UNIVERZA V LJUBLJANA
FAKULTETA ZA DRUŽBENE VEDE

Tamara Žgajnar

Družbeni mediji na spletu in kraja identitete

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANA
FAKULTETA ZA DRUŽBENE VEDE

Tamara Žgajnar

Mentorica: izr. prof. dr. Tanja Oblak-Črnič

Družbeni mediji na spletu in kraja identitete

Diplomsko delo

Ljubljana, 2009

Družbeni mediji na spletu in kraja identitete

Uporaba družbenih medijev na spletu iz leta v leto narašča, skladno s tem pa naraščajo tudi skrbi glede nevarnosti, ki jih uporaba teh spletnih orodij lahko predstavlja za uporabnika. Med morebitne varnostne grožnje spada tudi kraja identitete. V diplomski nalogi zato poskušam preko analize primarnih in sekundarnih virov ter z analizo teksta ugotoviti, ali je stopnja nevarnosti za uporabnike res tako velika ali pa gre bolj za ustvarjanje moralne panike s strani medijev. Za analizo sem izbrala *Facebook*, *Twitter*, *Flickr* in *YouTube*, pri katerih sem analizirala varnostne nastavitve, ki jih ponujajo svojim uporabnikom, in njihova načela o varnosti ter zasebnosti.
Pregled varnostnih nastavitev pri teh štirih družbenih medijih je pokazal, da vsi izmed njih uporabniku ponujajo veliko varnostnih mehanizmov, s katerimi lahko zavaruje svoje osebne podatke ter se s tem zaščiti pred krajo identitete. Na nevarnosti, ki jih lahko predstavlja objavljanje osebnih informacij, opozarjajo tudi v načelih o varnosti in zasebnosti. Uporaba spletnih družbenih medijev za uporabnike in njihovo zasebnost sama po sebi torej ne predstavlja velike grožnje. Odgovornost je predvsem na strani uporabnika in njegove premišljene uporabe orodij, ki jih družbeni mediji na spletu ponujajo.

Ključne besede: družbeni mediji na spletu, kraja identitete, identiteta, virtualna družbena omrežja

Social media and identity theft

Social media usage is growing every year. Along with it are growing concerns about potential dangers that usage of this on-line tools might create. Among these is also identity theft. I analyzed primary and secondary sources, and used text analysis to find out whether the users are really endangered or it is the fear of identity theft more of a moral panic created by the media. I used Facebook, Twitter, Flickr and YouTube to analyze their privacy settings and their privacy and safety policies.
Privacy settings review showed that users can secure their personal data with many different safety mechanisms offered by these four social media. Their privacy and safety policies include also several warnings and information about the dangers that publishing personal data on users' profiles may create. Analysis shows that social media usage does not necessarily represent a threat to its users. Responsibility lies primarily on users and their careful usage of tools offered by social media.

Key words: social media, identity theft, identity, virtual social networks

Kazalo

1 UVOD

Uporaba interneta iz leta v leto narašča. Pri tem niso izjema niti družbeni mediji na spletu, ki so med uporabniki interneta vsako leto bolj priljubljeni. Podatki iz leta 2009 (RIS 2009b) kažejo, da je junija v ZDA spletni družbeni medij Facebook obiskalo kar 87,3 milijona različnih obiskovalcev, kar je bilo 200 % več kot v enakem obdobju leta 2008. Podatki iz junija 2009 (RIS 2009a) kažejo, da so ameriški uporabniki za brskanje po vsebinah Facebooka v mesecu aprilu porabili 13,9 milijard minut časa. To je bilo kar 700 % več kot v enakem obdobju leta 2008. Tudi obisk spletnega družbenega medija Twitter, katerega uporaba se v ZDA najhitreje širi, je od leta 2008 do leta 2009, torej v enem letu, narasla iz dobrega milijona obiskovalcev do skoraj 21 milijonov (RIS 2009b). Statistike kažejo, da priljubljenost družbenih medijev na spletu narašča tudi v Sloveniji. Podatki iz prvega četrtletja 2009 (STAT 2009) kažejo, da se je delež posameznikov v starosti od 10 do 74 let, ki so internet uporabljali za različne oblike komuniciranja, torej tudi preko spletnih družbenih medijev, povečal. V Sloveniji je tako v začetku leta 2009 22 % ženskih in 23 % moških uporabnikov interneta oblikovalo ter urejalo lasten profil na vsaj enem izmed spletnih družbenih medijev. Že leta 2007 (RIS 2009c) je bil Myspace med desetimi najbolj obiskanimi spletnimi stranmi v Sloveniji, v zadnjem času pa se povečuje predvsem obisk Facebooka, ki ima tudi v Sloveniji že več kot 200.000 članov.

V zadnjih nekaj letih so se spletni družbeni mediji zelo razširili, razvili in postali popularni med uporabniki različnih starosti. Zaradi svojih povezovalnih, informacijskih, skupnostnih in zabavnih potencialov vsako leto pritegnejo vse večje število uporabnikov. Mayfield (2008, 5) ugotavlja, da njihova odprtost oz. dostopnost spodbuja sodelovanje, komentiranje in posredovanje informacij. Vse to seveda ob predpogoju, da imajo posamezniki zagotovljen dostop do interneta. Uporaba spletnih družbenih medijev posameznikom omogoča oblikovanje virtualnih socialnih omrežij, preko katerih lahko ohranjajo in utrjujejo že obstoječe odnose iz realnega sveta. Istočasno si lahko uporabniki svoje virtualno socialno omrežje razširijo tudi z ustvarjanjem novih odnosov in vezi z neznanci z različnih koncev sveta.

Splet in tudi spletni družbeni mediji uporabnikom omogočajo, da pri interakciji z drugimi ohranijo določeno mero anonimnosti. Le-ta jim daje možnost ustvarjanja nove in »nerealne« identitete, ki služi kot sredstvo identifikacije v virtualnem svetu. S tem uporabniki spletnih družbenih medijev nimajo nobenega zagotovila, da drugi uporabniki realno reprezentirajo sami

sebe. Zavajanje drugih in predstavljanje samega sebe z umetno ustvarjeno ali prevzeto identiteto je lahko sicer povsem brez posledic. Lahko pa predstavlja resno grožnjo za druge uporabnike spletnih družbenih medijev in vodi celo v krajo identitete.

Z vsemi prednostmi spletni družbeni mediji uporabnikom torej prinašajo tudi nova tveganja. Vse večjo pozornost tem tveganjem posvečajo tudi mediji. Tako je bil na primer leta 2008 (Pirc Musar in Rupnik 2008) v spletni izdaji Dnevnika objavljen članek o nevarnostih, ki jih predstavlja uporaba spleta. V njem avtorici izpostavita tudi nevarnost kraje identitete in objavljanja osebnih podatkov na spletnih družbenih medijih. Tudi letos je bilo v medijih objavljenih več člankov, ki obravnavajo prav nevarnost kraje identitete v povezavi z uporabo spleta. Eden izmed njih je bil članek v spletni izdaji Žurnala24 (Z. 2009), v katerem avtor obravnava spletno in mobilno nadlegovanje ter različne oblike nasilja nad uporabniki spleta, kamor uvrsti tudi krajo identitete. Čeprav mnogi mediji tako vse pogosteje opozarjajo na nevarnost kraje identitete zaradi aktivne uporabe spletnih družbenih medijev, pa situacija ni tako kritična. Mohan (2009, 157) ugotavlja, da strah pred krajo identitete kreirajo in vzpodbujajo mediji, policija, bančne institucije in osebne zgodbe prijateljev, sorodnikov ter sosedov, ki so morda bežno izkusili to nevarnost. Vendar pa strah pred tem, da bi postali žrtev, močno presega dejansko nevarnost in konkretne primere, obenem pa prihaja tudi do ekstremnih ukrepov za njihovo preprečevanje. Mohan (2009, 157) zato trdi, da bi strah pred krajo identitete lahko označili celo za moralno paniko.

V nadaljevanju besedila bom zato preko analize primarnih in sekundarnih virov poskušala ugotoviti, kakšno nevarnost za krajo identitete družbeni mediji na spletu dejansko predstavljajo – ali je strah upravičen ali pa gre dejansko bolj za ustvarjanje moralne panike. V prvem delu bom tako poskušala definirati, kaj družbeni mediji na spletu sploh so in kaj omogočajo posameznikom. V drugem delu se bom osredotočila na sam pojem identitete in na njeno povezavo z virtualnim svetom ter s spletnimi družbenimi mediji. Glavni poudarek v tretjem delu naloge bom posvetila možnostim za krajo identitete na spletnih družbenih medijih. V zadnjem delu naloge pa bom preko analize Facebooka, Twitterja, Flickrja in YouTuba predstavila, kakšne varnostne nastavitve in varnostna načela imajo ter s tem poskušala pokazati, kolikšno nevarnost za krajo identitete njihova aktivna uporaba res predstavlja.

2 DRUŽBENI MEDIJI NA SPLETU

Zametki prvih družbenih omrežij na spletu so bili že v 60. letih 20. stoletja (računalniški izobraževalni program Plato z univerze v Illinoisu), vendar pa je do pravega razvoja in zanimanja za družbene medije na spletu prišlo šele po razvoju in uveljavitvi interneta (Gross in Acquisti 2005, 1). V zadnjih nekaj letih so družbeni mediji in njihova uporaba prerasli iz majhnega nišnega fenomena v popularno spletno orodje, ki ga uporabljajo množice (Gross in Acquisti 2005, 1). Danes je na spletu vrsta različnih družbenih medijev. Poleg tega lahko pričakujemo, da bo razvoj in širjenje uporabe interneta prispevalo tudi k oblikovanju novih. Kljub vsej tej raznolikosti pa imajo spletni družbeni mediji eno glavno skupno lastnost – povezovanje ljudi. Kot ugotavljata Boydova in Ellisonova (2007, 1), večina spletnih družbenih medijev podpira in omogoča ohranjanje že obstoječih družbenih vezi ter omrežij. Vendar pa mnogi med njimi neznancem omogočajo povezovanje in spoznavanje z drugimi ljudmi, ki jih družijo skupni interesi, politično prepričanje ali druge dejavnosti. Različni družbeni mediji imajo tako različno ciljno publiko – nekateri nagovarjajo raznoliko občinstvo, drugi pa se osredotočajo na ljudi, ki jih druži skupen jezik, rasa, spolne preference, versko prepričanje ali nacionalna pripadnost. Uporabniki spletnih družbenih medijev lahko tako oblikujejo svoja spletna družbena omrežja, ki so sestavljena zgolj iz ljudi, s katerimi so že povezani, ali pa svoje družbeno omrežje razširijo izven kroga že poznanih ljudi in se povezujejo tudi z neznanci.

