SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINAR

Sigurnost podataka na socijalnim mrežama – Facebook

Saša Šter

Voditelj: doc.dr. Mile Šikić

Zagreb, svibanj 2010.

Sadržaj

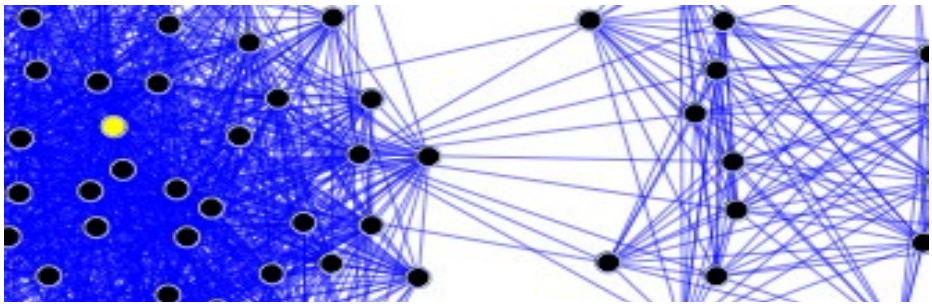
Uvod

U ovom seminaru bi se htio pozabaviti temom socijalnih mreža i sigurnošću podataka na istima. Za početak ću prvo reći par stvari o socijalnim mrežama, koja je njihova uloga kada i kako su nastale i na čemu se zasnivaju. Vrlo je važna pojava na kojoj se one zasnivaju jer je upravo to ono što izrabljuju više manje svi prevaranti i hakeri kada pokušavaju propustit neki virus ili bacit udicu na koju samo čekaju da se netko upeca. Dakle to je pojam teorije mreža kojeg ću se također dotaći. Zatim prelazim na širenje epidemija (virusa i nekih drugih malignih podatkovnih oblika) kroz socijalne mreže. Kojom se to brzinom događa i na koji način. Velik dio mog seminara će se pozabaviti propustima na jednoj od najpopularnijih socijalnih mreža Facebook-u. Također ću reći i par stvari o opasnostima koje prijete našim osobnim podatcima, lozinkama i korisničkim računima. Najčešći je slučaj u zadnje vrijeme da se osobni podaci najlakše pridobivaju i kradu upravo preko socijalnih mreža. Nadam se da će ovaj seminar biti od koristi široj populaciji jer će ljudi više obraćat pozornost na zaštitu podataka i samim time učinit si surfanje internetnom i korištenje socijalnih mreža sigurnijim. Najbitinije od svega će biti, ako uspijem to pokazati, da smo mi sami odgovorni za svoje sigurno surfanje internetnom i da ako nismo naivni i ne padamo na kojekakve prevare, možemo slobodno surfati internetom.

Socijalne mreže

Socijalne mreže su socijalne strukture napravljene od organizacija (odnosno dijelova) koje se zovu čvorovi i koji su vezani(povezani) sa jednim ili više specifičnih tipova međuovisnosti kao što su prijateljstvo, zajednički interesi, novčane razmjene, ljubavne veze, vjerovanja, znanje ili status u društvu.

Ono na čemu se temelje socijalne mreže proučava analiza socijalnih mreža. Ona proučava socijalne mreže kroz prizmu teorije mreže odnosno ono na čemu su i zasnovane (čvorovi i poveznice). Čvorovi su individualni učesnici u mreži, a poveznice su veze između učesnika. Rezultirajući graf je često vrlo kompleksan. Kao što sam već napomenuo postoje mnoge vrste i oblici veza. Čvorovi ne moraju nužno biti ljudi, mogu biti grupe, organizacije, nacije, web stranice itd. Analiziranje mreža ima veliku ulogu u prikupljanju informacija[1].



1.1 Slika dijela Grafa mreža (čvorovi i veze)

Istraživanje provedeno u nekolicini akademskih područja je pokazalo da socijalne mreže operiraju na više razina, od obitelji do nacija, i igraju kritičnu ulogu u načinu na koje su problemi u zadnje vrijeme rješavani, na koje se vode organizacije i razina do koje individualci uspjevaju da postignu svoje ciljeve. Primjeri za to su razne grupe koje nastaju kao podrška određenim cjelinama ili pojavama u društvu što kasnijim djelovanjem dovodi čak i do nekih promjena u društvu i sve češće spominjanje Facebook-a i nekih drugih socijalnih mreža na Hrvatskoj nacionalnoj televiziji također ima utjecaj na društvo u cjelini (slučaj Luke Ritza, razne humanitarne akcije, zabave i događaji, primjer promocije HTC Desire mobitela iz Vipa...).

.

1.2 Slika Facebook grupe za Luku Ritza

1.1 Teorija mreža

Teorija mreža je pojam kojeg sam već spomenuo, a koji je od veliko značaja jer se socijalne mreže upravo zasnivaju na tome. Teorija mreža je područe u računarskoj znanosti i znanosti mreža te dio teorije grafova. Ima mnogo primjena uključujući fiziku čestica, biologiju, ekonomiju i naravno sociologiju. Teorija mreža se bavi proučavanjem grafova kao reprezentaciju simetričnih odnosa ili općenitije kao asimetrične relacije među diskretnim objektima. Primjene teorije mreža su metabolične mreže, genske regulatorne mreže. WWW (world wide web) se također zasniva na tome itd. U brojnim istraživanjima je pokazano da se društveni odnosi mogu prikazati preko kompleksnih mreža[2].

