CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost društvene mreže Facebook

NCERT-PUBDOC-2010-10-317

Nacionalni CERT

Nacionalni CERT

Sadržaj

1 Uvod

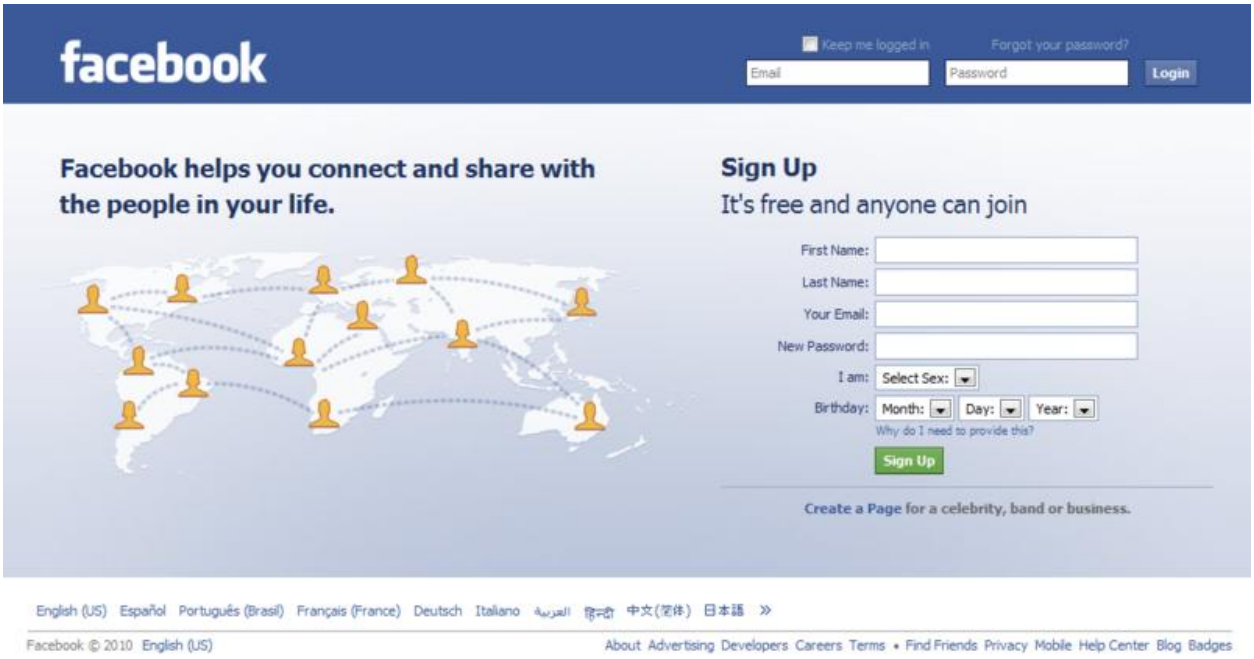
Facebook je najpopularnija društvena mreža, trenutno sa impozantnih pola milijarde korisnika. Korisnicima omogućuje komunikaciju na razne načine, pronalaženje starih prijatelja, dijeljenje raznog sadržaja, mrežno igranje, ostvarivanje poslovne suradnje, praćenje aktivnosti omiljenih sportaša, događanja, povezivanje u grupe i razne druge oblike interakcije. Tvrtke i druge organizacije se putem ove društvene mreže oglašavaju i tako ostvaruju novčanu zaradu te se približavaju klijentima ili imaju neki drugi oblik koristi. Programeri razvijaju aplikacije za Facebook-ovu platformu, a mobilni uređaju imaju posebne aplikacije za pristup za Facebook.

Ovakvim rastom i razvojem, nažalost raste i aktivnost kriminalaca koji raznim vrstama zloupotrebe pokušavaju doći do materijalne koristi. Veliki broj korisnika i vrlo velika količina interakcije omogućuju vrlo brzo širenje malvera i drugih oblika zlućudnog sadržaja. Zlućudni sadržaj kojeg šire prijatelji posebno je opasan jer ima određeni kredibilitet. Česte su razne vrste prijevara. Također, Facebook je ogromna baza osobnih podataka koji vrlo lako mogu doći u pogrešne ruke, odnosno zloupotrijebiti se. Korisnici nisu svjesni kome postaju dostupni podaci koje postavljaju na mrežu. Ovaj dokument daje pregled oblika i primjere zabilježenih sigurnosnih prijetnji te savjete kako se zaštititi.

2 Društvena mreža Facebook

2.1 Povijest

Facebook je društvena mreža koju je 2004. godine osnovao Amerikanac Mark Zuckerberg sa još nekolicinom kolega, za vrijeme studija na Sveučilištu Harvard. Mreža je prvotno bila zatvorena samo za studente Harvarda, ali se nakon toga brzo proširila na druga američka i kanadska sveučilišta, a potom i na srednje škole te tvrtke. U rujnu 2006. mreža je postala otvorena za sve osobe sa navršenih 13 godina i valjanom e-mail adresom. Nakon toga počeo je njezin eksponencijalni rast. U kolovozu 2008. broj korisnika premašio je 100 milijuna, a u srpnju 2010., 500 milijuna [1]. Time je Facebook postala najveća društvena mreža, ostavivši daleko iza sebe MySpace (koji je tijekom 2008. još vodio po broju korisnika) i druge mreže. Tvrtka Facebook jedna je od najbogatijih na svijetu, dok je web stranica njezine društvene mreže (facebook.com), druga najposjećenija web stranica, odmah iza tražilice Google. Glavni izvor prihoda tvrtke Facebook su reklame (slika 2.2. desno), a u tome surađuju i sa Microsoftom. Prihod u 2009. iznosio je 800 milijuna, a u 2010. očekuje se prihod od 1,1 milijardi američkih dolara.

