Sigurnost djece na internetu - zaštita osobnih podataka

Vukoje, Gordana

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike u Puli

GORDANA VUKOJE

SIGURNOST DJECE NA INTERNETU – ZAŠTITA OSOBNIH PODATAKA

Diplomski rad

Pula, rujan 2022.

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike u Puli

GORDANA VUKOJE

SIGURNOST DJECE NA INTERNETU – ZAŠTITA OSOBNIH PODATAKA

Diplomski rad

JMBAG: 0267018312, izvanredan student

Studijski smjer: Nastavni smjer informatike

Predmet: IT i edukacija

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: doc. dr. sc. Snježana Babić

Pula, rujan 2022.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisana Gordana Vukoje, kandidat za magistra nastave informatike – mag.educ.inf ovime izjavljujem da je ovaj Diplomski 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 Diplomskog rada nije napisan na nedozvoljeni 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

_____

U Puli _____

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, Gordana Vukoje dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom

Sigurnost djece na internetu – zaštita osobnih podataka

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____

Potpis

_____

ZAHVALE

Zahvaljujem se svojoj mentorici doc.dr.sc. Snježani Babić na ukazanom povjerenju, savjetima, razumijevanju i stručnom vodstvu pri izradi i pisanju ovoga diplomskog rada.

Prijateljicama Marini, Katarini, Tanji, Josipi i Marijeli zahvaljujem na podršci i motivaciji tijekom moga školovanja.

Zahvaljujem se svojoj majci Jelici i sestri Marini koje su mi bile snažan oslonac.

Suprugu Goranu, kćerki Martini i sinu Andreju na ljubavi, razumijevanju, podršci te strpljivosti tijekom moga školovanja.

SAŽETAK

Zaštita osobnih podataka danas je postala osobito važna. Računalni sustavi česte su mete napadačima koji primjenom zlonamjernih sadržaja nastoje zloupotrijebiti korisničke osobne podatke. Kibernetička sigurnost kao takva osigurava korisniku pouzdanosti i zaštitu pri upotrebi usluga i proizvoda virtualnog svijeta.

Često se u medijima govori o vršnjačkom nasilju koje je s pojavom interneta poprimilo nove dimenzije i karakteristike. No, ovoj se temi najčešće pristupa s pedagoško-psihološkog aspekta.

Kroz ovaj se rad ispituje na koji način i u kojoj mjeri učenici osnovnoškolske dobi upotrebljavaju i primjenjuju oblike softverske i hardverske zaštite prilikom korištenja interneta. Analizom rezultata provedenog istraživanja u ovome diplomskom radu može se zaključiti da je opća informatička pismenost učenika osnovnoškolske dobi na nižoj razini, osobito razina hardverske i softverske zaštite koju koriste na svojim računalima, stoga je od iznimne važnosti raditi na podizanju svijesti o kibernetičkoj sigurnosti učenika.

Ključne riječi: računala zaštita, softver, hardver, korisnik, cyber sigurnost, sigurnost djece na internetu

SUMMARY

The protection of personal data has become particularly important today. Computer systems are frequent targets for attackers who, by applying malicious content, try to abuse user personal data. Cyber security as such provides the user with reliability and protection when using services and products of the virtual world.

The media often talk about peer violence, which took on new dimensions and characteristics with the advent of the Internet. However, this topic is most often approached from a pedagogical-psychological point of view.

This paper examines how and to what extent elementary school students use and apply forms of software and hardware protection when using the Internet. By analyzing the results of the research conducted in this thesis, it can be concluded that the general IT literacy of elementary school students is at a lower level, especially the level of hardware and software protection they use on their computers, therefore it is extremely important to work on raising awareness of students' cyber security.

Keywords: computer protection, software, hardware, user, cyber security, children's safety on the Internet

Sadržaj:

SAŽETAK *6*

SUMMARY *7*

1. UVOD *10*

2. OSOBNI PODATCI I PRIVATNOST *11*

2.1. Opći pojam osobnih podataka **11**

2.2. Prikupljanje i obrada podataka **12**

2.3. Važnost tajnosti i zaštite osobnih podataka **13**

2.3.1. Važnost tajnosti i zaštite osobnih podataka u realnom svijetu 14

2.3.2. Važnost tajnosti i zaštite osobnih podataka u virtualnom svijetu 15

2.4. Privatnost kao međunarodno i europsko ljudsko pravo **17**

2.5. Zaštita osobnih podataka u Republici Hrvatskoj **18**

3. INTERNET, SIGURNOST, KRIMINALITET I OSOBNI PODATCI *22*

3.1. Pojmovno određenje i razvoj interneta **22**

3.2. Usluge na internetu **24**

3.2.1. Društveni mediji 24

3.3. Računalna sigurnost **26**

3.4. Kibernetička sigurnost **27**

3.1.1. Nacionalna strategija kibernetičke sigurnosti 27

3.5. Cyber kriminalitet **28**

3.5.1. Vrste, ciljevi i razlozi napada 29

3.6. Zlonamjerni sadržaji i prijetnje **33**

3.7. Sigurno komuniciranje na internetu **34**

4. DIGITALNA PISMENOST I SIGURNOST DJECE NA INTERNETU *37*

4.1. Digitalna pismenost **37**

5. HARDVERSKA I SOFTVERSKA ZAŠTITA OSOBNIH PODATAKA DJECE NA INTERNETU *40*

5.1. Hardverska zaštita osobnih podataka djece na internetu **40**

5.2. Softverska zaštita osobnih podataka djece na internetu **41**

5.3. Alati za zaštitu osobnih podataka djece na internetu **43**

6. PREVENCIJA KRAĐE OSOBNIH PODATAKA DJECE NA INTERNETU U OSNOVNIM ŠKOLAMA *44*

6.1. Uloga roditelja **44**

6.2. Uloga škole **44**

6.3. Uloga medija **46**

6.4. Zakonska regulativa **47**

7. ANALIZA PRETHODNIH ISTRAŽIVANJA *50*

8. PRIMJENA HARDVERSKE I SOFTVERSKE ZAŠTITE OSOBNIH PODATAKA PRI KORIŠTENJU INTERNETA NA PRIMJERU UČENIKA OSNOVNOŠKOLSKOG UZRASTA *53*

8.1. Metodologija istraživanja **53**

8.1.1. Cilj i metode istraživanja 53

8.1.2. Anketni upitnik i postupak prikupljanje podataka 53

8.1.3. Sudionici istraživanja 54

8.2. Rezultati istraživanja **56**

8.2.1. Rezultati ispitanika o načinu korištenja digitalnih uređaja i interneta 56

8.2.2. Rezultati ispitanika o poznavanju zaštite osobnih podataka i sigurnom digitalnom okruženju 59

8.2.3. Rezultati ispitanika o hardverskoj zaštiti digitalnih uređaja 60

8.2.4. Rezultati ispitanika o softverskoj zaštiti osobnih podataka pri korištenju interneta 60

8.2.5. Rezultati ispitanika o sigurnosti operacijskih sustava digitalnih uređaja 62

8.2.6. Rezultati ispitanika o zaštiti korisničkih računa na internatskim stranicama i aplikacijama 63

9. ZAKLJUČAK *67*

LITERATURA *69*

POPIS SLIKA *79*

POPIS TABLICA *79*

POPIS GRAFIKONA *80*

PRILOG 1. ..... *82*

PRILOG 2. ..... *85*

1. UVOD

Korištenje interneta i društvenih mreža donosi niz pozitivnih stvari kao što su učenje, stjecanje novih znanja i vještina, s druge strane pak predstavlja rizik i opasnosti od neželjenih sadržaja, komunikacije s nepoznatim ljudima, gubitka identiteta. Kroz ovaj se diplomski rad želi ispitati na koje načine i u kojoj mjeri učenici promjenjuju i poznaju oblike hardverske i softverske zaštite digitalnih uređaja pri korištenju interneta. Rad obuhvaća dva dijela, teorijski i empirijski dio. U prvom poglavlju definirani su osobni podatci, načini obrade i prikupljanja podataka te načini na koji se isti mogu otuđiti i zloupotrijebiti. Prvo se poglavlje temelji na zakonskim odredbama zaštite osobnih podataka donesenih na međunarodnoj i nacionalnoj razini u kojima se ističe pravo na poštivanje privatnog života te članke u kojima se posebno naglašava da se osobni podatci mogu i smiju obrađivati uz suglasnost osobe o kojoj je riječ.

Nadalje, u radu je prikazan razvoj interneta, opisani pojmovi računalna i kibernetička sigurnost te na što se odnose. Navedeni su i objašnjeni zlonamjerni sadržaji i prijetnje koji narušavaju kibernetičku sigurnost kao sustava mjera zaštite podataka i mrežnih sustava. Nadalje, prikazan je i strateški dokument Nacionalna strategija kibernetičke sigurnosti Vlade Republike Hrvatske kojom se želi zaštiti korisnike elektroničkih usluga. U radu se dalje definira i opisuje digitalna pismenost te važnost digitalne pismenosti kojemu pripada i svijest o važnosti kibernetičke sigurnosti.

U petom se poglavlju rada opisuju mjere i načini hardverske i softverske zaštite osobnih podataka pri korištenju interneta. Nadalje, opisuje se uloga roditelja, škole te medija u prevenciji krađe osobnih podataka djece na internetu te ističe nužnost edukacije svih sudionika odgojno-obrazovnog procesa.

Sedmo poglavlje rada donosi prikaz analize prethodnih istraživanja softverske i hardverske zaštite računala. Istraživanja su pokazala da se kroz dosadašnja istraživanja o zaštiti osobnih podataka naglasak stavlja na socio-društveni aspekt, opsuju se opasnosti koje donose društvene mreže, kako se učenici osjećaju, kome se mogu obratiti za pomoć u slučaju zloupotrebe osobnih podataka, a vrlo malo istraživanja koja govore o zaštiti i načinima kako spriječiti zlonamjerne sadržaje i prijetnje digitalnih uređaja.

U osmome poglavlju prikazani su rezultati ankete provedene u svrhu izrade diplomskog rada.

2. OSOBNI PODATCI I PRIVATNOST

Za naznačavanje važnosti tajnosti i zaštite osobnih podataka, bitno je razlikovati pojmove podatak i informacija. Podatak je definiran kao svaka poznata ili pretpostavljena činjenica na osnovi koje se oblikuje informacija. On sam po sebi nema značenje nego čini osnovu za stvaranje informacije. Stoga se može zaključiti da je informacija skup podataka s pripisanim značenjem. Danas informacija ima više značenja. Od mnoštva značenja koja posjeduje, u jednom svom dijelu obrađen je onaj aspekt informacije koji ju povezuje s konceptom poruke kao nositelja informacije. Informacija je u tom slučaju rezultat obrade, analize i organiziranja podataka na način koji dodaje znanje primatelju. Tajnost osobnih podataka je vrlo važna kako ne bi došlo do njihove zloupotrebe budući da pristupanje podatcima uz određeno znanje omogućuje identifikaciju pojedinaca. Znanje čovjeku omogućuje razumijevanje informacija, pa tako i prepoznavanje podataka kojim su ti podatci vezani u informaciju.[1]

2.1. Opći pojam osobnih podataka

Osobni su podatci informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Informacije koje zajedno prikupljene mogu rezultirati utvrđivanjem identiteta određene osobe, također čine osobne podatke.

Osobni podatci koji su deindentificirani, šifrirani ili pseudonimizirani, ali se mogu upotrijebiti za ponovno utvrđivanje identiteta osobe ostaju osobni podatci te su obuhvaćeni područjem primjene Opće uredbe o zaštite podataka o kojoj će biti riječ u nastavku radu.

Primjeri osobnih podataka uključuju:

- ime i prezime;
- kućnu adresu;
- adresu elektroničke pošte: ime.prezime@primjer.hr
- broj osobne iskaznice;
- adresa internetskog protokola (IP)
- fotografije i videozapisi;

[1] Družin, I. (2018): *Zaštita osobnih podataka u informacijskom društvu* [završni rad]. Zagreb: Sveučilište u Zagrebu, URL: http://darhiv.ffzg.unizg.hr/id/eprint/10579/1/Druzin_zavrsni.pdf?fbclid=IwAR0mBsOjaAUI24C7XRc4Jfwnxj0CFTJXnKFQ_A3E5UwOJaPPWHyEZ7w9yII, (10.6.2022.)

- podatci koje imaju bolnica ili liječnik, a koji mogu biti simbol kojim se utvrđuje jedinstveni identitet osobe.[2]

Pod definicijom osobnih podataka ne smatraju se registracijski broj društva, e-mail adrese u formi info@društvo.hr te anonimizirani podatci. Važnosti pravilnog postupanja s osobnim podatcima doprinose i načela obrade osobnih podataka:

- načelo zakonitosti, poštenosti i transparentnosti
- načelo ograničavanja svrhe
- načelo smanjenja količine podataka (ograničenost podataka s obzirom na svrhu)
- načelo točnosti
- načelo ograničavanja pohrane (samo onoliko koliko je potrebno u svrhe za koje se koristi)
- načelo cjelovitosti i povjerljivosti
- načelo pouzdanosti
- načelo zakonitosti obrade[3]

Navedena načela i definicija upozoravaju na više načina i mogućnosti za prikupljanje osobnih podataka. Zasigurno najzastupljeniji način prikupljanja, obrade i korištenja, u današnjem vremenu, je onaj putem informacijskih tehnologija, a posebice interneta. Internet je globalni informacijsko-komunikacijski sustav koji povezuje računalne mreže pojedinih zemalja i organizacija, te omogućava korisnicima da diljem svijeta putem svojih računala, mobitela ili drugih uređaja na kojim se koriste internetom međusobno komuniciraju, razmjenjuju informacije i koriste brojne druge usluge.[4]

2.2. Prikupljanje i obrada podataka

Razni se podatci kupuju i obrađuju kako bi se unaprijedile određene usluge, a danas je obrada podataka nezamisliva bez upotrebljavanja informacijsko-komunikacijskih tehnologija. Obrada podataka je manipuliranje podatcima kako bi se iskoristili za određenu namjenu. Obrada može biti ručna ili automatska, a prodor

[2]Europska komisija, *Što su osobni podaci?,* URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr (30.8.2022.)
[3] Kladar, D. (2018.) Kako se pripremiti za GDPR, Zagreb: Forum poslovni mediji, str.22.
[4] Varga, M., Šimović, V. i Milković, M. (2012.): Zaštita elektroničkih informacija. Varaždin, str.10.

računala dovodi do veće mogućnosti obrade podataka tako što čini informacijske sustave za obradu bržim, točnijim i efikasnijim. Glavne operacije obrade podataka su zapisivanje, kopiranje, provjera, klasificiranje, sortiranje, spajanje, izračunavanje, pretraživanje, sažimanje i prikaz rezultata. Ciklus obrade podataka sastoji se od tri koraka, a to su ulaz, obrada i izlaz. U ulazu je priprema ulaznih podataka za obradu gdje oblik od tih podataka ovisi o stroju kojim se obrada vrši. Ulazni podatci se procesom obrade mijenjaju ili pak kombiniraju s drugim informacijama kako bi se dobili podatci u prikladnom obliku. Na izlazu je skupljen rezultat obrade tih podataka.

Prikupljanje sve veće količine podataka su omogućili razvoj novih tehnologija i automatiziran način obrade podataka, čime su podatci postali dostupniji nego ikada. Korisnici su sve više zabrinutiji za svoju privatnost i nisu uvijek informirani o načinu na koji se njihovi osobni podatci obrađuju. Identifikacija osobnim podatcima je danas neizbježna za dobivanje određene usluge ili obavljanje određenog posla. Pojedinac se s pravom može bojati da mu neovlašteni uvid u njegove osobne podatke može onemogućiti dobivanje određene usluge.

