316.644-057.874(497.11)
343.436:004.738.5
343.45:004.738.5

Doc. dr. Muzafer Saračević
Univerzitet u Novom Pazaru, Departman za računarske nauke
muzafers@gmail.com

msc. Edin Korićanin
Univerzitet u Novom Pazaru, Departman za računarske nauke
edinkoricanin@uninp.edu.rs

NASILJE U INTERNET OKRUŽENJU I OPASNOST OD KRAĐE IDENTITETA: ANALIZA STAVOVA UČENIKA O ELEKTRONSKOM NASILJU I MOGUĆIM PREVENCIJAMA

VIOLENCE IN THE INTERNET ENVIRONMENT AND THE DANGERS OF IDENTITY THEFT: ANALYSIS OF ATTITUDES OF STUDENTS ON ELECTRONIC VIOLENCE AND POSSIBLE PREVENTION

APSTRAKT

U ovom radu opisani su neki od oblika nasilja u internet okruženju. Akcenat je stavljen na zloupotrebe kao što su uznemiravanje, uhođenje i krađa identiteta. U prvom delu rada su navedeni najčešći načini za krađu identiteta. Društvene mreže služe kao paravan za nasilje i krađu identiteta, a pored toga opisani su neki načini uznemiravanja i uhođenja posredstvom elektronske pošte. Navedeni su i neki saveti za delotvornu prevenciju i zaštitu od elektronskog oblika nasilja.

U poslednjem delu rada, navedena je analiza stavova učenika o mogućim zloupotrebama na internetu i prevenciji. Njihovi stavovi su analizirani kroz četiri kriterijuma procene (1. znanje o mogućim opasnostima na internetu, 2. rizično ponašanje na internetu, 3. moguća prevencija i savetovanje, 4. efikasnosti softverskih alata za zaštitu).

Ključne reči: Elektronsko nasilje, krađa identiteta, internet viktimizacija, digitalno nasilje, cyber kriminal.

ABSTRACT

This paper describes some of the forms of violence in the Internet environment. Emphasis is placed on abuses such as harassment, stalking and identity theft. In the first part of the paper are listed the most common methods of identity theft. Social networks are used as a cover for violence and identity theft, and in addition are described certain forms of harassment and stalking through electronic mail. There are mentioned some tips for effective prevention and control of electronic forms of violence.

In the last part of paper is given the analysis of pupils' views on the possible abuse on the Internet and prevention. Their attitudes were analyzed through four evaluation criteria (1: knowledge of the possible dangers on the Internet, 2: risky behavior on the Internet, 3: possible prevention and counseling, 4: efficiency of software tools for protection).

Key words: Electronic Violence, Identity Theft, Internet victimization, Digital violence, Cyber Crime.

UVODNA RAZMATRANJA

Informaciona bezbednost je jedna od najaktuelnijih i najvažnijih tema sa kojom su se danas susreli korisnici i provajderi informacione tehnologije. Sve do nedavno, mnogi korisnici nisu bezbednost posmatrali dovoljno ozbiljno. Oni su verovali da je, ukoliko su njihovi serverski i *mainframe* kompjuteri smešteni unutar zaštićenog objekta kome može pristupiti samo ograničeni broj ovlašćenih korisnika, malo verovatno da će se oni ikada suočiti sa slomom, odnosno, narušavanjem bezbednosti. Međutim, najširа upotreba PC-ja, PDA i bežičnih uređaja, potpomognuta velikim interesovanjem prema korišćenju Interneta i drugih kompjuterskih mreža, dovela je do toga da slika kompjutera koji bezbedno rade na nekoj fizički zaštićenoj lokaciji danas nije ni izbliza toliko realistična kao nekada (Seen, 2007: 832). Otuda i velika zabrinutost izvršnih rukovodilaca, menadžera i ostalih korisnika za što boljim obezbeđenjem sistema.

