Nevarnosti družabnih omrežij

Social Network Risks

Domen Božeglav,

Akademska in raziskovalna mreža Slovenije, Center za varnejši internet SAFE-SI

Povzetek

V članku predstavljamo različne nevarnosti, ki na uporabnike prežijo na družabnih omrežjih, kot so Facebook, Tviter in druga. Ogledali si bomo konkretne primere spletnih nevarnosti, s katerimi se srečujemo v okviru Centra za varnejši internet SAFE-SI ter Arnesovega SI-CERT. Pozornost bomo posvetili družabnim omrežjem kot medijem za širjenje zlonamerne kode in različnih prevar, sledili bodo primeri nevarnosti, ki izvirajo iz načrtnega ali nenačrtnega prekomernega objavljanja naših osebnih podatkov. Veliko družabnih aktivnosti se je v zadnjih letih z dvorišč preselilo na družabna omrežja, zato je nasilje med vrstniki danes najbolj pereč problem, s katerim se spopadajo mladostniki na spletu, dotaknili pa se bomo tudi spletne odvisnosti, ki ima pogostokrat simptome, ki so enaki tistim ob kemični odvisnosti. Na koncu članka bomo podali nekaj konkretnih predlogov, kako se uporabniki lahko zaščitijo pred različnimi tveganjem, tako na družabnih omrežjih kot na internetu na splošno.

Abstract

The paper presents various risks users face on social networks such as Facebook, Twitter and others. We'll examine specific examples of online risks encountered at SAFE-SI, the Slovenian National Awareness Centre, and ARNES' SI-CERT. We will focus on social networks as a medium for the distribution of malware and various frauds, followed by example risks arising from deliberate or inadvertent excessive publication of personal data. In recent years, much of our social activity has moved to social networks. As a consequence, peer violence is today the most pressing problem young people face online. We will also touch upon internet addiction, which often has the same symptoms as chemical addiction. The paper will finish by providing a few concrete suggestions on how users can protect themselves against various risks on social networks, and on the internet in general.

Uvod

Do prihoda družabnih omrežij smo bili uporabniki vajeni, da večina spletnih nevarnosti na nas preži na sumljivih spletnih straneh ali pa nas doseže preko elektronske pošte. S prihodom družabnih omrežij pa se je kar nekaj teh nevarnosti preselilo tudi na družabna omrežja, hkrati pa se vedno bolj soočamo tudi z novimi nevarnostmi, s katerimi se do sedaj na spletu še nismo srečevali. Tako se danes na družabna omrežja selijo goljufije in prevare, v nekaterih primerih pa se družabna omrežja uporabljajo tudi za distribucijo virusov in druge škodljive programske kode. Po drugi strani pa smo s prihodom družabnih omrežij uporabniki postali

sami sebi največji sovražniki, saj na le teh velikokrat nekritično objavljamo informacije o sebi in o drugih, prav tako pa se je velik del življenja posameznikov danes »preselil« z ulice na družabna omrežja.

Poleg požarnega zidu, protivirusnega programa in posodobljenega računalnika je naša najboljša zaščita na spletu poznavanje nevarnosti, s katerimi se na njem lahko srečamo. Le teh je danes sicer ogromno in praktično nemogoče se je seznaniti z vsako izmed njih. Zato pa nam bo ustrezno izobraževanje prineslo sposobnost prepoznavanja novih tveganj tisti hip, ko se bomo z njimi srečali. Tako kot se zavedamo, da moramo v množici ljudi poskrbeti, da nam kdo iz žepa ne ukrade denarnice, moramo v množici internetnega šuma prepoznati virus ali ukano ter presoditi, kaj na spletu lahko objavimo in kaj ne. Tega se zavedamo tudi sodelavci Slovenskega centra za varnejši internet SAFE-SI[1], zato delujemo preventivno in uporabnike spleta v čim večji meri izobražujemo in poizkušamo pripraviti na tveganja, ki se skrivajo med kopico uporabnih informacij, ki jih vsakodnevno prejemamo preko interneta.