Evans (v Orsini 2009, 2) družbene medije na spletu prikaže kot možnosti za demokratizacijo informacij in preoblikovanje ljudi iz bralcev vsebin k oblikovalcem vsebin. Ugotavlja, da družbeni mediji na spletu uporabijo »modrost množic« za povezovanje informacij na kolektiven način. Iz tega sledi, da imajo družbeni mediji na spletu tri pomembne značilnosti, in sicer: spodbujajo dvosmerno interakcijo, so kolektivni in demokratični (Orsini 2009, 2). Družbeni mediji so torej spletni sistemi, ki posameznikom omogočajo, da ustvarijo javen ali delno javen osebni profil, si oblikujejo spisek ostalih uporabnikov, s katerimi so povezani, in pregledujejo svoje povezave ter povezave drugih (Boyd in Ellison 2007, 2). Poleg dvosmernosti v komunikaciji, kolektivnosti in demokratičnosti je značilnost družbenih medijev na spletu tudi odprtost oz. dostopnost, saj večina omogoča uporabo ter sodelovanje vsem, vzpodbuja komentiranje in posredovanje informacij. Spletni družbeni mediji omogočajo tudi hitro oblikovanje skupnosti, v katerih lahko člani med seboj učinkovito komunicirajo in delijo skupne

interese. To vzpodbuja povezanost med uporabniki, obenem pa tudi drugačne oblike povezovanja z drugimi spletnimi mesti in viri.

2.1 Oblikovanje osebnega profila in medosebnih stikov

Ko se uporabnik registrira in pridruži spletnemu družbenemu mediju, najprej oblikuje svoj uporabniški profil. Uporabniški profil je kot nekakšna osebna izkaznica, kjer lahko uporabnik posreduje svoje osebne podatke, doda fotografijo, opis samega sebe itd. Pri večini spletnih družbenih medijev potem lahko začne z dodajanjem »prijateljev« v svoje spletno družbeno omrežje. »Prijatelji« so lahko ljudje, s katerimi ima uporabnik že oblikovan odnos v realnem svetu, lahko pa so tudi popolni tujci, ki jih spozna preko družbenega medija. Od posameznega spletnega družbenega medija je odvisno, ali dodajanje »prijateljev« poteka neregulirano ali pa je za to potrebna prošnja enega izmed uporabnikov in privolitev drugega uporabnika. Ko sta uporabnika spletna »prijatelja«, dobita dostop do profilov drug drugega, kjer lahko pregledujeta objavljene vsebine. Poleg dodajanja »prijateljev« lahko uporabniki spletnih družbenih medijev objavljajo kratka sporočila, fotografije, video posnetke, daljše zapise, spremljajo aktivnosti »prijateljev«, dodajajo dogodke, pošiljajo javna ali zasebna sporočila, se pogovarjajo z drugimi uporabniki itd. (Dwyer in drugi 2007, 1).

2.1.1 Oblikovanje profila na Facebooku

Facebook je spletni družbeni medij, katerega glavni namen naj bi bilo povezovanje ljudi z njihovimi prijatelji in drugimi, ki študirajo, delajo ali živijo v njihovem krogu (Facebook 2009). Za aktivno uporabo Facebooka se mora posameznik najprej registrirati. Postopek registracije je enostaven, saj je potrebno posredovati samo ime, priimek, naslov elektronske pošte, geslo, spol in rojstni datum. Obrazložitev zahteve po navedbi rojstnega datuma je, da naj bi ta podatek vzpodbujal avtentičnost uporabnikov in zagotavljal, da se registrirajo samo dovolj stari posamezniki. Starostna omejitev za uporabnike Facebooka je namreč 13 let.

Z registracijo dobi uporabnik dostop do vseh funkcij, ki jih Facebook ponuja. Svoj profil lahko uporabniki dopolnijo z različnimi informacijami. Facebook jim omogoča, da na svojem profilu objavijo podatke o sebi, kar obsega vse od objave imena do podrobnega opisa njihovih interesov, kontaktnih informacij in podatkov o izobrazbi. Preko profila se uporabniki nato povežejo z drugimi posamezniki na Facebooku in s tem širijo svoje virtualno socialno omrežje.

Sprejemanje »prijateljev« poteka regulirano, saj mora eden izmed uporabnikov najprej poslati prošnjo za »prijateljstvo« drugemu, le-ta pa jo mora potrditi. Šele s tem uporabnika dobita dostop do profilov in informacij drug drugega. Lahko si puščata sporočila na zidovih, pošiljata zasebna sporočila, se pogovarjata itd. Poleg tega lahko vsak uporabnik objavlja fotografije in video posnetke, na katerih lahko poimensko označi akterje. Uporabniki imajo tudi možnost za pisanje blogov, krajših zapisov, objavljanja povezav in oblikovanja skupin ali dogodkov. K sodelovanju oz. udeležbi na slednjih lahko povabijo svoje »prijatelje«. Z različnimi aplikacijami, med katere spada vse od koledarja z rojstnimi dnevi »prijateljev«, različnih virtualnih daril, ki si jih lahko »prijatelji« pošiljajo med seboj, do različnih spletnih iger, lahko uporabniki svoj profil dopolnijo glede na svoje interese. Sam izgled in možnosti, ki jih Facebook ponuja, se pogosto spreminjajo[1], s čimer se posamezniku ponujajo novi načini in možnosti za uporabo Facebooka.

2.1.2 Oblikovanje profila na Twitterju

Spletni družbeni medij Twitter svojim uporabnikom omogoča povezovanje z drugimi preko pošiljanja kratkih, 140 znakov dolgih sporočil. Preden lahko posameznik dobi dostop do vseh funkcij, ki jih Twitter ponuja, se mora registrirati kot uporabnik. Za to posameznik potrebuje ime in elektronski naslov. Določi tudi uporabniško ime in geslo ter na koncu vtipka avtomatizirano sporočilo.

Po registraciji lahko uporabnik dopolni svoj profil z različnimi informacijimi (biografija, trenutna lokacija, osebna spletna stran itd.). Poleg tega lahko posameznik k profilu doda tudi svojo fotografijo. Zaradi same narave tega spletnega družbenega medija, ki se osredotoča na mikrobloganje, je tudi količina informacij, ki jih lahko uporabnik posreduje na svojem profilu, omejena. Biografija je tako lahko dolga zgolj 160 znakov. Pri definiranju trenutne lokacije uporabnik določi samo mesto, kjer se nahaja, pri opisu osebne spletne strani lahko napiše samo povezavo do le-te. Dodajanje »prijateljev« oz. sledilcev, kot se člani uporabnikovega socialnega omrežja imenujejo na Twitterju, poteka bodisi regulirano ali neregulirano. V primeru, da ima uporabnik javen račun, kar pomeni, da imajo dostop do profila in sporočil, poslanih preko

[1] Samo v letu 2009 je prišlo do več sprememb v izgledu in funkcijah Facebooka. Med drugim je bila dodana možnost »všeč mi je«, s katero lahko uporabniki komentirajo status, fotografijo, povezavo itd. svojih »prijateljev«, dodana je bila možnost oblikovanja in uporabe Facebook uporabniškega imena, vpeljan je bil t.i. FriendFeed (Facebook 2009).

Twitterja vsi, lahko tudi kdor koli postane sledilec. Kadar ima uporabnik svoj račun zaklenjen, pa mora vsak, ki mu želi slediti, najprej poslati prošnjo.

2.1.3 Oblikovanje profila na Flickrju

Flickr je spletni družbeni medij, ki uporabnikom omogoča preprosto nalaganje, objavljanje in komentiranje fotografij na spletu. Fotografije, objavljene na Flickrju, lahko pregleduje kdor koli, čeprav ni registriran uporabnik. Le slednji imajo tudi možnost objavljanja fotografij. Ker Flickr spada pod okrilje Yahooja, se lahko tisti posamezniki, ki uporabljajo Yahoo Mail, registrirajo kar z uporabniškim imenom in geslom, ki ga uporabljajo za dostop do elektronske pošte. Drugi uporabniki morajo za registracijo izpolniti obrazec, potreben za uporabo Yahoo elektronskega naslova, ki zahteva ime, spol, rojstni datum, državo, poštno številko, izbiro gesla in uporabniškega imena ter varnostno vprašanje, ki je v pomoč v primeru, da uporabnik pozabi svoje geslo.

V okviru svojega profila lahko uporabnik izpolni različne kategorije (ime, priimek, časovni pas, v katerem se nahaja, spol, status itd.), vendar se vsak uporabnik sam odloči ali bo svoj profil dopolnil s temi informacijami, saj le-to ni pogoj za aktivno uporabo računa. Flickr uporabnikom ne omogoča zgolj nalaganja in objavljanja fotografij, ampak lahko uporabniki tudi označujejo in komentirajo fotografije, jih nalagajo v galerije in si s povezovanjem z drugimi uporabniki oblikujejo svoje socialno omrežje.

2.1.4 Oblikovanje profila na Youtubu

YouTube je spletni družbeni medij, ki uporabnikom omogoča nalaganje, pregledovanje, komentiranje, označevanje in ocenjevanje video posnetkov. Vsak uporabnik lahko gleda objavljene posnetke, ne da bi se zato moral registrirati. Za objavljanje, komentiranje, ocenjevanje, označevanje ali ogled video posnetkov z vsebino, ki je neprimerna za mlajše osebe, je potrebna registracija. Registracija zahteva izbiro uporabniškega imena, določitev lokacije, poštne številke, datuma rojstva, spola in potrditev pogojev uporabe.

Po registraciji lahko uporabnik svoj profil dopolni z mnogimi osebnimi informacijami, med drugim lahko doda svoje ime, starost, domače mesto, državo, šolo, poklic, hobije itd. Vendar pa nobena izmed teh informacij ni predpogoj za nadaljnjo uporabo. V okviru svojega profila lahko

nato uporabnik piše oz. objavlja tudi blog, oblikuje različne kanale, preko katerih objavlja svoje video posnetke, prilagaja ozadja itd.