1.1.1 Širenje podataka u kompleksnim mrežama

Širenje podataka u mreži je ujedno iskorišteno i za širenje raznih virusa ili phishing poruka. Podatci u kompleksnim mrežama se mogu širiti na dva bitna načina: očuvano širenje i neočuvano širenje. U očuvanom širenju, količina podatka koja uđe u kompleksnu mrežu ostaje očuvana tijekom svog cijelog prolaza. Model očuvanog širenje je najbolje opisan sa primjerom koji sadrži vrč koji ima fiksnu količinu vode te model još sadrži lijevke i cijevi. Vrč predstavlja izvor podataka dok voda predstavlja podatak koji se širi. Lijevci i pripadajuće cijevi predstavljaju čvorove i poveznice

između njih. Kako voda prelazi iz jednog lijevka u drugi, voda u potpunosti nestaje iz lijevka u kojem se prethodno nalazila. U neočuvanom širenju količina podataka koji uđu i prođe kroz kompleksnu mrežu promjeni se. Model neočuvanog širenja je najbolje opisan sa primjerom slavine i već spomenutih lijevaka i cijevi. U ovom slučaju je slavina beskonačan izvor podataka(voda). Nakon početka širenja i prolaza kroz čvorove i veze oni i dalje ostaju pod utjecajem podataka čak i kad podatci priječu na drugi čvor i veze jer je izvor podataka beskonačan. Takav neočuvani model širenja podataka je najpriklaniji za objašnjavanje prijenosa većine epidemija u našem slučaju virusa i phishing poruka[3].

1.2 Nesigurnost na socijalnim mrežama

Mnoge banke u svijetu, posebno u SAD, imaju problem s krađom pristupnih podataka svojih korisnika. Jednostavno ih netko nazove ili im pošalje elektroničku poštu i zatraži njihov PIN ili druge povjerljive podatke.

Zašto banka stalno zaboravlja moj PIN? Nije li to samo po sebi sumnjivo? Uostalom, banka ima potpuni pristup vašem računu i bez vašeg PINa. Jednostavno, jedini kojem bi vaš PIN mogao zatrebati je onaj tko želi raspolagati vašim računom, a niste vi niti vaša banka. Lako je zaključiti tko preostaje.

Ovaj trend kod nas još nije u toj mjeri uzeo maha, no budite spremni - vjerojatno čeka pred vratima.

1.2.1 Phishing

Ili u prijevodu ribarenje.

Fenomen krađe privatnih podataka na masovnoj skali zovemo phishing. Primite li poruku elektroničke pošte koja od vas traži da negdje upišete svoje tajne podatke, vi ste riba na koju kriminalac vreba.

Kada bi redom nazivali ljude u nekom kvartu predstavljajući se kao bankar i pokušali ih nagovoriti da vam odaju podatke o svom računu, namučili biste se dok ne bi pogodili pravu banku i dovoljno lakovjernog korisnika.

Slanjem masovne elektroničke pošte, ovaj posao mnogo je lakši - zahvaćate doslovno milijune korisnike istovremeno i potpuno vam je svejedno što mnogi od njih nisu čak ni u ciljnoj državi - jednostavno se neće upecati.

1.2.2 Manje od očitog

Phishing nije uvijek trivijalno prepoznati. Uputa u poruci elektroničke pošte da jednostavno provjerite svoje podatke ili pogledate novost na stranici banke ne zvuči nužno loše i ponekad može biti legitimna. No kliknete li na poveznicu unutar poruke da biste otvorili stranicu, pošiljaoc vas je uputio tamo gdje on želi.

 Kada ste upućeni da se negdje prijavite upisujući svoju lozinku ili PIN, obavezno sami upišite adresu u web preglednik, ne koristite poveznicu iz poruke!

1.3 Upozorenje za unos korisničkih podataka

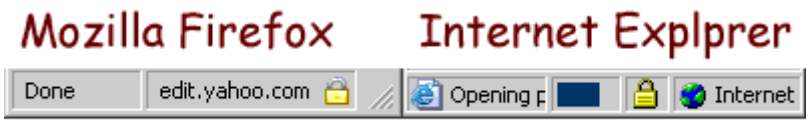
1.2.3 Virtualne otmice

Ne ulazeći u tehničke pojedinosti, web stranice trgovine ili novčarske institucije mogu se "preoteti", odnosno iza onoga što vidite i što izgleda kao vama poznata stranica može stajati kriminalac.

Da bi se ovome stalo na kraj, identitet stranica potvrđuju certifikati. Oni jamče da iza stranice zaista stoji onaj koji se predstavlja.

1.2.4 Provjera identiteta

Za početak provjerite nalazite li se na stranici obuhvaćenoj sigurnom komunikacijom (preduvjet za postojanje certifikata):



1.4 Slika Ispravnog certifikata

Ispravni certifikati prikazuju ovakvu ikonu i vrlo je važno da provjerite je li ona prisutna. Mozilla Firefox osim toga na sigurnim stranicama oboja traku s adresom žutom bojom:

1.5 Slika gdje je traka sa adresom obojana žutom bojom

Ispravni certifikati jednostavno rade - o tome nema posebne obavijesti, osim opisanih znakova da se nalazite na sigurnoj stranici. U slučaju da nešto s certifikatom nije u redu, primit ćete odgovarajuće upozorenje.


Uočite li upozorenje vezano uz certifikat, nikako ga ne ignorirajte! Ova upozorenja znak su da je certifikat neispravan i vjerojatno se radi o lažnoj web stranici. Upisivanje vaših tajnih podataka na toj stranici može rezultirati krađom vaših sredstava!