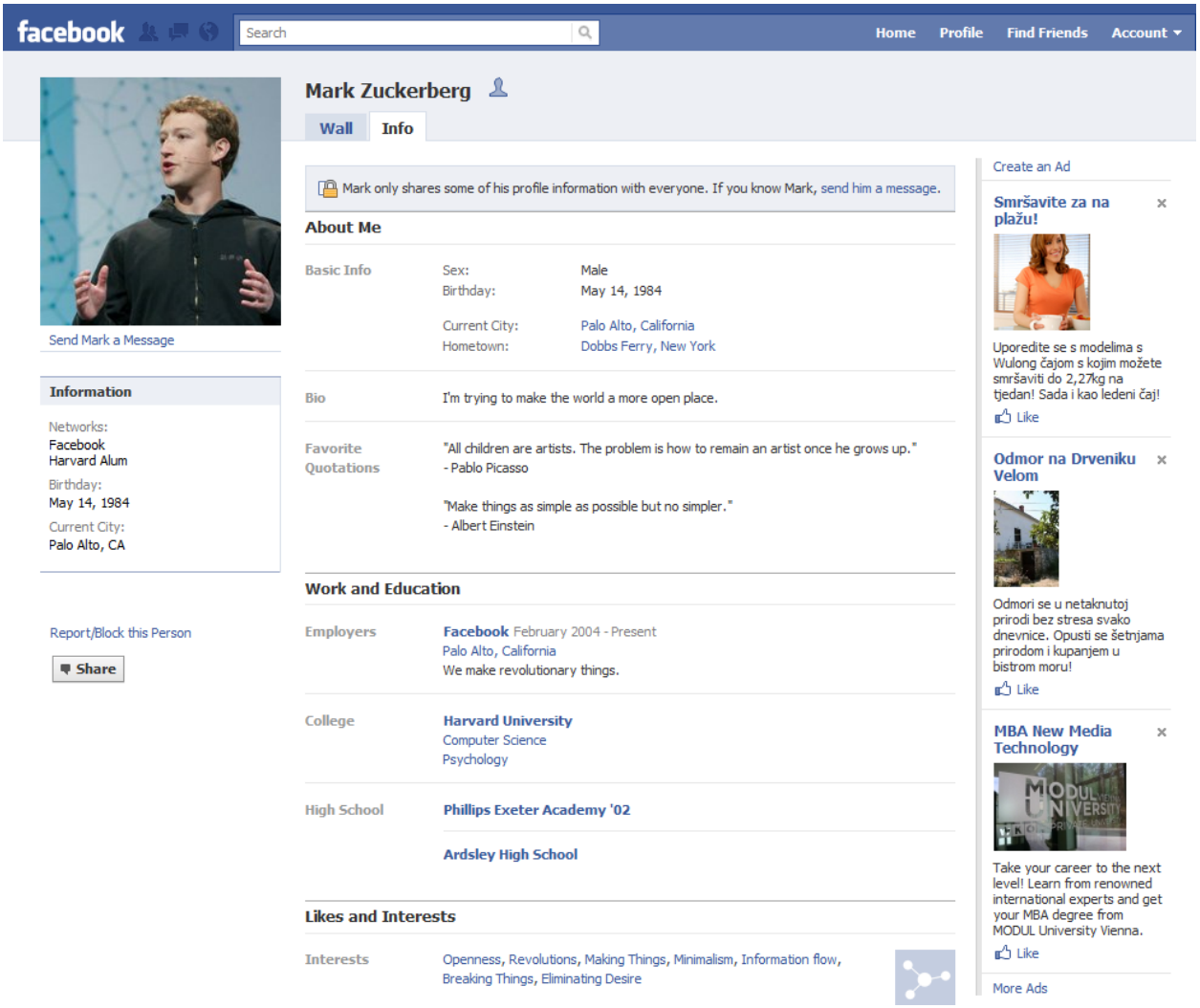


2.1: početna stranica Facebooka

2.2 Korištenje

2.2.1 Informacije na profilu

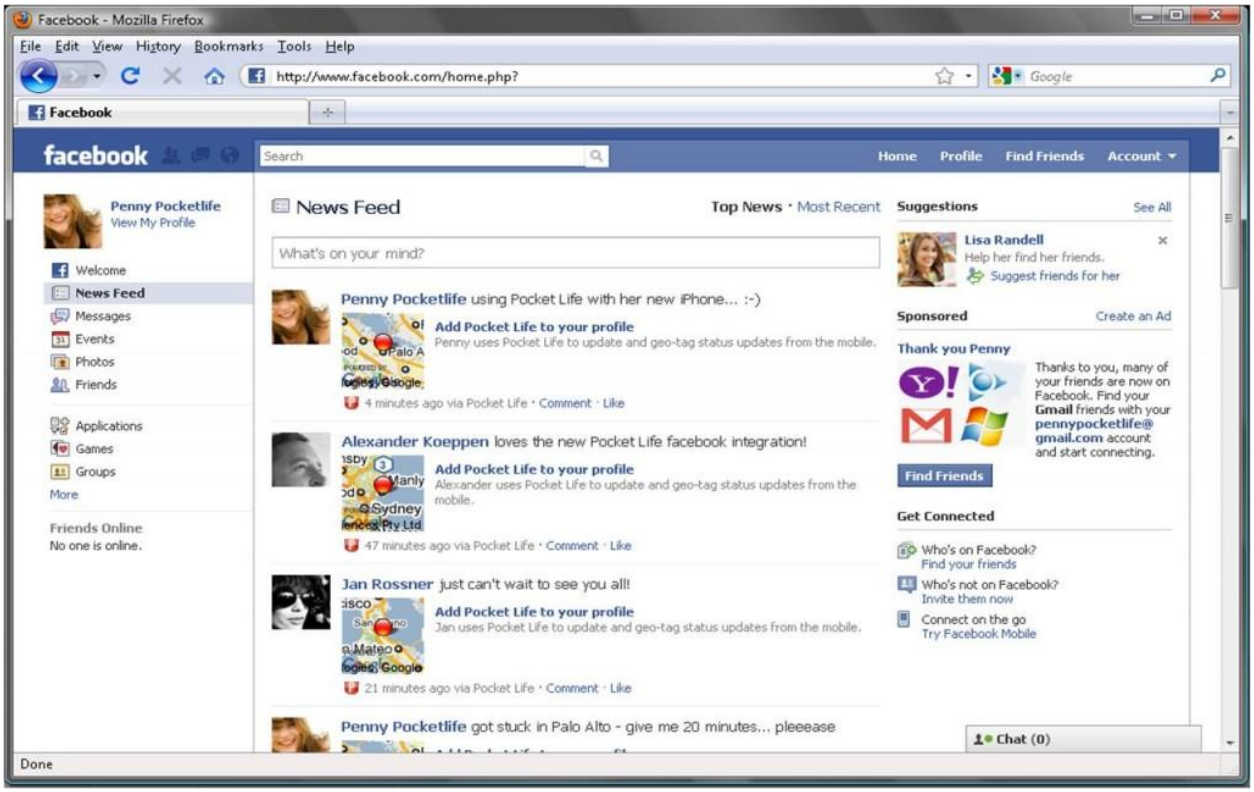
Nakon što otvore račun, korisnici na svojem profilu (slika 2.2) mogu dodavati razne informacije, sadržaj i naravno prijatelje (svaki profil ima listu prijatelja) koji će onda imati pristup tom sadržaju. Sama mreža novim korisnicima daje prijedloge što trebaju učiniti i time im olakšava snalaženje u novom okružju.



2.2: profil Marka Zuckerberga

Informacije koje korisnici mogu dodati na svoj profil: osobne informacije (datum i mjesto rođenja, mjesto pribivališta itd.), kontakt informacije (e-mail adresa, broj mobilnog telefona),

liste interesa (glazba, film, sport, politička i religiozna stajališta itd.) i informacije o školovanju i zaposlenju. Uz to, korisnici mogu na svoj profil dodavati fotografije (albume) i video zapise. „Profile picture“ predstavlja sliku koja se pojavljuje na stranici profila te je vezana uz profil kao što su i ime i prezime (pojavljuje se u pretrazi korisnika). Korisnik može u svoj profil dodati obiteljske i ljubavne veze koje se onda pojavljuju u profilu skupa sa drugim osobnim informacijama (okvir „Information“ na slici 2.2).



2.3: stranica "News Feed" na Facebooku

2.2.2 Grupe, događaji, zid i novosti

Postoje interesne i stranice ljubitelja (fanova) u koje se korisnici mogu učlaniti. Interesne grupe („groups“) često održavaju organizacije iz različitih sfera društvenog života (političke stranke, sportski klubovi, noćni klubovi, kazališta itd.) kao sredstvo promocije, odnosno marketinga. Stranice ljubitelja („like pages“) povezuju ljubitelje nekih sportaša, glumaca, marki automobila, TV serija, hrane itd. Osim što se može klikom na gumb „Like“ (sviđa mi se) priključit spomenutim stranicama ljubitelja, korisnik može i klikom dati do znanja prijateljima da mu se

sviđa i bilo koji drugi sadržaj (fotografija prijatelja, komentar itd.). Korisnik se također može pridružiti određenoj mreži („Network“) kao što su zemlja, grad, fakultet, tvrtka i sl. Neke od njih su otvorene, a neke zatvorene, odnosno za učlanjenje je potrebno dokazati pripadnost toj zajednici (obično putem e-mail adrese u vlasništvu te zajednice). Korisnici mogu i pokazati da li će prisustvovati nekim događanjima („Events“) kao što su koncerti, sportska događanja ili rođendan prijatelja (kao događanje kojeg je on kreirao). Na događanja korisnici mogu biti pozvani, sami ih pronaći (npr. reklama) ili ih sami kreirati.