2.2 Oblikovanje družbenih omrežij

Tako kot si ljudje ustvarjamo družbena omrežja v svojem vsakdanjem življenju, si tudi uporabniki družbenih medijev na spletu ustvarijo svoje virtualno družbeno omrežje. Ponavadi je veliko članov družbenega omrežja, ki si ga posameznik ustvari na spletu, del posameznikovega izvenspletnega družbenega omrežja. Vendar pa izvenspletna povezanost ni predpogoj, da posameznik postane član spletnega družbenega omrežja. Spletno družbeno omrežje je lahko sestavljeno tudi iz popolnih tujcev, ki z uporabnikom družbenega medija v realnem svetu nimajo nobenega stika. Kljub temu mnogi spletni družbeni mediji služijo kot podpora in pomoč pri ohranjanju že obstoječih družbenih omrežij, ki jih ima posameznik v realnem svetu. Vezi s člani teh družbenih omrežij so lahko šibke, vseeno pa posameznike, ki zaprosijo za »prijateljstvo« v spletnem družbenem omrežju, pogosto veže neki skupen element z lastnikom profila (Boyd in Ellison 2007, 11).

Vendar pa je eden izmed razlogov, zakaj ljudje postanejo uporabniki družbenih medijev na spletu, tudi spoznavanje novih ljudi. Zato uporabniki pogosto sprejmejo v svoje spletno družbeno omrežje tudi popolne neznance. Ross in Acquisti (2005, 3) ugotavljata, da so v povprečju spletna družbena omrežja obširnejša, obenem pa njihove člane vežejo tudi precej šibkejše vezi kot v družbenih omrežjih, ki si jih ljudje ustvarijo v realnem svetu. Na tisoče uporabnikov spletnih družbenih medijev je lahko kategoriziranih kot »prijatelji« posameznega uporabnika. Taka kategorizacija jim omogoča, da dostopajo do zasebnih informacij, ki jih uporabnik razkrije na svojem profilu. Povedano drugače, to pomeni, da so lahko osebni podatki, kot so polno ime, rojstni datum, naslov itd. dostopni popolnim neznancem, ki jih uporabnik sploh ne pozna. S tem posamezniki svojo zasebnost naredijo dostopno popolnim neznancem in se izpostavijo nevarnosti, da postanejo žrtev kraje identitete.

2.3 Komuniciranje na spletnih družbenih medijih

Ena glavnih dejavnosti v okviru družbenih medijev na spletu je interakcija z drugimi uporabniki. Uletova (2005, 73) ugotavlja, da sta znanje o okoliščinah in interpretiranje situacije, v kateri je posameznik, dva bistvena dejavnika, ki vplivata na komuniciranje. Posameznik si

mora torej razjasniti, v kakšni »komunikacijski situaciji« se je znašel. Le-ta pa je sestavljena iz udeležencev, kraja, dejavnosti in komunikacijskega dogajanja oz. povedano drugače iz tega, kdo, kje, kaj in kako komunicira. Razumevanje tega udeležencem v komuniciranju namreč pomaga, da se na različne situacije v procesu komunikacije ustrezno odzovejo (Ule 2005, 73). To je pomembno predvsem zato, ker je komuniciranje »bistveno odvisno od občutka za razlike med ljudmi in obenem od želje, da bi kljub tem razlikam razumeli drug drugega, torej, da bi ustvarili skupno podlago za pogovor« (Ule 2005, 78). Komuniciranje potemtakem temelji vsaj na minimalnem poznavanju med udeleženci interakcije.

Enak predpogoj za uspešno komuniciranje velja tudi pri interakciji v okviru spletnih družbenih medijev. Posamezniki morajo v virtualnem svetu posredovati določene informacije o samih sebi, saj s tem drugim omogočijo interpretiranje komunikacijske situacije. Ker pa virtualnost uporabnikom omogoča, da ohranijo določeno mero anonimnosti, jim to daje možnost, da si lahko ustvarijo povsem nove identitete, ki jim služijo kot sredstvo identifikacije v virtualnem svetu. Reprezentacije udeležencev v komuniciranju preko spletnih družbenih medijev so torej lahko delno ali povsem izmišljene. Mediji, ki vzpodbujajo računalniško-posredovano komuniciranje, so namreč zameglili meje posameznikove identitete (Rheingold 2000, 151).

3 INTERAKCIJA IN RAZKRIVANJE POSAMEZNIKOVE IDENTITETE NA SPLETU

Za socialno interakcijo je nujno potrebno, da udeleženci v komuniciranju med interakcijo razkrijejo vsaj nekaj podatkov o samih sebi. Udeleženci interakcije drug z drugim delijo določene informacije o tem, s kom pravzaprav komunicirajo, kar pomeni, da drug drugemu razkrijejo vsaj del svoje identitete (Lahlou 2008, 309-310). Vendar pa Lahlou (2008, 310) ugotavlja, da je vprašanje identitete posameznika zelo kompleksno, saj zajema tako to, kako posameznik dojema samega sebe s svojega subjektivnega stališča, kot tudi to, kako posameznik samega sebe definira pred drugimi. Na podlagi tega Lahlou predlaga tri vidike za določanje identitete – *fizični*, torej subjekt kot fizično telo; *družbeni*, torej subjekt kot družbena pozicija; in *biografski*, torej subjekt kot produkt preteklih izkušenj in želja.

Ko na identiteto gledamo s fizičnega vidika, le-ta vključuje človeka kot fizično telo. K identifikaciji posameznika pripomorejo njegove fizične značilnosti – zunanji izgled, obrazne

poteze, prstni odtisi, glas itd. Pri interakciji v virtualnem okolju pa je fizično telo zelo omejeno, saj udeleženci v komunikaciji niso fizično prisotni drug z drugim. Fizična identiteta je pri taki obliki interakcije uporabna lahko samo takrat, ko je povezana z datotekami, ki opisujejo posamezne karakteristike udeleženca v interakciji (npr. baza prstnih odtisov, glasovna identifikacija).

Drugi, družbeni vidik identitete, vključuje, kaj posameznik predstavlja drugim oz. kako posameznika dojemajo drugi okoli njega. Družbena identiteta je sestavljena iz kombinacije vlog in statusa, ki jih ima posameznik v družbi. Vloge pri tem predstavljajo vzorce obnašanja, ki jih drugi pričakujejo od posameznika, status pa predstavlja ravno obratno – vzorce obnašanja, ki jih posameznik lahko pričakuje od drugih. Kot taka lahko družbena identiteta posreduje uporabne namige udeležencem interakcij v virtualnem svetu.

Tretji vidik identifikacije posameznika pa je psihološki in subjektiven. Posameznika oblikujejo njegova preteklost, dejanja, želje, izkušnje. Posameznik je prav tako vir svojih prihodnjih dejanj, motivov in želja. Torej povezuje pretekla in bodoča dejanja. Ta vidik je najzanesljivejši kazalec posameznikove identitete tako pri interakciji v virtualnem kot v resničnem svetu, saj vključuje že potrjena nagnjena in je obenem pogosto predvidljiv, saj se ljudje bolj ali manj obnašajo po vzorcih iz preteklosti (Lahlou 2008, 310).

3.1 Rekonstrukcija identitete pri posredovanem komuniciranju preko spleta

Boydova in Ellisonova (2007, 9) ugotavljata, da kljub temu, da mnogi družbeni mediji na spletu spodbujajo uporabnike, da za potrebe interakcije ustvarijo čim bolj resnične reprezentacije samih sebe, uporabniki tega večkrat ne storijo. Identitete posameznikov, ki jih uporabniki srečujejo na družbenih medijih na spletu, so lahko tako resnične ali pa povsem izmišljene – posameznike v kibernetičnem prostoru namreč spoznavamo samo preko besedila, podob in ikon na monitorju, zaradi česar je prepoznavanje resnice precej oteženo (Gauntlett in Horsley 2004, 17). Interaktivnost in možnost zamenjavanja oz. ustvarjanja mnogih različnih identitet daje uporabnikom spletnih družbenih medijev možnost eksperimentiranja in prevzemanja drugega spola oz. povsem druge identitete (Gauntlett in Horsley 2004, 31). Wallace (v Giles 2003, 271) zato imenuje internet tudi »identitetni laboratorij«, saj ima kibernetni prostor velik potencial za rekonstrukcijo identitet. Giles (2003, 271) ugotavlja, da kibernetni prostor ponuja možnost za oblikovanje povsem novega koncepta o samem sebi, brez geografskih, telesnih, zgodovinskih in

podobnih omejitev. Posameznik lahko tako ustvari vrsto različnih oseb, preko katerih komunicira v virtualnem svetu. Družbeni mediji na spletu, kjer se morajo posamezniki pred uporabo registririati in nato oblikovati svoj profil znotraj družbenega omrežja, so s tem odličen prostor za oblikovanje virtualne identitete, tudi s pomočjo prevzemanja identitete nekoga drugega.

Pri komunikaciji iz oči v oči si sporočevalca ali sporočevalci še preden spregovorijo s svojo neverbalno govorico izdajo vsaj nekaj informacij o samih sebi. Kot ugotavlja Uletova (2005, 411) imamo v »neposrednih medosebnih stikih tipično nekatere nedvoumne zagotovljene znake za osebne identitete svojih partnerjev«. Česa takega pa pri posredovanem komuniciranju, kamor lahko uvrstimo tudi komuniciranje preko družbenih medijev na spletu, največkrat ni. Rheingold (2000, 151) ugotavlja, da se lahko uporabniki spleta in spletnih družbenih medijev pretvarjajo, da so nekdo drug, oziroma se lahko istočasno pretvarjajo, da so več različnih oseb. S tem je posameznikova identiteta na preizkušnji (Donath 1998, 51), saj nikoli ni povsem jasno, ali je posameznik res oseba, za katero se izdaja ali ni. Impersonacija, kot prevzemanje druge oz. lažne identitete imenuje Donathova (1998, 51), je na spletu in spletnih družbenih medijih precej preprosta, saj tam ni prav veliko indikatorjev, ki bi lahko izdali posameznikovo pravo identiteto. Identiteto sogovornika nam lahko razkrivajo samo socialne strukture in simboli, ki jih uporabljajo naši sogovorniki (Ule 2005, 411). S komuniciranjem preko spleta se posameznik izogne tudi drugim neverbalnim namigom, ki lahko izdajajo veliko o njegovi pravi identiteti. Kot ugotavlja Giles (2003, 270), tudi v primeru, ko posameznik govori z nekom in je ob tem neviden, način govorjenja izda kar nekaj informacij o govorcu. Govorčev naglas izdaja njegovo nacionalno pripadnost, družbeni položaj in kulturno ozadje; način artikulacije izdaja govorčevo kompetentnost in samozavest; takojšnji odgovori na vprašanja pa lahko izdajajo tudi nekatere govorčeve karakterne lastnosti. Internet uporabnikom omogoča, da se izognejo tem neverbalnim namigom, ki lahko onemogočijo ali stigmatizirajo bodočo komunikacijo. Posameznik lahko preko interneta ustvari tako identiteto, da izraža samozavest in kompetentnost, pri tem pa ga ne ovirajo sramežljivost, neartikuliranost ali predsodki, ki so del komunikacije iz oči v oči (Giles 2003, 270).