Obrada podataka omogućava brojne koristi koje nisu bile moguće u prijašnje vrijeme, primjerice navigacijske upute u stvarnom vremenu, obrada zdravstvenih podataka kako bi se otkrio uzrok bolesti. No, u prenesenom značenju se podatci mogu smatrati ispušnim plinom informacijskog doba uspoređujući ih sa ekološkim zagađenjem. Naime, ako su podatci „ispušni plin“, oni su nešto što svi proizvode dok se bave poslovima informacijskog doba, pa su podatci tako zagađenje informacijskog doba, a ekološki izazov bi bio zaštita privatnosti.[5]

2.3. Važnost tajnosti i zaštite osobnih podataka

Uloga tajnosti i zaštite osobnih podataka postala je veća nego ikada prije u današnjem razvijenom informacijskom društvu. Informacijsko društvo može se definirati kao društvo koje svoj kulturni, gospodarski i znanstveni razvoj zasniva na uvođenju i širenju računalne i telekomunikacijske tehnologije, a također se može zasnivati i na stvaranju, obradi i prijenosu informacija kao temelju za rast produktivnosti društva. Taj se pojam počeo upotrebljavati 90-ih godina u dokumentima Europske unije. Podatci i informacije se vrednuju kao važan segment za napredak, no postavlja

[5] Schneier, B. (2015): *Data and Goliath*, W. W. Norton & Company, New York, London

se pitanje kako poštovati pravo na privatnost pojedinaca, a istovremeno osigurati slobodan protok podataka potrebnih za napredak društva.[6]

Pitanje informacijskog doba koje se postavlja je kako osmisliti sustave koji će se koristiti osobnim podatcima za dobrobit društva, a kako istovremeno zaštititi svakog pojedinca. Tajnost i zaštita osobnih podataka su važni zbog očuvanja vlastite privatnosti koja je neophodna za ljudsko dostojanstvo, kao i za slobodu i neovisnost. Vlastitu privatnost treba nastojati čuvati i štititi kako bi svi bili uistinu sigurni.[7]

2.3.1. Važnost tajnosti i zaštite osobnih podataka u realnom svijetu

Koliko je zaštita osobnih podataka važna najbolje se može prikazati primjerom krađe identiteta gdje neka osoba može oštećenoj osobi nanijeti materijalnu ili neku drugu štetu. U današnje vrijeme se u medijima puno govori upravo o zlouporabi tuđih podataka, a kao česti primjer navodi se produljivanje ugovora kod telekom operatera gdje se nanosi materijalna šteta oštećenoj osobi. Kod situacije da netko pronađe osobnu iskaznicu osobe koja je korisnik usluga nekog operatera, osoba s tuđom osobnom iskaznicom dolazi do osobnih podataka korisnika. Putem broja osobne iskaznice može se doći do OIB-a te osobe. Osoba se može lažno predstaviti putem osobnih podataka oštećenog korisnika putem telefonske narudžbe, te može kupiti mobilni uređaj ili produljiti ugovor bez da to pravi vlasnik sazna.

Većina agenata u pozivnom centru pri razgovoru sa korisnikom vrši identifikaciju putem OIB-a ili putem broja osobne iskaznice. Agent pozivnog centra dobiva sve točne informacije i osobne podatke, no ni na koji način ne može znati da se ne radi o osobi o kojoj je riječ. Kako bi se spriječile takve prevare svaki iskusniji agent već po zahtjevima osobe koja zove može pretpostaviti i procijeniti radi li se uistinu o prevari. Jedan od najočitijih primjera takve krađe identiteta je kada osoba zove telefonom i naruči nekoliko novih brojeva na najjačim tarifama, a uz to naruči i nove mobilne uređaje koji su naravno visoke vrijednosti. Osoba koja ima lošu namjeru prilikom prikupljanja nečijih podataka najčešće te podatke koristi u svrhu obrade podataka, za zlouporabu i lažno predstavljanje.[8]

---

[6] Tuđman, M., Boras, D., Dovedan, Z. (1993): *Uvod u informacijske znanosti*. Zagreb: Školska knjiga, URL: http://dzs.ffzg.unizg.hr/text/Uvod%20u%20informacijske%20znanosti/, (10.6.2022.)
[7] Schneier, B. (2015): *Data and Goliath*, W. W. Norton & Company, New York, London
[8] Matusina, M. (2017): *Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka* [diplomski rad]. Zagreb: Sveučilište u Zagrebu

Dakle, važan pojam ove teme je krađa identiteta. To je svaka radnja u kojoj pojedinac ili skupina ljudi prikuplja osobne podatke druge osobe protivno zakonu. Zlouporaba tuđih osobnih podataka se događa u svrhu nanošenja štete osobi čiji su podatci. Šteta može biti materijalna i poticati financijske gubitke kod oštećene osobe ili povredu ugleda, časti i privatnosti što je kazneno djelo za koje je predviđena kazna zatvora.[9]

Osoba s ciljem izvršavanja prevare na vrlo jednostavan način dolazi do osobnih podataka. Najučinkovitija tehnika za prikupljanje osobnih podataka je socijalni inženjering, a temelji se na ljudskim greškama. Navedenom tehnikom osoba bez direktnog pokušaja upadanja u informacijski sustav neke tvrtke može doći do osobnih podataka manipulacijom ljudstva. Koristeći ljudske osobine poput povjerenja, straha od nepoznatog, znatiželje i nemarnosti moguće je prikupiti informacije. U realnom svijetu cilj socijalnog inženjeringa bi bio izvođenje prevara pomoću isprava oštećene osobe kako bi se nanijela novčana šteta toj osobi. Također osobe kao što su nezadovoljni radnici, špijuni ili bivši radnici mogu davati podatke u krive ruke s ciljem industrijske špijunaže kako bi došlo do ostvarenja konkurentnosti na tržištu. Socijalni inženjering sadrži brojne i raznovrsne načine za pribavljanje lozinki za neovlašteni pristup sustavu: Shoulder Surfing, metoda lažnog predstavljanja, kopanje po smeću, pretraživanje bačenih papira, pregledavanje tuđih bilješki i dr.[10]

2.3.2. Važnost tajnosti i zaštite osobnih podataka u virtualnom svijetu

Virtualni svijet odnosno internet se može gledati kao najveća svjetska enciklopedija. On se koristi kako za komunikaciju, tako i za učenje, kupovinu, zabavu. Na internetu se osobni podatci ostavljaju na raznim forumima, društvenim mrežama, online igrama, web oglasima i web trgovinama. Današnje tehnologije su toliko napredne da je nemoguće ostati anoniman, pa tako svaki poziv, svaka SMS poruka ili bilo kakva komunikacija putem različitih aplikacija ostaju zapisani u virtualnom svijetu. Sve što je objavljeno na internetu se ne može trajno obrisati, stoga je prijeko potrebno paziti što se i gdje objavljuje. Opasnost se ne uzrokuje samo objavljivanjem osobnih

[9] Agencija za zaštitu osobnih podataka: *Što je krađa identiteta?,* URL: https://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi, (10.6.2022.)
[10] CARNet (2010): *Napredne tehnike socijalnog inženjeringa NCERT-PUBDOC-2010-02-292*, URL: https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-02-292.pdf, (10.6.2022.)

podataka, već se ona pojavljuje i objavljivanjem fotografija iz svakodnevnog života gdje se pokazuju životne navike pojedinaca.

Postoji veliki broj primjera gdje su se krađe dogodile upravo zbog objavljivanja privatnih stvari na društvenim mrežama pod opcijom da se to može javno vidjeti.

Najčešće korištena zlonamjerna tehnika napada u virtualnom svijetu je XSS tehnika. Ona se još uvijek najviše koristi unatoč velikom i neprekidnom istraživanju i eksperimentiranju s mnoštvom novih zlonamjernih tehnika. Kada web aplikacije uzimaju podatke od korisnika i dinamički ih uključuju u web stranice bez detaljne provjere tada nastaje XSS ranjivost. To napadaču omogućuje da u web pregledniku napadnutog korisnika prikazuje svojevoljne komande i uz to prikazuje proizvoljni sadržaj u pregledniku. Napadač tako dobiva pristup određenim stranicama na način da zaobiđe sigurnosnu prijavu i lozinku napadnutog korisnika. XSS napadom se mogu otuđiti korisnički računi. Kako bi napadač korištenjem web preglednika ispitao odgovor dinamičke stranice, on distribuira vlastiti XSS URL zahtjev. Osim toga napadač mora poznavati i HTML i JavaScript jezik da bi proizveo URL koji nije previše sumnjivog izgleda, te bi tako napao stranicu koja je osjetljiva na XSS napade. Primjerice Facebook stranica povremeno šalje korisniku na e-mail link za verifikaciju e-mail adrese. Napadač putem elektroničke pošte može poslati poveznicu napadnutom korisniku kako bi taj korisnik potvrdio lozinku, a otvaranjem poveznice se otvara internet stranica koja je vrlo slična izgledom početnoj stranici Facebook-a. U tom trenutku napadnuti korisnik ne može ni pretpostaviti da se radi o napadu, te upisuje svoje ime i lozinku. Tim korakom napadač dobiva podatke kojima može ukrasti račun od Facebook profila.

Napadači se također koriste i ostalim raznim tehnikama kako bi dobili pristup računalnom sustavu. Počinitelji uglavnom prvotno nastoje pribaviti podatke o računalnom sustavu i načinu na koji se on koristi. Metoda koja se često upotrebljava je eng. *Spoofing* koji sadrži više metoda pomoću kojih napadači dolaze do željenih podataka, a sve se temelji na nedovoljnoj pažnji korisnika, npr. Login Spoofin, Web Spoofing, E-mail Spoofing, DNS Spoofing, IP Spoofing, Metode Prisluškivanje, Optičko špijuniranje, Druženje, Pretraživanje, Probe i dr.[11]

Društvene mreže danas sve više zadiru u privatnost pojedinaca budući da je sve veći broj korisnika društvenih mreža, pa je tako veća i količina podijeljenih informacija.

[11] Ibid.

Društvena mreža Facebook pruža puno mogućnosti zaštite osobnih podataka, tako da bi se korisnici trebali pozabaviti s time i dobro proučiti što sve i na koji način mogu zaštiti, iako postoji dosta ljudi koji imaju otvorene profile bez da skrivaju osobne podatke. Budući da takve postavke o privatnosti zahtijevaju više pozornosti i vremena neki ljudi nisu spremni izdvojiti toliko vremena ili nemaju volje proučavati koje su im mogućnosti.

Internet stranice znaju mnogo podataka o svojim posjetiteljima, više nego što oni sami to misle. Svaka stranica ili portal ima prostor za oglašavanje. Oglasi se prikazuju na temelju različitih čimbenika: aktivnosti korisnika na drugom uređaju, kolačići na pregledniku i postavke na Google računu korisnika, vrste web stranica koje korisnik posjećuje i slično. Ukoliko osoba ne daje podatke na internet i nigdje se ne registrira, ona svejedno nema garantiranu privatnost. To dokazuje primjer kada osoba pretražuje nešto, primjerice određeno mjesto za ljetovanje, tada Google pretraživač skuplja podatke o osobi i putem njih dobiva informaciju da tu osobu zanima određeno mjesto i na temelju prikupljenih informacija narednih nekoliko dana će se osobi oglašavati to mjesto i na Facebook-u i na svim ostalim stranicama i portalima, što daje dojam kao da ga netko prisluškuje i nadgleda.

Zaštita na internetu se može postići ukoliko se pazi što se objavljuje i kakve se slike i informacije dijele s prijateljima s društvenih mreža. Uvijek je dobro promisliti prije dijeljenja bitnih podataka koje mogu donijeti posljedice ukoliko do njih dođu krive osobe. Ukoliko dođe do propusta u samom software-u oni se brzo isprave, no potencijal za štetu koji propust može uzrokovati je ogroman.[12]

2.4. Privatnost kao međunarodno i europsko ljudsko pravo

Privatnost je kao ljudsko pravo utvrđeno nizom međunarodnih dokumenata, ponajprije u čl. 12. Opće deklaracije o ljudskim pravima te u čl.17. Međunarodnog pakta o građanskim i političkim pravima. U europskom kontekstu nalazi se u čl. 8.1. Konvencije za zaštitu ljudskih prava i temeljnih sloboda kao „Pravo na poštovanje privatnog i obiteljskog života“ i č. 7. Povelje o temeljnim pravima EU-a, tako da „Svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja.“ Povelja o temeljnim pravima daje i poseban članak koji se odnosi specifično na zaštitu

[12] SciTechBlog (2010): *Facebook fixes security bug in chat program*, URL: https://scitech.blogs.cnn.com/2010/05/05/blog-finds-possible-security-flaw-in-facebook-chat/ (10.6.2022.)

osobnih podataka, koji definira i položaj osobe o kojoj se podaci prikupljaju i glasi: “Svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose. Takvi podaci moraju se obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje. Poštovanje tih pravila podliježe nadzoru neovisnog tijela.“[13] Standardi zaštite privatnosti i osobnih podataka dodatno su razrađeni i putem nacionalnih zakonodavstava.

Zaštita privatnosti i osobnih podataka je globalni izazov u digitalnom okruženju čemu je doprinio razvoj interneta i tehnologija. Zbog toga je 2013. godine Opća skupština UN-a usvojila „Rezoluciju 68/167, u kojoj je izrazila duboku zabrinutost zbog negativnog utjecaja koji nadzor i presretanje komunikacija mogu imati na ljudska prava. Opća skupština pozvala je sve države da preispitaju svoje postupke, praksu i zakonodavstvo vezano za nadzor komunikacija, presretanje i prikupljanje osobnih podataka te je naglasila potrebu da države osiguraju potpunu i učinkovitu provedbu svojih obveza iz međunarodnog prava ljudskih prava.“[14] Od 2015. godine u sklopu UN-a djeluje i Specijalni izvjestitelj za pravo na privatnost u čijemu je mandatu, između ostalog, i prikupljanje podataka s ciljem izvještavanja o pravu na privatnost te sastavljanje preporuka za zaštitu i promociju prava na privatnost, kao i prijavljivanje i praćenje povreda prava na privatnost te praćenje globalnih trendova vezanih uz pravo na privatnost i nove tehnologije. Na razini EU-a je donesena Opća uredba o zaštiti podataka Europske unije, protokol Vijeća Europe za ažuriranje i modernizaciju Konvencije o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka, Rezolucija (1986.) o poboljšanju zaštite korisnika i sigurnosti u cyber prostoru i dr.

