Rizici djece na internetu

Gromila, Alen

SVEUČILIŠTE JURJA DOBRILE U PULI
FAKULTET INFORMATIKE PULA

Alen Gromila

RIZICI ZA DJECU NA INTERNETU

Završni rad

Pula, rujan, 2019.

SVEUČILIŠTE JURJA DOBRILE U PULI
FAKULTET INFORMATIKE PULA

Preddiplomski studij
Informatika
Predmet: Sigurnost računalnih sustava
Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija

Alen Gromila

0069068549

RIZICI ZA DJECU NA INTERNETU

Završni rad

Pula, rujan, 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani/a Alen Gromila , ovime izjavljujem da je ovaj završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio seminarskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

Pula, rujan 2019. godine

ZAHVALA

Zahvaljujem se mentoru prof. dr. sc. Mariu Radovanu i komentoru mr. sc. Walteru Stembergeru na korisnim savijetima, susretljivosti te vremenu i trudu uloženom pri izradi ovog završnog rada.

SAŽETAK

U radu su analizirani rizici, prijetnje i opasnosti sa kojima se djeca svakodnevno susreću koristeći internet i društvene mreže. Obuhvaćeno je cijelo područje od prvog pristupa djeteta internetu, do online komunikacije i utjecaja roditelja u cijelom tom procesu. Također, u radu se obrađuju i teme vezane za cyberbullying i njegov utjecaj na djecu, kao i mjere zaštite.

Ključne riječi: rizik, dijete, internet, cyberbullying

SADRŽAJ:

1. UVOD

Tema ovog završnog rada su rizici za djecu na internetu. Internet je u današnje vrijeme najrasprostranjeniji i najviše korišteni alat, a njegovi korisnici su različite dobi. Konkretno u ovom radu proučavani su i opisani rizici korištenja interneta od strane djece. Dobna skupina kreće se od najmlađe dobi pa sve do osamnaeste godine, što bi obuhvaćalo život djeteta kroz osnovnu i srednju školu. Također kroz rad, dotaknuta je i tema roditelja, njihovo ponašanje online, te nadzor i kontrola koju obavljaju nad djetetom i koliko to utječe na njegovu sigurnost. Kroz povijest, sigurnost informacijskih sustava razvijala se postepeno. Obzirom da na samom početku nije postojao velik broj računala, niti rizici korištenja i opasnosti nisu bile velike. Sve većom popularizacijom i korištenjem pametnih telefona, tableta i računala te samim razvitkom interneta, rizici koji se javljaju su veći i opasniji, posebice za djecu, koja nisu u potpunosti upućena u online svijet. Kroz rad su dani i objašnjeni osnovni pojmovi poput GDPR-a i cyberbullyinga te su za iste dani i praktični primjeri. Osim rizika i opasnosti kojima su djeca izložena prilikom korištenja interneta, dane su i zaštitne mjere, kojima se rizici i opasnosti mogu umanjiti.

2. POVIJESNI RAZVOJ INFORMACIJSKE SIGURNOSTI

Sigurnost informacijskih sustava je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja (Vukelić, 2016.). Informacijska sigurnost također uključuje i oporavak informacijskih sustava, detekciju i odvraćanje napada te primjenu zakonskih propisa koji se odnose na privatnost, računalni kriminal, računalnu forenziku i slično (Vukelić, 2016.).

Razvoj informacijske sigurnosti započinje 1950-ih godina i nastavlja se sve do danas. Na samom početku, u razdoblju 1950-ih i 1960-ih, sigurnosnih prijetnja nije bilo puno, razlog tome je što je su u to vrijeme računala bila skupa i malobrojna te je proporcionalno tome i broj korisnika bio mali. Većinom su računala korištena samo u vladi i vojsci te se je sigurnost odnosila samo na fizički pristup računalu, obzirom da su na njemu bili pohranjene važne i tajne informacije. Najveća pozornost davala se je pouzdanosti računala (Vukelić, 2016.).

U razdoblju 1960-ih i 1970-ih dolazi do pojave prvih osobnih računala. sigurnosne prijetnje su i dalje u malom broju, a razlog tome su stand-alone računala i specifični softveri. povećanje prijetnji sigurnosti kreće 1970-ih godina, razvojem standardiziranih aplikacija. Fokus sigurnosti pomiče se s samog računala na informacije koje se u njemu nalaze. Vlada i vojska su i dalje vodeći korisnici računala te se dokumenti i izvještaji o sigurnosti odnose na povjerljivost informacija. Također u tom razdoblju dolazi do pojave termina InfoSec. 1974.godine ističe se potreba o zaštiti informacija, prvi put se spominje pitanje integriteta, povjerljivosti i dostupnosti kroz sigurnosni trokut (Vukelić, 2016.).

1980-ih godina započinje veća upotreba računala u različitim sektorima. Kako za vladu i vojsku, tako se računalo sve više upotrebljava u sektoru gospodarstva te se time mijenjaju i prioriteti korištenja ovisno o potrebama korisnika. Prioritet je očuvanje integriteta informacija, dok prijetnju predstavljaju nedovoljno obučeni zaposlenici. Obzirom na veću upotrebu vidljivi su i pomaci u zakonodavstvu i standardizacija. U tom razdoblju, točnije 1998. godine, zabilježen je i prvi Dos napad, The Morris worm (Vukelić, 2016.).

Razdoblje 1990-ih i početak 21. stoljeća obilježilo je nekoliko bitnih promjena. 1988. godine pojavljuje se termin Information Assurance (AI), koji osim integriteta, dostupnosti i povjerljivosti, obuhvaća još i autentikaciju i neporecivost, točnije korištenje, pohranu i prijenos informacija. Fokus se sa sigurnosti samih informacija prebacuje na sigurnost sustava tj. s tehničkog na organizacijski dio. 1995, godine javlja se Standard - BS7799. Povjerljivost, dostupnost i integritet nadopunjuju se potrebom u posjedovanju te točnosti, jasnoći i prijenosu informacija u cjelini. U poslovnom smislu počinje se pratiti i učinkovitost sigurnosnih mjera, sigurnost poslovanja - rješenje unaprjeđuje poslovanje (Vukelić, 2016.). Na Slici 1 prikazan je osnovni sigurnosni trokut, koji se sastoji od povjerljivosti, integriteta i dostupnosti. Pod povjerljivost spadaju svi oni rizici koju uključuju neovlašteno korištenje podataka, hakiranje, razni virusi i slično. Integritet u drugu ruku podrazumijeva da se podatci (informacije) ne smiju mijenjati i koristiti od strane neovlaštenih osoba i bez dopuštenja (privole). Dostupnost, kao treći aspekt informacijeske sigurnosti obuhvaća i podrazumijeva dostupnost samih informacija i podataka (Bukovac, 2016.).

Slika 1. Osnovni sigurnosni trokut (Bukovac, 2016.)

Te zadnje promatrano razdoblje, razdoblje današnjice u kojoj se razvija sve veća korporativna sigurnost, u kojoj se smatra kako je sigurnost integralni dio korporacija. Računala se koriste u velikom broju, kako u firmama, tako i pojedinačno. Obzirom da je upotreba društvenih mreža konstantna, sve se više pažnje posvećuje privatnosti informacija, odnosno osobnim podatcima. Također, sve je više opasnosti te je naglasak na odgovornosti i podizanju svijesti o sigurnosti (Vukelić, 2016.).

3. PRISTUP I KOMUNIKACIJA DJECE ONLINE

3.1. Prvi pristup i upoznavanje djece s internetom

Upoznavanje djece s internetom počinje od njihove najranije dobi, točnije dok su ona još u kolicima. Sve češće se može vidjeti kako djeca dobivaju tablete i pametne telefone te dok su vani, umjesto da se igraju i borave u prirodi, ona gledaju određeni sadržaj na internetu. Ako se preskoči predškolski uzrast djece, i krene promatrati djecu od sedme godine na dalje, tada zapravo kreće prvi pravi pristup internetu. Obzirom da tehnologija sve više napreduje i internet je postao neizostavan, kako za obrazovanje tako i za život općenito, više ne postoji mogućnost da se on ukine ili ne koristi. Ako se malo bolje razmisli, djeca prvu pravu poduku o internetu i njegovoj primjeni dobivaju u višim razredima osnovnih škola, na satovima informatike, a do tada, ona već naveliko koriste internet, kako pretraživanja, tako i razne društvene mreže. Korištenje laptopa od strane predškolske djece prikazano je na Slici 2.

Slika 2. Korištenje laptopa kod predškolskog uzrasta (https://sites.google.com/site/sigurnostnainternetu55/djeca-na-internetu)

Koliko su djeca upoznata sa svim mogućnostima koje internet pruža, ali istotako i o rizicima i opasnostima koje se nalaze na njemu, teško je reći, ovisi od pojedinca do pojedinca.

Činjenica je da je internet olakšava i doprinosi puno bržem načinu učenja, također i pomaže u razvoju djece, ali isto tako ima i svojih nedostataka, a jedan od njih je sigurnost njegovog korištenja, odnosno sigurnost djece prilikom njegova korištenja. Djeca različite dobi internetu pristupaju preko mobitela, tableta i kompjutora, koriste ga u raznorazne svrhe, za učenje, zabavu, za međusobno komunikaciju preko društvenih mreža i sl. Na to koliko su djeca sigurna u njegovom korištenju utječe i to, koliko su ona nadgledana prilikom korištenja i koliko vremena provode dnevno online. Obzirom da u današnje vrijeme gotovo svako djete do svoje sedme godine koristi pametne telefone, roditelj je taj koji bi trebao provjeravati koliko njegovo dijete vrijemena provodi na internetu te koje sadržaje pregledava. Kada bi se tako postupalo, djeca bi bila puno manje izložena rizicima na internetu. Također rizici koji se nalaze na internetu nisu jedini problem koji može negativno utjecati na razvoj djeteta u toj dobi. Istraživanje koje je provedeno u Sjedinjenim Američkim Državama 2016. godine pokazalo je kako su djeca u vrtiću, koja su često koristila pametne telefone i tablete, dvostruko češće sklonija izgubiti živce nego njihovi vršnjaci, koji nisu bili izloženi u toj mjeri (http://hr.n1info.com/Tehnologija/a345130/Zasto-mobitel-ne-smijete-dati-maloj-djeci.html).

