Dr. Tomaž Bratina, Univerza v Mariboru, Pedagoška fakulteta,
tomaz.bratina@uni-mb.si

Bodoči učitelji in poznavanje (ne)varnosti na spletu

Izvirni znanstveni članek

UDK 37.091.64:004

POVZETEK

Uporaba sodobnih oblik posredovanja učnih vsebin izkorišča možnosti, ki jih ponuja IKT. Komponente IKT, vezane na posredovanje učnih vsebin, uporabljajo računalniška omrežja oziroma splet. Od učiteljev in učencev zato uporaba sodobnih oblik posredovanja učnih vsebin zahteva določeno znanje, ki ni neposredno povezano z učno vsebino. Gre za znanje, povezano z odgovorno in varno uporabo spletnih storitev. Spletne storitve v času študija najpogosteje predstavljajo sistemi za posredovanje in upravljanje z učnimi vsebinami, vendar te niso edine. Varna in odgovorna raba spletnih storitev sodi v okvir digitalnih kompetenc in enako tudi varno obnašanje na spletu. Zmotno je namreč prepričanje, da zgolj poznavanje dela s spletnimi sistemi pomeni tudi njihovo varno uporabo. Varna uporaba spletnih storitev razen digitalne kompetentnosti uporabnika zahteva tudi zavedanje in poznavanje nevarnosti, ki jih delo na spletu prinaša. V članku predstavljamo, kako študenti, bodoči učitelji, poznajo in se zavedajo nevarnosti na spletu.

Ključne besede: izobraževanje učiteljev, digitalna varnost, digitalne kompetence, učne vsebine, IKT

Future Teachers' Knowledge on Internet Safety (Risks)

ABSTRACT

The modern way of delivering learning materials makes use of the advantages provided by ICT. ICT components which are related to the distribution of learning materials use computer networks or World Wide Web. Consequently, the teacher and the student alike need to possess certain knowledge which is not related to the subject matter itself. The knowledge in question regards a responsible and safe usage of online services. During their studies, students most commonly use online services through Learning Contents Management Systems, though this is not the only way. A responsible and safe usage of web applications is an essential part of one's digital competences, which comprise, among other things, also safe behaviour online. A common belief that knowing how to work with specific online services automatically implies safe usage of the latter is wrong. The only foundation for a safe and responsible usage of online services is being aware of the risks and possessing adequate knowledge on the possible threats. This article discusses the level of knowledge and awareness of the possible threats in using the Internet in students - future teachers.

Key words: teacher education, digital security, digital competences, learning contents, ICT

Uvod

Pridobivanje informacij in znanja iz različnih virov je postalo nekaj vsakdanjega. To še posebej velja za učeče, ki učne vsebine najpogosteje sprejemajo v obliki multimedijskih učnih gradiv. Posredovanje omenjenih učnih gradiv je tehnološko pogojeno oziroma vezano na sisteme za posredovanje in upravljanje z učnimi vsebinami (angl. learning contents management system – LCMS). Pomembna zahtevana značilnost sistemov LCMS je njihova stalna dostopnost; to omogoča različne načine interakcije, pravilna uporaba pa zato predstavlja prednost tako za učitelja kot za študenta. Čeprav lahko najdemo veliko prednosti, se v tem skrivajo tudi določene nevarnosti. Z uporabo učnih vsebin, posredovanih s pomočjo sistemov LCMS, se pri študentu vzbudi občutek zanesljivosti in varnosti. Učne vsebine namreč prihajajo iz znanega in relativno zanesljivega ter varnega okolja. Tudi posredovanje občutljivih podatkov, kot so na primer študentovi osebni podatki, se na prvi pogled ne zdi problematično. Študent v zameno za občutljiv podatek prejme dostop do učnih vsebin, kar se zdi zadovoljivo. Ker sistemi LCMS tudi

sicer ponujajo dokaj visoko stopnjo varnosti, se ob njihovi uporabi pri študentih utegne pojaviti določena mera brezbrižnosti do obstoječih nevarnosti in potrebe po varovanju podatkov. Znano je, da nekateri študenti svoje dostopne podatke zaupajo drugim iz različnih bolj ali manj smiselnih razlogov. Zato obstaja velika verjetnost, da bo podoben vzorec zaupanja študent uporabil tudi pri pridobivanju znanja in informacij iz drugih virov ali ob uporabi drugih spletnih aplikacij.

