CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost djece na Internetu

CCERT-PUBDOC-2008-06-230

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Internet je definitivno revolucionarni događaj u povijesti čovječanstva. Njegova se korisnost ne iscrpljuje na tome da svatko može bilo kada od bilo kuda doći do bilo koje objavljene informacije te komunicirati s bilo kime (sinkrono ili asinkrono). Posebnu, revolucionarnu važnost ima činjenica da u suštini:

- nitko nikoga ne može spriječiti da objavi bilo što, čitavom svijetu;
- nitko nikoga u suštini ne može spriječiti da dođe do bilo koje objavljene informacije te da
- pojedinac može obavijest poslati tisućama ljudi u trenu, bez ikakvog dodatnog utroška vremena ili novca, kao da šalje samo jednom primatelju.

Ova svojstva omogućavaju nikad ranije viđenu slobodu izražavanja, kao i mogućnost učenja te stvaranja i djelovanja interesnih skupina bez ikakvih prostornih ili društvenih ograničenja.

Nuspojava je i to da pojedinac može biti praktično potpuno anoniman, te stvarati višestruke, prividne identitete.

Sve prekrasne mogućnosti koje proizlaze iz ovih svojstava imaju i tamnu stranu. Kao i svaka druga tehnologija, i Internet se može zloupotrijebiti. Čovjek ju može pogrešno ili zlonamjerno upotrijebiti protiv sebe sama, ali i protiv drugih ljudi.

„Internet safety“ ili „e-safety“ je novi pojam koji se odnosi na korištenje IKT (informacijske i komunikacijske tehnologije) na takav način da se nađe prihvatljiva sredina između

- osobnog prava da se pristupi informaciji i da se objavi informaciju te
- prava da se bude zaštićen od štetnih posljedica korištenja IKT.

Djeca brzo uče i prihvaćaju "novotarije", puno brže i lakše od odraslih. Tipična situacija u gotovo svakoj obitelji je da djeca koriste širi spektar tehnologija i usluga dostupnih Internetom nego njihovi roditelji (i učitelji). Istovremeno, oni nemaju ni znanja, ni iskustva ni zrelosti raspoznati istinu od laži, usporediti i vrednovati oprečne informacije te zaštititi sebe, obitelj, prijatelje i zajednicu.

Stoga je sigurnost djece na Internetu posebno važna i predmetom važnih projekata uglednih organizacija ili međunarodnih tijela [1].

Ovaj dokument je namijenjen prije svega roditeljima i učiteljima. Napisan je tako da i djeca mogu razumjeti rizike, ugroze i napade.

Cilj dokumenta je približiti uzroke i posljedice, osnovna svojstva tehnologije i dati pravu mjeru ulozi zaštitnih tehnika i sustava odgoja i obrazovanja.

2. Aktivnosti

Kad se razmišlja o aktivnostima koje djeca izvode koristeći Internet obično se misli na elektroničku poštu i pretraživanje. Međutim, paleta je bitno bogatija i dnevno se dopunjuje i proširuje.

2.1. Pretraživanje

Najčešći oblik korištenja Interneta, jednako za odrasle i za djecu, je pretraživanje sadržaja korištenjem tzv. pretraživača ili tražilica poput: Google, Yahoo, Altavista, ...

Problem je u tome što se traženjem legitimne, benigne informacije, dobivaju i reference na druge oblike: pogrešne, neispravne, lažne, zlonamjerne. Korisnik stoga mora imati dovoljno znanja, ali i zrelosti da provjeri, usporedi i ocijeni informaciju. Ponekad njenu točnosti i istinitost nije moguće sa sigurnošću utvrditi. Tada je važna sposobnost prihvaćanja i korištenja informacije s dozom opreza. Ovo vrijedi i za odrasle i za djecu, no djeca nemaju znanje i iskustvo, a ni zrelost odraslih, pa su ranjivija. Stoga

informacijska pismenost ovog tipa (ne samo baratanje softverskim alatima) mora biti posebno važan dio nastavnog plana i programa.

Drugi način traženja informacija je formiranje upita u bazama podataka. Najčešće korišteni javni servisi su: wikipedia, encarta, webopedia, encyclopedia britanica, ...

Treći je oblik pretraživanje knjižnica kojima se dolazi do informacije o postojanju nekog teksta, čak i sažetaka ili izvoda cijelog teksta. Nakon toga je moguće preko uobičajenih tražilica pronaći puni digitalni tekst. Ako ne postoji ili je zaštićen, ljudi često koriste neku od mreža koje ilegalno nude digitalne verzije tekstova na kojima postoji zaštita autorskog prava.

2.2. Razgovor

Druga glavna aktivnost svih korisnika Interneta je "razgovor". Najčešće je on u tekstualnom obliku.

Dok odrasli najčešće koriste elektroničku poštu, djeca su sklonija tzv. "Instant messagingu" kojeg u mobilnim komunikacijama predstavljaju SMS (eng. Short Message Service) poruke, a u Internetu: chat, news grupe i sl.

Sve intenzivnije se koriste i govorne komunikacije, najčešće Skype sustavom koji nudi funkcionalnost glasovnog telefoniranja putem Interneta.

Video telefonija, tj. sinkrona komunikacija zvukom i pokretnom slikom je danas krajnje jednostavna i jeftina, a sve je više alata koji (besplatno) omogućavaju istovremeno komuniciranje više sudionika.

2.3. Izvođenje programa

Treća skupina aktivnosti su pokretanja i izvođenja računalnih programa.

Programe možemo izvoditi lokalno, na vlastitom računalu ili računalu u školi, knjižnici ili kojem drugom javnom mjestu.

Program koji izvodimo mogli smo dobiti na CD/DVD mediju ili USB memoriji, odnosno mogli smo ga preuzeti s Interneta.

Programi se mogu izvoditi i na udaljenom računalu, tzv. poslužitelju. To se može učinit izravno, ako se prijavimo kao korisnik tog računala i u terminalskom radu pokrećemo programe. Češće je slučaj da programe pokrećemo posredno, dajući izravne ili neizravne naredbe odgovarajućem softveru na poslužitelju koji zatim u naše ime izvodi programe. Čak je moguće poslužitelju poslati program s našeg lokalnog računala i zatražiti da ga izvede.

Problem s izvođenjem programa je u tome da mi zapravo ne znamo što oni rade.

Čak i kad su stvarno napravljeni za funkciju koju mi trebamo, ne možemo znati, rade li istovremeno još nešto što nama možda ne odgovara.

Naime, ti programi mogu biti neispravni, pa mogu učiniti štetu podacima na računalu, drugim programima, komunikacijama i cijelom sustavu.

Pored toga, mogu biti dopunjeni zlonamjernim potprogramima koji će istovremeno dok program naizgled radi nešto korisno za nas, izvoditi napad ili ilegalno prikupljanje podataka.

