International Journal of Scholarly Papers for Media and Society Research

Media dialogues
MEDIJSKI DIJALOZI
ISSN 1800-7074 (*print*)
ISSN 2536-5622 (*on line*)

Varga, M. (2008), „Hazards and Protection of Young People on the Internet",
Media dialogues / Medijski dijalozi, Vol. 1, No. 3, pp. 69-87.

mr **MATIJA VARGA**,
Tehnička škola Čakovec,
Hrvatska

HAZARDS AND PROTECTION OF YOUNG PEOPLE ON THE INTERNET

Apstract: *Problems that are trying to be solved today concerning young people are: (1) suppression of Internet and "online" gaming dependence, (2) reducing the number of stolen identities, and the problem (3) of protection against possible online abuse. Internet addiction among young people does exist, as it has been proven in numerous national and international research analyses. This paper presents ways of combating internet addiction of young people. One way of combating internet and gaming addiction, which is described in detail, is setting up parental control in the operating system (used by young people) by IT professionals. In addition to the method mentioned above, a number of interesting actions, projects and lectures are being implemented today to protect young people on the Internet. When it comes to protecting user accounts on e-social networks, young people should frequently change their password, and set a strong one. To prevent computer exploits of young people over the internet, a managing local computer network and control system is often introduced, and thus controlling the online data flow, which is also described in more detail.*

Key words: *internet, young people, e-social network, internet dependence, antivirus software, open DNS.*

OPASNOSTI I ZAŠTITE MLADIH NA INTERNETU

Apstrakt: *Problemi koji se danas nastoje riješiti kod mladih su: (1)suzbijanje ovisnosti o internetu i „online" igricama, (2)smanjenje broja krađe identiteta mladih, te problem (3)zaštite mladih od mogućeg zlostavljanja putem interneta. Ovisnost o internetu kod mladih postoji, a to je dokazano u radu na temelju prikaza i analize rezultata brojnih domaćih i stranih istraživanja. U radu su prikazani načini suzbijanja ovisnosti mladih o internetu. Jedan od načina suzbijanja ovisnosti mladih o internetu i „online" igricama koji se detaljnije opisuje je postavljanje roditeljskog nadzora u operacijskom sustavu (kojeg koriste mladi) od strane informatičkih stručnjaka. Osim navedenog načina zaštite mladih od ovisnosti o internetu, danas se za zaštitu nastoje provoditi brojne zanimljive akcije, projekti i predavanja. Kada je riječ o zaštiti korisničkih računa na e-društvenim mrežama mladih, mladi bi trebali učestalo mijenjati lozinku, te postaviti lozinku jake snage. Za sprječavanje pokušaja napada mladih preko računala nerijetko se uvode sustavi za upravljanje lokalnom mrežom računala i kontrolu, te se na taj način kontrolira tijek podataka mladih na internetu što je također detaljnije opisano u radu.*
Ključne riječi: *internet, mladi, e-društvene mreže, internetska ovisnost, antivirusni softver, otvoreni DNS.*

1. UVOD

Prvi dio rada prikazuje objašnjenja i komentare rezultata provedenih istraživanja o ovisnicima na internetu, zlostavljanju mladih na internetu, te na ostale opasnosti koje prijete na internetu.

Drugi dio rada prikazuje mogućnosti i načine zaštite mladih na internetu i zaštitu elektroničkih podataka. U današnje vrijeme kada je internet potreban i važan resurs za mlade, te za njihov proces e-učenja, potrebno je posvetiti veliku pažnju računalnoj sigurnosti i računalnim sigurnosnim mehanizmima, zaštiti djece i mladih na internetu, te zaštiti elektroničkih podataka o mladima. Djecu i mlade je potrebno usmjeriti prilikom korištenja interneta na pozitivnosti koje internet pruža. Na internetu kao novom mediju nije sve tako „crno", postoje i brojne „svijetle" točke interneta.

Cilj rada je preporukama i načinima zaštite, zaštiti mlade od opasnosti, ovisnosti i zlostavljanja koja im prijete na internetu kao najpopularnijem mediju mladih.

Postavljeni zadaci rada su: ukazati na moguće opasnosti i prijetnje za mlade koje postoje na internetu, prikazati mogućnosti zaštite elektroničkih podataka mladih na internetu, dati savjet na koji način koristiti određene e-društvene mreže, utjecati na mlade korisnike interneta u cilju smanjenja lažnog predstavljanja na internetu i suzbijanja ovisnosti, napomenuti mladima koje besplatne antivirusne programe mogu koristiti (bolje je imati bilo kakav antivirusni program, nego koristiti Windows operacijski

sustava bez antivirusnog programa), opisati od koje kombinacije znakova se treba sastojati optimalna ili jaka lozinka, dokazati i objasniti kakvu štetu mogu nanijeti najopasniji crvi, virusi i trojanski konj. Ovim radom se nastoji utjecati na mlade navođenjem pravila ponašanja na internetskim e-društvenim mrežama, upozoriti mlade korisnike interneta da jednom objavljeni podaci na internetu zauvijek ostaju na internetu u većini slučajeva, (te da ih je teško „maknuti" jer postoje internetske arhive koje trajno pamte podatke), upozoriti mlade da paze koje podatke šalju putem chata, jer se sugovornik može predstaviti lažnim imenom, dati preporuke o načinima suzbijanja povreda prava djece i mladih na internetu, upozoriti na problem ovisnosti mladih o e-društvenim mrežama i online igricama, prikazati sustave za nadzor i kontrolu tijeka podataka mladih na internetu, prikazati postavke privatnosti društvenih mreža i spomenuti način postavljanja roditeljske zaštite u operacijskim sustavima.

2. UPOZNAVANJE S INTERNETOM

Internet je globalni informacijski sustav za komunikaciju koji povezuje i spaja računalne mreže pojedinih zemalja i organizacija, te omogućava posjednicima računala koji su ujedno i korisnici interneta diljem svijeta da putem svojih lokalnih i telefonskih mreža međusobno komuniciraju, razmjenjuju informacije i koriste brojne druge usluge (Dragičević, 2004. s. 28.). Internet je danas jako široki pojam, te postoje brojne definicije interneta. Internet se razvio iz projekta američkog Ministarstva obrane pod nazivom Arpanet, kojeg su krajem šezdesetih godina pokrenuli u SAD. Internet je nekontrolirani medij, preko kojeg se danas mogu razmjenjivati informacije velikom brzinom. Internetom se razmjenjuju određene informacije brže nego putem televizije i radio medija. Internet je širokopojasna rasprostranjena mreža koja povezuje računala bez obzira na veličinu, te skupinu kojoj pripadaju, a koja su spojena na internet. Internet jednostavno možemo opipati ukoliko ga promatramo s fizičke razine.

Danas na internetu možemo raditi „na stotine" stvari. Ako se pita mlade što sve mogu raditi na internetu, njihov prvi odgovor je igranje igrica. U ovom slučaju mišljenje mladih je usmjereno na igranje zabavnih igrica kojih ima daleko više na internetu nego edukativnih. Mlade treba usmjeriti na igranje edukativnih igrica. Osim za zabavu internet služi za mnogo ozbiljnije stvari. Internet omogućava pronalazak adrese ili broja telefona osobe koju želimo kontaktirati, kupovanje i prodavanje osobnih stvari, slušanje glazbe, gledanje videa, planiranje putovanja, rezervaciju i plaćanje avionskih karata, slanje i primanje elektroničke pošte webmail-om ili e-mail-om, e-učenje, dopisivanje s drugim korisnicima interneta preko internetskih servisa, praćenje najnovijih vijesti, istraživanje, kupovanje, prodavanje vrijednosnih papira i praćenje kretanja vrijednosti dionica, učenje na daljinu, prikupljanje podataka o povijesnim ličnostima, prevođenje tekstova sa stranog jezika na korisniku razumljiv jezik, pronalaženje određenog mjesta pomoću geografskog informacijskog sustava, kontroliranje potrošnje usluga pomoću pružatelja internetskih usluga, razgovaranje i gledanje s udaljenom osobom, skidanje datoteke, objavljivanje svojih slika i izražavanje svojeg

mišljenja putem web mjesta, upload web stranica, upravljanje CMS i LMS sustavima, skidanje besplatnih antivirusnih programa**.** Sve navedene mogućnosti su ujedno i prednosti interneta. Internet kao medij danas može poslužiti za utjecaj na mišljenje javnosti i određene populacije.

