliko se korisnik želi zaštititi od ovakvih prijevara, ne smije unositi svoj broj telefona na ovakve web stranice.

Slika 3. Prijevara na socijalnoj mreži Facebook, IQ kviz
Izvor: 5 Facebook Scams You Should Protect Yourself From

4.2. Prijevara o slanju novca

Dok korisnik pretražuje po web stranici socijalne mreže Facebook, odjednom dobije poruku od prijatelja kako je zapeo u nekoj drugoj zemlji i da je opljačkan, nema novčanik te mu je potreban novac kako bi izašao van iz zemlje. Od korisnika se traži da pošalje novac putem usluge Western Union. Prije svega treba razmisliti i uvidjeti koliko je ovaj scenarij sulud jer ako je korisnik stvarno izvan zemlje te je opljačkan, prvo bi otišao na policiju i zatražio pomoć umjesto traženja novca preko socijalne mreže.

U većini slučajeva najčešće se radi o prevarantu koji je ukrao korisnički račun te od prijatelja na ukradenom profilu traži novac. Na Slika 4. nalazi se izgled usluge Western Union.

Slika 4. Prijevara na socijalnoj mreži Facebook, traženje novca
Izvor: 5 Facebook Scams You Should Protect Yourself From

4.3. Phishing prijevare

Phishing prijevare su jedan od najčešćih načina kako korisnički račun na socijalnoj mreži Facebook postaje ugrožen. Napadač ugrozi korisnički račun te ga potom koristi kako bi automatski objavljivao poveznice na zid (eng. wall) svih korisnikovih prijatelja. Ponekad sustav šalje poruke prijateljima s naslovom „Pogleda ovaj smiješni video sebe!“ (eng. *“Check out this funny video of you!”*), a u poruci se nalazi poveznica koja preusmjerava na lažnu web stranicu za prijavu na socijalnu mrežu Facebook, kao što prikazuje Slika 5.Iako je vrlo lako je izbjeći ovu vrstu prijevare, opet je jako puno korisnika prevareno upravo na opisani način. Najlakši način kako razlikovati je li ovo prijevara ili nije je pogledati URL (eng. *Uniform Resource Locator*) adresu web stranice na koju je preusmjeren korisnik. Ako URL adresa na koju je korisnik preusmjeren nije jednaka očekivanoj, onda se radi o prijevari. Najbolji način zaštite je uvijek ponovno u Internet preglednik upisati poveznicu na socijalnu mrežu Facebook, http://www.facebook.com, jer se na taj način korisnik može osigurati da se prijavljuje na pravu web stranicu.

Slika 5. Lažna web stranica za prijavu na socijalnu mrežu Facebook
Izvor: 5 Facebook Scams You Should Protect Yourself From

4.4. Crv Koobface

Tvrtka Facebook je naporno radila na sprječavanju crva Koobface, ali se on nastavio širiti. U napadu ovog crva korisnik dobiva poruku koja izgleda kao da dolazi od nekog od njegovih prijatelja. U poruci pišu stvari kao: “Paris Hilton Tosses Dwarf On The Street; Examiners Caught Downloading Grades From The Internet; Hello; You must see it!!! LOL. My friend catched you on

hidden cam; Is it really celebrity? Funny Moments" i mnogi drugi natpisi. U poruci će se nalaziti i poveznica koja bi trebala voditi na web stranicu YouTube. Ako korisnik klikne na video, od njega će se tražiti nadogradnja programa „Flash player" te će ga se tražiti preuzimanje dokumenta koji sadrži crva Koobface, a on automatski otima korisnički račun. Ukoliko korisnik preuzme i instalira ovu datoteku bit će automatski prijavljen na socijalnu mrežu Facebook te će slati slične poruke svojim prijateljima. Najbolji način za izbjegavanje ove vrste prijevare je izbjegavanje svih neobičnih poveznica koje se nalaze na zidu korisnika ili u ulaznoj pošti. Također, nikada ne treba preuzimati datoteku nakon što se klikne na poveznicu.