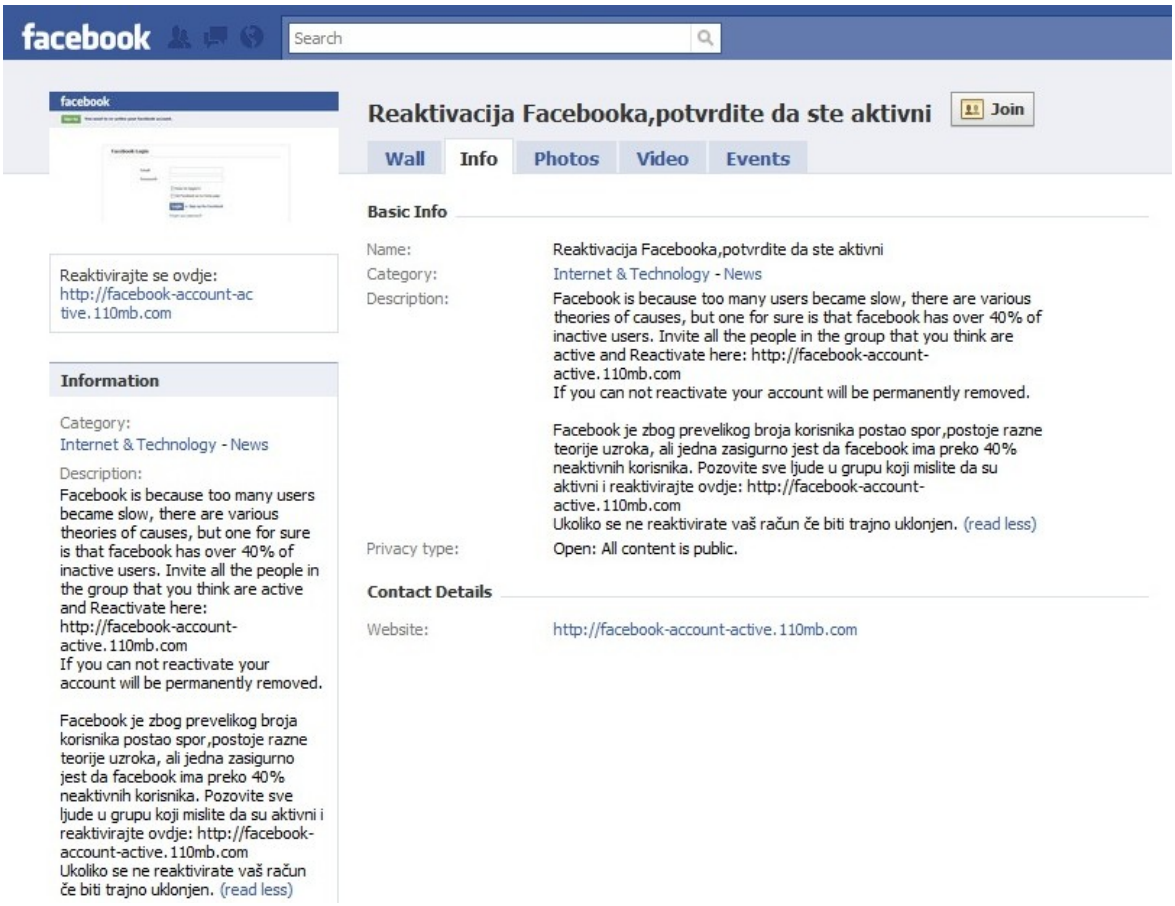
1.6 Upozorenje

Facebook i podatkovne prevare

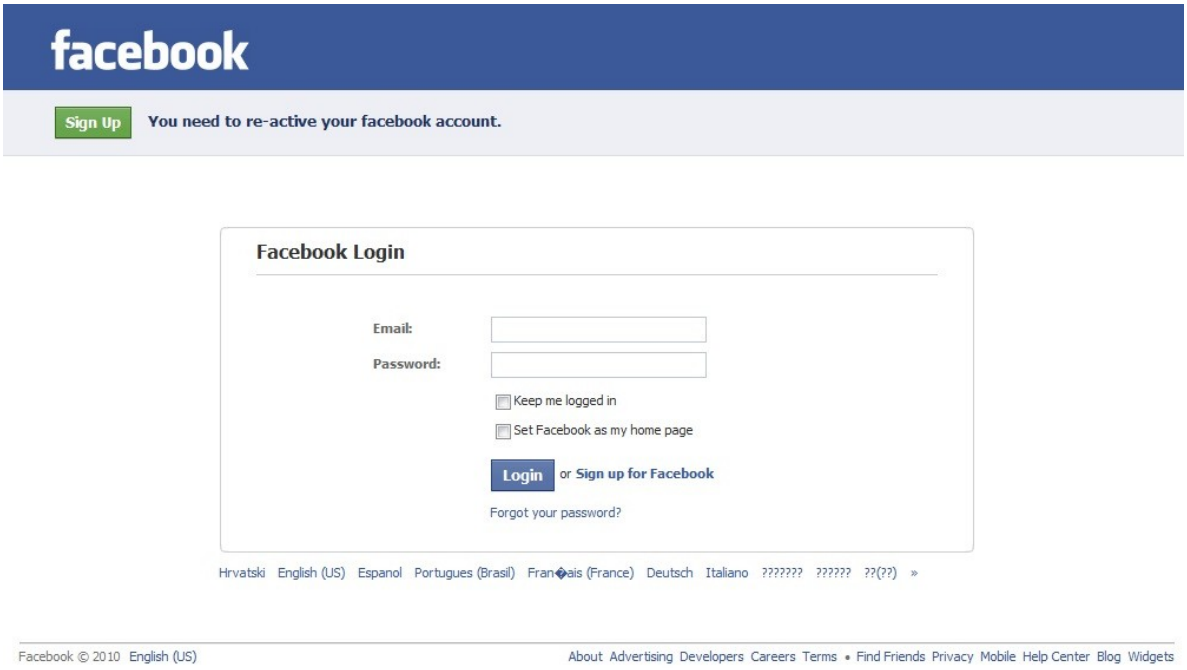
Više manje svaki od ovih navedenih primjera je pronašao svoju ogromnu priliku kako na Facebook-u tako i na ostalim socijalnim mrežama. Facebook kao relativno novi član socijalnih mreža i kao jedan od najposjećenijih trenutno je pravi mal raj za prevarante. S obzirom na sve aplikacije koje se mogu bez ikakvog nadzora stvarati na Facebook-u jasno je da njemu prijeti velika opasnost.