2.5. Zaštita osobnih podataka u Republici Hrvatskoj

U Republici Hrvatskoj je pravo na privatnost zajamčeno čl. 36. i 37. Ustava RH. Tako se u čl. 36. navodi da su zajamčena i nepovrediva sloboda i tajnost dopisivanja i svih drugih oblika općenja[15], a u čl.37. stoji da se svakom jamči sigurnost i tajnost osobnih podataka te da se bez privole ispitanika osobni podatci ne smiju prikupljati,

[13] Povelja Europske unije o temeljnim pravima (2016/C, 202/02), čl.8.
[14] Kucaljudskihprava.hr (2019): *Privatnost kao ljudsko pravo*, URL: https://www.kucaljudskihprava.hr/2019/12/18/privatnost-kao-ljudsko-pravo/, (10.6.2022.)
[15] Ustav RH (NN 56/90,…05/14), čl.36.

obrađivati te ih je moguće koristiti samo uz uvjete predviđene zakonom. Također je zabranjena uporaba osobnih podataka suprotna utvrđenoj svrsi njihova prikupljanja.[16] Pitanje uporabe osobnih podataka u Hrvatskoj je uređeno Zakonom o zaštiti osobnih podataka.[17]

U Republici Hrvatskoj je zaštita osobnih podataka osigurana svakoj fizičkoj osobi bez obzira na njezino državljanstvo i prebivalište, te također neovisno o spolu, vjeri, boji kože, jeziku, političkom ili drugom uvjerenju, rođenju, imovini ili ostalim osobinama. U Hrvatskoj je za zaštitu podataka zadužena Agencija za zaštitu osobnih podataka. Svatko tko smatra da mu je povrijeđeno neko pravo zajamčeno Zakonom o zaštiti osobnih podataka može podnijeti zahtjev za utvrđivanje povrede prava Agenciji za zaštitu osobnih podataka.

U Republici Hrvatskoj su prava u vezi zaštite osobnih podataka do 25.svibnja 2018. godine bila uređena Zakonom o zaštiti osobnih podataka. On je trenutno izvan snage, no od 25. svibnja 2018. godine u RH je važeća Opća uredba o zaštiti podataka[18]. Riječ je o Uredbi (EU) 2016/679 Europskog parlamenta i Vijeća od 27.travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ. Osim toga, u Hrvatskoj je na snazi Zakon o provedbi Opće uredbe o zaštiti podataka[19], također od istog datuma kada je na snagu stupila i Uredba.

Temeljno pravo svakog čovjeka kako u Hrvatskoj tako i u cijelome svijetu je poštivanje njegovog privatnog života i tajnost i zaštita osobnih podataka. Takvom se zaštitom jamči privatnost osobe u današnjem digitalnom dobu i jača se sigurnost te osobe. Osobnim podatkom se smatra svaka informacija koja se odnosi na identificiranu osobu ili osobu koja se može identificirati.[20]

Svaka se osoba identificira po nekom obilježju. Nekada su se u Hrvatskoj osobe u služenim ustanovama identificirale po jedinstvenom matičnom broju građana (JMBG), a ukoliko netko zna JMBG određene osobe, iz njega može očitati spol vlasnika, te datum i mjesto rođenja. Kasnije je uveden osobni identifikacijski broj (OIB) koji je novi identifikacijski broj, a dodaje se računalno bez odavanja osobnih podataka o korisniku poput spola, datuma, godine i mjesta rođenja.

---

[16] Ibid., čl.37.
[17] Kucaljudskihprava.hr (2019): *Privatnost kao ljudsko pravo*, URL: https://www.kucaljudskihprava.hr/2019/12/18/privatnost-kao-ljudsko-pravo/ (10.6.2022.)
[18] Opća uredba o zaštiti podataka (SL EU L119)
[19] Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)
[20] Europski parlament: *Zaštita osobnih podataka*, URL: https://www.europarl.europa.eu/factsheets/en/home, (10.6.2022.)

Osobe se također mogu identificirati po psihološkom, kulturnom, fizičkom, socijalnom, mentalnom ili gospodarskom identitetu. Osobni podatci mogu biti broj kartice bankovnog računa, adresa e-pošte, telefonski broj ili privatna fotografija. Osobni podatci također mogu biti i odabir političke stranke, zdravstveno stanje, podatci o kaznenom i prekršajnom postupku koji su drukčije klasificirani i zbog toga im je potrebno osigurati posebnu zaštitu.[21]

Kako bi se mogla vršiti bilo kakva identifikacija potrebno je prvo prikupiti podatke, a onda ih obraditi. Obradom se smatra svaka radnja na osobnim podatcima. Radnje koje su vezane s osobnim podatcima odnose se na prikupljanje, spremanje, snimanje, prilagodbu, organiziranje, uvid, svrstavanje, povlačene, brisanje, uništavanje, arhiviranje, te provedbu matematičkih operacija nad njima.[22]

Pod nazivom „Agencija za zaštitu osobnih podataka“ nalazi se pravna osoba koja ima javne ovlasti. Takva agencija ima potpunu samostalnost u svom djelovanju. Nije zavisna o zakonodavnoj i izvršnoj vlasti u Republici Hrvatskoj.[23] Glavna organizacija, odnosno agencija koja se bavi zaštitom osobnih podataka je upravo Agencija za zaštitu osobnih podataka (AZOP).

Agencija djeluje kao nadzorno tijelo. Glavni zadatci Agencije su učinkovito djelovanje na ispunjavanje svih prava i obaveza iz područja zaštite osobnih podataka koje se Hrvatskoj nameću kao punopravnoj članici Europske unije i Vijeća Europe. Jedan od bitnih zadataka je i povećanje odgovornosti svih sudionika u procesu obrade osobnih podataka koji su vezani uz primjenu propisa koji su obuhvaćeni zakonskim okvirom zaštite osobnih podataka u Hrvatskoj uz odgovarajuću primjenu mjera informacijske sigurnosti.[24] Agencija također ima i određene trajne zadaće koje se dotiču zaštite. Glavna takva zadaća je podizanje i promoviranje svijesti svih sudionika i cjelokupne javnosti o samoj zaštiti podataka i njezinoj važnosti, zatim o pravima i obvezama tih istih sudionika. Sukladno tome zadaće Agencije su i predlaganje mjera za stručno osposobljavanje i usavršavanje različitih tipova službenika u agenciji i izvan nje, kao i svih službenika za zaštitu osobnih podataka. Trajna zadaća joj je također i ukupna provedba svih upravnih i stručnih poslova koji proizlaze iz Zakona o zaštiti osobnih podataka. Također, Agencija za zaštitu osobnih podataka dužna je koristiti

[21] Matusina, M. (2017): *Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka* [diplomski rad]. Zagreb: Sveučilište u Zagrebu
[22] Dragičević, D. (2015): *Pravna informatika i pravo informacijskih tehnologija*. Zagreb: Narodne Novine
[23] Azop.hr: *Djelatnost agencije*, URL: https://azop.hr/djelatnost-agencije, (11.6.2022.)
[24] Azop.hr: *Djelatnosti i ustrojstvo agencije*, URL: http://azop.hr/djelatnost-agencije, (11.6.2022.)

odnose s javnošću kako bi obavještavala sve građane Republike Hrvatske o promjenama do kojih dolazi kod zaštite ili noviteta koji se pojavljuju kod osobnih podataka.

Godine 2018. su povodom obilježavanja Dana sigurnijeg interneta tri mobilna operatora, HAKOM, Centar za nestalu i zlostavljanu djecu te Centar za sigurniji Internet, uz podršku Ureda pravobraniteljice za djecu, potpisali prvu Povelju o sigurnosti djece na internetu u RH.[25]

[25] Hakom.hr (2018): *06. veljače obilježava se Dan sigurnijeg interneta. Potpisana prva „Povelja o sigurnosti djece na internetu*. URL: https://www.hakom.hr/UserDocsImages/2018/dokumenti/Press%20release%20Potpisivanje%20Povelje%20o%20sigurnosti%20djece%20na%20internetu.pdf, (11.6.2022.)

3. INTERNET, SIGURNOST, KRIMINALITET I OSOBNI PODATCI

3.1. Pojmovno određenje i razvoj interneta

Internet je postao najmoćniji medij današnjice koji je od svijeta napravio tzv. „globalno selo“, jer ono omogućava interakciju stotinama milijuna računala diljem svijeta. Internet i cyber društvo su mjesta ili pojave koja tek dobivaju na značaju ili se svakim trenutkom šire i dobivaju na težini.

Povijest interneta kao široko rasprostranjene mreže informacijske infrastrukture poprilično je složena i podrazumijeva tehnološke, organizacijske i društvene aspekte djelovanja.

Internet je naziv za globalnu računalnu mrežu koja vezuje računala i manje računalne mreže uz pomoć Internet protokola, što korisnicima interneta omogućuje komunikaciju i razmjenu podataka s ostalim korisnicima, bez obzira u kojem dijelu svijeta se nalaze.[26] Drugim riječima, internetom se naziva spoj različitih računalnih mreža u jedinstvenu svjetsku računalnu mrežu koja nudi velik broj informacijskih i komunikacijskih usluga. Ta globalna mreža omogućuje korisnicima da međusobno komuniciraju razmjenjujući e-poruke, pronalazeći informacije na webu ili prenoseći datoteke protokolom za prijenos datoteka FTP-a.

Danas internet mijenja navike ljudi, način komunikacije pa i društvo u cjelini. U zadnjih se desetak godina značajno promijenio način na koji ljudi rade, kupuju i provode slobodno vrijeme, način na koji se druže s drugim ljudima i to sve zahvaljujući internetu.[27]

Internet je nastao u posljednjem desetljeću prošloga stoljeća, a sve je započelo 60-ih godina 20. stoljeća. Može se reći da je nastao vrlo spontano, bez planova o razvitku „velike multimedijalne globalne mreže“.[28] U Tablici 1. prikazani su najvažniji događaji i pripadajuće godine za razvoj Interneta.

[26] Čerić, V. et al. (2004): *Informacijska tehnologija u poslovanju*. Zagreb: Element
[27] Leiner, B. M. et al. (2009): *Brief History of the Internet*. URL: https://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf, (25.4.2022.)
[28] Tesla.carner.hr - Nacionalni portal za učenje na daljinu: *Uvod u Internet*. URL: https://tesla.carnet.hr/mod/book/view.php?id=5428&chapterid=883, (25.4.2022.)

Tablica 1. Pregled najvažnijih godina/događaja za razvoj Interneta

1969.	Početak pravog razvoja Interneta
1971.	Poslan prvi e-mail
1979.	Pokrenuti MUDO-ovi[29]
1980.	Zaživio Usenet[30]
1.1.1983.	Nakon prvog mrežnog protokola Network Control Program, dolazi novi mrežni protokol TCP/IP → pravi početak razvoja Interneta → zaživio u većini računala ARPANET-a
1988.	IRC[31] omogućuje ljudima diljem svijeta komunikaciju u virtualnim sobama u realnom vremenu
1990.	ARPANET umirovljen i prenesen na NSFnet[32] koji je uskoro spojen sa CSnet[33], a zatim je spojen s EUnet-om[34] → nastanak WEB-a ili globalne Mreže

Izvor: Izrada autorice prema: Hajdarović, M. (2006): *Povijesni razvoj interneta*. URL: http://povijest.net/2018/?p=2374, (25.4.2022.)

Internet je dobio ime po Internet protokolu (*eng. Internet Protocol*) – standardnom komunikacijskom protokolu koji danas koriste sva umrežena računala. Taj je protokol zaživio u većini računala ARPANET-a 1. siječnja 1983. godine i taj se datum može smatrati pravim početkom interneta.[35]

Ubrzanom širenju interneta u svakodnevni život doprinijelo je uspostavljanje jedne od najatraktivnijih mrežnih usluga, *World Wide Web* (WWW) početkom 20-ih godina 20. stoljeća. WWW je donio mogućnost povezivanja tekstnih stranica jednostavnim klikom miša, povezivanjem slika i drugih materijala, a ubrzo i uključivanje materijala raznih vrsta na stranicu.[36] Uspostava WWW servisa dovela je do saznanja da Internet može biti iskorišten i kao tehnička infrastruktura za razmjenu podataka potrebnih u

[29] MUDO-vi = Multi-User Dungeos – virtualni svemir kojeg vrti program na serveru
[30] Usenet = kratica od „user's network" i češće se koristi naziv „newsgropus" – sastoji se od tisuća virtualnih korisničkih oglasnih ploča sa raznim temama dostupnim u cijelom svijetu.
[31] IRC=Internet Relay Chat
[32] NSFnet =National Science Foundation Network
[33] CSnet=Computer Science Network
[34] EUnet=European Network
[35] Hajdarović, M. (2006): *Povijesni razvoj interneta*. URL: http://povijest.net/2018/?p=2374, (25.4.2022.)
[36] Ibid.

poslovanju, ali i kao medij unutar kojega se može obavljati poslovanje. Već nakon nekoliko godina na internetu se počele predstavljati tvrtke, koje su osim prezentacije proizvoda počele nuditi i same proizvode te usluge.[37] Do kraja 1991. godine umreženo je preko 5000 centara u preko 35 država svijeta.[38]

U Republici Hrvatskoj je umrežavanje na široj osnovi počelo 90-ih godina prošloga stoljeća razvojem CARNeta[39] u području znanosti i tehnologije. Daljnjim razvojem, komunikacijske tehnologije i komercijalne tvrtke ponudile su korištenje interneta građanima i tvrtkama, pa je ono danas i u našim krajevima prošireno u gotovo svim društvenim i gospodarskim djelatnostima.[40]

3.2. Usluge na internetu

Najpoznatije usluge na internetu su: (1) već spomenuti *World Wide Web* koji koristi HTTP za prijenos web stranica napisanih u HTML-u – riječ je o najnovijem servisu, ali također i najbrže rastućem; (2) razgovor ili čavrljanje (chat) – može biti komunikacija glasom (oba računala moraju imati zvučne kartice, mikrofone i zvučnike/slušalice), te pismena komunikacija (npr. IRC, ICQ i u zadnje vrijeme sve popularniji Skype); (3) elektronička pošta – koristi POP, SMTP i ostale protokole – riječ je o jednoj od prvih usluga na internetu; (4) prijenos datoteka – uz standardni FTP danas se sve više koristi *peer to peer* protokoli; (5) Usenet – mreža namijenjena razmjeni poruka u interesnim grupama. Korisnici interneta mogu pristupati raznim informacijama, razgovarati s drugim ljudima, koristiti e-poštu ili pristupati forumima, kupovati putem interneta, igrati *online* igrice, koristiti stranice za Internet bankarstvo, učiti i dr.[41]

3.2.1. Društveni mediji

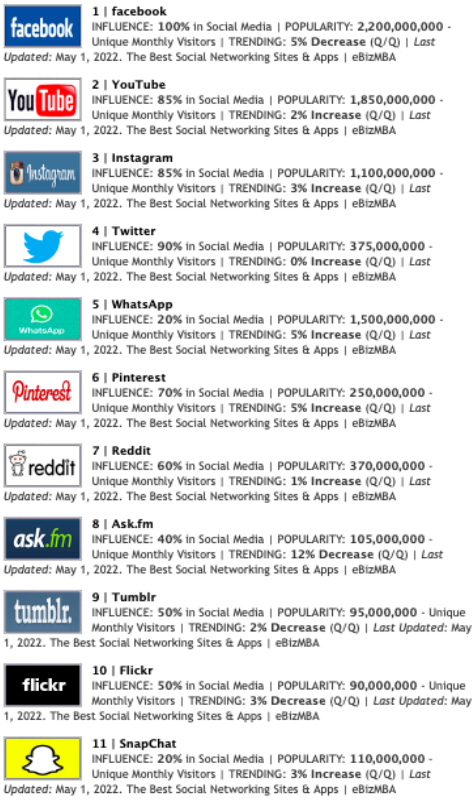
Društveni mediji su grupa internet aplikacija koje služe stvaranju i razmjenjivanju sadržaja kreiranih od strane korisnika, te kao takvi podržavaju ljudsku potrebu za interakcijom u društvu uz korištenje interneta i tehnologije koja se zasniva na webu. Društveni mediji pružaju mogućnost pojedincu da istupi u javnost sa svojim mišljenjem.