4.5. Drugi zlonamjerni programi i poveznice

Napadači i pošiljatelji neželjene pošte stalno razvijaju svoje strategije za krađu lozinki i preuzimanje korisničkih računa. Najbolje je uvijek biti svjestan postojanja ovih načina za iskorištavanje te pripaziti na poveznice koje se objavljuju na korisničkim profilima ili se nalaze u ulaznoj pošti. Treba izbjegavati preuzimanje bilo kojih datoteka koje se od korisnika traže.

Neke aplikacije na socijalnoj mreži Facebook su između ostalog koristile alatne trake kako bi programeri zaradili od svojih aplikacija. Neke od ovih alatnih traka mogu značajno naštetiti korisnikovom osobnom računalu. Ako korisnik pogriješi te podlegne nekoj od ovih prijevara, trebao bi odmah promijeniti svoju lozinku.

Poveznice na socijalnim mrežama mogu voditi na web stranice na kojima se nalaze zlonamjerni programi ili koje su napravljene za phishing napad. Ne treba preuzimati sadržaj ako se to nakon klika na poveznicu traži, jer korisnik ne može znati što preuzima. Mogu biti opasne poveznice na korisnikovom profilu, zidu, u privatnim porukama i druge.

4.6. Zlonamjerni program za špijuniranje

Glavni istraživač tvrtke AVG Technologies, Roger Thompson, na svom blogu pisao je o napadu zlonamjernog programa za špijuniranje (eng. spyware) koji koristi socijalnu mrežu Facebook. U ovm napadu napadači stvaraju nove web stranice socijalne mreže Facebook. Iz agencije FBI kažu kako su vidjeli puno ovakvih primjera napada na različitim korisničkim profilima, ali s istom slikom i poveznicom. Iz ovoga je vidljivo kako su napadači pronašli način kako stvoriti korisnički profil na socijalnoj mreži Facebook, što znači kako su pronašli način kako zaobići sustav CAPCHA. Svrha tehnologije CAPTCHA je razlikovanje korisnika Interneta i računala. Svaku radnju koju obavlja automatizirani računalni program moguće je spriječiti s CAPTCHA testom. Za korisnike CAPTCHA test je jednostavan i mogu nastaviti dalje, dok je za računala teško jer nemaju dobar sustav za raspoznavanje kao ljudi.

4.7. Oglasi koji navode korisnike na prijevaru

Savezni regulatori ulaganja izdali su upozorenje u 2010. godini o profinjenoj i brzo rastućoj prijevari koja traži žrtve na socijalnim mrežama. Koristeći reklame na socijalnoj mreži Facebook, napadači privlače koje uvjere kako trebaju pozvati svoje prijatelje. Ova prijevara se zove „investicijski program visokog prinosa" (eng. high-yield investment program - HYIP) i koristi niz web stranica i socijalnih medija, YouTube, Twitter i Facebook, kako bi namamio investitore. Ove reklame su uspješne jer koriste socijalne mreže kako bi primamili mlade i neiskusne žrtve nudeći im naknadu ako preporuče reklame prijateljima.

4.8. Crv koji se širi socijalnim mrežama

Sigurnosna tvrtka Kaspersky upozorava na crva koji se širi socijalnim mrežama. Izgleda kao video isječak koji dolazi korisniku od njegovog prijatelja, ali je to kopija crva koji će pretvoriti

uređaj u zombija[1] u botnet[2] mreži. Ne treba misliti kako je sadržaj na socijalnim mrežama siguran samo zato što ga šalje prijatelj. Ovaj crv se širi na socijalnim mrežama Facebook i MySpace. Zaraženi uređaji prenose crva slanjem poruka prijateljima zaraženih korisnika. Kada se otvori video isječak pokaže se prozor za preuzimanje izvršne datoteke koja izgleda kao posljednja inačica programa Flash Player. Umjesto programa koji se prikazuje to je crv koji će zaraziti još jednu žrtvu. Kada se zaraženi uređaji prijave na socijalnu mrežu oni automatski šalju zlonamjerne poruke novim žrtvama.