3. Napadači

Napadači na sigurnost djece mogu biti razne osobe, iz raznih pobuda. Oni to mogu raditi svjesno i namjerno ili bez svjesne namjere da ugroze sigurnost djeteta koje postaje žrtva njihovog napada.

3.1. Djeca

Djeca su najčešći "napadač" na drugu djecu. Prije svega zato što najčešće međusobno komuniciraju te zato što čine zajednicu u kojoj jedni drugima potvrđuju status i odnose.

Upravo od druge djece oni saznaju za informacije koje nisu primjerene njihovom uzrastu, za alate koji su neprovjereni, sumnjivi, štetni ili ilegalni.

Namjerno ili nehotice, svojim aktivnim sudjelovanjem na Internetu, komuniciranjem i objavljivanjem informacija, djeca će povrijediti svoje kolege ili nepoznate, davanjem ili prenošenjem netočnih, pogrešnih ili lažnih informacija. Ovo je djelovanje poznato pod nazivom "cyber bullying".

Poticat će kolege na aktivnosti koje su nezakonite, nemoralne ili neprimjerene djeci, bez obzira bave li se sami tim aktivnostima. To će ponekad raditi izravnim poticanjem, a ponekad neizravnim. Ponekad se to pretvara i u pritisak: dijete je prisiljeno, odjeća se obveznim ili je ucijenjeno (ili se tako osjeća) i zbog toga izvodi aktivnosti .za koje samo nema interes, potrebu, ili hrabrost.

3.2. Lopovi

Lopovi jednostavno žele prisvojiti nešto tuđe kako bi ostvarili korist za sebe, često materijalnu. Djecu uglavnom iskorištavaju kao posrednika, najčešće da dođu do informacije koja će im omogućiti krađu.

"Obični" lopovi mogu od djece pokušati saznati kad će obitelj biti na dopustu, a stan ili kuća bez nadzora kako bi provalom otuđili vrijednosti. Mogu pokušati saznati i brojeve kreditnih kartica, lozinke i druge podatke putem kojih će pokušati ostvariti korist.

"Cyber criminals" će od djece pokušati saznati što više privatnih podataka o njihovim roditeljima, učiteljima ili drugim osobama što će im pomoći u pokušaju da pogode šifre, običaje korištenja elektroničkih usluga i poslovanja kako bi se uspješno lažno predstavljali kao žrtva (u pravilu odrasla osoba) koju napadaju.

Ako se radi o djeci javnih osoba, privatne informacije o roditeljima, obitelji, susjedima ili prijateljima iz razreda koja su djeca slavnih osoba, pokušat će prodati žutom tisku, drugim lopovima, teroristima ili drugim napadačima.

Osim toga, lopovi će vrlo rado iskoristiti djecu da za njih obave dio posla. Naime, profesionalci dobro znaju da je tragove teško zametnuti i da se na većini poslužitelja sve aktivnosti bilježe u dnevnike. To znači, da će se napad na sigurnost nekog računala moći kasnije analizirati i pratiti trag do počinitelja.

Stoga profesionalci, umjesto da sami provale na računalo žrtve, nagovore prevarom dijete da to učini za njih. Na primjer, naizgled nedužnim razgovorom na chatu o najnovijim fotografijama sonde s Marsa, zainteresirat će dijete da ih vidi, te ga uputiti na računalo na kojem se (tobože) nalaze. Dijete će se ubrzo ponovo javiti lopovu s tužnom vijesti da je za ulaz u računalo potrebna lozinka. Lopov će ju susretljivo ponuditi, ili objasniti kojim alatom dijete i samo može pronaći lozinku. Nakon što dijete provali i preuzme informacije, one se nalaze na njegovom osobnom računalu. Na tom računalu su sustavi zaštite u pravilu slabi, ako uopće postoje, a dnevnici korištenja su manjkavi ili ih nema. To znači, da lopov može bez straha kopirati podatke koje je dijete kopiralo sa žrtvinog računala. Naime, kad istražitelji počnu pratiti trag napada, on će ih dovesti do računala djeteta, ali na najmu dalje više neće pronaći tragove lopova koji je dijete nagovorio i preuzeo žrtvine podatke.

3.3. "Ideolozi"

Rasisti, nacionalisti, vjerski fanatici i pripadnici sekti i kultova Internetom imaju prilike proširiti svoje "učenje" do velikog broja potencijalnih sljedbenika.

Lukava retorika njihovo je oružje kojim pokušavaj uvjeriti u "svoju stvar" buduće sljedbenike.

3.4. Nasilnici

Nasilnici su ljudi koji nalaze zadovoljstvo maltretiranjem slabijih od sebe.

Slabiji su u fizičkom ili tehničkom smislu, emocionalnom ili intelektualnom.

Možda je najjednostavnija definicija nasilništva: "činiti nekome nešto što ga smeta samo zato što ti to možeš, a on se ne može od toga obraniti".

Nasilnici u Internetu imaju pregršt metoda da gnjave druge korisnike: porukama koje primatelj nije tražio (SPAM), napadima kojima uskraćuju usluge legitimnim korisnicima (Denial of Service napad), širenjem neistinitih informacija, mijenjajući poruke ili web stranice legitimnih korisnika tako da okrnje ugled izvornog autora ili onoga o čemu tekst govori i sl.

3.5. Trgovci robljem

Za trgovce robljem (i organima) prilično je lako neinformiranu i nepripremljenu djecu dovesti do toga da im pokažu kako izgledaju, gdje i kada se kreću i na koji su način (ne)zaštićeni, što će im omogućiti da odaberu buduće žrtve i relativno lako i uz minimalni rizik ih otmu i prodaju.

3.6. "Crackeri"

"Crackerima" se nazivaju osobe koje provaljuju u tuđe informacijske sustave, bez obzira rade li to zbog novca, slave, užitka, eksperimenta.

Treba ih razlikovati od hakera koji su pasionirani istraživači informacijske tehnologije i sustava, ali nikad ne pređu crtu između onog što je legalno i onog što nije.

Izvjestan problem predstavlja način razmišljanja: "Ako nikome ne štetim, onda smijem raditi i ono što, strogo govoreći, nije dozvoljeno zakonom".

Naime, taj način razmišljanja je onaj "tobogan" kojim se haker prebacuje u crackera. Najjednostavniji je primjer, kad se razmišlja na sljedeći način: "našao sam nezaštićeno računalo, na kojem korisnik gotovo ništa ne radi. On neće imati štete ako ga ja malo koristim za svoje potrebe, dok ga on ne koristi."

Crackeri za djecu mogu biti opasni na dva načina.

Prvi je kad napadnu računalo koje dijete koristi, i kopiraju osobne podatke s njega. Čak i ako oni sami neće zloupotrijebiti te podatke, od njih se podaci, uz njihovu volju ili bez nje, mogu proširiti do onih koji će te podatke zlorabiti.