Svaki korisnički profil ima tzv. zid („Wall“), mjesto gdje sam vlasnik profila ili neki njegov prijatelj mogu ostaviti poruku koju će onda vidjeti svi koji imaju pristup profilu. Osim korisnika i grupe posjeduju svoj „zid“. Tu je i „Status“ kojim korisnicima informiraju svoje bližnje o svojim akcijama i sl. Na početnoj („Home“) stranici korisnici mogu pratiti „News Feed“ (slika 2.3), tj. informacije o novostima kod prijatelja, njihovom statusu, zidu, rođendanima, događajima kojim prisustvuju, komentarima itd. „News Feed“ stranica predstavljena je 2006., a početkom 2010. je doživjela veliki redizajn i dobila nove mogućnosti. Tako sada korisnici mogu birati vrstu i količinu novosti (informacija) koje dobivaju od nekog prijatelja ili aplikacije.

2.2.3 Komunikacija

Korisnici Facebooka mogu si međusobno slati (privatne) poruke, bez obzira jesu li prijatelji. Sustav je sličan elektroničkoj pošti, svaki korisnik ima pretinac „Messages“ gdje može vidjeti pristigle poruke, a unutar njega je i pretinac sa poslanim porukama („Sent“). U komunikaciji ovim porukama može sudjelovati i više korisnika gdje svi vide sve poruke. Od 2008. je dostupan i „Chat“, odnosno sustav za stvarnovremensku razmjenu poruka između prijatelja. Podržana je jedino razmjena poruka između dva korisnika (1:1), ali jedan korisnik može istovremeno „chatati“ sa više prijatelja. Postoje mnogi samostalni klijenti za stvarnovremensku razmjenu poruka koji imaju podršku za Facebook Chat (eBuddy, Trillian, Miranda i dr.).

2.2.4 Aplikacije

Facebook sadrži mnoge aplikacije koje korisnici mogu koristiti. Neke od njih su ugrađene, a neke nezavisne (*third-party*). Jedna od najpopularnijih ugrađenih je Photos, aplikacija za postavljanje slika na mrežu. Ta aplikacija je jedan od razloga zašto je Facebook toliko popularan jer ne postoji ograničenje na broj slika koje korisnici mogu postaviti, za razliku od servisa za

dijeljenje slika kao što su Flickr i Photobucket. Postoji samo ograničenje na broj slika u pojedinom albumu (od svibnja 2009. navedeno ograničenje iznosi 200). Uz slike je vezana mogućnost „tag“, odnosno označavanja ljudi koji su na fotografiji. Tako npr. korisnik može označiti („tagati“) svojeg prijatelja na fotografiji koji onda o tome dobije obavijest i poveznicu na fotografiju. Facebook je u srpnju 2010. objavio kako se na mreži nalazi 50 milijardi fotografija [1].

2.4: igra Farmville

„Facebook Platform“ je skup programskih sučelja i alata koje omogućuju nezavisnim (*third-party*) proizvođačima softvera, razvoj aplikacija koje se integriraju sa Facebookom. Korištenjem ove platforme, Facebook je razvio nekoliko novih aplikacija. Neke od njih su „Gifts“ [1] (pokloni) koja prijateljima omogućuje slanje i primanje virtualnih poklona, „Marketplace“ tržnica koja korisnicima omogućuje postavljanje besplatnih oglasa i ranije spomenuta „Events“ (događanja). Neke od najpopularnijih aplikacija su mrežne (društvene) igre koje su dobrim dijelom i pomogle popularnosti Facebooka. Tvrtka Zynga najpoznatiji je proizvođač mrežnih igara za društvene mreže. Neke od najpopularnijih igara na Facebooku kao što su FarmVille (na slici 2.3;

[1] svaki korisnik je imao pravo poslati jedan besplatni poklon, a nakon je morao platiti 1 američki dolar po poklonu; aplikacija je ukinuta 1.8.2010. zbog pojave sličnih besplatnih aplikacija

najpopularnija Facebook igra, u ožujku 2010. imala je čak 85 milijuna igrača [2]), Mafia Wars i Texas Holdem Poker dolaze od tog proizvođača.

Krajem 2008., postao je dostupan „Facebook Connect“, skup programskih sučelja koji omogućuje logiranje Facebook korisnika (svojim Faceboook identitetom) na web stranice i servise treće strane. Korisnici su tako putem tih stranica mogu povezati sa prijateljima sa Facebooka i slati informacije na svoj profil.

2.3 Značaj

Osim što je najpopularnija društvena mreža na Internetu, Facebook se nametnuo i kao veliki medij za oglašavanje različitih organizacija i pokreta. Različite tvrtke, političke stranke i drugi prepoznali su važnost i snagu novog medija u borbi za kupcima, odnosno glasačima. Ljudi se često okupljaju u različite grupe kako bi izrazili svoje nezadovoljstvo politikom vlade ili druge stavove i sl. Za vrijeme predsjedničke kampanje u SAD-u 2008., preko milijun ljudi instaliralo je posebnu aplikaciju na računalu kako bi mogli komentirati debate između političara. Tijekom iste godine, stotine tisuća Kolumbijaca, protestiralo je protiv FARC-a, kolumbijske revolucionarne gerilske skupine. U prosincu 2008., Vrhovni sud teritorija australskog glavnog grada (ACT) donio je odluku koja propisuje da se Facebook može koristiti za izdavanje sudskih obavijesti okrivljenima [3].

Istraživanje koje je provela tvrtka Microsoft u prosincu 2009., pokazalo je da čak 79% menadžera i drugih odgovornih za zapošljavanje, informiraju se o kandidatima pretražujući Web [4]. Dakle, potrebno je ozbiljno shvatiti kakav se sadržaj postavlja na Facebook profilima. Bilo je nekoliko slučajeva otpuštanja zaposlenika uzrokovanih njihovim aktivnostima na Facebooku.

Mnoge tvrtke su zabranile svojim zaposlenicima korištenje Facebooka na poslu, vjerujući da to umanjuje produktivnost.

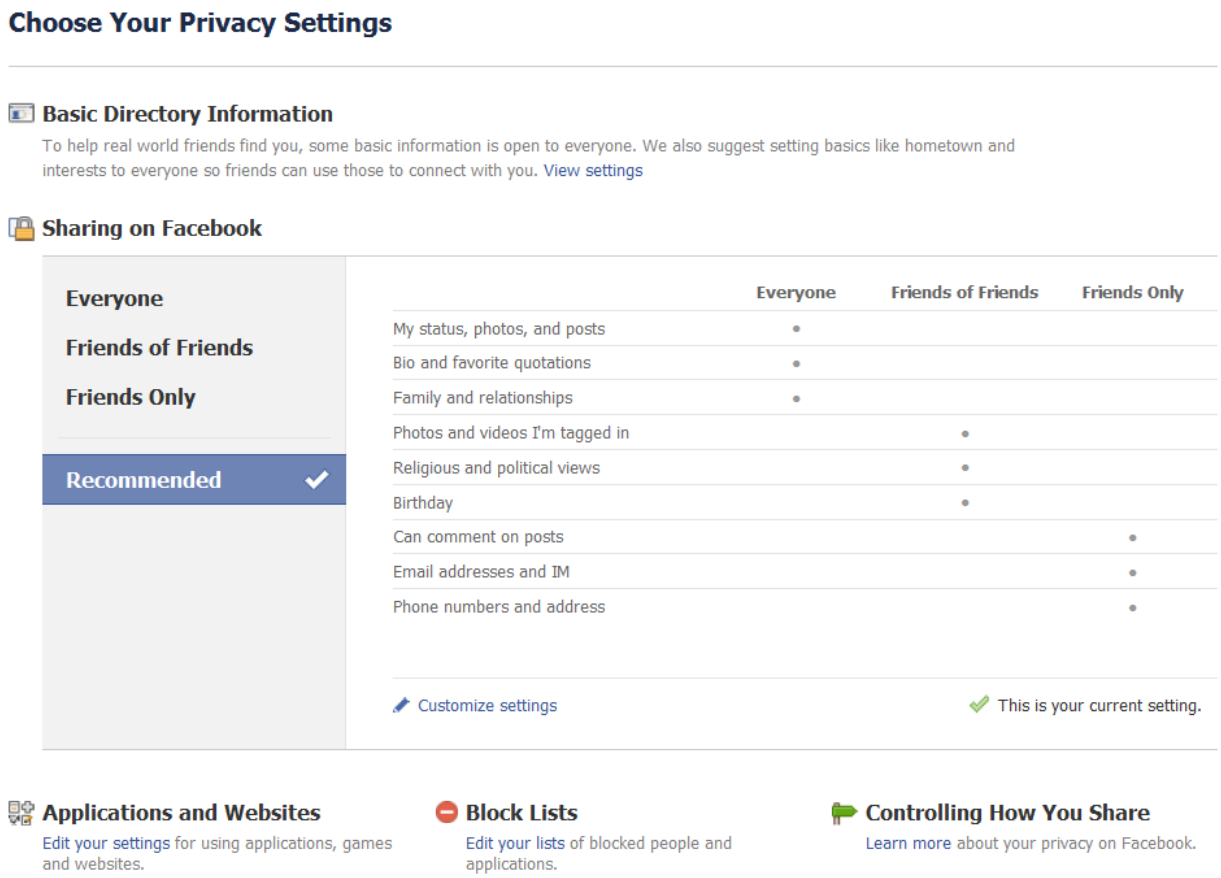
Utjecaj na elektronsku industriju, najbolje se vidi na primjeru najnovijih mobilnih uređaja (smartphone). Svi vodeći proizvođači svjetski takvih uređaja i operacijskih sustava za njih (Apple, RIM, Google, Nokia i dr.), razvili su posebne aplikacije za pristup Facebooku, koje su na uređajima inicijalno dostupne.