V kontekstu brezbrižnosti in pretiranega zaupanja je potrebno posebej izpostaviti družbena omrežja, ki s svojim načinom delovanja nevarno obnašanje spodbujajo (Kugler, 2012). Že tvorba osebnih profilov je eden izmen največjih varnostnih izzivov. Številni uporabniki povsem nekritično posredujejo različne občutljive informacije in jih delijo z drugimi bolj ali manj znanimi ali popolnoma neznanimi osebami. Člani skupnosti družbenega omrežja se obravnavajo kot prijatelji in zaupanja vredne osebe, čeprav številni izmed njih uporabljajo lažne identitete. Takšen, navidezno družinski odnos nepazljivemu uporabniku daje občutek lažne varnosti.

Med varno obnašanje na spletu ne štejemo le skrbnega ravnanja z osebnimi podatki, ampak tudi poznavanje drugih oblik nevarnosti ter skrb za varnost datotek. Vse našteto uvrščamo pod pojem digitalna varnost. Zato je digitalno varnost potrebno razumeti kot enega izmed ključnih elementov digitalnih kompetenc, kar je še posebej pomembno pri vzgoji bodočih učiteljev.

V naši raziskavi smo preverili poznavanje nevarnosti na spletu in odnos do digitalne varnosti pri študentih Pedagoške fakultete Univerze v Mariboru.

Digitalne kompetence

Pod pojem digitalnih kompetenc uvrščamo smiselno uporabo IKT v izobraževanju, družbenih odnosih in drugih področjih, vezanih na medosebne odnose (Ala Mutka, Punie in Redecker, 2008). Enostavneje lahko digitalne kompetence označimo kot sposobnost uporabljati različne vrste IKT-opreme. V izobraževanju digitalne kompetence razumemo predvsem kot nabor znanj in izkušenj, ki jih potrebujeta učitelj in učenec v procesu izobraževanja. Mednje štejemo znanja iz naprednega urejanja besedila, delo s preglednicami in grafi, obdelavo slike, videoposnetka in zvoka, tehnike predstavitev in uporabo spleta ter vse oblike elektronske komunikacije (Krašna, 2010). Med znanja in spretnosti pri uporabi spleta ter elektronske komunikacije pa brez dvoma sodi tudi digitalna varnost.

Digitalna varnost

Digitalno varnost predstavlja zavedanje o nevarnostih, njihovo poznavanje in posameznikovo samozaščitno delovanje med uporabo (Bratina in Krašna, 2011). V okvire digitalne varnosti sodijo med drugim tudi naslednji elementi:

- varovanje podatkov (datoteke, zbirke podatkov …),
- posredovanje in objavljanje osebnih podatkov,
- nepooblaščeno pridobivanje osebnih podatkov – spletno ribarjenje (angl. *phishing*), kraja identitete,
- brezbrižnost do nevarnosti,
- poznavanje nevarnosti pri uporabi IKT.

V izobraževanju učiteljev je velik poudarek namenjen uporabi IKT v izobraževanju. Učne vsebine obsegajo tudi elektronsko komunikacijo in uporabo spleta za podporo izobraževanju ali kot vir učnih vsebin. Večina študentov osnovna znanja in izkušnje elektronskega komuniciranja ter uporabe spleta pridobi že v prejšnjih izobraževanjih. Ker gre v primeru izobraževanja bodočih učiteljev za specifično populacijo, je njihove digitalne kompetence (posledično tudi znanja o digitalni varnosti) potrebno smiselno nadgraditi. Z vidika digitalne varnosti pa lahko predznanje študentov predstavlja določeno oviro. Realno je namreč pričakovati določen nivo izurjenosti v uporabi elektronske komunikacije in uporabe spletnih virov. Veliko bolj pa je vprašljiv nivo znanja in poznavanja vidikov digitalne varnosti.

Osebni podatki na družbenih omrežjih

Pri objavljanju občutljivih podatkov je zelo pomembno poznavanje in zavedanje o potencialnih nevarnostih. Še posebej so pri tem izpostavljena družbena omrežja, katerih širitev in masovna uporaba spodbujata lažen občutek varnosti, nove naprave pa omogočajo še lahkotnost (z enim klikom oddaljeno) objave občutljivih podatkov. Mednje sodijo tako osebni podatki kakor tudi podatki finančne narave ali celo kombinacije obojih. Nekateri znani incidenti začasno spremenijo odnos uporabnikov do varnosti na spletu, toda številni posamezniki hitro pozabijo in se premalo zavedajo, da je nevarnost stalno prisotna (Gabriel, 2010).

Prav aktivni in bodoči učitelji (študenti pedagoških smeri) imajo pomembno ter nenadomestljivo vlogo v razvoju digitalne varnosti, še posebej z vidika opozarjanja učencev in staršev na potencialne nevarnosti na spletu.