Druga opasnost je kad (s dobrom ili zlom namjerom) svoja znanja, metode i alate za provaljivanje i zlouporabu informacijskih sustava dijele s "običnom" djecom, koja će ih onda upotrijebiti iz znatiželje, neznanja ili nekog drugog razloga te se dovesti u situaciju da čine nezakonita, nemoralna ili jednostavno štetna djela.

3.7. Seksualni prijestupnici

Seksualni prijestupnici mogu se zadovoljiti "samo" time da nagovore dijete da im pošalje svoje fotografije ili da uključi web kameru i uživo prenosi svoju sliku.

Na tome ne mora stati već se njihova aktivnost može preseliti i u fizički svijet. Mogu namamiti dijete na sastanak s njima radi seksualnih aktivnosti koje nisu primjerene djetetu.

3.8. Teroristi

Teroristi mogu, kako bi ispunili svoju višu svrhu, imati za cilj oteti dijete, poput trgovaca robljem, prikupiti informacije o drugim ciljevima poput lopova ili vrbovati nove sljedbenike poput "ideologa".

4. Rizici, ugroze i napadi

Velik je broj rizičnih situacija koje su moguće za svako dijete koje koristi internet. U stvari to je umnožak kombinacija aktivnosti koje djeca provode i vrsta napadača.

Radi preglednosti i stjecanja uvida u osnovne rizike napravljena je pojednostavljena podjela.

4.1. Pristup neprimjerenim informacijama

Kad se govori o sigurnosti djece na Internetu prva stvar koja većini ljudi padne na pamet je pornografija.

Dakle, radi se o "obitelji" rizika koji se odnose na pristup djece sadržajima koji nisu primjereni njihovom uzrastu: stupnju znanja, razvoja i zrelosti. Ovdje zasigurno možemo pribrojiti informacije vezane uz oružje, droge pa i lijekove, financije i sl.

U poglavlju o metodama zaštite diskutiraju se mehanička rješenja koja imaju vrlo ograničenu učinkovitost i dvojbenu korist. Pravo rješenje ovog problema leži u odgovarajućem obrazovanju i odgoju mladih, al i njihovih roditelja i učitelja koji bi trebali nastojati imati stalan i kvalitetan kontakt s djecom koji uključuje diskutiranje i takvih, rubnih (za kompetencije djece) tema.

Poseban problem predstavlja činjenica da je mjerilo primjerenosti nekog sadržaja za neki dječji uzrast pitanje lokalne (ili nacionalne) kulture i običaja. Što je u jednoj kulturi tabu tema, u drugoj je javna stvar.

4.2. Bavljenje nezakonitim, nemoralnim ili neprimjerenim aktivnostima.

Čak i kad ih nitko izravno ne napada, djeca mogu biti ugrožena samom aktivnošću koju provode.

Djeca mogu raditi nezakonite, nemoralne ili neprimjerene stvari čak i kad ih nitko nije nagovorio i kad ih nitko izravno ne poučava.

Kopiranje autorskih djela bez plaćanja naknade najjednostavniji je i daleko najrašireniji oblik nezakonite aktivnosti. Rijetko koji roditelj će ju danas u našim krajevima prepoznati kao posebno opasnu aktivnost, ili kao napad na svoje dijete.

4.2.1. Nezakonite aktivnosti

Zna se da je provala na tuđe računalo nezakonita, pa ipak u prevelikom broju slučaja roditelj će osjetiti ponos zbog "sposobnosti" svog djeteta. Svjedoci smo senzacionalističkih i navijačkih objava u medijima kad neki "naše gore list" provali u računalo kakve ugledne svjetske organizacije (npr. 15-godišnji zadranin Vice Mišković uz pomoć alata kojeg je pronašao na Internetu u veljači 1997. godine provaljuje u Pentagon, bazu Anderson AFB).

Prava je istina da u većini tih slučajeva dijete i ne posjeduje posebna znanja, već je samo slijedilo upute koje je našlo negdje na Internetu ili ih je dobilo od "prijatelja" s kojim razgovara na chatu [vidi 3.2].

Osim provale, djecu je lako nagovoriti i na pokretanje programa sa svog računala za koje ne znaju što uopće rade ili koji naizgled rade nešto korisno, ali istovremeno napadaju nekog trećeg.

4.2.2. Nemoralne aktivnosti

U nemoralne aktivnosti svakako ubrajamo nasilničko ponašanje prema vršnjacima te odraslima koji slabije koriste tehnologiju ili koji su javno eksponirani. Širenje neistina, otkrivanje privatnih informacija i sl. aktivnosti su metode koje djeci znaju biti zabavne jer ne razmišljaju o žrtvi i ukupnim posljedicama.

„Cyberbullying“ je nasilničko ponašanje korištenjem IKT. Brojni su pojavni oblici:

- agresivno emitiranje uvredljivih, ponižavajućih i drugih napadačkih poruka prema žrtvi, često i kroz nekoliko komunikacijskih kanala;
- objavljivanje intimnih, privatnih informacija o žrtvi;
- objavljivanje neistina i laži o žrtvi;
- krađa identiteta žrtve i napadanje drugih;
- krađa identiteta žrtve i izvršavanje nečasnih ili nezakonitih aktivnosti;
- uništavanje informacijskih resursa žrtve (provala u računalo i brisanje podataka)
- onesposobljavanje žrtvinih resursa (poplava komunikacijskih poruka koja sprečava normalan rad);
- isključivanje pojedinca iz privatnih krugova komunikacija i aktivnosti koje bi morao ili trebao smjeti sudjelovati itd.

Dodatni problem nasilničkog ponašanja je i taj što će nerijetko i ono dijete koje je žrtvom nasilništva, također pribjeći nasilju i izvršiti ga nad napadačem ili nekom drugom nedužnom žrtvom. Jedan od važnih faktora koji pridonose ovom, u osnovi osvetničkom ponašanju, jest i percepcija anonimnosti, tj. (pogrešno) vjerovanje da se nasilje na Internetu može raditi anonimno [vidi 5.3.2].

Iako djeca ovakav oblik nasilničkog ponašanja najčešće usmjeravaju prema svojim kolegama i poznanicima, posebnu privlačnost ima ovaj tip nasilništva i prema odraslima, posebno onima za

koje djeca osjećaju da imaju neku moć nad njima. Djeca imaju osjećaj da primjenom IKT mogu izvršiti savršenu osvetu, postići pravdu, ispraviti nepravdu.

4.2.3. Neprimjerene aktivnosti

Neprimjerene aktivnosti također mogu naići na odobravanje neupućenih roditelja. Primjerice, kad 13-godišnjakinja „dođe u novine" jer uspješno trguje na svjetskim burzama, rijetko je to zbog njene duboke upućenosti u financijske tijekove i sveobuhvatnog poimanja svjetske ekonomije i tržišta kapitala.

