Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-683-686

SOCIO-PSIHOLOŠKI I BEZBEDNOSNI RIZICI NARUŠAVANJA PRIVATNOSTI NA DRUŠTVENIM MREŽAMA

Nenad Putnik[1], Lepa Babić[2], Boris Kordić[1]
[1]Fakultet bezbednosti, Beograd
[2]Singidunum Univerzitet, Beograd

Abstract:
Svest prosečnog korisnika društvenih mreža o sopstvenoj bezbednosti kroz zaštitu privatnosti nije ni približno srazmerna stvarnoj pretnji. Osnovne greške prosečnog korisnika računara su greška naivnosti i greška poverenja, a posledice su propusti u preduzimanju mera zaštite privatnosti. Kod supstancijalne upotrebe društvenih mreža greške posebno pogađaju pojedince jer deluju na psihičku stabilnost osobe, dok kod instrumentalne upotrebe pogađaju društvene grupe jer deluju na socijalni identitet. Neophodno je usmeriti aktivnosti društva na obrazovanje korisnika za bezbednosnu upotrebu društvnih mreža na internetu.

Key words:
društvene mreže,
internet,
bezbednost,
zaštita privatnosti,
identitet.

UVOD

Kontinuirani razvoj informaciono-komunikacione tehnologije doveo je do značajnih promena u načinu funkcionisanja društva. Ulazak računara i interneta u masovnu upotrebu, počev od proizvodnih pogona, kancelarija, do dečijih soba, omogućio je nesagledive razvojne potencijale komunikacije među ljudima. Informatička revolucija nije stvorila samo nova tehnička pomagala već i sopstveni jezik, te razvila specifične oblike komunikacije [1]. Druga strana tog razvoja je činjenica da se svako tehničko-tehnološko dostignuće može upotrebiti ne samo za dobrobit pojedinca i društva već i na njihovu štetu.

Posmatrajući sa tehnološkog, socio-psihološkog, a potom i bezbednosnog stanovišta, internet je načinio prekretnicu u shvatanju i funkcionisanju svakodnevnog života i rada. Raznovrsne informacije (tekstualne, audio, video itd.) su, putem web-prezentacija i pratećih aplikacija, postale dostupne za saznavanje, upotrebu i razmenu među stotinama miliona ljudi širom Planete. Takva virtuelno-informaciona povezanost bila je inspiracija i osnova za kreiranje i implementaciju onoga što danas ustaljeno nazivamo društvenim mrežama, a među kojima su kod nas najpoznatije Facebook, Twitter i LinkedIn (v. Tabelu 1).

Pojedinac se na društvenoj mreži samopredstavlja na način koji data društvena mreža omogućava. To može biti kroz vizuelne sadržaje (fotografije, video snimci), javno iskazanu pripadnost pojedinim grupama, prikazana interesovanja, komentare, podatke o sebi, i slično. Samopredstavljanjem pojedinac može prikazati svoj stvarni identitet, a može kreirati lažne identitete. Jednom postavljen identitet čini pojedinca izloženim svim mogućim reakcijama članova društvene mreže i šire. One mogu biti kako pozitivne tako i negativne, ili se mogu doživeti kao pozitivne ili negativne. U ovom radu ćemo razmotriti negativne aspekte narušavanja privatnosti na društvenim mrežama.

Tabela 1

Pregled najpopularnijih društvenih mreža	Društvene mreže i broj korisnika[a]	
	Naziv društvene mreže	Prosečan broj korisnika na mesečnom nivou
1.	Facebook	900,000,000
2.	Twitter	290,000,000
3.	LinkedIn	250,000,000
4.	Pinterest	150,000,000
5.	Google Plus+	126,000,000
6.	Tumbir	125,000,000
7.	Instagram	100,000,000
8.	Flickr	80,000,000
9.	VK	79,000,000
10	MySpace	40,000,000
11.	Tagged	38,000,000
12.	Meetup	35,000,000
13.	Ask.fm	34,000,000
14.	MeetMe	10,500,000
15.	ClassMates	10,000,000