[37] Tesla.carner.hr - Nacionalni portal za učenje na daljinu: *Uvod u Internet*. URL: https://tesla.carnet.hr/mod/book/view.php?id=5428&chapterid=883, (25.4.2022.)
[38] Hajdarović, M. (2006): *Povijesni razvoj interneta*. URL: http://povijest.net/2018/?p=2374, (25.4.2022.)
[39] CARNet=Croatian Academic and Research Network
[40] Element.hr: *Početak interneta i nastanak weba*, URL: https://element.hr/artikli/file/1259, (25.4.2022.)
[41] Sites.google.com: *Usluge interneta*, URL: https://sites.google.com/site/sveointernetu/home/usluge-interneta,(25.4.2022.)

U literaturi se navodi kako društveni mediji predstavljaju skup različitih novih izvora informacija na internetu, koje stvaraju, pokreću, distribuiraju i upotrebljavaju korisnici s ciljem edukacije drugih korisnika o proizvodima, uslugama, brendovima, pojedincima, te izazovima.[42] Također, društveni mediji su skup internet aplikacija, platformi i medija čiji je cilj suradnja između ljudi, te zajedničko stvaranje i razmjena sadržaja.[43] Online društvene mreže i društveno umrežavanje postaje vrlo popularno među djecom i mladima.

U svijetu postoje brojne društvene mreže, zavisno od zemlje do zemlje, no najpoznatije su Facebook, YouTube, Twitter i Instagram koje su osvojile i Hrvatsku. Istraživanja pokazuju da se Hrvati koriste i domaćim društvenim mrežama poput Iskrice, Trosjeda, Tulumarke i sl.[44] U nastavku Slika 1. prikazuje neke od najvećih društvenih mreža koje korisnici rabe za upoznavanje novih ljudi, druženje te ponovno uspostavljanje kontakta s drugim korisnicima.

Slika 1. Najveće stranice za društveno umrežavanje prema sveukupnoj posjećenosti



Izvor: eBizMBA (2017): Top 15 most popular social networking sites, URL: http://www.ebizmba.com/articles/social-networking-websites, (1.5.2022.)

[42] Mangold, G. W., Faulds, D. J. (2009): „Social media: The newhybrid element of the promotionmix," *Business Horizonts* 53(4): 357.-365., str.357.
[43] Palmer, A., Koenig, L.N. (2008): „An experiental, socialnetwork-based approach to direct marketing". International Journal of Direct Marketing 3(3): 162.-176., str.170.
[44] Grbavac, J., Grbavac, V. (2014): „Pojava društvenih mreža kao globalnog komunikacijskog fenomena." *Media, culture and public relations* 5(2): 206.-219.

Iz prethodne slike je jasno vidljivo kako je Facebook najveća društvena mreža, a njega slijede YouTube, Instagram, Twitter, WhatsApp, Pinterest, Reddit, Ask.fm, Tumbir, Flickr, SnapChat,…

3.3. Računalna sigurnost

Računalna je sigurnost skup mjera i postupaka kojima se osiguravaju podatci pohranjeni u računalima, često dostupni i preko računalne mreže. U današnje doba, kada se najveći dio podataka pohranjuje u računalnima, kadšto i samo u tom obliku, te kada se velik dio poslovanja, komunikacije i sl. odvija u računalnom okruženju, gubitak ili zloporaba podataka može prouzročiti velike štete. Stoga je računalna sigurnost osobito važna, a obuhvaća zaštitu podataka od gubitka ili oštećenja, kao i od neovlaštena pristupa njima.[45] Računalna se sigurnost odnosi na zaštitu podataka i komunikaciju na mreži, pri tome se vodeći trima osnovnim načelima:

- integritet podataka se odnosi na promjene informacija koje moraju biti odobrene od strane autora,
- dostupnost sustava se odnosi na kontinuirani rad na održavanju produktivnosti istog i
- povjerljivost - otkrivanje podataka mora biti autorizirano, a podatci zaštićeni od napada bilo koje vrste.

Kada je riječ o računanoj zaštiti, pri čemu se stavlja naglasak prije svega na programsku zaštitu informacijskih sustava, važno je istaknuti kako je ovaj aspekt jedan od najranjivijih i najčešće ugrožen. Sve brže internet veze omogućavaju brzu, laku i jednostavnu distribuciju softvera, a računalna mreža je glavni medij koji to omogućuje.

Računalna se sigurnost dijeli na:

- sigurnost hardvera uključuje fizičku zaštitu i kontrolu prometa mreže (zaštitni zidovi hardvera, proxy poslužitelji, sigurnosno kopiranje, …)
- sigurnost softvera uključuje sprječavanje zlonamjernih napada, neovlaštene izmjene koje mogu dovesti do neispravnosti ili kršenja intelektualnog vlasništva programa te

[45] Enciklopedija.hr (2021.) Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, URL: https://www.enciklopedija.hr/natuknica.aspx?id=68380, (22.6.2022.)

- sigurnost mreže štiti pouzdanost, cjelovitost mreže i podataka, a primjenjuje se putem hardvera i softvera (antivirusni programi, vatrozidi (*eng. Firewall*) za blokiranje neovlaštenog pristupa, …).

3.4. Kibernetička sigurnost

Kibernetička sigurnost (*eng. cyber security*) obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom sustavu, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi.[46] Kibernetička sigurnost odnosi se na sustav tehničkih mjera zaštite kako bi se postigla dostupnost i povjerljivost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom – virtualnom prostoru unutar kojeg se odvija komunikacija. Pojam kibernetička sigurnost se primjenjuje u različitim kontekstima, od poslovanja do mobilnih aplikacija, te se dijeli u sljedeće kategorije:

- mrežna sigurnost štiti računalne mreže od „uljeza“ – bilo ciljanih napadača ili zlonamjernih softvera,
- sigurnost aplikacija usmjerena je na zaštitu softvera i uređaja,
- informacijska sigurnost štiti privatnost podataka – u prijenosu i pohrani podataka,
- operativna sigurnost odnosi se na dopuštenja koja korisnici imaju pri pristupanju mreži te postupke koji određuju kako i gdje se podatci dijele i pohranjuju i
- edukacija krajnjih korisnika.

3.1.1. Nacionalna strategija kibernetičke sigurnosti

Godine 2015. Vlada RH donosi strateški dokument kojim želi započeti sveobuhvatno planiranje zaštite korisnika elektroničkih usluga u javnom i gospodarskom sektoru te građanstvu u cjelini - Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njenu provedbu. Strategija i Akcijski plan za njenu provedbu predviđaju pristup kibernetičkom prostoru kao virtualnoj dimenziji društva s ciljem učinkovite provedbe zakona i zaštite demokratskih vrijednosti u kibernetičkom

[46] Središnji državni ured za razvoj digitalnog društva (2022.): *Kibernetička sigurnost*, URL: https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436, (22.6.2022.)

prostoru. Donošenjem Strategije i Akcijskog plana i uvođenjem sustavnog i sveobuhvatnog pristupa području kibernetičke sigurnosti namjerava se postići niz ciljeva koji su od iznimne važnosti za razvoj društva u cjelini, a napose:

- sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, kibernetička dimenzija društva;
- provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora;
- uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima potrebnim za osiguravanjem više razine opće sigurnosti u kibernetičkom prostoru;
- jačanje svijesti o sigurnosti svih korisnika kibernetičkog prostora;
- poticanje razvoja usklađenih obrazovnih programa;
- poticanje istraživanja i razvoja, napose u području e-usluga;
- sustavni pristup međunarodnoj suradnji u području kibernetičke sigurnosti.[47]

Strategija označuje početak sustavnog i trajnog poboljšanja, praćenja i napretka zaštite kibernetičke sigurnosti.

3.5. Cyber kriminalitet

Iako se iz godine i godinu pojavljuje sve veća stopa računalnog kriminaliteta neka određena i svjetski usvojena definicija ne postoji ni danas. Mnoga stajališta i brojne rasprave o samome pojmu računalnog kriminaliteta dovele su do situacije u kojoj računalni kriminalitet još uvijek ne predstavlja zaokruženu kategoriju u smislu fenomenološke kategorije, nego se još uvijek smatra jednom vrstom radnje kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, odnosno forma koja će u budućnosti postati i više nego dominantna.[48] Tako su nastale i neke definicije koje su zapravo uske kako bi se objasnio računalni kriminalitet. To se događa prvenstveno zbog činjenice da mnoge definicije u računalni kriminalitet ubrajaju samo ona kaznena djela koja nije moguće počiniti bez posebnog stručnog znanja ili samo ona djela koja se ne

[47] Mup.gov.hr (2015.) *Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Strategije*, URL: https://mup.gov.hr/UserDocsImages//dokumenti/kiberneticka_sigurnost//Sa%C5%BEetak%20Nacionalne%20strategije%20kibernetiki%C4%8Dke%20sigurnosti.pdf , (18.6.2022.)
[48] Dragičević, D. (2004): *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb: Informatorov biro sustav, str.111.

bi mogla počiniti bez korištenja kompjutera, odnosno računala. Tako je i danas najčešće upotrebljavana definicija koja kaže „da je računalni kriminal svako ono djelo koje je počinjeno pomoću posebnog znanja o stručnom korištenju kompjuterske tehnologije“.[49] Ipak, jedna od najpoznatijih definicija je ona koja je nastala u sklopu OECD-a još 1983. godine. Prema toj definiciji svijet smatra računalnim kriminalitetom sva protupravna, nemoralna i nedopuštena ponašanja u vezi s automatskom obradom podataka ili njihovim prijenosom.[50]

Računalni kriminal označava oblik kriminala pri kojem su kaznena djela načinjena računalom i putem interneta kako bi se na nezakonit način došlo do informacija koje nisu dostupne svima.

U današnje vrijeme sve bržeg razvoja informatičke industrije i tehnologije, dolazi i do sve više oblika računalnog kriminala koji su i sve češći. Samom razvoju računalnog kriminala najviše doprinosi internet čiji je razvoj napadačima otvorio mnoge nove načine za napade na podatke i sigurnosne sustave, a razvoj tehnologije olakšao i ubrzao te nezakonite postupke kojima dolaze do željenih informacija.

Računalni kriminal kao takav, obuhvaća različite nezakonite radnje poput piratstva, prisluškivanja, napada različitim virusima, crvima, provaljivanje u informacijske sustave te krađu podataka i njihovo mijenjanje ili brisanje. Takve radnje uglavnom se rade preko interneta, a informacijski sustavi se, sa većim ili manjim uspjehom, ovisno o vrsti napada, protiv njih svakodnevno bore.[51]

Računalni kriminal u današnje vrijeme je sve prisutniji i nažalost često nanosi veliku štetu tvrtkama ili organizacijama, posebno ako je riječ o velikim hakerskim napadima ili onima čiji su cilj podatci od velike važnosti. Takav kriminal često negativno utječe na poslovanje mnogih i može prouzročiti ozbiljnu štetu i negativne posljedice po sigurnost podataka ljudi diljem svijeta.

3.5.1. Vrste, ciljevi i razlozi napada

Danas su među najpoznatijim napadima, odnosno računalnim kriminalitetima krađe identiteta, spamovi, zlonamjerni programi, ali i brojne druge stvari o kojima se ne govori toliko u javnosti. Tako se mogu prepoznati još i sljedeći tipovi računalnog kriminaliteta:

[49] Ibid.
[50] Ibid.
[51] MUP KS: *Zaštitimo se od cyber kriminala*, URL: http://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (15.5.2022.)

- krađa osobnih podataka,
- kršenje autorskih prava,
- prijevare,
- dječja pornografija,
- cyberstalking,
- zlostavljanje.[52]

Danas se među najplodonosnijim vrstama napada na računalne sustave u sklopu kriminaliteta ubrajaju i razne prijeteće e-mail poruke. To su najčešće zastrašujuće i prijeteće e-mail poruke koje upozoravaju na "opasne" stvari koje se ljudima događaju te pokušavaju zastrašiti primatelje s ciljem da proslijedi upozorenje svojim prijateljima i poznanicima.[53] Smatra se kako su prijeteći e-mailovi postojani još od samog početka računalnog kriminaliteta.

Računalni kriminal danas je okarakteriziran brojnim napadima na računalne sustave. Poneki takvi napadi uzrokuju veliku opasnost za društvo, ali se većinom radi o manjim napadima koji služe za sitne prevare i tome slično. Najčešći ciljevi napada koji se izvode na internetu ili putem njega jesu:

- korisničke lozinke,
- podaci i informacije,
- datoteke,
- kompjuterski programi,
- web stranice,
- onemogućavanje korištenja kompjuterskog sustava,
- materijalni (tehnički) resursi informacijskog sustava.[54]

Kada su u pitanju razlozi napada, ponajprije je potrebno istaknuti da sigurnosti informacijskih sustava prijete svakodnevni napadi različitih hakera koji žele ugroziti podatke i sustav sigurnosti podataka. Napadi su djela ili postupci koji pokušavaju iskoristiti ranjivost informacijskih sustava kako bi u isti ušli te ukrali ili saznali podatke za koje nemaju ovlašteni pristup. Napadi na informacijske sustave mogu biti različiti,

[52] Politička akademija BiH: *Računalni kriminalitet – Prijetnje i posljedice na političke i ekonomske odnose*, URL: http://www.academia.edu/17744563/Ra%C4%8Dunalni_kriminalitet_Prijetnje_i_posljedice_na_politi%C4%8Dke_i_ekonomske_odnose, (15.5.2022.)
[53] Šimundić, S., Franjić, S., Vdovjak, K. (2012): „HOAX." *Zbornik radova pravnog fakulteta u Splitu*; 49(3): 459.-480., str.466.
[54] Dragičević, D. (2004): *Kompjutorski kriminalitet i informacijski sustavi*- Zagreb: Informatorov biro sustav, str.47.

ovisno o tome što napadač ili haker točno želi napraviti sa informacijama do kojih dođe te koji su mu ciljevi zbog kojih napada informacijski sustav.

Najčešći razlozi napada na sustave informacija su: pristup informacijama, izmjena podataka i uskraćivanje informacija. Dakle, napadači mogu napadati sustave sigurnosti informacija kako bi došli do informacija do kojih normalnim, zakonitim putem ne mogu doći te kako bi saznali neke povjerljive ili tajne podatke koji ih zanimaju bez da bilo što rade s njima, već da ih saznaju.

Napadači kao cilj svog ulaska u informacijski sustav mogu imati mijenjanje podataka, pa oni u sustav sigurnosti provaljuju kako bi na silu izmijenili neke podatke što im inače nije dozvoljeno ili za to nisu ovlašteni.

Kao treći razlog napada na informacijski sustav postavlja se problem kada napadači ulaskom u informacijski sustav žele uskratiti uslugu ili informacije onima koji imaju pristup njima ili žele poremetiti rad cijelog sustava informacija ili mreže podataka te tako naštetiti sigurnosti samih podataka.

S obzirom na navedene ciljeve napadača pri napadu na podatke, ti napadi se mogu podijeliti i na one napade prilikom kojih informacije ostaju nepromijenjene, a napadač ih čita i saznaje ali ne mijenja. Takvi napadi su pasivni napadi. Za razliku od njih, aktivni napadi na podatke rezultiraju promjenom postojećih podataka.

Naravno, napadi na podatke ne moraju uvijek biti od strane onih koji za pristup podatcima nisu ovlašteni. Napadi se mogu dogoditi i od strane zaposlenika neke tvrtke ili onih koji su ovlašteni za pristup podatcima, ali svejedno žele namjerno i bez valjanog zakonitog razloga promijeniti podatke iako ne bi smjeli.