Bez obzira govori li se o pozitivnim ili negativnim stranama interneta i njegovoj primjeni kod djece, mora se biti svjestan da je to opasan alat pomoću kojeg se može utjecati na daljni razvoj djeteta, kako na razmišljanje i stavove, tako i na njegovu sigurnost.

3.2. Online komunikacija

Komunikacija je proces razmjene informacija preko dogovorenog sistema znakova, odnosno proces slanja informacija sebi ili bilo kojem drugom entitetu. Njezin direktan prijevod, odnosno značenje bilo bi podijeliti, odnosno učiniti nešto općim ili zajedničkim. Komunikacija je obično opisana sa 3 glavne dimenzije, a to su sadržaj, forma i cilj. Sadržaj i forma obuhvaćaju poruke koje se šalju prema određenom cilju. Sam cilj predstavlja drugi sugovornik, bilo to čovijek ili organizacija do kojeg ta poruka treba stići (https://hr.wikipedia.org/wiki/Komunikacija).

Online komunikacija je na neki način podvrsta same komunikacije, a predstavlja način sporazumijevanja preko određenog posrednika. Bolje rečeno, komunikacija preko društvenih mreža i interneta. Online komunikacija, odnosno razgovori na mreži, postali su svakodnevica. Sve veći broj ljudi se njome koristi, jedan dio njih iz razloga kako bi uštedjeli dragocijeno vrijeme, dok drugi dio njih kako bi izbjegli neugodan kontakt oči u oči. Dakako online komunikacija ima svojih prednosti i mana. Prednosti online komunikacije su te, što je komunikacija izrazito jednostavna i dostupna svakom tko posjeduje mobitele, tablete ili računala. Također, udaljenost između dvije osobe ne predstavlja nikakvu zapreku, a osim toga postoji i veliki broj ostalih ljudi i poznanika koji se jednostavni i brzo mogu pronaći i kontaktirati. Sa financijske strane isto tako ne predstavlja preveliku obvezu, jer je jako raširena i jeftina. Uz sve te prednosti postoje i neke mane online komunikacije. Iako ih nema puno, one nisu toliko zanemarive. Za početak, prilikom online razgovora, iako postoji i video razgovor, komunikacija nije ista, odnosno ne postoji pravi osjećaj razgovora i ambijenta. Na emocijonalnoj razini, puno se je teže povezati sa sugovornikom te također postoji šansa da netko taj razgovor prisluškuje ili snima. Ukoliko se radi samo o online razgovoru, bez ikakvog vizualnog kontakta, postoji velika mogućnost da ne komuniciramo sa osobom kojom mislimo. Sa sve većom proširenošću online komunikacije javljaju se i sve veći rizici, jedan od tih je stvaranje "fake" (lažnih) profila, na kojima se osoba ne predstavlja onakva kakva stvarno je, te to može uzrokovati velike probleme. Prilikom takvih razgovora vrlo je važno poznavati osobu sa kojom kontaktiramo i biti siguran u njezine namjere. Osim odraslih osoba, sve je više djece koja komuniciraju online. Iako postoji, dobna granica za pristupanje društvenim mrežama više se ne poštuje. Narovno, društvenim mrežama mogu pristupiti svi

uzrasti, bez obzira na dob, spol, nacionalnost i slično. U današnje vrijeme online razgovori najčešće se odvijaju preko društvenih mreža Facebooka, Messengera, Instagrama, WhatsAppa i sličnih aplikacija (Slika 3.). Svaka od navedenih mreža ima mogućnost postavka privatnosti, jedini problem je što ih svatko ne zna postaviti i prilagoditi. Najvećem riziku online komunikacije izložena su upravo djeca. Iako većina njih koristi društvene mreže, njihove postavke privatnosti, ukoliko ih sami postavljaju, nisu uvijek dobro postavljene. Razlog tome je što, iako društvene mreže imaju dobnu granicu za pristup, puno djece, mlađe od dozvoljenog godišta i bez znanja roditelja otvaraju svoje profile te tako roditelji nisu u mogućnosti pomoći djetetu u postavljanju postavki privatnosti. Samo jedan od mnogobrojnih rizika je taj što veliki broj djece, uz želju da pronađe što veći broj prijatelja, kontaktira osobe koje osobno ne poznaje i započinje razgovor s njima.

Slika 3. Dostupnost društvenih mreža i aplikacija (https://www.seguidormania.com/blog/continue-construindo-seu-marketing-social-dos-meios-de-comunicacao-social-com-estas-grandes-dicas/)

Kako bi se provjerilo koliko su djeca zapravo sigurna i na koji način koriste internet, 21. studenog 2017. godine u Zagrebu provedeno je nacionalno istraživanje sigurnosti djece i mladih na internetu, EU Kids Online istraživanje u Hrvatskoj. U istraživanju je sudjelovalo 1017 djece u dobi od 9 do 17 godina te onaj roditelj koji ima više uvida u prakse djeteta na internetu. Neki od preliminarnih rezultata vezanih za online komunikaciju sa nepoznatom

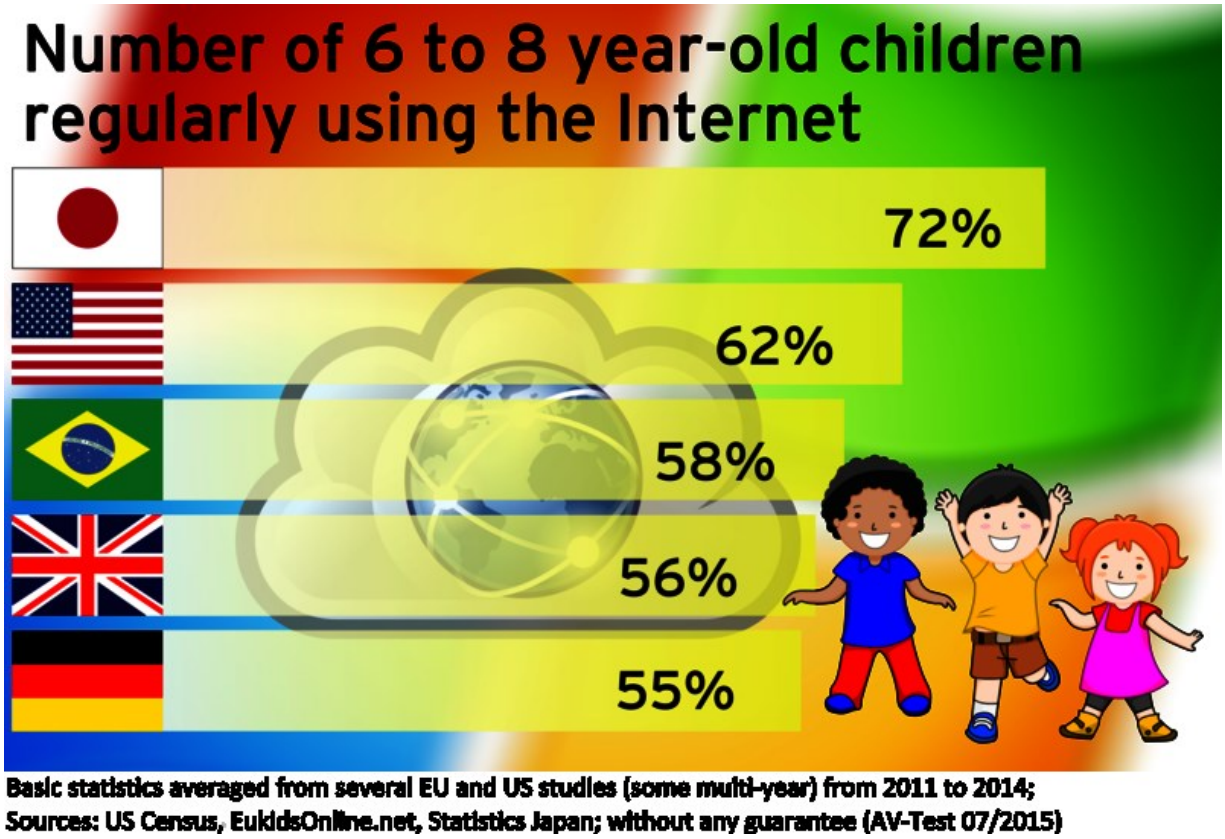
osobom su ti da svako deseto dijete u dobi od 15 do 17 godina prihvaća sve zahtjeve za prijateljstvom drugih ljudi na društvenim mrežama. Istovremeno, gotovo svako četvrto dijete te dobi svakoga tjedna traži na internetu nove prijatelje ili kontakte. Ovakav rezultat sugerira da su mladi usmjereni na socijalizacijski aspekt kojeg nude društvene mreže i internet. Svako peto dijete u dobi od 9 do 17 godina u potpunosti ili uglavnom ne zna promijeniti postavke privatnosti, npr. na društvenim mrežama. Još jedan zabrinjavajući podatak je taj da gotovo svako treće dijete u dobi od 9 do 17 godina je u posljednjih godinu dana komuniciralo na internetu s osobama koje nisu ranije upoznali uživo. To je činilo svako deseto dijete u dobi od 9 do 11 godina, svako četvrto dijete u dobi od 12 do 14 godina te gotovo 1/2 djece u dobi od 15 do 17 godina. Također više od 1/10 djece u dobi od 9 do 17 godina se u posljednjih godinu dana susrelo uživo s osobom koju su upoznali na internetu (http://hrkids.online/post/second-press/). Iako je od istraživanja prošlo nepune dvije godine, rezultati koji su dobiveni ukazuju na to kako online komunikacija nije toliko bezazlena koliko se smatra te da ukoliko dijete koristi internet, izloženo je mnogim rizicima i opasnostima.