4.9. Trojanski konj Zeus

Sigurnosna tvrtka Zscaler ThreatLabZ izvještava kako novi crv na socijalnoj mreži Facebook ubrzano širi trojanskog konja „Zeus Banking Trojan“. On se prijavljuje na socijalne mreže pomoću ugroženih korisničkih računa i ukradenih podataka za prijavu te postavlja fotografije koje korisnici preuzimaju. Nakon toga korisnici prime čuvar zaslona (eng. screen saver) koji sadrži trojanski konj „Zeus Banking Trojan“ i druge zlonamjerne datoteke. Trojanski konj Zeus napravljen je kako bi ukrao podatke za prijavu banaka. Krade osjetljive informacije pomoću phishing napada i unosa s tipkovnice. Jednom kada se instalira na računalo, ovaj zlonamjerni program čeka da korisnik posjeti svoj bankovni račun na Intrnetu te tada potajno uzima informacije o računu.Socijalna mreža Facebook i dalje je na meti napada zlonamjernih programa i daje lagani mehanizam za njihovo širenje. Zlonamjerni program kao Zeus iskorištava mogućnost dijeljenja na socijalnim mrežama i to da korisnici vjeruju svojim prijateljima.

[1] Zombi je računalo koje je zaraženo pomoću iskorištavanja neke ranjivosti. Takvo računalo sadrži skriveni program koji omogućuje upravljanje računalom iz daljine. Najčešće se koristi za izvođenje napada na neko drugo računalo

[2] Botnet mreža sastoji se od niza povezanih računala koja međusobno surađuju i kojima upravlja jedan napadač. Napadači je koriste za napade koji im omogućavaju veću dobit, kao što su: distribuirani napad uskraćivanja usluge (eng. Distributed Denial-of-Service - DDoS), slanje neželjene elektroničke pošte, phishing napadi i napadi krađe identiteta.

5. Zaštita korisnika na socijalnim mrežama

Danas korisnici provode sve više vremena na jednoj ili više socijalnih mreža, kao što su Facebook, Twitter i MySpace. Nažalost, zbog toga ima sve više hakera, kradljivaca identiteta i drugih zlonamjernih napadača. Nakon godina usmjerenosti na korisnike osobnih računala s operacijskim sustavom Windows, računalni zločinci usmjerili su pažnju na velike socijalne mreže. One su popularne mete jer imaju puno potencijalnih žrtava. Samo socijalna mreža Facebook ima oko 845 milijuna mjesečno aktivnih korisnika. Zaštita korisnika na socijalnim mrežama nije puno drugačija od borbe protiv tradicionalnih računalnih napada. Tehnologija može puno pomoći, ali zdravi razum i skepticizam su još važniji. Slika 6prikazuje zaštitu korisnika na socijalnim mrežama.

Slika 6. Zaštita korisnika na socijalnim mrežama
Izvor: Protect Yourself Against Social-Network Scams

5.1. Ažuriranje programa

Ako korisnik ima osobno računalo s operacijskim sustavom Windows, najmanje što treba napraviti je pokrenuti sigurnosni paket na njemu koji je i besplatan. Treba koristiti moderne web preglednike kao što su trenutne inačice web preglednika Internet Explorer, Mozilla Firefox i Chrome. Svi oni imaju ugrađenu tehnologiju koja štiti od lažnih web stranica koje koriste prevaranti na socijalnim mrežama. Također je potrebno preuzeti nove inačice operacijskog sustava jer se u njima nalaze potrebne nadogradnje za sigurnosne propuste.