2.1 Struktura interneta

Internetom mogu biti povezani mail serveri, web serveri, ftp serveri ili poslužitelji, lokalna računala, stolna računala, prijenosna računala, mobilni uređaji, te dijelovi mreže kao što su: dsl modem, kabelski modem, usmjernik i preklopnik. Internetom se povezuje sve veći broj netradicionalnih krajnjih sustava kao što su: TV uređaji, uređaji u automobilima, okviri za slike, kućni elektronski i sigurnosni sustavi i web kamere (Kurose & Ross, 2005, p. 2.).

2.2 Internetske usluge

Osnovne vrste internetskih usluga su: WWW*(World Wide Web)*, elektronička pošta, FTP*(File Transfer Protocol)*, Telnet, IRC*(Internet Relay Chat)*. U današnje vrijeme većina korisnika interneta misli da je *World Wide Web* ujedno internet, ali on se bitno razlikuje od interneta. Korisnici interneta, oznaku WWW navode prilikom upisa URL adrese u adresni prostor internet preglednika.

2.3 Povezivanje na internet

Povezivanje na internet omogućava ISP (pružatelj internet usluga). Tvrtka koja je ujedno ISP daje svojim korisnicima uređaj za pristup internetu tj. usmjernik, te korisničko ime i lozinku korisnika koju kasnije može sam korisnik promijeniti. Za pristup internetu danas se koriste pristupni uređaji: kabelski modem i ADSL usmjernik.

3. OVISNICI O INTERNETU

Sve što izaziva ugodu pri konzumaciji, a patnju kad nedostaje, možemo nazvati ovisnošću. Uzroci ovisnosti često proizlaze iz društvene krize, nedovoljnog samopouzdanja, potrebe za konformizmom, iz dosade, obilja i dokoličarenja (Pezo, 2011). U današnje vrijeme mladi gotovo da i ne mogu normalno funkcionirati bez internetskih tehnologija. Jedna od težih opasnosti na internetu koja prijeti mladima je ovisnost o internetu. Ovisnost o internetu se ubraja u skupinu suvremenih ovisnosti. Sve više mladih je ovisno o mediju internet.

Koga svrstati u skupinu ovisnika o internetu? Cjelodnevni korisnici interneta koji su na određeni način prisiljeni raditi na internetu nisu ujedno i ovisnici interneta. Ovisnici o e-društvenim mrežama tipa „Facebook“ postoje. „Facebook“ je servis koji uništava korisnika i linijski pojačava njegovu ovisnost. Vrijeme brzo prolazi, dok ovisnik pretražuje, pregledava profile, slike i tekstualni sadržaj na profilima svojih poz-

nanika, prijatelja, te poznatih osoba iz privatnog i javnog života. Pregledavanju profila korisnika „Facebooka" nigdje nema kraja. Svaki prijatelj ima svoje prijatelje kojima se može pregledati sadržaj osobnog profila. Postavlja se pitanje: „Možemo li svakodnevno ili učestalo korištenje interneta smatrati ovisnošću o internetu?" Danas je internet toliko moćan medij, bez kojeg ne može funkcionirati poslovni svijet, gospodarstvo, bankarstvo, školstvo, policija, zdravstvo, te ostali privatni i javni sektor itd. Ljudi su primorani koristiti internet kao medij u određenim situacijama. Korisnici koji zbog ostvarenja određenih životnih potreba moraju raditi duže vrijeme na internetu ne možemo smatrati ovisnicima. U skupinu ovisnika o internetu mogu se ubrojiti: ovisnici o elektroničkoj pošti, korisnici koji neprestano pregledavaju „Facebook" profile drugih njima interesantnih osoba, korisnici koji učestalo gledaju određene spotove i video isječke na „YouTube-u", korisnici internetskih igrica koje nisu edukativne, korisnici interneta koji učestalo pregledavaju pornografske sadržaje, ovisnici o seksualnim raspravama na internetu, korisnici chat usluge koji bi se danonoćno dopisivali, osobe koje postaju frustrirane ako se ne mogu spojiti na internet radi zabave, korisnici „online" kockanja, klađenja i aukcijskog nadmetanja, korisnici informacija o drugim osobama, gledatelji filmova na pojedinim internetskim servisima, kupci koji kupuju putem e-trgovina, sudionici online kartanja, ovisnici o skidanju pjesama, ovisnici o blogovima, ovisnici o forumima itd.

Na temelju istraživanja ovisnosti o internetu metodom „anketiranja", brojni istraživači došli su do zaključka da postoje ovisnici o internetu na temelju postavljenih kriterija. Istraživanje u susjednoj zemlji koje se provelo sredinom 2002. na uzorku od 1194 ispitanika *(N=1194)* govori o pojavi i laganom porastu broja ovisnika o računalu i internetu kod mladih u srednjim školama. Autorica već u to vrijeme dolazi do zaključka da internet nudi puno različitih mogućnosti tj. usluga koje smanjuju ili otežavaju kontrolu vremena provedenog na internetu. Autorica navodi da internet pruža mogućnost da se olakša usamljenost, neprihvaćenost i pritisak društva (Jeriček, 2011). Istraživanja o ovisnosti na internetu počela su se učestalije provoditi unatrag petnaestak godina pa i više u pojedinim zemljama. Andre Hanh i Matthias Jeruzalem iz Sveučilišta Humboldt-Berlin proveli su istraživanje o ovisnicima na internetu na temelju uzorka od 8.266 ispitanika od čega je 7.091 ispitanika iz savezne republike Njemačke. U istraživanju se navodi da 3,2% ispitanika formalno zadovoljava kriterije internetske ovisnosti. Grupa koja zadovoljava kriterij ovisnosti provodi 34.6 sati u tjednu na internetu (, dakle 5 sati dnevno u prosjeku). Slijedeća skupina korisnika interneta koja je također rizična provodi 28.6 sati tjedno na internetu (, dakle 4.09 sati dnevno u prosjeku). Neprimjetni internet korisnici, koriste internet samo 7.6 sati tjedno.[1] 3,2% ispitanika koji su ovisnici (od ukupnog broja) nije puno, pogotovo ukoliko se radi o zaposlenicima koji rade s internetskim tehnologijama unutar tvrtke. Ako navedenih 3,2%

[1] Internetsucht: Jugendliche gefangen im Netz.(2011).
URL:http://www.onlinesucht.de/internetsucht_preprint.pdf(11.6.2011).

ispitanika provodi 5 sati dnevno na internetu poslije radnog vremena, to može predstavljati veliki problem za osobu. Takvom korisniku je nužno potrebna apstinencija.