Varovanje datotek in podatkovnih zbirk

Varnostno kopiranje osebnih datotek uporabniki večinoma jemljejo premalo resno. Povprečen uporabnik se pomena varnostnih kopij zave šele ob nenadni odpovedi nosilca podatkov ali okvari računalnika, ko je reševanje izgubljenih podatkov težavno ali celo nemogoče. V nekaterih primerih tak pripetljaj lahko

povzroči celo resne ekonomske in tudi pravne posledice. Velik problem je nedvomno izguba učiteljevih podatkov. Učitelj si pri svojem delu ustvarja različne tipe podatkov – od zelo pomembnih, kot so šolske ocene, seznam opravljenih obveznosti, poročila o uspešnosti učencev, razredne statistike, do nekaterih manj pomembnih. Ne glede na vrsto je izguba podatkov vedno problematična. Tudi na univerzitetnem nivoju izobraževanja izguba podatkov o in pri študentih lahko privede do resnih zapletov. Zaradi izgube zapiskov predavanj ima študent npr. težave pri pripravi na izpit, izguba seminarskih ali izpitnih nalog, protokolov opravljenih vaj ipd. pa mu lahko celo onemogoči napredovanje.

Spletno ribarjenje (angl. phishing)

Spletno ribarjenje je zelo pogosta nevarnost pri uporabi spleta in učinkovito orodje za nepooblaščeno zbiranje osebnih podatkov. Na tak način se v glavnem zbirajo podatki finančne narave. Običajno v ta namen nepridipravi pripravijo lažne spletne strani, ki so na videz enake spletnim stranem znanih ponudnikov – banke ali druge finančne ustanove (npr. PayPal). Nepozoren ali zaveden uporabnik svoje podatke vpisuje v na videz pristne obrazce, podatki pa se nato posredujejo posameznikom, ki jih zlorabijo. Tovrstni napadi so najuspešnejši na družbenih omrežjih, kjer po podatkih kanadske organizacije za varnost Better Bussines Bureau (Phishing Attacks Continue to Pose Significant Risk, 2012) beležijo kar 70-odstotno uspešnost. Po podatkih delovne skupine za boj proti kraji identitete ameriškega predsednika (Combating Identity Theft a Strategic Plan, 2007) je eden izmed glavnih načinov pridobivanja osebnih podatkov v procesu kraje identitete prav spletno ribarjenje.

Kraja identitete

Kraja identitete je oblika goljufije, ko nekdo drug uporablja osebne podatke prizadetega posameznika. Pogosto se kraje identitete izvajajo za kasnejši dostop do osebnih in finančnih virov ali koristi kakršne koli druge vrste, vedno pa v imenu prizadetega posameznika (Identity Theft, 2011). Posledice so za prizadete pogosto zelo resne in težko popravljive. V nekaterih primerih lahko vrnitev v prvotno stanje traja zelo dolgo ali pa sploh ni več mogoče. Kraje identitete se zelo uspešno izvajajo na družbenih 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 celo osebni interesi, lahko privede do uspešne kraje identitete (Lewis, 2012). Predvsem iz osebnih podatkov in tudi prej navedenih podatkov lahko izkušen kriminalec zelo uspešno izvede krajo identitete.

Znanje in poznavanja nevarnosti na spletu

Najboljša zaščita pred mnogimi nevarnostmi pri uporabi sodobnih načinov komuniciranja je predvsem primerna raven znanja in poznavanja nevarnosti. Le uporabnik, ki dobro pozna različne oblike nevarnosti in vedno ravna samozaščitno, je dokaj dobro zaščiten pred številnimi grožnjami na spletu.

Namen

Z raziskavo smo želeli preveriti začetno stanje poznavanja digitalne varnosti ter morebitne spremembe pri generacijah. Na podlagi ugotovitev bo mogoče prilagoditi, spremeniti ali razširiti obstoječe učne vsebine, vezane na digitalno varnost pri uporabi IKT.

Skladno z namenom so nas zanimali naslednji vidiki digitalne varnosti:

- Katere osebne podatke študenti objavljajo na družbenih omrežjih in v kakšni obliki?
- Ali študenti skrbijo za varnost in stalno dostopnost do svojih podatkov?
- Kakšno je poznavanje zasnove spletnega ribarjenja kot vse bolj razširjene grožnje?
- Ali se študenti zavedajo nevarnosti in mehanizmov kraje identitete?
- Kako študenti ocenjujejo nivo lastnega znanja in poznavanja nevarnosti na spletu?

Metodologija

Za zbiranje podatkov smo izvedli spletno anketiranje z uporabo orodja za izdelavo spletnih anket (1ka, 2011). Zbiranje podatkov je potekalo z uporabo osebnih računalnikov anketiranih in spletne povezave ter je bilo anonimno.

Vzorec je obsegal 179 študentov dveh generacij na Pedagoški fakulteti Univerze v Mariboru.