Izvor: *Top 15 Most Popular Social Networking Sites – February 2014.* (2014). Preuzeto 20. februara 2014, sa http://www.ebizmba.com/articles/social-networking-websites

NARUŠAVANJE PRIVATNOSTI NA DRUŠTVENIM MREŽAMA

Kvalitativna i kvantitativna ekspanzija društvenih mreža ima i svoju „tamnu stranu". Narušavanje privatnosti korisnika i zloupotreba privatnih podataka su trenutno neki od najvećih problema, odnosno negativan nusprodukt ekspanzije usluge društvenog umrežavanja na internetu. Analitičari smatraju da će popularnost društvenih mreža u budućnosti opasti upravo zbog sve češćih zloupotreba informacija [2].

Privatnost se obično definiše kao pravo svakog građanina da kontroliše svoje lične informacije i da odlučuje o njima (da ih čuva ili otkriva drugim licima). Privatnost je fundamentalno ljudsko pravo. Priznaju ga Univerzalna deklaracija o ljudskim pravima, Međunarodni sporazum o građanskim i političkim pravima i mnoge druge međunarodne i regionalne konvencije o ljudskim pravima [3].

Iako se za sve usluge na internetu, odnosno ni za sam internet, ne može reći da u prvi plan stavljaju privatnosti korisnika, kod društvenih mreža se privatnost najdrastičnije, najkonkretnije i najčešće narušava. To se odvija kroz nekoliko segmenata od kojih su korisnički i aplikacijski (tehnički) aspekt najkonkretniji. Najčešće korisnici sami postavljaju određene lične informacije, podatke i materijal koji spada u domen privatnog saržaja, te ih potom dele drugim korisnicima. Na taj način oni nesvesno i direktno omogućavaju narušavanje vlastite privatnosti, jer omogućavaju da se njihovi lični podaci zloupotrebe kako od strane drugih korisnika, tako i od strane same društvene mreže [4].

Može se reži da je privatnost korisnika narušena samom objavom bilo kojih informacija na društvenom web sajtu jer one automatski pripadaju kompaniji i ostaju sačuvane na njenim serverima čak i kada korisnik ugasi nalog. Takođe, ostavljanjem komentara na statusu "prijatelja", profil korisnika koji je ostavio komentar postaje vidljiv ne samo prijateljima njegovog prijatelja nego i njihovim prijateljima. Ukratko, podatak koji se unese postaje svima potencijalno vidljiv.

Problem se dodatno usložnjava prihvatanjem nepoznatih osoba za prijatelje na društvenim mrežama. Ovim činom korisnik rizikuje da njegovi lični podaci budu iskorišćeni u različite svrhe. Privatni podaci, kao što je adresa elektronske pošte, mogu dospeti na spem (eng. spam) liste, tako da korisnik prima mimo svoje volje elektronsku poštu koja je najčešće komercijalnog ili propagandnog karaktera. Posećivanje sumnjivih linkova na Fejsbuku dovodi korisnika u rizik da se zarazi nekim malicioznim softverom, da izloži sve svoje podatke nekome ili da pokrene skriptu koja će spemovati sve njegove prijatelje i tako se dalje širiti [5].

Imajući u vidu da se većina, ako ne i sve društvene mreže, baziraju na ekonomskim principima poslovanja (omasovljavanje je logičan cilj), tehnička platforma društvenih mreža je tako koncipirana da od korisnika prikuplja određene podatke neophodne za upoznavanje i komunikaciju sa drugima (što je i suština društvenih mreža), ali ona isto tako prikuplja i određene podatke koji se filtriranjem segmentiraju i koriste u marketinške svrhe. Upravo ova mogućnost zloupotrebe određenih podataka od strane društvenih mreža predstavlja jedan od segmenata narušavanja privatnosti korisnika koji u poslednje vreme sve više dobija i određenu globalnu, ali i regionalnu političku i normativnu stranu posmatranja i reagovanja. Usled navedenog, privatnost na društvenim mrežama je sigurno relativizirana, čemu doprinose kako sami korisnici koji dobrovoljno daju određene podatke o sebi (pristupom i korišćenjem društvene mreže), tako i same društvene mreže (prikupljanjem i filtriranjem, te segmentiranjem korisničkih podataka za ciljane marketinške kampanje).