Tablica 1. Prikaz ovisnosti korisnika interneta o uslugama u postocima

Internetska ovisnost:				
Ovisnost o:	Neprimjetna ovisnost	Potencijalna ovisnost	Ovisnost	Zbroj:
dopisivanju	17,8%	26,6%	35,1%	79,50%
glazbi	11,7%	14,9%	14,7%	41,30%
igrama, klađenju	5,4%	7,8%	11,1%	24,30%
pornografija	6,9%	12,5%	9,8%	29,20%
drugom	21,4%	11,2%	7,1%	39,70%
online bazama podataka	16,6%	8,5%	5,2%	30,30%
online trgovinama	5,6%	4,1%	3,3%	13,00%
komunikacijskim sustavima	5,7%	4,4%	3,2%	13,30%
video-livestreamingu	2,7%	2,9%	3%	8,60%
online aukcijama	2,4%	2,3%	2,9%	7,60%
chatu za odrasle	1,2%	2,6%	2,8%	6,60%
razmjeni	2,5%	1,8%	1,7%	6,00%
kockanju s pravim novcem	0,1%	0,4%	0,1%	0,60%

Na temelju tablice 1[2] koju su prikazali autori André Hahn i Matthias Jerusalem u svom radu pod naslovom: „Internetsucht: Jugendliche gefangen im Netz“ može se vidjeti da se internetska ovisnost može dekomponirati na: (1)neprimjetnu ovisnost, (2)potencijalnu ovisnost i (3)ovisnost. Kada je u pitanju „čista“ ovisnost, na temelju tablice 1. se može zaključiti kako su korisnici interneta najviše ovisni o: dopisivanju koje omogućuje usluga chat (35,1%), glazbi (14,7%), igrama i klađenju(11,1%), te pornografiji(9,8%). 34% ispitanika od ukupnog broj ispitanih osoba u dobi od 15 do 29 godina se smatra ovisnicima o internetu. Korisnici interneta su svrstani u skupinu ovisnika jer (kako se navodi u istraživanju) provode više od 48 sati tjedno na internetu, a najugroženije su osobe koje provode 10 sati dnevno na internetu.[3] Provoditi 10 sati dnevno na internetu je previše pa može naštetiti zdravlju korisnika. U današnje vrijeme na temelju kratkih informativnih anketa koje nisu u većini slučajeva reprezentativne može se zaključiti da postoji određeni broj ovisnika o internetu. Prema nekim procjenama navodi se da je u Hrvatskoj 2009. bilo oko 130.000 ovisnika o internetu

[2] Obrada i analiza podataka tablice od strane autora rada prikupljenih pomoću materijala pod naslovom: Internetsucht: Jugendliche gefangen im Netz.(2011).
URL:http://www.onlinesucht.de/internetsucht_preprint.pdf, (11.6.2011).

[3]). URL: hrcak. srce.hr/file/97974. Pregledni rad. (11.6.2011).

između 20 i 30 godina. Kako se navodi u preglednom radu „Kriza odgoja i ekspanzija suvremenih ovisnosti“ takvim se problemom još nitko nije kod nas sustavno multidisciplinarno bavio (Miliša i Tolić, 2011). Što svakako nije dobro. Praksa u zapadnim zemlja je malo drugačija, te se stručnjaci bave takvom vrstom problema kod korisnika interneta.

Računalna ovisnost može kod mladih izazvati brojne fizičke, psihološke i socijalne probleme koje treba najozbiljnije shvatiti. Ovisnici na internetu nerijetko imaju probleme sa spavanjem noću, zanemarivanjem obaveza koje su postavljene pred njih, učenjem, tjelesnom težinom, gubitkom volje i motivacije za druge djelatnosti i hobije. U današnje vrijeme sve više mladih uči i radi seminarske radove metodom „copy-paste“. Korištenjem takve metode mladi ponekad ne pročitaju sadržaj i informacije pojedine web stranice o nekoj temi već s malo razumijevanja kopiraju pronađeni sadržaj. Kako bi se zaštitili mladi od ovisnosti o internetu nastoje se provoditi zanimljive akcije, projekti i predavanja kao što su: „Deset dana bez ekrana“[4], objavljivanje prezentacija o opasnostima na internetu od strane mup-a[5], učestalo objavljivanje članaka o ovisnosti djece na internetu, održavanje predavanja za mlade u školama na temu „Opasnosti na internetu“, u tjednu kada je dan sigurnosti djece na internetu (8.2.), nastavnike informatike u školama navode voditelji aktiva i predstavnici Agencije za odgoj i obrazovanje na održavanje nastave na temu „Sigurnost djece i mladih na internetu“ barem jedan sat, kako mladi ne bi doživjeli jedan od oblika zlostavljanja.

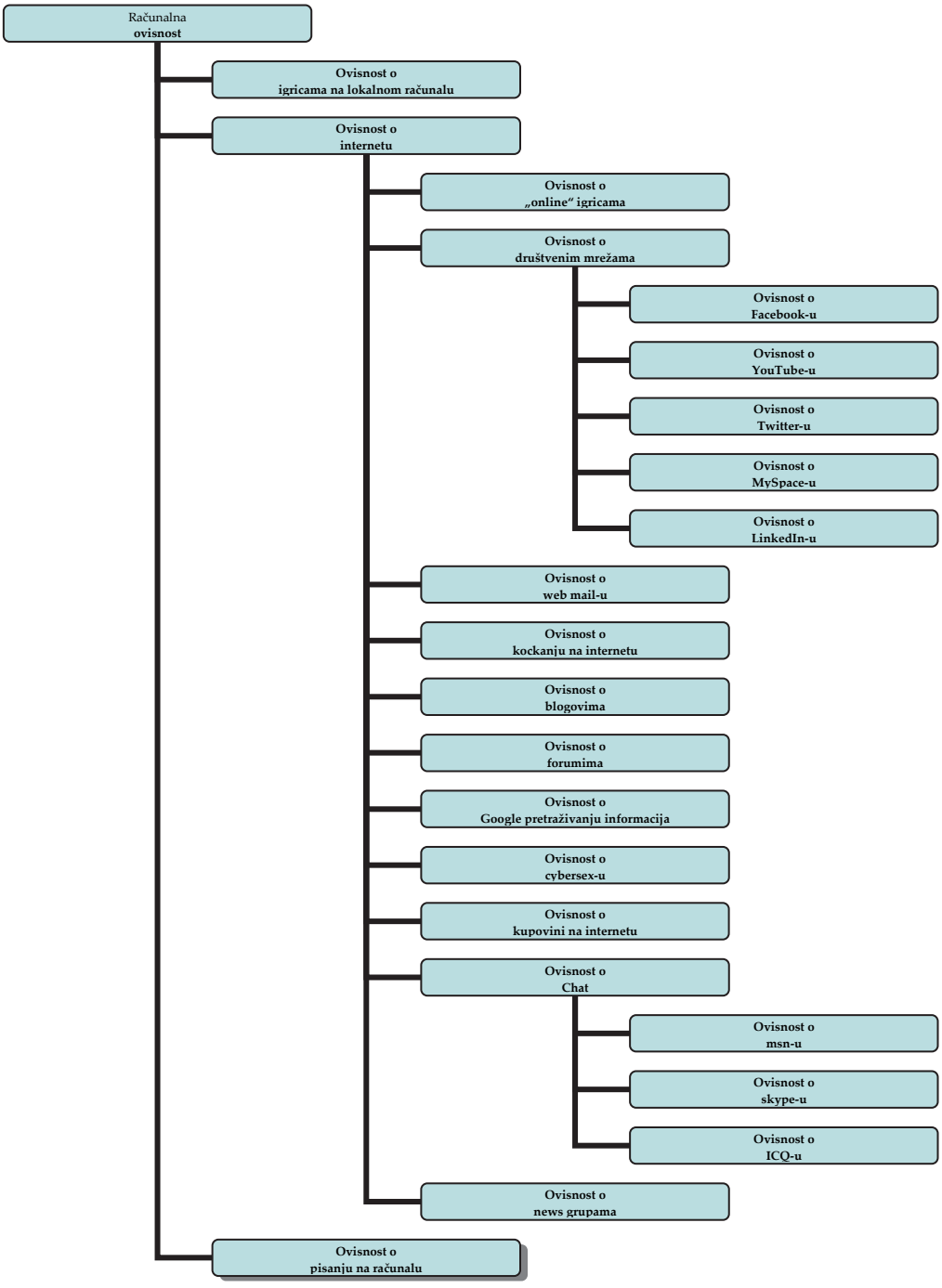
Slika 1.[6] prikazuje dekompoziciju računale ovisnosti po razinama. Ukoliko je korisnik računala ovisan o e-društvenim mrežama i „online“ igricama ujedno je ovisan i o računalu. Na prvoj razini prikazane su: ovisnost o igricama na lokalnom računalu, ovisnost o internetu i ovisnost o pisanju na računalu. Za vrijeme izvođenja nastave iz informatike nerijetko mladi pokažu interes da pišu umjesto u bilježnice, na računalu. Na drugoj razini prikazane su: ovisnost o „online igricama“, ovisnost o e-društvenim mrežama, ovisnost o web mail-u, ovisnost o kockanju na internetu, ovisnost o blogovima, ovisnost o forumima, ovisnost o Google pretraživanju informacija, ovisnost o cybersex-u i ovisnost o kupovini na internetu. Ovisnost o e-društvenim mrežama je dekomponirana samo na ovisnosti o najpopularnijim i najčešće korištenim društvenim mrežama.