Generacija (štud. leto)	f	f %
2010/11	70	49,1
2011/12	109	60,9

Preglednica 1: Struktura študentov v vzorcu

Podatke smo obdelali s programom SPSS, in sicer z metodami deskriptivne (f, f %) in inferenčne (χ^2-preizkus) statistike, katerih izidi so omogočili ugotavljanje stanja digitalnih varnostnih vidikov v posamezni generaciji in morebitne razlike v varnostnih vidikih med generacijama.

Rezultati

Osebni podatki na družbenih omrežjih

Študente smo prosili, da označijo, na kakšen način objavljajo različne vrste osebnih podatkov. Za posamezen podatek so anketirani označili, ali ga objavijo v pravi ali v lažni obliki. Na voljo je bilo 21 različnih vrst osebnih podatkov, pri čemer smo nekatere zaradi manjše razpršenosti kasneje združili v skupne kategorije. 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. Preglednici prikazujeta način objavljanja podatkov, ki jih študenti objavljajo na družbenih omrežjih, ter razlike med generacijama.

Katere podatke objavljate na družbenih omrežjih in v kakšni obliki?	**Pravo**	**Lažno**	**Koef.**
Ime in priimek (tudi samo ime ali samo priimek)	9,5 %	3,3 %	2,88
Rojstni podatki	9,1 %	0,7 %	13,00
Spol	10,2 %	0,0 %	∞
Podatki o izobrazbi	7,5 %	2,2 %	3,41
Podatki o bivanju	9,4 %	11,4 %	0,82
Elektronski naslov	8,2 %	2,8 %	2,93
Telefonska številka	1,7 %	9,9 %	0,17
Finančni in administrativni podatki	2,4 %	33,6 %	0,07
Družinski podatki	16,3 %	22,8 %	0,71
Spolna nagnjenja oz. usmeritev	5,5 %	3,3 %	1,67
Podatki o družabnem življenju	4,4 %	5,0 %	0,88
Svoje slike	8,9 %	1,7 %	5,24
Slike drugih oseb	6,9 %	3,3 %	2,09

Preglednica 2: Razmerja med deleži načinov objave osebnih podatkov na družbenih omrežjih

Koeficient predstavlja razmerje med objavo pravih in lažnih podatkov. Če koeficient znaša 1, pomeni, da so podatki v enaki meri objavljeni v pravi in lažni

obliki. Če je koeficient večji od 1, je več podatkov objavljenih v pravi kot v lažni obliki. Bližje kot je koeficient vrednosti 0, večji je delež lažne objave podatka.

Izidi so presenetljivi, saj kažejo na dokaj brezskrbno objavljanje občutljivih podatkov na družbenih omrežjih. Podatke o osebnem imenu in datumu rojstva študenti v večini primerov objavijo prave. Le majhen delež jih te podatke objavi kot lažne. Izpostaviti je potrebno, da študenti svoj spol objavljajo izključno v pravi obliki. Če podatke o imenu, starosti in spolu združimo, opazimo, da so ti podatki skoraj izključno objavljeni v pravi obliki. Tudi podatke o izobrazbi študenti objavljajo večinoma v pravi obliki, kar pa glede zaposlitvenih možnosti ni mogoče vedno šteti kot problematično.

Nekoliko višjo previdnost je opaziti pri podatkih o bivanju, čeprav je delež pravih objav še vedno dokaj visok. Elektronske naslove študenti pričakovano objavljajo v pravi obliki, saj sicer sodelovanje na družbenih omrežjih ni učinkovito. Želja po zaščiti zasebnosti se kaže pri omejevanju objave telefonske številke. Premalo pozornosti študenti namenjajo zaščiti družinskih podatkov, kar ni dobro. Delež objave teh podatkov v pravi obliki in delež objave osebnih podatkov v pravi obliki sta visoka. Omogočata namreč lažji dostop do teh podatkov, ki so najpogosteje zlorabljeni v okviru kraje identitete.

Varnosti finančnih podatkov študenti namenjajo veliko pozornost, saj jih v glavnem vsi objavijo le v lažni obliki. Tak izid je zadovoljiv in kaže, da se mladi zavedajo posledic zlorab tovrstnih podatkov. Objavljanje svojih slik in slik drugih oseb je na družbenih omrežjih postalo splošno sprejeto. 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 pri objavljanju slik drugih morali biti bolj odgovorni.