NAČINI ZLOUPOTREBE PRIVATNIH SADRŽAJA

Korisnici društvenih mreža, usled nedostatka edukacije u pogledu opasnosti kojima su izloženi, na svoje profile nepromišljeno ostavljaju informacije i multimedijalne sadržaje koji mogu biti zloupotrebljeni od drugih, različito motivisanih korisnika interneta. Osim što su izloženi riziku od narušavanja lične privatnosti i zloupotrebe privatnih sadržaja, korisnici su izloženi i riziku od političke ili ideološke manipulacije.

Informacije obznanjene na javnoj društvenoj mreži se najčešće koriste za planiranje i izvršenje širokog spektra kriminalnih radnji: pljačke, kidnapovanja, fizičkog i psihičkog maltretiranja itd. Preciznije, lični podaci sa društvenih mreža bivaju (zlo)upotrebljeni u cilju realizacije početne faze kriminalne aktivnosti, dok se ostale faze realizuju na "klasičan" način. U tom smislu, društvene mreže se koriste u cilju pronalaženja saradnika i samih izvršilaca kriminalne aktivnosti, vrbovanja žrtvi za pripremanje dela, za prikupljanje relevantnih informacija, pomaganje u vršenju određenih aktivnosti, obezbeđivanje sredstava i slično. Sa pojavom društvenih mreža i širenjem usluga elektronskih transakcija kriminalci su, takoreći, počeli ne samo da inoviraju metode za izvođenje prevara već i da automatizuju tehnike prikupljanja ličnih podataka u cilju postizanja što veće zarade.

Sajber kriminalci najčešće koriste tehnike socijalnog inženjeringa i fišinga kako bi došli do ličnih podataka žrtve [6]. Na ovaj način žrtve mogu da pretrpe značajne finansijske gubitke ili, u ozbiljnijim slučajevima, čak i gubitak sopstvenog „elektronskog identiteta", koji biva iskorišćen za kriminalne ciljeve. Štetu pričinjenu krađom ličnih podataka, dakle, ne bi trebalo izražavati samo u finansijskom gubitku već i u gubitku psihičkog integriteta ličnosti, reputacije i kredibiliteta oštećenog pred različitim državnim institucijama (finansijskim, administrativnim, osiguravajućim itd).

Svaki pojedinac je ranjiv na različite vrste otvorenih i prikrivenih napada zlonamernih aktera, bilo da oni za cilj imaju pravljenje neslanih šala ili jasne kriminalne namere. Osećaj narušavanja i gubitka ličnog mira i privatnosti može imati dugotrajne psihološke posledice. Deca su posebno osetljiva kategorija korisnika društvenih mreža. Najčešće informacije koje deca ostavljaju na korisničkom profilu bivaju zloupotrebljene od strane njihovih vršnjaka. Reč je fenomenu tzv. *sajber bulinga* (*engl.* cyber-bullying) odnosno zadirkivanja, kinjenja ili, u težim oblicima, zlo-

stavljanja u virtuelnom svetu. Sajber buling je fenomen koji je u neprestanom porastu. Rezultati istraživanja, koje je sprovedeno u pet srednjih škola u Beogradu, pokazali su da je 10% učenika uzrasta od 11 do 15 godina sprovodilo ovu vrstu aktivnosti prema drugim učenicima. Osim toga, istraživanje je pokazalo da je 20% učenika bilo žrtva ovakvih, virtuelnih, kampanja [7]. Ovaj vid torture može ostaviti značajne psihološke posledice, o čemu se u stručnoj literaturi vodila široka debata nakon otkrivanja prvog slučaja virtuelnog silovanja [8].