3 Sigurnosne prijetnje

Otkrivanje osobnih podataka povlači za sobom rizik korištenju istih od strane zlonamjernih korisnika (napadača) kako bi nekom korisniku ili organizaciji nanijeli određenu vrstu štete. Također, napadači mogu krađom profila ili na neki drugi način zlonamjerno iskoristiti vjerodostojnost kojem im daje lažno predstavljanje.

Veliki broj korisnika i ogromna količina interakcije na Facebooku, pogodna je i za vrlo brzo širenje malvera, zlonamjernih poruka (prijevara slanjem velike količine neželjenih poruka itd.) i drugih načina zloupotrebe. Postojanje mnogih dodataka, odnosno aplikacija na društvenoj mreži Facebook dodatni je problem. Napadači mogu zavarati korisnika imitirajući izgled neke aplikacije te navesti korisnika na instalaciju malvera.

Sigurnosne prijetnje mogu se ugrubo podijeliti u četiri kategorije (koje čine četiri sljedeća potpoglavlja) iako se one često isprepleću.



3.1: postavke privatnosti (Privacy Settings)

3.1 Prijetnje privatnosti i identitetu

Kako bi korisnik znao koje svoje podatke izlaže i kome su oni dostupni, potrebno je da bude upoznat sa politikom privatnosti. S vremenom je problem privatnosti postajao sve veći i složeniji, tako da je politika dokument koji definira politiku privatnosti na društvenoj mreži Facebook, postajao sve opširniji. Korisnik mora biti svjestan da uvijek postoji mogućnost kršenja pravila, odnosno zloupotrebe korisničkih podataka. U drugom dijelu potpoglavlja dan je pregled oblika zloupotrebe.-

3.1.1 Politika privatnosti na Facebooku

Politika privatnosti (privacy policy) društvene mreže Facebook dostupna je na adresi http://www.facebook.com/policy.php. Korisnik u svojim postavkama (slika 3.1) može odabrati koji će njegovi podaci biti dostupni javno, a koji samo prijateljima. Ime i prezime, kao i slika profila, dostupni su uvijek javno. Informacije i sadržaj koji je u postavkama korisnika klasificiran da je dostupan „za sve“ (Everyone), javno je dostupan, ne samo za korisnike Facebooka, nego i za sve korisnike weba, web tražilice itd. Takav sadržaj može se importirati, eksportirati i distribuirati bez ograničenja. Kada neki korisnik npr. napiše poruku na zidu drugog korisnika, ta poruka onda podliježe sigurnosnim postavkama ovog drugog. Facebook koristi osobne podatke poput datuma rođenja kako bi prilagodio sadržaj i reklame koje će prikazati korisniku.

Korištenjem aplikacija i web stranica koje su nezavisne od Facebooka (Facebook Platform), korisnik pristaje dijeliti svoje podatke izvan Facebooka. Međutim, spomenuti nezavisni servis mora poštovati dogovor o pravima i odgovornostima[2] (točnije 9. paragraf, točka 2). Spomenuti dogovor daje niz ograničenja na korištenje prikupljenih podataka od korisnika. Tako se servis obvezuje da će od korisnika tražiti samo one podatke koje su potrebni za rad aplikacije, da će imati politiku privatnosti koja će reći korisniku kako će se njegovi podaci koristiti i koju će poštovati, da će omogućiti korisniku brisanje svih podataka te da podatke neće dijeliti sa nekom vrstom oglašivačke mreže. Rizik leži u tome, da nitko ne može garantirati da servis neće prekršiti neko od pravila ili ga pokušati pogrešno interpretirati. Moguće je i da dođe do određenih propusta, odnosno grešaka kod upravljanja podacima od strane Facebooka.

[2] dostupan na web adresi http://www.facebook.com/terms.php

3.1.2 Oblici zloupotrebe

Zlonamjerni korisnik može preuzeti podatke sa korisničkih profila kako bi ih zloupotrijebio. Prikupljene podatke je moguće iskoristiti u sljedeću svrhu:

- uzrokovanja štete ugledu osobe (ili neku drugu neugodnost npr. zastrašivanje)
- ucjenjivanja korisnika
- otkrivanja povjerljivih podataka
- nanošenja fizičke boli
- krađe identiteta
- lažno predstavljanje
- uhođenja (čak i industrijske špijunaže)
- ciljanog (personaliziranog) oglašavanja
- prepoznavanja pomoću lica (iz fotografija)

Fotografije, video-zapise i sl., zlonamjerni korisnik može iskoristiti za uzrokovanje štete ugledu osobe ili čak za ucjenu. Jedan od primjera kako naštetiti ugledu osobe je otvaranje lažnog profila sa naravno lažnim sadržajem. „Cyber-bulling“ je termin za psihičko maltretiranje putem Interneta ili neke druge (mobilne) mreže. Na Facebooku je bilo već mnoštvo takvih slučajeva. Bilo je i slučajeva nanošenja fizičkih ozljeda (pa čak i ubojstava) nakon dogovora o sastanku preko Facebooka. U tim slučajevima, napadači su se često na Facebooku lažno predstavljali kako bi namamili žrtvu.