Tablica 1. Rezultati nacionalnog istraživanja sigurnosti djece i mladih na internetu (http://hrkids.online/post/second-press/)

POSTAVLJENO PITANJE	DOB (godine)	POZITIVAN ODGOVOR (%)	
Uvijek kada želim ili kada trebam, mogu pristupiti internetu.	9-11	1/2	50
	12-14	2/3	66,67
	15-17	3/4	75
U proteklih godinu dana primio/-la sam neprimjerenu ili uvrijedljivu poruku.	9-11	1/3	33,33
	12-14	1/2	50
	15-17	3/4	75

U Tablici 1. priložena su dva pitanja, koja su također bila postavljena u spomenutom istraživanju, a tiču se same dostupnosti interneta. Iz rezultata danih u tablici može se vidjeti kako je internet uvijek dostupan barem polovici djece od devete do jedanaeste godine starosti, a kako se povećava i uzrast, povećava se i postotak djece kojima je on stalno dostupan. Tako djeca od dvanaeste do četrnaeste godine, njih čak 2/3 ima stalan pristup internetu, dok taj postotak raste na 75% kod djece uzrasta od petnaeste do sedamnaeste godine. Pitanje koje je važno za ovaj rad, kako bi se bolje pojasnili rizici za djecu na internetu

i cyberbullying u nastavku, je drugo pitanje u danoj tablici. Na pitanje koliko je djece primili neprimjerenu poruku u poslijednjih godinu dana 33,33% djece dalo je potvrdan odgovor u dobi od devete do jedanaeste godine. Također i kod ovog pitanja pozitivan broj odgovora proporcionalno raste sa brojem godina, tako kod djece od dvanaeste do četrnaeste godine, pozitivan odgovor dobiven je od polovice ispitanih. Kod dobne skupine od petnaeste do sedamnaeste godine, pozitivno je odgovorilo čak njih 75%.



Slika 4. Rezultati ispitivanja u ostalim državama (https://www.av-test.org/en/news/test-parental-control-software-for-windows-and-mac-os-x/)

Na Slici 4. prikazani su rezultati ispitivanja u drugim državama. Pitanje koje je postavljeno odnosilo se je na to koliko djeca od šeste do osme godine redovno koriste internet. Ispostavilo se je da se najveći broj ispitanika (njih 72%) nalazi u Japanu tj. da je tamo djeci te dobi internet najviše dostupan. Nakon Japana slijede Sjedinjene Američke Države sa 62%, potom Brazil sa 58%. Razlika između Ujedinjenog kraljevstva, gdje 56% djece redovno koristi internet i Savezne Republike Njemačke, čiji je postotak 55%, nije velika. Bez obzira o kojoj se državi radi, i ako se stavi na stranu činjenica da je u jednu ruku internet dobar za učenje, motoriku i razvoj, ovi rezultati su ipak malo zabrinjavajući. U svakoj od država, preko pola

populacije te dobi redovno koristi internet, što zapravo znači da ta djeca u dobi od šest do osam godina, umjesto da vrijeme provode vani igrajući se sa prijateljima, oni koriste kako bi pretraživali internetske stranice, koristili društvene mreže, igrali igrice i slično. Nažalost ovi podatci su samo privremeni, postotak korištenja nažalost raste iz godine u godinu. Treba biti svijestan da napredak tehnologije, koliko god pomaže u unaprijeđenju života, isto tako odmaže u razvoju i sigurnosti djece na ispravan način.

Još jedan način online komunikacije odvija se preko raznih igrica, koje se skidaju na pametne telefone i tablete. Naime, većina tih igrica ima mogućnost razgovora sa drugim suigračima (chat preko igrice). Nerijetko se može vidjeti kako roditelji, dok primjerice objeduju u restoranu ili piju kavu u kafiću, svojem djetetu daju pametni telefon ili tablet, kako bi ono bilo mirno i pustilo ih da odmore. Rizik kojem u tom trenutku oni izlažu svoje dijete je izrazito velik. Ukoliko na pametnom telefonu ili tabletu postoji jedna od takvih igrica, vrlo je vjerojatno kako će dijete stupiti u kontakt s nepoznatom osobom. Iako jedna vrsta razmišljanja, u kojoj se smatra da dijete tako stječe nove prijatelje i unaprijeđuje svoj način komunikacije, je djelomično točan, on sa sobom nosi puno više opasnosti. Nitko ne može biti u potpunosti siguran sa kime komunicira preko takvih razgovora. Kroz razgovor se ne vidi sugovornik, njegova dob, spol niti stvarna namjera. Postoji mogućnost da osoba koja se predstavila djetetu kao vršnjak njegove dobi, je u stvarnosti odrastao čovjek od četrdesetak godina. Djeca su iskrena, naivna i u toj dobi jako neinformirana vezano za sigurnost u online razgovorima i baš zbog toga su izloženi ovakvim opasnostima. Istotako, pošto se ne vidi suigrač/sugovornik, kako biti siguran da je to uistinu osoba za koju smo uvjereni da ju poznajemo? Jedna od mogućnosti može biti i ta da je toj osobi netko preuzeo profil na igrici i da igra umjesto nje. Ista stvar može se primjeniti i na igrice koje se igraju preko računala. Iako bi igrica trebala služiti tome da djecu nakratko zabavi, pruži im mali odmak od stvarnosti i prepusti ih njihovoj maštи, neka djeca na igricama provode veliki broj sati dnevno. Što više vremena dijete provodi online i u komunikaciji sa nepoznatim osobama, to su nažalost veće šanse da rizik bude veći. Ukoliko roditelj ne nadgleda svoje dijete, barem povremeno, kako biti siguran da, ukoliko dijete stupi u online kontakt sa nepoznatom osobom, da će taj razgovor stvarno ostati samo online. Online komunikacija je izrazito opasna, pogotovo za djecu manje dobi te bi na to trebalo posvetiti puno više pažnje i vremena. Educirati i upozoriti, kako samu djecu na moguće rizike, tako i njihove roditelje.

3.3. Utjecaj i uloga roditelja

Svaka osoba, bila ona roditelj ili ne, svakodnevno barem jedanput koristi mobitel, tablet ili računalo. Činjenica je da je u današnje vrijeme teško zamisliti život bez moderne tehnologije, no da li je ona stvarno potrebna u tolikoj mjeri? Koliko ona utječe na razmišljanje pojedinca, na promjenu stavova i želja te koliki je njezin utjecaj u sve manjoj komunikaciji ljudi. Usporedivši jedan najobičniji prizor, primjerice šetnju gradom, nekad i danas, mogu se uočiti velike promjene. Nekada su ljudi šetali ulicom, držali dijete za ruku, međusobno se pozdravljali i razgovarali, dok danas, sve više ljudi samo prođe jedno pored drugoga, ni ne primjetivši prijatelja ili kolegu. Razlog tome je što većina njih, dok hoda ili primjerice sjedi u kafiću ne odvaja pogled od svog pametnog telefona i društvenih mreža. Koliko je to zapravo prešlo u naviku i koliki je utjecaj svega toga na djecu, sve je češća tema današnjice. Također, pogledali li se najugoženija skupina u svemu tome, a to su djeca, može se vidjeti kako, iako djeca borave u parku, jako je malo prizora kada se ona uistinu igraju. Većinu vremena, bili oni s roditeljima ili u skupini, provode na mobitelima, što je jako zabrinjavajuće.

Slika 5. Obitelj 21. stoljeća (https://www.tigermobiles.com/blog/the-best-mobile-phone-family-plans/)

Na Slici 5. nalazi se prikaz klasične obitelji 21. stoljeća, u kojoj, bez obzira na godine, sve generacije zajedničko vrijeme provode na pametnim telefonima, tabletima i prijenosnim računalima. Zajedničko vrijeme koje je moglo biti provedeno u razgovoru iskoristilo se je u pretraživanju internetskih stranica i na različitim dostupnim aplikacijama.

Iako je internet neizostavan u današnje vrijeme, trebalo bi malo više voditi računa koliko i kako ga djeca koriste. Korištenje interneta sa sobom nosi i razne rizike. Uloga roditelja bi trebala biti ta, da svoju djecu u što većoj mjeri zaštite od tih rizika, a ne da ih još dodatno izlažu njima. Puno stvari se radi nesvjesno ili nenamjerno i nerazmišljajući. Proširenost i uporaba društvenih mreža je došla do razne na kojoj je zabrinjavajuća. Promatrana skupina u ovom dijelu su roditelji i njihovi postupci. Puno roditelja na dnevnoj bazi fotografira svoju djecu i stavlja te iste slike online. Iako možda, ne razmišljajući na taj način, oni direktno svoje dijete dovode do potencijalnih rizika. Ovisno o postavkama na samoj društvenoj mreži i o tome kako ju koji roditelj postavi, ali tu sliku može vidjeti jako puno ljudi. Nažalost, nisu svi na društvenim mrežama iskreni i onakvi kakvi se predstavljaju te nitko ne zna namjere pojedinca. Svaki korak koji se radi online, trebao bi biti dobro promišljen. Niti jedan roditelj ne bi volio da je njegovo dijete na bilo koji način ugroženo ili izloženo ikakvim rizicima, pogotovo u najranijoj dobi. Baš je zato potrebno više pažnje i vremena posvetiti edukacijama, kako bi roditelji, a i svi ostali sigurnije mogli koristiti internet i tehnologiju.

Ranije spomenuti utjecaj roditelja, može se promatrati i kao utjecaj roditelja na djecu. Odnosno djeca dok su malena, upijaju znanje iz svoje okoline i oponašaju ga te tako uče, razvijaju se i odrastaju. Ako dijete dok je još malo, svakodnevno gleda svoje roditelje kako koriste svoje pametne telefone i provode vrijeme na internetu, kolika je vjerojatnost da to dijete neće htjeti isto, samo puno ranije.