Opšte uzev, primetno je da digitalni mediji opskrbljuju neprijatelja znatno bogatijim i moćnijim arsenalom alata kojima se može upustiti u psihološko ratovanje. Sajber klevetanje ili digitalne kampanje za ozloglašavanje imaju potencijal da dopru do neverovatno velikog broja ljudi, ogromnom brzinom, i da nanesu velike frustracije i kolateralnu štetu žrtvi. Ponovno uspostavljanje poverenja i spasavanje reputacije u jeku virtuelnih kampanja za ozloglašavanje predstavljaju veliki izazov žrtvama. Lakoća sa kojom javne kampanje „ocrnjivanja" mogu biti otpočete na internetu stvara značajnu disproporcionalnost u korist napadača. Meta napada se stavlja u položaj da se brani i u stanju je nesigurnosti povodom napadačevog identiteta, motiva, lokacije, ciljeva, kao i toga da li je napad izvršio pojedinac ili grupa ljudi. Ona, najčešće, i ne zna kome se može obratiti za pomoć u takvoj situaciji budući da je u većini država izražena konfuzija nadležnosti nad ovakvim deliktima.

Obznanjeni ili otuđeni privatni sadržaji korisnika društvenih mreža i drugi lični podaci mogu biti iskorišćeni za ucenjivanje i vrbovanje korisnika da pristupe subverzivnim društvenim grupama ili aktivističkim pokretima. U digitalnom okruženju su rizici od manipulacije korisnicima društvenih mreža i njihovog vrbovanja u ovakve organizacije postali znatno izraženiji jer je lična privatnost korisnika samo formalna, dok se tehničke mogućnost za ekstrakciju ličnih podataka neprestano uvećavaju.

PSIHOLOŠKI BEZBEDNOSNI RIZICI NARUŠAVANJA PRIVATNOSTI NA DRUŠTVENIM MREŽAMA

Postoje razmišljanja da prostor interneta zahvaljujući svojim osobinama nosi u sebi mogućnost da zamagli granice identiteta. Međutim, na mnogim poljima se potvrđuje podudarnost online i offline identiteta. Pokazalo se da je pitanje privatnosti podjednako važno u online socijalnom prostoru kao i u offline prostoru [9], kao što se dešava i obrnuta stvar, da su online obmane podjednako zastupljene kao i offline [10]. Stoga treba biti rezervisan prema shvatanjima da ljudi na internetu lakše prikazuju svoje istinsko ja [11]. Pre možemo očekivati da će pitanje online identiteta biti prožeto sličnim problemima koje susrećemo i kod offline identiteta.

Društvene mreže na internetu su nastale kao paralelna realnost i proširenje društvene sredine koja omogućava ljudima virtuelni međusobni odnos [12]. Istraživanja društvenih mreža na internetu su sve razvijenija u poslednje vreme. Dosadašnja istraživanja su utvrdila postojanje tri dimenzije upotrebe prijateljskih mreža na internetu, i to informacionu, prijateljsku i povezujuću [13], a otkrivene su četiri primarne potrebe za učešće u grupama na Facebook-u: druženje, zabava, traganje za vlastitim statusom i informisanje [14].

Pitanje identiteta u socijalnom prostoru je usko povezano sa pitanjem privatnosti. Kad se privatnost posmatra iz individualnog ugla onda je prihvatljiva teorija privatnosti u četiri kategorije [15]: ne-intruzija ili pravo da se bude ostavljen na miru, isključenost ili pravo da se bude nedostupan za druge, ograničenje ili pravo da se zaštite delovi znanja o sebi slično čuvanju tajne, i kontrola ili pravo na sposobnost kontrolisanja širenja informacija o sebi. S druge strane, ukoliko je reč o društvenom aktivizmu ljudi nekad misle da su stavovi izrečeni na društvenim mrežama privatna stvar kao diskusija sa kolegama u kafani [16]. Međutim, mnogo su veće posledice online izgovorenih stavova zbog kojih su pojedini akteri, čak i kad je njihov identitet prikriven, dospeli na sud zbog lične odgovornosti [17]. Treba uzeti u obzir da pojedine društvene mreže imaju veći broj pristalica nego što je stanovništvo mnogih država.