U skladu sa tim, sprovode se sve radikalnije promene u organizaciji službe informacione bezbednosti. Pitanja informacione bezbednosti i problem zaštite informacija su sa krajnjih margina dospela u situaciju da budu delokrug rada samog top - menadžmenta kompanija. Znači, interesovanje i pažnja koja se u svetu posvećuje informacionoj bezbednosti nisu odraz pomodarskog trenda, već realnost nadolazećeg informacionog društva. Sa narušavanjem poslovnih informacija dolazi do narušavanja i privatnih (ličnih), a samim tim dolazi do pojave tzv. elektronskog nasilja sa kojim se otvaraju vrata raznim zloupotrebama, a među njima su uznemiravanje, uhođenje i krađa identiteta.

Elektronsko nasilje (ili digitalno nasilje) uključuje bilo kakav oblik slanja poruka putem interneta ili mobilnih telefona, a sve sa ciljem povređivanja, uznemiravanja ili bilo kakvog drugog nanošenja štete detetu, mladom ili odraslom čoveku koji ne može da se zaštiti od takvih postupaka (Eoghan, 2001: 356). Pojavljuje se u obliku tekstualnih, zvučnih ili video poruka, fotografija ili poziva.

Termin "*Cyber kriminal*" je širi pojam od elektronskog nasilja, zato što obuhvata širok spektar kriminala kao što su internet nasilje, dela vezana za kršenje autorskih i srodnih prava, dela vezana za sadržaje, dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema itd. (Willard, 2008: 257).

Kompjuterska forenzika (*Cyber* forenzika), je primena naučno dokazanih metoda za prikupljanje, obradu, tumačenje i korišćenje digitalnih dokaza u cilju obezbeđivanja ubedljivog opisa aktivnosti ovog tipa kriminala. Kompjuterska forenzika, takođe, uključuje čin izrade digitalnih podataka pogodnih za uključivanje u krivične istrage. Kada je lopov dobio podatke, računari se često koriste za kreiranje lažne identifikacije, falsifikovanih čekova i drugih dokumenata za činjenje prevare. Kompjuterska forenzika u velikoj meri pomaže policijskim službenicima da identifikuju obe strane, žrtve i počinioce krađe identiteta (Vacca, 2005: 147).

MOGUĆE PRETNJE NA INTERNETU I KRAĐA IDENTITETA

Privatnost na internetu uključuje pravo na zaštitu ličnih informacija u vezi sa čuvanjem, upotrebom, obezbeđenjem od trećih lica i prikazivanje ličnih informacija preko interneta. Zaštita može da podrazumeva i lične identifikacione informacije ili informacije koje se odnose na posetioca određene veb stranice.

Krađa identiteta na Internetu je vrsta prevare kojom se od korisnika računara putem lažne poruke e-pošte ili veb-sajta saznaju lični i finansijski podaci. Internet pruža nove načine za lopove da ukradu tuđe lične informacije i da počine prevaru. Lopovi mogu da postignu svoj cilj na nekoliko načina, kao što je korišćenje Internet čatovanja i trojanskih konja koji služe da sa tuđeg računara pokupe lozinke, korisnička imena i brojeve kreditnih kartica koje korisnik koristi na računaru prilikom registrovanja, prijave na nekom web sajtu ili obavljanja online kupovine i pošalju ih nazad do lopova. Mnogi onlajn biznisi danas, takođe, čuvaju lične podatke o korisnicima i kupcima na svojim veb-sajtovima, i te informacije se koriste kada se osoba vrati na veb-sajt. Ovo predstavlja još jedan način da se pristupi tuđim ličnim informacijama. Pored toga, postoji i tzv. *e-mail phishing*, gde lopovi pokušavaju da prikupe tuđe lične informacije slanjem lažnih e-mailova (Ramzan, 2010: 101). Krađa identiteta na Internetu se može izvršiti na više načina, od kojih su najčešći:

- putem elektronske pošte ili ćaskanjem (eng. *phishing*)
- putem zlonamernog softvera (npr. trojanski konji, *spyware, keyloger…*)
- putem društvenih mreža (*Facebook, Twiter, Linkedin* itd.)