5.2. Procjena poruka

Svaka poruka koju korisnik dobije na socijalnoj mreži treba se dobro procijeniti, a pogotovo ona koja predlaže korisnicima da slijede poveznicu koja ih vodi na web stranicu na kojoj se nalazi nekakav video isječak ili fotografija. Ako korisnik dobije zagonetnu bilješku od poznanika koja izgleda zanimljivo, prije nego što klikne na nju, trebao bi poslati poruku natrag tom prijatelju i pitati ga što je to. Ako je napadač preuzeo kontrolu nad korisničkim računom nekog prijatelja, korisnik bi mu učinio veliku uslugu upitom o sadržaju koji je od njega dobio jer bi mu na ovaj način to dao do znanja.

5.3. Poveznice

Na socijalnim web stranicama postoji puno skraćenih URL adresa koje su ovakvog oblika: „bit.ly/cXjlkY“, te one preusmjeravaju na web stranice s duljim adresama. Ovakve kratke URL adrese su posebno raširene na socijalnoj mreži Twitter jer postoji ograničenje na 140 znakova u jednoj poruci. Problem skraćenih URL adresa je što se ne može u njima prepoznati gdje stvarno vode, dok se na njih ne klikne. Velika većina takvih poveznica je bezopasna te obično korisna, a socijalna mreža Twitter uvela je mjere za zaštitu korisnika od opasnih odredišta.

5.4. Zaštita lozinki

Ako hakeri provale u korisnički račun na socijalnoj mreži korisnikovog prijatelja i iskoriste ga za slanje neželjene pošte korisniku to može biti neugodno. Vrlo opasno može biti ako isti haker neovlašteno izmjenjuje korisnički račun i pokreće napade. Kako ne bi došlo do preuzimanja korisničkih računa trebalo bi zaštiti lozinke kao vrlo važne informacije, što i jesu. Zaštitu lozinki treba započeti tako da ona bude zagonetna s nasumičnim znakovima, brojevima i rečeničnim znakovima. Trebalo bi ih periodički mijenjati ako nema nikakvih problema, a ako ima naznaka kako je netko preuzeo kontrolu nad korisničkim trebalo bi je odmah promijeniti. Također, mora se pretpostaviti kako su svi neželjeni zahtjevi za korisničkim imenom i lozinkom prijevare.

5.5. Dijeljenje sadržaja

U posljednje vrijeme ljudi su se počeli uzrujavati jer se opasnosti socijalnog umrežavanja u virtualnom svijetu pojavljuju i u stvarnom svijetu. Popularna aplikacija za pametne telefone „Foursquare“ omogućuje korisnicima da obavijeste svoje prijatelje na socijalnim mrežama gdje se trenutno nalaze. Korisnici se pomoću aplikacije prijavljuju na označenim lokacijama, restoranima, noćnim klubovima i društvenim događanjima. Kao upozorenje na ovu nepotrebnu funkcionalnost, neki su korisnici pokrenuli stranicu pod nazivom „Molim vas opljačkajte me“ (eng. *Please Rob Me*) koja je objavljivala sadržaj s mobilne aplikacije Foursquare.

6. Budućnost

U budućnosti se može očekivati sve više korisnika koji su članovi jedne ili više socijalnih mreža. Korisnici će sve većim razvojem mobilnih uređaja (pametni telefoni, tablet računala) biti ugroženiji. Mobilni uređaji se mogu lako izgubiti ili ih netko može ukrasti, a korisnici se s njih spajaju na socijalne mreže te će to zlonamjerni korisnici iskoristiti.

Socijalne mreže će sve više biti povezane sa stvarnim životom, kao što već danas postoje aplikacije za pametne telefone koje prate svaki korak korisnika i te podatke objavljuju na socijalnim mrežama. Primjerice mobilne aplikacije koje prate koliko korisnik prijeđe kilometara dok trči ili vozi bicikl. Korisnici takve podatke objavljuju na socijalnim mrežama zajedno s rutom koju su prešli. Sve je veća povezanost s mobilnim uređajima pa tako i sa socijalnim mrežama.

