Raba spletnih socialnih omrežij med otroki in nevarnosti

Lili Brečko

Namen prispevka:
Je ugotoviti dejansko rabo spletnih socialnih omrežij med otroki; predstaviti nevarnosti, ki pretijo nad otroki, ki nepravilno/neozaveščeno uporabljajo spletna socialna omrežja, ter pripraviti napotke in priporočila, kako vplivati na otroke, da bodo čim varneje uporabljali spletna socialna omrežja

Metode:
Priprava prispevka temelji na diskripciji znanih dejstev, opravljena sta pregled in analiza izbranih pisnih ter spletnih virov. V okviru diplomske naloge v juniju 2012 je bila izvedena anketa, preverja stanje glede uporabe spletnih socialnih omrežij med otroki starimi 9 in 10 let.

Ugotovitve:
V spletnih socialnih omrežjih je vsak dan več uporabnikov, med katerimi so tudi otroci. Dandanes ni nič nenavadnega, da otroci, stari 8 do 12 let, že uporabljajo spletna socialna omrežja in imajo svoj profil, čeprav predpisi določenih spletnih socialnih omrežij predpisujejo starost vsaj 13 let. Facebook, Twitter in Google+ so samo nekatera aktualna spletna socialna omrežja pri katerih lahko neozaveščeni otroci naletijo na nevarnosti, kot so kraja identitete, pošiljanje neprimernih vsebin (pornografija), zloraba osebnih podatkov, spletno nadlegovanje, kibernetsko zasledovanje,…

Omejitve/uporabnost raziskave:
Pomanjkanje ustrezne in celovite literature in teoretične prakse, ki omejuje pripraviti dobro priporočila za varno rabo spletnih socialnih omrežij med otroki.

Praktična uporabnost:
Prispevek prinaša predloge za starše in učitelje kako čim bolje ozavestiti in poučiti otroke o varni rabi spletnih socialnih omrežij in spleta.

Izvirnost/pomembnost prispevka:
Prispevek bo najbolj uporaben za starše in učitelje predvsem v smislu kako čim bolje ozavestiti in poučiti otroke o varni rabi spleta in spletnih socialnih omrežij, ter se seznaniti s kakšnimi nevarnostmi se lahko srečajo otroci, ki o tem niso ozaveščeni.

Ključne besede: Spletno socialno omrežje, otroci, dostopnost, varnost, nadzor, spletno prijateljstvo

1 Uvod

Razvoj informacijsko komunikacijskih tehnologij se odvija z eksponentno hitrostjo in danes si zelo težko predstavljamo, da je bila prva spletna stran postavljena le dve desetletji nazaj (Dimc in Dobovšek, 2012).

V spletnih socialnih omrežjih je iz dneva v dan več uporabnikov, med katerimi so tudi otroci. Danes ni nič nenavadnega, da otroci nižjih razredov, stari od 8 do 12 let, že uporabljajo spletna socialna omrežja in imajo svoj profil, čeprav predpisi na določenih spletnih socialnih omrežjih (Facebook, Google+) predpisujejo starost vsaj 13 let, česar pa nihče ne preverja. Težava se pojavi, ker otroci nimajo ustreznega znanja, kako primerno zaščititi svoj profil, katere podatke in slike objaviti, in na splošno, kako komunicirati na spletnem socialnem omrežju. Težava je, da otroci tekmujejo, kdo ima več virtualnih prijateljev, s tem pa je povezano potrjevanje oseb, ki jih ne poznajo, za posameznim profilom pa se lahko skriva kdorkoli.

To, da si otroci ne bi ustvarjali profilov na spletnem socialnem omrežju, je težko preprečiti. Če starši otroku to prepovedo na domačem računalniku, bo našel možnost pri sosedu, prijatelju, v šolski knjižnici ali preko svojega mobilnega telefona. Preprečevanje uporabe spletnih socialnih omrežij lahko nadomestimo s svetovanjem in izobraževanjem, da bodo otroci to počeli relativno varno.

Poseg v zasebnost, ustvarjanje napačnega mnenja o posamezniku, uporaba osebnih podatkov, pedofilija, posilstva, zlorabe in zasledovanje je samo nekaj nevarnosti, na katere lahko naletijo slabo ozaveščeni otroci na spletnih socialnih omrežjih.

2 Nevarnost spletnih socialnih omrežij

Dimc in Dobovšek (2012:21) menita, da je kibernetski prostor mednarodno okolje v pravem pomenu besede, kjer ni običajnih fizičnih omejitev, kot je razdalja, in tudi ne fizičnih ovir, kot so carinske kontrole in mejni prehodi. Storilec ni lokacijsko omejen pri izbiri svoje žrtve niti pri izbiri obsega kaznivega dejanja. S tem je olajšana tudi možnost pobega storilca, saj ne gre za klasičen pobeg z mesta kaznivega dejanja, temveč samo za zabrisanje digitalnih sledil.

V pozni moderni dobi je svet postal odvisen od dostopa in izmenjavanja informacij preko interneta, v zadnjih letih pa so se temu pridružile tudi druge oblike komuniciranja, ki združujejo in povezujejo prebivalstvo v globalnem kibernetskem prostoru. Z novimi možnostmi povezovanja pa so se pojavile tudi nove oblike groženj, ki vplivajo na varnost in zasebnost uporabnikov kibernetskega prostora. Najaktualnejše so predvsem grožnje, povezane s spletnimi socialnimi omrežji (Bernik in Prislan, 2012).