Katere podatke objavljate na družbenih omrežjih in v kakšni obliki?	**2010/11**		**2011/12**		**Trend**
	Pravo	Lažno	Pravo	Lažno	
Ime in priimek (tudi samo ime ali samo priimek)	9,5 %	3,0 %	9,4 %	2,1 %	-
Rojstni podatki	9,1 %	0,4 %	8,7 %	2,1 %	+
Spol	9,9 %	0,0 %	10,2 %	0,3 %	≈
Podatki o izobrazbi	8,2 %	1,3 %	8,6 %	2,1 %	+
Podatki o bivanju	8,5 %	11,6 %	9,7 %	11,3 %	≈
Elektronski naslov	8,0 %	2,6 %	8,3 %	2,6 %	≈
Telefonska številka	1,2 %	12,0 %	1,3 %	8,8 %	≈
Finančni in administrativni podatki	2,2 %	36,1 %	1,3 %	29,4 %	≈

Katere podatke objavljate na družbenih omrežjih in v kakšni obliki?	2010/11		2011/12		Trend
	Pravo	Lažno	Pravo	Lažno	
Družinski podatki	16,9 %	21,5 %	14,3 %	27,2 %	≈
Spolna nagnjenja oz. usmeritev	5,5 %	3,9 %	6,0 %	4,6 %	≈
Podatki o družabnem življenju	4,4 %	4,7 %	4,9 %	5,4 %	≈
Svoje slike	9,5 %	0,4 %	9,5 %	1,4 %	+
Slike drugih oseb	7,2 %	2,6 %	7,8 %	2,8 %	≈

Preglednica 3: Načini objave osebnih podatkov na družbenih omrežjih glede na generacijo in prikaz trenda

Razlik med generacijama študentov v načinu objavljanja podatkov nismo zasledili. Nekoliko več previdnosti pri mlajši generaciji zasledimo le pri objavi družinskih podatkov, kljub temu pa je trend nespremenjen. Pri objavi finančnih in administrativnih podatkov pa se utegne v prihodnosti pokazati, da bodo uporabniki bolj previdni in podatkov ne bodo objavljali niti v pravi niti v lažni obliki. Kljub nespremenjenemu trendu je pri mlajši generaciji opaziti določen upad pri obeh načinih objave.

Varnostne kopije datotek

Podatki o aktivnostih študenta, poročila o opravljenih obveznostih, ocene ipd. so pomembni za napredek študenta in morajo biti stalno razpoložljivi. To velja tako za učitelja kot tudi za študenta, ki mora svoje digitalne izdelke hraniti skozi celotno šolanje. Iz prakse poznamo številne primere, ko so se končni izdelki izgubili, tik preden bi morali biti oddani. Pri anketiranih študentih smo zato preverjali ozaveščenost o nujnosti varnostnega kopiranja pomembnih digitalnih izdelkov.

Ali delate varnostne kopije datotek?	f	f %
Varnostne kopije delam dnevno	8	4,5
Varnostne kopije delam tedensko	5	2,8
Varnostne kopije delam dvakrat na mesec	7	3,9
Varnostne kopije delam mesečno	14	7,8
Varnostne kopije delam nekajkrat letno	31	17,3
Varnostnih kopij ne delam	114	63,7
Skupaj	**179**	**100**

Preglednica 4: Izdelava varnostnih kopij

Skoraj dve tretjini študentov varnostnih kopij ne delata, kar kaže na zelo slabo skrb za zapise podatkov. Študenti se očitno ne zavedajo, kaj pomeni izguba podatkov. Tudi hranjenje podatkov v oblaku ni v celoti zanesljiva rešitev, saj v primeru izpada omrežja ali zaustavitve storitev dostop do podatkov ni mogoč. Če k skupini, ki ne dela varnostnih kopij, prištejemo še tiste, ki to počnejo le nekajkrat letno, je izid še slabši. Kar 81 % študentov ne skrbi za varnost zapisa podatkov.

Študijsko leto / Ali delate varnostne kopije datotek?	2010/11		2011/12	
	f	f %	f	f %
Varnostne kopije delam dnevno	2	2,9	6	5,5
Varnostne kopije delam tedensko	2	2,9	3	2,8
Varnostne kopije delam dvakrat na mesec	3	4,3	4	3,7
Varnostne kopije delam mesečno	6	8,6	8	7,3
Varnostne kopije delam nekajkrat letno	13	18,6	18	16,5
Varnostnih kopij ne delam	44	62,9	70	63,7
Skupaj	**70**	**100**	**109**	**100**

Preglednica 5: Izdelava varnostnih kopij glede na študijsko leto

Primerjava odgovorov dveh generacij študentov pokaže spodbudno rast deleža študentov mlajše generacije, ki varnostne kopije delajo vsak dan. Žal pa število tistih študentov, ki varnostnih kopij ne delajo, pri mlajši generaciji celo naraste. Razlika med generacijama v odločanju za varovanje zapisov podatkov ni statistično značilna ($\chi^2 = 0{,}951$; $P = 0{,}966$). Izid kaže, da se odnos do varovanja zapisov podatkov ne spreminja. Kar slabi dve tretjini (64 %) študentov obeh generacij ne delata varnostnih kopij. Skupaj s študenti, ki varnostne kopije delajo le enkrat letno, kar 80,5 % študentov obeh generacij ne skrbi za varnost zapisov podatkov.