Čak i kad bi tome bilo tako, radilo bi se o iznimci koja nikako ne može biti opravdanjem da se (sva) djeca bave burzovnim poslovanjem.

U neprimjerene aktivnosti ubrajamo sve one koje nisu, strogo govoreći, nezakonite, ali djeca nemaju dovoljno znanja ili zrelosti da se njima bave, što može rezultirati neželjenim posljedicama. Ovdje se ubrajaju igre na sreću, angažiranje na poslovima koji se nude putem Interneta, prikupljanje informacija o trećim osobama, ali i lažno predstavljanje kao punoljetne osobe s iskustvom u nekom području te davanje savjeta onim koji ih trebaju, a misle da ih dobivaju od odraslih stručnjaka.

4.3. Odavanje privatnih informacija

Djeca su jednostavan, brz i nezaštićen medij kroz koje beskrupulozan i iskusan napadač može saznati obilje privatnih i inače zaštićenih informacija o njihovim roditeljima, prijateljima ,susjedima i učiteljima.

Metode socijalnog inženjeringa [2] izuzetno su uspješne i na odraslima upravo kod dobronamjernih ljudi. Djeca su dobronamjerna i znatiželjna, a time još lakši plijen.

4.3.1. Identifikacijske informacije

Kao predradnja kasnijim provalama u računala, prisluškivanjima komunikacija i lažnom predstavljanju, napadači moraju prikupiti što više stvarnih, privatnih informacija o žrtvi.

Predstavljajući se kao znatiželjni vršnjak, ili nudeći nagrade lako će u svega nekoliko kontakata saznati sve ključne riječi koje bi tipični korisnik mogao upotrijebiti kao svoju lozinku, identifikacijske brojeve i kodove i slične podatke koji su potrebni kod potvrđivanja autentičnosti korisnika putem npr. telefonske autorizacije u banci ili drugdje.

4.3.2. Financijske informacije

Lopovima, teroristima i drugima je posebno zanimljivo saznati imovinsko stanje žrtve. Nije potrebno postaviti izravno pitanje o imućnosti obitelji (na koje djeca ionako teško mogu dati mjerljiv odgovor), ali je nizom razgovora vrlo brzo moguće procijeniti stambene prilike, vrstu radnog mjesta, pokretnine i druge komponente imovinskog stanja.

4.3.3. Sigurnost obitelji

U slučajevima planiranja pljačke, otmice, ili sličnih napada, napadačima je jako važno znati osobne navike članova obitelji: vremenski raspored odlazaka i dolazaka, osobe koje priskaču u pomoć kad treba, oružje u kući, alarmni sustavi, i sl.

4.4. Ovisnosti

Nekoliko se desetljeća zabrinuto diskutira o tome kako je televizija zamijenila društveni život djece, roditelje i učenje. Sve se češće na isti način govori i o Internetu.

Ovisnost o Internetu je i znanstveno potvrđena [3].

Kao i druge ovisnosti, ona gotovo nikad nije nastala sama od sebe ,već je odraz pojedinčevih problema i nesnalaženja u njihovom rješavanju.

Internet je čaroban svijet prepun mogućnosti i u njemu se lako izgubiti. Jednostavno se izolirati (od problema ili strahova), a istovremeno biti jako aktivan.

Štoviše, oni koji imaju potrebu za društvenim kontaktom, ali u stvarnom životu osjećaju razne prepreke, u prividnom svijetu mogu graditi i svoje prividne identitete i osjetiti se potpuno zaštićenima te takvi stupati u kontakte. Privlačnost takvog svijeta je golema.

To samo po sebi ne mora biti loše. Naime, građenjem prividnih identiteta i intenzivirajući tako kontakte s drugima, dijete gradi svoje iskustvo i smanjuje neke inhibicije. Štoviše, to ga može ohrabriti da smjelije kontaktira i u stvarnom životu.

Međutim, nekima se puno lakše potpuno zatvoriti u svoj prividni svijet.

Oblici mogućih ovisnosti su brojni, a mnogi će se tek razviti.

4.4.1. Igre

Računalne igre su možda najpoznatiji oblik ovisnosti. One omogućuju djetetu nešto što mu često i škola i obitelj ne uspijevaju dati: da u svakom slijedećem koraku bude sve bolji.

Dok djeca iz škole prečesto odlaze s osjećajem da ima još nešto što ne znaju i ne mogu (uz sve takvo s čime su došli jutros u školu), dok obitelj često od njih traži previše, a premalo stigne dati, računalne igre skoro zajamčeno nude uspjeh ako se dovoljno dugo trenira.

Pri tome nije potrebno trenirati cijele godine da bi se na kraju dobilo zadovoljstvo, već se osjećaj uspjeha dobiva iz sata u sat, iz minute u minutu.

Uspjeh je mjerljiv, često u brojkama, i osoban.

4.4.2. Kockanje i klađenje

Na Internetu je sve veći broj mogućnosti igara na sreću. Istina, potrebna je kreditna kartica da bi se otvorio prvi ulog, ali nakon toga, uz malo sreće, igrati se može dugo.

Kako je cijela današnja civilizacija okrenuta materijalnom uspjehu koji glorificira, a kako su moderne ikone koje se serviraju djeci u pravilu do blagostanja došle brzim i kratkim postupkom planetarnog uspjeha i slave, jedino kockanje i klađenje može dati nadu mladima da i oni mogu tako.

Slast dobitka "iz ničega" je opojna, pa može u potpunosti zaokupiti dječji duh.

4.5. Indoktrinacije

Pojedinci i grupe koji žele steći sljedbenike svojih "ideologija" kroz Internet imaju snažno sredstvo masovne, ali i pojedinačne komunikacije te mogućnost gradnje virtualnih identiteta po volji: mogu biti istovremeno i buntovnici i proroci, i spašeni i spasitelji, i ratnici i žrtve.

Mladi su rijetko u sredini: oni vole ili biti što sličniji nekoj skupini, ili što različitiji od drugih u okolini.

Kroz Internet pri ruci im je pregršt ideologija da im u tome pomognu.

4.5.1. Rasizam

Rasizam počiva na misli o tome kako je upravo odabrani pojedinac poseban, bolji. Kako je pripadnik "odabranih" onih koji imaju po rođenju neka posebna svojstva, a time i prava. U svakom slučaju, „oni vrijede više od drugih“.