Prikaz utjecaja roditelja na dijete prikazan je na Slici 6. Na slici se nalaze roditelji, koji uz objed koriste svoje mobitele i tako ne obraćaju pažnju na svoje dijete. Dječak predškolske dobi pozorno promatra postupke svojih roditelja i stiječe krive navike pri odrastanju.

Slika 6. Utjecaj roditelja na djete (https://www.thetimes.co.uk/article/is-it-time-to-start-some-family-phone-rules-3lzk03xp5)

Djeca u sve ranijoj dobi dobivaju svoje pametne telefone i provode vrijeme na internetu, koliko god se mislilo da je taj način razvoja dobar, on sa sobom nosi i rizike. Uloga roditelja, osim kontroliranja sadržaja koje njegovo dijete pregledava i koliko vremenski provodi online trebala bi biti i ta, da on postupa isto. Odnosno da, ako želi da dijete smanji vrijeme koje provodi na pametnima telefonima i internetu, to mora učiniti i sam roditelj. Manja upotreba interneta i tehnologije ne samo da smanjuje rizike i opasnosti koji se nalaze na internetu, već i doprinosi do većeg međusobnog druženja i sretnijeg djetinstva.

3.4. Aplikacije o zaštiti osobnih podataka

Osobni podatci su sve informacije koje se odnose na pojednica, čiji je indetitet utvrđen ili se može utvrditi. Osobne podatke također čine i različite informacije, pomoću kojih se, kad se one prikupe zajedno, može utvrditi identitet određene osobe. Osobni podatci koji su deidentificirani, šifrirani ili pseudonimizirani, ali se mogu upotrijebiti za ponovno utvrđivanje identiteta osobe, ostaju osobnim podatcima te su obuhvaćeni područjem primjene OUZP-a (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr).

Opća uredba o zaštiti podataka (OUZP) je uredba donesena od strane Europskog parlamenta i Vijeća te ona uređuje obradu osobnih podataka povezanih s pojedincima u EU-u koju vrše pojedinac, društvo ili organizacija. Uredba se ne primjenjuje na obradu osobnih podataka preminulih ili pravnih osoba. Pojedinac mora poštovati pravo o zaštiti podataka kada osobne podatke upotrebljava izvan "osobnog prostora" za sociokulturne ili financijske aktivnosti (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_hr).

U slučaju kada su osobni podatci učinjeni anonimnima i kada se preko njih ne može utvrditi identitet pojedinca, tada se oni više ne smatraju osobnim podatcima. Primjer osobnih podataka je ime i prezime, adresa stanovanja, mail adresa (adresa elektroničke pošte), broj važećih isprava (npr. osobne iskaznice), podatci o lokaciji (koji se lako mogu saznati putem mobitela pomoću funkcije lokacija), adresa pomoću koje pristupamo internetu (adresa internetskog protokola-IP), identifikacijski broj kolačića i slično (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr).

Kako bi se zapravo došlo na ideju o izradi aplikacija o zaštiti osobnih podataka, potrebno je naglasiti kako su osobni podatci izuzetno izloženi riziku, posebno prilikom pristupanja internetskim stanicama i društvenim mrežama. Promatramo li najmlađu skupinu koja se služi internetom, djecu, kako je već u ranijem poglavlju opisano, ona dosta često svoje osobne podatke izlažu riziku. Bilo to davanje nepoznatoj osobi svoju adresu ili otkrivanje punog imena i prezimena, podatci pojedinca od trenutka kada se oni postave online, predstavljaju veliki rizik za sigurnost osobe-djeteta, o čijim se podatcima radi.

Zbog gore navedenih razloga počele su se izrađivati aplikacije o zaštititi osobnih podataka, koje se jednostavno, preko internet trgovina, mogu besplatno preuzeti na pametni telefon ili tablet. Aplikacija AZOP, koju je razvila Agencija za zaštitu osobnih podataka, namjenjena je djeci i mladima kao vodič, kako se ponašati i zaštititi na internetu i društvenim mrežama. Aplikacija zajedno sa time sadrži još i kratki internetski pojmovnik te savjete za roditelje, nastavnike, školske pedagoge i psihologe (https://www.medijskapismenost.hr/aplikacija-iz-koje-djeca-i-mladi-mogu-uciti-o-zastiti-osobnih-podataka/)

Promatrana aplikacija sastoji se od nekoliko cjelina pomoću kojih se djecu educira o različitim aspektima važnosti privatnosti djece i mladih u svijetu modernih tehnologija. Cjeline od koji se sastoji aplikacija su privatnost i osobni podatci, što ti internet pruža, sigurnost na internetu, pravila lijepog i finog ponašanja na internetu za djecu i mlade te posjetnik kako se nikada neću ponašati na internetu i društvenim mrežama (https://www.medijskapismenost.hr/aplikacija-iz-koje-djeca-i-mladi-mogu-uciti-o-zastiti osobnih-podataka/).

4. ZAŠTITA I SIGURNOST DJECE NA INTERNETU

4.1. Zakonska regulativa sigurnosti – GDPR

Opća uredba o zaštiti podataka (General Data Protection Regulation), novi je zakon o zaštiti privatnosti i osobnih podataka. Primjenjuje se u svih 28 država, članica EU-a. Razlog zašto je uopće nastao krije se u zloupotrebi podataka. Odnosno GDPR-om se pokušava korisnicima dati više nadzora nad načinom na koji se njihovi podatci (zlo)upotrebljavaju. Zaštita osobnih podataka izrazito je važna kod velikih organizacija i tvrtki. Ukoliko one čuvaju i štite podatke svojih korisnika, korisnici će biti zadovoljni njihovom uslugom te će se odužiti tako što će i dalje ostati kod njih,a ne se primjerice probacit kod konkurencije. Analiza koju je provodila RSA Security, u kojoj je sudjelovalo preko 7500 osoba iz Francuske, SAD-a, Italije, Njemačke i Ujedinjenog Kraljevstva, pokazala je da korisnici drže do privatnosti svojih podataka i ne opraštaju tvrtkama koje gube njihove podatke. Čisto za primjer, čak 62% ispitanika za gubitak osobnih podataka, krivi organizaciju ili tvrtku, a ne hakere koji su te iste podatke ukrali. To je dokaz, koliko je zapravo GDPR važan. Zaključak same analize je da se tvrtke sve više okreću digitalnom svijetu te da pri tome moraju voditi računa o nadzoru i zaštiti podataka i to na dnevnoj bazi (https://gdprinformer.com/hr/vodic-kroz-gdpr).

Slika 7. GDPR (http://gdprinstitute.eu)

Slika 7. prikazuje ukratko što je to GDPR i od čega se sastoji. GDPR sa sobom zapravo nosi promjenu koncepta zaštite podataka, koja se isto provodi u svim zemljama, članicama Europske unije. Također ovom uredbom, moguće je puno strože kažnjavanje, ono obuhvaća i razvoj novih sustava, strategija i proizvoda, organizacije imaju puno veću odgovornost prilikom korištenja podataka. Regulativa sustiže razvoj tehnologije i daje nova prava pojedinca.

GDPR se primjenjuje samo na osobne podatke iz kojih se isključuju anonimizirani podatci, kako je već ranije u radu opisano. Podatci koje GDPR smatra osobnima su osnovni podatci o korisniku/pojednicu poput imena i prezimena, broja osobne iskaznice i lokacijskih podataka, podatci s kreditnih kartica, zdravstveni karton (invalidnost, povijest bolesti i sl.), biometrijski podatci (sken rožnic, otisak prsta i sl.), genetski podatci (DNA), vjerska i filozofska uvjerenja, etnička pripadnost, ekonomsko stanje, članstvo u sindikatu, IP adrese, osobne poruke e-pošte, kolačići u pregledniku i pseudonimizirani podatci (https://gdprinformer.com/hr/vodic-kroz-gdpr).

Prilikom obrade podataka postoje i određena načela koja je potrebno poštivati i koja predstavljaju najključniji dio GDPR-a. Podatci se smiju obrađivati samo na valjanoj zakonskoj osnovi, na pošten i prema ispitaniku transparentan način, obavezno je navođenje svih svrha u koje se podatci prikupljaju. Prikupljati se smiju samo podatci koji su relevantni i potrebni za ispunjavanje svrhe u koju se obrađuju, podatci trebaju biti točni i ažurni. Podatci se ne smiju pohranjivati duže od razdoblja potrebnog za ispunjavanje svrhe u koju su prikupljenji. Onaj tko prikuplja podatke, dužan je osobne podatke zaštititi od nezakonite i nedozvoljenje obrade, slučajnog gubitka ili uništenja te također mora biti u stanju dokazati usklađenost sa svim navedenim načelima (https://gdprinformer.com/hr/vodic-kroz-gdpr).

Razlog zašto se govori o GDPR-u u temi rizici za djecu na internetu je upravo taj što većina djece kreće u vrtiće, a nakon toka upisuju osnovnu školu. Upisom u osnovnu školu, djeca daju svoje osobne podatke, jer drugačije to niti ne bi bilo moguće. Škole se sve više moderniziraju i gotovo svi podatci se nalaze online, što znači da su osobni podatci djece na neki način ugroženi i da podliježu GDPR-u. Škole i ostale javne ustanove istotako su dužni poštivani GDPR i postupati u skladu s njegovim načelima. Osobne podatke koje škola obrađuje su podatci učenika i zaposlenika. Podatci učenika obrađuju se zbog provođenja

odgojno-obrazovne djelatnosti (https://sindikat-preporod.hr/opca-uredba-o-zastiti-podataka-u-skoli/). Postoji razlika između podataka koji su dostupni o učeniku. Podatci se dijele na osobne podatke i na osjetljive podatke. U osobne podatke o učeniku spadaju ime, prezime, adresa učenika, podatci za kontakt, zapisi o disciplinskim postupcima, svjedodžbe i izvješća o napretku. Posebnu kategoriju podataka, osjetljivu, čine biometrijski podatci o učeniku (njegova slika), vjerska uvjerenja (da li učenih pohađa vjeronauk), zdravlje (alergije i bolesti) ili prehrambeni zahtjevi (koji mogu ukazivati na učenikovu vjeru ili zdravlje). Podatci koji su u toj kategoriji, učenike mogu izložiti riziku. Takve podatke škola ne smije obrađivati, bez privole roditelja djeteta (https://www.schooleducationgateway.eu/hr/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm).