Izidi so zaskrbljujoči in kažejo na slabo razumevanje pomena varovanja zapisov podatkov ter težav ob morebitni izgubi le-teh. Slaba polovica (46,2 %) študentov, ki varnostne kopije dela, le-te hrani na USB-ključkih, približno četrtina (23,1 %) pa na trdem disku drugega računalnika. Oba načina sta nezanesljiva in ne varujeta dovolj zanesljivo pred izgubo podatkov. Naprav za varnostno kopiranje ne uporablja nihče.

Spletno ribarjenje – razumevanje nevarnosti

Pomembna ovira pred uspešnim spletnim ribarjenjem je razumevanje mehanizma grožnje, saj bi že razumevanje principov številne uporabnike obvarovalo pred to nevarnostjo. Zato smo z vprašanjem, ki je obsegalo tudi definicije drugih nevarnosti, preverjali, ali anketirani razumejo mehanizem nevarnosti spletnega ribarjenja.

Kaj pomeni spletno ribarjenje?	**f**	**f %**
Iskanje informacij na spletu	29	16,2
Lažno predstavljanje na spletu	19	10,6
Kraja uporabniških imen in gesel s pomočjo lažne spletne strani	114	63,7
Nabiranje prijateljev na družbenih omrežjih	17	9,5
Skupaj	**179**	**100**

Preglednica 6: Razumevanje nevarnosti spletnega ribarjenja

Izidi kažejo, da sta skoraj dve tretjini (63,7 %) študentov seznanjeni z nevarnostjo spletnega ribarjenja in da razumejo način delovanja »napadalcev«. Kljub temu stanje ni spodbudno. Razlog je v dokaj velikem številu študentov, ki pojem spletno ribarjenje zamenjujejo z iskanjem informacij na spletu (16,2 %) in kot pridobivanje prijateljev na družbenih omrežjih. Delež študentov, ki napačno razumejo pomen in nevarnost spletnega ribarjenja, je več kot tretjinski (36,3 %).

Študijsko leto / Kaj pomeni spletno ribarjenje?	2010/11		2011/12	
	f	f %	f	f %
Iskanje informacij na spletu	13	18,6	16	14,7
Lažno predstavljanje na spletu	5	7,1	14	12,8
Kraja uporabniških imen in gesel s pomočjo lažne spletne strani	43	61,4	71	65,1
Nabiranje prijateljev na družbenih omrežjih	9	12,9	8	7,3
Skupaj	**70**	**100**	**109**	**100**

Preglednica 7: Razumevanje nevarnosti spletnega ribarjenja glede na generacijo

Primerjava razumevanja in poznavanja nevarnosti spletnega ribarjenja med generacijama študentov kaže na manjši porast razumevanja mlajše generacije. Razberemo tudi upad napačnega razumevanja v korist mlajše generacije. Razlika med generacijama v razumevanju in poznavanju nevarnosti spletnega ribarjenja ni statistično značilna ($\chi^2 = 3{,}162$; $P = 0{,}367$). Na podlagi izidov lahko sklenemo, da sta razumevanje in poznavanje nevarnosti spletnega ribarjenja pri obeh generacijah še vedno slabi. Več kot tretjina (38 %) študentov obeh generacij nevarnosti spletnega ribarjenja ne pozna ali ne razume. Izid je hkrati tudi koristen napotek za načrtovanje učnih vsebin s področja IKT v izobraževanju.

Kraja identitete – razumevanje nevarnosti

Razumevanje nevarnosti kraje identitete, ozaveščenost o njej in zavedanje o možnosti, da tudi sami lahko postanejo žrtev kraje identitete, uporabnike spodbudi k zaščiti. Ozaveščen in izobražen uporabnik poskrbi za varnost občutljivih podatkov in jih ne zaupa brez presoje. Zato smo želeli preveriti, ali anketirani študenti razumejo pomen pojma kraja identitete. Vprašanje je kot možne odgovore ponujalo možnosti, ki so sicer povezane s podatki o identiteti posameznika, vendar z njimi kraja identitete ni mogoča. Pravilen je bil le en odgovor.