Napadi na sigurnost informacijskih sustava uvelike ovise o učinkovitosti sustava zaštite podataka. Ovisno o tome je li sustav uspio obraniti podatke ili je u sustav provaljeno te je došlo do krađe podataka ili njihove izmjene, napade se može podijeliti na uspješne i neuspješne.

Uspješni napadi rezultiraju negativnim posljedicama po vlasnike tih podataka te dolazi do neovlaštenog pristupa istima, krađe ili izmjene podataka koji su bili cilj napadača. Za razliku od njih, neuspješni napadi označavaju one pri kojima je informacijski sustav uspio podatke očuvati sigurnima te je onemogućen pristup napadačima na podatke koji su ostali sigurni.

Prema svemu navedenom može se zaključiti kako postoji velik broj računalnih napada koji pripadaju računalnom kriminalitetu. Već dugi niz godina postoje brojne teorije zašto se takve stvari događaju, ali u današnjem svijetu razlozi za napade su

različiti, a popeli su se i na višu razinu kada se uništavaju računalni sustavi svjetski poznatih institucija o kojima ovise milijuni ljudi, kao i napadi na računalne sustave vodećih država svijeta kako bi se postigla kontrola nad određenim stvarima i slično. Do napada dolazi najčešće kada postoji:[55]

- neovlašteni pristup tuđem računalnom sustavu,
- neovlašteno mijenjanje podataka i/ili programa,
- neovlašteno brisanje podataka i/ili programa,
- presnimavanje nekog malicioznog programa,
- korištenje tuđeg računala na mreži za pristup drugom sustavu,
- stvaranje uvjeta za nastanak, odnosno samo nastajanje štete na infrastrukturi koja može dovesti do sprječavanja ili otežavanja daljnjeg rada sustava,
- krađa, oštećenje ili uništenje tehničke osnovice ili medija za pohranu podataka.[56]

Samom razvoju računalnog kriminala najviše doprinosi upravo internet čiji je razvoj napadačima otvorio mnoge nove načine za napade na podatke i sigurnosne sustave, a razvoj tehnologije olakšao i ubrzao te nezakonite postupke kojima dolaze do željenih informacija.

Zaštita od ove vrste kriminaliteta postaje sve važnija, posebice kada je riječ o novim zloupotrebama počinjenim na računalima ili uz njihovu pomoć. Smatra se kako se danas takav kriminalitet i takve prijevare pronalaze na svim lokalnim, nacionalnim i regionalnim razinama, a sve većim ispreplitanjem računalnih mreža ovakve se prijevare šire diljem svijeta.

Računalni kriminal je sve učestaliji problem i najbolje ga je pokušati prevenirati korištenjem različitih sigurnosnih sustava te korištenjem oblika zaštite podataka. Ukoliko dođe do sigurnosnog napada na podatke, bitno je takve napade uočiti, otkriti i, ako je ikako moguće, spriječiti te naposljetku kazniti.

[55] Ibid., str.49.
[56] Ibid., str.49.

3.6. Zlonamjerni sadržaji i prijetnje

Globalne kibernetičke prijetnje bilježe ubrzani rast na godišnjoj razini zbog umrežavanja svakodnevne uporabe informacijskih sustava. Neke od najčešćih prijetnji kibernetičkoj sigurnosti su:

Adware – softver koji automatski preuzima oglase ili ih prikazuje nakon instaliranja nekoga softvera ili korištenja aplikacija

Backdoor – sadržaji koji nisu instalirani od strane korisnika, a napadaču omogućuju pristup njegovu sustavu

Botnet – mreža računala stvorena od strane napadača koja mu daje kontrolu nad zaraženim računalom

Crv (Worm) – nepoželjni, zlonamjerni program koji se umnožava i na taj se način širi računalnom mrežom

Dictionary napad – napadač u rječničku bazu unosi poznate podatke, lozinke, nizove riječi i na taj način pogađa lozinku korisnika

Malver (Malware) – softver koji napadaču omogućava pristup računalu korisnika bez njegova znanja

Pametno pogađanje lozinke – otkrivanje lozinke korisnika temeljem prikupljenih podataka o korisniku

Phishing – masovno zasipanje velikog broja osoba porukama u kojima se na prijevaru traži odavanje tajnih podataka.[57] Najčešći oblik phisinga su lažne poruke koje se šalju korisnicima, a sadrže poveznice na neke od zlonamjernih poslužitelja.

Phishing URL – poveznica koja vodi do lažne internetske stranice s ciljem krađe povjerljivih podataka

Spam – neželjena e-poruka poslana korisniku s ciljem prodaje ili promidžbe sadržaja bez privole korisnika

Virus – računalni program koji svojom reprodukcijom može zaraziti računala tako da bez dopuštenja ili znanja korisnika kopira samog sebe u datotečni sustav ili memoriju ciljanog računalnog sustava[58]

[57] Cert.hr (2016.) *Mali pojmovnik kibernetičke sigurnosti*, URL: https://www.cert.hr/wp-content/uploads/2009/07/Pojmovnik.pdf, (22.6.2022.)
[58] Ibid.

3.7. Sigurno komuniciranje na internetu

U doba globalizacije i tehnologija, veliku revoluciju u svijetu računala i komunikacije izazvao je internet. Internet je danas postao novo oruđe komunikacije, odnosno nove okoline javnog sudjelovanja, te kao takav javlja se kao val ideja o tome na koji način nove interaktivne tehnologije utječu na nastanak nove elektroničke sfere. Internet povezuje i međusobno udružuje više različitih oblika komunikacijskih odnosa, primjerice čuvanje i razmjenu informacija, kao i reprodukciju i razmjenu komunikacijskih kanala. Internet je tako registar informacija i sredstvo komunikacije.[59] Zahvaljujući internetu danas je moguće iznimno brzo dijeliti informacije, istraživati i komunicirati s ljudima iz svih dijelova svijeta. Internet ujedno predstavlja i jedan od najuspješnijih primjera rezultata sustavnog ulaganja i predanosti istraživanju i razvoju informacijske infrastrukture. Može se reći da je u svome razvoju, internet je prerastao onaj osnovni okvir razmjene informacija te postao jedno od osnovnih sredstava modernog i poslovnog života.

No, pojava interneta također uzrokuje razvoj jednog potpuno novog života koji se vodi na mreži i koji donosi brojne izazove i probleme kao što je pitanje sigurnosti i slobode. Pojavljuju se i novi oblici komunikacije koji su uvjetovani prirodom društvenih medija. Nove komunikacijske i informacijske tehnologije svojim su ubrzanim razvojem putem interneta i društvenih mreža utjecale na sve sfere čovjekova života. Uslijed tehnološkog rasta došlo je do pojave nove tehnološke paradigme odnosno informacionalizma koji postavlja temelje za razvoju umreženog društva.

Društveni mediji se konstantno razvijaju i šire te snažno utječu na komunikaciju u društvu koja poprima nove oblike. Korisnici danas mogu sami oblikovati sadržaj od interesa te time dolazi do brojnih revolucija na samoj mreži među kojima je i najznačajniji haktivizam. Internet utječe na sva područja društvenog života u kojima se ljudi suočavaju sa brojnim mogućnostima koje nudi nova komunikacijska okolina, ali i sa brojnim izazovima. Danas se pojedinci sve teže mogu zaštititi od ljudi koji pregledavaju tuđe podatke jer je sve javno dostupno i anonimnost je spala na najniži nivo. Ipak, nova komunikacijska okolina je omogućila korisnicima mnoštvo informacija koje su potrebne te samim time olakšala studiranje, pronalazak posla, kupnju određenih proizvoda, promociju i sl. Ipak, velik broj informacija su upravo lažne te je to jedan od glavnih problema cyber društva. Iz svega navedenog daje se zaključiti da

[59] Oblak, T. (2002): „Internet kao medij i normalizacija kibernetskog prostora.“ *Medijska istraživanja* 8(1): 61.-76., str.62.

internet, odnosno cyber-okolina i internetske forme oglašavanja imaju svoje dobre i loše strane, a korisnici bi ih trebali iskoristiti na za njih najbolji način.

Može se zaključiti da internet danas predstavlja široko rasprostranjenu mrežu informacijske infrastrukture čija je povijest poprilično složena i uključuje tehnološke, organizacijske i društvene aspekte djelovanja. Internet mijenja navike ljudi, način komunikacije i društvo u cjelini. U zadnjih desetak godina uvelike se promijenio način na koji ljudi rade i provode slobodno vrijeme, način na koji upoznaju nove ljude i grade odnose s njima - sve zahvaljujući internetu. Neki u promjenama koje je donio internet vide samo negativne strane, no bez obzira na mogućnost postojanja istih, društvo ne može stagnirati već se razvija usporedno s razvojem tehnologije, a taj razvoj donosi i nove obrasce življenja koje se ne mora nužno etiketirati kao loše samo zato što se razlikuju od prošlih. Razvoj virtualnih društvenih zajednica jedan je od važnijih fenomena internetskog doba koji su uvelike promijenili načine na koje se ljudi druže i surađuju.

Komercijalizacijom interneta, odnosno pojavom mogućnosti obrtaja novca putem "online" kupovine i internet bankarstva, pojavila se potreba za sigurnijim načinom komunikacije. Danas se internet koristi za dopisivanje, dnevno informiranje, skidanje sadržaja, pretraživanja, igranje igrica i klađenje, kupovanje, marketing,…

Postavlja se pitanje kakva bi to komunikacija trebala biti da bi bila sigurna. Iako je „sigurno“ pomalo nejasan izraz, donekle siguran oblik komunikacije trebao bi biti takav da su podatci korisnika privatni, odnosno da ih ne iznosi trećoj strani. Također, sigurna komunikacija je ona u kojoj je kibernetičkim kriminalcima iznimno teško provaliti u sustav korisnika pogađanjem lozinke, iskorištavanjem lošeg koda i sl., i stoga je bitno osigurati što jaču lozinku i dodatne sigurnosne provjere. Nadalje, komunikacija korisnika mora biti dosljedno pouzdana, bez prekida ili ranjivosti za iskorištavanje.
Najsigurniji oblici internetske komunikacije su:

- IRC kanali - internetski relay chat (IRC) je protokol aplikacijskog sloja koji omogućuje komunikaciju više ljudi putem teksta (i ponekad razmjenu datoteka) putem klijenata na njihovim pojedinačnim uređajima. Weechat i Pidgin su dvije od najpopularnijih opcija u tom kontekstu;
- sigurne aplikacije za dijeljenje datoteka - značajke poput višefaktorske provjere autentičnosti, 256-bitne enkripcije i isteka datoteke omogućuju razmjenu datoteka bez brige;

- šifrirane e-poruke - proširenje aplikacije ili dodatak poput Enigmaila ili namjensku uslugu kao što je Infoencrypt
- druge aplikacije za šifriranje poruka. E-pošta, dijeljenje datoteka i IRC razgovori nisu jedini sigurni načini internetske komunikacije. Gotovo svaki način komunikacije mogao bi se učiniti sigurnim uključivanjem boljih protokola za šifriranje i provjeru autentičnosti te dodatnih sigurnosnih značajki poput isteka podataka.[60]

Korisnici bi trebali biti izbirljivi po pitanju aplikacija koje oglašavaju njihovu „sigurnost“. U tom kontekstu potrebno je pročitati recenzije korisnika, usporediti ih s konkurentima i sl. Korisno je koristiti i VPN (virtualna privatna mreža), odabrati i često mijenjati jake lozinke, razmišljati pažljivo o informacijama koje korisnik osobno odašilje i objavljuje na svojim društvenim mrežama te je korisno izbjegavati oslanjati se na telekomunikacije. Naime, svaki vid komunikacije koji se oslanja na mobitele i računala je generalno nesiguran. Stoga je najbolje komunicirati u trenutku povezivanja na zaštićenu Wi-Fi mrežu, umjesto korištenja vlastite 4G mreže.[61]

[60] Alton, L. (2017): *The 4 Most Secure Forms of Online Communication*, Isaca.org, URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/the-4-most-secure-forms-of-online-communication (17.5.2022.)
[61] Ibid.

4. DIGITALNA PISMENOST I SIGURNOST DJECE NA INTERNETU

Ubrzan rast i razvoj tehnologija, posebice interneta, utječe na to da se svake godine gotovo udvostručuje broj informacija. Ljudi gotovo svakodnevno produciraju informacije na lako dostupnim internet platformama. U tom kontekstu se zemljopisne granice i vremenske barijere polagano brišu, te je sve veći broj dostupnih podataka i informacija do kojih je moguće doći vrlo brzo, lako i jednostavno.

„Digitalna kultura dio je kulture društva, dio kulturne politike te označava proces transformacije same ideje kulture u društvu. Ono što najviše razlikuje nekadašnju građansku kulturu od digitalne kulture jest virtualnost kao paradigma bivanja i djelovanja u kulturi. Ti novonastali proizvodi i sustavi stvaraju svoju publiku i svoja pravila komuniciranja.“[62]

Tijekom povijesti, a osobito u današnje vrijeme pismenost se ističe kao vrlo bitna odlika svakog obrazovanog čovjeka. Pismenost je dio svake kulture i tradicije. Tijekom povijesti načini i vrste pismenosti su se mijenjale, a danas je osobito važna digitalna pismenost. Ova vrsta pismenosti povezuje kulture i tradicije diljem svijeta, poslovni svijet, školske i mnoge druge aspekte.

4.1. Digitalna pismenost

Iako se koncept digitalne pismenosti donekle preklapa s konceptom informacijske pismenosti, informacijska je pismenost širi koncept koji obuhvaća sve informacije dostupne u različitim oblicima.[63]

Digitalnu ili internetsku pismenost podrazumijeva sposobnost čitanja i razumijevanja hiperteksta ili multimedijskih tekstova, sa razumijevanjem slika, zvukova i teksta prikazanog u obliku dinamičnog, nelinearnog hiperteksta. Korisnik potom barata informacijama dostupnima putem interneta i dostupnom digitaliziranom građom (u knjižnicama, muzejima, suvremenim vodičima kroz kulturne spomenike i slično). Također, informacijsko-komunikacijske tehnologije uvijek se koriste za potrebe posla i u slobodno vrijeme za potrebe komunikacije.

[62] Zgrabljić Rotar, N. (2011): „Masovni mediji i digitalna kultura.“ U: *Digitalno doba, Masovni mediji i digitalna kultura.* Zadar: Sveučilište u Zadru, str. 38.
[63] Vrkić Dimić J. (2014): “Suvremeni oblici pismenosti.” *Školski vjesnik*; 63(3): 381-394., str. 386.

„Konkretne vještine obuhvaćene pojmom digitalne pismenosti uključuju sposobnost prosuđivanja o online izvorima, pretraživanje interneta, upravljanje multimedijalnom građom, komuniciranje putem mreže“[64] te kreiranje i razmjenu informacija, kao i participaciju u virtualnim zajednicama.[65]

Uporabom ovakve vrste pismenosti, važno je razviti kritičko mišljenje kako bi se postiglo što bolje i efikasnije učenje; odnosno razvila vještina „znati kako učiti“. Komunikacija putem interneta preselila se na računala, a pogotovo na pametne telefone. Time se omogućio lakši pristup informacijama mladima koji su željni novih informacija kako za područje njihovog društvenog, tako i obrazovnog života. U skladu sa brzim učenjem i znatiželjom, mladi relativno brzo razvijaju konkretne komunikacijske kompetencije kao određeni stupanj njihove komunikacijske pismenosti kroz sposobnost da pronađu, vrednuju, organiziraju, odabiru i ispravno koriste potrebne informacije, da ih interpretiraju u određeno znanje i dublje razumijevanje kojima će u konačnici razviti neke nove ideje odnosno nova znanja. Ovisno o informacijskim kompetencijama korisnika, njegovoj dobi, konkretnom upitu i količini potrebnih informacija, digitalno dostupan informacijski izvor može i ne mora biti koristan.