Slika 8. Objava učenika u novinama (https://www.mercurynews.com/2019/05/24/college-scandal-this-bay-area-student-newspaper-nixed-a-popular-map-of-where-seniors-are-bound-for-college/)

Stupanjem na snagu GDPR dovodi određene promjene u školsku svakodnevicu. Većina škola koristi oglasne ploče, na kojim objavljuje rang liste, popise učenika i slično. Stupanjem na snagu ovog zakona, škola je dužna zaposliti zaštitara ili prikladnu odraslu osobu, koja bi

nadzirala oglasnu ploči i tako spriječila da se podatci koji se nalaze na njoj snimaju i izlažu mogućnosti krađe. Slična stvar događa se i kada učenici sudjeluju u natjecanjima. Na svako natjecanje učenik pristupa šifrom (lozinkom), kako bi ono ostalo anonimno te kasnije preko te lozinke dobiva rang listu i svoje rezultate. Ovaj postupak vrijedi i po GDPR-u uz određene dodatke. Primjerici ukoliko maloljetni učenik pristupa natjecanju te koristi svoju lozinku, ali obzirom da je maloljetan, od roditelja mora dobiti potpisanu privolu, kako bi se njegovi podatci mogli koristiti dalje u natjecanju i objavi rezultata. Također bez pristanka roditelja, fotografija učenika uslikana na natjecanju, sa nagradama ili samo u okrugu škole, ne smije bit korištena na školskim stranicama. Prikaz dosadašnjeg korištenja slike učenika prikazan je Slikom 8.

Jedna od novosti uvođenjem GDPR-a je ta da se učenici smatraju odraslom i odgovornom osobom već sa 16 godina. Smanjenje dobne granice za dvije godine velika je promjena, a ona sa sobom nosi velike odgovornosti i brige. Odnedavno u Republici Hrvatskoj vrijedi da roditelj može online vidjeti sve ocjene svojeg djeteta. Promjenom dobne granice, roditeljima djece starije od 16 godina, ocjene nisu dostupne, već moraju zatražiti privolu od djeteta kako bi imali uvid u podatke (https://www.jutarnji.hr/vijesti/hrvatska/gdpr-donosi-i-niz-promjena-u-skole-roditelji-nece-moci-vidjeti-ocjene-i-izostanke-u-imeniku-svoje-djece-koja-su-navrsila-16-godina-bez-njihove-privole/7399272/).

4.2. Prijetnje, ranjivost i napad

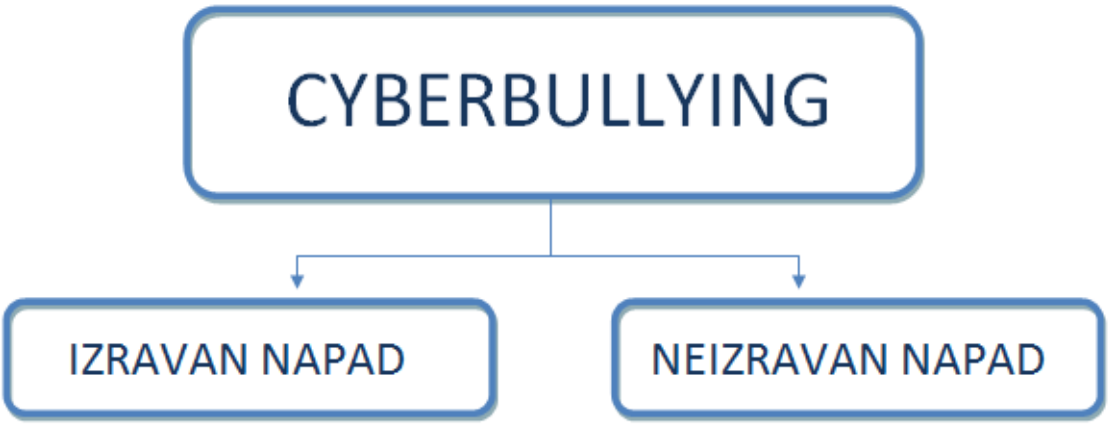
Prijetnje, ranjivost i napad vezani su za sigurnost informacijskih sustava. Ona može biti ugrožena na više načina. Prijetnja, u kontekstu informacijske sigurnosti je objekt, osoba ili drugi entitet koji predstavlja stalnu opasnost za imovinu organizacije, također, prijetnaj je definirana kao mogući uzrok neželjenog incidenta koji može uzrokovati štetu sustavu ili organizaciji (Vukelić, 2016.). Prijetnja u kontekstu rizika djece na internetu predstavlja sve moguće prijetnje koje se mogu dogoditi, za vrijeme korištenja interneta. Primjerice zlonamjerne poruke, cyberbullying, vrijeđanje, krađa lozinka i slično. Prijetnja može prouzrokovati meželjenu situaciju, čija posljedica može biti trajno nanošenje štete imovini, ukoliko se govori o informacijskoj sigurnosti te psihološka i fizička šteta na djetetu, ukoliko se govori o sigurnosti djece na internetu. Prijetnje možemo podijeliti prema izvoru na one nastale od ljudi, bilo namjerno ili nenamjerno i na one nastale zbog opreme i prirodnih nepogoda. Svaka prijetnja ima obilježja koja pružaju korisne informacije o samoj prijetnji, a to su izvor, motiv, učestalost ponavljanja i razorna moć (Vukelić, 2016.).

Ranjivost se može definirati kao stanje ili skup stanja koja mogu omogućiti nekoj prijetnji da utječe na resurse. U smislu informacijske sigurnosti ona se povezuje s propustima u programskom kodu, neprikladan izbor tehnologija i alata, propust u implementaciji i sl (Vukelić, 2016.). Ranjivost u smislu rizika djece na internetu predstavlja osobnost svakog djeteta koje se nalazi online te njegove reakcije na dobivene poruke i ostalo što se oko njega događa. Također u to spada i povodljivost djeteta te utjecaj jednog djeteta na drugo u cilju iskorištavanja i vjerovanja.

Napad su akcije direktno usmjerene na ugrožavanje sigurnosti informacija, računalnih sustava i mreža. Interes počinitelja može se definirati kao napad ili provala radi ostvarenja koristi ili štete ili upad radi samodokazivanja. Podjela napada dijeli se na aktivni (uz mijenjanje podataka) i pasivni (samo neovlašteni pristup, bez mijenjanja podataka) (Vukelić, 2016.). Promatrano kroz temu rizika djece na internetu u napad bi spadali neki od idućih primjera. Primjerice slanje virusa kroz poruke ili preuzimanje, gdje se idrektno napada dijete ili računalo koje on koristi, te kroz razne poruke i vrijeđanja ili nagovaranje i direktan fizički susret sa lošim namjerama.

4.3. Cyberbullying

Cyberbullying u prijevodu nasilje preko interneta, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom, kako za pojedinca, tako i za opće dobro. Također to je nasilje koje se odvija između vršnjaka, na način kada je jedno dijete izloženo napadu drugog djeteta ili grupe djece, putem interneta ili mobilnog telefona (https://www.poliklinika-djeca.hr/publikacije/nasilje-preko-interneta/).



Slika 9. Vrste cyberbullyinga

Postoje dvije vrste cyberbullyinga, izravan i neizravan napad (napad preko posrednika). Na Slici 9. prikazana je podjela cyberbullyinga na dvije vrste. Izravan napad podrazumijeva kada jedno dijete drugom šalje uznemirujuće poruke mobitelom, e-mailom ili na chatu. Također u to spada i krađa/ promjena lozinke na e-mailu ili nadimak na chatu, objavljivanje neistina na internetu te slanje poruka uznemirujućeg sadržaja putem inerneta ili mobilnog telefona, bilo slika, videa ili postavljanje internetskih anketa o žrtvi. Napad preko posrednika je vrsta cyberbullinga kada počinitelj napada žrtvu preko treće osobe koja najčešće toga nije svjesna. Primjer toga je probijanje šifre ili uzimanje mobitela i u tuđe ime slanje poruka neprimjerenog sadržaja trećoj osobi (https://www.slideshare.net/novimediji/nasilje-na-internetu).

Nasilje preko interneta opasnije je od uobičajenog vršnjačkog nasilja, tu se nalazi veća publika, napisane riječi bole i ostaju duže od izgovorenih, nažalost tu je i anonimnost, koja štiti nasilnika te ne postoji mogućnost izbjegavanja zlostavljanja, a jedan od razloga je što je internet dostupan 24 sata dnevno. Anonimnost nasilniku pružaju nadimci, ukoliko se govori o internetu i nepoznat broj, ako je riječ o mobitelu. Nasilnicima je preko tipkovnice lakše uplašiti žrtvu, a istotako i teže je otkriti počinitelja i njegovu lokaciju (https://odrastisretan.wordpress.com/2013/05/19/cyberbullying-medu-djecom-i-mladima/).

Slika 10. Posljedice cyberbullyinga (http://cnzd.org/vijesti/poziv-za-ukljucivanje-u-trening-za-trenere-na-temu-sigurnost-i-zastita-djece-i-mladih-na-internetu-koji-ce-se-odrzati-u-splitu)

Posljedice Cyberbullyinga su često veće nego što se može zamisliti. Takva vrsta nasilja utječe na psihološko i fizičko odrastanje djece. Djeca koja su zlostavljana na taj način često su emocionalno uznemirena za vrijeme ili poslije korištenja interneta, izbjegavaju druženje s prijateljima i uobičajene svakodnevne aktivnosti, izbjegavaju školu i grupna okupljanja, također može se dogoditi da dijete popusti u školi te da ima napade bijesa, nagle promjene raspoloženja i ponašanja, gubitak sna i apetita (os-dcesaric-os.skole.hr/upload/os-dcesaric-os/.../ELEKTRONICKO%20NASILJE.pps). Na Slici 10. prikazana je djevojčica te njezino emocionalno stanje, nakon što je na njoj izvršeno elektroničko nasilje.