4.5.2. Nacionalizam

Poput rasizma i nacionalizam daje osjećaj posebnosti, ali ovaj puta pripadnost velikoj grupi, lokalno poznatih ljudi. Uz njega su vezani i geografski i povijesni simboli, kao i simboli moderne kulture. Dok se rasizam praktički svugdje javno osuđuje, nacionalizam je (slično kao i alkohol) u raznim oblicima „društveno prihvatljiv“ i nerijetko se javne osobe njime hvale, predstavljajući ga kao domoljublje. U takvim je društvenim okolnostima mladima jako teško objektivno procijeniti informacije koje do njih dolaze, kad one promiču nacionalizam.

I napadi rasista i nacionalista na djecu mogu se suzbijati samo odgovarajućim obrazovnim sadržajima i društvenom klimom te vjerodostojnim izvorima informacija koji uklanjanju tabue, mistifikacije i jasno diskutiraju povijesne neistine.

4.5.3. Sekte i kultovi

Sekte i kultovi su možda najopasniji od svih ideologija jer ciljaju doslovno na pojedinca i igraju se njegovim intelektualnim prednostima.

Današnji je svijet prepun kontradikcija, nedosljednosti, nelogičnosti i nepravdi.

Kod mladih je osjećaj za nepravdu izuzetno jako razvijen te ih svaki dokaz nepravde jako uznemirava.

Kad im se izlože nelogičnosti nekog stanja ili postupka, te ilustriraju nepravdom, postanu jako zainteresirani i osjećaju se pozvanima sudjelovati u razrješenju problema.

Lukave sekte to iskorištavaju do maksimuma i navode mlade da se u svrhu djelovanja sekte u potpunosti predaju zajednici i djeluju čak i potpuno ekstremno, ne poštujući i ne brinući ni za svoj ni za tuđi život. „Ideolozi" vješto skrivaju svoje prave namjere govoreći o aktualnim temama siromaštva, okoliša, globalizma, duhovnosti i sl. Osjećaj da (jedini) razumiju pravu prirodu problema i da će svojim sudjelovanjem osobno doprinijeti izgradnji boljeg svijeta potpuno mobilizira mladog čovjeka i štiti ga od bilo kojeg pokušaja izvlačenja iz okrilja sekte.

Teme, terminologija i komunikacijske tehnike koje „ideolozi" koriste toliko su slični legitimnim aktivnostima da je praktički nemoguće sagraditi bilo koji mehanizam automatskog filtriranja sadržaja.

Jedini način obrane od ove vrste napada jest stvoriti mladima kanale kroz koje mogu izraziti svoje potrebe za razumijevanjem društva i sudjelovanjem u njegovu razvoju.

4.6. Navođenje na rizično ponašanje

Eksperimentiranje ili korištenje droga, crackiranje, nasilništvo nad drugima, rizični seksualni odnosi su samo neki od oblika rizičnog ponašanja na koje se mlade može privući bilo usporedbom s glamuroznim ikonama iz medijskog života, bio obećanim materijalnim blagostanjem, bilo buntovništvom ili na bilo koji drugi način koji je provjereno učinkovit način motivacije kod mladih.

Ono što Internet čini puno "opasnijim" jest to da se putem njega gotovo besplatno može trenutno doći do tisuća pa i miliona slušatelja i gledatelja.

Poseban oblik rizičnog ponašanja je mamljenje djece na fizički susret s nepoznatom osobom. Tada je dijete izloženo riziku fizičkog napada (uključujući seksualni), pljačke, otmice. Djeca će u ovakvu situaciju biti namamljena potpuno nevinim pozivom na druženje radi razgovora ili razmjene predmeta vezanih uz njihove obične hobije i interese. Napadač će se predstaviti kao vršnjak ili čak i starija osoba koja imponira djetetu: slavna osoba, trener u potrazi za talentima, učitelj koji će pomoći oko zadaće kad roditelji ne znaju za slabu ocjenu i sl.

5. Metode zaštite

Tri su osnovna pristupa povećanju sigurnosti djece: sprečavanje napada, nadzor nad aktivnostima djece i intervencija te osposobljavanje djece za samoobranu.

5.1. Sprečavanje napada

Najpoželjnije rješenje kojem svi težimo je odagnati napade, prepriječiti ih, onemogućiti. Idealno bi bilo ako bi to netko ili nešto moglo učiniti bez naše aktivne uključenosti.

Naime, svi ti napadi su dodatno opterećenje za ionako pretrpani život brojnim drugim aktivnostima i problemima. Za borbu protiv napada na djecu uglavnom nemamo ni znanja, ni sredstava, ni vremena.

Stoga ne čudi porast broja "rješenja" koja će učiniti našu djecu sigurnima. Sva su "mehanička" i ne traže poseban angažman roditelja i učitelja.

U osnovi svih tih rješenja je jedna metoda: sprečavanje da sadržaj dođe do djeteta, pa se i zovu "filtriranje sadržaja" (eng. content filtering).

U praksi se to može primijeniti na dva načina:

- postavljanjem odgovarajuće programske podrške na vlastito računalo, tj. računalo koje dijete koristi, ili
- postavljanjem na poslužitelj kod pružatelja internetskih usluga.

U obje varijante suština metode je u tome da svaki upit koji dijete pošalje, odlazi na računalo ili program koji služe za filtriranje. Taj će program onda pribaviti željeni sadržaj, provjeriti ga i odlučiti hoće li ga proslijediti djetetu ili neće.

Provjera se radi na dva načina: provjera komunikacije ili provjera sadržaja.

Kod provjere komunikacije, program provjerava s kime komuniciramo, i uspoređuje to sa svojim popisom. Naime, slično kao i kod telefoniranja, i u Internetu svaki uređaj koji uspostavlja komunikaciju ima jedinstven broj na svjetskoj razini: internet adresu (eng. IP address). Ako se zna da su na nekoj adresi nepoćudni sadržaji ili da ju koristite ljudi kojima se ne može vjerovati, program neće dopustiti bilo kakvu komunikaciju s tom adresom.

Provjera sadržaja komunikacije je bitno složenije i bolje rješenje. U njemu se pregledava sadržaj i na osnovi različitih algoritama "važe" njegova podobnost prema unaprijed postavljenim kriterijima.

Ako se sadržaj ocijeni neprimjerenim, neće biti proslijeđen.

Popise adresa, odnosno tema koje su nepoćudne tipično sastavljaju tvrtke koje prodaju ova programska rješenja. Tijekom rada, njihov se program spaja na središnji poslužitelj proizvođača i preuzima nove popise nepoćudnih adresa ili sadržaja.

Kod rješenja koja se instaliraju na vlastitom računalu, roditelj može i sam dodavati zabranjene adrese, odnosno može odabrati kategorije sadržaja koje ne dozvoljava da dolaze do djeteta.

U stvari, postoje dvije osnovne politike koje se mogu primijeniti:

- propusti samo ono što je dozvoljeno ili
- propusti sve što nije zabranjeno.

Na žalost, unatoč našim željama i potrebama i unatoč tvrdnjama proizvođača pojedinih filtara sadržaja, potpuna mehanička zaštita ne postoji.