Digitalno znanje je danas vrlo dostupno, a pravilnim informiranjem, obrazovanjem i obukom korisnika za pronalaženje i korištenje određenoga izvora, omogućuje se samostalni pronalazak informacija u kratkom vremenu, a ponekad s manjim financijskim troškovima.[66]

Interaktivna tehnologija utječe na standard življenja, u isto vrijeme brinući o vlastitoj privatnosti i sigurnosti računala. Iz tog razloga, svaka osoba danas bi trebala u određenoj mjeri biti informatički pismena.[67]

Kada se govori o informatičkoj pismenosti u školi, tada ona podrazumijeva korištenje i razumijevanje dostupne informatičke tehnologije uglavnom kroz nastavni predmet Informatika. Informatička pismenost u najranijoj dobi obuhvaća svladavanje tehnika i vještina rukovanja osobnim računalima, tabletima ili bilo kojim drugim pametnim uređajima te korištenjem tipkovnice s ciljem unošenja jednostavnih podataka ili traženja jednostavnih, djeci zanimljivih informacija. Ova faza poznata je i

[64] Špiranec, S. (2003): „Informacijska pismenost-ključ za cjeloživotno učenje.“ Edupoint; 3(17)
[65] Demunter, C. (2006): „How skilled are Europeans in using computers and Internet?“. *Eurostat: Statistics in Focus*; 17
[66] Jakovac Baier A., Hebrang Grgić, I. (2015): „Informacijska (ne)pismenost: istraživanje mladih korisnika knjižnica u Vukovaru.“ *Knjižničarstvo*, Glasnik Društva knjižničarstva Slavonije i Baranje; 19(1-2): 27.-46., str. 32.
[67] Bošković, T. (2017): *Medijska pismenost i suvremeno društvo* [diplomski rad]. Rijeka: Filozofski fakultet Sveučilišta u Rijeci, str.4.-5.

kao faza igranja jer djeca kroz igru ovladavaju tehnikama korištenja računala odnosno tipkovnice.[68]

Jedan od primjera važnosti poznavanja tehnologije za mlade može se vidjeti iz online učenja (učenje na daljinu), koje je u novije vrijeme popularno uslijed pandemije Covid-19.

Informacijska pismenost danas je prepoznata kao jedna od „vještina koje su nužna za inovativno učenje pojedinca. Ista se, također, može definirati kao skup znanja, stavova i vještina koje se tiču prepoznavanja informacijske potrebe, odnosno pribavljanje potrebnih informacija i njihovog vrednovanja, uporabe i stvaranja informacija na legalan i etičan način uz poštovanje ljudskih prava s ciljem zadovoljenja osobnih, profesionalnih i društvenih ciljeva“.[69]

Danas su korištenjem interneta i internetskih usluga granice javnog i privatnog izblijedile, često se poistovjećuje realni i virtualni svijet što dovodi do lake i jednostavne zlouporabe osobnih podataka korisnika, znati načini i mjere zaštite osobnih podataka dio su digitalne pismenosti korisnika stoga je biti digitalno pismen, u današnje vrijeme, jedna od važnih kompetencijskih vještina koje korisnik mora imati.

[68] Ibid.
[69] Jokić A., Koljenik D., Faletar Tanacković S., B.Badurina B. (2016): „Vještine informacijske i informatičke pismenosti studenata informacijskih znanosti u Osijeku: pilot-istraživanje.“ *Vjesnik bibliotekara Hrvatske* 59(3-4): 63-92., str.66.

5. HARDVERSKA I SOFTVERSKA ZAŠTITA OSOBNIH PODATAKA DJECE NA INTERNETU

Zaštita osobnih podataka predstavlja, danas, jedan od najvažnijih problema i procesa računalnih sustava jer se velik broj podataka i informacija nalazi u digitalnom obliku. Sigurnost se definira kao stupanj zaštite od neke opasnosti, štete, gubitka,… . Kako se povećava broj zlouporabe osobnih podataka korisnika pri korištenju interneta, zaštita podataka postala je iznimno važna. U nastavku rada navest će se neke od oblika hardverske i softverske zaštite osobnih podataka.

5.1. Hardverska zaštita osobnih podataka djece na internetu

Hardverska zaštita podataka obuhvaća različite tehničke uređaje i strukture koje štite podatke od neovlaštenog pristupa istima.

Hardverski vatrozid (eng. firewall)

Hardverski su vatrozidi sadržani s usmjerivačem ugrađenim u hardver računala, nadziru promet na računalima i uređajima koji su povezani s mrežom usmjerivača u lokalnoj mreži. Hardverski vatrozidi pružaju sigurnost tijekom korištenja interneta. Primjenjuju filtriranje web paketa za provjeru o izvoru i odredištu te pouzdanost IP adresa ili zaglavlja, informacije se tada uspoređuju sa sigurnosnim pravilima, unaprijed definiranim. Hardverski vatrozidi blokiraju veze koje sadrže zlonamjerne prijetnje i sadržaje. Veliki nedostatak istih je da štite računalo na samo jednom mjestu (npr. kod kuće), ne u pokretu, stoga je preporuka korištenje softverskog vatrozida.

Hardverski ključ (eng. dongle)

Hardverski ključ ili tzv. dongle (*eng. dongle*) je dio hardvera koji se koristi u svrhu zaštite softvera i podataka na takav način da se povezuje na računalo. Ranije se povezivanje vršilo preko serijskog ili paralelnog porta, a danas najčešće putem USB porta računala. Drugi poznati nazivi za to su još hardlock ili key. Osnovna svrha tih uređaja je sprječavanje kopiranja i neovlaštenog korištenja softvera i podataka. Samo uz postojanje i pomoć tog ključa se može pokrenut određena aplikacija i pristupiti

podacima. Taj uređaj se spaja sa računalom kako bi se mogao pokretati osigurani (zaštićeni) softver (aplikacija) i pristupati zaštićenim podatcima.[70]

Sustav za detekciju neovlaštenog pristupa

Sustav za detekciju neovlaštenog pristupa su uređaji koji se upotrebljavaju za otkrivanje pokušaja napada na sustav (IDS). Na temelju baze sa definiranim pravilima prati aktivnost na sustavu te detektira i prijavljuje sve događaje koji nisu u skladu sa definiranim pravilima. Razlikuju se dva osnovna tipa sustava za detekciju neovlaštenog pristupa:

- sustav za detekciju neovlaštenog pristupa pojedinačnim računalima (eng. Hot-based IDS)
- sustav za detekciju neovlaštenog pristupa na računalnoj mreži (eng. Network IDS). [71]

5.2. Softverska zaštita osobnih podataka djece na internetu

Brzi razvoj interneta i internetskih usluga rezultira i većim brojem zloupotrebe osobnih podataka istih vrlo je važno zaštiti osobne podatke prilikom korištenja istih. Neki od oblika softverske zaštite osobnih podataka korisnika su:

Ograničenje pristupa računalu

Ograničenje pristupa računalu odnosi se na zaštitu lozinkom (unošenje sigurnosnog pina pri otključavanju uređaja, otključavanje otiskom prsta, …). Lozinke mogu biti i slabe točke zaštite sustava. Osnovne pogreške pri korištenju lozinki su jednostavnost, ista lozinka na više korisničkih računa, pohranjivanje lozinki, … . Kako bi se spriječile ove pogreške, treba slijediti određena pravila za stvaranje lozinki:

- Kompleksnost – kombinacija velikih i malih slova, kombinacija brojeva te posebnih znakova
- Vijek lozinke – lozinku treba mijenjati nakon određenog vremena te

[70] Adnan Ramakić, Zlatko Bundalo (2013.), *SOFTVERSKO-HARDVERSKA ZAŠTITA PODATAKA U RAČUNARSKIM SISTEMIMA*, URL: https://tfb.ba/repozitorij/2/RIM/RIM2013/rim2013_057%20C%20-%20101%20-%20Ramakic%20Adnan_pdf_59.pdf (3.9.2022.)
[71] Carnet.hr (2004.), *Sustav za prevenciju neovlaštenog pristupa*, URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-08-86.pdf (4.9.2022.)

- Duljina lozinke – ne treba biti kraća od zadanog broja duljine (12 znakova).

Izrada sigurnosnih kopija

Izrada sigurnosnih kopija (eng. *backup*) je kopija podataka sa svrhom osiguravanja istih u slučaju oštećenja ili gubitka podataka, dokumenata ili programa.

Antivirusni program

Antivirusni program je softverski alat detekcije i uklanjanja računalnih virusa. Njegova je uloga zaštita računala od zlonamjernih sadržaja, ukoliko je neka datoteka ili prilog u e-pošti zaražen isti prepoznaje i upozorava korisnika te zaustavlja njegovo izvršavanje na računalu. Antivirusni programi također imaju zaštitu u realnom vremenu (eng. Real Time Protection), što podrazumijeva praćenje dolaska i pojavljivanje svake nove datoteke na nekom računalu, prije upotrebe datoteke, antivirusni program skenira datoteku i djeluje po potrebi. Kako bi računalo bilo zaštićeno od novih virusa potrebno ih je ažurirati na dnevnoj bazi jer on čini sigurnosnu barijeru između sigurne korisnikove mreže i interneta.

Softverski vatrozid (eng. firewall)

Vatrozid podrazumijeva program kojim se nadzire, propušta ili odbacuje mrežni promet, predstavljaju prvu i temeljnu metodu povećanja sigurnosti računalnih sustava. Dijele se na:

- poslovne – programsko rješenje koje štiti poslovnu mrežu preusmjeravajući mrežni promet kroz poseban uređaj te
- osobne – programsko rješenje koje štiti korisničko računalo.

Zadatci vatrozida su, prije svega, prijava neovlaštenog pokušaja spajanja na računalo, određivanje lokalnih mrežnih servisa kojima je dopuštena mrežna interakcija, nadziranje lokalnih mrežnih servisa, sprječavanje detektiranja otvorenih mrežnih priključaka od potencijalnih napadača, nadziranje lokalnih mrežnih servisa te pružanje informacija o aplikaciji koja zahtjeva mrežnu komunikaciju.[72]

[72] Cis.hr, *Zaštita mreže – vatrozid*, URL: https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html (30.8.2022.)

Antispyware

Antispyware alati pomažu pri blokiranju malicioznih programa, prate podatkovni promet web stranica, e-pošte, spremljenih datoteka.

5.3. Alati za zaštitu osobnih podataka djece na internetu

S djecom je, dakle, potrebno razgovarati i upoznati ih s opasnostima koje je moguće sresti na internetu. Osim toga, potrebno ih je i zaštiti alatima za kontrolu korištenja računala. Takvi alati učinkovito štite djecu od nepoćudnih sadržaja i zlonamjernih korisnika na način da provode filtriranje sadržaja kojima djeca pristupaju i kontroliraju vrijeme boravka djeteta na internetu. Filtriranje se pritom provodi tako što se blokiraju pojedine web stranice ili se pak blokira pristup nekim neprimjerenim sadržajima. Također je pomoću takvih alata moguća kontrola korištenja nekih programa na računalu (igrice, chat i dr.). Osim toga, alati za obiteljsku zaštitu omogućuju i praćenje aktivnosti djeteta na računalu tako što pružaju popis posjećenih web stranica i programa koji su pokretani, prikazuju aktivnosti na tipkovnici (sadržaj komunikacije) i pružaju analizu razmijenjenih e-mail poruka.[73]

Microsoft Windows Vista i Windows 7 primjerice imaju već ugrađenu funkcionalnost roditeljske zaštite, odnosno alat je već uključen u operacijski sustav i nije potrebna dodatna instalacija. Nadalje, korištenjem Windows Live Obiteljska sigurnost moguće je za svakog člana obitelji stvoriti zaseban račun i podesiti mu postavke. Dobar primjer alata je i Parental Control Bar. To je besplatan alat organizacije WRAAC. Riječ je o roditeljskom i dječjem načinu rada prilikom čega su u dječjem načinu uključena određena ograničenja. Takav alat omogućuje izradu popisa zabranjenih web sjedišta, definiranje filtara za blokiranje nepoćudnih sadržaja, kontrolu vremena korištenja računala i pojedinih programa te izradu dnevnih izvještaja o načinu korištenja računala.[74]

[73] Carnet.hr: *Sigurnost na internetu*, URL: https://www.carnet.hr/wp-content/uploads/2019/09/Sigurnost-na-Internetu-1.pdf, (30.5.2022.)
[74] Ibid.

6. PREVENCIJA KRAĐE OSOBNIH PODATAKA DJECE NA INTERNETU U OSNOVNIM ŠKOLAMA

U prevenciji krađe osobnih podataka djece na internetu trebaju sudjelovati brojni akteri, odnosno svi sudionici koji su uključeni u djetetov odgojno-obrazovni proces.

6.1. Uloga roditelja

Smatra se da je uloga roditelja u odgoju djeteta povezana sa pojavom nasilnog ponašanja među djecom. Ukoliko su roditelji nezainteresirani za svoje dijete, ne daju mu potrebnu pažnju i ljubav, neprijateljski su raspoložena i odbijaju ih, djeca stvore sliku da su nevažna i da roditelje nije briga za njih što u konačnici može dovesti do delikventnog ponašanja.[75] Obitelj i obiteljsko okruženje su najbitniji u životu djeteta i stoga su izrazito važni čimbenici rizika i zaštite upravo oni u krugu obitelji. Shodno tome, esencijalna je kvaliteta odnosa s roditeljima. Kod elektroničkog je nasilja iznimno važna dobra komunikacija među roditeljima i djecom, povezanost i bliskost unutar obitelji.[76] Prema istraživanju EUKidsOnline iz 2020. godine provedenom na međunarodnoj razini djeca u Hrvatskoj se najrjeđe suočavaju sa zlouporabom osobnih podataka. Rezultati hrvatskog dijela istraživanja pokazali su nužnost edukacije roditelja o računalnoj sigurnosti kako bi mogli raditi na podizanju svijesti o važnost kibernetičke sigurnosti. Obzirom da se djeca danas od najranije dobi koriste digitalnim uređajima, a samim time i provode vrijeme na internetu potrebno ih je poučiti kontrolirati sadržaje koje pretražuju na internetu.

6.2. Uloga škole

Uloga škole u prevenciji i zaštiti osobnih podataka djece je od iznimne važnosti. Škola je mjesto u kojemu se učenici po prvi puta susreću s informatičkim pojmovima, uče o dijelovima računala te kako zaštiti sebe i svoje osobne podatke na internetu. Najprije, bitna je kvalitetna uprava i vođenje škole, ugodna radna atmosfera i jasna školska politika. S druge strane, naglasak škole mora biti na učenju, važno je sustavno pratiti napredak učenika. Disciplinski standardi moraju biti takvi da potiču zajedničko

[75] Bilić, V., Buljak Flander, G., Hrpka, H. (2012): *Nasilje nad djecom i među djecom*. Zagreb: Naklada Slap
[76] Velki, T. (2012): „Uloga nekih obiteljskih čimbenika u pojavi nasilja nad djecom“. *Psihologijske teme* 21 (1): 26-60.

planiranje, sustav nagrađivanja mora biti jasno postavljen, očekivanja moraju biti dosljedna. Bitno je i da se učenici i stručni djelatnici aktivno uključuju u funkcioniranje škole, naglasak mora biti na razvoju osobne odgovornosti i socio-emocionalne kompetentnosti te je potrebno stvoriti okruženje u kojemu će se stvarati prilike i motivirati učenike za aktivnu i trajnu uključenost u procese učenja. Prije svega, nužno je u školama osvijestiti nastavnike, učenike i roditelje na važnost sigurnosti djece na internetu. Danas se najčešće uz pojam sigurnost djece na internetu veže socio-društveni aspekt stoga je nužno najprije na razini škole, a zatim i u široj javnosti govoriti i raditi na podizanju svijesti o računalnoj sigurnosti, naučiti učenike načinima i oblicima hardverske i softverske zaštite svojih digitalnih uređaja, jer kada se nauče zaštiti svoje uređaje, zaštiti će i svoje osobne podatke.