Kaj pomeni kraja identitete?	**f**	**f %**
Kraja osebnih dokumentov	31	17,3
Zloraba osebnih podatkov	142	79,3
Objavljanje sporočil pod vzdevkom	4	2,2
Opravljanje izpita v imenu druge osebe	2	1,1
Skupaj	**179**	**100**

Preglednica 8: Razumevanje nevarnosti kraje identitete

Večina študentov (79,3 %) obeh generacij je seznanjena s pomenom in nevarnostjo kraje identitete. Stanje je zadovoljivo, čeprav obstaja slaba petina (17,3 %) študentov, ki pod nevarnostjo kraje identitete razume krajo osebnih dokumentov. Tak delež napačnega razumevanja nekoliko poslabša sicer zadovoljivo sliko, ker kaže na resno nerazumevanje mehanizma kraje identitete.

Študijsko leto / Kaj pomeni kraja identitete?	2010/11		2011/12	
	f	f %	f	f %
Kraja osebnih dokumentov	15	21,4	16	14,7
Zloraba osebnih podatkov	51	72,9	91	83,5
Objavljanje sporočil pod vzdevkom	3	4,3	1	0,9
Opravljanje izpita v imenu druge osebe	1	1,4	1	0,9
Skupaj	**70**	**100**	**109**	**100**

Preglednica 9: Razumevanje nevarnosti kraje identitete glede na generacijo

Med študenti obeh generacij ne obstaja statistično značilna razlika v razumevanju in poznavanju nevarnosti kraje identitete ($\chi^2 = 3{,}935$; $P = 0{,}269$). Študenti obeh generacij dobro razumejo nevarnost, saj njihov skupni delež znaša v povprečju 78 %. Kljub temu pa iz izidov razberemo, da v obeh generacijah obstaja približno petina študentov, ki pod nevarnostjo kraje identitete razume krajo osebnih dokumentov. Delež napačnega razumevanja je glede na resnost tovrstne grožnje dokaj velik in ga je v izobraževanju potrebno upoštevati.

Ocena lastnega znanja in poznavanja nevarnosti na spletu

Študente smo prosili za oceno lastnega poznavanja nevarnosti na spletu in posledično načina obnašanja na spletu.

Kako ocenjujete svoje poznavanje nevarnosti na spletu?	f	f %
Me ne zanima	0	0,0
Ne poznam	2	1,1
Slabo poznam	113	63,1
Dobro poznam	62	34,6
Vem skoraj vse	2	1,1
Skupaj	**179**	**100**

Preglednica 10: Ocena lastnega poznavanja nevarnosti na spletu

Izidi niso spodbudni, saj skoraj dve tretjini (63,1 %) študentov slabo poznata nevarnosti na spletu. Le dobra tretjina (34,6 %) pa poznavanje ocenjuje kot dobro. Zadovoljni smo lahko z ugotovitvijo, da študentov, ki jih nevarnosti na spletu ne zanimajo, ni.

Študijsko leto / Kako ocenjujete svoje poznavanje nevarnosti na spletu?	2010/11		2011/12	
	f	f %	f	f %
Me ne zanima	0	0,0	0	0,0
Ne poznam	0	0,0	2	1,8
Slabo poznam	41	58,6	72	66,1
Dobro poznam	27	38,6	35	32,1
Vem skoraj vse	2	2,9	0	0,0
Skupaj	**70**	**100**	**109**	**100**

Preglednica 11: Ocena lastnega poznavanja nevarnosti na spletu glede na generacijo

Med generacijama študentov izidi ne pokažejo statistično značilne razlike v oceni lastnega poznavanja nevarnosti. Obstaja pa tendenca ($\chi^2 = 6{,}629$; $P = 0{,}085$), da mlajša generacija ocenjuje svoje poznavanje nevarnosti nižje kot starejša. Verjeten razlog bi utegnil biti, da se utegnejo prihodnje generacije bolj zavedati obstoja nevarnosti in zato izražajo nekoliko višji nivo samokritičnosti. Posledično zato mlajša generacija svoje poznavanje nevarnosti na spletu ocenjuje nekoliko nižje. Vendar gre v tem primeru le za predvidevanje.

Gledano v celoti, je nivo poznavanja nevarnosti na spletu ne glede na generacijo prenizek. Takšen izid pomeni napotek za pripravo učnih vsebin s primernim poudarkom na spoznavanju obstoječih in prihodnjih nevarnosti. Hkrati naj tudi spodbujajo večjo kritičnost pri uporabi spleta in ravnanja z občutljivimi podatki.