Spletna socialna omrežja so zelo priljubljena, saj so nam v veliko pomoč pri ohranjanju družinskih, osebnih in poslovnih stikov, zato podatek, da spletna socialna omrežja uporablja že skoraj 800 milijonov uporabnikov, ni presenetljiv. Da so spletna socialna omrežja uporabna le za ohranjanje stikov, velja le v primeru, da jih uporabniki uporabljajo zgolj za ta namen. V primeru raztresanja osebnih in zasebnih podatkov lahko ti hitro zaidejo v napačne roke in so lahko zelo uporabni za spletne kriminalce. Ti na njih dobijo dovolj uporabnih informacij za organiziranje in izvedbo različnih kriminalnih dejanj.

2.1 Kraja identitete

Definicija identitete vsebuje značilnosti človeka kot biološka vrsta, individualna osebnost, družbeno bitje in član kulture (portal za izobraževanje iz zdravstvene nege, 2008). Kraja identitete je v Sloveniji opredeljena kot kaznivo dejanje zlorabe osebnih podatkov, pri katerih storilec pridobi določene ključne osebne podatke.

Neznana oseba lahko pridobi naše podatke in se predstavlja v našem imenu. Posledica tega je lahko, da okrni naš ugled pred družino, prijatelji, znanci in celo delodajalci ter pridobi dostop do naših osebnih podatkov, informacij, slik, videoposnetkov in denarja. Oseba najlaže prevzame identiteto takrat, ko smo nepazljivi, ko po nesreči ali z namenom razkrijemo geslo za elektronsko pošto. Drugi način je phishing oziroma kraja podatkov, ko nas elektronsko sporočilo pripravi, da razkrijemo svoje uporabniške podatke. (Varni na internetu, 2010).

Največji del kaznivih dejanj tatvine identitete temelji na tehnikah socialnega inženiringa, pri čemer storilec za stik z žrtvijo potrebuje elektronski naslov, kar je izredno lahko ponarediti tako, da bo videti, kot da prihaja od prijatelja, znanca ali sorodnika (Moj mikro, 2007).

2.2 Neprimerne vsebine

Zelo pogosto preganjano kaznivo dejanje kibernetske kriminalitete je prikazovanje, izdelava, posest in posedovanje pornografskega gradiva po 176. členu Kazenskega zakonika, v katerem lahko vidimo, da je protipravno ravnanje tisto ravnanje, pri katerem se otroku (osebi, mlajši od 15 let) proda, prikaže ali kako drugače omogoči dostop do pornografskih vsebin. K novemu zakonskemu členu je bil dodan tretji odstavek, ki opredeljuje, da je kazniva tudi posest pornografskega gradiva, kar predstavlja novost, saj po prej veljavni zakonodaji ni bila kazniva, kaznivo je bilo le posredovanje (Bernik in Prislan, 2012).

Kaznivo dejanje so tudi izdelava, razširjanje, posedovanje, posredovanje otroške pornografije in omogočanje dostopnosti do otroške pornografije. Z ustavo Republike Slovenije in kazenskim zakonikom je prepovedan tudi sovražni govor, ki zajema govorno, pisno in nebesedno komunikacijo (parada, trakovi, simboli), katerega glavni cilj je razčlovečiti tiste, proti katerim je usmerjen, njegov namen pa je ponižati, prestrašiti in spodbuditi nasilje (Spletno oko, 2008).

Pojav interneta je omogočil lažje širjenje nasilnih in sovražnih vsebin, rasizma in nacionalizma, ki prav tako sodijo med neprimerne vsebine.

2.3 Zloraba osebnih podatkov

Zloraba osebnih podatkov je kaznivo dejanje kibernetske kriminalitete po 143. členu Kazenskega zakonika, kjer je opredeljeno kot: »Kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se osebni podatki nanašajo, in kdor vdre v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.« (Kazenski zakonik, 2004).

2.4 Spletno nadlegovanje

Spletno nadlegovanje ali drugače Cyber Bullying je uporaba informacijskih in telekomunikacijskih tehnologij za premišljeno, ponavljajoče se in sovražno vedenje posameznikov ali skupin z namenom škodovati drugim. Danes je večina mobilnih telefonov opremljenih s kamerami in snemalna tehnika olajša delo tistim posameznikom, ki nadlegujejo druge osebe. Skrb vzbuja nadlegovanje otrok s strani sovrstnikov, ki so za svoja leta morda nekoliko zrelejši in že obvladajo uporabo spleta v pozitivne in v negativne namene. Žrtev za norčevanje običajno ne ve, če ve, kaj dosti sama ne more storiti. Posledice nadlegovanja so

lahko hude in dolgotrajne, saj gre za psihično nadlegovanje, ki je nemalokrat hujše od fizičnega. Večina spletnega nadlegovanja poteka znotraj spletnih socialnih omrežij (Moj mikro, 2010).

Informacijski pooblaščenec (2009) vključuje v primere metod spletnega nadlegovanja: ustvarjanje lažnih profilov, ustvarjanje sovražnih spletnih strani, sovražni govor in žaljivke, zasledovanje uporabnikov na spletu, krajo identitete, objavljanje posnetkov, zlorabe osebnih podatkov in objavljanje posnetkov, posnetih z mobilnimi telefoni na spletu.

2.5 Kibernetsko zalezovanje

Umek in Čarman (2008) definirata izraz »zalezovanje« ali »stalking« kot neželene vdore, vmešavanje ene osebe v življenje druge. Za zalezovanje je značilno, da so vdori ali nadlegovanja in da v žrtvi vzbujajo strah.

Shinder in Tittel (2002) menita, da je kibernetsko zalezovanje oblika elektronskega nadlegovanja, pri kateri storilec nadleguje, zasleduje ali grozi žrtvi.