Pri komuniciranju na spletnih družbenih medijih tako na nek način udeleženci v komunikaciji tavajo v temi, ko pride do vprašanja, s kom pravzaprav komunicirajo. Internet je za uporabnike prostor, kjer se lahko »igrajo z vidki svoje identitete ter osebnosti« (Ule 2005, 407). To naj bi

po mnenju Uletove (2005, 407) posameznike vzpodbujalo k zavesti, da so identitete pravzaprav konstrukcije in niso naravna danost, torej so tudi predmet lastnega udejstvovanja.

Posameznikova identiteta se torej s časom spreminja in nadgrajuje. Komuniciranje v virtualnem svetu, kamor spada tudi komuniciranje preko spletnih družbenih medijev, pa poleg tega posameznikom omogoča tudi eksperimentiranje z njihovo identiteto. Pri registraciji na spletne družbene medije, oblikovanju profilov, prezentiranju samih sebe drugim uporabnikom in interakciji z njimi, posameznik lahko dodaja ali odstrani različne vidike svoje identitete in si ustvari identiteto, ki mu najbolj odgovarja. V virtualnem računalniškem svetu so posamezniki tako gospodarji oz. gospodarice svoje identitete – tam menjavajo in na novo opredeljujejo svoje identitete (Praprotnik 2003, 59-61). Kot ugotavlja Praprotnik (2003, 61), menjavanje in novo opredeljevanje identitete poteka v okolju, kjer prevladuje »postmodernistična etika vrednosti raznovrstnih identitet, ki poudarja igro ter uporabnike in uporabnice spodbuja k izražanju zamolčanih vidikov svoje osebnosti«. Internet uporabnikom predstavlja prostor, kjer lahko kreirajo svoje lastne identitete, predstavljajo svoje ideje in vzpostavljajo novo realnost (Praprotnik 2003, 66).

3.2 Razkrivanje identitete pri posredovanem komuniciranju preko spleta

Virtualna identiteta, ki si jo posameznik ustvari, je, kot ugotavlja Praprotnik (2003, 74), zanj vedno uspešna. Posameznik se preko svoje virtualne identitete namreč brez večjih težav predstavlja tako, kot mu najbolj ustreza in zgolj s tistimi elementi svoje identitete, ki mu odgovarjajo. Težava virtualnih identitet tako ne leži na strani posameznika, ki jo ustvari, temveč se težava pojavi na strani naslovnika. Tisti, ki sodelujejo v interakciji s posameznikom, ki ustvari virtualno identiteto, morajo tej virtualni identiteti namreč verjeti na besedo. Čeprav je konstrukcija identitete v virtualnem svetu za posameznika vedno uspešno izvedena, to ne predstavlja nikakršnega zagotovila, da bodo sodelujoči v interakciji tej virtualni identiteti tudi verjeli in jo vzeli resno (Praprotnik 2003, 74).

Pri komuniciranju iz oči v oči ima udeleženec v interakciji precej oprijemljivo predstavo o identiteti drugih sodelujočih v interakciji. Fizično telo je precej jasen in priročen znak o posameznikovi identiteti; norma je namreč eno telo, ena identiteta (Donath 1998, 1). Kot Donathova (1998, 1) nadalje ugotavlja, je človekov jaz oz. njegova identiteta sicer lahko zelo zapletena in se skozi čas ter glede na različne življenjske okoliščine spreminja, vendar telo kljub

temu predstavlja neki stabilen temelj. Vendar pa ta telesni temelj posameznikove identitete obstaja samo v realnem svetu. V virtualnem svetu ta fizični vidik manjka, saj virtualnost sestavljajo informacije in ne materija. Virtualni svet posameznika osvobaja njegovega telesa, kar vodi do tega, da ima lahko posameznik toliko virtualnih person, kot si jih želi ustvariti. Vendar pa ta dva svetova nista povsem nepovezana – vse virtualne persone namreč vodijo nazaj do posameznikovega telesa, ki sedi za računalnikom (Donath 1998, 1).

Namigi o identiteti posameznikov pri interakciji v virtualnem svetu so torej precej bolj redki in težje opazni kot pri interakciji v realnem svetu. Kot ugotavlja Praprotnik (2003, 70), lahko uporabniki zaznajo samo socialno identiteto. Že sama možnost uporabe interneta je namreč neke vrste selekcija, s čimer se posredno razkrije majhen delček posameznikove identitete. Dostop do različnih orodij, tudi do spletnih družbenih medijev, je namreč omejen zgolj na tiste, ki imajo računalnik in dostop do interneta. Poleg tega mora imeti uporabnik vsaj osnovno znanje o uporabi računalnika in interneta, da lahko uporablja ta orodja. Čeprav to razkriva neka splošna dejstva o posameznikovi identiteti, so bolj podrobni identifikacijski kazalci v interakciji na spletu težko opredeljivi[2] (Praprotnik 2003, 70-71).

Vendar pa je danes situacija pri spletnih družbenih medijih precej drugačna, kot je bila nekaj let nazaj na spletnih mestih, ki so bila predmet Praprotnikove analize. Kazalci identitete o uporabnikih družbenih medijev na spletu so pri tistih medijih, ki poleg tekstovnega komuniciranja omogočajo tudi objavo fotografij, video posnetkov in povezav, precej bolj neposredni. Ti spletni družbeni mediji namreč uporabnikom omogočajo, da objavijo tudi informacije, ki niso omejene le na tekstovno raven, ampak vsebujejo tudi vizualne elemente. Tako lahko fotografije in posnetki, ki jih posameznik objavi na spletnem družbenem mediju, drugim uporabnikom razkrijejo tudi fizični vidik posameznikove identitete.

[2] Nekaj o posameznikovi identiteti razkrivajo njegovo besedišče, sintaksa in stil pisanja (Praprotnik 2003, 70-71). Dodaten pokazatelj identitete je lahko elektronski naslov, ki ga posameznik uporablja. Če v naslovu posameznik uporablja svoje pravo ime, s tem drugim uporabnikom izda svoje ime in priimek. Preko elektronskega naslova lahko posameznik razkrije tudi druge vidike svoje identitete. V primeru, da uporablja elektronski naslov akademske institucije, katere član je, ali pa elektronski naslov podjetja, v katerem je zaposlen, s tem drugim razkrije informacije iz svojega profesionalnega življenja. Medtem ko je bilo v prvih letih razvoja interneta težje priti do naslova elektronske pošte in so bili vsi računi institucionalni (Donath 1998, 36), lahko uporabniki danes brez težav pridejo do komercialnega naslova elektronske pošte, ki za registracijo ne zahtevajo pravega imena uporabnika. S tem tudi elektronski naslov ne izdaja nobene informacije o identiteti lastnika.

4 UPORABA DRUŽBENIH MEDIJEV NA SPLETU IN NEVARNOST KRAJE IDENTITETE

V človekovi naravi je, da se želi zaščititi pred nevarnostmi. Večina ljudi zato želi del svojih navad in značilnosti skriti pred drugimi, da bi se izognili nadzoru, nezaželenim dejavnostim, kritiziranju, zasledovanju, izrabljanju itd. Vendar pa želijo po drugi strani ti isti ljudje vzpostaviti odnos z drugimi posamezniki ali skupinami. Da bi to lahko dosegli, morajo druge opozoriti nase. Torej ne smejo biti popolnoma nevidni. To pomeni, da morajo drugim posredovati tudi določeno mero informacij o samih sebi. Družbeno življenje je potemtakem nenehno krmiljenje med izogibanjem tveganju in iskanju zadovoljitve (Lahlou 2008, 311-312). Z razvojem interneta in različnih možnosti komuniciranja, ki jih ponuja, so se pojavile tudi nove varnostne dileme in grožnje. Eden vidik teh tveganj je nevarnost kraje identitete.

Kot že sam termin »kraja identitete« nakazuje, ne gre zgolj za odtujitev materialne lastnine, temveč so na udaru intimne informacije, ki posameznika opredeljujejo kot svojevrstno entiteto in ga ločujejo od drugih (Caeton 2007, 12). Krajo identitete lahko razumemo kot skupek dejanj, katerih cilj je kraja osebnih informacij določenega posameznika. Do kraje največkrat pride zaradi morebitnega profita, ki ga lahko kraja identitete prinese, kar je bolj poznano kot *finančna kraja identitete*. Primer take kraje identitete je vdiranje v računalniške sisteme in kraja podatkov, kraja PIN številke preko bankomatov itd. Druga oblika kraje identitete je t.i. *kriminalna kraja identitete*, pri kateri osumljenec kaznivega dejanja ob identifikaciji navede lažne podatke in se pretvarja, da je nekdo drug. Tretja oblika pa je t.i. *prevzem identitete*, kjer nekdo prevzame identiteto nekoga drugega, da na novo začne življenje z novo identiteto, ali pa zato, da ustvari virtualno persono z identiteto nekoga drugega (Lavi, Wall, Cole in Pontelli v Monahan 2009, 156-157).

Kot ugotavlja Monahan (2009, 167) so ljudje prepričani, da je potrebno prevzeti in aktivno uporabljati zadnje tehnologije za ohranjanje stika s prijatelji in sorodniki, za uspešnost na poslovnem področju, ohranjanje konkurenčnosti in prednosti pred drugimi. Veliko ljudi tako verjame, da so tehnološki sistemi sinonim za napredek (Winner v Monahan 2009, 167). Vendar so si po mnenju Monahana (2009, 167) družbe pri tem pozabile zastaviti vprašanje o tem, kako ti informacijski sistemi povečujejo ranljivost njihovih uporabnikov, kar vključuje tudi nevarnost kraje identitete.