1.3 Lažne grupe

Na Facebook-u postoji gomila načina da se iskoristi glupost i naivnost ljudi i jedan od njih su lažne grupe. Tako će se često dogodit da se pojave grupe sa nazivom " Uključite se u grupu da vam Facebook ne ukine račun", "Gašenje neaktivnih profila – priključi se i pokaži da si aktivan član" i razne druge varijante na temu. Unutar grupe postoji link koji vodi na stranicu koja zahtjeva unos vaših podataka i koja je lažna.



1.7 Primjer lažne grupe



1.8 Primjer za lažnu grupu i lažni link

1.4 Lažne 'Fan page' stranice

Gotovo identičan slučaj koji je sa grupama na Facebook-u takav je i sa 'Fan page'-ovima još jednom od mnogih slobodno korištenih aplikacija. Jedan od novijih slučaja u toj domeni je prijevara sa lažnim 'Gift Cards'-ima (nagradnim bonovima za kupovinu). U zadnje vrijeme se stvorila stvarno hrpa 'Fan page'-ova koji nude predobre da bi bili istiniti bonovi za kupovinu u iznosima od 500$ za hranu, 10$ za Walmart ponude i najveci bon od 1000$ za Ikeu. Na stranicama Ikea-e se može primjetiti da su posredovanje Facebook-a otkrili prevaru i objavili je na svojim stranicama kao SCAM odnosno prevaru, ali ne prije nego je 70 000 ljudi palo na taj trik. Stvar je slijedeća da se na tim stranicama objavljuju lažni postovi koji impliciraju da naravno ti poklon bonovi stvarno funkcioniraju i tako navlače ostale korisnike ali ono što se zapravo događa je da link na toj stranici vodi do neke marketinške web stranice koja pokušava pokupiti podatke o korisniku i generirati promet za oglašivače, po riječima Simon Axten-a, glasnogovornika iz Facebook-a[4]. Iako prevare tipa poklon bonovi već godinama kruže internetom oni su tek novina na Facebook-u.

Što rade iz Facebook-a po tom pitanju? Zbog toga što praktički bilo tko tko ima pristup stranicama Facebook-a može stvoriti 'Fan page', a i zato što stvarno postoje

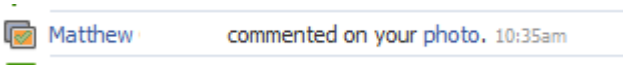
legitimni 'Fan page'-ovi koji nude stvarne bonove , to je jedan kompliciraniji problem za rješiti. Trenutno ono što se radi je to da se praktiči igraju opali krticu, odnosno sa timom inženjera prate probleme i brišu grupe, aplikacije i stranice čim ih pronađu. Naravno da postoje pokušaji da se stekne prednost i nekako optimizira rješavanje problema i u neku ruku da se preteknu prevaranti te s time smanje broj prevarenih korisnika i vrijeme utrošeno na rješavanje tih problema. Evo što kaže po tom pitanju Axten – " Počeli smo stvarati automatski sistem koji će detektirati sumnjive podatke i ponašanja puno brže nego što su i prijavljeni"[4].

1.9 Slika sa Ikea-ine stranice

1.5 Opasne aplikacije

Uz mogućnost slobodnog i vrlo jednostavnog kreiranja vlastitih aplikacija na Facebook-u bilo je neizbježno da se prije ili kasnije neki internet negativci okoriste s time, a možda i najplodnije tlo su im aplikacije.

Tako za primjer bi naveo jednu vrlo suptilnu ali vjerujem i vrlo uspješnu prevaru odnosno neku vrstu zaraze. Događa se slijedeće, a to je da vam se pojavi notifikacija inače oblik obavijesti na Facebook-u koja vam govori o trenutnim akcijama koje su vršene nad vašim podacima i interakcijama na Facebook-u i ta obavijest vam kaže recimo da vam je netko komentirao na sliku i to izgleda kao na slici 1.9.



Slika 1.10 Krvi oblik obavijesti

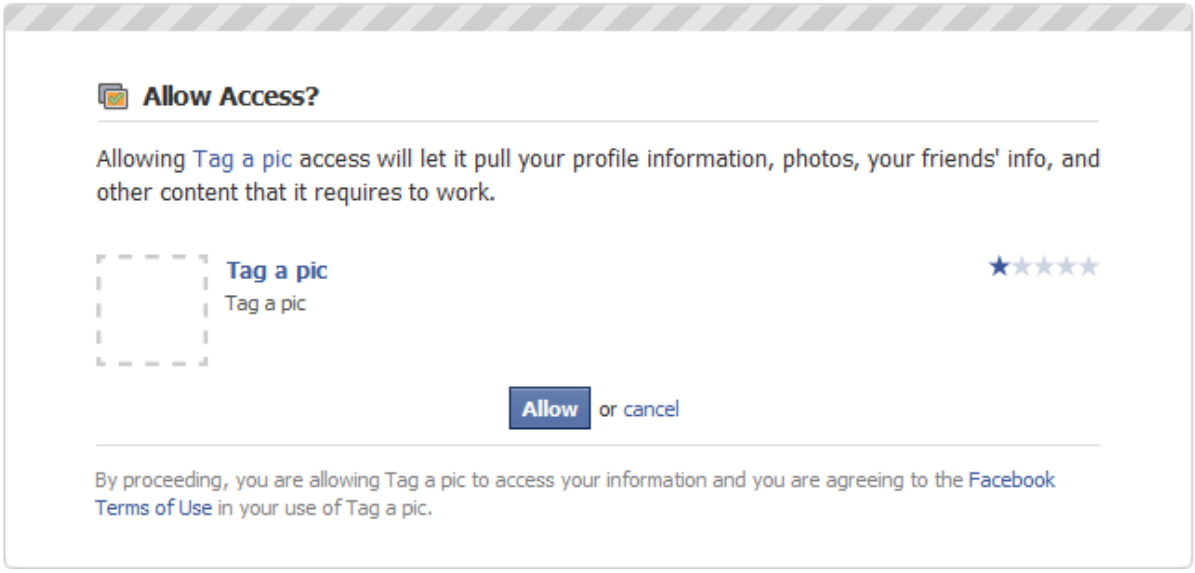
Na prvi pogled brzinski gledano kako to i većina nas radi ne bi primjetili da je u biti oblik te notifikacije krivi jer pravi izgleda ovako kao na slici 1.10. Može se primjetiti da je razlika u hyperlinku (plavim slovima) kod jednog i kod drugog primjera što je naizgled stvarno neprimjetljivo.