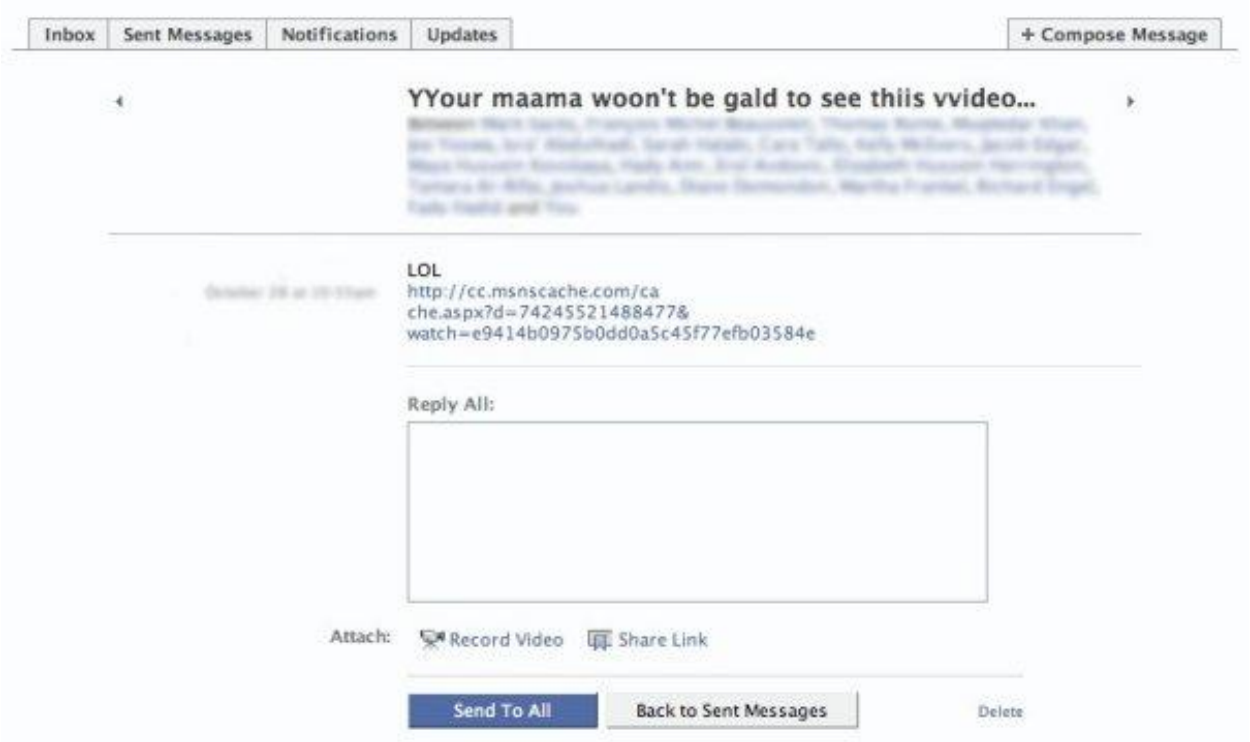
Napadač može iskoristiti podatke prikupljene sa Facebooka za otkrivanje povjerljivih podataka na nekim drugim servisima (pretraživanjem Weba). Moguće je da putem Facebooka sazna odgovore na sigurnosna pitanja koja se koriste u slučaju zaboravljanja lozinke na različitim web servisima (npr. Paypal ili neki drugi servis za plaćanje) i tako otme korisnički račun te korisniku nanese financijsku štetu. Na isti način zlonamjerni korisnik može ukrasti i račun na Facebooku te ga onda koristiti za lažno predstavljanje. Ako zaposlenik objavi na Facebooku neke osjetljive podatke o svojoj tvrtki, tada je moguće naštetiti i njezinom poslovanju i ugledu.

U srpnju 2010., kanadski sigurnosni istraživač Ron Bowes, postavio je na javni P2P servis BitTorrent, bazu koja se sastoji od podataka iz čak 170 milijuna korisničkih računa sa Facebooka

(koji su inače javno dostupni) [5]. Ovako velike brojke, su meta za napadače koji u većini slučajeva koriste zakon velikih brojeva za svoja razna zlodjela. Navedene podatke mogu iskoristiti i oglašivačke tvrtke, za razne oblike personaliziranog oglašavanja i slanje takvih reklama bez pristanka korisnika.

3.2 Neželjene poruke

Širitelji neželjenih poruka (spama) koriste Facebook (na sličan način kao i elektronsku poštu) za širenje velikih količina spam poruka. Primjer takve poruke prikazan je na slici 3.2. Poruke se šalju preko Facebook-ovog sustava za razmjenu poruka, ali i preko komentara. Obično mame korisnika da klikne na neki link rečenicama kao što su (prevedeno): „Moraš vidjeti ovaj video!“ i „90% korisnika ne može gledati ovaj video duže od 30 sekundi“.



3.2: primjer spam poruke

Svrha poruka može biti reklamiranje određenog proizvoda, odvlačenje korisnika na pornografske web stranice, izazivanje preopterećenja mreže, ali i mnogo opasnija. Poruke tako mogu

sadržavati poveznice na zlođudne web stranice na kojima se prijevarom (više o tome u sljedećem potpoglavlju) od korisnika pokušavaju ukrasti povjerljivi podaci ili instalirati neki malver. Ako se zlođudna spam poruka proširi dovoljno brzo na dovoljan broj korisnika, moguće je da korisnici ne znajući, izazovu distribuirani napad uskraćivanja usluge (DDoS).

U posljednje vrijeme, pojavio se novi oblik spama, tzv. „likejacking“ (po uzoru na „clickjacking“), prikazanog na slici 3.3. Širitelji spama koriste jednostavni oblik socijalnog inženjeringa (zanimljivu poruku) kako bi naveli korisnika da klikne link. Nakon što korisnik klikne link, biva preusmjeren na zlonamjernu web stranicu, na kojoj piše samo „Klikni ovdje za nastavak“ (eng. Click here to continue). Ako klikne, korisnik zapravo radi „like“ na taj sadržaj, te mu se početna spam poruka (sa linkom) pojavljuje u novostima i profilu, spremna da korisnikovi prijatelji, također kliknu na nju. Riječ je o nevidljivom okviru (*iFrame*) preko kojeg je dostupan Like gumb.

3.3: tipična "likejacking" poruka [izvor: Sophos]

U studenom 2008., okružni sud u San Joseu, donio je presudu protiv Adama Guerbueza i njegove tvrtke Atlantis Blue Capital [6]. Tvrtka je bila dužna platiti (barem na papiru) Facebooku astronomskih 873 milijuna američkih dolara, a sve zbog slanja milijuna spam poruka korisnicima do čijih je podataka došao raznim prijevarama (phishing i dr.). Bila je to najveća presuda takve vrste u povijesti.

3.3 Prijevare

Zlonamjerni korisnici koriste i razne oblike prijevara na Facebooku, uglavnom kako bi došli do financijske koristi.

3.3.1 Phishing

Jedan od oblika prijevara je phishing koji uključuje razne vrste manipulacije nad korisnikom (socijalni inženjering) kako bi on otkrio svoje povjerljive podatke (kao što su podaci kreditnih

kartica itd.). Napadači koriste web stranicu koja imitira izgled nekog servisa za plaćanje (najčešće PayPal) i korisnik kad se „logira“ na takvu stranicu, napadačima zapravo predaje svoje povjerljive podatke. Na isti način (imitiranjem web stranice Facebooka obično sa domenom koja ima „facebook.com“ u nazivu), napadači mogu oteti i korisničke račune za Facebook i koristiti ih za druge oblike napada. Bilo je slučajeva u kojima su napadači sa ukradenih Facebook profila, kontaktirali prijatelje i lažno se predstavljajući pokušali izvući novac od njih.

Sličan oblik prijevare su i besplatne alatne trake (toolbar) za Facebook igre. Jedan od takvih slučajeva bila je lažna alatna traka koja navodno omogućuje varanje na poker igrama proizvođača Zynga (a to je obična laž) [7]. Alatna traka (slika 3.4) je izgledala potpuno legitimno (po uzoru na Zynginu originalnu) te je čak sadržavala originalni logotip Facebooka. Međutim, kad bi korisnik kliknuo na taj logo, bio bi preusmjeren na lažnu Facebook stranicu koja naravno krade korisničke podatke. Prevaranti se često služe lažima (glasinama), kao u ovom slučaju, koje se na velikoj društvenoj mreži vrlo brzo šire.