Postoji nekoliko razina na kojima je moguće provoditi školske preventivne programe, od šire i uže zajednice, preko razine škole, razreda te pojedinca, što je prikazano u tablici u nastavku.

Tablica 2. Razine školskih preventivnih programa i aktivnosti kojima se prevenira nasilje

RAZINA	AKTIVNOSTI
Razina uže i šire zajednice	- Strategije zajednice protiv dostupnosti oružju i ilegalnih supstanci - Suradnja i partnerstvo između različitih organizacija, u svrhu rješavanja problema djece, obitelji itd. - Razvijanje nužnih resursa koji pomažu u zadovoljavanju raznih ljudskih potreba, obiteljskih i partnerskih odnosa, partnerstva između škole i obitelji i zajednice - Aktivnosti za razvoj zajednice koja će djecu i mlade u riziku vidjeti kao potencijal, a ne problem
Razina škole	- Programi u školi (u zgradi), povezani sa školom (u neposrednoj blizini, suradnici surađuju sa školom) i u zajednici (programi koji čine resurse škole i od velike su joj pomoći, podrške i potrebe) - Rekonstrukcija školskog okruženja koja je u interesu razvojnih potreba učenika - Unaprjeđenje uvjeta za razvoj socijalnih kompetencija učenika - Unaprjeđenje školske klime - Uvođenje dopunske nastave, posebnih programa i savjetovanja - Educiranje nastavnika i razvoj vještina za vođenje razreda - Educiranje stručnih suradnika

Razina razreda	- Unapređenje učeničkih vještina na emocionalnoj, socijalnoj i kognitivnoj razini - Posebni programi za razvoj novih vještina korisnih u svakodnevnom životu i rješavanju svakodnevnih problema
Razina učenika/pojedinca	- Promjena ponašanja učenika - Učenje raznih vještina na emocionalnoj, socijalnoj i kognitivnoj razini - Alternativne aktivnosti

Izvor: Bašić, J. (2012): *Prevencija poremećaja u ponašanju u školi.* Velika Gorica:: Tiskara 11.-22.

Škola za dijete mora biti sigurno okruženje. U tom kontekstu odgojno-obrazovni sustav treba poticati odgovorno ponašanje djece na internetu putem različitih aktivnosti:

- koje se odnose na tehnologiju i alate,
- koje se odnose na znanstvena istraživanja nasilja na internetu,
- vezane uz zakonske regulative nasilja na internetu,
- edukativnog tipa.[77]

Zadatak učitelja je, osim toga, razvijati digitalnu pismenost kod djece, o kojoj je bilo riječi ranije u radu.

U konačnici, bitno je naglasiti da sva djeca imaju pravo uživati u sigurnom i dobrom školskom okruženju koje promiče zdravlje, dobrobit i učenje, a dijete ne smije trpjeti zlostavljanje ili uznemiravanje bilo koje vrste. Također se zaključno može reći da škola ima veliku ulogu u razvoju odgovornog korištenja interneta. Suvremeni odgojno-obrazovni sustav mora biti orijentiran razvoju digitalne kompetencije kod učenika te razvoju medijske pismenosti.

6.3. Uloga medija

Mediji kao jedan od najvažnijih aktera socijalizacije djece i mladih, također imaju bitnu ulogu u suzbijanju nasilničkih oblika ponašanja na internetu. Naime, mediji imaju utjecaj na društvena ponašanja, te su iz tog razloga nezaobilazno sredstvo u

[77] Cajner Mraović, I., Gosarić, S., Kikić, S. (2019): „Povezanost školske klime s postupanjem učenika i razlozima za nepostupanje u situacijama nasilja na društvenim mrežama.“ *Napredak: Časopis za interdisciplinarna istraživanja u odgoju i obrazovanju*; 160(3-4): 241.-263., str.248.

„informiranju, formiranju, prenošenju vrjednota, stvaranje vizije svijeta i života, oblikovanju životnih stilova i identiteta.“[78]

Djeca su danas izložena medijima puno više nego ikada prije. Stoga se može reći da je djetinjstvo postalo medijsko.[79] Dijete nije sposobno razlikovati stvarnost od zamišljenog te se može početi poistovjećivati s nasilničkim likovima te može doći do pretvaranja nasilja u svakodnevicu.

O tome kakav će utjecaj mediji imati na dijete u prvom redu ovisi o ponašanju odraslih. To znači da je presudna aktivnost/pasivnost odraslih koji reguliraju izloženost djece medijima. Iz tog razloga, digitalna pismenost kao cjeloživotna kompetencija je izrazito bitna za odrasle. Znanje roditelja, njegovo shvaćanje i kritički odnos prema medijima odredit će postupke koje će prenijeti na djecu.[80] Ako roditelji provode sate čitajući internetske portale, mobitel mu je neizostavni dnevni dodatak, a u svoje slobodno vrijeme ne uvodi nikakve aktivnosti osim tehnologija, nemoguće je i od djeteta očekivati da će biti spremno ugasiti televiziju u prikladnom trenutku. Štetan može biti i isključiv „za“ ili „protiv“ medija stav roditelja. Razgovor s djetetom je najučinkovitiji način njegova medijskog opismenjavanja. Dijete ne može razumjeti kako je medijski sadržaj utjecao na njega i stoga je bitno da roditelj razgovara o onome što dijete zanima u vezi s medijima, odnosno da razgovaraju o gledanom filmu ili emisiji. Djeca predškolske dobi ne razlikuju imaginarno od stvarnog te ih mogu miješati, a utjecaji medijskih poruka su dalekosežni i ne moraju biti odmah vidljivi. Dakle, bitno je da roditelj kontinuirano prati svoje dijete na putu njegova medijskog opismenjavanja.[81]

6.4. Zakonska regulativa

Važna je i zakonska regulativa. Ustav Republike Hrvatske i međunarodni dokumenti štite osobe mlađe od 18 godina. „Deklaracija o pravima djeteta“ prvi je međunarodni dokument o zaštiti prava djece (1959.), s ciljem zaštite položaja djece u svijetu.[82] Jedan od najvažnijih dokumenata je UN-ova „Konvencija o pravima djeteta“ (1989.) koja sadrži 54 članka koja reguliraju položaj djece u društvu. Do 1996. godine

[78] Mandarić, V. (2012): „Novi mediji i rizično ponašanje djece i mladih.“ *Bogoslovska smotra*; 82(1): 131.-149., str.132.
[79] Pašica, A., Turza-Bogdan, T. (2020): „O medijima i govorno-jezičnome razvoju djece s roditeljskog motrišta.“ *Hrvatski: časopis za teoriju i praksu nastave hrvatskoga jezika, književnosti, govornoga i pismenoga izražavanja te medijske kulture* 18(1-2): 73.-92., str.75.
[80] Pašica, A., Turza-Bogdan, T. (2020): „O medijima i govorno-jezičnome razvoju djece s roditeljskog motrišta.“ *Hrvatski: časopis za teoriju i praksu nastave hrvatskoga jezika, književnosti, govornoga i pismenoga izražavanja te medijske kulture* 18(1-2): 73.-92., str.75.
[81] Ibid.
[82] Službena stranica Grada Rijeka: *Deklaracija o pravima djeteta*. URL: https://www.rijeka.hr/teme-za-gradane/obitelj-i-drustvena-skrb/djeca-i-mladi/sigurnost-i-zastita-prava-djece-i-mladih/deklaracija-pravima-djeteta/ (30.5.2022.)

potpisalo ju je 187 zemalja svijeta. Godine 1991. i Republika Hrvatska je potpisala ovu Konvenciju. Ovim činom se Hrvatska „obvezala pred međunarodnom zajednicom da će primjenjivati sva pravila kojima se jamči zaštita prava djece.“[83] Potpisivanje Konvencije u Hrvatskoj je pokrenulo formiranje dodatnih zakonodavnih okvira vezano uz nasilje među djecom.[84] Republika Hrvatska danas je stranka ili potpisnica brojnih međunarodnih pravnih instrumenata UN-a i Vijeća Europe po pitanju zaštite žrtava nasilja. Oni, zajedno s nacionalnim zakonodavstvom i strateškim dokumentima, čine pravni okvir za zaštitu žrtava nasilja.[85]

Obiteljski zakon jasno propisuje da dijete ima pravo na skrb za život i zdravlje, odnosno na sigurnost i odgoj u obitelji koji je primjeren njegovim tjelesnim, psihološkim i ostalim razvojnim potrebama.[86] Roditeljska skrb, u smislu Obiteljskog zakona, između ostalog podrazumijeva pravo i dužnost zaštite osobnih prava djeteta na: zdravlje, razvoj, njegu i zaštitu, ostvarivanje osobnih odnosa, odgoj i obrazovanje te određivanje mjesta stanovanja.[87] Roditelji su dužni i odgovorni štititi prava i dobrobit djeteta.[88] „Svatko je dužan prijaviti centru za socijalnu skrb povredu djetetovih osobnih i imovinskih prava. Povreda osobnih prava podrazumijeva osobito: tjelesno ili mentalno nasilje, spolne zlouporabe, zanemarivanje ili nehajno postupanje, zlostavljanje ili izrabljivanje djeteta.“[89]

Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi propisuje da su školski djelatnici dužni poduzeti mjere zaštite prava učenika, a o svakom kršenju tih prava moraju odmah obavijestiti ravnatelja škole koji je to dužan javiti tijelu socijalne skrbi (ili drugom nadležnom tijelu).[90]

Tu je i „Nacionalna strategija za prava djece u RH za razdoblje od 2014.-2020.godine“, koja, između ostalog, kao neke od mjera zaštite od nasilje u školama ističe podršku financiranju programa suzbijanja nasilja među djecom i nad djecom u školskom okruženju, osiguravanje kontinuirane edukacije djelatnika, djece i roditelja

[83] Ibid.
[84] Stepanić, L. (2019): „Vršnjačko nasilje i preventivni programi.“ *Varaždinski učitelj: digitalni stručni časopis za odgoj i obrazovanje* 2(2): 67.-77., str.75.
[85] Ministarstvo za demografiju, obitelj, mlade i socijalnu politiku (2017): *Nacionalna strategija zaštite od nasilja u obitelji za razdoblje od 2017.do 2020. godine*. URL: https://mdomsp.gov.hr/UserDocsImages/Vijesti2017/Nacionalna%20strategija%20zastite%20od%20nasilja%20u%20obitelji%20za%20razdoblje%20do%202017.%20do%202022.%20godine.pdf, str.3., (30.5.2022.)
[86] Obiteljski zakon (NN 103/15, 98/19), čl.84.
[87] Ibid., čl.92.
[88] Ibid., čl.127.
[89] Ibid., čl.132.
[90] Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 126/12, 94/13, 152/14, 07/17, 68/18, 98/19, 64/20), čl.80.

vezano uz vršnjačko nasilje te uvođenje programa vršnjačke medijacije u školski kurikulum.[91]

[91] Ministarstvo socijalne politike i mladih (2014*): Nacionalna strategija za prava djece u RH za razdoblje od 2014. – 2020. godine.*, URL: https://mdomsp.gov.hr/userdocsimages/arhiva/files/91286/NACIONALNA%20STRATEGIJA%20ZA%20PRAVA%20DJECE%20U%20RHZA%20RAZDOBLJE%20OD%202014.%20DO%202020.%20GODINE.pdf, (30.5.2022.)

7. ANALIZA PRETHODNIH ISTRAŽIVANJA

Istražujući temu softverske i hardverske zaštite računala može se zaključiti da se kroz dosadašnja dostupna istraživanja naglasak stavlja na socio-društveni aspekt sigurnosti i zaštite na internetu. Naglasak je prvenstveno stavljen na ponašanje i opasnosti koje donose društvene mreže, te kako zaštiti svoje podatke i profile na društvenim mrežama. Vrlo je važno znati, naučiti i osvijestiti djecu i mlade načine kako se i kome obratiti kada sudjeluju i postanu žrtve nasilja na internetu, ali je i od iznimne važnosti naučiti ih kako se zaštiti i spriječiti zlouporabu osobnih podataka te ih upoznati s načinima i metodama zaštite hardvera i softvera. Tablica 3. prikazuje ciljeve i činitelje istraživanje o sigurnosti djece i mladih s aspekta hardverske i softverske zaštite.

Tablica 3. Sigurnost djece na internetu – prikaz istraživanja

Sigurnost djece na internetu Softverska zaštita djece na internetu		
Naziv istraživanja	**Autori istraživanja**	**Ciljevi i činitelji istraživanja**
Digital Education: The Cyberrisks of the online classroom	I. Zalessky, S. Furnell	- zlonamjerni softver, kršenje privatnosti, krađa identiteta, phishing - e-mail
Game Based Cyber securty Training: are Serious Games suitable for cyber securty training?	M. Hendrix, A.Al-Sherbat, V. Bloom	- prepoznavanje krađe identiteta i neželjena e-pošta
Security Awareness of Compter users: A phishing threat avoidance perspective	N. Asanka Gamagedora Arachchilage	- phishing, krađa internetskog identiteta, korisničko ime i lozinka
Nacionalna strategija kibernetičke sigurnosti	Vlada Republike Hrvatske	- zaštita podataka, implementacija sadržaja o kibernetičkoj svijesti kao međupredmetni sadržaj na svim razinama obrazovanja
Nacionalna taksonomija računalno-sigurnosnih incidenata	Zavod za sigurnost informacijskih sustava	- širenje zlonamjernih virusa, spam – neželjena pošta, phishing
Perceived security and privacy of cloud computing applications used in educational ecosystem	T. Orehovački, D. Etinger, S.Babić	- cloud aplikacije, stvaranje, pohranjivanje, organiziranje i dijeljenje različitih sadržaja što rezultira velikim brojem korisnika istih te ih čini lakom metom za prijetnje vezane uz sigurnost i privatnost

		- prednosti i nedostatci aplikacija za cloud računalstvo te način kako zaštiti privatnost svojih korisnika
Cybersecurity Education in Universities	Fred B. Schneider	- obrazovanje nastavnika i kadra za računalnu sigurnost ključna je za izgradnju pouzdanih sustava
Nacionalno istraživanje o sigurnosti djece na internetu – EU Kids online	Ciboci, L., Ćosić Pregrad, I., Kanižaj, I., Potočnik, D., Vinković, D.	- prednosti i rizici korištenja interneta među djecom raste u dobi od 9 do 14 godina - većina djece ima pristup internetu kada god to želi - količina vremena koju djeca provode na internetu raste s dobi djeteta - djeca pristupaju internetu svaki dan - vrijeme provode na društvenim mrežama i igranju igrica - korištenje društvenih mreža raste s dobi djeteta
Istraživanje i korištenju interneta, mobitela i drugih tehnologija	Poliklinika za zaštitu djece i mladih Grada Zagreba i Hrabri telefon	- 91% djece izjašnjavaju se kao korisnici interneta - 31% djece navodi da ima više od jedne e-mail adrese - 7% djece i mladih navodi da je zloupotrebljavalo nečije ime i prezime i objavilo tuđe privatne stvari na internetu
Teens, Social Media and Privacy	M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, M. Beaton	- djeca i mladi dijele na internetu svoje osobne podatke - 60% profila na društvenim mrežama su privatna - većina djece i mladih navode da znaju upravljati svojim postavkama privatnosti
Istraživanje o iskustvima i ponašanjima djece na internetu i društvenoj mreži Facebook	Poliklinika za zaštitu djece i mladih Grada Zagreba	- 99% djece ima pristup internetu kod kuće ili u školi - 63% djece navodi da im je profil vidljiv samo osobama koje poznaju - 8% ima otvoren profil vidljiv svima