Slika 1.11 Pravi oblik obavijesti

Ali zato ono što slijedi kada se klikne na krivi link je itekako primjetljivo, a to je da se ne pojavi odma sadržaj iz obavijesti već jedan novi prozor koji nas navlači na kojekakve zlonamjerne stranice ili viruse ili neke druge oblike zaraza koji su jednako mogući ali ja nisam htio okušati sreću da saznam što se krije iza toga.

Može se primjetiti odma iz slike, odnosno stranice na koju nas krivi hyperlink vuče da nešto s njome ne štima. Za početak nema slike u aplikaciji što je kod regularnih aplikacija obvezan slučaj i ocjena je za tu aplikaciju samo jedna zvjezdica što je oblik rangiranja Facebook aplikacija i što nam govori da je ova aplikacija poprilično loša što ne mora nužno značiti da je zlonamjerna i zadnje ali ne i najmanje bitno je to da aplikacija nema nikakav opis svog djelovanja, ali s obzirom čemu će sve ta aplikacija

imati pristup svakom malo iskusnijem korisniku interneta je jasno da to nije stranica kojoj bi htjeli dati dopuštenje za tako nešto.



1.12 Aplikacija sa zlim namjerama

Još jedna od takvih aplikacijskih prevara koja nije nužno sama aplikacija na Facebook-u nego ranije spomenuti 'Fan page' koji vodi do te aplikacije koja se zove 'Chameleon' i trebao bi služiti za namještanje Facebook pozadine tj. Facebook teme. Ali, prijavljeno je da skidanjm tog programa se javlja upozorenje na antivirusnom programu u kojem govori da program u sebi sadrži trojanca koji ako nije na vrijeme maknut čini to da se neprestano pojavljuju razne reklame na stranicama i blogovima koji se posjećuju i s vremenom ih bude toliko da počnu rušiti učitane stranice. Jedino rješenje je skeniranje cijelog kompjutera i micanje samog korijena te pakosne zaraze što nije nikako lagano.

Pošto internet prevaranti najviše ciljaju na one stvar do kojima je ljudima stalo i na njihovu taštinu i objesnost tako je najednostavnije prevare zapakirati u mejlove koji sadrže već gore spomenute besplatne bonove, promjene na stranici ili u najnovijem slučaju preko lažnih kodova za igrice. Tako se jedna od najnovijih prevara bazira na Zynga igricama na Facebook-u. Svi koji su ikad igrali te igrice vidjeli su rangove svojih prijatelja i vjerujem da većini je postojao uvijek taj netko koga želite pobjediti i/ili prestići, što uopće nije stvar taštine ili nečeg drugog nego samo još jedne od stvari kojima možete zadirkivati prijatelje. Tko ne bi sad prihvatio takvu neku ponudu da uz samo par klikova ima milione na pokeru ili prestigne sve prijatelje u 'Bouncig

Balls'-u, bude najjači u 'Mafia Wars'-ima ili u 'MMA Fighter'-u. Ja znam da ja ne bih ali vjerujem da ima puno ljudi koji bi to učinili, pogotovo onih još vrlo mladih i naivnih i željnih upravi takvih stvari. Aplikacija koje će vas u tom slučaju prevariti zove se 'Zynga toolbar' i izgleda u biti vrlo nevino i čak legitimno se pojavljuje na vrhu vaše alatne trake sa pravim Facebook logom. Ali uz pobliže gledanje i kada se klikne na Facebook logo ste preusmjereni na stranicu koja podsjeća na stranicu originalnog Facebook-a ali je dizajnirana da vam ukrade vaše osobne podatke (u vrhu stranice na slici se može vidjeti lažni 'Zynga toolbar' sa Facebook logom koji vas vodi na krivu stranicu). Nakon unošenja vaših korisničkih podataka se možete pozdraviti sa vašim profilom i za vaše dobro je da odmah promjenite sve ostale vaše pristupne podatke na drugim stranicama pogotovo bankovnim računima, ostalim mail poslužiteljima i raznim drugim stranicama na kojima imate identične pristupne podatke što nije rijedak slučaj[5].

1.13 Lažni Facebook logo

Kao što možemo primjetiti i u ovom slučaju prevara funkcionira gotovo na isti način kao i prethodne, a to je da vas neki lažni link pošalje na neku lažnu stranicu na kojoj ćete pomalo naivno i ne baš tako lažno izgubiti svoje podatke i svoj profil i kompromitirati svoje ostale račune.