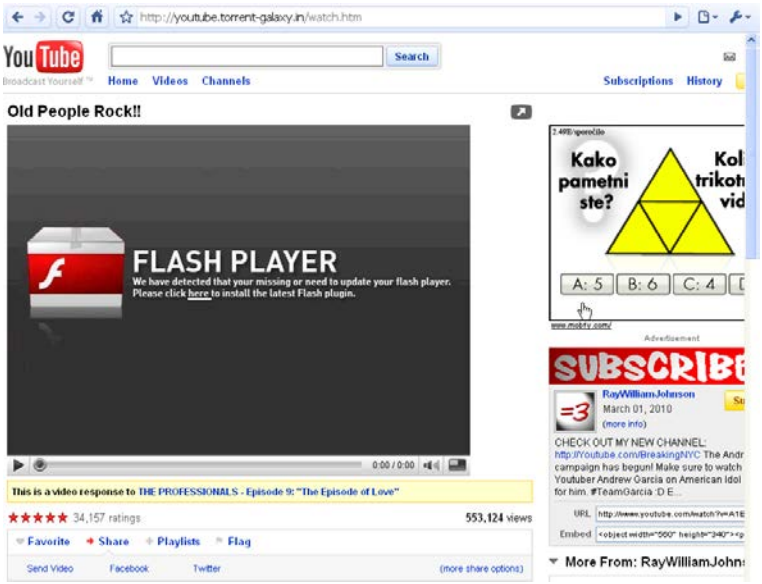
Tipi nevarnosti na družabnih omrežjih

Ko govorimo o nevarnostih na spletu in družabnih omrežjih, lahko le te razvrstimo v več kategorij. Tako lahko govorimo o tveganjih, ki na nas prežijo zaradi pomanjkljivosti na strojni ali programski opremi ter na tveganja, pri katerih je potrebna naša direktna interakcija, da postanemo žrtve. V raziskavi, ki jo je Microsoft opravil za obdobje med januarjem in junijem 2011 se je pokazalo, da je med uporabniki, ki so se okužili z zlonamerno kodo, kar 44,8 % aktivno pripomoglo k okužbi svojega računalnika. Hkrati je bilo zgolj 2,4 % okužb posledica napak v programski opremi, pa še za to programsko opremo so na spletu že bile dostopne posodobitve, vendar jih uporabniki niso namestili [1, str. 14-15]. Na družabnih omrežjih se tudi po oceni avtorja članka srečujemo predvsem s takšnimi tipi nevarnosti, pri katerih je za zlorabo potrebna uporabnikova direktna interakcija. Le teh je veliko, v nadaljevanju pa se bomo posvetili nekaj ključnim skupinam tveganj, s katerimi se najpogosteje srečujemo v okviru SAFE-SI.

[1] http://www.safe.si/, Projekt Center za varnejši internet SAFE-SI izvajajo Fakulteta za družbene vede, Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata pa ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za izobraževanje, znanost, kulturo in šport [2].

Širjenje virusov in prevar

Družabna omrežja pri širjenju virusov in prevar najpogosteje igrajo vlogo posrednika med dejanskim mestom okužbe in uporabnikom. Tako na primer uporabnik Facebooka preko statusnega polja, v katerem spremlja objave svojih prijateljev, prejme obvestilo kolega, ki ga vabi k ogledu določene vsebine. Uporabnik je nato preusmerjen na lažno spletno stran, ki ga poizkusi pod pretvezo prepričati, da bi na svoj računalnik namestil zlonamerno kodo. Povezava na spletno stran, ki želi podtakniti zlonamerno kodo, je bila tako objavljena celo na FB profilu enega izmed takratnih aktualnih slovenskih politikov. Uporabniki, ki so povezavi sledili, so bili nadalje preusmerjeni na spletne strani, ki so posnemale znani portal za predvajanje video posnetkov YouTube. Le te pa so nadalje uporabnika želele prepričati, da misleč da nalaga orodje za predvajanje videa, namesti virus [3] (na Sliki 1 lahko opazimo, da se v resnici nahajamo na spletnih straneh Torent-galaxy in ne YouTube, kot nas sicer želijo prepričati avtorji strani). Uporabnik, ki ukane ni odkril, in si je preko zgoraj omenjene spletne strani dejansko namestil virus, je na profilih svojih prijateljev najprej poskrbel za nadaljnje širjenje virusa. Prav tako pa je na svoj računalnik namestil program, ki napadalcu omogoča oddaljen dostop do njegovega računalnika, kar v praksi pomeni, da je napadalec lahko beležil njegove aktivnosti na spletu, videl vsa gesla, ki jih je nič hudega sluteči uporabnik vpisoval v spletne strani in uporabniku celo podtikal lažne spletne strani. »Dezinfekcija« računalniškega sistema, na katerem se nahaja tak virus, je sicer zahtevno in zamudno opravilo, bi se pa uporabnik takšne nevarnosti lahko obranil, če bi imela njegova protivirusna programska oprema ta virus že zaveden v svoji bazi. V tem primeru gre gotovo za eno izmed nevarnosti, ki lahko uporabniku potencialno povzroči razmeroma veliko škodo, na podobno povezavo pa bi lahko naleteli praktično na vsakem družabnem omrežju.