Obzirom na rasprostranjenost društvenih mreža i aplikacija, cyberbullying više nije tako rijetka pojava. Danas na dnevnoj bazi djeci dolaze svakakve uznemirujuće poruke i sadržaji. Za početak, veliki dio toga može se vidjeti na televizoru, preko reklama. Obzirom da reklame postoje na različite teme i prikazuju različite sadržaje to može laku utjecati na djecu, kako na nasilnika, kojemu daje dodatne ideje, tako i na žrtvu, jer ju određene scene mogu dodatno preplašiti.

Djeca počinju koristiti internet u sve mlađoj dobi te nažalost zbog toga sve manja djeca prolaze kroz to da se nad njima vrši cyberbullying ili da ona zapravo provode elektroničko nasilje. Cyberbullyingom se cilja na veću populaciju, ako se nešto objavi online u istom trenutku to može vidjeti veći broj ljudi nego kada bi se zasebno govorilo jednom po jednom. Nažalost takvom vrstom nasilja potiće se grupna mržnja, odvijaju se napadi na privatnost, uznemiravanje, uhođenje, vrijeđanje, nesvjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih koomentara. Također može uključivati i slanje okrutnih, zlobnih, a katkad i prijetećih poruka, kao i kreiranje internetskih stranica, koje sadrže priče, crteže, slike i šale na račun vršnjaka (https://www.poliklinika-djeca.hr/publikacije/nasilje-preko-interneta/).

Istraživanje koje je provedeno 2017. godine na uzorku od 1017 djece i roditelja u Hrvatskoj, eU Kids Online, došlo je do zaključka da je najkorištenija društvena mreža među djecom od 9 do 17 godina u Hrvatskoj, Facebook, dok se na drugom mjestu nalazi Instagram (http://www.djecamedija.org/wp-content/uploads/2018/05/sigurnost-djece-na-internetu-2018-v2.pdf).

4.3.1.Utjecaj cyberbullyinga na djecu

Kako bi se pokazalo da je cyberbullying jako česta pojava kod djece, u nastavku je dano nekoliko stvarnih primjera. Kako bi se bolje razumjeli neki od navedenih članaka, u Tablici 2. dano je pojašnjenje za neke od korištenih cyberbullying pojmova.

Tablica 2. Rječnik cyberbullying pojmova (http://www.djecamedija.org/wp-content/uploads/2018/05/sigurnost-djece-na-internetu-2018-v2.pdf)

CYBERBULLYING POJAM	OBJAŠNJENJE
Catfishing	Otvaranje lažnih profila putem kojih napadač navodi drugu osobu na ljubavnu vezu putem interneta.
Cyber uhođenje	Učestala radnja koja uključuje prijetnje i nanošenje štete nečijoj privatnosti.
Flaming	Namjerno slanje agresivnih, uvredljivih i neprimjerenih poruka s ciljem poticanja online svađe i nasilja.
Grooming	Mamljenje djece radi seksualnih potreba.
Happy slapping	Grupa napada pojedinca, nasilje snima mobitelom ili kamerom i kasnije snimku objavljuje na internetu.
Malware	Zlonamjerni programi koji mogu ugroziti računalo.
Phishing	Prevara koja korisnika navodi na otkrivanje korisničkog imena i lozinke i upisivanje u krivotvorenu internetsku stranicu.
Sexting	Slanje neprimjerenih seksualnih poruka i fotografija putem mobitela ili interneta.
Spam	Neželjena elektonička pošta, najčešće u obliku reklama i lažnih oglasa koja može biti i opasna, ako u sebi sadržava virus, koji otvaranjem poruke momže naštetiti računalu.
Trolling	Namjerno učestalo širenje sarkastičnih komentara upućenih slučajno odabranoj osobi s ciljem izazivanja sukoba.

O Cyberbullyingu u Hrvatskoj počelo se je pisati prije otprilike šest godina, kada je on već naveliko postojao. U članku iz 2015. godine objavljenom na internetskoj stranici tportal.hr-a, može se vidjeti kako su već tada, kad se internet manje koristio, 25% djece i adolescenata u Republici Hrvatskoj bili žrtve elektroničkog nasilja. U članku stoje i sljedeći podatci: " Policija je u zadnje dvije godine zaprimila 2306 anonimnih prijava zlostavljanja preko interneta, a samo ove godine zaplijenila 2500 fotografija, 3000 videozapisa i 400 GB sadržaja dječje pornografije" (https://www.tportal.hr/vijesti/clanak/cak-25-posto-djece-i-adolescenata-u-rh-zrtve-cyberbullyinga-20151214).

Ovi podatci pokazuju koliko je ova tema zapravo jako malo zastupljena u javnosti, obzirom koliko bi se trebalo razgovarati o njoj. Činjenica da je toliko djece zlostavljano na ovakav način, trebala bi potaknuti sve ljude da malo razmisle o svom ponašanju, da koliko je god to moguće, roditelji, kontroliraju svoju djecu, bilo to s kime i koliko ili na kakav način pišu. Kada bi svaki pojedinac napravio jedan korak prema poboljšanju i spriječavanju ovakvih događaja, puno bi pomogli ne samo žrtvama cyberbullyinga, nego i sami sebi. Od 2015. godine do danas popularnost interneta puno je porasla. Nažalost društvene mreže su preuzele vodstvo u komunikaciji između ljudi i djece te doprinijele nekim jako lošim navikama i utjecajima. Preko društvenih mreža, današnja djeca mjere svoju popularnost, što je izrazito zabrinjavajuće, odnosno kako se navodi u članku, jedan lajk je postao mjerna jedinica za popularnost. Kako bi prikupili što više lajkova na svojim fotografijama, te tako stekli popularnost, djeca ne razmišljaju o rizicima koje te fotografije sa sobom nose. Objavljene fotografije može vidjeti svatko, ukoliko to nije drukčije namješteno u postavkama privatnosti, a dosta često su i komprimitirajućeg sadržaja. Te fotografije svatko može preuzeti te proslijediti dalje, te tako ugroziti sigurnost pojedinca. Jedan od načina elektroničkog nasilja predstavlja i takav vid fotografija, koje druge osobe objavljuju bez znanja i dopuštenja ulikane osobe sa slike. Na slike se nadovezuju neugodni komentari te to sve zajedno jako utječe na djetetovo (žrtvino) odrastanje. Kako sve mlađa djeca koriste internet, to znači da su i sve mlađa djeca u kontaktu sa cyberbullyingom. Bilo da su oni nasilnici ili žrtve. Upravo godine predstavljaju još jedan problem prilikom kažnjavanja nasilnika: " Policija kao kaznena djela procesuira povredu privatnosti djeteta, nedozvoljenu upotrebu osobnih podataka i nametljivo ponašanje, ali samo ako je počinitelj stariji od 14

godina"(https://www.tportal.hr/vijesti/clanak/cak-25-posto-djece-i-adolescenata-u-rh-zrtve-cyberbullyinga-20151214). Sve je više nasilnika koji su mlađi od četrnaeste godine života, a njihovi stavovi i ponašanje na jako su lošoj razini. Nažalost za sada još uvijek nije moguće njihovo kažnjavanje, najveća kazna je pozivanje odnosno obavještavanje centra za socijalnu skrb i kažnjavanje roditelja/skrbnika za kazneno djelo povrede djetetova prava, ako se utvrdi da je takvo ponašanje posljedica zanemarivanja maloljenika u obitelji (https://www.tportal.hr/vijesti/clanak/cak-25-posto-djece-i-adolescenata-u-rh-zrtve-cyberbullyinga-20151214).

Slika 11. Primjeri cyberbullyinga (https://schoolsthatrock.co.za/how-to-keep-your-child-save-cyberbullying/)

Na Slici 11. prikazane su najčešće uvrede sa kojima se djeca susreću kada je riječ o cyberbullyingu, nažalost uvrede mogu biti puno veće i zlobnije od navedenih, a nerijetko imaju i najgore završetke.

U članku iz 2012.godine, objavljenog na portalu Dnevno.hr, može se vidjeti koliko su zapravo društvene mreže olakšale nasilje te do koje razine je sve došlo (https://www.dnevno.hr/vijesti/hrvatska/facebook-odnosi-prve-zrtve-sve-cesci-slucajevi-ubojstva-i-samoubojstva-djece-66176/).

"Šokantni su podaci da sve više maloljetnika gubi život i to zbog nasilja kojem je bilo izloženo. Jedan od posljednjih takvih slučaja dogodio se u Nizozemskoj. Sve je počelo kad je žrtva Joyce na Facebooku pisala uvrede o prijateljici Polly koja je na kraju sa dečkom Wesleyom odlučila ubiti Joyce. Maloljetnu Joyce na kraju je ubio vršnjak i to za 100 eura, koliko mu je platila Polly, a dogovor o ubojstvu pao je na Facebooku." (https://www.dnevno.hr/vijesti/hrvatska/facebook-odnosi-prve-zrtve-sve-cesci-slucajevi-ubojstva-i-samoubojstva-djece-66176/).

"Stravičan slučaj cyberbullyinga dogodio se i u Americi. Trinaestogodišnja Megan Meier iz Missourija započela je vezu putem interneta sa 16-godišnjim Joshom koji je tvrdio da živi u susjednom gradu. Nekoliko tjedana kasnije Josh joj je rekao da više ne želi biti s njom jer je čuo da nije dobra osoba i rekao joj da bi svijet bez nje bio bolje mjesto. Par dana kasnije Megan se objesila. Policija je nakon nekoliko tjedana saznala da je Josh izmišljena osoba koju je stvorila Lori Drew, majka Meganine bivše prijateljice." (https://www.dnevno.hr/vijesti/hrvatska/facebook-odnosi-prve-zrtve-sve-cesci-slucajevi-ubojstva-i-samoubojstva-djece-66176/).