1.6 Facebook profili za neznalice

Ne, vi niste tolko zgodni i ne ne izgledate toliko dobro da vas dodaje tako zgodna djevojka i/ili tako zgodan dečko. Ne oni ne padaju na vašu šaljivost i vaše simpatične ironične komentare jer oni ne postoje, oni su tu da vam malo kradu podatke i izrabljuju ih, a usput da i vas vjerojatno zaraze sa kojim virusom, badwareom ili nečim trećim.

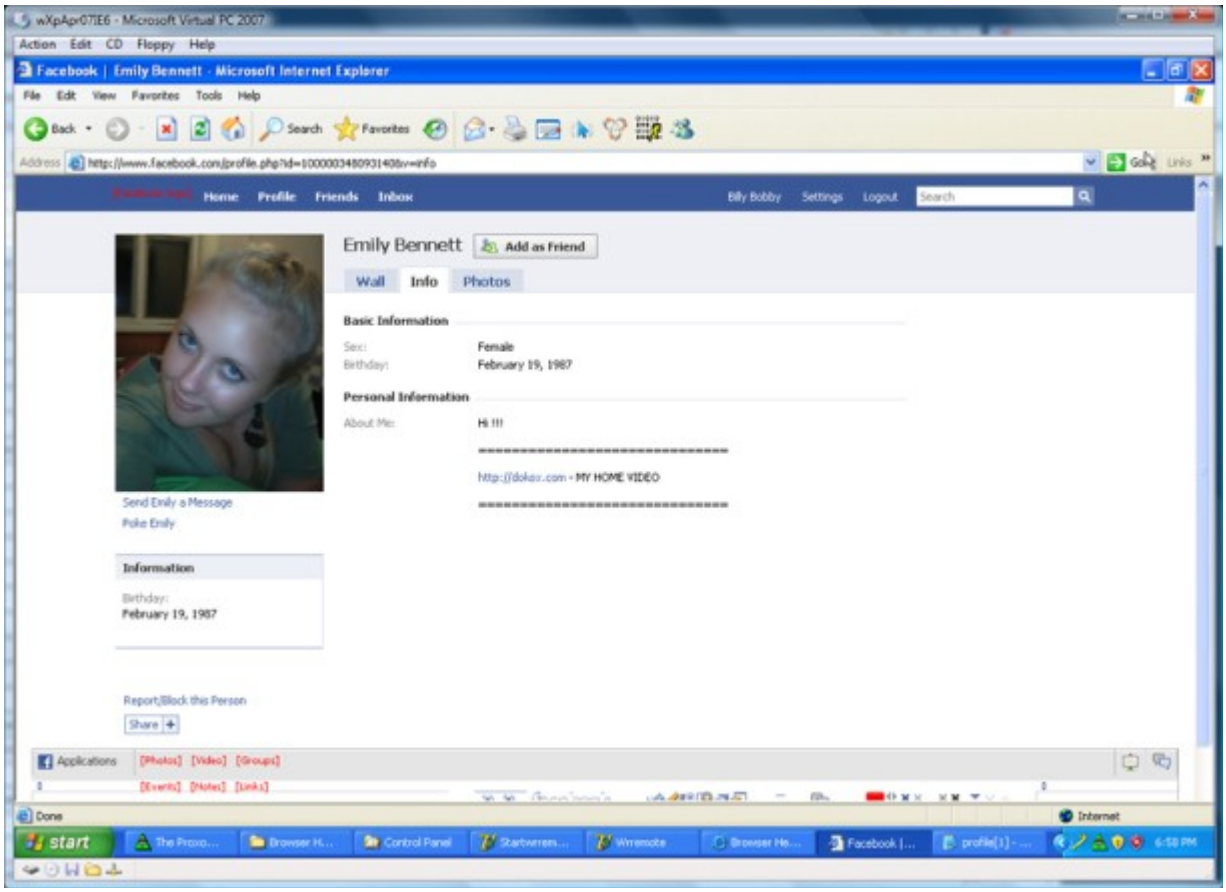
Nedavno je otkriveno da je čak 40% profila na Facebook-u, a vjerojatno i na ostalim socijalnim mrežama lažno. Postavlja se pitanje iz kojih razloga nastaju ti lažni profili? Neki od površnih razloga zbog kojih su nastali profili su nadgledanje i špijuniranje pa čak i testiranje svoje veze odnosno cure/dečka, nadgledanje učenika ili studenata od strane profesora, radi posla odnosno stvaranje dojma da posao cvijeta uz veliki broj obožavatelja i onaj koji nas ovdje interesira radi kompromitiranje korištenja Facebook-a i vaših računa od strane raznih spamera ili internet kriminalaca koji neće stati ni pred čime da vas prevare.