Slika 1: Distribucija virusa preko lažne YouTube strani

Vsak dan pa se na družabnih omrežjih srečujemo z manjšimi prevarami, ki pa za žrtev nimajo tako drastičnih posledic. V večini primerov gre tako za povezave oz. aplikacije, ki nam lažno obljubljajo prikaz atraktivnih oziroma kontroverznih video vsebin. Tako vam bo nekdo preko Facebook aplikacije na primer obljubljal domači pornografski posnetek znane pevke, ali pa posnetek, v katerem gromozanska kača poje svojega čuvaja (slika 2). Če se odločite za ogled povezave, boste nadalje verjetno preusmerjeni na spletno stran z ikono filma, preden si boste film lahko ogledali, pa boste pozvani, da ga delite s svojimi kolegi in izpolnite anketo. V takšnih primerih je presenetljivo glavni razlog za prevaro ravno v tem, da izpolnite anketo, saj avtor prevare od svojega naročnika prejme določeno plačilo za vsako anketo, ki jo izpolnijo nič hudega sluteče žrtve prevare. Tudi v konkretnem primeru videa s kačo, ki naj bi pojedla človeka, je bil uporabnik najprej usmerjen na spletno stran, ki je obljubljala prikaz videa, ob kliku na predvajanje posnetka pa je bil povabljen k izpolnjevanju ene izmed 3 anket [4]. Uporabnik video posnetka seveda ni videl niti po tem, ko je izpolnil anketo.

Slika 2: Povezava na lažni video posnetek

Dobra novica sicer je, da se sploh v zadnjem času skrbniki družabnih omrežij aktivno borijo proti takšnim prevaram in onemogočajo aplikacije oz. povezave, ki bi nas pripeljale do teh

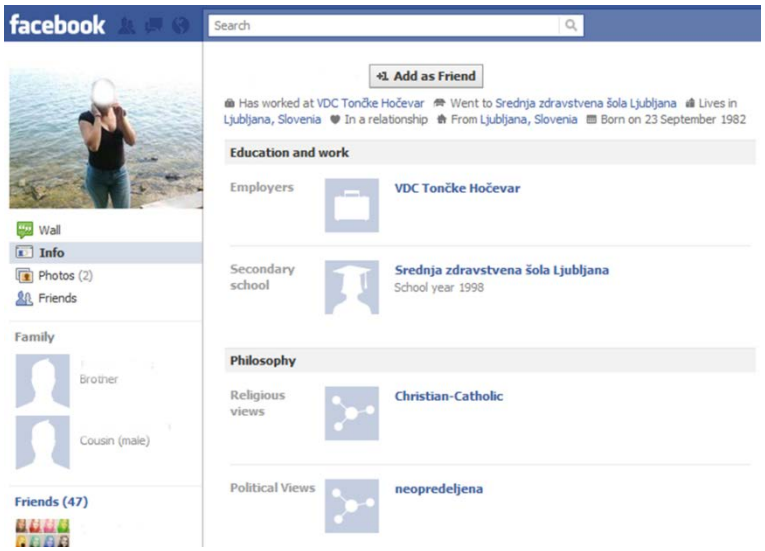
nevarnosti, najbolj pa bomo kljub vsemu varni le, če bomo sami pozorni na povezave, ki jih odpiramo.