Cyberbullying nije samo prolazna tema, kao što se može vidjeti iz prethodna dva članka, uvrede i poniženja koja se događaju online na djecu puno više i jače utječu. Kada djeca više ne mogu podnijeti takvo nasilje, najčešće se prvo povuku u sebe, a zatim se krenu samoozlijeđivati. Naposlijetku, kao najgora varijenta, sve veći broj djece izabire put bez povratka te presude sami sebi.

Nažalost takvih slučaja ima ne samo u svijetu, nego i u Hrvatskoj. U članku koji je 2018. godine objavljen na portalu 100 posto, objavljene su i poruke, koje je dobivala djevojčica koja je ostala bez majke. Poruka glasi " Nemaš ni mamu ni tatu i sad ideš u dom. Neka ti, tako ti i treba, hvala bogu što si izgubila roditelje, sad nemaš više nikog" i "Još samo da ti sestra umre i to je to, ali bolje da i ti umreš prije nje, droljo." (https://100posto.hr/news/vrsnjacko-nasilje-u-hrvatskoj-postaje-sve-brutalnije-roditelji-preuzmite-stvar-u-svoje-ruke-evo-najbrutalnijih-ispada). Po okrutnosti poruke može se vidjeti kako djeca uopće nemaju granica kada je u pitanju vrijeđanje i omalovažavanje svojih vršnjaka. Riječi se uopće ne biraju i jedini je cilj povrijediti osobu online te povećati svoju navodnu popularnost. Takvo ponašanje problem je cijelog društva i zajednice, a također i jedan od glavnih podloga cyberbullyinga.

Sva ta vrijeđanja dovela su i do smrtnih slučajeva u Hrvatskoj. Petnaestogodišnja djevojka iz Zagorja, počinila je samoubojstvo nakon što je neko vrijeme bila izložena cyberbullyingu. "Grupa zasad nepoznatih djevojaka i dječaka grubo ju je vrijeđala preko profila na latvijskoj društvenoj stranici Ask.fm. Brutalne uvrede, psovke, sramoćenje i omalovažavanje nisu prestajali tjednima, navodi Slobodna Dalmacija (https://www.slobodnadalmacija.hr/novosti/crna-kronika/clanak/id/202851/zasto-je-umrla-15-godisnja-mj-ubila-se-zbog-vrijeanja-na-internetu-ili-je-rijec-o-ubojstvu).

"Nažalost, vrijeđanja nisu stala niti nakon njezine smrti. “Ko joj j... mater, nek se ubila”, napisao je jedan mladić na Facebook stranici napravljenoj u njeno sjećanje." (https://www.slobodnadalmacija.hr/novosti/crna-kronika/clanak/id/202851/zasto-je-umrla-15-godisnja-mj-ubila-se-zbog-vrijeanja-na-internetu-ili-je-rijec-o-ubojstvu).

"Lani evidentrirali 362 slučaja cyberbullyinga" naslov je članka objavljenog na stranici večernji.hr. iz 2019. godine. Najčešće je riječ o onim najmlađima, učenicima 3,4 i 5 razreda osnovnih škola (https://www.vecernji.hr/lifestyle/policija-nam-je-otkrila-broj-zrtava-cyberbullyinga-lani-evidentirali-362-slucaja-1318419).

Elektroničko nasilje iako je već previše rasprostranjeno, još uvijek ne staje. većini počinitelja teško se ulazi u trag, a posljedice koje takvo nasilje izaziva ponekad su i smrtonosne. Potrebno je krenuti od pojedinca, a završitio na promjenama određenih zakoja, koji bi kažnjavali nasilnike, bez obzira na godine. Naposlijetku, ako se on ne kazni dok je još to moguće, do koje mjere njegovo nasilje može ići i koliko djece ugroziti.

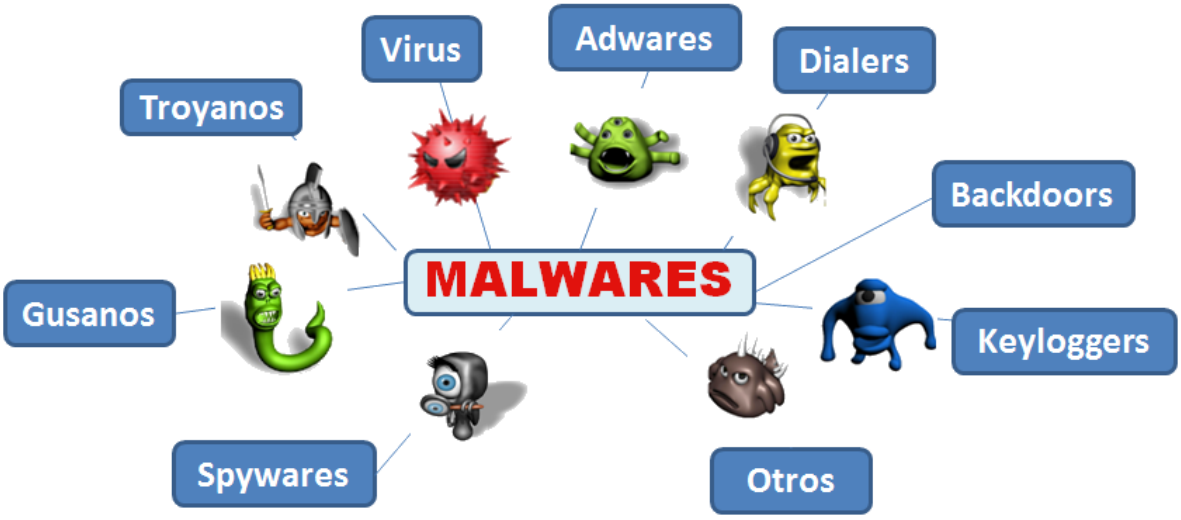
4.4. Zaštitne mjere

Zaštitne mjere su svi postupci, procedure i mehanizmi kojima se štite resursi informacijskog sustava od prijetnji te se smanjuje njihova ranjivost, otkrivaju se neželjeni događaji i smanjuje se njihov učinak te se pospješuje oporavak. Uloga zaštitnih mjera je prevencija, odvraćanje, otkrivanje, ograničavanje, korigiranje, oporavak, nadzor i osvješćivanje. Uloge mogu biti pojedinačne ili kombinacija više njih. Kod podjele (Slika 12.), zaštitne mjere dijele se na zaštitu samih podataka, programsku zaštitu, organizacijsku zaštitu te fizičku i tehničku zaštitu (Vukelić, 2016.).

Slika 12. Podjela zaštitnih mjera

Rizici sa kojima se djeca susreću na internetu mogu se promatrati u dvije kategorije. To su rizici koji ugrožavaju računalo i rizici koji ugrožavaju samu djecu i korisnike interneta. Zaštitne mjere kojima se može smanjiti ugožavanje računala, ukoliko se provode, su održavanje operacijskog sustava ažurnim, korištenje antivirusnih programa, puštanje uključenog vatrozida, a također zaštiti može doprinijeti i stvaranje sigurnosnih kopija važnih datoteka te pažnja prilikom preuzimanja raznih sadržaja sa interneta. Rizici koji se javljaju prilikom korištenja interneta od strane djeteta, uvelike ovise i načinu otvorenosti djeteta. Kako bi se rizik smanjio potrebno je biti pažljiv prilikom objavljivanja osobnih podataka, potrebno je poznavati osobe sa kojima se komunicira online, također treba imati na umu da na mreži nisu sve stranice pouzdane te svi korisnici društvenih mreža iskreni (http://os-

senkovec.skole.hr/upload/os-senkovec/newsattach/482/Sigurnost_djece_na_internetu-savjeti_za_roditelje.PDF).



Slika 13. Zloćudni softveri (https://blog.dimensidata.com/tips-mencegah-masuknya-virus-dan-malware-pada-komputer/)

Na Slici 13. prikazani su zloćudni (zlonamjerni) softveri, softverski programi koji su napravljeni tako da se neprimjetno ubace u sistem računala te naprave određenu štetu. Neki od štetnih softvera su virusi, crvi, trojanski konj, špijunski softver i slično (https://bs.wikipedia.org/wiki/Malware).

Zaštitne mjere vezane za elektroničko nasilje također proilaze od osobnih podataka te njihove dostupnosti online poput adrese i broja mobitela. Prilikom stvaranja profila ili računa lozinke je potrebno sačuvati samo za sebe. Kada se koriste društvene mreže, najbolja zaštita je postavljanje svog profila u postavkama na privatno, kako nepoznate osobe ne bi mogle pristupiti i kontaktirati djete/korisnika. Kod objavljivanja fotografija sebe i svojih bližnjih potrebno je paziti na nekoliko stvari. Treba imati na umu da sve što se jednom nađe online, zapravo zauvijek tako i ostane. Fotografije koje se objavljuju ne bi smjele biti u nikakvim neprimjerenim pozame te neprimjerenog sadržaja. Treba biti oprezan sa slanje i objavljivanjem iz razloga što se takve stvari uvijek mogu prosljeđivati do ostalih korisnika. Prilikom dobivanja poruka od nepoznatih osoba ili nepoznatih e-adresa, iste se ne bi smjele otvarati. U slučaju dobivanja zahtjeva za prijateljstvo ili poruka od nepoznatih osoba, oni se ne bi smjeli prihvaćati niti otvarati, obzirom da se nikad ne može biti sigurno tko se iza tih

profila krije niti koje su mu namjere. Svađe i ružno dopisivanje preko društvenih mreža trebalo bi izbjegavati. Jedna od najbitnijih stvari, obzirom da se nikad ne zna tko se stvarno krije iza profila, susrete s nepoznatom osobom treba izbjegavati. Još jedna važna stavka prilikom korištenja društvenih mreža i ostalih online aplikacija, bilo bi poželjno isključivati lokaciju na mobilnim uređajima te ne stalno objavljivati gdje se dijete i sa kime nalazi (http://www.djecamedija.org/wp-content/uploads/2018/05/sigurnost-djece-na-internetu-2018-v2.pdf).

