Bodoči učitelji in ravnanje z občutljivimi podatki na spletu

Dr. Tomaž Bratina

Pedagoška fakulteta Univerze v Mariboru

Razen znanj, potrebnih za uporabo IKT v izobraževanju, morata učenec in učitelj znati odgovorno uporabljati spletne storitve. Med varno in odgovorno rabo spletnih storitev sodi tudi ravnanje z občutljivimi podatki. Z razmahom socialnih omrežij postaja ravnanje z občutljivi podatki dokaj brezbrižno. Prispevek opisuje poznavanje in razumevanje spletne varnosti bodočih učiteljev.

Uvod

Od posameznika se danes pričakuje, da je usposobljen za pridobivanje informacij oziroma znanja s spleta. To še posebej velja za učence oziroma študente, ki učne vsebine najpogosteje sprejemajo v obliki multimedijskih učnih gradiv ter s pomočjo sistemov za posredovanje in upravljanje z učnim vsebinami. Značilnost teh sistemov je njihova povezava v splet in dostopnost. To je vsekakor prednost, ki pa lahko skriva tudi določeno mero nevarnosti. Z uporabo učnih vsebin, posredovanih s pomočjo omenjenih sistemov, ki so relativno varni, se pri uporabniku vzbudi občutek zanesljivosti in varnosti. Zato obstaja velika verjetnost, da bosta podoben vzorec zaupanja učenec in študent uporabila tudi pri pridobivanju znanja in informacij iz drugih virov ali v katerih drugih spletnih aplikacijah.

Socialna omrežja, občutljivi podatki in digitalna varnost

Posebej je v kontekstu brezbrižnosti in pretiranega zaupanja potrebno izpostaviti socialna omrežja, ki s svojim načinom delovanja nevarno obnašanje kar spodbujajo (Kugler 2012). Izdelava osebnih profilov je eden izmen največjih varnostnih izzivov. Številni uporabniki povsem nekritično posredujejo številne občutljive informacije in jih delijo z drugimi bolj ali manj znanimi, celo popolnoma neznanimi osebami. Člani omrežja se obravnavajo kot prijatelji in zaupanja vredne osebe, čeprav številni izmed njih lahko uporabljajo lažne identitete. Takšen, skorajda družinski odnos, nepazljivemu uporabniku daje občutek lažne varnosti. Primerno ravnanje z občutljivimi podatki je le eden izmed vidikov varnosti v digitalnem svetu. Pomembno je tudi poznavanje drugih oblik nevarnosti ter skrb za varnost datotek. Vse omenjene vidike strokovnjaki uvrščajo pod enoten pojem digitalna varnost (Krašna in Bratina 2011). Zato je digitalno varnost potrebno razumeti kot enega izmed ključnih elementov digitalnih kompetenc, kar je še posebej pomembno pri vzgoji bodočih učiteljev. Prav aktivni in tudi bodoči učitelji imajo pomembno ter nenadomestljivo vlogo v procesu razvoja digitalne varnosti. Še posebej z vidika opozarjanja učencev in staršev na potencialne nevarnosti na spletu. V naši raziskavi smo preverili, kakšno je stanje nekaterih vidikov digitalne varnosti pri študentih Pedagoške fakultete v Mariboru.

Kraja identitete

Kraja identitete je oblika goljufije, kjer nekdo drug uporablja osebne podatke prizadetega posameznika. Pogosto se kraje identitete izvajajo za kasnejši dostop do osebnih in finančnih virov ali koristi kakršne koli vrste, vedno pa v imenu prizadetega posameznika (Identity Theft 2011). Posledice so za prizadete osebe pogosto zelo resne in težko popravljive. V nekaterih primerih lahko vrnitev na nekdanje stanje traja zelo dolgo ali celo ni možna. Kraje identitete se zelo uspešno izvajajo tudi na socialnih omrežjih, saj uporabniki zelo ravnodušno ravnajo z občutljivimi podatki. Brezskrbna objava podatkov, ki so na videz nepomembni (na primer zakonski stan, točni datumi zaključka izobraževanj, imena živali in osebni interesi) lahko privede do uspešne kraje identitete (Lewis 2012). Predvsem iz osebnih podatkov, kakor tudi drugih prej navedenih podatkov lahko izkušen kriminalec zelo uspešno izvede krajo identitete. Po podatkih delovne skupine za boj proti kraji identitete, je eden izmed načinov pridobivanja osebnih podatkov v procesu kraje identitete tudi ribarjenje. Gre za lažne spletne strani, ki so na videz enake spletnim stranem znanih ponudnikov. Najpogosteje gre za bančne ustanove. Nepozoren ali zaveden uporabnik svoje podatke vpisuje v na videz pristne obrazce, podatki pa se nato posredujejo posameznikom, ki jih zlorabijo. Najuspešnejši so tovrstni napadi na socialnih omrežjih, kjer po podatkih kanadske organizacije za varnost BBB (2012) beležijo kar 70% uspešnost.