1.14 Pretrazivanje po prezimenu Nikolic je otkrilo veliki broj sumnjvih i vjerojatno neaktivnih/lažnih profila

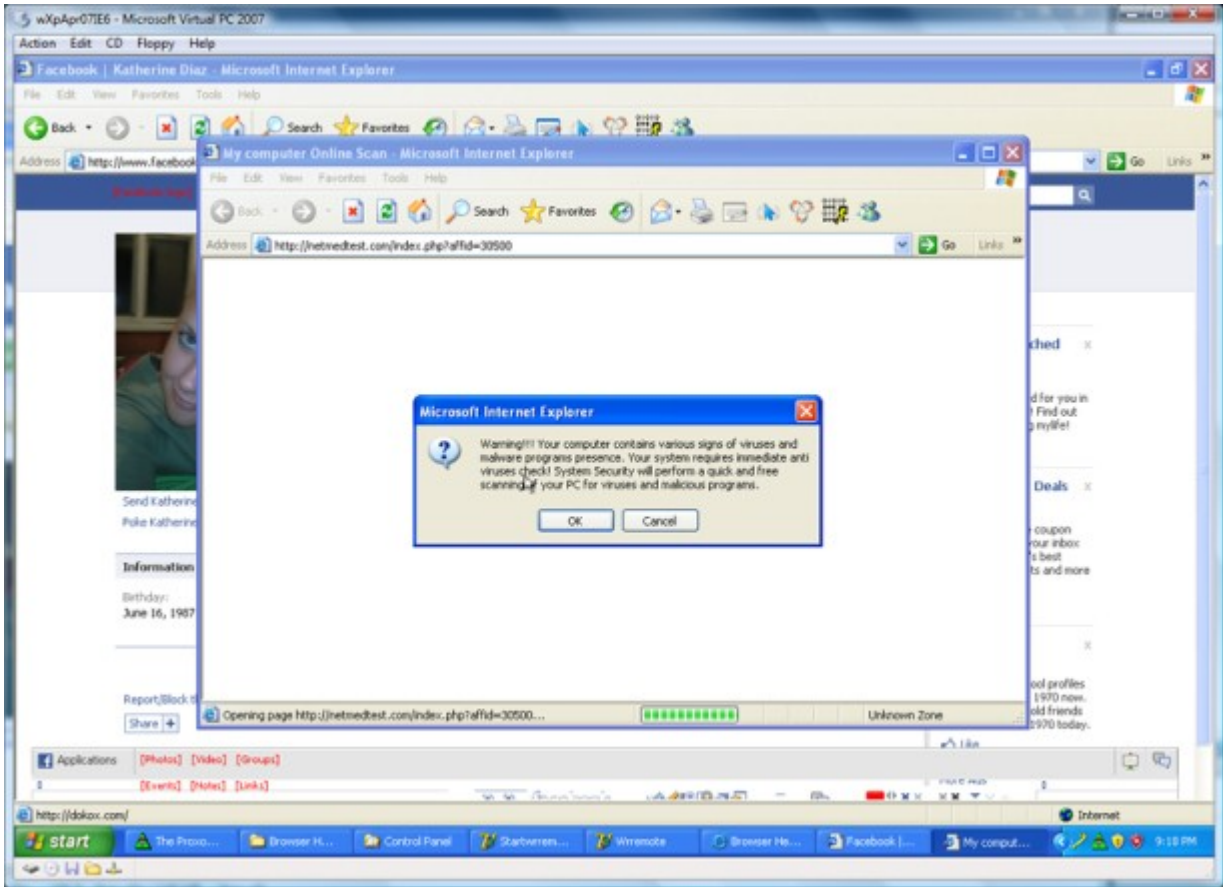
1.15 Slika jednog takvog lažnog profila

Kako se koriste lažni profili? Prva i najosnovnija stvar je da se na profil sliku stavi neka zgodna djevojka i/ili neki zgodni dečko što uvelike povećava šanse za stvaranjem prijatelja. Druga stvar je pod info nabacati hrpu stvari za koje se zna da bi mogle goditi i odgovorati ciljanoj skupini (znači da je status veze slobodna, da traži vezu, da je djevojka slobodnog pogleda na svijet, stranka po mogućnosti HDZ i naravno da je kršćanka...). Pa dobro što onda ako sam dodao nekog tko ima lažni profil kako to meni može smetati, e pa upravo ovako. Pošto ljudi općenito imaju tendenciju više vjerovati atraktivnijim osobama onda je veća šansa da če posjetiti linkove koje te osobe stavljaju ili skinuti programe za koje te osobe garantiraju da su im promjenile život itd. Tu dakle nastupaju spameri i tvorci virusa koji to navelike iskorištavaju.