Sklep

Kljub znanim primerom in obširni propagandi varne rabe spleta ugotavljamo dokaj visok nivo brezskrbnosti glede varovanja osebnih podatkov in podatkov sploh. Najmanj se nevarnosti zavedajo uporabniki družbenih omrežij. Skoraj tretjina uporabnikov podatke, kot so ime in priimek, rojstni podatki in spol, objavlja v pravi obliki, čeprav so kot taki podvrženi kraji identitete. Med podatki, ki jih uporabniki vse premalo premišljeno objavijo kot prave, so tudi družinski podatki. Odnos do finančnih podatkov je zadovoljiv. Višja stopnja brezbrižnosti pa se izkaže pri objavi fotografij drugih oseb, saj se uporabniki premalo zavedajo morebitnih posledic objave fotografij brez soglasja druge osebe. Študenti izkazujejo zelo veliko stopnjo brezbrižnosti do varovanja podatkov. Izidi kažejo, da odnos do nevarnosti izgube pomembnih podatkov ostaja nespremenjen ne glede na generacijo študentov. Razlog utegnemo najti v dejstvu, da se v preteklosti še niso srečali z izgubo pomembnih podatkov ali pa pretirano zaupajo v zanesljivost prenosnih pomnilnih medijev. Nevarnosti spletnega ribarjenja se vse generacije študentov v

veliki meri zavedajo. Kljub temu pa zasledimo tretjinski delež študentov, ki pojem spletno ribarjenje napačno razumejo. Ti študenti so posledično bolj izpostavljeni tej obliki nevarnosti. Takšen delež nepoznavanja posredno pritrjuje ugotovitvam o dokaj veliki uspešnosti spletnih kriminalcev pri uporabi metode spletnega ribarjenja. Kraja identitete je ena izmed najbolj resnih nevarnosti na spletu, ki se je študenti v skoraj 80 % zavedajo. Še vedno pa obstaja slaba petina študentov, ki krajo osebnih dokumentov zamenjuje s krajo identitete. Razlik med generacijami v pojmovanju nevarnosti kraje identitete ni. Zato je glede na resnost grožnje temu dejstvu potrebno v izobraževanju nameniti več pozornosti. Ocena lastnega znanja in poznavanja nevarnosti na spletu kaže dokaj nizko raven. Dve tretjini študentov izražata slabo znanje in poznavanje nevarnosti na spletu. Pozitivna je ugotovitev, da študentov, ki jih nevarnosti ne zanimajo, ni.

Izidi raziskave kažejo, da je učne vsebine s področja IKT potrebno stalno prilagajati in vključevati vsebine s področja varnosti na spletu. To je še posebej pomembno v procesu izobraževanja učiteljev, saj bodo kasneje učitelji tisti, ki bodo znanja prenašali na učence že v zgodnji fazi rabe spleta. S tem bodo neposredno tudi vzgajali generacije mladih, ki bodo poznali in razumeli nevarnosti na spletu, se nevarnosti zavedali in bili na njih pripravljeni ter se jim učinkovito uprli.

LITERATURA

1ka. (2011). (F. U. CMI, Producent & Faculty of Social Sciences). Pridobljeno 3. 1. 2011, s http://www.1ka.si/.

Ala Mutka, K., Punie, Y. in Redecker, C. (2008). *Digital Competence for Lifelong Learning*. Pridobljeno s http://ftp.jrc.es/EURdoc/JRC48708.TN.pdf.

Bratina, T. in Krašna, M. (2011). Students' attitude toward digital security. V L. Gómez Chova (ur.), *International Technology, Education and Development Conference* (str. 2831–2839). Valencia: International Association of Technology, Education and Development (IATED).

Combating Identity Theft A Strategic Plan. (2007). Washington: The President's Identity Theft Task Force.

Gabriel, K. (2010). *The Dangers of Internet Security Breaches on Social Networking Sites*. Pridobljeno 3. 1. 2011, s http://www.titaniumantivirus.org/in-the-cloud-security/the-dangers-of-internet-security-breaches-on-social-networking-sites/.

Identity Theft. (2011). Pridobljeno 4. 1. 2011, s http://en.wikipedia.org/wiki/Identity_theft.

Krašna, M. (2010). Digital competences and multimedia. V *Paper at the International Conference on New Horizons in Education, INTE 2010, June 23-25, 2010*. Famagusta, Turkish Republic of Northern Cyprus.

Kugler, L. (8. 2. 2012). *How to secure your Facebook profile in a post-Timeline world*. Pridobljeno 6. 7. 2012, s http://howto.techworld.com/personal-tech/3336013/how-secure-your-facebook-profile-in-post-timeline-world/.

Lewis, K. (2012). *How Social Media Networks Facilitate Identity Theft and Fraud*. Pridobljeno 6. 7. 2012, s http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx.

Phishing Attacks Continue to Pose Significant Risk. (12. 3. 2012). Pridobljeno 1. 7. 2012, s http://vi.bbb.org/.