[4] Projekt predstavljen od Zlatka Miliše.

[5] Ministarstvo unutarnjih poslova Republike Hrvatske.

[6] Izrada autora rada (dekompozicija ovisnosti na računalu).

Slika1. Dekompozicija ovisnosti o računalu



4. OBLICI POVREDA MLADIH NA INTERNETU

Najčešći oblik povreda mladih na internetu je zlostavljanjem. Rizici koji postoje na internetu od kojih bi se mladi trebali čuvati prilikom „surfanja" i na neki način ometaju komunikaciju na internetu, te mlade mogu dovesti u opasnost su: komercijalni, promidžbeni, napadački, seksualni i vrijednosni. U komercijalne rizike i opasnosti koje prijete mladima se ubrajaju: brojne reklame i promidžbene aktivnosti opojnih sredstava, alkoholnih pića i duhanskih proizvoda. Rizik za mlade može predstavljati neželjena pošta putem koje se mogu distribuirati čudni i zlonamjerni sadržaji, te sponzorske reklame. Objavljivanje osobnih podataka mladih, praćenje mladih, ilegalno skidanje određenog sadržaja, financijske prijevare i kockanje predstavljaju veliki problem za mlade. Prilikom surfanja mladih na internetu postoji rizik da dožive napad od strane zlonamjernih osoba. Na internetu se mladi mogu susresti s nasiljem i poticanjem mržnje. Mladi se mogu susresti s pornografskim sadržajem, nasilničkim ponašanjem i uznemiravanjem drugih od strane trećih osoba. Postoji mogućnost da se mladi upoznaju sa strancem koji ima čudne namjere. Mladi mogu kreirati i postaviti neprikladne materijale na web (*upload*). U vrijednosne rizike na širokopojasnoj rasprostranjenoj mreži s kojima se mladi mogu susresti se ubrajaju: obmanjujuće informacije i savjeti, rasističke izjave i poticanje na mržnju prema određenoj rasi. Na internetu s malom nepažnjom mladi mogu naštetiti sami sebi. Nije mali broj slučajeva u kojima se na određenoj internetskoj stranici nalaze pogrešni podaci u koje mladi vjeruju tj. pogrešne informacije ili dezinformacije na temelju kojih mladi uče na pogrešan način, te njihov razvoj ide u smjeru osobe tipa genijalni idijot. Dezinformacije se razlikuju od informacija po tome što nemaju nikakvu vrijednost za mlade.

Osim navedenih oblika povrede mladih na internetu postoje još povrede u obliku uznemiravajućih i prijetećih poruka, poticanje mržnje od strane grupe korisnika na servisima za dopisivanje prema određenoj osobi, poticanje na daljnje vršnjačko nasilje, vrijeđanje i širenje nasilnih i uvredljivih komentara, kreiranje stranica koje sadrže slike, crteže, priče i šale na račun vršnjaka, slanje neprimjerenih fotografija svojih kolega, iznošenje osobnih podataka i informacija o obiteljskim prilikama, špijuniranje mladih preko web kamere njihovog računala. Špijuniranje mladih preko web kamere njihovog računala jedan je od najtežih oblika povrede mladih. Da bi takva vrsta špijunaže funkcionirala špijun mora imati pristup računalu korisnika koji je meta, te mora imati ovlaštenja na računalu mete. Primjer ovakvog načina zlostavljanja mladih dogodio se u Americi gdje su djelatnici škole špijunirali putem web kamere svoje učenike. Mladi su u tom slučaju dobili računala od škole kako bi mogli pristupiti podacima tj. resursima škole.[7] Kako bi se ovaj oblik povrede mladih preko interneta suzbio potrebno je voditi računa o tome od koga se uzimaju i kupuju računala. Ako mladi uzmu ili posude računalo od nedovoljno poznate osobe ili organizacije koja

[7] Špijunaža djece web kamerom. 2011. URL: http://dnevnik.hr/vijesti/hrvatska/skola-spijunira-ucenike-web-kamerom.html.(8.6.2011).

prodaje ili servisira računalo, bilo bi poželjno da obrate pažnju na takvu mogućnost napada, te da isključe kameru ukoliko je nemaju potrebu koristiti. Primjer 1. Dio teksta koji predstavlja oblik povrede mlade djevojke na internetu od strane grupe neprijatelja koji imaju čudne namjere (Petrić, 2002. s. 275).

Pxxxx tx maxxxxxx balava. mxxx mi od njega. on je MOJ! ixxx tx mxxxx ruxxx. fuj. -.-'
srijeda u 19:22 · Sviđa mi se · Hella HateLove, Valentina Valentić, TruLa Manda i 32 drugih su rekli da im se ovo sviđa.
Barbara Barbić tak treba..nedaj ga..hahahahaha..:)
srijeda u 19:23 · Sviđa mi se · 2 ljudi
Anamarija Marić štera ve pak?? hahahaha XD
srijeda u 19:23 · Sviđa mi se · 3 ljudi
KarLa Karlić 8.z hahahaha. pak sutra budem joj u školi facu poštelala. xxxx ti mxxxx grdu.
Barbara Barbić pak daj se smiri..rekla si kaj joj neš nišš govorila..
srijeda u 19:24 · Sviđa mi se · 1 osoba
Anamarija Marić ahhaahahaah sudjelujem:D
srijeda u 19:24 · Sviđa mi se · 1 osoba:
KarLa Karlić ma nekva balavica ružna s naše škole. :)
srijeda u 19:25 · Sviđa mi se · 3 ljudi
KarLa Karlić normalno. :D
srijeda u 19:28 · Sviđa mi se · 2 ljudi
Kevin Johnson Pa ko bi to itak mogel biti :P Stvarno,ko ? Napiši v inbox pa da procijenim ako je stvarno ružna :P
srijeda u 19:31 · Sviđa mi se
KarLa Karlić pak ona LARA LARIĆ.
srijeda u 19:31 · Sviđa mi se · 5 ljudi[8]

5. ANTIVIRUSNI PROGRAMI ZA ZAŠTITU RAČUNALA MLADIH

Antivirusni programi štite operacijski sustav računala i samo računalo mladih od zlonamjernih programa virusa. Mladi već u školi imaju dovoljno znanja da kreiraju nove vrste virusa (zlonamjernih programa) koji uništavaju ili znatno usporavaju rad drugih računala. Nerijetki su slučajevi kada mladi jedni drugima namjerno šalju viruse putem računala i elektroničke pošte kako bi naštetili primatelju virusa. U većini slučajeva kod mladih su računala puna virusa.