Problem filtriranja komunikacije zasnovane na IP adresama leži u činjenici da na višekorisničkim računalima mnogo korisnika koristi istu IP adresu za komunikaciju. Neprihvatljivo je zabraniti sav promet s jednim računalom samo zato što jedan njegov korisnik poduzima aktivnosti koje bi mogle biti opasne za djecu. Kod javnih servera to bi značilo da su praktično stalno u prekidu rada.

Kod filtriranja sadržaja komunikacije problem leži u samom ljudskom jeziku i komunikaciji. Vrlo je teško sa sigurnošću programski odrediti o kojoj temi dva sudionika na Internetu zapravo razgovaraju, govori li neka web stranica o povijesti rasizma ili aktivno zagovara rasizam, radi li se o temi iz farmakologije ili uputi o pravljenju droge.

Tehnički problem leži u tome što ne treba veliko znanje da se sustav filtriranja sadržaja zaobiđe, pa djeca koja ne žele kontrolu to mogu relativno lako i postići. Čak i kad nemaju znanja da sami smisle kako to napraviti, „korak po korak“ upute lagano su dostupne, naravno na Internetu, ili od vršnjaka.

No, zapravo možda najveća negativna nuspojava alata za filtriranje sadržaja leži u tome što se odgovorni: roditelji i učitelji, počinju osjećati sigurnima i ne-odgovornima kad se primijeni metoda filtriranja, umjesto da veliku energiju ulože u rad s djecom, podizanje njihove svijesti i osposobljavanje za samozaštitu.

5.2. Nadzor i intervencija

Neki misle da je druga metoda za zaštitu djece nadzor rada djece i intervencija odraslih. Sastoji se od toga da se, uz pomoć odgovarajućih programa, prati što djeca rade dok koriste Internet i kakve i od koga informacije im dolaze. Kad se uoče problematične informacije, njihov pristup djeci se onemogućava, a izvori takvih informacija se stavljaju na crnu listu. Djeci se i verbalno zabranjuje takva komunikacija.

Ako se zanemare kritike na račun narušavanja dječje privatnosti i davanja lošeg odgojnog primjera te stvaranja odnosa nepovjerenja, temeljni je problem što su djeca rođeni i strasni komunikatori i rijetko tko ima dovoljno vremena da temeljito poruči svu njihovu komunikaciju. Čak ako to i uspijemo, nakon toga se moramo osloniti na sustave filtriranja, koji imaju već opisana ograničenja. A što se tiče zabrane djeci, poznata je izreka: „Najsigurniji način da se nešto učini, jest da djetetu zabranite da to učini“.

5.3. Samozaštita i samoobrana

Sve novije studije i preporuke rađene u Europi i svijetu [1] se slažu u tome da metode zabrane i sprečavanja pristupa informacijama su neučinkovite i pogrešne te da je jedina prava metoda zaštite osposobiti djecu za samozaštitu i samoobranu.

Prije razmišljanja o načinima na koji se djeca sama mogu i trebaju štititi, važno je uočiti temeljne percepcije koje djeca imaju o Internetu.

5.3.1. Istinitost informacija

Baš kao i s televizijom i novinama i odrasli imaju dojam da kad se netko potrudio nešto napisati i tiskati, ili čak snimiti film o tome, onda je to vjerojatno istinito. Djeca su još podložnija toj percepciji.

Korisnici informaciju ocjenjuju vjerodostojnijom ako je potpisana od nekog autoriteta ili nekog tko zvuči kao autoritet („nacionalni …“, „Državni …“, „Institut …“, dr. , prof., ravnatelj, ….)

Oblikovanje informacije također utječe na dojam o njenoj istinitosti [4]. Grafički dobro oblikovana vijest, s vizualnim prilozima djeluje važnijom i istinitijom od „čistog“ teksta.

5.3.2. Anonimnost

Korisnici Interneta u pravilu imaju percepciju da su anonimni i „nedodirljivi“ dok komuniciraju Internetom. Glavni uzrok tome leži u činjenici da je u brojnim servisima na Internetu moguće stvoriti korisnički račun proizvoljnim odabirom korisničkog imena i lozinke. Čini se da nitko ništa ne provjerava i da se možemo predstaviti kao bilo tko. Komuniciramo s korisnicima na drugom kraju svijeta, a kad god poželimo možemo prekinuti komunikaciju i oni nam ne mogu ni pozvoniti na vrata ni nazvati nas na naš telefon. Međutim, anonimnost je u stvarnosti malo složenija. Postoje dva pogleda na to.

Prvi je da je stvarnu, potpunu anonimnost jako teško postići. Potreban je poseban trud i dosta znanja. Naime, sve se aktivnosti na računalima, sav promet u komunikacijskim sustavima tehnički nadziru i bilježe u dnevnike (eng. log). Bilo koju aktivnost se zato može povezati s fizičkom osobom koja ju je počinila. Stoga, pogrešno je računati da na Internetu možemo raditi što god želimo, i da nas nitko ne može otkriti i tražiti da snosimo odgovornost i posljedice naših djela. Stvarna anonimnost je nedostižna za većinu običnih korisnika.

Drugi pogled je da je za većinu običnih korisnika drugi korisnik u praksi ipak anoniman. Otkrivanje pravog identiteta nekog korisnika je složen, dugotrajan i skup postupak za koji su u pravilu potrebne i posebne, zakonom propisane, ovlasti.

To se konkretno može prevesti na pravilo dobre prakse svojevrsno „dvojno pravilo anonimnosti“:

- ne računaj da nekažnjeno možeš raditi što želiš, jer ako bude potrebno, ovlašteni će te ipak identificirati,
- nemaš načina da sa sigurnošću utvrdiš identitet osobe s kojom komuniciraš.

5.3.3. Informacijska pismenost

Vjerojatno je najteže, od svih metoda samozaštite, kod djece razviti informacijsku pismenost. U punom smislu ona se može razviti tek odrastanjem. Ovdje se ne misli na uobičajena znanja i vještine korištenja IKT, već prije svega na kritičko razmišljanje i sposobnost procjene istinitosti informacija koje primaju.

Jedini način da se postigne zadovoljavajuća razina informacijske pismenosti kod djece jest da ona postane sastavni dio svih elemenata obrazovnog programa. Da se istraživački rad, kritičko mišljenje i dijalog koriste kao temeljni način učenja i središnja aktivnost. Potrebni su i posebni programi koji će obrađivati sve poznate oblike nenamjernog i namjernog dezinformiranja, obmanjivanja i napada.