Kibernetsko zalezovanje je vedno večji problem, saj ljudje na spletu izdajajo preveč osebnih podatkov, kar kibernetski zalezovalci izkoristijo. Na spletnih socialnih omrežjih zalezovalci žrtvi pošiljajo sporočila, jo vsakodnevno spremljajo. Sprva nedolžno spletno zalezovanje se lahko prenese v realno življenje, v katerem je ogroženo resnično življenje žrtve (ugrabitev, posilstvo, pedofilija ali umor). Zalezovalci lahko z žrtvami komunicirajo tudi v obliki klicanja na telefon, pošiljanje pošte in daril, pošiljanje sporočil preko faksa.

2.6 Seksting

Seksting (ang. Sexting) je nova beseda, ki označuje pošiljanje svojih golih fotografij preko mobilnega telefona ali interneta svojim vrstnikom. To početje je najbolj značilno za najstnike, stare 13 do 19 let, zanemarljivo pa ni tudi pri mlajših od 13 let. Razlogi sekstinga so lahko različni. Nekaterim mladim se zdi to zabavno in ne vidijo možnih negativnih posledic takega vedenja. Za nekatere najstnike je to način iskanja pozornosti, potrditve in stika z nasprotnim spolom. Nekateri se počutijo prisiljene, če tega ne bodo storili, saj se bojijo, da bodo izgubili priljubljenost ali možnost za zvezo s simpatijo. Do sekstinga pogosto pripelje tudi izsiljevanje in pritisk vrstnikov. Nezaželenih posledic sekstinga ni malo, saj se lahko gole slike razširijo širše, kot je bilo sprva mišljeno. Na primer: Slike, ki so bile namenjene simpatiji, a jih ta po prekinitvi zveze pošlje prijateljem, sošolcem. Posledice so lahko težave v šoli, nadlegovanje vrstnikov, za slike pa lahko izvedo starši in učitelji. Posledice sekstinga lahko segajo tudi daleč v našo prihodnost, saj nikoli ne moremo vedeti, kam vse so se slike razširile in kdaj kasneje v življenju bodo spet priplavale na površje in nam grenile življenje. Širjenje golih fotografij mladoletne osebe pa se šteje tudi kot kaznivo dejanje širjenja otroške pornografije (safe.si, 2011).

2.7 Varnost in nadzor spletnih socialnih omrežij

Tisti, ki so danes naši prijatelji, bodo lahko že jutri postali naši sovražniki. Za profilom in sliko našega domnevnega prijatelja se lahko skriva nekdo drug. Naš »prijatelj« lahko naše podatke posreduje tretji osebi brez naše vednosti, in podobno. Možnosti, da nam nekdo zlorabi zasebne podatke na spletnih socialnih omrežjih, je veliko. Vendar kot povsod v življenju tudi na

internetu oziroma pri uporabi spletnih socialnih omrežjih ni 100 % varnosti, vendar pa lahko največ za varno uporabo in lastno varnost na spletnih socialnih omrežjih poskrbimo sami.

Pri prvi prijavi na spletno socialno omrežje se je dobro pozanimati o vidnosti objavljenih vsebin in podatkov ter se odločiti, ali bo profil javen ali dostopen samo prijateljem (Isakovič, 2009). Pred zlorabo osebnih podatkov se lahko zavarujemo tako, da omejimo količino objavljenih informacij in osebnih podatkov na profilu. Treba se je zavedati, da je internet javni vir podatkov, ki je dostopen vsakomur. Ko je podatek objavljen na spletu, se ga ne da več preklicati oziroma izbrisati. Četudi podatek zbrišemo s spletne strani, je lahko že začasno ali trajno shranjen na računalniku nekoga drugega in ga je mogoče zlorabiti.

Zato je treba omejiti količino objavljenih osebnih podatkov, pri katerem v profilu in tudi nikjer drugje ne objavljamo svojih osebnih podatkov, kot so številke bančnih kartic, bančnega računa, davčne številke, EMŠO, naslov bivališča, številko mobilnega telefona, ki bi jih nekdo lahko zlorabil za tatvino identitete in v našem imenu sklepal pravno veljavne posle, na primer bančni kredit. Z objavo takšnih podatkov postanemo ranljivi in nezaščiteni. Veliko pozornost na spletnih socialnih omrežjih je treba nameniti neznancem, saj splet omogoča ljudem, da se predstavljajo z lažnimi imeni, željami, lastnostmi, ki jim ne gre slepo zaupati. Priporočeno je, da ne komuniciramo z vsakomer, ki želi komunicirati z nami. Vedno je dobro preveriti njihovo dejansko identiteto. V nobenem primeru pa ni priporočljivo neznancem posredovati svojih osebnih podatkov in sprejemati ponudbe za srečanje v živo brez spremstva (Zveza potrošnikov Slovenije, 2009).

Za zaščito v spletnih socialnih omrežjih je dobro uporabljati kompleksna, močna in različna gesla, saj v primeru kraje enega gesla tako ne bodo ogroženi tudi drugi podatki.