Prekomerno objavljanje osebnih podatkov

S prihodom družabnih omrežij smo uporabniki začeli pogostokrat popolnoma nekritično objavljati večjo količino osebnih podatkov. Tako bomo npr. na našem Facebook profilu objavili sliko včerajšnje večerje skupaj z našim rojstnim datumom, na Tviterju pa radi objavljamo kje se ta hip nahajamo in s tem potencialnim vlomilcem olajšamo delo[2]. Razlogov za takšno nekritično objavljanje podatkov o nas na družabnih omrežjih je več, avtor članka pa je mnenja, da je ključni razlog ta, da želimo, da tudi drugi vidijo, kaj se z nami dogaja. Morda celo želimo s takšnimi objavami do neke mere zbuditi ljubosumnost pri naših prijateljih na družabnih omrežjih. Celo osebne podatke, s pomočjo katerih je danes možna tudi kraja identitete, na družabnih omrežjih pogosto delimo kar s celim svetom, kar dokazuje profil uporabnice, ki je poleg imena, priimka, datuma rojstva in fotografij na družabnem omrežju objavila tudi posebej občutljive osebne podatke, kot so politično in versko prepričanje (slika 3).

Ne glede na to, da družabna omrežja danes ponujajo pestro izbiro nastavitev prikaza posameznih podatkov, uporabniki v veliko primerih le teh ne izkoristimo. Tako ostanemo na privzetih nastavitvah prikaza osebnih podatkov, ki pa so v večini primerov dokaj odprte, kar je sicer razumljivo, saj je želja lastnikov družabnih omrežij čim več ogledov in prikazov vsebin, kar jim seveda prinaša večje prihodke od oglaševanja. Za primerjavo, v letu 2005 je bilo na družabnem omrežju Facebook ob kreiranju profila ostalim uporabnikom Facebooka privzeto vidnih 4 od 11 opazovanih skupin osebnih podatkov, v letu 2010 pa že kar 9 od 11 [6].

[2] Dekletu, ki je na družabnem omrežju objavilo, da je nekaj ur ne bo doma, so njeni tako imenovani prijatelji z družabnih omrežij v tem času dejansko vlomili v stanovanje in jo okradli [5].



Slika 3: Objava osebnih podatkov na Facebooku

Posebno poglavje v tej zgodbi pa so tudi načrtne objave vsebin, najpogosteje fotografij, ki morda ne sodijo na splet. Po eni strani takšno vsebino enkrat, ko je objavljena, zelo težko umaknemo s spleta, po drugi strani pa se nam v določenem življenjskem obdobju nekatere vsebine zdijo ustrezne in celo atraktivne, ko pa postanemo starejši, pa se naše mnenje lahko popolnoma spremeni. Na posvetu ob Dnevu varne rabe internetu, ki je potekal na Osnovni šoli Trnovo, so prisostvovali tudi osnovnošolci. Na tem posvetu je bila ohrabrujoča informacija, da se danes med otroki že dogaja nekakšna regulacija znotraj skupnosti, ki v primeru, da nekdo objavi neprimerno vsebino, spodbudi skupnost, da ustvari pritisk na tistega, ki je to vsebino objavil in ga prisili, da to neustrezno vsebino umakne.

Družabna omrežja kot dvorišča (stranišča)

Če smo medsebojne spore pred desetletjem še reševali na dvoriščih, pa se danes takšne »obšolske« dejavnosti vedno bolj selijo na družabna omrežja. V primeru, da nam učitelj pred desetletjem ni bil všeč, smo to preprosto napisali na steno šolskega ali fakultetnega stranišča, množica ljudi, ki jo je takšno obvestilo dejansko doseglo, pa je bila razmeroma majhna. Danes za učitelje odpiramo skupine in strani na družabnih omrežjih, kjer pa so ta obvestila naenkrat dosegljiva celemu svetu. Tako smo na Arnesu obravnavali primer, kjer je skupina dijakov iskala podporo za zažig lastne šole (slika 4). Ta primer nazorno nakazuje, kako nam lahko splet v takšni situaciji zamegli razum. V roku nekaj ur je preko družabnega omrežja Facebook podporo zažigu šole s svojim pravim imenom, priimkom in sliko izrazilo kar 60 učencev. Vendar pa je avtor članka prepričan, da v živo takšne podpore učenci verjetno nikoli ne bi izrazili, prav tako pa meni, da otroci niti pomislili niso, kako hudo dejanje podpirajo s tem, ko

preko spleta pritisnejo gumb. Govorili bi lahko celo o pomanjkanju odgovornosti. Podobnih strani, namenjenih šolam in učiteljem je kar nekaj, vendar pa se učitelji in ravnatelji pogosto ne zavedajo, da lahko od skrbnikov Facebooka zahtevajo umik spornih ali škodljivih vsebin.