Maliciozni programi su mali programi koji su napravljeni na način da se mogu ugraditi u datoteke koje sadrže druge veće programe. Nakon što se pokrenu takvi programi, aktivirati će se računalni virus koji će izazvati štetu.[9] Računalni virusi su

[8] Kopirane poruke s chat internetske usluge koje pokazuju da postoji nasilje među mladim korisnicima interneta. Informacije su prikupljene presretanjem poruka.
[9].

najčešća i vrlo vjerojatno najopasnija vrsta od svih malicioznih računalnih programa. S obzirom na brzinu širenja i brojnost, uvelike će obilježiti budućnost razvoja interneta i usluga koje on pruža, te zasigurno biti glavni problem pogotovo mladim korisnicima i administratorima informacijskih sustava (Bača, 2004. s. 85). Poznatija vrsta virusa u školskim učionicama je: Bumat! RTS itd. Nerijetko se danas virusi šire elektroničkom poštom. Virusi mogu izbjeći detekciju i na taj način prevariti antivirusni program. Virus može biti prisutan na računalu, a da ga korisnik računala i antivirusni program ne prepoznaju. Zlonamjerne osobe programiraju virus na način da se sakrije njegovo postojanje, kako bi se povećala njegova šansa za rasprostranjivanje.

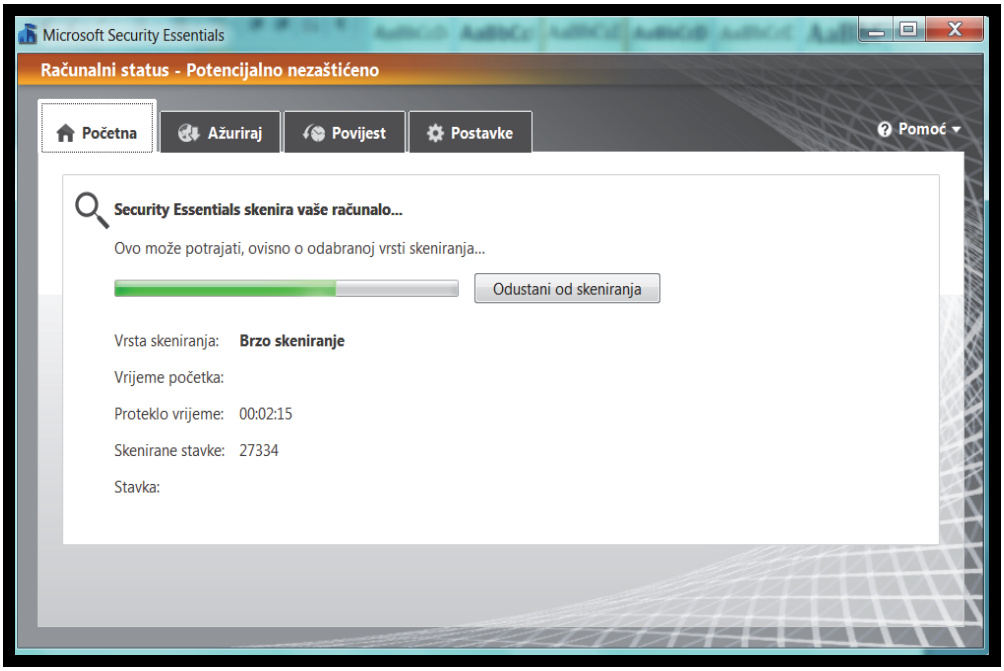
Trojanski konj je vrlo opasan. On obavlja uvijek nešto što ne bismo očekivali npr. krade „lozinke" ili kopira datoteke bez našeg saznanja. Nove teorije o virusima i crvima razlikuju trojance od njih. Uobičajena meta trojanaca su lozinke. Trojanci mogu sakriti neke funkcije koje korisniku ili programeru otkrivaju neke virtualne i privilegirane informacije o sustavu. Trojanci se distribuiraju preko elektroničke pošte i usluga za trenutnu razmjenu poruka, te preko skladišta za datoteke na internetu. Njihova distribucija je sve više povezana s virusima i crvima koji se šire preko elektroničke pošte. Trojanci se često maskiraju kao igrice, programske šale i druge programe koji se često razmjenjuju preko interneta i elektroničke pošte, posebice kada se ne primjenjuju sigurnosna načela. To je jedan od razloga zašto su informatičke učionice u školama pune trojanaca. Trojanski konji se mogu podijeliti s obzirom na vrstu napada: (1)trojanski konji koji napadaču šalju podatke s zaraženog sustava, (2)destruktivni trojanski konji koji brišu i kompromitiraju podatke, (3)DDoS (*Denial of Service*) trojanski konji koji se koriste za izvršavanje napada s uskraćivanjem usluge, (4)*Proxy* trojanski konji koji kanaliziraju mrežni promet ili se koriste za izvršavanje napada s drugog sustava, (5)FTP trojanski konji koji služe kao FTP poslužitelj na računalu koje su inficirali, (6)trojanski konji koji onemogućuju funkcioniranje sigurnosnih programa antivirusne zaštite i sigurnosne stijenke, (7)trojanski konji s udaljenim upravljanjem (RAT – *Remote Administration Trojan*).

Crv se razlikuje od klasičnih virusa po tome što ima snagu reprodukcije, predstavlja zaokruženu cjelinu i ne zahtijeva host-aplikaciju za prenošenje. Primjeri crva prikazani su slikom 5. Crvi koji su detektirani antivirusnim programom su: Helompy.A, Taterf.AW, RjumpJ, Mocmex.F, Confiker.B, Brontok@mm, Small, Muhuhu itd. Velik broj virusa koji zaokupljaju pažnju medija i novina u principu ne pripada virusima, nego je riječ o crvima. Crvi mogu sadržavati viruse, te ih je na taj način moguće iskoristiti za isporuku u određeni računalni sustav.

Osim virusa i crva znatnu štetu programskoj podršci (softveru) mogu nanijeti logičke bombe. To su programi koji dolaze ne aktivirani i čekaju na aktivaciju. Dok se ispuni uvjet za aktiviranje, aktiviraju se i počinju s uništavanjem podataka, te kvarenjem programske podrške. Nije rijetki slučaj da se logičke bombe prenose virusima. Prije korištenja operacijskog sustava računala, poželjno je ažurirati antivirusni program kako bi zadobio nove datoteke.

Zlonamjerne osobe se trude nanijeti štetu korisnicima računala proizvodnjom virusa, proizvođačima programa i operacijskih sustava. One nastoje dokazati, kako proizvođači računalnog programa nisu izradili operacijski sustav i aplikaciju na odgovarajući način s zaštitnim i sigurnosnim mehanizmima, te nastoje dokazati da antivirusni programi ne pružaju dovoljno zaštite. Na taj način se zlonamjerne osobe nadmeću s proizvođačima antivirusnih programa. Takve zlonamjerne osobe koje razvijaju viruse nemaju prevelike koristi od proizvodnje virusa i žele sačuvati anonimnost. Nerijetki slučajevi su kada ista osoba razvija antivirusni program i viruse. Tu nema nadmetanja jer proizvođači virusa zajedno s proizvođačima antivirusnih programa rade u istom interesu. Interes je u ovom slučaju želja za profitom. Tehnologija virusa se neprestano razvija iz razloga što neki proizvođači softvera proizvode automatski generator virusa, te na taj način omogućavaju ostalim proizvođačima virusa „neprogramerima“ da generiraju viruse bez pisanja kodova.

Slika 2. Prikaz skeniranja diska antivirusnim programom



Slika 2.[10] prikazuje skeniranje diska antivirusnim programom kako bi se utvrdilo da li postoje neželjene datoteke na disku računala. Računalni status je potencijalno ne zaštićen, što se vidi iz priložene slike 2. Da bi se zaštitio operacijski sustav u ovom slučaju potrebno je ažurirati antivirusni program. Crvi, virusi i logičke bombe

[10] Izrađena na temelju opcije skeniranje, antivirusnim programom (Microsoft Security Essentials).

se ubrajaju u aktivne napade koji se znatno razlikuju od pasivnih napada gdje napadač tj. zlonamjerna osoba djeluje pasivno tj. ne uništava programsku potporu već presreće i izmišlja poruke.