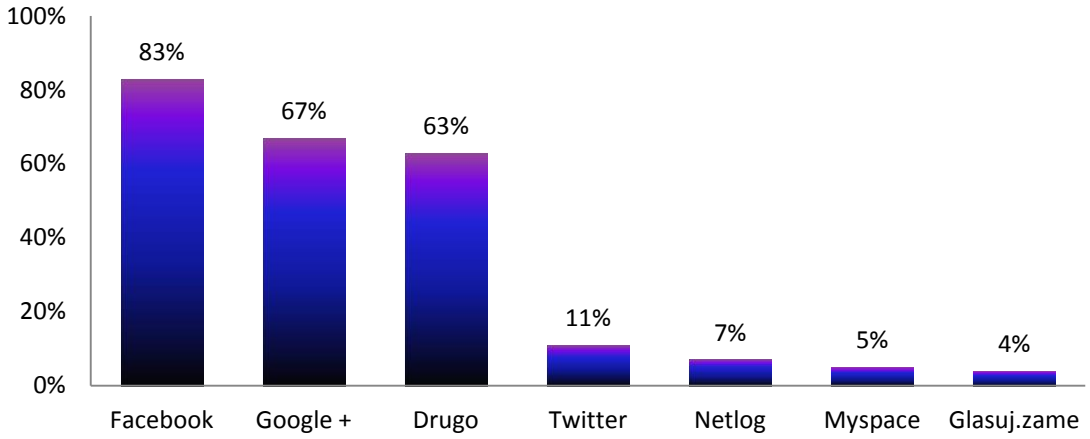
Konkurenca nam danes omogoča, da dobimo požarne zide, antivirusne programe in programe za filtriranje neprimerne vsebine za dostopno ceno. Možne so tudi brezplačne aplikacija za varno rabo interneta. S programi za zaščito, osveščanjem, vključevanjem starejših in mlajših v različne delavnice varne rabe interneta, osveščanjem starejših bi način varne rabe prenesli tudi na svoje otroke, in predvsem bi morali spremeniti mnenje večine ljudi, »da smo varni na internetu«, in s tem omejili bazo podatkov, ki jo ljudje prostovoljno objavljajo na spletnih socialnih omrežjih. Že na takšen način bi močno otežili delo storilec, ki samo čakajo na trenutek našega »nespametnega vedenja«.

3 Ugotavljanje stanja rabe spletnih socialnih omrežij med otroki

V nadaljevanju bomo predstavili raziskovalno delo, ki smo ga opravili v okviru izdelave diplomske naloge, kjer smo preverjali rabo spletnih socialnih omrežij med otroki. Ciljna populacija so bili otroci, stari devet in deset let, kar pomeni, da so v raziskavi sodelovali učenci 4 in 5 razredov osnovne šole. V anketi je sodelovalo 150 učencev dveh osnovnih šol v mesecu juniju 2012. Zaradi nepravilno izpolnjenih anket smo jih 29 izključili. V raziskavo so bile vključene samo ankete, katerih anketiranci uporabljajo spletna socialna omrežja. Ker 21 otrok ne uporablja spletnih socialnih omrežij, smo za analizo podatkov obdelali odgovore 100 učencev. Med 121 pravilno izpolnjenimi anketami smo ugotovili, da spletna socialna omrežja uporablja 82,6 % anketiranih otrok. Od tega je bilo nekoliko več ženskih uporabnic (51 %) kot moških (49 %).

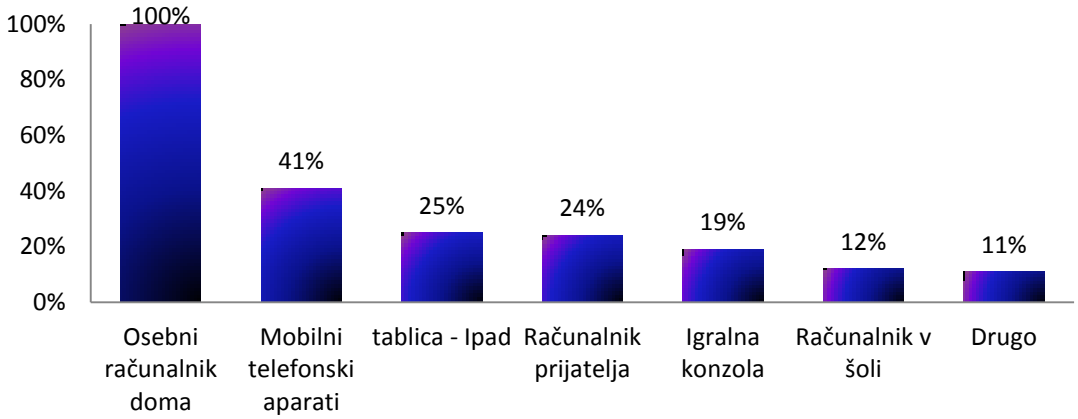
3.1 Najpogostejša uporaba spletnih socialnih omrežij

Na prvem mestu se je znašel Facebook s 83 %, drugo najpogostejše spletno socialno omrežje je bilo Google+ (67 %). Otroci za ostala spletna socialna omrežja, kot so Twitter (11 %), Netlog (7 %), Myspace (5 %) in Glasuj.zame (4 %) ne kažejo veliko zanimanja, saj je njihova raba v primerjavi s Facebookom in Google+ zelo majhna. Pri tem vprašanju so uporabniki spletnih socialnih omrežij imeli možnosti tudi odgovor »drugo«, za katerega se je odločilo 63 % anketirancev.