Namen in metodologija raziskave

V procesu izobraževanja učiteljev je pomemben poudarek namenjen uporabi IKT v izobraževanju. Opraviti imamo s specifično populacijo in je zato njihove digitalne kompetence potrebno smiselno nadgraditi. Z raziskavo smo želeli preveriti začetno stanje poznavanja digitalne varnosti ter morebitne spremembe skozi čas. Na podlagi ugotovitev bomo prilagodili, spremenili ali razširili obstoječe učne vsebine vezane na digitalno varnost pri uporabi IKT. Za zbiranje podatkov smo izvedli spletno anketiranje z uporabo orodja za izdelavo spletnih anket. Vzorec je obsegal 179 študentov Pedagoške fakultete v Mariboru. Podatke smo obdelali s programom SPSS in statističnimi metodami, ki so pokazale na stanje digitalnih varnostih vidikov v posamezni generaciji in morebitne razlike v varnostnih vidikih med generacijama. Študente smo povabili, da za različne vrste osebnih podatkov označijo, na kakšen način jih objavljajo. Podatke o hišni številki, ulici, poštni številki ali kraju bivanja smo združili v kategorijo lokacijski podatki. Podatke o davčni številki, EMŠO, TRR in plači smo združili v finančne in administrativne podatke. V skupino podatkov o družini smo združili podatke o številu družinskih članov, starših, sorodnikih in partnerjevem imenu.

Rezultati in analiza

Izidi kažejo na dokaj brezskrbno objavljanje občutljivih podatkov na socialnih omrežjih. Podatke o osebnem imenu in datumu rojstva študenti v večini primerov objavijo kot prave. Le nekaj jih te podatke objavi kot lažne. Izpostaviti je potrebno, da študenti svoj spol objavljajo izključno v pravi obliki. Če osebne podatke združimo v skupino, opazimo, da je skoraj tretjina (28,8 %) osebnih podatkov objavljenih v pravi obliki in le 4 % v lažni. Tudi podatke o izobrazbi študenti objavljajo večinoma v pravi obliki, česar pa glede zaposlitvenih možnosti ni mogoče šteti kot problematično.

Nekoliko višjo previdnost je opaziti pri podatkih o bivanju, čeprav je 9,4 % delež pravih objav še vedno dokaj visok. Elektronske naslove študenti pričakovano objavljajo v

pravi obliki, saj sicer sodelovanje v socialnih omrežjih ni učinkovito. Želja po zaščiti zasebnosti se kaže pri omejevanju objave telefonske številke. Premalo pozornosti študenti namenjajo zaščiti družinskih podatkov. Deleža objave teh podatkov v pravi obliki in delež objave osebnih podatkov v pravi obliki sta visoka in omogočata lahek dostop do podatkov, ki so najpogosteje zlorabljeni v okviru kraje identitete.

Varnosti finančnih podatkov namenjajo študenti veliko pozornost, saj jih v glavnem vsi objavijo le v lažni obliki. Tak izid je zadovoljujoč in kaže, da se mladi zavedajo posledic zlorab tovrstnih podatkov. Objavljanje svojih slik in slik drugih oseb je postalo splošno sprejeto v socialnih omrežjih. Opaziti je sicer nekoliko previdnejše objavljanje slik drugih oseb, kljub temu pa so v obeh primerih slike večinoma objavljene v pravi obliki. Zavedati pa se je potrebno, da objava slik drugih oseb brez njihove privolitve lahko privede do sankcij. Zato bi prav objavljanje slik drugih oseb moralo biti bolj odgovorno.

Zaupanje dostopnih podatkov drugim osebam

V praksi pogosto opažamo, da si študenti med seboj izmenjujejo podatke za dostop do spletnih storitev. Razlogi so različni, kažejo pa na podoben efekt (pre)visoke stopnje zaupanja, ki je gotovo tudi posledica obnašanja na socialnih omrežjih. Pogostost tega pojava nas je spodbudila, da preverimo, kako pogosto študenti posredujejo svoja uporabniška imena in gesla drugim osebam.

Iz izidov razberemo, da je pojav posredovanja uporabniških imen in gesel dokaj pogost. Slaba polovica študentov (42,5 %) to počne izjemoma, približno desetina (9,5 %) pa po potrebi. Pri tem se postavlja vprašanje, kdaj in zakaj bi bilo potrebno, da nekomu drugemu zaupamo svoje uporabniško ime in geslo. Nekaj študentov podatke zaupa le poznani osebi. Skupen delež tistih, ki so že zaupali uporabniška imena ali gesla oziroma to počnejo pogosteje, pokaže, da kar 58,7 % študentov neodgovorno ravna s tovrstnimi podatki. Tudi obvestila na vseh vstopnih portalih, da sta uporabniško ime in geslo zaupna podatka, s katerimi je potrebno ravnati skrbno, niso dovolj. Zavedanje pomena varovanja tovrstnih podatkov je zelo slabo in naloga učiteljev je, da mladim približajo pomen varovanja in odgovornega ravnanja s takimi podatki.