Med tehnološke sisteme zadnjih nekaj let, pri katerih se pojavlja tudi vprašanje ranljivosti in varnosti uporabnikov, spadajo tudi družbeni mediji na spletu. Po mnenju Seppä (2008, 3) težava spletnih družbenih medijev ni le v vprašanju zasebnosti in varovanju osebnih podatkov, temveč tudi v ranljivostih, ki so jim lahko podvrženi. Informacije, posredovane v interesu interakcije, so lahko zlorabljene na različne načine – od posredovanja podatkov razpošiljevalcem nezaželene pošte, nadlegovanja uporabnikov, spletnega in fizičnega zasledovanja, diskriminacije uporabnikov, izsiljevanja in celo do kraje identitete (Seppä 2008, 3; Gross in Acquisti 2005, 3). Kraja identitete na spletnih družbenih medijih se lahko pojavi v obliki prevzema identitete v dobesednem pomenu besede. Torej, da se nekdo registrira na spletni družbeni medij z lažno identiteto oz. identiteto nekoga drugega. Uporabniki lahko zaradi objave različnih osebnih informacij v okviru svojega profila na spletnih družbenih medijih postanejo žrtve tako prevzema identitete izven virtualnega sveta kot tudi t.i. finančne kraje identitete.

4.1 Primeri potencialnih nevarnosti za krajo identitete

Enostaven registracijski postopek je prva izmed možnih nevarnosti za krajo identitete. Podatki, ki so potrebni za registracijo, namreč puščajo veliko možnosti za posameznikovo eksperimentiranje, morebitno zlorabo in prevzem identitete. Kako preprosto je prevzeti identiteto za potrebe registracije in oblikovanja profila na spletnih družbenih medijih, kažejo primeri mnogih javno izpostavljenih posameznikov[3].

Druga izmed potencialnih nevarnosti za krajo identitete je širjenje socialnega omrežja z dodajanjem novih »prijateljev«. Primer tega, kako nevarno je lahko sprejemanje neznancev med spletne »prijatelje«, je eksperiment, ki so ga izvedli v eni imed oddaj na britanski medijski mreži BBC (Finance 2007). Avtorji oddaje o pravicah potrošnikov so na spletnem družbenem mediju Facebook ustvarili lažen uporabniški profil mladega dekleta. Preko tega profila so potem povabili 100 naključnih uporabnikov, da bi postali njeni spletni »prijatelji«. 35 uporabnikov se je povabilu odzvalo, kljub temu da o tej izmišljeni uporabnici niso vedeli nič. S tem so ustvarjalci dobili dostop do vseh osebnih podatkov, ki so jih ti uporabniki objavili na svojem profilu. Na podlagi podatkov, ki so jih pridobili na profilu enega izmed teh uporabnikov, so ustvarjalci

[3] Na spletnem družbenem mediju Facebook imajo mnogi slovenski politiki več kot en profil. Tudi mnogi znani iz sveta zabave se na tem družbenem mediju pogosto srečujejo s prevzemom identitete (npr. Angelina Jolie). Do ustvarjanja lažnih profilov oz. do prevzemanja identitete prihaja tudi na spletnem družbenem mediju Twitter, kjer so med drugimi postali žrtve tudi angleška igralca Emma Watson in Evan McGregor ter celo Dalai Lama.

oddaje na spletu pridobili še nekaj javno dostopnih informacij o njem ter na njegovo ime odprli elektronski bančni račun in zaprosili za kreditno kartico. Tako je ta uporabnik zgolj s tem, da je sprejel neznanko za svojo spletno »prijateljico«, postal žrtev finančne kraje identitete.

Tretjo potencialno nevarnost pa predstavlja dodajanje in uporaba aplikacij. Kakšno nevarnost lahko predstavljajo aplikacije, kaže eksperiment, ki ga je izvedela britanska medijska mreža BBC (Kelly 2008). Avtorji eksperimenta so najprej ustvarili lažen profil na Facebooku in nato ustvarili posebno aplikacijo za ta spletni družbeni medij. Aplikacija se je imenovala *Miner* in je bila narejena tako, da se je lahko zamaskirala kot igra, kviz ali šala dneva, v resnici pa je bila namenjena nelegalnemu in tajnemu pridobivanju podatkov s profilov drugih uporabnikov. Kljub videzu nedolžne aplikacije je le-ta zbirala osebne podatke, tako od uporabnika profila, ki je aplikacijo dodal, kot tudi od njegovih »prijateljev«. Zbrane podatke je potem aplikacija preko elektronske pošte posredovala avtorjem aplikacije. Ko so avtorji aplikacijo dodali na lažni profil, ki so ga ustvarili, so ugotovili, da lahko z aplikacijo pridobijo različne informacije. Sicer s profila niso mogli pridobiti vseh podrobnosti, vendar so pridobili informacije o uporabnikovem imenu, domačem mestu, šoli, interesih in njegove fotografije.

4.2 Zasebnost, razkrivanje osebnih podatkov in kraja identitete

Boydova (2008, 18) zasebnost definira kot občutek nadzora nad informacijami, kontekstom, v katerem poteka izmenjava le-teh, in nad občinstvom, ki ima lahko dostop do teh informacij. Dejstvo, da nihče ne ve določene informacije, te informacije ne naredi zasebne. Informacija je zasebna zato, ker je to, kdo informacijo ve, omejeno in nadzorovano (Boyd 2008, 18). Uporabniki spletnih družbenih medijev lahko do določene mere sicer regulirajo koliko in kateri podatki bodo dostopni tudi drugim in ne zgolj njihovim »prijateljem«. Vendar pa je težava v tem, da mnogi uporabniki, ki svoje osebne podatke naredijo tako javne in lahko dostopne na svojih profilih na spletnih družbenih medijih, ne pomislijo na varovanje zasebnosti in podatkov ter se ne zavedajo nevarnosti kraje identitete (Seppä 2008, 3).

Kot ugotavlja Seppä (2008, 3), je leta 2008 samo 25 odstotkov uporabnikov Facebooka dejansko uporabljajo varnostne nastavitve o zasebnosti profila in spremenilo privzete nastavitve, ki največkrat omogočajo tudi neznancem dostop do profila in vsebin objavljenih na njem. Podatki iz leta 2005 (Gross in Acquisti 2005, 9) pa kažejo, da je bilo kar 30 odstotkov od

250.000 uporabnikov Facebooka, ki so jim poslali vabilo za »prijateljstvo«, pripravljenih sprejeti in razkriti vse informacije s profila popolnim neznancem in njihovim spletnim »prijateljem«.

Veliko uporabnikov tako na svojem profilu povsem javno objavi veliko podatkov o sebi (ime, rojstni datum, domači naslov, elektronski naslov, telefonska številka itd.) in dodaja različne aplikacije, ki so lahko potem na različne načine zlorabljene. Tako kljub nevarnostim zlorabe osebnih podatkov, ki jih uporabnik objavi na spletnem družbenem mediju, uporabniki prostovoljno in zavestno posredujejo te podatke (Gross in Acquisti 2005, 3).

Razlogi za tako ravnanje so po mnenju Grossa in Acquistija (2005, 3-4) različni. Do takega razkrivanja podatkov na spletnih družbenih medijih lahko pride zaradi tega, ker a) uporabnik predvideva, da bodo koristi, ki jih lahko pridobi s selektivnim razkrivanjem podatkov neznancem, večje kot pa potencialna nevarnost vdora v njegovo zasebnost; b) pritiska vrstnikov ali sledenja in posnemanja vedenja drugih; c) pretirano sproščenega odnosa ali nezainteresiranosti za osebno varnost in varovanje podatkov; d) nepoznavanje in neinformiranost o nevarnostih razkrivanja osebnih podatkov na spletnih družbenih medijih; e) zaupanja v spletne družbene medije in njihove uporabnike, ali pa f) nezadostne ocene nevarnosti, ki je lahko rezultat razkrivanja podatkov na spletu.

5 PREGLED VARNOSTNIH NASTAVITEV NA SPLETNIH DRUŽBENIH MEDIJIH

Kot poudarja Lahlou (2008, 318) vdor v zasebnost in zloraba osebnih podatkov nista odvisna od tega, kaj nekdo stori ali razkrije, temveč od tega, komu te podatke razkrije. Vdor v zasebnost, prav tako pa tudi kraja identitete, torej vedno vključujeta nekoga »Drugega«. Uporabnikom spletnih družbenih medijev nadzor nad tem, komu bodo razkrili svoje osebne podatke, omogočajo varnostne nastavitve. Z njimi lahko uporabnik regulira dostop do informacij, ki jih objavi na svojem profilu. Kakšne možnosti ima uporabnik pri oblikovanju svojega profila in s kakšnimi varnostnimi nastavitvami ga lahko zaščiti, je odvisno od posameznega družbenega medija na spletu. Ravno zato bom v nadaljevanju analizirala štiri različne spletne družbene medije. Poskušala bom ugotoviti, kakšne možnosti glede varovanja podatkov in s tem preprečevanja morebitne kraje identitete uporabnikom omogočajo varnostne nastavitve ter kakšna načela o varnosti in zasebnosti veljajo na teh spletnih družbenih medijih.

Za pregled varnostnih nastavitev in varnostnih načel sem izbrala štiri spletne družbene medije – Facebook, Twitter, Flickr in YouTube. Z analizo primarnih virov bom poskušala predstaviti, kakšne smernice glede varnosti uveljavljajo analizirani spletni družbeni mediji. Med viri, ki jih bom uporabila, so načela o varnosti in nasveti o varnosti, ki jih imajo spletni družbeni mediji objavljene na svojih spletnih straneh. Poleg tega bom uporabila tudi metodo analize teksta, s katero bom poskušala ugotoviti, kakšne varnostne nastavitve uporabnikom omogočajo posamezni spletni družbeni mediji. Pregled bo temeljil na varnostnih nastavitvah in varnostnih načelih, ki so bila v veljavi v petek, 2. oktobra 2009.

5.1 Facebook

Posamezniki, ki si v okviru spletnega družbenega medija Facebook ustvarijo svoj profil, lahko nadzor nad svojimi zasebnimi informacijami izvajajo na treh ravneh. Prva raven predstavlja nadzor nad tem, komu omogočijo dostop do objavljenih vsebin. Druga raven zajema nadzor nad tem, kaj pošiljajo oz. objavljajo. Tretja raven pa zajema nadzor nad aplikacijami, ki jih uporabljajo.