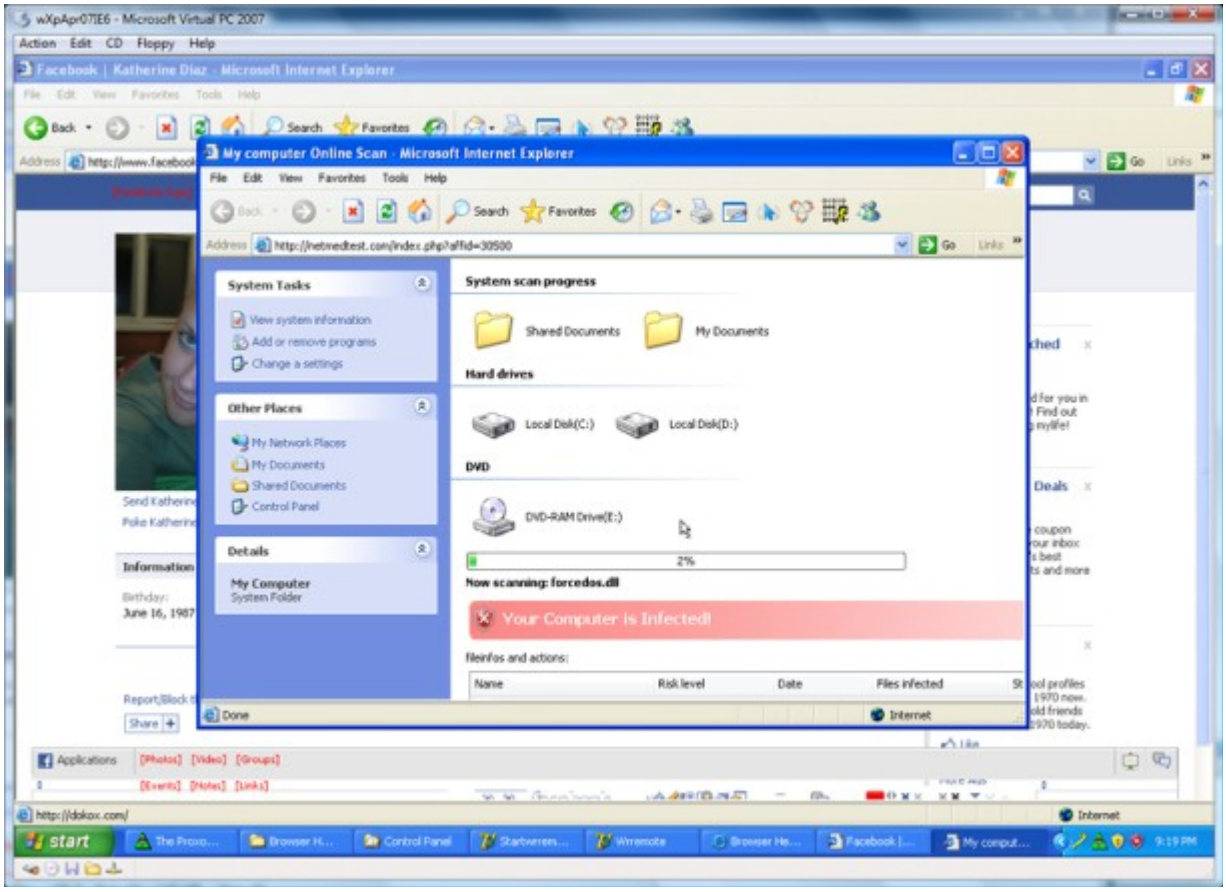
Nedavno su iz AVG-a tvorci antivirusnog programa LinkScanner otkrili neugodnu pojavu odnosno epidemiju gotovo identičnih lažnih Facebook profila koji su namijenjeni da zaraze korisnikov kompjuter sa 'spyware'-ima. Primjećeno je da postoji velika mogućnost da su ti profili stvoreni automatski što bi automatski značilo da je netko probio Facebook-ov 'captcha' kod koji upravo štiti od takvih automatski generiranih profila. Profil je naravno napravljen u skladu sa prijašnjim točkama koje treba ispuniti jedan takav profil da bi bio uspješan. Atraktivna slika, poželjno godište i naravno link na kućni uradak zgodne djevojke što bi biše mogli poželjeti. Naravno da su se oglasili i odmah iz Facebook-a i rekli da rade na uklanjanju svih tih profila te da sumnjaju da je 'captcha' probijen već da je velika mogućnost da su profili stvarani ručno odnosno da je nekome bilo plaćeno da ih kreira. Također je link stavljen na crnu listu na većini browsera i blokiran je URL na Facebook-u[6].



1.16 Prvi korak prihvaćanje prijateljstva



1.17 Drugi korak klikanje na link



1.18 Treći korak kompjuter je zaražen

Naravno kao i u prijašnjim slučajevima upozoravaju se korisnici da 2 puta razmisle prije nego što poduzimaju ikakve akcije koje su im sumnjive i da ako im je nešto sumnjivo da postoji vrlo velika vjerojatnost da je ili lažno ili zlobno za vaš kompjuter.

Zaključak

Sa sve većim brojem korisnika i sve kreativnijim i lukavijim načinima krađe podataka jasno je da su ljudi surfajući na internetu izloženi i vrlo lake mete.

Više manje svaka od ovih priča i cjelina nam govori o tome hoćemo ili nećemo biti prevareni ovisi o nama i jedino o nama.

Nadam se da sam načinom na koji sam objasnio mreže i širenje virusa i zaraza kroz njih uspio barem djelomično dočarati vam kolika opasnost prijeti ne samo vama nego i svim vašim prijateljima, a i njihovim prijateljima u slučaju da niste oprezni ili vi ili oni. U današnjem svijetu u kojem se sve više ljudi oslanja na internet mislim da mi je dužnost bila rasvjetiliti vam neke načine prevara i mogućiti vam lakše i sigurnije surfanje i korištenje interneta, a pogotovo socijalnih mreža. Facebook nije iznimka, jednako je tako i na ostalim socijalnim mrežama.

Zapamtite, ne možete biti prevareni osim ako to sami ne želite.

Literatura

[1] *Social network* - http://en.wikipedia.org/wiki/Social_network

[2] *Network Theory* - http://en.wikipedia.org/wiki/Network_theory

[3] Članak preuzet sa Carnetovog portala za učenje pod naslovom *'Ribanje na velikom Ribnjaku*' - https://lms.carnet.hr/lms/mentor2/pages/course/viewCourse.jsp?bean:CourseHandler.courseId=20881&bean:CourseHandler.enterCourse=20881&roleId=12&dd=1273361248240#

[4] Robert McMillan, *'Facebook takes steps to deal with giftcards scams'* - http://www.pcworld.com/businesscenter/article/193682/facebook_takes_steps_to_deal_with_gift_card_scams.html

[5] Željka Žorz, *'Rougue toolbars phish for facebook credentials'* - http://www.net-security.org/secworld.php?id=9065

[6] Jolie O'Del, *'Fake Facebook profiles are spreading spyware'* -http://www.readwriteweb.com/archives/fake_facebook_profiles_are_speading_the_spyware.php

Sažetak

Uvodom sam objasnio razloge pisanje seminara i odabrane teme te ono čega ću se dotaći tijekom pisanja seminara što se nadam i da sam uspio. Zatim sam se u temi Socijalne mreže dotakao pojma i objasnio ukrako čemu one služe. Dio pod naslovom Teorija mreža je bio neophodan za kasnije uvod u širenje podataka. Nesigurnost na socijalnim mrežama je bila uvod u daljnje razmatranje raznih oblika nesigurnih podataka i prevarama kojima smo izloženi, što je sve bilo uvod za dio seminara koji se bavi podatkovnim prevarama na Facebook-u, a to su sljedeći 'Lažne grupe', 'Lažne 'Fan page' stranice', 'Opasne aplikacije' i 'Facebook profili za neznalice' u kojima sam se dotakao više manje svih znanih prevara na Facebook-u.