Slika 4: Zbiranje podpore za zažig šole

Na tem mestu moramo omeniti tudi nasilje med vrstniki, ki je po raziskavi EU Kids online glavni dejavnik nelagodja otrok na spletu [7, str. 24-25]. Tako lahko govorimo o izolaciji posameznikov, nadlegovanju preko spleta, poudariti pa moramo, da so še posebej rizični tisti posamezniki, ki so tudi v »fizičnem svetu« velikokrat žrtve takšnega nasilja. Po mnenju avtorja sicer večina razlogov za nasilje med vrstniki, ki se odvija na spletu, izvira iz ravno iz tega fizičnega sveta, zato jih je v le tem tudi potrebno reševati. Po naših izkušnjah je v večini primerov zelo dobrodošla tudi pomoč zaposlenih na šoli.

Ostale nevarnosti

Različnih pasti je na spletu ogromno, zato bralca vabimo k ogledu spletni strani SAFE-SI[3] in Arnesovega projekta Varninainternetu[4], kjer se lahko seznanijo z aktualnimi primeri spletnih tveganj ali zgolj najdejo informacije o tem, kako se pred njimi ustrezno zaščitijo. Na tem mestu omenimo le še spletno odvisnost[5], katere simptomi so zelo podobni kemični odvisnosti. Napotek staršem, učiteljem, mladostnikom in drugim uporabnikom spleta je, naj pozorno

[3] http://www.safe.si/
[4]http://www.varninainternetu.si/
[5] Bralca vabimo k izpolnjevanju vprašalnika, s katerim lahko preveri, če je zasvojen s spletom in novimi tehnologijami: http://www.safe.si/c/1109/Ali_sem_eodvisnik/?preid=672

opazujejo svoje početje in početje svojih bližnjih ter v primeru suma na odvisnost čim hitreje reagirajo oziroma najdejo ustrezno pomoč.

Kaj lahko storimo sami

Najprej poskrbimo za ustrezno zaščito računalnika, kar pomeni nameščen požarni zid, protivirusni program z aktualnimi posodobitvami ter posodobljen operacijski sistem in aplikacije ter module, kot je na primer Adobe Flash. Zagotovimo, da so naša gesla ustrezna[6] ter da na računalniku uporabljamo več uporabniških imen z različnimi pravicami dostopa. Še posebej na družabnih omrežjih bodimo pozorni, kaj objavljamo, saj nikoli ne vemo, kdaj lahko kateri izmed naših spletnih prijateljev zlorabi naše zaupanje. Prav tako ne zaupajmo osebam, ki jih ne poznamo, ne glede na to, s kako privlačno sliko se nam predstavljajo. In ne-nazadnje, seznanimo se s čim več različnimi primeri spletnih tveganj, saj bomo tako zelo povečali verjetnost, da bomo podobno tveganje v prihodnosti sposobni prepoznati tudi sami.

Literatura

1. Microsoft. *Microsoft Security Intelligence Report. Vulume 11*. 2011. Dostop: http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf (5. 6. 2012).

2. SAFE-SI. *O projektu*. 2012. Dostop: http://www.safe.si/c/712/O_projektu/ (5. 6. 2012).

3. SI-CERT. *Politika je lahko tudi nevarna!* 2010. Dostop: http://www.cert.si/obvestila/obvestilo/article/politika-je-lahko-tudi-nevarna.html (5. 6. 2012).

4. Facecrooks. *Snake Eats Man! Caught on Tape – Facebook Scam*. 2012. Dostop: http://facecrooks.com/Scam-Watch/video-snake-eats-man-caught-on-tape-facebook-scam.html (5. 6. 2012).

5. Fox59. *Woman robbed by facebook friend*. 2010. Dostop: http://www.fox59.com/news/wxin-facebook-friend-robbery-080610,0,3487314.story (6. 6. 2012)

[6] Glej na primer: http://nakedsecurity.sophos.com/2012/05/25/how-long-would-it-take-to-crack-your-password/

6. McKeon, Matt. *The Evolution of Privacy on Facebook*. 2010. Dostop: http://mattmckeon.com/facebook-privacy/ (5. 6. 2012).

7. Livingstone, Sonia in Leslie Haddon. *EU Kids Online*. 2012. Dostop: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/Final%20report.pdf (5. 6. 2012).