Kao i za sve ostalo u životu, najvažnije je uspostaviti takav odnos djeteta i roditelja (kao i djeteta i učitelja) da za sve nedoumice, želje i potrebe dijete slobodno i odmah dođe roditelju. Roditelj (ili učitelj) bi trebao biti prva osoba kojoj će se dijete obratiti ako tijekom korištenja Interneta bude napadnuto, prestrašeno, zabrinuto, povrijeđeno ili kad mu se učini da nešto nije kako treba ili kad mu samo nešto nije jasno.

5.3.4. Čuvanje privatnih podataka

U potpunosti sačuvati privatnost na Internetu je jako teško. Stoga je možda najbolja preporuka djeci (i odraslima) da svoj pravi identitet koriste samo u sustavima u kojima je to nužno potrebno:

poslovni sustavi njihovih škola, banke ako ih koriste i sustavi koji im trebaju za školovanje, a traže pravi identitet korisnika. U svim ostalim sustavima, posebno društvenih mreža trebaju dobro odvagnuti, je li njihovim sugovornicima, u čiji identitet nikada ne mogu biti potpuno sigurni, zaista potrebno znati njihovo pravo ime i adresu.

Čak i kada je nužno dati svoje prave podatke, treba odvagnuti jesu li svi traženi podaci zaista potrebni za tu funkciju. Autori informacijskih sustava često rutinski koriste obrasce za registraciju u kojima ima pitanja koja i nisu nužna za tu konkretnu primjenu. Djecu treba poučiti da imaju pravo od vlasnika sustava tražiti da im dopusti korištenje sustava čak i kad ne žele dati sve svoje privatne podatke koji standardni digitalni obrazac traži, ako ti podaci nisu potrebni za obavljanje funkcije sustava.

Jednostavno pravilo, koje se gotovo uvijek može primijeniti, jest da nikad ne daju privatne podatke trećih osoba: braće i sestara, roditelja, prijatelja i ostalih. Svoje privatne podatke smije davati samo ta osoba.

Treba ih poučiti i da se i naizgled nevažni podaci mogu zloupotrijebiti, da su oni privatni i ne trebaju se dijeliti s osobama u čiji identitet nismo potpuno sigurni: u kojim si klubovima do sada trenirao i kada, parkiraju li roditelji auto na cesti ili u garaži, u kojoj je ulici vaša vikendica na moru, koje pivo voli piti brat i sl.

5.3.5. Provjera sugovornika

Na Internetu komuniciramo s dvije vrste sugovornika: poznatim i nepoznatim. Poznati govornici su oni koje poznajemo osobno u fizičkom svijetu i do kojih možemo doći i nekim drugim komunikacijskim sredstvom: telefonom ili fizički.

Sve ostale osobe su nepoznate. To vrijedi i za one s kojima se već dugo i često dopisujemo, s kojima smo razmijenili puno razmišljanja, koji s nama dijele mišljenje, interese, strasti, tugu i veselje, ako ih nikada nismo fizički sreli.

Prva, jednostavna provjera se može napraviti tako da pokušamo naći osobu koju oboje fizički poznajemo. Ako taj naš poznanik može potvrditi identitet sugovornika, to je prvi korak do svrstavanja sugovornika među poznate osobe. No, da bi zaista dobio taj status, potrebno je da ga prije ili kasnije, upoznamo i uživo. Dok se to ne dogodi, pomoći će ako još neki poznanik potvrdi da poznaje tu osobu. Što više potvrda „fizičkih“ poznanstava to je sugovornik bliži statusu poznate osobe.

Danas je moguće upotrijebiti i video telefoniju (Skype npr.) kako bismo uživo vidjeli osobu. Na taj ćemo način dobiti prvu potvrdu da se zaista radi o vršnjaku, i da je to zaista osoba s kojom razmjenjujemo poruke (tako da za vrijeme video veze provjerimo neke ranije razmijenjene odgovore i pitanja). Osobu možemo i „fotografirati“ za vrijeme veze i fotografiju spremiti.

No, i dalje ne možemo biti sigurni ni u jedno drugo svojstvo te osobe (stvarnu dob, adresu, zanimanje, hobije, i sl.).

U pravilu, stalno treba imati na umu da o osobi znamo samo ono što nam je sama rekla o sebi (iako je to i u fizičkom životu vrlo često tako).

5.3.6. Pravila fizičkog kontakta

Pravilo koje možemo djeci reći je vrlo jednostavno: ne sastajte se fizički s nepoznatom osobom.

Dakle, osobu koju smo upoznali na Internetu, a ne poznajemo ju fizički, nećemo ići upoznati sami u fizičkom svijetu. To možemo učiniti samo uz pratnju roditelja ili osobe koju roditelji odrede.

Eventualno se dijete smije naći fizički s nekim koga poznaje samo preko Interneta, ako mu se pridruži poznanik koji tu osobu fizički poznaje i ako o tome obavijesti roditelje.

Taj poznanik mora biti netko s kime dijete ima dugotrajan i dobar odnos i poznaje ga fizički.

5.3.7. Odgovorno ponašanje

Iako se na prvi pogled čini jednostavnim, prilično je teško definirati odgovorno ponašanje. To bi bilo ono koje neće nikome naškoditi. Na Internetu, i općenito kod korištenja IKT, to je još složenije nego inače. Naime, mi svakodnevno moramo koristiti alate čiju punu funkcionalnost niti

poznajemo niti razumijemo, a koji imaju i greške i neka nedokumentirana svojstva kojih nismo svjesni.

Rezultat takvog, sasvim legitimnog i dobronamjernog, korištenja unatoč našoj najboljoj namjeri može biti štetan bilo za nas, bilo za nekog drugog. No, to je izgleda inherentni rizik novih svjetova koji su nastali globalnim širenjem Interneta, i svi korisnici ga moraju prihvatiti.

Eksperimentiranje s tehnologijom nikad ne smije naštetiti nekom drugom. Bilo da smo tu štetu prouzročili namjerno, ili iz nemara. „Igranje s vatrom" tj. isprobavanje aktivnosti koje bi mogle nešto uništiti, prekinuti, ili pokvariti čarobno je i privlačno mladima, stoga im se mora omogućiti da se time bave u kontroliranim, „laboratorijskim" uvjetima. Kroz tečajeve i radionice, s ciljevima koji vode k rastu i razvoju njihovih sposobnosti, treba im omogućiti da zadovolje svoju znatiželju i oslobode kreativni potencijal. Istovremeno ih treba poučiti kako će pretpostaviti moguće negativne posljedice svojih potencijalnih aktivnosti i objasniti im njihovu osobnu odgovornost za posljedice.

Naš utjecaj na djecu se stoga mora usmjeriti podjednako na tumačenje „klasičnih" pravila odgovornog ponašanja i na svojstva Interneta i novog svijeta u nastajanju, onako kako mi najbolje razumijemo.