3.4 web stranica lažne Zynga alatne trake

3.3.2 „Hoax“ i „scam“ prijevare

Na društvenoj mreži Facebook česte su i „hoax“ poruke neistinitog sadržaja, poslane s ciljem dezinformiranja, zbunjivanja ili zastrašivanja što većeg broja primatelja. Pri tome ih korisnici prosljeđuju svojim prijateljima uvjereni da im tako pomažu. Manje ozbiljnim „hoax“ porukama je obično cilj se što više proširiti (zlonamjernici koriste mogućnost vrlo brzog širenja na društvenoj mreži), dok oni ozbiljniji žele prevariti korisnika kako bi on sam oštetio svoj sustav, donirao novac i sl. „Scam“ je ozbiljniji oblik „hoaxa“, često sa ozbiljnim financijskim, pravnim

ili drugim posljedicama za žrtvu. Najčešći oblik „scama“ na Facebooku su oni vezani uz iznuđivanje novca. Tipični primjeri „hoaxa“ na Facebooku, su poruke o nepostojećim virusima i slično, a obično završavaju savjetom korisniku da obavijest iz poruke stavi na svoj zid na profilu. Neki drugi oblici su tračevi o Facebooku, kao što je bio primjer tzv. „Automation Labs Warning“ [8]. Riječ je o poruci koja je tvrdila da korisnik pretraživanjem riječi „automation labs“ u opciji blokiranih ljudi, dobije popis ljudi koji imaju uvid u sve profile na Facebooku, odnosno da su neka vrsta špijuna. Naravno to je laž, a rezultati pretrage su ustvari, samo ljudi koji su na neki način povezani sa tim riječima.

Osim što se šire porukama, „hoax“ i „scam“ se šire i putem grupa ljubitelja (fan pages) koje su otvorili zlonamjerni korisnici. Tipičan primjer takvih grupa [9] su lažni (novčani) popusti na proizvode u Ikei, supermarketima, lažni pokloni, kuponi (slika 3.5) i sl. Takve grupe znaju imati i po nekoliko stotina tisuća članova, a za pristup grupi, često traže neke osobne informacije, metodama sličnim phishingu. Te podatke, napadači mogu iskoristiti za nanošenje materijalne štete žrtvama ili za prodaju oglašivačkim agencijama. U svakom slučaju, riječ je o prijevari jer se sve radi bez pristanka korisnika. Potrebno je se uvijek voditi poslovicom „Ako je predobro da bi bilo istinito, nije istinito“.

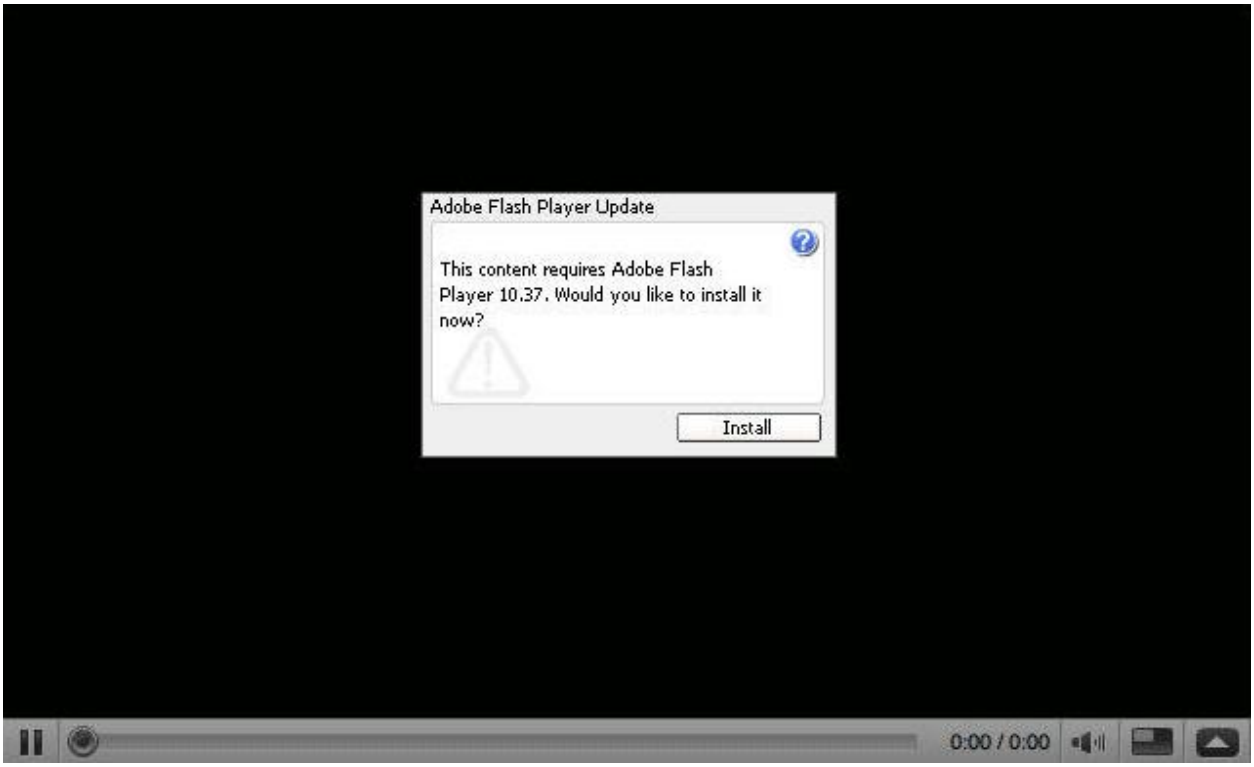
3.5: stranica lažnog poklona (kupona), izvor: [9]

Još jedan oblik „scam“ prijevara, za koji napadači koriste Facebook za širenje, su lažne donacije. Kod njih, napadači obično koriste neke stvarne događaje kako bi dobili na uvjerljivosti. Najpoznatiji slučaj u posljednje vrijeme bile su lažne donacije za stradale u potresu na Haitiju.

3.4 Malver i drugi napadi

3.4.1 Koobface

Koobface [10] (anagram riječi Facebook) je crv koji se pojavio u svibnju 2008. i širi se preko zlonamjernih poruka sa zaraženih računala putem društvenih mreža, uključujući Facebook. To mogu biti spam poruke na novostima (News Feed) ili privatne poruke (koje preko možemo dobiti i od zaraženog prijatelja). Riječ je o vrlo složenom malveru, koji zaraženo računalo (tzv. zombie) pretvara u dio tzv. botneta (velike mreže zaraženih računala i kontrolnih poslužitelja). Njegova arhitektura je modularna, a svaki modul (komponenta) služi za određenu zlonamjernu aktivnost. Nakon što zaraze računalo, napadači mogu malver nadograđivati novim komponentama ili postojeće mijenjati novim inačicama. Sve u svrhu proširenja funkcionalnosti botneta, odnosno omogućavanja šireg spektra napada.



3.6: lažna Koobface nadogradnja

Komponenta zadužena za širenje je onaj dio koji je vidljiv na Facebooku. Korisniku se šalje poruka koja ga navodi da pogleda video-zapis na web stranici koja imitira servis YouTube (slika 3.6). Kad korisnik pokrene video-zapis, otvara se prozor za instalaciju lažnog dekodera kojeg korisnik „mora“ instalirati kako bi mogao pogledati video-zapis. Riječ je o datoteci setup.exe kojoj je svrha otkrivanje koje društvene mreže korisnik posjećuje (pretragom cookie datoteka) te preuzimanje ostalih komponenti malvera.

Jedna od komponenti malvera, zaraženo računalo pretvara u web poslužitelj koji onda koristi za posluživanje zlođudnih web stranice (poput spomenute lažne stranice YouTubea). Druga komponenta služi za razbijanje CAPTCHA[3]-e. Radi tako da korisniku prikazuje poruku kako će mu računalo biti ugašeno ukoliko ne riješi CAPTCHA provjeru. Riješene provjere, malver šalje kontrolnom poslužitelju, a botnet ih dalje koristi za svoje širenje. Ista komponenta, prikazuje korisniku na računalu različite reklame, kao što su reklame za lažne (zlođudne) anti-virusne programe.

Najopasnija komponenta Koobface-a je skupina malvera namijenjena krađi povjerljivih podataka. Ima mogućnost krađe podataka iz različitog niza softvera, kao što su web preglednici, klijenti za elektronsku poštu i razmjenu poruka u stvarnom vremenu (ICQ, Trillian itd.), FTP klijenti itd. Svi prikupljeni podaci šalju se na poslužitelj kojeg odredi napadač.