Graf 1: Uporaba spletnih socialnih omrežij

3.2 Naprave za dostop do spletnih socialnih omrežij

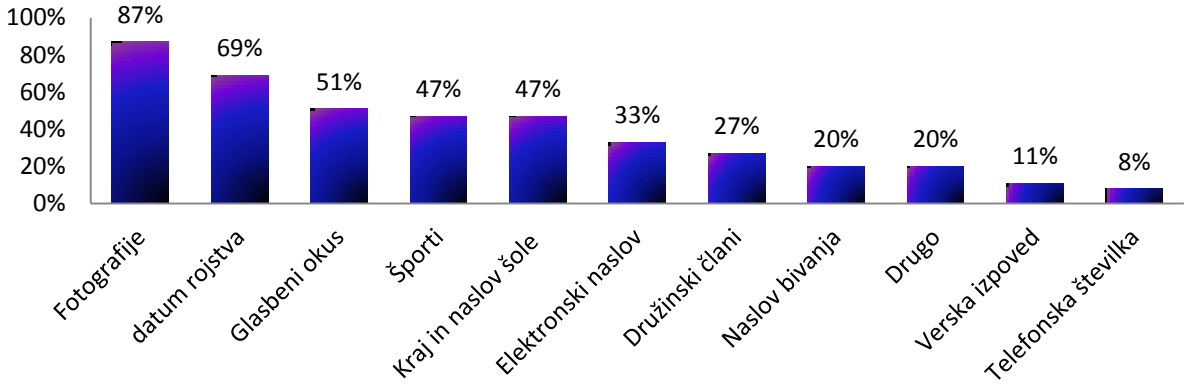


Graf 2: Dostop do spletnih socialnih omrežij

Za dostop do spletnih socialnih omrežij otroci uporabljajo različne možnosti. Največ, kar 100 % otrok, za dostop do spletnih socialnih omrežij uporablja osebni računalnik doma. Kot drugo najpogostejšo možnost za dostop otroci uporabijo mobilni telefonski aparat (41 %). Otroci za dostop uporabljajo tudi tablični računalnik-ipad (25 %), nekoliko manj (24 %) pa za dostop na spletna socialna omrežja uporabijo tudi računalnik prijatelja. Za dostop do spletnih socialnih

omrežij pa otroci uporabljajo še igralno konzolo (19 %), računalnik v šoli (12 %) in drugo (11 %), za kar so navajali računalnik v mestni knjižnici, pri sosedu in preko televizije. Na vprašanje je bilo več možnih odgovorov, zato skupek presega 100 %.

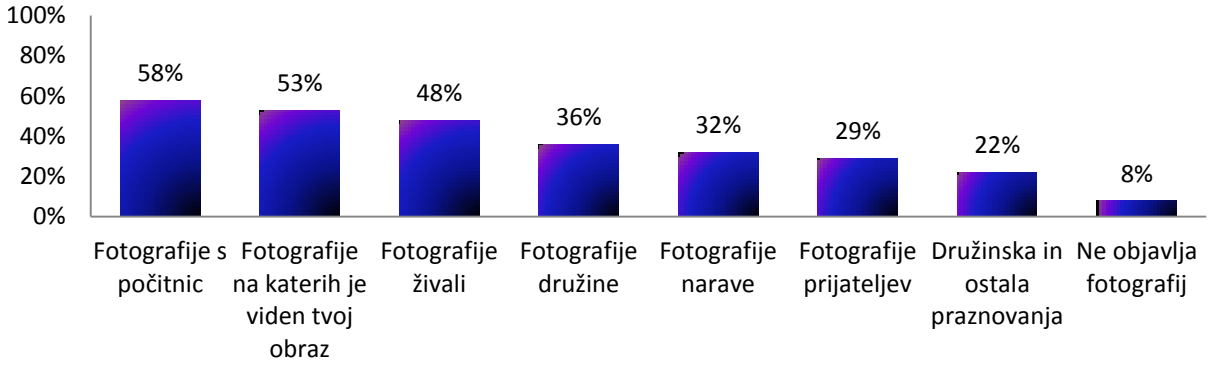
3.3 Objava podatkov na spletnih socialnih omrežjih



Graf 3: Objava podatkov na profilu

Naslednje vprašanje se je nanašalo na informacije, ki jih uporabniki delijo na spletnih socialnih omrežjih. Graf nam prikazuje, da kar 87 % anketirancev na profilu objavlja fotografije, 69 % jih objavlja datum rojstva, 51 % glasbeni okus, 47 % anketirancev objavi, katero šolo obiskuje, prav tako pa 47 % anketirancev objavi podatke o svojem priljubljenem športu. Tretjina anketirancev, kar je 33 % na spletnem socialnem omrežju, objavi elektronski naslov. 27 % anketirancev objavlja podatke o družinskih članih, 20 % naslov bivanja, 11 % versko prepričanje in 8 % anketirancev na spletnem socialnem omrežju zaupa tudi svojo telefonsko številko. Anketiranci so imeli možnost odločitve za drugo, kar jih je obkrožilo 20 %.

3.4 Objava fotografij na spletnih socialnih omrežjih

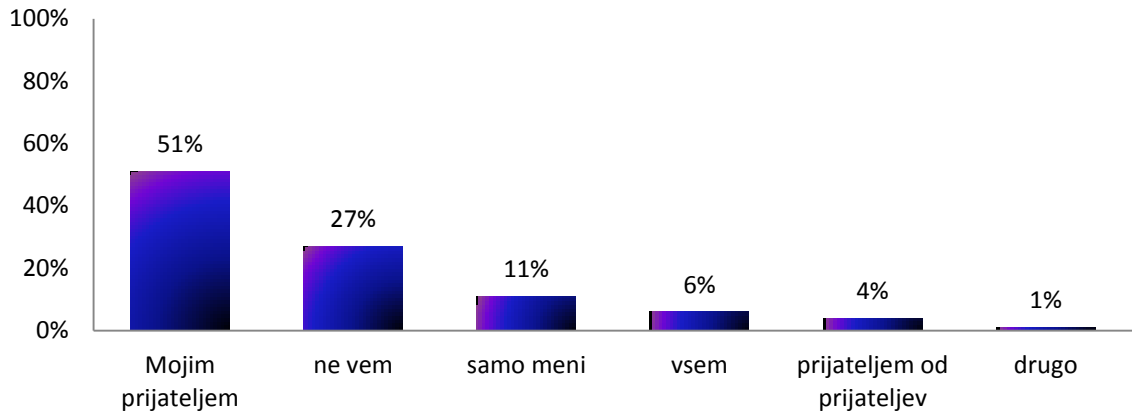


Graf 4:Objava fotografij

V okviru objave podatkov in fotografij nas je tudi zanimalo, katere fotografije otroci najpogosteje objavljajo na svojem profilu. Iz grafa je razvidno, da 58 % otrok objavlja fotografije s počitnic, dobra polovica (53 %) objavlja fotografije, na katerih je otrok viden, slaba polovica otrok (48 %) pa objavlja fotografije živali. Otroci objavljajo tudi fotografije narave (32 %), fotografije prijateljev (29 %), fotografije družinskih in ostalih praznovanj (22 %). 8 % otrok

na spletnem socialnem omrežju ne objavlja fotografij. Na vprašanje je bilo možnih več odgovorov, zato skupni seštevek presega 100 %.