Treba očekivati sve više prijevara na socijalnim mrežama jer svakim danom ima sve više korisnika. Korisnici trebaju biti pažljivi, a to znači paziti što objavljuju i preuzimaju na svoje uređaje. Moraju biti svjesni kako zlonamjerni korisnici iskorištavaju svaku ranjivosti te će smišljati sve bolje prijevare.

U budućnosti treba očekivati nove i maštovitije prijevare jer će prevaranti na sve načine pokušati prevariti nove i stare korisnike. Prevaranti će pokušavati smisliti prijevare koje do sad nisu viđene jer onda korisnici ne znaju što ih čeka, a lažni osjećaj sigurnosti na socijalnim mrežama će ih nagnati na isprobavanje novih stvari.

7. Zaključak

Prijevare na socijalnim mrežama postale su svakodnevne zbog samog fenomena socijalnih mreža. Na njima je lako dijeli sadržaj s drugim korisnicima pa je zbog toga cilj napadača prvo namamiti jednog korisnika, a onda u njegovo ime slati prijateljima zamaskirane prijevare kao video isječke, fotografije i obavijesti koje sadrže poveznice na web stranice na kojima se nalaze prijevare.

Na korisničkim profilima socijalnih mreža nalazi se puno privatnih informacija o svakom korisniku kao što su datum rođenja, obiteljske veze i fotografije. Kada bi ove informacije došle u ruke prevaranta on bi ih mogao iskoristiti za krađu identiteta, narušavanje privatnosti, krađu podataka za prijavljivanje i u druge svrhe. Kradljivci žele što više korisnika prevariti u što kraćem vremenu i smišljaju uvijek nove napade i prijevare.

Javljaju se i socijalne prijetnje i prijevare jer je vrlo lagano pratiti i uhoditi određenog prijatelja. Zlonamjerni korisnici mogu vidjeti sve prijateljeve podatke, znaju kada je prijavljen na socijalnoj mreži, po njegovim objavama mogu zaključiti kada se nalazi kod kuće, odnosno mogu vidjeti gdje se nalazi u pojedinom trenutku te ga na taj način uhoditi.

Zaključak je kako napadači nikada neće odustati, a socijalne mreže su idealno mjesto za njih zbog svih svojih navedenih obilježja. Uvijek će se težiti k smišljanju novih prijevare koje će korisnika namamiti i iskoristiti. Sve je veća povezanost korisnikovog stvarnog života s onim kojeg vodi na socijalnim mrežama pomoću mobilnih uređaja koji ih povezuju. Daljnjim razvojem mobilnih uređaja koji su povezani sa socijalnim mrežama sve se više preklapaju stvarni i virtualni život korisnika i zbog toga treba biti vrlo pažljiv jer se prijevare nalaze na svakom koraku.

8. Leksikon pojmova

XSS napad (Cross-site scripting napad)

Napadačka tehnika koja prisiljava web aplikaciju da korisniku proslijedi zlonamjerni izvršni kod, koji se zatim učitava i izvršava u korisnikovom pregledniku.

https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

URL (Uniform Resource Locator)

URL predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom web poslužitelju.

http://searchnetworking.techtarget.com/definition/URL

Društveni inženjering (Oblik zavaravanja osoba, umjesto računala)

Društveni inženjering je oblik zavaravanja ljudi (a ne računala) kako bi obavili određene radnje ili izdali povjerljive informacije. Glavni cilj društvenog inženjeringa je prikupljanje informacija pomoću kojih će napadač lakše napasti informacijskih sustav ili ostvariti neovlašten pristup.

http://searchsecurity.techtarget.com/definition/social-engineering

Virus (Računalni virus)

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

http://www.ust.hk/itsc/antivirus/general/whatis.html

Phishing (Napad na računalni sustav)

Phishing je način prikupljanja nekih osjetljivih informacija, kao što su korisnička imena, lozinke i detalji kreditnih kartica, zamaskiravanjem u pouzdan entitet elektroničkih komunikacija.