5.3.8. Vječnost i neuništivost informacija na Internetu

Ključne su odgojne i obrazovne aktivnosti koje će kod djece razviti svijest o ponašanju koje ne šteti drugima, o negativnim stranama osvetništva i „uzimanja pravde u svoje ruke", o „batini s dva kraja" koju predstavlja napadanje, ruganje, vrijeđanje i sramoćenje drugih. Uz to, posebno je važno razviti svijest o specifičnoj „internetskoj" pojavi: vječnosti i neuništivosti informacije.

Naime, kad jednom na Internetu objavimo neku informaciju, nemoguće ju je obrisati, povući, uništiti.

Ona se širi sustavom, pohranjuje u rezervne kopije i arhive, pohranjuje kod brojnih korisnika do kojih je došla ili koji su došli do njih. Prije ili kasnije ona može ponovo izaći na površinu i biti ponovo dostupna mnogima, čak iako smo ju mi uklonili sa svih mjesta na koja smo ju mi postavili i na svim mjestima na kojima smo ju pronašli.

Ono što nam se danas čini šalom, benignom informacijom, nevažnim tračem, već sutra će nam možda stvarati neugodnost, ili će nekom drugom otežavati život. Čak i ako se budemo iskreno kajali i pokušali učiniti sve da popravimo situaciju, ono što smo „injektirali" u Internet, nastavit će živjeti negdje u njemu, izvan našeg, ili bilo čijeg dohvata.

Stoga je više nego ikada, više nego igdje potrebno temeljito promisliti prije nego objavimo informacije na Internetu.

6. Resursi vezani uz sigurnost djece

Sigurnost djece na Internetu je suvremena i važna tema. Osim znanstvenih istraživanja brojni su projekti koji služe informiranju odraslih, pomoći djeci, grade ili obrađuju alate za zaštitu, stvaraju sigurni okoliš za djecu i dr.

6.1. Informacije za odrasle

Kako bi sigurnost djece na Internetu bila što učinkovitija, potrebna je i kvalitetna edukacija roditelja, učitelja i cijele društvene zajednice. Odrasli danas mogu informacije o zaštiti djece dobiti i putem Interneta. U nastavku je na tu temu navedeno par značajnijih web adresa:

- informacije o neprofitnoj organizaciji "Childnet International" koja se bavi zaštitom djece na Internetu:

http://www.childnet-int.org/

- informacije za učitelje koji su nesigurni u svoje znanje o Internetu i njegovom korištenju:

www.allaboutexplorers.com

- nagrađena web stranica namijenjena učiteljima, roditeljima i djeci, a sadrži praktične informacije za zaštitu djece na Internetu:

http://www.kidsmart.org.uk/

6.2. Informacije za djecu

Djeca se putem Interneta također mogu informirati o vlastitoj sigurnosti i negativnim posljedicama nesvjesnog korištenja Interneta. U nastavku je na tu temu navedeno par značajnijih web adresa:

- istinite priče mladih ljudi o njihovim negativnim iskustvima „cyberbullyinga", davanja previše osobnih podataka nepoznatim ljudima i dr.:

http://www.netsmartz.org/netteens.htm

- informacije o tome kako sigurno koristiti svoje osobne informacije i općenito o elementima sigurnosti na Internetu:

http://www.digizen.org.uk/

- informacije o negativnim posljedicama nepromišljenog objavljivanja osobnih informacija (slika, podataka,…):

http://www.prnewswire.com/mnr/adcouncil/26474/

- objašnjeni pojmovi i primjeri vezani za sigurnost djece na Internetu:

http://www.saferinternet.org/ww/en/pub/insafe/safety_issues.htm

6.3. Alati za zaštitu

Jedan od načina zaštite djece na Internetu je i korištenje *web-filtering* alata za filtriranje sumnjivih i neprimjerenih web sadržaja. U nastavku su navedeni neki od poznatijih komercijalnih alata:

- NetNanny, URL: http://www.netnanny.com,
- CyberPatrol, URL: http://www.cyberpatrol.com,
- SafeEyes, URL: http://www.safeeyes.com.

Osim komercijalnih inačica postoje i besplatni alati, kao što je:

- K9 WebProtection, URL: http//www.k9webprotection.com.

6.4. Sigurni okoliš

Djecu je potrebno upoznati kako se osigurati od loših stvari na koje mogu naići tijekom korištenja Interneta ili kako da ne postanu žrtve onih koji narušavaju njihovu sigurnost.

Video isječci koji prikazuju kako sigurno koristiti Internet (*Safe Social Networking*) i koje su opasnosti i posljedice mogu se pronaći na slijedećoj adresi:

- http://www.safesocialnetworking.com/

7. Zaključak

Vrste, oblici i broj napada na sigurnost korisnika Interneta i dalje će rasti. Djeca će uvijek biti ispred odraslih u korištenju novih tehnologija i intenzitetu komuniciranja. Isto će tako uvijek biti nezaštićenija od odraslih.

Nove će se tehnologije zaštite (automatizirane, strojne, mehaničke zaštite) stalno razvijati. Uz to, povećavat će se pritisak za njihovu primjenu, kako od roditelja, učitelja, administracija tako i od industrije.

Međutim, ključno je uočiti da se protok informacija ne može spriječiti, da je najteže razlučiti prihvatljive od neprihvatljivih sadržaja i da je ključ sigurnosti djece u njihovu odgoju i obrazovanju, te kvalitetnom odnosu s roditeljima i učiteljima.

Roditelji, škole i šira društvena zajednica moraju neprekinuto raditi na tome. Potrebni su programi koji će:

- pomagati roditeljima i učiteljima da razumiju tehnologije, njihove dobre i loše strane te načine na koje ih koriste djeca,
- istraživati nove tehnologije i njihove primjene,
- podizati svijest djece o posljedicama korištenja tehnologije,
- razvijati odgojne i obrazovne programe za sigurno korištenje IKT,
- provoditi te programe.

Pored toga potrebne su i nacionalne vizije, strategije i politike te aktivna međunarodna suradnja.

8. Reference

[1] Balanskat, Anja; Richardson, Janice; Varbanova, Tanya. e-Safety policies and initiatives across Europe 2007, 2007. URL: http://insight.eun.org/ww/en/pub/insight/misc/specialreports/e_safety_policies.htm (2008-08-11)

[2] CARNet CERT. Socijalni inženjering, 2006. URL: http://www.cert.hr/filehandler.php?did=264

[3] Young Sik Lee, Doug Hyun Han, Kevin C. Yang, Melissa A. Daniels, Chul Na, Baik Seok Kee, Perry F. Renshaw. Depression like characteristics of 5HTTLPR polymorphism and temperament in excessive internet users, July 2008 (Vol. 109, Issue 1, Pages 165-169).

[4] B.l.Fogg , Ph.D., Cathy Soohoo, David Danielson, Stanford Persuasive Technology Lab. How Do People Evaluate a Web Site's Credibility? October 29, 2002.