Ono što razlikuje online identitet je sloboda od fizičkog prisustva među drugima. S druge strane, socijalna sredina kao spoljašnji faktor značajan za formiranje identiteta i te kako je prisutan na društvenim mrežama na internetu. Identitet osobe, npr. na Facebooku, podjednako se formira informacijama koje osoba stavlja na svoj profil kao i informacijama koje postavljaju njegovi ili njezini prijatelji. Uglavnom se društvene mreže na internetu koriste na dva osnovna načina: supstancijalan i instrumentalan način [18]. Supstancijalan način je posebno povezan sa zadovoljavanjem osnovnih psiholoških potreba pojedinca koje pomažu u učvršćivanju ličnog i socijalnog identiteta i pozitivnog samopoimanja. Instrumentalan način je povezan sa zadovoljavanjem kako socijalnih potreba tako i potrebe za informisanjem. Negativni uticaji dezinformacija i manipulacija u sajber prostoru kod supstancijalne upotrebe društvenih mreža na internetu posebno pogađaju individualne žrtve jer deluju na psihičku stabilnost osobe, dok kod instrumentalne upotrebe posebno pogađaju društveni aspekt grupne pripadnosti jer deluju na socijalni identitet osobe.

U posebnu kategoriju treba odvojiti krađu identiteta koja ima za cilj raspolaganje novčanim i drugim materijalnim dobrima osobe čiji je identitet ukraden. Nagle promene u sajber svetu zahtevaju konstantnu edukaciju za jačanje motivacije i sposobnosti korisnika za upotrebu tehničkih sredstava u cilju prevencije krađe identiteta [19]. Pojedini nalazi ukazuju da su samoregulativni mehanizmi korisnika usmereni na zaštitu privatnosti razočaravajući [20].

S druge strane, internet pruža bezbrojne mogućnosti istraživanja identiteta kroz kreiranje avatara i višestrukih identiteta. U pojedinim kutlurama je uobičajeno da se kreiraju profili koji prikrivaju offline identitet osobe tako što imaju dugačije ime i ne nose slike osobe koja ih je kreirala. Na taj način pojedinci koriste online prostor društvenih mreža da se prikažu u skladu sa svojim željama i potreba, a u skladu sa socijalnom sredinom u kojoj žive.

ZAKLJUČAK

Svest prosečnog korisnika računara o narušavanju sopstvene bezbednosti i privatnosti nije ni približno srazmerna stvarnoj pretnji. Podela na online i offline dovodi kod korisnika do nejasnog razlikovanja šta je privatno a šta javno. Izrečene i postavljene misli, slike i druga značenja na društvenim mrežama dobijaju mnogo veću javnost nego u našem svakodnevnom životu. Osnovna greška prosečnog korisnika računara je pretpostavka da on nema šta da krije i da samim tim nije interesantan onima koji bi mogli da iskoriste bezbednosne propuste u njegovom sistemu i da naruše njegovu privatnost. Druga velika greška je ta što prosečan korisnik ima apsolutno poverenje u kompanije kojima daje svoje lične podatke. To poverenje kod korisnika stvara iluziju potpune privatnosti i sigurnosti sistema koji koristi. Zbog toga on ne preduzima dodatne mere da bi se zaštitio, već samo konzumira uslugu koja mu je ponuđena. Čak i onaj procentualno mali broj korisnika koji su donekle zabrinuti za svoju privatnost i trude se da je na bilo koji način zaštite, veoma često prave značajne bezbednosne propuste.

Zahvalnice

Ovaj naučni rad je proistekao iz saradnje dva projekta: "Bezbednost i zaštita organizovanja i funkcionisanja vaspitno-obrazovnog sistema u Republici Srbiji (osnovna načela, principi, protokoli, procedure i sredstva)", Ministarstvo nauke Republike Srbije, br. 47017, za period 2011.-2014. godine, i "Unapređenje konkurentnosti Srbije u procesu pristupanja Evropskoj uniji", Ministarstvo nauke Republike Srbije, br. 47028, za period 2011.-2014. godine.

LITERATURA

[1] Z. Cvetković, "Kompjuterski kriminal", Branič, vol. 114, pp. 2-3, 2001.