Facebookovi uporabniki imajo možnost nadzora nad zasebnimi informacijami z omejevanjem dostopa do njihovega profila in podatkov na njem. Dostop do tega lahko omejijo že z nadzorom nad tem, kdo jih lahko v okviru iskalnika »prijateljev«, ki ga ponuja Facebook, sploh najde. Posameznik lahko določi, da njegov profil najdejo bodisi a) vsi uporabniki, b) njegova omrežja in »prijatelji«, ali c) zgolj »prijatelji«. Poleg tega lahko uporabniki regulirajo tudi, kaj lahko tisti, ki jih pri iskanju najdejo, sploh vidijo. Uporabnik se sam odloči, katera izmed naslednjih informacij bo poleg njegovega imena vidna: prikazna slika, seznam »prijateljev«, povezava, kjer ga drugi lahko dodajo kot »prijatelja«, povezava, kjer mu drugi lahko pošljejo sporočilo, in strani, ki jih ima rad. Dodaten varnostni mehanizem za to, kdo lahko dostopa do uporabnikovega profila, je tudi to, da mu mora vsak najprej poslati prošnjo za »prijateljstvo«, ki jo mora uporabnik potrditi. Le s potrditvijo prošnje lahko torej dva uporabnika postaneta »prijatelja« in dostopata do informacij drug drugega.

Uporabniki imajo več različnih možnosti za regulacijo dostopa do samega profila in informacij na njem. Njihov profil je lahko povsem javno dostopen, s čimer imajo varnostne nastavitve o zasebnosti nastavljene na privzeto. To pomeni, da so njihov profil, osnovne informacije, osebni podatki, status in povezave, fotografije in video posnetki, na katerih so

označeni, seznam »prijateljev«, objave na zidu, podatki o izobrazbi in zaposlitvi vidni ter hkrati tudi dostopni vsakomur. V primeru, da uporabnik ne želi, da do njegovega profila in informacij dostopa kdor koli, lahko za vsako izmed zgoraj naštetih kategorij izbira, komu bo določena kategorija vidna. Vsak uporabnik ima možnost, da kategorije določi sam in s tem še bolj specifično opredeli, komu bodo njegovi podatki dostopni. Dostop lahko omeji zgolj na določene »prijatelje«, pri čemer uporabnik naredi seznam, komu izmed »prijateljev« dovoli dostop. Na podoben način pa lahko tudi sestavi seznam zgolj določenih »prijateljev«, ki jim ne dovoli dostopa do vsebin. Omejitve so lahko tudi manj specifične in zajemajo na primer vse »prijatelje«, omrežja, ki jim pripada, ali »prijatelje« in njihove »prijatelje«. Pri določenih kategorijah (fotografije in video posnetki, na katerih je posameznik označen, objave na zidu, informacije o izobrazbi in zaposlitvi) pa lahko uporabnik celo onemogoči dostop vsem drugim in ima dostop do teh kategorij zgolj on. Poleg nastavitev dostopa do informacij Facebook uporabnikom tudi omogoča, da si ogledajo profil z vidika svojih »prijateljev« in s tem nazorno oz. praktično vidijo, kako varnostne nastavitve delujejo in kaj onemogočajo. Enak način nadzora lahko uporabnik izvaja tudi nad fotografijami oz. albumi, ki jih objavi na svojem profilu. Za vsak posamezni album lahko uporabnik omeji dostop na specifično določene skupine »prijateljev« in s tem regulira, kdo lahko dostopa do njih in jih pregleduje. Albume lahko tudi popolnoma zaklene in do njih dostopa samo on.

Regulacija in nadzor nad aplikacijami, ki obsegajo vse od koledarja z rojstnimi dnevi »prijateljev« do spletnih iger, poteka na podoben način kot regulacija samega profila in fotografij. Aplikacije lahko uporabnik naredi vidne in dostopne zgolj njemu, lahko pa je dostop do njih širši. Varnostne nastavitve uporabniku tudi omogočajo, da nezaželene aplikacije odstrani in med zaželenimi izbira, katere želi kot zavihek na prvi strani profila. V primeru, da uporabnik sprejme aplikacijo, le-ta dobi dostop do njegovega profila in informacij na njem. Prav tako dobi dostop do posameznikovega profila tista aplikacija, ki jo na svoj profil doda kateri izmed njegovih »prijateljev«. Vendar pa mora tudi v tem primeru aplikacija upoštevati posameznikove varnostne nastavitve, kar pomeni, da ima lahko zelo omejen dostop. V primeru, da ima posameznik vključene vse varnostne nastavitve in maksimalno zavarovan svoj profil, ima aplikacija dostop samo do njegovega imena, omrežij in seznama »prijateljev«. Pred nevarnostjo zlorabe osebnih podatkov zaradi aplikacij pa se lahko uporabniki Facebooka zavarujejo tudi tako, da aplikacije oz. programe, ki jim ne zaupajo, preprosto blokirajo. S tem blokirani programi

ne morejo dostopati do nobenih informacij o uporabniku, prav tako ga ne morejo niti kontaktirati.

V splošnih načelih Facebooka (Facebook 2009) je zapisano, da sta dve temeljni načeli, na katerih temelji Facebook, to, da bi moral imeti posameznik nadzor nad svojimi osebnimi informacijami in dostop do informacij, ki jih drugi želijo deliti. Ti dve načeli naj bi pomenili, da posamezniki sami izbirajo, katere informacije bodo objavili na profilu, preko varnostnih nastavitev sami določajo, s kom bodo te podatke delili in imajo možnost enostavnega dostopa do objavljenih informacij. Poudarjajo, da želijo svojim uporabnikom ponuditi varnostna orodja, ki bi jim omogočala nadzor nad tem, kako in komu bodo delili svoje informacije.

V Facebookovih nasvetih o varnosti (Facebook 2009) je izpostavljeno, da uporaba lažnih imen predstavlja kršitev Facebookovih pogojev uporabe. Vendar pa to ni zagotovilo, da do tega ne prihaja. V varnostnih nasvetih zato opozarjajo, da morajo biti uporabniki pri pošiljanju prošenj za »prijateljstvo« neznancem in sprejemanju le-teh za »prijatelje« zelo previdni. Poleg tega svojim uporabnikom predlagajo, da nikoli ne razkrijejo svojega gesla, prilagodijo varnostne nastavitve in jih redno pregledujejo, so zelo previdni pri objavljanju osebnih informacij, še posebej takih, ki omogočajo enostavno identifikacijo, da prijavijo morebitne kršitve pogojev uporabe ter blokirajo in prijavijo vse, ki jim pošiljajo neprimerne vsebine. Kljub vsem tem nasvetom in opozorilom, ki se nanašajo tudi na impersonacijo oz. prevezemanje identitete drugih, ki jih Facebook ponuja svojim uporabnikom, pa enostavna registracija omogoča ravno to. Obrazložitev zahteve po navedbi rojstnega datuma je, da naj bi ravno ta podatek vzpodbujal avtentičnost uporabnikov in zagotavljal, da se registrirajo samo dovolj stari posamezniki. Težava pri tem je le, da ima posameznik povsem prosto izbiro, kateri datum in leto si izbere kot svoj rojstni datum. Torej ta podatek dejansko ne predstavlja zanesljivega kazalca avtentičnosti registriranih uporabnikov.

Varnostne nastavitve, ki jih ponuja Facebook, uporabniku torej nudijo precej dobre in učinkovite načine, kako se zavarovati pred krajo idenititete zaradi zlorabe osebnih podatkov, objavljenih na profilu. Enostaven postopek registracije po drugi strani omogoča enostavno impersonacijo oz. prevzemanje identitete.

5.2 Twitter

Tako kot uporabniki Facebooka, imajo tudi uporabniki Twitterja možnost nadzora nad svojimi zasebnimi podatki na različnih ravneh. Nadzorujejo lahko dostop do svojega profila, poleg tega pa lahko izvajajo nadzor nad tem, kaj objavljajo.

Uporabniki Twitterja lahko pustijo svoj račun javen, imajo pa tudi možnost, da ga zavarujejo. V nastavitvah lahko izberejo možnost »zaščiti moje objave«, kar pomeni, da lahko uporabniku in njegovim objavam sledijo samo izbrani posamezniki. V takem primeru se uporabnikove objave tudi ne pojavljajo na javnem časovnem traku, kjer so objavljene vse objave uporabnikov z javnimi računi.

Zaradi preprostega postopka registracije se uporabniki Twitterja pogosto soočajo z impersonacijo oz. s prevzemanjem identitete. Twitter se zato posebej podrobno ukvarja s problemom prevzemanja identitete in je oblikoval posebna načela o impersonaciji (Twitter 2009). V njih impersonacijo označijo kot dejanje, pri katerem se posameznik zaradi zabave ali želje po zavajanju pretvarja, da je neka druga oseba ali podjetje. V primeru, da impersonacija ni narejena v namene parodije, le-ta pomeni kršenje pravil uporabe Twitterja. Parodija naj bi bila po njihovem mnenju določena s preprostim vprašanjem »Ali bi se razumna oseba zavedala, da gre za šalo?«. V primeru, da je odgovor na to vprašanje pritrdilen, lahko impersonacijo razumemo kot parodijo in ne pomeni kršenja pravil. S takim poenostavljenim definiranjem parodije določanje in sankcioniranje impersonatorjev oz. tistih, ki se poslužujejo ene izmed oblik kraje identitete, vsebujeta veliko mero subjektivnosti in nenatančnosti. Vsi tisti računi, ki naj bi imeli z impersonacijo jasen namen zavajati, so trajno izbrisani; tisti, ki naj bi spadali v kategorijo parodije, pa ostanejo aktivni brez kakršnih koli sankcij. Vendar pa morajo tudi slednji pri vseh objavah jasno nakazati, da gre za šalo in lažni profil, drugače se tudi taki računi trajno odstranijo. Vsak, ki postane žrtev impersonacije ali je pravno pooblaščen v imenu nekoga, ki je žrtev, ima možnost kontaktirati Twitter, kjer poskrbijo, da je lažen račun odstranjen.