DRUŠTVENE MREŽE KAO PARAVAN ZA NASILJE I KRAĐU IDENTITETA

Istraživanje u akademskoj sredini je pokazalo da društvene mreže funkcionišu na više nivoa, počevši od porodice do nivoa nacije, i igraju kritičnu ulogu u određivanju načina na koji će se neki problemi rešiti, kako će organizacije funkcionisati i stepen do koga će pojedinac uspeti u dostizanju individualnih ciljeva.

Zbog velikog pristupa ličnim podacima korisnika, često dolazi do velike zloupotrebe nad tim podacim. Nisu retki slučajevi, da razni programeri ili hakeri, upadaju u sisteme mreža, gde čine znatne štete, kako i korisnicima, tako i administratorima. Najčešće žrtve su maloletnici, koji su laka meta ovih vrsta zloupotreba (Kovačević & Lepojević, 2009: 6). Upravo zbog sličnih razloga, mnogi od servisa imaju zaštitu za maloletnike, koja im donekle pruža sigurnije korišćenje servisa. Postoji i niz malicioznih stavki, tj. virusa, koji, skrivajući se u obliku marketinga, ili različitih dodataka, mogu upasti u računarski sistem i izvršiti velike štete. Zbog toga, korisnik uvek treba da bude oprezan sa ovim stavkama (Stevanović, 2006: 2).

ELEKTRONSKA POŠTA: UZNEMIRAVANJE I UHOĐENJE

Elektronska pošta se možda čini kao pouzdan način konverzacije između dvoje ljudi, bezbedan od prisluškivanja trećeg lica. Međutim, poruka može biti presretnuta bilo gde u putu između pošiljaoca i primaoca u bilo kom trenutku. Ukoliko šaljete email sa posla, vaš šef može legalno da ima uvid u vašu elektronsku poštu, a ukoliko vaša firma u bilo kom trenutku bude pravno procesuirana, tužilac, ili strana koja vas tuži ima zakonsko pravo da preispita vašu elektronsku poštu, a vi zakonsku obavezu da im je date na uvid. Ako pošaljete email od kuće, hakeri mogu da ga presretnu, ili ukoliko ste pod istragom nadležnih organa, isti mogu zapleniti elektronski zapis uz odgovarajući nalog. Čak i vaš internet provajder legalno može da kontroliše vašu e-poštu.

Elektronska pošta je ranjiva od obe vrste napada - aktivnih i pasivnih. Pasivne pretnje su usmerene na konkretan sadržaj poruke (engl. Release of message contents) i analizu saobraćaja (engl. Disclosure of Information), dok su aktivne usmerene na modifikaciju sadržaja (engl. Modification of message contents), odgovore (engl. Replay), lažno predstavljanje (engl. Masquerade) i nedostupnost usluge.

Neke od zloupotreba putem elektronske pošte (Ramzan, 2010: 126):

Objavljivanje informacija (engl. *Disclosure of Information*): Većina imejlova se trenutno emituje javno, bez enkripcije. Pomoću nekih raspoloživih alata, treće lice može čitati vašu imejl poštu.

Analiza saobraćaja (engl. *Traffic Analysis*): Sumnja se da neke zemlje rutinski prate elektronsku poštu u cilju državne bezbednosti. Ovo rade da bi olakšali borbu protiv industrijske špijunaže i političkog prisluškivanja.

Modifikacija sadržaja (engl. *Modification of message contents*): Poruka može biti promenjena u toku prenosa ili skladištenja.

Lažno predstavljanje (engl. *Masquerade*): Moguće je poslati poruku u ime neke druge organizacije ili neke druge osobe, tj. lažno se predstaviti.

Odgovor na primljenu poruku(engl. *Replay*): Već primljene poruke se mogu poslati nekim novim primaocima. Ovo može dovesti do gubitka, konfuzije ili povređivanja reputacije pojedinca ili organizacije.

Prevara (engl. *Spoofing*): Lažne poruke se mogu ubaciti u sistem drugog korisnika. To može biti postignuto u okviru lokalne mreže ili iz bilo kog drugog okruženja, koristeći virus poznatiji kao trojanski konj.