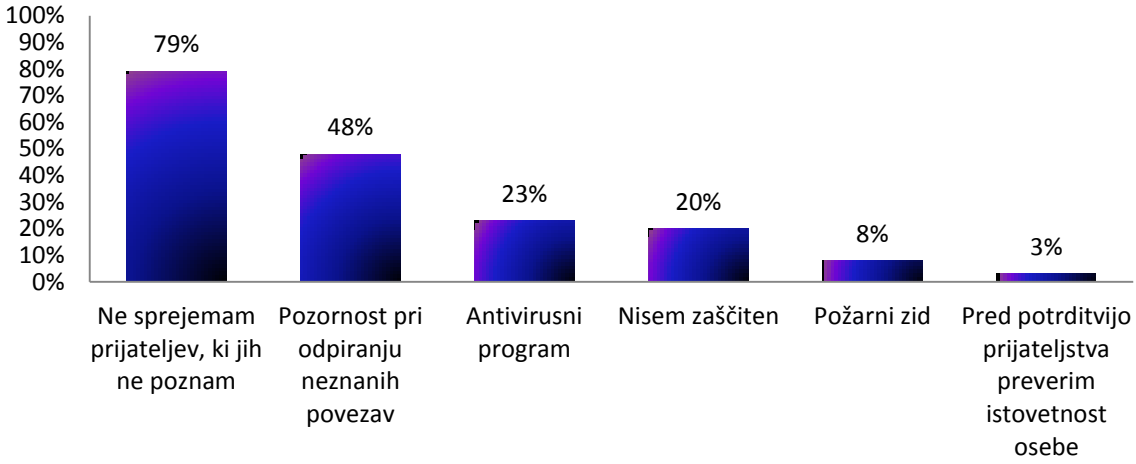
3.5 Vidnost podatkov



Graf 5: Vidnost podatkov

Pri dobri polovici anketirancev (51 %) lahko podatke, ki jih objavijo na svojem profilu, vidijo samo njegovi prijatelji. Na drugem mestu (27 %) je odgovor, da otroci ne vedo, kako imajo nastavljen profil in komu so vidni njihovi podatki. 11 % anketirancev ima nastavitve zasebnosti nastavljene tako, da so podatki na njihovem profilu vidni samo njim. Prijatelji prijateljev lahko vidijo podatke 4 % anketirancev.

3.6 Zaščita pri uporabi spletnih socialnih omrežij

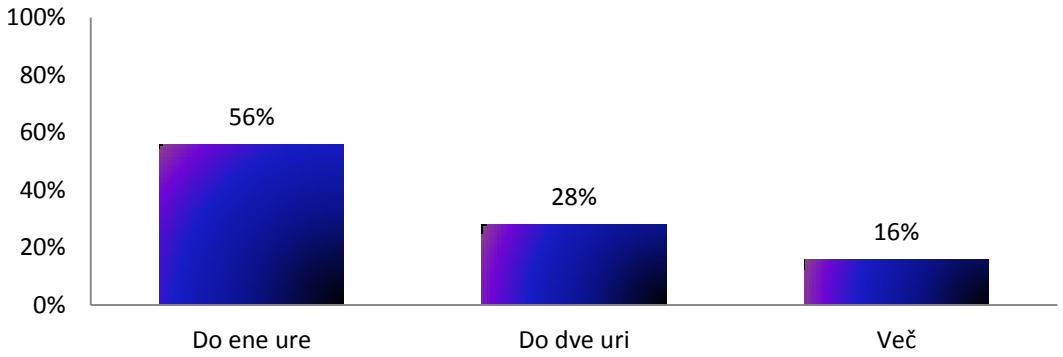


Graf 6: Zaščita pri uporabi spletnih socialnih omrežij

Z vprašanjem »Kako se zaščitiš pri uporabi spletnih socialnih omrežij«, smo želeli izvedeti, kako otroci, stari devet in deset let, skrbijo za varno rabo na spletnih socialnih omrežjih. Večina (79 %) otrok ne sprejema »prijateljev«, ki jih ne pozna. Slaba polovica (48 %) anketirancev nameni posebno pozornost pri odpiranju neznane elektronske pošte, neznanih povezav ter neznanih

spletnih strani. 23 % anketirancev za varno rabo spletnih socialnih omrežij uporablja protivirusni program. Samo 8 % otrok za varnost uporablja požarni zid in samo 3 % otrok pred sprejemom prijatelja preveri istovetnost osebe. Kar 20 % anketiranih otrok ne uporablja ničesar za zaščito na spletnih socialnih omrežjih. Možnih je bilo več odgovorov, zato skupni seštevek presega 100 %.

3.7 Namen časa za uporabo spletnih socialnih omrežij



Graf 7**:** Namen časa za uporabo spletnih socialnih omrežij

Za zadnje vprašanje me je zanimalo, koliko časa na dan otroci uporabljajo katerokoli od obstoječih spletnih socialnih omrežij. Več kot polovica (56 %) uporablja spletna socialna omrežja do ene ure na dan. Za tem sledijo uporabniki, ki namenijo dve uri časa dnevno (28 %), in uporabniki, ki namenijo več kot dve uri dnevnega časa za spletna socialna omrežja (16 %).