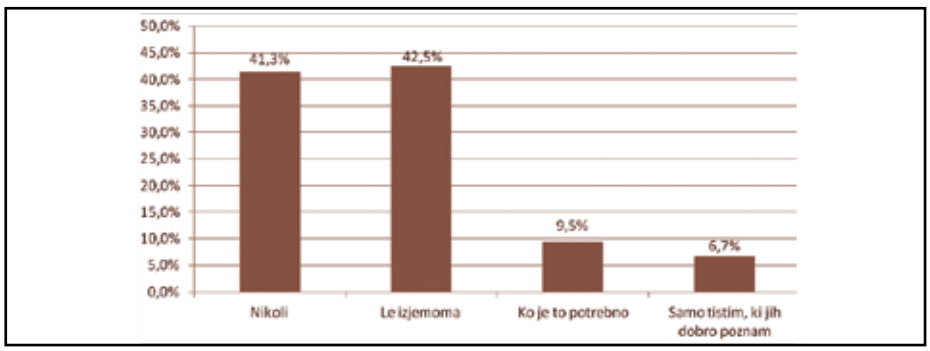
Kraja identitete – razumevanje nevarnosti

Najboljša zaščita pred nevarnostjo kraje identitete je razumevanje mehanizmov in ozaveščenost o nevarnosti kraje identitete. Vsak uporabnik se mora zavedati možnosti, da lahko postane žrtev. Le tako bo vedno skrbel za varnost občutljivih podatkov in jih ne bo zaupal brez predhodne presoje. Zanimalo nas je, v kolikšni meri so študenti seznanjeni s pojmom in mehanizmom kraje identitete in kako prepoznajo varno spletno stran.

Večina študentov (79,3 %) obeh generacij je seznanjenih s pomenom in nevarnostjo kraje identitete. Stanje je zadovoljivo, čeprav obstaja slaba petina (17,3 %) študentov, ki pod nevarnostjo kraje identitete razumejo krajo osebnih dokumentov. Tak delež napačnega razumevanja nekoliko poslabša sicer ugodno sliko, saj kaže na resno nerazumevanje mehanizma kraje identitete. V okviru raziskave smo preverili tudi poznavanje in razumevanje nevarnosti ribarjenja. Razberemo, da sta skoraj dve tretjini (63,7 %) študentov seznanjeni z nevarnostjo ribarjenja in razumejo način delovanja napadalcev. Kljub temu stanje še ni spodbudno. Razlog je v dokaj velikem številu študentov, ki pojem zamenjuje z iskanjem informacij na spletu (16,2 %) in kot pridobivanje prijateljev na socialnih omrežjih. Več kot tretjina (36,3 %) študentov napačno razume pomen in nevarnost ribarjenja.

Sklep

Ugotavljamo dokaj veliko brezbrižnost pri ravnanju z občutljivimi podatki, saj se le ti posredujejo s preveliko lahkotnostjo. Izidi raziskave kažejo, da je med učne vsebine s področja IKT potrebno vključiti tudi vsebine, povezane z varnostjo na spletu. To je še posebej pomembno v procesu izobraževanja učiteljev, ki bodo ta znanja prenašali na učence že v zgodnji fazi rabe spleta. S tem bodo neposredno vzgajali generacije otrok, ki bodo poznali in razumeli nevarnosti na spletu, se jih zavedali, bili na njih pripravljeni ter se jim učinkovito zoperstavili. •



Literatura

- 1ka. FDV, Univerza v Ljubljani CMI: http://www.1ka.si/ (Dostop 10.4 2012).
- Ala-Mutka, Kirstie, Yves Punie, in Christine Redecker. Digital Competence for Lifelong Learning. JRC Technical Notes. <http://ftp.jrc.es/EURdoc/JRC48708.TN.pdf>.
- Bratina, Tomaž, in Marjan Krašna, 2011: Students' attitude toward digital security. Louis Gómez Chova (Ur.). International Technology, Education and Development Conference. Valencia.
- Combating Identity Theft A Strategic Plan. Washington, 2007: The President's Identity Theft Task Force.
- Gabriel, Kristin, 2010: The Dangers of Internet Security Breaches on Social Networking Sites.<http://www.titaniumantivirus.org/in-the-cloud-security/the-dangers-of-internet-security-breaches-on-social-networking-sites/> (Dostop 3.6. 2012).
- Identity Theft, 2011: < http://en.wikipedia.org/wiki/Identity_theft> (Dostop 4. 4 2012).
- Krašna, Marjan, 2010: Digital competences and multimedia: Paper at the International Conference on New Horizons in Education, INTE 2010, June 23-25, 2010. Famagusta, 2010.
- Krašna, Marjan, in Tomaž Bratina, 2011: Digital competences in education: digital security. International Technology, Education and Development Conference (INTED). Valencia: International Association of Technology, Education and Development (IATED). 1634-1641.
- Kugler, Logan, 2012: How to secure your Facebook profile in a post-Timeline world. < http://howto.techworld.com/personal-tech/3336013/how-secure-your-facebook-profile-in-post-timeline-world/> (Dostop 6. 7. 2012).
- Lewis, Kent, 2012: How Social Media Networks Facilitate Identity Theft and Fraud. <http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx> (Dostop 6. 7. 2012).
- Phishing Attacks Continue to Pose Significant Risk, 2012: < http://vi.bbb.org/> (Dostop 1. 7. 2012).