Nedostupnost usluge (engl. *Denial of Service -DoS*): Može se blokirati sistem za slanje elektronske pošte, tako što će se isti pretrpati sa mailovima. Može se izvesti i slanjem imejla sa trojanskim konjem ili nekim sličnim virusom. Moguće je i blokirati korisnički nalog unošenjem pogrešne lozinke iznova.

SAVETI ZA DELOTVORNU PREVENCIJU OD ELEKTRONSKOG NASILJA

Škola može imati ogroman uticaj i ulogu u podsticanju internet bontona i unapređenju informatičke pismenosti. Informacione tehnologije se uspešno koriste kako za formalni oblik, tako i za neformalni oblik učenja. Uloga škole u ovom slučaju jeste istraživanje i pružanje tačnih informacija u različitim načinima korišćenja interneta u cilju osiguravanja učenicima samopotvrđivanje, asertivnost, participaciju i razvijanje prijateljstava (Diamanduros & Downs, 2008: 5).

Veoma je bitno da se učenicima pokaže, da odrasli, kao digitalne pridošlice, itekako prate sve aktuelne promene u informacionim tehnologijama. Novi oblici komuniciranja pružaju digitalnim pridošlicama uvid u interesovanja digitalnih urođenika. Dakle, nastoji se da se definišu jasna pravila u korišćenju interneta i mobilnih telefona u školskoj sredini.

Pet ključnih oblasti za delotvornu prevenciju od elektronskog nasilja (UNICEF Vodič, 2008):

- Isticanje pozitivnog korišćenja tehnologije.
- Razumevanje i razgovor o modernim načinima komuniciranja i opasnostima elektronskog nasilja.
- Uspostavljanje novih i dorada postojećih pravila i posledica.
- Omogućavanje prijavljivanja elektronskog nasilja.
- Evaluacija uticaja preventivnih aktivnosti.

ANALIZA STAVOVA UČENIKA O MOGUĆIM ZLOUPOTREBAMA NA INTERNETU I MOGUĆIM MEHANIZMIMA KOJI SE ODNOSE NA PREVENCIJU

U ovom delu rada navedena je analiza stavova učenika o mogućim zloupotrebama na internetu i prevenciji. Anketiranje je izvršeno u jednoj osnovnoj školi u Novom Pazaru. Istraživanje ima za cilj da ukaže na statistički značajne mogućnosti podizanja nivoa svesti o mogućim zloupotrebama na internetu i prevenciji od elektronskog nasilja. Istraživanje je sprovedeno u periodu od 18. do 27. novembra 2014. godine. U elektronskoj anketi se prijavilo ukupno36 ispitanika (učenici od 6. do 8. razreda).

Učenici su ocenjivali iskaze ocenom od 1 do 5 (*1 - uopšte se NE slažem, 2 - uglavnom se NE slažem, 3 - neodlučna/an sam, 4 - uglavnom se slažem, 5 - u potpunosti se slažem).* Anketu su popunjavali elektronskim putem na web adresi: http://muzafers.polldaddy.com/s/anketa. Anketa se sastoji od ukupno 20 iskaza, koji su raspoređeni u 4 dela, a svaki deo daje procenu sa različitih aspekata:

1. deo: znanje o mogućim opasnostima na internetu,

2. deo: rizično ponašanje na internetu,

3. deo: moguća prevencija i savetovanje,

. deo: efikasnosti softverskih alata za zaštitu.