4 Zaključna razprava in varna raba spletnih socialnih omrežij

V spletnih socialnih omrežjih je potrebna previdnost pri objavi podatkov in informacij o sebi. Če je profil javen, ga lahko vidi in deli naprej vsak uporabnik interneta, tudi učitelji, profesorji, delodajalci, prijatelji ali popolni neznanci. Pri izbiri ponudnika spletne strani za mreženje se je treba pozanimati, kako skrbijo za zasebnost in varnost svojih uporabnikov. Dobro je prebrati pravila uporabe in njihovo politiko varovanja zasebnosti. V drobnem tisku se pogosto »skrivajo« pomembne informacije, komu bodo posredovali podatke, komu bodo na voljo v vpogled in ali jih je mogoče trajno izbrisati (Safe.si, 2010). Zato je pred registracijo v spletno socialno omrežje treba pozorno prebrati navodila in drobni tisk ter se popolnoma seznaniti s podrobnostmi spletnih socialnih omrežij, ki jih bodo uporabljali ali jih uporabljajo otroci.

Kot v resničnem življenju otrok imajo starši prav tako ključno vlogo tudi pri tem, da si otroci oblikujejo pozitivno predstavo, vzdržujejo dobre odnose in dober sloves v spletnih socialnih omrežjih.

Pojavi se večno vprašanje staršev, kako svojemu otroku zagotoviti varno deskanje po spletu. V digitalni dobi prepoved in popoln nadzor nista možna, saj lahko otroci do spleta dostopajo skoraj povsod (Košir, 2011). V nadaljevanju je navedenih nekaj varnostnih nasvetov za starše in učitelje, ki so prav tako pomemben člen življenja otrok.

Na spletni strani Safe.si (2011) je navedenih nekaj nasvetov za varno mreženje na spletnih socialnih omrežjih:

- Zaščita računalnika s požarnim zidom in protivirusnim programom, ki ga je treba redno posodabljati. V primeru neznanja se poišče strokovna pomoč.
- Postavitev računalnika v dnevni prostor ter raziskovanje interneta skupaj z otroki. Pustiti otrokom, da tudi oni starše poučijo o novi tehnologiji.
- Prepoved interneta ni način reševanja težav. Z otroki se je treba pogovoriti o tem, kaj počnejo na spletu. Vohunjenje z raznimi programi ni najboljša rešitev in je poseg v otrokovo zasebnost. Otroci naj zaupajo svojim občutkom – če jim je zaradi česar koli na spletu neprijetno, naj staršem to povedo.
- Pomoč otroku razumeti, kateri podatki so osebni. Otroci na spletu naj ne objavljajo naslova bivanja, telefonske številke, naslova šole, naslova elektronske pošte in drugih pomembnih osebnih informacij. Priporočljivo je uporabljati vzdevek, ki ne razkriva popolnega imena in njihove identitete.
- Pogovor z otroki, naj na spletnih socialnih omrežjih objavljajo samo fotografije, informacije, komentarje in videoposnetke, za katere jim je vseeno, če jih vidijo tudi drugi. Poučiti jih moramo, da slike divjih zabav in žaljivi ter zbadljivi komentarji ne sodijo na splet, saj so tam na voljo vsem uporabnikom, in ko se enkrat objavijo, tam ostanejo za vedno.
- Priporočilo otrokom, naj uporabljajo nastavitve zasebnosti, s čimer omejijo, kdo vse lahko vidi njihov profil v družabnem omrežju. Prav tako je treba otroke poučiti o tem, kako se spreminjajo nastavitve. Predvsem si je treba vzeti čas in skupaj z otrokom občasno pregledati osebni profil, ter mu svetovati in pomagati zaščititi profil.
- Prav tako je pomembno otroke naučiti, da bodo spoštovali zasebnost drugih. Še posebej naj bodo previdni pri objavljanju osebnih podatkov drugih oseb in prijateljev brez njihovega dovoljenja, kamor sodijo tudi fotografije. Treba se je zavedati, da je takšno početje tudi kaznivo dejanje.
- Otroke je treba poučiti, da je nadlegovanje preko interneta in drugih tehnologij nedopustno. Z njimi se moramo pogovoriti o pravilih lepega obnašanja na spletu in o tem, kar je prav in kaj ne, ter da se to nikakor ne razlikuje od resničnega življenja. Otrokom je treba dopovedati, da imajo natipkane besede in fotografije veliko težo ter da lahko v resničnem življenju pustijo veliko posledic: Prizadenejo osebo, ki jih prejme, in naredijo slab vtis na tistega, ki jih pošilja. Starši lahko neprimerne vsebine, kontakte oziroma nadlegovanja prijavijo na sami spletni strani spletnega socialnega omrežja, kjer obstajajo mehanizmi za prijavo zlorab.
- Otrokom je treba prepovedati in jih opozoriti na posledice sestajanja s »prijatelji« z interneta. Moramo jim je pojasniti, da internetni prijatelji morda niso to, za kar se izdajajo.
- Gesla so skrivnost, zato naj jih otroci ohranijo zase in jih pogosto menjujejo. Otroci gesla za dostop do spletnih omrežij, elektronske pošte in programov za takojšnje sporočanje nemalokrat zaupajo svojim prijateljem in niti ne pomislijo, da se tudi najboljša prijateljstva lahko razdrejo. Vse to pa lahko privede do zlorabe gesel in medsebojnega obračunavanja, tudi tako, da nekdo v njihovem imenu piše neprimerne komentarje ali objavlja neprimerne fotografije oziroma videoposnetke.
- Otroka je treba ozavestiti, naj se preko spletne kamere ne pogovarja s tujci, sploh pa naj na njihovo morebitno željo ne kažejo intimnih delov svojega telesa, saj se lahko ti posnetki snemajo in znajdejo kjerkoli in kadar koli na spletu.
- Otroka je treba opozoriti, da za dostop do spletnih socialnih omrežij nikoli ne uporablja javnih računalnikov (knjižnice, šole) ali nezaščitenih brezžičnih omrežij.
- Pomembno je tudi ozaveščanje o spletnih goljufijah na spletnih socialnih omrežjih in otroku razložiti, da če jih prijatelj na družabnem omrežju prosi za denarno pomoč, naj