http://www.webopedia.com/TERM/P/phishing.html

Crv (Računalni crv)

Računalni crv je samo-replicirajući zlođudni program koji koristi mrežu računala kako bi poslao vlastite kopije na druge čvorove mreže bez pomoći korisnika. Ovakvo širenje računalnom mrežom je obično posljedica ranjivosti računala.

http://virusall.com/computer%20worms/worms.php

Trojanski konj (Zlođudni program koji se pretvara kao legitimna aplikacija)

Trojanski konj je oblik zlođudnog programa koji se pretvara kao legitimna aplikacija. U početku se pretvara kao da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zlođudnih programa se ne širi samostalno.

http://www.webopedia.com/TERM/T/Trojan_horse.html

Cyber kriminalac (Osoba koja se bavi cyber kriminalom)

Cyber kriminalac je osoba koja koristi računala i Internet za počinjenje kaznenih dijela.

http://www.webopedia.com/TERM/C/cyber_crime.html

Zlonamjerni program (Programi namijenjeni ugrožavanju računalnog sustava)

Zlonamjerni programi (eng. malware) su programi (mogu biti i skripte i kodovi) namijenjeni ometanju operacija u računalu, prikupljanju osjetljivih informacija ili dobivanju neovlaštenog pristupa računalnim sustavima. To je općenit naziv koji se koristi za sve vrste programa ili koda koji su namijenjeni zlonamjernom iskorištavanju računala i podataka u njemu bez korisnikova znanja.

www.wisegeek.com/what-is-a-malware-virus.htm

9. Literatura

[1] The social networking phenomenon that is taking over the world country by country, http://www.independent.co.uk/news/media/the-social-networking-phenomenon-that-is-taking-over-the-world-country-by-country-1849468.html, prosinac 2012.

[2] The Social Networking Phenomenon, http://www.marcy.com/blog/2009/03/04/the-social-networking-phenomenon/, ožujak 2009.

[3] Exploring The Social Networking Phenomenon, http://hassam.hubpages.com/hub/Exploring-The-Social-Networking-Phenomenon, 2009.

[4] Giles Hogben: Security Issues and Recommendations for Online Social Networks, http://fredstutzman.com/papers/ENISA2007.pdf, listopad 2007.

[5] Michael Cooney: FBI warns of social networking fraud, malware escalation, http://www.networkworld.com/news/2009/1001-fbi-social-network-fraud.html, listopad 2009.

[6] Kathy Kristof: Facebook Fraud: Massive Scam Targets Social Networks, http://www.cbsnews.com/8301-505144_162-36942599/facebook-fraud-massive-scam-targets-social-networks/, lipanj 2010.

[7] Nick O'Neill: 5 Facebook Scams You Should Protect Yourself From, http://www.allfacebook.com/facebook-scams-2010-01, siječanj 2010.

[8] Harry McCracken: Protect Yourself Against Social-Network Scams, http://www.foxnews.com/scitech/2010/03/23/protect-social-network-scams/, ožujak 2010.

[9] Focus Editors: The Security Risks of Social Networks, http://www.focus.com/fyi/security-risks-social-networks/

[10] The 5 Most Common Social Networking Scams, http://www.scambusters.org/socialnetworking.html

[11] Elinor Mills: New worm targets Facebook, MySpace, http://news.cnet.com/8301-1009_3-10004970-83.html, kolovoz 2008.

[12] David Cohen: WARNING: Zeus Banking Trojan Targets Facebook Users, http://www.allfacebook.com/facebook-warning-2011-11/, studeni 2011.

[13] Social Media Malware, Spam Up 70%, http://www.marketingprofs.com/charts/2010/3392/social-media-malware-spam-up-70, veljača 2010.

[14] Abebe Rorissa: Benchmarking Visual Information Indexing and Retrieval Systems, http://www.asis.org/Bulletin/Feb-07/rorissa.html, ožujak 2007.