Tabele 1-4. Različiti kriterijumi procene

KRITERIJUM PROCENE 1: ZNANJE O MOGUĆIM OPASNOSTIMA NA INTERNETU	1	2	3	4	5
Internet je bezbedno okruženje ako se koristi odgovarajući anti-virus softver	22	9	1	2	2
Elektronska pošta je bezbedan web servis	21	10	1	2	2
Slanje poruka neprimerenog sadržaja nije dozvoljeno na društvenim mrežama	25	7	2	1	1
Objavljivanje privatnih podataka ili neistine na četu, blogu ili internet stranici ne spada u internet nasilje	12	8	10	3	3
Prosleđivanje tuđih fotografija ili bilo kakvog sadržaja o drugome sa zahtevom za komentarisanje ne spada u krađu identiteta	18	10	6	2	0
Ukupno 36 učenika	**54.44**	24.44	11.11	5.56	4.44
KRITERIJUM PROCENE 2: RIZIČNO PONAŠANJE NA INTERNETU	1	2	3	4	5
Dok se dopisujem nemam uvek na umu mogućnost lažnog predstavljanja sa druge strane.	21	8	1	4	2
Otišao/la bi na sastanak s osobom koju sam upoznao/la putem mobilnog, na društvenoj mreži, četu ili putem bloga.	23	8	0	1	4
Uvek šaljem fotografije o sebi, svojoj porodici i prijateljima, jer smatram da ih ne mogu zloupotrebiti	17	7	0	9	3
Uvek brišem s mobilnog podatke i fotografije koje mi je neko poslao jer mislim da pomoću njih policija neće brže pronaći osobu koja mi preti.	29	5	0	2	0
Ne tražim pomoć od drugih da ne bi pomislili da sam učinio nešto nedopušteno	22	6	1	3	4
Ukupno 36 učenika	**62.22**	18.89	1.11	10.56	7.22
KRITERIJUM PROCENE 3: MOGUĆA PREVENCIJA	1	2	3	4	5
Javnost u Srbiji je dobro upoznata sa pojmom cyber - elektronsko nasilje	18	12	3	2	1
Deca nisu kategorija internet korisnika koja je najugroženija, već kompanije	24	8	3	1	0

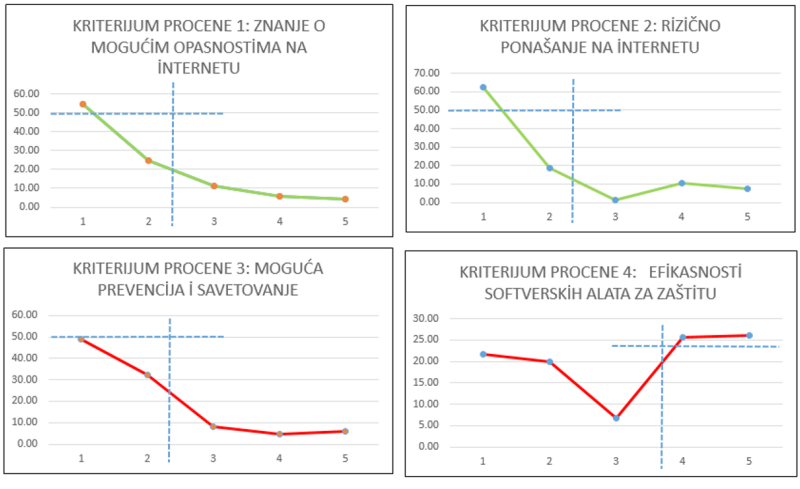
Radionice pri školama nisu najbolji oblik edukacije iz oblasti prevencije elektronskog nasilja već informativni članci u medijima i internet kampanje	17	10	5	2	2
Neće mnogo pomoći u borbi protiv elektronskog nasilja u Srbiji ni mreža javnih institucija i nevladinih organizacija	15	12	0	2	7
Veliki gradovi (Beograd, Novi Sad, Niš,..) su delovi Srbije gde su najneophodnije edukacije iz oblasti prevencije elektronskog nasilja	14	16	4	1	1
Ukupno 36 učenika	**48.89**	32.22	8.33	4.44	6.11
KRITERIJUM PROCENE 4: EFİKASNOSTİ SOFTVERSKİH ALATA ZA ZAŠTİTU	1	2	3	4	5
Smatram da mi nije potrebna softverska zaštita zato što ne ostavljam svoje podatke na internetu i ne ponašam se rizično	14	15	1	4	2
Više koristim softverske alate (aplikacije) koje besplatno preuzimam sa interneta od komercijalnih	4	5	0	12	15
Smatram da preko elektronske pošte ne mogu biti ugrožen zato što postoji uključen softver unutar internet pretraživača koji me štiti	9	7	3	11	6
Facebook je bezbedan kada je u pitanju opasnost od krađe identiteta zato što postoji automatizovan softver koji briše duplikate	7	5	5	8	11
Smatram da me antivirus koji trenutno imam štiti u potpunosti od svih oblika nasilja i krađe identiteta u internet okruženju	5	4	3	11	13
Ukupno 36 učenika	21.67	20.00	6.67	**25.56**	**26.1**