Za zaštitu računala i operacijskog sustava na računalu u javnim prostorijama i organizacijama (fotokopiraonama, knjižnicama i sličnim centrima, školama, internet kafićima, informatičkim učionicama itd.) koriste se programi koji po ponovnom pokretanju računala, vraćaju operacijski sustav u početno stanje. Kako korisnici računala s navedenim programima gube sve podatke onog trenutka kad se računalo ponovno pokrene, treba omogućiti korisnicima mogućnost spremanja podataka i datoteka na USB memoriju ili drugu particiju diska na kojoj ostaju podaci nakon ponovnog pokretanja računala. Dva poznatija programa koja zadržavaju početno stanje sustava su: Windows SteadyState i DeepFrezz. Navedeni programi su namijenjeni sustavskim administratorima, knjižničarima, profesorima, učiteljima, zaposlenicima u kopirnicama itd. Nakon instalacije Windows SteadyState alata potrebno je podesiti određene postavke. Kako bi Windows SteadyState imao određenu funkcionalnost potrebno je željenu particiju diska zaključati, jer nakon instalacije zaštita nije uključena. Windows SteadyState omogućuje da se određeni sustavi nadograđuju automatski.

6. KRAĐA IDENTITETA MLADIH NA E-DRUŠTVENIM MREŽAMA

Smanjenje slučajeva krađe identiteta na društvenim mreža, danas se nastoji suzbiti podizanjem kaznenih prijava od strane MUP-a i slanjem posebnog izvješća državnom odvjetniku za mladež protiv mladih zlonamjernih osoba koje kradu identitet žrtve, te u njeno ime objavljuje osobne podatke.[11] Krađa identiteta na e-društvenim mrežama je isto jedan oblik zlostavljanja mladih.

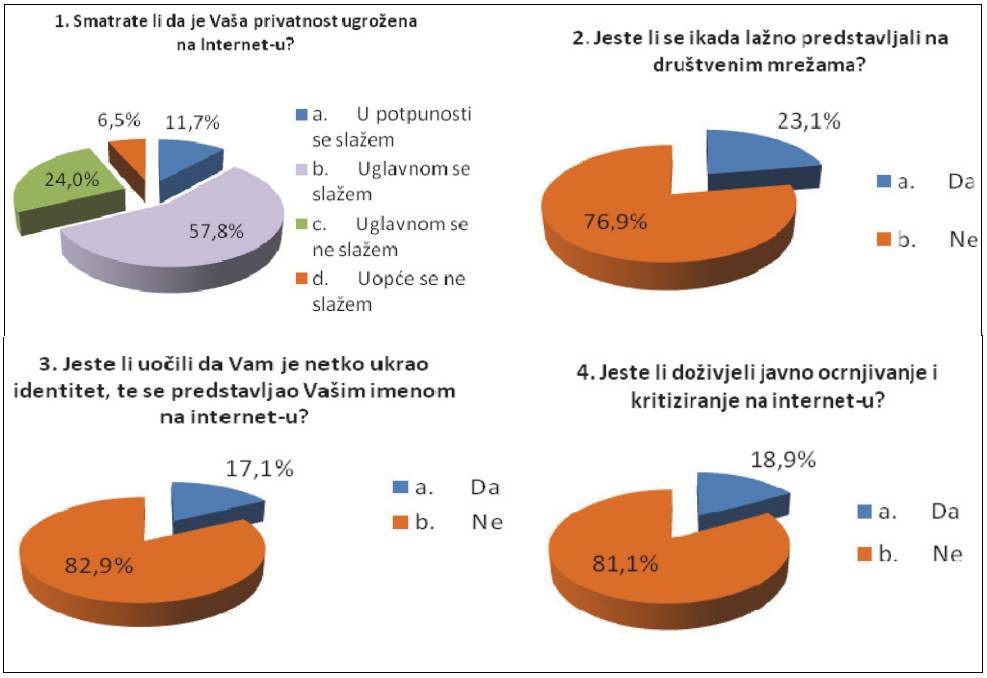
Na temelju neobjavljenog istraživanja autora ovog rada koje se odvijalo u 4. i 5. mjesecu 2011. godine na uzorku od 204 ispitanika *(N=204)* koji su uglavnom školarci tj. učenici osnovnih i srednjih škola s područja Međimurske županije od 13 do 19 godina starosti, došlo se do zaključka da je privatnost mladih ugrožena na internetu što je bio i cilj istraživanja. Mladi koji su anketirani predstavljaju terenski uzorak populacije. Navedeni terenski uzorak je reprezentativan, što znači da ima svojstva koja su relevantna za predmet istraživanja. Osim navedenog cilja istraživanja, jasni zadaci istraživanja bili su: dobiti informacije o potencijalnoj opasnosti na internetu od lažnog predstavljanja kod mladih u određenim školama, dobiti informacije o konkretnom broju krađe identiteta na internetu iz odabranog uzorka, dobiti informacije o tome koliko se ispitanici javno ocrnjuju na internetu (pošto je internet javna računalna mreža). Na temelju prikupljenih informacija nastavnik informatike nastoji utjecati na mlade u cilju suzbijanja: (1)ugrožavanja mladih na internetu, (2)lažnog predstavljanja na

[11] Kaznena prijava.2011. URL:http://dalje.com/hr-hrvatska/zbog-otvaranja-laznog-profila-na- facebooku-maloljetnik-kazneno-prijavljen/362144. (3.6.2011). Parafrazirano.

internetu, (3)ocrnjivanja mladih na internetu kod one skupine mladih, gdje je navedeno zlostavljanje prisutno. U školama gdje je provedeno istraživanje nastojati će se pozitivno djelovati na ispitanike u cilju smanjenja bilo kojeg drugog oblika zlostavljanja mladih. Rezultati su obrađeni i prikazani 3D tortnim rascijepanim grafikonima u MS Excelu, alatu za analitičku obradu podataka.

Slika 3.[12] prikazuje da se 57,8% ispitanika izjasnilo, kako se uglavnom slaže da im je privatnost ugrožena na internetu, 11,7% ispitanika se izjasnilo da se u potpunosti slaže da im je privatnost ugrožena na internetu, 24% ispitanika od ukupnih 100% se izjasnilo kako se uglavnom ne slaže da im je privatnost ugrožena na internetu. Privatnost korisnika interneta nije ugrožena, ako mladi korisnik interneta ne dopusti zlonamjernim osobama objavljivanjem svojih osobnih i drugih podataka da mu ugroze privatnost. Na temelju istog istraživanja, došlo se do zaključka da se većina ispitanika ne predstavlja lažno na e-društvenim mrežama što je dobro i pohvalno. 76,9% ispitanika od ukupnog broja ispitanika se izjasnilo da se nikada nisu lažno predstavljali na internetu, dok se 23,1% ispitanika lažno predstavljalo.

Slika 3. Prikaz rezultata ankete dobivenih na uzorku od 204 ispitanika



[12] Slika 3. prikazuje rezultate obrade podataka prikupljenih anketiranjem u školama. Tortni grafikoni su izrađeni u alatu za analitičku obradu podataka.

Stanje u školama (u kojima se istraživanje provelo) kod mladih u po-gledu krađe identiteta na području Međimurske županije nije alarmantno (Slika 3.). 82,9% ispitanika od ukupnih 100%, odgovorilo je da im nitko nije ukrao identitet na internetu, niti se nije nitko predstavljao imenom mladih anketiranih ispitanika. 17,1% ispitanika imalo je neugodan slučaj, kada je netko drugi (napadač) pisao i komunicirao na internetu u ime mladih ispita-nika, te na početku komunikacije bez njihovog saznanja. 81,1% ispitanika nije doživjelo javno ocrnjivanje na internet-u, dok je 18,9% ispitanika doživjelo jav-no ocrnjivanje i kritiziranje na internetu i na taj je način bilo zlostavljano.