Koobface također preusmjerava pretrage upućene na Google, Yahoo i druge web tražilice na poslužitelj pod kontrolom napadača koji onda korisniku servira zlođudne reklame. Osim toga, preusmjeravaju se i svi DNS upiti, odnosno korisnika se vodi na lažne stranice iako je on upisao web adresu legitimne. Ovdje postoji velika opasnost od phishing napada. Često je uloga navedenih preusmjeravanja i nedopuštanje korisniku da dođe do anti-virusnih alata.

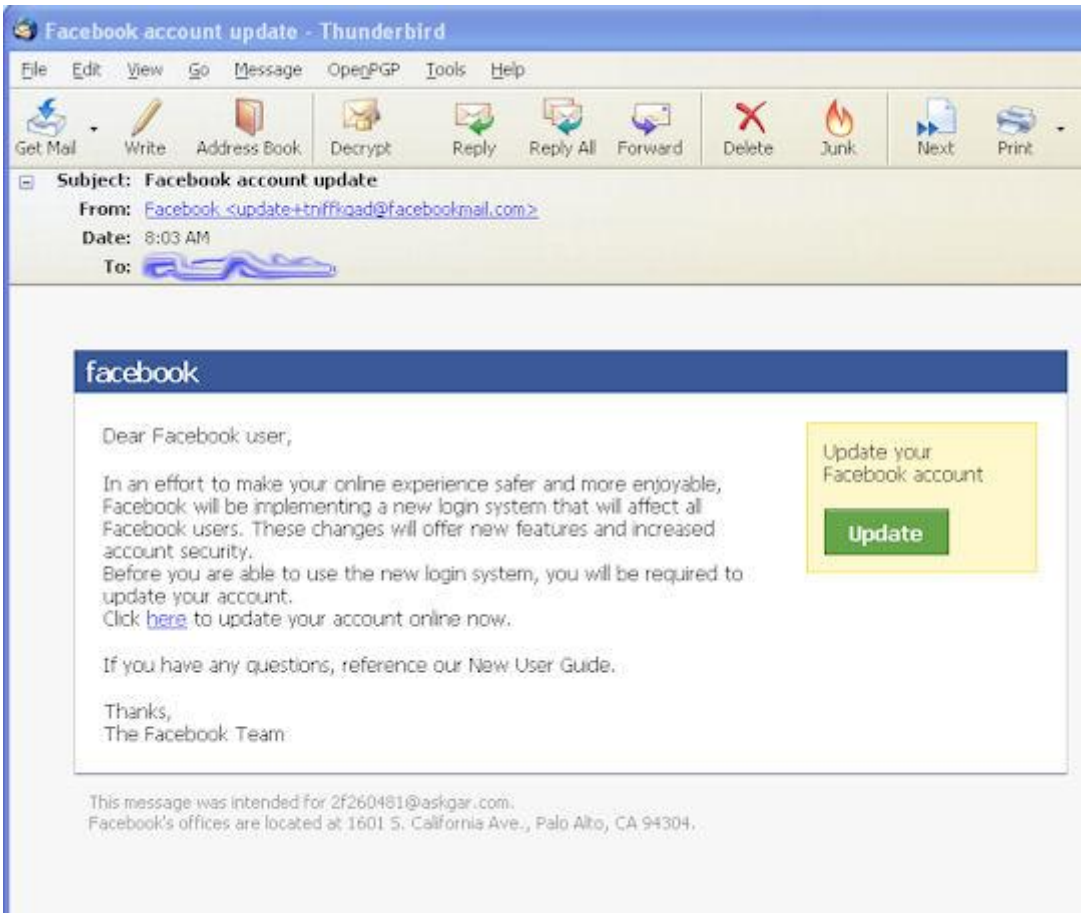
3.4.2 Ostali malver

Razne vrste malvera koriste Facebook i podatke prikupljene sa njega za širenje. Osim što mogu koristiti Facebook-ove sustave za slanje poruka, mogu koristiti i elektronsku poštu. Kao što smo vidjeli, ova društvena mreža je i velika baza podataka te napadači lako dolaze do podataka kao što su adrese elektronske pošte. Zabilježeno je da poznati botnet Zeus [11] šalje e-mail poruke korisnicima Facebooka koje navodi na lažnu nadogradnju računa. Nakon, što klikne „Update“

[3] tip provjere kojom se pokušava osigurati da jedna strana u komunikacijskom kanalu nije računalo, već čovjek (obično je riječ o iskrivljenim i prešaranim slovima na slici koje korisnik mora prepisati); razni web servisi (uključujući Facebook) uobičajeno ih koriste kod registracije novih korisnika

(Nadogradi) u e-mail poruci, koja izgleda kao legitimna poruka od strane Facebooka (slika 3.7), pojavi se lažna web stranica Facebooka. Kad korisnik upiše svoje podatke, otvara se web stranica za preuzimanje „nadogradnje“, odnosno zloćudne datoteke (updatetool.exe). Navedena datoteka je trojanski konj koji krade bankarske podatke (brojeve kreditnih kartica, korisnička imena i lozinke sa servisa za plaćanje).

Postoje i mnoge druge vrste malvera (i botnet-ova) vezane uz Facebook, a i nove će se sigurno pojaviti u budućnosti.



3.7: e-mail poruka Zeus botneta

3.4.3 „Cross-site scripting“ napadi

Cross-site scripting (XSS) vrsta je napada na aplikacijskoj razini koji koristi ranjivost neke dinamičke web stranice (točnije njezinih skripti). Dinamičke web stranice su takve stranice čiji se sadržaj stvara na temelju ulaznih korisničkih podataka kako bi se ostvarila određena

interakcija sa korisnikom. Napad se izvodi tako da se zloćudni programski kod ubacuje u ulazne podatke korisnika kako bi se, nakon posjeta ranjive web stranice, izveo u korisnikovom (žrtvinom) web pregledniku. U tu svrhu, napadači obično koriste kombinaciju koda u programskom jeziku JavaScript i HTML-u. Naime, kod korištenja skriptnih jezika koji se izvršavaju na strani klijenta (kao što je JavaScript), dinamičke web stranice nemaju potpunu kontrolu sadržaja kojeg interpretira korisnikov web preglednik.

Postoje tri vrste XSS napada, a to su:

- neperzistentni (jednokratni)
- perzistentni (trajni)
- temeljen na DOM (*Document Object Model*) objektima

Perzistentni XSS napad posebno je opasan za društvene mreže (i najčešći) zbog činjenice da zloćudni kod ostaje pohranjen na web stranici (Facebooku) spreman za izvršiti napad (zaraziti) tisuće korisnika u vrlo kratkom roku. Kod neperzistentnog napada, zloćudni se kod nalazi u URL-u na koji napadač navodi nekog korisnika (tipično putem e-mail spam poruka), a slično je i kod treće vrste XSS napada, jedina postoji razlika u tehničkoj izvedbi napada.

Uspješan XSS napad na Facebook, napadaču omogućuje:

- čitanje žrtvinih privatnih poruka
- dohvaćanje privatnih fotografija
- slanje poruka žrtvinim prijateljima, u ime žrtve
- dodavanje novih aplikacija
- krađu kontakata

Često su propusti vezani uz aplikacije, a napadači koriste tehnike ubacivanja koda u njihov sadržaj (gumbove, poklone i sl.). Dosad se pojavio cijeli niz ovakvih sigurnosnih propusta, ali Facebook ih je vrlo brzo ispravljao. Sigurnosni stručnjaci upozoravaju na nove propuste istog tipa gotovo svakog mjeseca.