DISKUSIJA I ZAKLJUČNA RAZMATRANJA

Ako analiziramo pojedinačne rezultate, za svaki kriterijum procene, možemo videti da preko 50% učenika poseduje dovoljno znanja o mogućim opasnostima na internetu (kriterijum 1), a preko 60% učenika zna kada se rizično ponaša na internetu (kriterujim 2). Svakako je važno staviti akcenat na podizanje svesti kod dece i njihovih roditelja na sve moguće pretnje kada

se koriste moderne tehnologije u ostvarivanju komunikacije sa drugima. Potrebno je definisati posledice i sankcije za sve one koji krše pravila ili čine nasilje. Takođe je veoma bitno da se učenicima i njihovim roditeljima pruži podrška od strane škole, za bilo kakav oblik nasilja, čak i u slučajevima kada se nasilje dogodilo izvan škole.

Međutim, iskazi u okviru kriterujma br.3 su ispravno ocenjeni ispod 50%, odnosno većina ne zna na pravi način da potraži pomoć i pravi savet za delotvornu prevenciju od elektronskog nasilja. Na osnovu dobijenih rezultata dolazimo do zaključka da prijavljivanje nasilja može biti težak korak, kako za one osobe koje trpe nasilje, tako i za posmatrače. Zato se nastoji da se i učenici i njihovi roditelji upoznaju sa različitim načinima prijavljivanja elektronskog nasilja u školi i među učenicima. Radnici škole i stručni saradnici moraju biti upoznati sa mogućnostima prijavljivanja i kome je potrebno obratiti se u takvim situacijama. Iskazi u okviru kriterujma br.4 su ispravno ocenjeni ispod 25%, što opet govori o slaboj upućenosti učenika u oblast primene softverskih alata za zaštitu i njihovu pouzdanost i efikasnost.



Grafikoni 1-4.
(1) znanje o mogućim opasnostima na internetu, (2) rizično ponašanje na internetu, (3) moguća prevencija i savetovanje, (4) efikasnosti softverskih alata za zaštitu.

Na osnovu zbirnih rezultata za sve četiri procene (Tabela 5), možemo videti da su 10.97 % učenika izjasnilo da se u potpunosti slažu sa navedenim iskazima, dok 11.53% učenika se delimično slaže sa navedenim iskazima. Pošto su iskazi formulisani u formi koja je suprotna od ispravnog odgovora,

dolazimo da rezultata da oko 22% učenika nije baš najbolje upućeno u oblast elektronskog nasilja i da bi se trebalo poraditi na dodatnoj edukaciji.

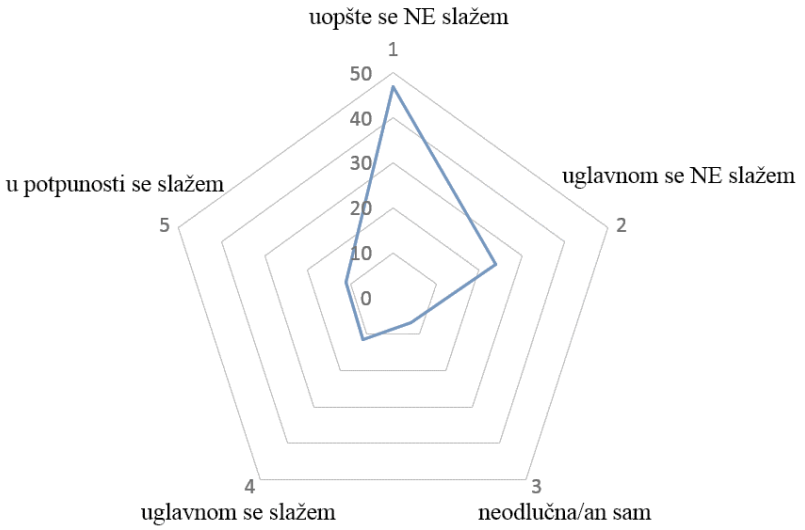
Sa druge strane, čak 46.81 % učenika je negiralo date iskaze, odnosno izjasnili su se da se u potpunosti ne slažu sa navedenim iskazima, dok 23.89% učenika se delimično ne slaže sa navedenim iskazima. Dolazimo da rezultata da oko 70% učenika bi znalo da prepozna oblik elektronskog nasilja. Tabela 5 daje detalje po broju selektovanih procena (od 1 do 5) za sva četiri kriterijuma.