se najprej osebno ali po telefonu prepričajo, ali je za denarno pomoč res prosil njegov prijatelj, in če dejansko potrebuje denar.

- Bernik (2011) je mnenja, da je otrokom treba razložiti, da večje število prijateljev ne pomeni, da je nekdo boljši od njega, in da je tovrstno tekmovanje lahko nevarno. Zato je pomembno, da starši skupaj z otroki pregledujejo otrokove prijatelje, se o njih pogovorita in odstranita osebe, ki jih otrok ne pozna.
- Osveščena uporaba interneta in spletnih socialnih omrežij je proces, za katerega moramo stalno skrbeti, ga nadgrajevati in ga ni moč kupiti. Potrebno je stalno izobraževanje o nevarnostih in grožnjah, ki nam pretijo na internetu, zato je pomembno, da se starši in učitelji udeležujejo različnih predavanj in izobraževanj in te prenesejo tudi na svoje otroke oziroma učence.

Pomembno je tudi, da otroku ne postavljamo omejitev, pač mu moramo dati možnost lastne odločitve in presojanja o tem, kaj je dobro in kaj ne, kot pri vseh ostalih stvareh v življenju. Tu se delo staršev konča, saj morajo starši skozi vzgojo otroke naučiti kakovostne presoje, kajti kmalu otroci znajo več kot starši. Če so jih starši naučili ustrezne presoje, se nimajo česa bati, otroci pa zrastejo v samostojne ter odgovorne osebe, še navaja Bernik (2011).

Literatura

Bernik, I in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.

Bratuša, T. (1. 1. 2007). Varnost za telebane: Kraja identitete. Moj mikro.si. Pridobljeno s http://www.mojmikro.si/preziveti/varnost/varnost_za_telebane_kraja_identitete

Facebook in mladoletniki. *(17. 6. 2011). Ringaraja.net.* Pridobljeno s http://www.ringaraja.net/clanek/facebook-in-mladoletniki_4614.html

Isakovič, J. (26.6.2009). Družabno mreženje. *Moj mikro.si.* Pridobljeno s http://www.mojmikro.si/preziveti/kar_tako/druzabno_mrezenje

Kaj je dobro vedeti o spletnih socialnih omrežjih?. (2010). *Safe.si.* Pridobljeno s http://www.safe.si/c/1149/Druzabna_omrezja/?preid=691

Kaj je otroška pornografija?. (2008). *Spletno oko.si*. Pridobljeno s http://www.spletno-oko.si/index.php?fl=0&p1=603&p2=573&p3=701&id=701

Kaj je sovražni govor?. (2008). *Spletno oko.si.* Pridobljeno s http://www.spletno-oko.si/index.php?fl=0&p1=603&p2=573&p3=702&id=702

Kaj starši lahko naredijo za varnost svojih otrok. (2011). *Safe.si*. Pridobljeno s http://www.safe.si/c/691/Top_10_nasvetov

Kodelja, M. in Banovič, Z. (15. 5. 2010). Kdo je žrtev spletnega nadlegovanja. *Moj mikro.si.* Pridobljeno s http://www.mojmikro.si/v_srediscu/razkritje/kdo_je_zrtev_spletnega_nadlegovanja

Košir, I. (30. 5. 2011). Otroci varni na spletu. *Žurnal.si.* Pridobljeno s http://www.zurnal24.si/otroci-varni-na-spletu-clanek-124556

Kraja identitete. (2010). *Varni na internetu.si*. Pridobljeno s https://www.varninainternetu.si/article/kraja-identitete/

Psihologija identiteta sebstvo karakterji etičnost zavest stereotip. (15. 6. 2008). *Zdravstvena.info.* Pridobljeno s http://www.zdravstvena.info/vsznj/psihologija-identiteta-sebstvo-karakterji-etnicnost-zavest-streotip/.

Seksting-kaj lahko naredite?. (2012). *Safe.si.* Pridobljeno s http://www.safe.si/c/1565/Seksting/?preid=673

Shinder, D. L. in Tittel, J. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* Rockland: Syngress Publishing, Inc.

Smernice glede varstva pred spletnim nadlegovanjem. (2009). *Informacijski pooblaščenec.* Pridobljeno s https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-glede-varstva-pred-spletnim-nadlegovanjem.pdf

Umek, P. in Čarman, P. (2008). *Ko se zalezovanje konča z umorom*. Pridobljeno s http://www.fvv.uni-mb.si/dv2008/zbornik/clanki/Umek-Carman.pdf

Varnost spletnih socialnih omrežij. (2009). *Zveza potrošnikov Slovenije*. Pridobljeno s http://www.zps.si/testiranje/tehnologija/internet/varnost-spletnih-socialnih-omrezij.html?Itemid=628

Varstvo osebnih podatkov na internetu. (2011). *Informacijski pooblaščenec.* Pridobljeno s https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/