6.1 Sigurnost lozinke kod mladih

Svaka mlada osoba mora imati korisničko ime i lozinku, da bi imala pristup određenom servisu na internetu tj. pružatelju određene internetske usluge. Lozinku mladi trebaju mijenjati obično svakih mjesec dana, a po potrebi bi se trebala mijenjati više puta mjesečno. Nisu rijetki slučajevi kada jedna mlada osoba sazna lozinku druge osobe, te joj zlonamjerna osoba u ime druge osobe nanosi štetu što je isto jedan od oblika zlostavljanja mladih. Optimalna lozinka koju koriste mladi na internetskim servisima bi trebala sadržavati minimalno sedam znakova. Za lozinku bi bilo poželjno da sadrži kombinaciju velikih i malih slova, te brojeve. Nikako se ne preporuča za lozinku koristiti osobna imena, prezimena, imena roditelja, djece, datum rođenja, naziv mjesta boravišta, naziv ulice i sl., a takve lozinke mladi najčešće koriste. Za lozinku se ne preporuča korištenje skupa istih znakova. Zbog sigurnosti, mladi ne bi smjeli lozinku zapisivati na papir i ostavljati u ladici svoje sobe kako ne bi njihov prijatelj, brat, sestra ili prijateljica došli do podataka, te ostvarili pristup korisničkom profilu. Pisanje neprimjerenih izjava po tuđem profilu na internetu možemo svrstati u oblik zlostavljanja osobe. Najčešći napad mladih na lozinke tj. profile svojih prijatelja je ispitivanjem ili pogađanjem lozinki. Ispitivanje ili pogađanje lozinki napad je u kojem počinitelj pokušava pristupiti određenom sustavu nasumičnim pogađanjem lozinke, pri čemu se u većini slučajeva koristi metoda pokušaja i pogreške. Iako ovaj napad izgleda malo naivan ponekad može biti učinkovit, pogotovo kada napadač dobro poznaje osobu koja je postavila lozinku.

Drugi najčešći napad na lozinke kod mladih je tako zvani „Phishing“. Korisnik korisničkog računa od napadača dobiva neželjeni mail u kojem se traži dostavljanje korisničkog imena i lozinke u slijedećih nekoliko dana, te piše: „ukoliko se ne pošalje korisničko ime i lozinka možete trajno izgubiti account“. Primatelj takve elektroničke pošte ima osjećaj da je mail poslan od strane administratora s internet poslužitelja koji korisniku pruža samu uslugu. Napadač koristi naziv ISP pružatelja internet usluga tako da pošta bude uvjerljivija. Ponekad su mladi lakovjerni pa najčešće nasjedaju na takve mail-ove. Preporuka mladima je da se ne nasjeda na takve mail-ove, te da se ne šalju osobni korisnički podaci kao odgovor na takvu e-poštu.

6.2 Postavke privatnosti na e-društvenoj mreži

Postavke privatnosti „Facebooka“ mogu se regulirati isključivanjem i brisanjem. Isključivanje „Facebook“ profila mladih znači da će podaci i sadržaji na profilu biti skriveni od pogleda drugih prijatelja, ali se spremaju na „Facebook“ poslužiteljima, u slučaju da korisnik želi ponovno aktivirati svoj profil. Ime korisnika se pojavljuje kao crni tekst na koji se ne može kliknuti jer je profil skriven.

Brisanjem „Facebook“ računa trajno se uklanja stranica. „Facebookov“ centar za pomoć oko osobnih informacija vezanih uz korisnički račun navodi da trajno brisanje uključuje brisanje informacija kao što su: ime, e-mail adresa i poštanska adresa. Kopije nekih materijala (fotografije, bilješke, itd.) mogu ostati na serverima „Facebooka“ zbog tehničkih razloga. Trajno pohranjivanje fotografija od strane „Facebooka“ nije dobro za korisnike usluge e-društvene mreže. Svi materijali na „Facebooku“ bi trebali biti distancirani od bilo kakvih osobnih identifikatora i potpuno nedostupni drugim korisnicima. „Facebook“ također ne koristi sadržaje povezane s računima koji su deaktiviran ili izbrisana. Tu je prisutno više dnevno kašnjenje prije nego što se doista potpuno izbrišu svi podaci na „Facebooku“, jer je uzeta mogućnost da u međuvremenu korisnik može promijeniti svoje mišljenje. Prilikom korištenja e-društvene mreže, „Facebook“ korisnik bi trebao dobro promisliti na temelju čega se servis financira, te dali može ostvariti dobit samo od klasičnog oglašavanja, te kako je (ili kako će) „Facebook“ postigao vrijednost koja se pretpostavlja u dionicama na 100 milijardi dolara.

7. PREPORUKE ZA SUZBIJANJE POVREDA PRAVA MLADIH NA INTERNETU

Kako bi se suzbile povrede prava mladih na internetu, internetski servisi nude pravila korištenja. Preporuka je da se korisnici pridržavaju navedena pravila. Korisnik mora potvrditi da će se pridržavati postavljena i navedena pravila korištenja internetskih servisa prilikom kreiranja profila ili korisničkog računa elektroničke web pošte. Svaki pružatelj internetskih usluga nastoji staviti rigorozna pravila, ali ta pravila se korisnici internetskih usluga rijetko pridržavaju, a mladi u većini slučajeva ni ne čitaju pravila nego ih automatski potvrde klikom miša.

Pravila koja bi se mladi morali pridržavati prilikom korištenja usluga dopisivanja na internetu su: ne smiju se promovirati aktivnosti vezane uz drogu, alkohol i druga opojna sredstva. Svaki pružatelj pojedine usluge na internetu ima pravila koja se korisnik mora pridržavati, takva navedena pravila se ne smiju ismijavati ili omalovažavati. Opće je poznato da pružatelji usluga za dopisivanje ne dozvoljavaju da se objavljuju u prostoru za pisanje adrese URL stranica i linkovi gdje se nalazi sadržaj vezan za seks ili ilegalna glazba. Na chat-u i grupama se ne smiju stavljati linkovi na krekerske stranice.

U povrede prava mladih na internetu se ubraja krađa identiteta na e-društvenim mrežama. Način na koji bi se suzbila ovakva povreda mladih na internetu je omogućavanje da se korisnici autoriziraju na internetskim servisima biometrijski. Na taj način bi se lako mogli pronaći mladi koji se predstavljaju tuđim imenima svojih kolega i drugih korisnika. Jedini je problem kod uvođenja sustava za biometrijsku autorizaciju internet korisnika, financijska isplativost, te postojanje takve mogućnosti i opcije kod internetskih servisa. U današnje vrijeme pružatelji internet usluga, te proizvođači operacijskih sustava nude adrese elektroničke pošte na koje se žrtve krađe identiteta mogu žaliti i prijaviti slučaj, u interesu da se takvim slučajevima stane na kraj.

8. KONTROLA TIJEKA PODATAKA NA INTERNETU

Da bi se zaštitili mladi na internetu potrebno je koristiti određene alate koji simuliraju roditeljski nadzor, jer nemoguće je biti uz dijete koje „surfa" po internetu 24 sata. Danas postoje alati koji blokiraju pristup određenim stranicama na internetu. Takvu mogućnost nude alati za upravljanje učionicom ili lokalnom mrežom računala. Oni mogu blokirati npr. „Facebook" i „YouTu-be". SynchronEyes Classroom Management alat koriste nastavnici u nastavi kako bi imali nadzor i kontrolu tijeka podataka nad računalima i u računalnim mrežama na kojim rade mladi.