V svojih varnostnih načelih (Twitter 2009) Twitter poudarja, da je poleg tistih osebnih podatkov, ki so potrebni za registracijo, posredovanje oz. objavljanje dodatnih osebnih podatkov stvar posameznikove izbire in je povsem prostovoljno. Vendar pa naj bi tako ravananje pripomoglo k boljši identifikaciji samega sebe ter pri iskanju novih prijateljev in možnosti v

okviru Twitterja. Varnostna načela posebej obravnavajo tudi varnost uporabnikov, kjer je izpostavljeno, da naj bi Twitter uporabljal tako administrativne, fizične, kot tudi elektronske ukrepe, namenjene varovanju uporabnikovih podatkov in preprečevanju nepooblaščenega dostopa do njih. Tudi v pogojih uporabe (Twitter 2009) je izpostavljeno, da je za objavljeno vsebino in morebitne posledice odgovoren vsak uporabnik. Kar uporabnik objavi na Twitterju, je namreč lahko nemudoma vidno skorajda po celem svetu. Nasvet, ki ga zato nudijo v pogojih uporabe je, da se uporabniki zavedajo, da so to, kar pošiljajo preko Twitterja.

Podobno kot pri Facebooku tudi Twitter preko varnostnih nastavitev svojim uporabnikom ponuja več različnih mehanizmov, s katerimi se lahko uspešno zavarujejo pred krajo identitete. Enostavna registracija pa tudi v primeru Twitterja predstavlja večjo težavo, saj omogoča enostavno prevzemanje identitete.

5.3 Flickr

Varnostne nastavitve na spletnem družbenem mediju Flickr uporabnikom omogočajo nadzor tako nad tem, kdo vidi podatke, objavljene na njihovem profilu, kot tudi to, kdo ima dostop do objavljenih fotografij. V primeru, da posameznik dopolni svoj profil z različnimi osebnimi informacijami, ima možnost nadzora nad tem, komu bodo ti podatki vidni. V okviru nastavitev zasebnosti profila lahko določi, kdo bo videl njegov elektronski naslov, ime za kratka sporočila, pravo ime in kraj. Dostop do teh informacij lahko pusti bodisi a) vsem uporabnikom spleta, b) vsem uporabnikom Flickerja, c) vsem svojim kontaktom na Flickrju, ali pa d) samo prijateljem in/ali družini. Elektronski naslov lahko naredi tudi povsem nedostopen, torej ga zaklene tako, da ga ne more videti nihče.

V okviru nastavitev računa lahko uporabnik nastavi varnostne nastavitve tudi za fotografije, ki jih objavi na svojem profilu. Nastavitve mu omogočajo, da regulira, kdo lahko fotografije pregleduje, prenaša, deli z drugimi, tiska, komentira. Uporabnik lahko regulira tudi to, kdo lahko dodaja fotografije, na katerih je uporabnik, in kdo lahko objavlja zapiske o njegovih fotografijah. Dostop do teh funkcij lahko uporabnik omogoči bodisi a) komurkoli, četudi ni uporabnik Flickrja, b) uporabnikom Flickrja, c) svojim kontaktom na Flickerju, d) zgolj svojim prijateljem in/ali družini, ali pa e) dostop do teh funkcij onemogoči vsem ostalim in do njih dostopa samo on. Prav tako uporabnik določi, ali želi, da so njegove fotografije objavljene v galeriji. Regulira lahko tudi, ali želi, da so njegov profil in fotografije dostopni preko različnih iskalnikov. V

primeru, da uporabnik objavi fotografije z neprimerno vsebino, lahko take fotografije kategorizira kot neprimerne za otroke ali kot neprimerne za vse ostale uporabnike, s čimer nima dostopa do njih nihče razen uporabnika.

Flickr, za razliko od Facebooka in Twitterja, nima oblikovanih nobenih posebnih načel ali nasvetov o varnostni. Na spletni strani (Flickr 2009) sicer v kratkem odseku obravnava zasebnost svojih uporabnikov. Vendar pa so tam le na kratko naštete in povzete varnostne nastavitve, s katerimi lahko uporabniki zavarujejo svoj profil in objavljene fotografije.

Podobno kot pri prvih dveh spletnih družbenih medijih tudi pri Flickrju enostaven postopek registracije omogoča prevzemanje identitete, vendar pa lahko posameznik svoj profil in osebne informacije, ki jih objavi na njem, zavaruje z varnostnimi mehanizmi, ki mu jih ponujajo varnostne nastavitve. Glede na to, da je glavni namen Flickrja nalaganje in objava fotografij, so varnostne nastavitve z vidika kraje identitete še toliko bolj pomembne. Preko fotografij, ki jih objavi posameznik, se namreč lahko razkrivajo mnogi vidiki njegovega osebnega življenja, kar lahko še hitreje vodi k morebitni zlorabi podatkov in h kraji identitete.

5.4 YouTube

Varnostne nastavitve na YouTubu uporabnikom omogočajo nadzor na dveh ravneh. Uporabniki lahko regulirajo dostop do podatkov, objavljenih na profilu, poleg tega pa lahko regulirajo tudi video vsebine, ki jih objavijo, in dostop do njih.

Ko se uporabnik YouTuba registrira in oblikuje svoj račun, so nekatere njegove informacije javno dostopne oz. vidne drugim uporabnikom. Vendar pa ima vsak uporabnik možnost, da do določene mere regulira, kateri podatki o njem bodo povsem zasebni. Tisti uporabniki, ki svoj profil dopolnijo z zasebnimi podatki, imajo možnost, da naredijo vse izmed njih nevidne drugim. To pomeni, da lahko do njih dostopajo samo sami, kadar obiščejo svoj profil. V takem primeru je javno objavljeno samo posameznikovo uporabniško ime in podatek o tem, kdaj si je oblikoval svoj profil.

Poleg tega, da uporabniki sami odločajo, kakšne vsebine bodo objavili, jim YouTube ponuja tudi dve možnosti glede regulacije dostopa do objavljenih vsebin. Posnetke lahko pustijo javno dostopne, kar pomeni, da si jih preko YouTube spletne strani lahko ogleda kdor koli. Lahko pa

svoje posnetke zaščitijo in jih naredijo zasebne, kar pomeni, da si jih lahko ogledajo samo oni sami.

Kot pri YouTubu poudarjajo v svojem varnostnem centru (YouTube 2009), lahko na uporabnikovo zasebnost vpliva tako razkrivanje osebnih podatkov, kot tudi objavljanje video vsebin, ki imajo lahko kasneje negativen učinek na uporabnika. Podobna opozorila se pojavljajo tudi v načelih o zasebnosti YouTuba (YouTube 2009), kjer poudarjajo, da lahko vsak osebni podatek ali video vsebina, ki jo uporabniki objavijo na spletnem družbenem mediju, uporabijo in zbirajo tudi drugi ljudje.

Ravno objavljanje video vsebin, ki razkrivajo več vidikov iz zasebnega življenja uporabnika, lahko predstavlja precej večje tveganje za morebitno krajo identitete, kot pa objavljeni podatki na profilu posameznega uporabnika. Glede na to, da YouTube svojim uporabnikom ponuja zgoraj opisane varnostne nastavitve, uporabnikom pravzaprav predstavlja največjo nevarnost za zlorabo njihovih osebnih podatkov, ki lahko vodi tudi v krajo identitete, njihovo nepremišljeno ali neodgovorno objavljanje video vsebin.

Tabela 5.1 Pregled ugotovitev analize nastavitev pri spletnih družbenih medijih

ANALIZIRAN SPLETNI DRUŽBENI MEDIJ / KRITERIJ ANALIZE	FACEBOOK	TWITTER	FLICKR	YOUTUBE
registracijski postopek, ki zagotavlja avtentičnost uporabnika	×	×	×	×
možnost regulacije dostopa do profila	√	√	√	√
možnost reguliranega dodajanja »prijateljev«	√	√/× *	√	/
možnost reguliranja dostopa do objavljenih vsebin (fotografij, video posnetkov itd.)	√	√	√	√
možnost nadzora nad aplikacijami	√	/	/	/
oblikovana načela o varnosti	√	√	×	√
oblikovana načela o zasebnosti	√	√	×	√

Legenda: √ - omogoča, × - ne omogoča, / - ne podpira te funkcije
* odvisno od tega, ali ima uporabnik profil zaklenjen ali ne

6 ZAKLJUČEK

V letu 2009 je obisk Facebooka v primerjavi z letom 2008 v ZDA narasel za 200 % (RIS 2009b). Čas, ki so ga ameriški uporabniki porabili za pregledovanje vsebin na tem družbenem mediju v letu 2009, je v primerjavi z letom 2008 narasel kar za 700 % (RIS 2009a). Tudi v Sloveniji je priljubljenost spletnih družbenih medijev vse večja. V začetku leta 2009 je tako 22 % ženskih in 23 % moških uporabnikov interneta oblikovalo ter urejalo lasten profil na vsaj enem izmed spletnih družbenih medijev (STAT 2009).

Statistike torej kažejo, da so spletni družbeni mediji iz leta v leto bolj priljubljeni med uporabniki interneta. Istočasno s priljubljenostjo pa narašča tudi zaskrbljenost glede njihove

uporabe, varovanja osebnih podatkov in različnih nevarnosti, povezanih s tem. Mednje spada tudi kraja identitete, vendar pa, kot je pokazal pregled literature in varnostnih nastavitev štirih spletnih družbenih medijev, nevarnost zanjo le ni tako zelo ekstremna. Res je, da spletni družbeni mediji uporabnikom omogočajo, da na svojih profilih objavijo poljubno količino osebnih podatkov, vendar jim hkrati ponujajo tudi varnostne nastavite, s katerimi jih lahko zaščitijo. Seveda se ob tem pojavi tudi vprašanje, kaj s temi podatki delajo sami spletni družbeni mediji oz. posamezniki in korporacije, ki stojijo za njimi. Vendar pa cilj in fokus te naloge ni bila korporativna politika rokovanja s podatki, objavljenimi v okviru spletnih družbenih medijev, in pravice, ki si jih lastniki le-teh pridržujejo. Cilj naloge je bil ugotoviti, ali zaradi narave spletnih družbenih medijev in možnosti, ki jih omogočajo uporabnikom, le-ti za uporabnike res predstavljajo veliko grožnjo za krajo identitete.