[2] Đ. Klipa, & R. Dragović, "Bezbednost i tehnološki aspekti društvenih mreža", preuzeto 21.12.2013. sa http://www.e-drustvo.org/proceedings/YuInfo2012/html/pdf/385.pdf

[3] J. Kurbalija, Uvod u upravljanje internetom, Beograd: Albatros Plus, 2011.

[4] A. Miladinović, Fejsbuk i kriminalitet, Banja Luka: Internacionalna asocijacija kriminalista, 2013.

[5] I. Tešić, "Iluzija privatnosti na internetu", preuzeto 21.12.2013. sa http://www.infoteh.rs.ba/zbornik/2013/radovi/STS/STS-25.pdf

[6] N. Putnik, Sajber prostor i bezbednosni izazovi, Beograd: Fakultet bezbednosti, 2009.

[7] B. Popović-Ćitić, S. Djurić, & V. Cvetković, "The prevalence of cyberbullying among adolescents: A case study of middle schools in Serbia", School Psychology International, vol. 32(4), pp. 412–424, 2011.

[8] D. Džonson, Kompjuterska etika, Beograd: Službeni glasnik, 2006.

[9] S. Hongladarom, "Personal Identity and the Self in the Online and Offline World", Minds & Machines, vol. 21, pp. 533–548, 2011.

[10] N. Baym, Personal connections in the digital age, Polity Press, 2010.

[11] S. Zhao, S. Grusmucka, & J. Martina, "Identity construction on Facebook: digital empowerment in anchored relationships", Computers in Human Behavior, vol 24(5), pp. 1816–1836, 2008.

[12] B. Kordić, & L. Babić, "Facebook i druženje kod srednjoškolaca", Teme, vol 35(4), pp. 1627-1640, 2011.

[13] J. Raacke, & J. Bonds-Raacke, "MySpace and Facebook: applying the uses and gratifications theory to exploring friend-networking sites", Cyberpsychology & Behavior, vol. 11(2), pp. 169–174, 2008.

[14] N. Park, K. F. Kee, & S. Valenzuela, "Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes", Cyberpsychology & Behavior, vol. 12(6), pp. 729–33, 2009.

[15] H. T. Tavani, "Philosophical theories of privacy: Imprications for an adequate online privacy policy", Metaphilosophy, vol. 38(1), pp. 1–22, 2007.

[16] M. Sveningsson-Elm, „How do notions of privacy influence research choices?" in Internet inquiry: Conversations about method. Sage Publications, Inc. 2008.

[17] J. Richardson, "The Changing Meaning of Privacy, Identity and Contemporary Feminist Philosophy", Minds & Machines, vol. 21, pp. 517–532, 2011.

[18] B. Kordić, & N. Putnik, "Društvene mreže na internetu i bezbednosti učenika", u Bezbednosni rizici u obrazovno-vaspitnim ustanovama, B. Popović-Ćitić i sar. (Urednici). Beograd: Fakultet bezbednosti, 2012, str. 169-182.

[19] G. R. Milne, A. J. Rohm, & S. Bahl, „Consumers' Protection of Online Privacy and Identity", The Journal of Consumer Affairs, vol. 38(2), pp. 217-232, 2004.

[20] N. K. Katyal, "Criminal Law in Cyberspace", University of Pennsylvannia Law Review, vol. 149(4), pp. 1003–1115, 2001.

SOCIO-PSYCHOLOGICAL AND SECURITY RISKS OF VIOLATION OF PRIVACY ON SOCIAL NETWORKS

Abstract:
Awareness of the average user of social networks of their own security by protecting privacy is not nearly proportional to the actual threat. The basic error of average computer users are naiveness and confidence error, and the consequences are failures to take measures to protect privacy. With substantial use of social networking errors particularly affect individuals because they act on the person's mental stability, while the instrumental use affects social groups because they act on social identity. It is necessary to direct the activities of the society towards the education of users for secure use of social networks on the Internet.

Key words:
social networks,
internet,
security,
protection of privacy,
identity.+