8.1 Sustavi za upravljanje lokalnom mrežom računala

Nastavnicima sustavi za upravljanje mrežom računala pružaju brojne mogućnosti u nastavi. Sustavi poput SynchronEyes Classroom Managementa omogućuju prezentaciju sadržaja sa svoga ekrana svim učenicima u razredu, zatim omogućuju aktivno uključivanje učenika u nastavu kroz podršku za kreiranje grupa učenika, te omogućuju prezentaciju pojedinih rješenja na svim računalima u razredu, pregled rada učenika JIT[13], aktivnu kontrolu rada učenika putem mogućnosti kontrole ulaznih jedinica, kreiranje i provođenje testova znanja, kao i evaluaciju rezultata JIT, distribuiranje i prikupljanje digitalnih rješenja učenika, upravljanje nastavom u smislu omogućavanja izvršavanja pojedinih aplikacija i pristupa internetu, upravljanje učionicom i računalima učenika, te upravljanje njihovim radovima koji se trenutno nalaze u digitalnom obliku.

8.2 „Roditeljska" zaštita kod OS-a i OpenDNS

Informatičari na računalu u pojedinim operacijskim sustavima mogu postaviti roditeljsku zaštitu tj. roditeljski nadzor nad računalom. Pošto je velika većina pogoto-

[13] JIT –just in time (u realnom vremenu)

vo starijih roditelja informatički nedovoljno pismeno da bi postavili takav tip nadzora, za dobrobit mladih bi se trebali obratiti informatičaru ili informatičkoj tvrtki kako bi informatičar postavio roditeljski nadzor nad korisničkim računom mladih. Putem značajke roditeljskog nadzora se može upravljati načinom na koji mladi koriste računalo. Informatičar na računalu vlasnika, može postaviti ograničenja na sate tijekom kojih mladi smiju koristiti računalo, na vrste igrica koje smiju ili ne smiju igrati i programe koje smiju pokrenuti. Kada značajka roditeljskog nadzora blokira pristup igri ili programu, pojavljuje se obavijest da je program blokiran. Mladi mogu kliknuti vezu u obavijesti da bi zatražili dopuštenje pristupa igri ili određenom programu. Pristup se može dopustiti unosom korisničkih podataka. Da bi se postavio roditeljski nadzor za dijete, potreban je vlastiti administratorski korisnički račun. Prije početka je potrebno provjeriti imaju li mladi za koje se želi postaviti roditeljski nadzor standardni korisnički račun. Značajka roditeljskog nadzora može se primijeniti samo na standardne korisničke račune. Uz kontrole koje nudi Windows 7 npr. može se instalirati dodatna kontrola zasebnog davanja usluga, npr. filtriranje web-a i izvješćivanje o aktivnostima. Mladima se u operacijskim sustavima može ograničiti pristup i otvaranje točno određenih programa koje trebaju koristiti. OpenDNS omogućuje filtriranje web-stranica kojima korisnik želi pristupiti na temelju unesenih URL adresa. Postoje dvije liste: (1) lista dozvoljenih domena i (2) lista zabranjenih domena. U top deset blokiranih sadržaja OpenDNS-om ulaze: stranice gdje se nalazi pornografija u 85% slučajeva, seksualnost 80,1%, neukusan sadržaj 77,3%, Proxy/ Anonimizer 76,2%, reklamne mreže 69%, golotinja 69,2%, diskriminacija i mržnja 58,7%, donje rublje 58,5%, kockanje 58% i droga 57,3%. U top tri blokiranih web-mjesta ulaze: „Facebook“, „MySpace“, „YouTube“.[14] Na temelju na-vedenog istraživanja također se može zaključiti da postoji ovisnost o cybersex-u, društvenim mrežama, slušanju glazbe, chatu itd., jer nisu bezrazložno OpenDNS-om blokirane i filtrirane stranice u većini slučajeva upravo s tim sadržajem.

9. ZAKLJUČAK

Nije teško zaključiti da će se ispitanici najčešće lažno predstavljati na onim internetskim servisima koje najviše koriste. U organizacijama gdje je provedeno istraživanje (Međimurska županija) nastojati će se pozitivno djelovati na mlade u cilju smanjenja lažnog predstavljanja na internetu. Radom i primjerom je dokazano postojanje nasilja među mladima na internetu i u stvarnosti, te (na temelju rezultata istraživanja) postojanje ovisnosti o internetu u Republici Hrvatskoj i inozemstvu. Slijedeći problem koji se danas nastoji riješiti je suzbijanje ovisnosti mladih o internetu i online igricama. Jedan od načina koji se navodi u radu za suzbijanje ovisnosti mladih o internetu je postavljanjem roditeljskog nadzora od strane informatičkih stručnjaka pomoću

[14] OpenDNS 2010 Report. 2011. URL: http://www.opendns.com/pdf/opendns-report-2010.pdf. (24.6.2011).

opcija operacijskog sustava i OpenDNS-om. Osim toga za zaštitu mladih od ovisnosti o internetu nastoje se provoditi zanimljive akcije, projekti i predavanja kao što su: „Deset dana bez ekrana[15]“, objavljivanje prezentacija o opasnostima na internetu od strane mup-a[16], učestalo objavljivanje članaka o ovisnosti djece na internetu, održavanje predavanja za mlade u školama na temu „Opasnosti na internetu“. U tjednu kada je dan sigurnosti djece na internetu (8.2.), nastavnike informatike u školama navode ravnatelji, voditelji aktiva i predstavnici Agencije za odgoj i obrazovanje na izdvajanje jednog nastavnog sata za tumačenje teme: „Sigurnost djece i mladih na internetu“ mladima, kako mladi ne bi doživjeli jedan od brojnih oblika zlostavljanja koja su navedena u samom radu. Kada je riječ o zaštiti korisničkih računa na e-društvenim mrežama mladih, mladi bi trebali učestalo mijenjati lozinku, te postaviti optimalnu lozinku jake snage. Kako bi se spriječio pokušaj napada preko računala nerijetko se uvode sustavi za upravljanje lokalnom mrežom računala, te se na taj način kontrolira tijek podataka mladih na internetu.

REFERENCES (Literatura)

Bača, M. (2004), *Uvod u računalnu sigurnost*, Narodne novine d.d., Zagreb.

Dragičević, D. (2004), *Kompjuterski kriminalitet i informacijski sustavi*, IBS, Zagreb.

Jeriček, H. (2011), „Internet i ovisnost o internetu u Sloveniji“, *Medijska istraživanja,* God. 8 br. 2, ss. 85-101.

Kurose, F., Ross W. (2005), *Umrežavanje računala*, Računarski fakultet, Wesley.

Miliša, Z., Tolić, M. (2010), „Kriza odgoja i ekspanzija suvremenih ovisnosti“, *Medianali,* Vol. 4 No. 8, ss. 135-146.

Petrić, D. (2002), *Internet uzduž i poprijeko*, BUG & SysPrint, Zagreb.

Pezo, A. (2011), „Na putu k stvarnoj zaštiti djece na internetu“ (31.5.2011).

Sveučilište Masačusets, Bruklin: Politehničko sveučilište, CET, Pearson Addison.

http://dalje.com/hr-hrvatska/zbog-otvaranja-laznog-profila-na-facebooku-maloljetnik-kazneno-prijavljen/362144 (3.6.2011).

OpenDNS 2010 Report, (2011), http://www.opendns.com/pdf/opendns - report-2010.pdf. (24.6.2011).

http://dnevnik.hr/vijesti/hrvatska/skola-spijunira-ucenike-web-kamerom.html.

[15] Projekt predstavljen od Zlatka Miliše.

[16] Ministarstvo unutarnjih poslova Republike Hrvatske.