Preko pregleda literature in analize varnostnih nastavitev sem ugotovila, da se uporabniki lahko soočijo s krajo identitete v dveh vidikih. Impersonacija oz. prevzemanje identitete se najpogosteje pojavlja že pri sami registraciji na spletni družbeni medij, saj jim je skupno to, da imajo zelo preprost postopek registracije. Enostavni podatki in malo varnostnih mehanizmov puščajo posameznikom možnost, da pri registraciji enostavno ustvarijo neresnične identitete oz. prevzamejo identiteto nekoga drugega. Najpogosteje se to dogaja osebam, ki so javno izpostavljene oz. poznane. Čeprav naj bi se to dogajalo zelo pogosto, pa, kot kaže, v Sloveniji to le ni tako pereč problem oz. žrtve ne menijo, da je to tako velik prekršek, da bi zahteval ukrepe. Po podatkih informacijske pooblaščenke namreč še nihče ni prijavil take kršitve (Safe.si 2009). Obenem pa je tudi impersonacija oz. prevzemanje identitete ob registraciji lahko kmalu neuspešna, če nato posameznik ne ohranja in »dokazuje« svoje prevzete identitete tudi z obnašanjem, objavami in nadaljnjimi reprezentacijami samega sebe na svojem profilu ter v interakciji z drugimi.

Druga oblika kraje identitete, s katero se lahko srečajo uporabniki spletnih družbenih medijev, je kraja identitete zaradi zlorabe podatkov, ki jih objavijo na svojem profilu. Zaradi zlorabe teh podatkov lahko pride tako do prevzema identitete kot do finančne kraje identitete. Vendar pa sem preko analize varnostnih nastavitev in načel pri štirih družbenih medijih ugotovila, da lahko za preprečitev take oblike kraje identitete veliko naredi sam uporabnik. Vsi analizirani spletni družbeni mediji namreč svojim uporabnikom omogočajo, da svoj profil in osebne podatke, ki jih na njem objavijo, ustrezno zavarujejo ter preprečijo dostop do njih. Torej

se morajo pred krajo identitete v prvi vrsti zavarovati uporabniki sami. Podatki iz leta 2008 (Seppä 2008, 3) kažejo, da je le ena četrtina uporabnikov Facebooka spremenila privzete nastavitve, svoj profil zaklenila in onemogočila vpogled v informacije, objavljene na profilu komur koli. Torej morajo sami uporabniki najprej dvigniti svojo zavest o nevarnostih, ki jih s seboj prinaša objavljanje osebnih podatkov na spletnih družbenih medijih. S tem se bo namreč tudi povečala verjetnost, da se bodo zavarovali vsaj v tej meri, da bodo svoj profil zaklenili in pregledovanje objavljenih vsebin dovolili zgolj svojim »prijateljem«. Poleg spremembe varnostnih nastavitev lahko uporabnikom pred krajo identitete pomaga tudi premišljeno objavljanje vsebin na profilih. Uporabniki bi tako morali pred objavo osebnih podatkov, fotografij, video posnetkov itd. na katerem koli spletnem mediju premisliti, če je vsebina primerna za objavo in ne predstavlja prevelike potencialne nevarnosti za vdor v njihovo zasebnost ali celo krajo identitete. Učinkovita obramba pred morebitno krajo identitete je tudi premišljeno sprejemanje spletnih »prijateljev« v spletno družbeno omrežje. Čeprav je ena izmed funkcij družbenih medijev na spletu tudi spoznavanje novih ljudi, lahko prav to predstavlja grožnjo za krajo identitete. Na spletu namreč ni neizpodbitnega zagotovila, da je identiteta, s katero se predstavlja posameznik, resnična. Zgodi se lahko, da je namen neznanca, ki uporabnika zaprosi za »prijateljstvo« na spletnem družbenem mediju, ravno nelegalno pridobivanje informacij, kar lahko pripelje do kraje identitete. Ko je posameznik enkrat »prijatelj« uporabnika, ima tudi dostop do njegovega profila ter na njem objavljenih vsebin in podatkov. Brez previdnosti pri sprejemanju »prijateljev« v spletno družbeno omrežje so namreč tudi varnostne nastavitve o zasebnosti profila brez pomena.

7 LITERATURA

Boyd, Danah M. in Nicole B. Ellison. 2007. Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13 (1). Dostopno prek: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (25. avgust 2009).

Boyd, Danah. 2008. Facebook's Privacy Trainwreck. *Convergence: The International Journal of Research into New Media Technologies* 14 (1): 13-20. Dostopno prek: http://con.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/14/1/13 (15. september 2009).

Caeton, Daniel A. 2007. The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web. *Bulletin of Science, Technology & Society* 27 (1): 11-23. Dostopno prek: http://bst.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/27/1/11 (15. september 2009).

Donath, Judith S.. 1998. Identity and deception in the virtual community. *Communities in Cyberspace*. Dostopno prek: http://smg.media.mit.edu/papers/Donath/IdentityDeception/IdentityDeception.pdf (24. junij 2009).

Dwyer, Catherine, Starr Roxanne Hiltz in Katia Passerini. 2007. *Trust nad privacy concern within social networking sites: A comparison of Facebook and MySpace*. Proceedings of the Thirteenth Americas Conference on Information Systems. Dostopno prek: http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf (27. avgust 2009).

Facebook. Dostopno prek: www.facebook.com (2. januar 2009).

Flickr. Dostopno prek: www.flickr.com (10. junij 2009).

Gauntlett, David in Ross Horsley. 2004. *Web.Studies*. London: Edward Arnold Limited.

Giles, David. 2003. *Media Psychology*. New Jersey: Lawrence Erlbaum Associates.

Gross, Ralph in Alessandro Acquisti. 2005. *Information Revelation and Privacy in Online Social Networks (The Facebook case)*. ACM Workshop on Privacy in the Electronic Society. Dostopno prek: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf (8. januar 2009).

Kelly, Spencer. 2008. Identity 'at risk' on Facebook. *BBC News*, 1. maj. Dostopno prek: http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm (25. avgust 2009).

Lahlou, Saadi. 2008. Identity, social status, privacy and face-keeping in digital society. *Social Science Information* 47 (3): 299-330. Dostopno prek: http://ssi.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/47/3/299 (20. september 2009).

Mayfield, Antony. 2008. *What is Social Media?* Dostopno prek: http://www.docstoc.com/docs/4827195/What-is-Social-Media (30. april 2009).

Monahan, Torin. 2009. Identity theft vulnerability. *Theoretical Criminology* 13 (2): 155-176. Dostopno prek: http://tcr.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/13/2/155 (12. september 2009).

Orsini, Merrily. 2009. How Home Health Care Agencies Can Join the Chorus of Empowered Voices. *Home Health Care Management & Practice* 20 (10): 1-6. Dostopno prek: http://hhc.sagepub.com.nukweb.nuk.uni-lj.si/cgi/rapidpdf/1084822309343871v1 (12. september 2009).

Pirc Musar, Nataša in Jasna Rupnik. 2008. Zanke in pasti na spletnih straneh. *Dnevnik.si*, 28. januar. Dostopno prek: http://www.dnevnik.si/tiskane_izdaje/dnevnik/295017/ (6. oktober 2009).

Praprotnik, Tadej. 2003. *Skupnost, identiteta in komunikacija v virtualnih skupnostih*. Ljubljana: ISH.

Rheingold, Howard. 2000. *The Virtual Community. Homestanding on the Electronic Frontier*. London: MIT.

RIS. 2009a. *Posamezniki na Facebooku preživijo 700 % več časa*. Dostopno prek: http://www.ris.org/2009/06/Raziskave/Posamezniki_na_Facebooku_prezivijo_700__vec_casa/ (15. oktober 2009).

--- 2009b. *Facebooku največ obiskovalcev in uporabniškega časa*. Dostopno prek: http://www.ris.org/2009/08/Raziskave/Facebooku_najvec_obiskovalcev_in_uporabniskega_casa/?&cat=682&p1=276&p2=285&p3=1318&p4=1327&id=1327 (15. oktober 2009).

--- 2009c. *Spletna socialna omrežja*. Dostopno prek: http://www.ris.org/index.php?fl=2&lact=1&bid=9805&menu=0 (4. november 2009).

Safe.si. 2009. *Kraja identitete na spletu – kaj storiti?* Dostopno prek: http://www.safe.si/index.php?fl=2&lact=1&bid=1560&page=6&parent=6 (15. oktober 2009).

Seppä, Ville. 2008. *The Future of Social Networking*. Seminar on Internetworking. Dostopno prek: http://www.cse.hut.fi/en/publications/B/1/papers/Seppa_final.pdf (9. januar 2009).

STAT. 2009. *Uporaba interneta v gospodinjstvih in pri posameznikih, Slovenija, 2009*. Dostopno prek: http://www.stat.si/novica_prikazi.aspx?id=2670 (15. oktober 2009).

Ule, Mirjana. 2005. *Psihologija komuniciranja*. Ljubljana: FDV.

Virtualni 'prijatelji' lahko ukradejo vašo identiteto. 2007. *Finance*, 24. oktober. Dostopno prek: http://www.finance.si/194604 (25. avgust 2009).

Twitter. Dostopno prek: www.twitter.com (3. januar 2009).

Z., A. 2009. Pazite se nadlegovalcev! *Zurnal24.si*, 10. februar. Dostopno prek: http://www.zurnal24.si/znanost-in-tehnologija/pazite-se-nadlegovalcev-131204 (6. oktober 2009)

Youtube. Dostopno prek: www.youtube.com (3. januar 2009).

PRILOGA A: Tabela pregleda ugotovitev analize nastavitev pri spletnih družbenih medijih

Tabela 5.1 Pregled ugotovitev analize nastavitev pri spletnih družbenih medijih

ANALIZIRAN SPLETNI DRUŽBENI MEDIJ / KRITERIJ ANALIZE	FACEBOOK	TWITTER	FLICKR	YOUTUBE
registracijski postopek, ki zagotavlja avtentičnost uporabnika	×	×	×	×
možnost regulacije dostopa do profila	√	√	√	√
možnost reguliranega dodajanja »prijateljev«	√	√/× *	√	/
možnost reguliranja dostopa do objavljenih vsebin (fotografij, video posnetkov, itd.)	√	√	√	√
možnost nadzora nad aplikacijami	√	/	/	/
oblikovana načela o varnosti	√	√	×	√
oblikovana načela o zasebnosti	√	√	×	√

Legenda: √ - omogoča, × - ne omogoča, / - ne podpira te funkcije
* odvisno od tega, ali ima uporabnik profil zaklenjen ali ne