Kako bi se gore navedene zaštitne mjere lakše i pažljivije poštivale, obzirom da se govori o zaštitnim mjerama i rizicima djece na internetu, potrebno je uključiti i roditelje, odrasle osobe. Neki od savjeta kako pomoći i smanjiti rizike djeteta na internetu dani su na web stranici Poliklinike za zaštitu djece i mladih Grada Zagreba. Za početak potrebno je računalo postaviti u zajedničku sobu, primjerice dnevni boravak, kako bi uvijek uz dijete ili u blizini djeteta bio roditelj. Time bi se olakšala i povećala kontrola sadržaja pretraživanja te imao bolji pregled online prijatelja i dopisivanja. Važno je da roditelji nauče poznavati internet, da se znaju koristiti njime i osnovnom terminologijom, jer tako mogu pomoći djetetu prilikom korištenja. Bitno je postaviti određeni skup pravila zajedno sa djecom, kako bi se definiralo vrijeme korištenja i svrha korištenja računala i interneta. Moguće je da će dijete htjeti upoznati online prijatelja ili prijateljicu. Kod takvih susreta, pogotovo prvog, dijete nikad ne smije ići samo već u pratnji odrasle osobe te na kraju, u slučaju da postoje bilokakve naznake da su osobe s neprijateljskim namjerama stupile u kontakt sa djetetom, saznali osobne podatke ili prijete djetetu, potrebno je kontaktirati policiju te potražiti pomoć (https://www.poliklinika-djeca.hr/za-roditelje/izazoviroditeljstva/o-djeci-i-internetu/).

4.4.1. Postojeće zaštitne mjere za djecu

Zbog sve većeg korištenja interneta i sve većih rizika kojima su djeca izložena, kako u svijetu tako i u Hrvatskoj, sve se više pažnje posvećuje zaštitnim mjerama. Hrvatski telekom tako je u svoju ponudu uvrstio i paket roditeljske zaštite u skolpu koje se omogućuje filtriranje internetskog sadržaja kako bi djeca sigurno surfala i komunicirala i bez roditeljskog nadzora. Također na internetskim stranicama Hrvatskog Telekoma dostupan je i kviz o roditeljskoj zaštiti, gdje roditelji mogu provjeriti svoje znanje i saznati sve informacije o sigurnom korištenju interneta (https://www.hrvatskitelekom.hr/dodatne-usluge/roditeljska-zastita/brosura).

Osim Hrvatskog Telekoma i firma Microsoft također na svojim stranicama nudi alat za zaštitu/sigurnost djece na internetu. Iako, obzirom na užurbanost zajednice, ljudi imaju sve manje vremena za ovakav način obrazovanja i zaštite, trebalo bi pronaći barem malo vremena, pogotovo roditelji, kako bi lakše zaštitili djecu od rizika na internetu. Alat Family Safety pruža internetsku stranicu i besplatan program koji se može instalirati na računalo kojim se koristi djete. Na taj način omogućuje se djetetu da samostalno koristi računalo i internet, a u isto to vrijeme obavlja se praćenje online aktivnosti. Pomoću alata Family Safety može se i onemogućiti pristup internetskim stranicama za koje roditelj smatra da nisu prikladne za njegovo dijete, kao i filtriranje komunikacije samo s osobama s kojima dijete ima nešto zajedničko. Uz pomoć Windows Live Hotmail, Windows Live Messenger i Windows Live Spaces, roditelj može izabrati osobe s kojima će njegovo dijete moći komunicirati. Time se djetetu onemogućava razgovor sa nepoznatim osobama, jer se one ne nalaze na popisu kontakata koji su djeci dostupni (https://djecamedija.org/rk/sigurnost/sigurnost-djece-na-internetu-uz-pomoc-microsoft-alata/).

5. ZAKLJUČAK

U ovom radu analizirani su rizici, prijetnje i opasnosti sa kojima se djeca susreću prilikom korištenja interneta. Te opasnosti su mnogobrojne i uvelike ovise o djetetovoj dobi, vremenu provedenom na internetu i naravno sadržajima kojima dijete pristupa. Opasnosti i rizici dijele se u dvije skupine, one koje nanose štetu uređaju, odnosno rizici u vidu raznih virusa, kojima se indirektno utječe na sigurnost djeteta, primjerice krađa podataka sa računala i slično ili opasnosti kojima je dijete direktno izloženo kada se nalazi online, poput cyberbullyinga i online razgovora. Obzirom da je život bez interneta u današnjem okruženju nezamisliv, kako djeci tako i roditeljima, potrebno je malo podignuti svijest o sigurnosti korištenja interneta i društvenih mreža. Kako bi se smanjila izloženost djeteta tolikim rizicima, za početak potrebno je malo odgoditi njegovo korištenje. Pod odgađanje bi se ubrajalo odgajanje i čuvanje djece najmlađe dobi, ali bez korištenja tableta i pametnih telefona. Ako je dijete kao malo naučeno da svakodnevno koristi tablete, pametne telefone i računala, za gledanje crtanih filmova i igranje igrica, teško će se kasnije odviknuti od toga. Kako bi se smanjila izloženost djece tolikim rizicima, vrlo je važna uloga roditelja. Djeca predškolske dobi i nižih razreda osnovne škole, koliko god to bilo teško prihvatiti, trebala bi imati dnevno ograničenje za korištenje tehnologije i interneta. Iako internet i tehnologija jednim dijelom pomažu prilikom učenja i razvijanje djeteta, s druge strane imaju suprotan efekt. Dok je dijete u razvoju, zasigurno do petog razreda, a i na više, kako bi kasnije bolje i lakše funkcioniralo, potrebno mu je razmišljanje i samostalni rad. Uloga roditelja je vrlo važna kao i povjerenje između djece i roditelja. Roditelji bi trebali nadgledati djecu prilikom korištenja interneta, ne toliko kako bi ih kontrolirali, već kako bi bili sigurni da su ona na neki način zaštićena. Osim samog ograničenja vremena i upotrebe pametnih telefona, tableta i računala potrebno je educirati djecu i roditelje. Edukacije o internetu, zaštiti podataka i samoj sigurnosti uvelike su potrebne obzirom na brzinu napredovanja tehnologije. Uvijek postoji mogućnost da će se dio vršnjaka okrenuti protiv nekog, da će to dijete doživijeti cyberbullying, da će mu možda netko hakirati računalo ili profil na društvenoj mreži, iako to nažalost nije moguće u potpunosti ukloniti, zajedničkim radom, edukacijama i radionicama moguće je smanjiti rizike i opasnosti kojima su djeca svakodnevno izložena te im tako osigurati sretnije i zaštićenije djetinstvo.

6. LITERATURA

Knjige i radovi:

- Bukovac, T., (2016): Sigurnost informacijskih sustava; Sveučilište u Zagrebu, http://darhiv.ffzg.unizg.hr/id/eprint/9366/1/Tomislav%20Bukovac_diplomski.pdf
- Vukelić, B., (2016): Sigurnost informacijskih sustava; Veleučilište u Rijeci, https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf

Internet:

- http://hr.n1info.com/Tehnologija/a345130/Zasto-mobitel-ne-smijete-dati-malo j-djeci.html
- http://hrkids.online/post/second-press/
- http://os-senkovec.skole.hr/upload/os senkovec/newsattach/482/Sigurnost_djece_na_internetu-savjeti_za_roditelje.PDF
- http://www.djecamedija.org/wp-content/uploads/2018/05/sigurnost-djece-na-internetu-2018-v2.pdf
- https://100posto.hr/news/vrsnjacko-nasilje-u-hrvatskoj-postaje-sve-brutalnije-roditelji-preuzmite-stvar-u-svoje-ruke-evo-najbrutalnijih-ispada
- https://djecamedija.org/rk/sigurnost/sigurnost-djece-na-internetu-uz-pomoc-microsoft-alata/
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_hr
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr
- https://gdprinformer.com/hr/vodic-kroz-gdpr
- https://sindikat-preporod.hr/opca-uredba-o-zastiti-podataka-u-skoli/
- https://www.dnevno.hr/vijesti/hrvatska/facebook-odnosi-prve-zrtve-sve-cesci-slucajevi-ubojstva-i-samoubojstva-djece-66176/

- https://www.hrvatskitelekom.hr/dodatne-usluge/roditeljska-zastita/brosura
- https://www.jutarnji.hr/vijesti/hrvatska/gdpr-donosi-i-niz-promjena-u-skole-roditelji-nece-moci-vidjeti-ocjene-i-izostanke-u-imeniku-svoje-djece-koja-su-navrsila-16-godina-bez-njihove-privole/7399272/
- https://www.medijskapismenost.hr/aplikacija-iz-koje-djeca-i-mladi-mogu-uciti-o-zastiti-osobnih-podataka/
- https://www.poliklinika-djeca.hr/publikacije/nasilje-preko-interneta/
- https://www.poliklinika-djeca.hr/publikacije/nasilje-preko-interneta/
- https://www.poliklinika-djeca.hr/za-roditelje/izazoviroditeljstva/o-djeci-i-internetu/
- https://www.schooleducationgateway.eu/hr/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm
- https://www.slideshare.net/novimediji/nasilje-na-internetu
- https://www.slobodnadalmacija.hr/novosti/crna-kronika/clanak/id/202851/zasto-je-umrla-15-godisnja-mj-ubila-se-zbog-vrijeanja-na-internetu-ili-je-rijec-o-ubojstvu
- https://www.tportal.hr/vijesti/clanak/cak-25-posto-djece-i-adolescenata-u-rh-zrtve-cyberbullyinga-20151214
- https://www.vecernji.hr/lifestyle/policija-nam-je-otkrila-broj-zrtava-cyberbullyinga-lani-evidentirali-362-slucaja-1318419
- os-dcesaric-os.skole.hr/upload/os-dcesaric-os/.../ELEKTRONICKO%20NASILJE.pps

POPIS SLIKA

POPIS TABLICA