Tabela 5. Sumirani rezultati za sve 4 procene

Kriterijum procene:	1	2	3	4	5
1: Znanje o mogućim opasnostima na internetu	54.44	24.44	11.11	5.56	4.44
2: Rizično ponašanje na internetu	62.22	18.89	1.11	10.56	7.22
3: Moguća prevencija i savetovanje	48.89	32.22	8.33	4.44	6.11
4: Efikasnosti softverskih alata za zaštitu	21.67	20	6.67	25.56	26.11
%	**46.81**	**23.89**	**6.81**	**11.53**	**10.97**

Iz navedenog anketiranja, dolazimo do zaključka da je neophodna dodatna edukacija o nasilju u internet okruženju. Ono što je važno, jeste da se pruži tačan uvid u samu defniciju elektronskog nasilja, odnosno bitno je naglasiti po čemu se elektronsko nasilje razlikuje od drugih oblika nasilja, koje su njegove specifičnosti i kakvi su uticaji takvog oblika nasilja. Potrebno je osmisliti i odrediti jasna pravila i dosledno ih se pridržavati. Svakako se preporučuje vođenje evidencije o iskustvima učenika putem interneta, odnosno napraviti evaluaciju uticaja preventivnih aktivnosti (Istraživanje: Bezbednost dece na Internetu, 2009). Redovne provere su veoma važne u cilju utvrđivanja da li su preventivne strategije uspešne i primerene učeničkim potrebama. Korisno je podeliti materijale i preneti informacije o preduzetim merama, postignutim rezultatima, ali i aktuelnim izazovima i pitanjima s celom školskom zajednicom.

Na Grafikonu 5 je prikazan procentualni udeo ocena za sva četiri kriterijuma.



Grafikon 5. Sumirani rezultati za sva 4 kriterijuma (%)

Vrednosti i pravila koja postoje u školi za vršnjačko nasilje je potrebno primeniti i na nasilje u elektronskim medijima. UNICEF je, pre pet godina, započeo javnu kampanju protiv vršnjačkog zlostavljanja, a već četiri godine se u školama sprovodi njegov program „Za sigurno i poticajno okruženje u školi". Do sada se u program uključilo više od 250 osnovnih i srednjih škola. Eksterna evaluacija pokazala je da program uspešno smanjuje količinu vršnjačkog zlostavljanja i uspostavlja sigurnije okruženje za decu. Elektronsko zlostavljanje nije do sada bilo obuhvaćeno programom, jer je relativno nov oblik zlostavljanja, kako vršnjačkog tako i opšteg.

Bitno je napomenuti da specifičnosti okruženja na Internetu, čine elektronski vid zlostavljanja sve rasprostranjenijim, po nekim mišljenjima, čak i opasnijim po psihološku ravnotežu žrtve od tradicionalnog vršnjačkog zlostavljanja. Zaključak je da internet okruženje ne pruža dovoljno povratnih informacija o reakcijama onoga kome su uznemiravajuće poruke poslate, što kod zlostavljača smanjuje osećaj da nanosi istinsku emotivnu i psihološku štetu drugoj osobi, smanjujući stepen samokontrole i uvida u stepen nasi