4 Sigurnosne mjere

4.1 Facebook Security

Na svojim počecima, društvena mreža Facebook (kao i ostale) bila je usmjerena na širenje, odnosno što brže povećanje broja korisnika. Malo pozornosti se davalo sigurnosti, ali s vremenom, sa raznim novim sigurnosnim prijetnjama, Facebook je počeo davati sve više pažnje tom segmentu. Facebook Security je web stranica, odnosno Facebook grupa (dostupna na adresi: http://www.facebook.com/security) kojoj je namjena edukacija korisnika o sigurnosnim prijetnjama. Na njoj, također, korisnici mogu prijaviti potencijalno novootkrivene prijetnje ili tražiti pomoć. Za svakog korisnika je dobro učlaniti se u ovu grupu kako bi bio pravodobno informiran.

Kako bi korisnicima donio veći stupanj sigurnosti, Facebook je ušao i u partnerstvo sa poznatim proizvođačem sigurnosnih rješenja, McAffe [12]. Tvrtka McAffe osigurava svakom korisniku Facebooka besplatno korištenje njihovih sigurnosnih alata na period od 6 mjeseci, a nakon toga i specijalne popuste. Tvrtka Websense je prva koja je u svoju ponudu uvrstila sigurnosni paket koji je specijaliziran za Facebook, to je Defensio, inačice 2.0 [13].

Facebook ima i sustav za povrat suspendiranih korisničkih računa [14]. To su otuđeni korisnički računi koje je Facebook suspendirao, nakon otkrivanja zloupotrebe istih. Sustav je još u testnoj fazi te je Facebook poslao e-mail poruke samo jednom dijelu korisnika kojima su oteti računi. U poruci, korisniku se objašnjava što se dogodilo i koje sve korake mora poduzeti kako bi povratio svoj račun. U tom procesu se raznim pitanjima utvrđuje da li je osoba koja prolazi kroz proceduru zaista i legitimni vlasnik računa.

Još jedna nova sigurnosna opcija, također u testnoj fazi, je i sustav „Login Notifications“ [15]. Opcija (dostupna pod „Account Security“ unutar postavki računa), korisniku nudi definiranje liste (imena) računala sa kojima pristupa Facebooku. Svaki put kada korisnik pristupa mreži sa novog računala (ili starog bez „cookie“ datoteke), mora ga imenovati. Ako je uneseno ime računala koje se prethodno nije koristilo, vlasnik računa dobije obavijest o tome (SMS), kako bi bio u mogućnosti zaštititi svoj račun (promjenom lozinke) u slučaju neovlaštenog pristupa.

Postoje još mnogi sigurnosni sustavi koji su, kako ističe Facebook, nevidljivi običnom korisniku, a mnogi drugi su u stalnom razvoju.

4.2 Kako se zaštititi

Savjeti za zaštitu na društvenoj mreži Facebook:

- koristiti složene lozinke – lozinke koje nemaju veze sa osobnim podacima (ime, prezime, datum rođenja i sl.), koje se ne koriste na drugim web servisima (forumi, web stranice itd.), koje ne sadrže riječi koje se mogu pronaći u rječniku, koje sadrže kombinaciju velikih i malih slova, brojeva i znakova
- ne pohranjivati lozinke u web preglednik (opcija „Remember Password“ itd.) – sigurnosni propusti u web preglednicima mogu dovesti do krađe lozinki
- ne slijediti sumnjive poveznice u e-mail porukama, privatnim ili drugim vrstama poruka na Facebooku (čak i ako dolaze od prijatelja) – takve poveznice su često vezane uz lažne nadogradnje, zanimljive video-sadržaje i sl., a dovode do preuzimanja malvera ili do phishing stranica
- uvijek obratiti pozornost na URL adresu u slučaju praćenja poveznice, klikanja na gumb ili sl. – domena mora odgovarati „facebook.com“ (a ne „facebook.com.nešto.nešto“)
- pratiti sigurnosna upozorenja (stranica Facebook Security itd.)
- koristiti redovito ažuriran anti-virusni program
- ne postavljati povjerljive podatke (u bilo kojem obliku)
- postaviti odgovarajuće sigurnosne i postavke za ograničavanje dostupnosti podataka (Privacy Settings) – obratiti pozornost na „Public search“ opciju koja omogućuje javno pretraživanje profila, podatke dostupne aplikacijama i dr.
- ne dodavati neznance kao prijatelje

Europska agencija za mrežnu i informacijsku sigurnost (ENISA) u svojem je dokumentu [16] iznijela svoje viđenje rizika i preporuka za zaštitu, vezano uz društvene mreže.

5 Zaključak

Nema dvojbe da su i kriminalci, odnosno napadači prepoznali mogućnosti koje im pruža Facebook. Koristeći razne oblike prijevara, zloćudnog koda i sl., koje šire putem spam poruka koristeći Facebook-ove sustave za interakciju, korisnicima nanose razne oblike štete. Privatni podaci sa Facebooka, dostupni su praktički javno, što predstavlja opasnost od niza sigurnosnih prijetnji. Facebook nije dovoljno zaštitio navedene podatke iako je u posljednje vrijeme uložio puno truda u zaštitu korisnika. Korisnici se ne mogu pouzdati da će Facebook zaštititi njihove podatke.

Najbolja zaštita, kao i obično kad se govori o zaštiti na Internetu, edukacija je korisnika. Nadalje, proizvođači sigurnosnih rješenja (softvera), tek su krenuli u razvoj specijalnih alata namijenjenih društvenim mrežama i u budućnosti se očekuje njihov znatniji doprinos borbi protiv zloupotrebe. Očekuje se i da Facebook razvije neki oblik sustava koji bi bio inicijalno uključen za svaki profil te koji bi automatski i pravovremeno obavještavao korisnike o opasnostima.

Svaki korisnik dok koristi Facebook ili neku drugu društvenu mrežu, dobro mora biti svjestan opasnostima kojima se izlaže.

6 Literatura

1. Scaling Facebook to 500 Million Users and Beyond, http://www.facebook.com/note.php?note_id=409881258919, 21.6.2010.
2. Farmville, Top Facebook Games Continue To Shed Users http://www.gamasutra.com/view/news/28837/Farmville_Top_Facebook_Games_Continue_To_Shed_Users.php, 4.6.2010.
3. Lawyers to serve notices on Facebook, http://www.theage.com.au/articles/2008/12/16/1229189579001.html, 16.12.2008.
4. Research shows online reputations matter, http://www.microsoft.com/privacy/dpd/research.aspx, 12/2009.
5. 100 million Facebook user profiles published to BitTorrent, http://news.techworld.com/security/3233983/100-million-facebook-user-profiles-published-to-bittorrent/ , 2.8.2010.
6. Making Facebook Safe Against Spam, http://www.facebook.com/notes/facebook-security/making-facebook-safe-against-spam/40999515765 , 24.11.2008.
7. Warning: Fake Zynga Toolbars Will Steal Your Facebook Password, http://www.allfacebook.com/toolbars-facebook-password-2010-03 , 25.3.2010.
8. Automation Labs Facebook Privacy Warning Hoax, http://www.hoax-slayer.com/automation-labs-facebook-warning.shtml , 2/2010.
9. Facebook Scams Alert, http://www.brickandclick.com/2010/04/facebook-scams-alert-remember-the-one-rule-that-rules-them-all.html, 2.4.2010.
10. Baltazar, Costoya, Flores - The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained, Trend Micro Threat Research, tehnički dokument, srpanj 2009.
11. Bank Trojan botnet targets Facebook users, http://news.cnet.com/8301-27080_3-10385498-245.html , 28.10.2009.
12. Better Security through Software, http://blog.facebook.com/blog.php?post=248766257130 , 13.1.2010.
13. http://defensio.com/ , službena stranica alata Websense Defensio
14. New Tools to Secure a Compromised Account, http://blog.facebook.com/blog.php?post=107720572130&ref=mf , 17.7.2009.
15. Staying in Control of Your Facebook Logins, http://blog.facebook.com/blog.php?post=389991097130 , 13.5.2010.
16. ENISA (European Network and Information Security Agency): Security Issues and Recommendations for Online Social Networks, http://www.enisa.europa.eu/act/it/library/pp/soc-net, 10/2007.