		- 12% sudionika nije sigurno kome je sve vidljiv profil - svako šesto dijete izjavljuje da uopće ne brine o sigurnosti svog profila
Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: Navike Facebook generacije	Siniša Kušić	- 51% učenika navodi da nije pročitalo „Izjavu o pravima i odgovornostima“ prije otvaranja profila - 37% učenika ima otvoren profil iako znaju da krše dobnu granicu kreiranja profila
Inspecting Quality of Games Designed for Learning Programming	Tihomir Orehovački, Snježana Babić	- 56,01 % sudionika igra računalne igrice barem jednom tjedno - 54, 86% provode između jednog i tri sata tjedno na igrajući igrice - 36, 57% učenika provodi manje od sat vremena u interakciji na mobilnim igricama - 20, 58% ispitanika svakodnevno igra računalne i mobilne igrice
The Importance of Cybersecurity Education in School	Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F.	- škole moraju postati centri znanja za razvoj i podizanje svijesti o cyber sigurnosti za zajednicu - nastavnici trebaju organizirati aktivnosti ili školske programe cyber sigurnosti

Izvor: autorica rada temeljem dosadašnjih istraživanja i rezultatima istih

Dosadašnja istraživanja potvrđuju činjenicu da su djeca i mladi svakodnevni korisnici interneta te kako njihovo korištenje digitalnih tehnologija raste s dobi. Djeca i mladi se najčešće služe internetom kako bi igrali igrice te komunikaciju pri tome ne razmišljajući o zaštiti svojih računala. Stoga je iznimno važno, prema provedenim istraživanjima, osposobiti prije svega učitelje i nastavnike kako bi škole postale mjesta gdje će se podizati svijest o važnosti kibernetičke sigurnosti.

8. PRIMJENA HARDVERSKE I SOFTVERSKE ZAŠTITE OSOBNIH PODATAKA PRI KORIŠTENJU INTERNETA NA PRIMJERU UČENIKA OSNOVNOŠKOLSKOG UZRASTA

8.1. Metodologija istraživanja

U ovome je poglavlju definiran i opisan cilj istraživanja, predstavljen problem istraživanja, opisani ispitanici koji su sudjelovali u istraživanju, opisan način prikupljanja podataka te su na kraju rada predstavljeni rezultati provedenog istraživanja.

8.1.1. Cilj i metode istraživanja

O sigurnosti djece na internetu, u doba kada je internet pristan u svim društvenim sferama i životnim fazama razvoja pojedinca, vrlo je važno poučavati djecu i mlade kako se zaštiti na internetu. Često se govori o temi zaštite osobnih podataka i načinima kako se zaštiti kada do zlouporabe istih dođe, no vrlo je važno znati načine kako spriječiti i kako se zaštiti da do toga niti ne dođe. Većina istraživanja pristupa ovoj temi sa socio-društvenog te pedagoško-psihološkog aspekta, ovim istraživanjem želi se ispitati kako i koje oblike softverske i hardverske zaštite ispitanici primjenjuju.

Cilj je ovoga istraživanja ispitati na koji način i u kojoj mjeri učenici osnovnoškolske dobi upotrebljavaju softversku i hardversku zaštitu prilikom korištenja interneta. Istraživanje je provedeno u osnovnoj školi, a sudjelovali su učenici petih, šestih razreda te učenici sedmih i osmih razreda kojima je informatika izborni predmet.

8.1.2. Anketni upitnik i postupak prikupljanje podataka

Za empirijski dio istraživanja sastavljen je anketni upitnik. Anketni upitnik izrađen je u Google alatu – Google obrasci, Forms. Istraživanje je provedeno u razdoblju od 23. svibnja do 3. lipnja 2022. godine. Anketni upitnik proveden je u digitalnom obliku, link za pristup (https://forms.gle/X512AUCnns8rNfZM7).

Ključni činitelji na temelju kojih su sastavljena pitanja anketnog upitnika pronađeni su u Kurikulumu nastavnog predmeta Informatika za osnovne i srednje škole. Anketni

upitnik sadržava devetnaest pitanja. Postavljena pitanja su zatvorenog tipa te pitanja višestrukog izbora. Prva dva pitanja odnose se na podatke o sudionicima te se ubrajaju u skupinu sociodemografskih pitanja, ostala pitanja odnose na mjere i načine hardverske i softverske zaštite računala ispitanika te načine korištenja digitalnih uređaja i interneta.

Istraživanju su pristupili učenici petih, šestih, sedmih i osmih razreda osnovne škole. Istraživanje je provedeno anonimno, bez rizika korištenja i objave osobnih podataka ispitanika. Provedeno je na satu nastave Informatike, osobnim dolaskom na iste. Učenicima je link za pristup anketnom listiću proslijeđen na osobne mail adrese, nakon čega su pristupili rješavanju ankete. Predviđeno vrijeme rješavanja anketnog listića je 15 minuta, a anketnom listiću pristupilo je 159 učenika.

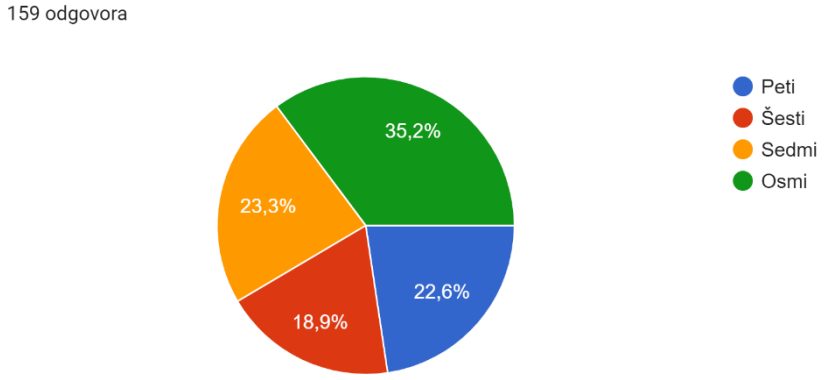
8.1.3. Sudionici istraživanja

Osnovne škole u kojima je provedeno istraživanje su: Osnovna škola „Antun Matija Reljković“, Bebrina te Osnovna škola „Antun Mihanović“, Slavonski Brod. Primjer dozvale za provedbu istraživanja u osnovnoj školi priložen je u nastavku rada (Prilog 2).

Prije provedbe istraživanja ispitani su nastavnici, razrednici učenika koji su sudjelovali u istraživanju, na koji način upoznavaju učenike o sigurnosti djece na internetu te koje mjere poduzimaju kako bi podigli svijest o potrebi hardverske i softverske zaštite računala prilikom korištenja interneta. Zaključak provedenog razgovora je da nastavnici na satu razrednika kroz različite radionice učenike upoznavaju o opasnostima na koje mogu naići koristeći internet, naglasak je prije svega stavljen na socio-društveni aspekt. Učenici u vrlo maloj mjeri, samo tijekom nastave Informatike uče o pojmovima hardverska i softverska zaštita, što potvrđuju i teme zastupljene u Kurikulumu nastavnog predmeta Informatika za osnovne i srednje škole. U istraživanju primjene hardverske i softverske zaštite digitalnih uređaja pri korištenju interneta sudjelovalo je 159 učenika petih, šestih, sedmih i osmih razreda osnovne škole. Učenici su anonimno i dobrovoljno pristupali anketnom listiću u razdoblju od 23. svibnja do 3. lipnja 2022. godine.

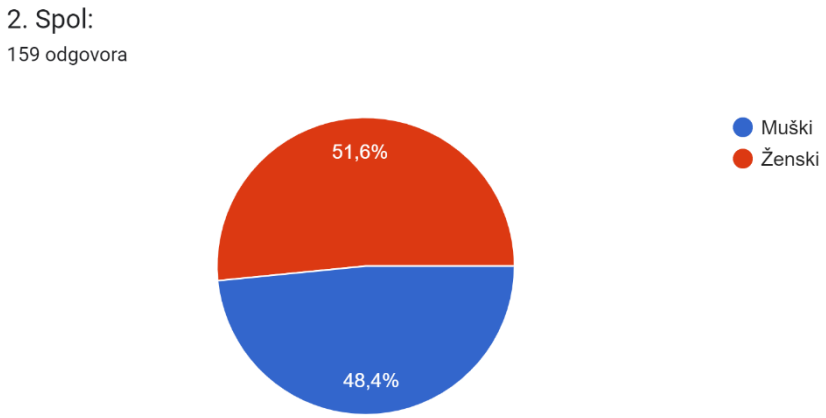
Od ukupno 159 ispitanika, njih 36 (22,6 %) učenici su petog razreda osnovne škole, 30 (18,9 %) učenici su šestog razreda osnovne škole, 37 (23,3 %) učenici su sedmog

razreda osnovne škole te njih 56 (35,2 %) učenici su osmog razreda osnove škole. Na Grafikonu 1. prikazan je postotak ispitanika obzirom na razred koji pohađaju.



Grafikon 1. Prikaz postotka ispitanika obzirom na razred koji pohađaju (Izvor: autorica rada)

Grafikon 2. prikazuje postotak zastupljenosti ispitanika muškog i ženskog spola. Sudjelovalo je 82 (51,6 %) ispitanika ženskog spola te 77 (48,4 %) ispitanika muškog spola.



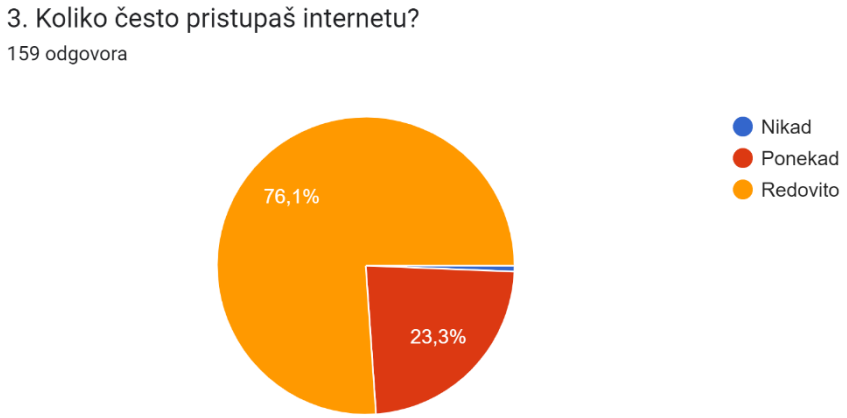
Grafikon 2. Prikaz postotka ispitanika s obzirom na spol (Izvor: autorica rada)

8.2. Rezultati istraživanja

Ispitivanju je pristupilo 159 učenika. U nastavku slijedi prikaz rezultata istraživanja.

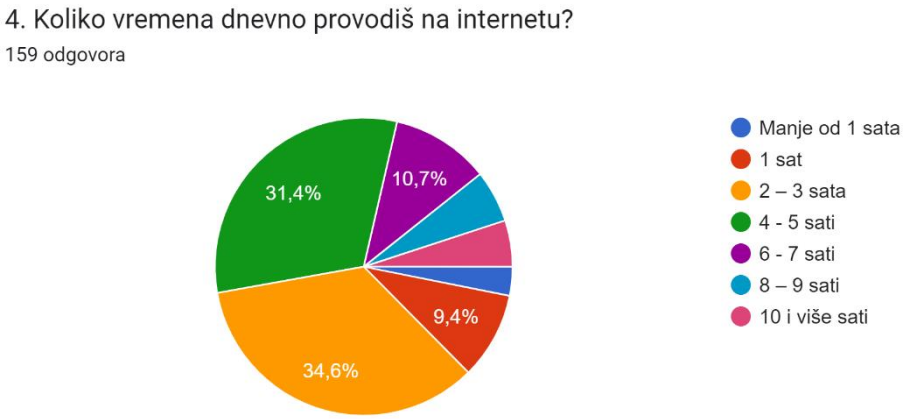
8.2.1. Rezultati ispitanika o načinu korištenja digitalnih uređaja i interneta

Treći grafikon jasno pokazuje i potvrđuje tezu da je internet prisutan u svim životnim fazama pojedinca pa tako i učenika osnovne škole. Samo jedan ispitanik (0,6 %) od 159 ispitanika nije nikada pristupio internetu, dok 121 (76,1 %) ispitanik, što je većinski dio, redovito pristupa i koristi internet. 37 (23,3 %) ispitanika ponekad pristupa internetu.



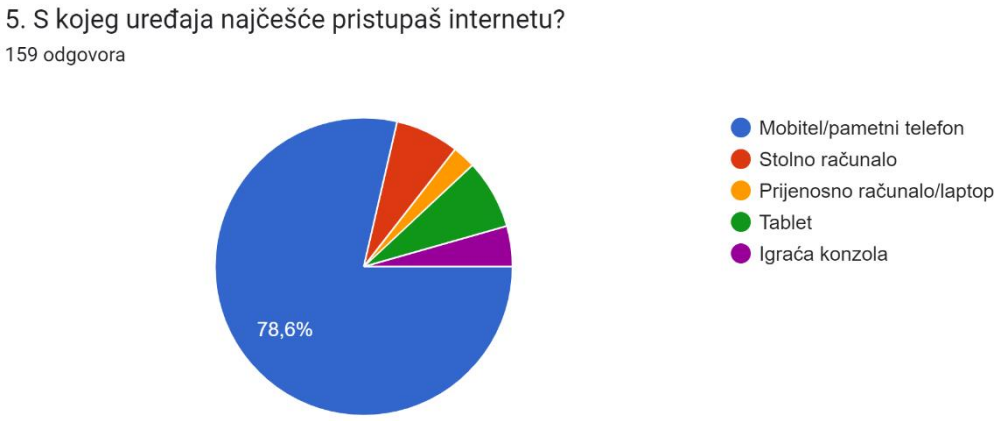
Grafikon 3. Prikaz postotka učestalosti pristupa ispitanika internetu (Izvor: autorica rada)

S obzirom na prisutnost interneta u svakodnevnom životu, od iznimne je važnosti pokazatelj koliko vremena dnevno ispitanici provode na internetu. Grafikon 4. prikazuje da u podjednakom postotku ispitanici provode na internetu 2-3 sata ili 4-5 sati. Od 159 ispitanika njih 55 (34,6 %) provode na internetu 2-3 sata dnevno, 50 ispitanika (31,4 %) dnevno provode na internetu 4-5 sati. 6-7 sati dnevno na internetu provodi 17 (10,7 %) ispitanika, njih 15 (9,4 %) ispitanika provodi manje od sat, 9 ispitanika (5,7 %) 8-9 sati, a najmanji broj ispitanika 8 (5 %) provodi 10 i više sati dnevno na internetu.



Grafikon 4. Prikaz postotka vremena koje ispitanici provode na internetu(Izvor: autorica rada)

U petom pitanju jasan je pokazatelj da većina učenika osnovnoškolske dobi posjeduje vlastiti mobitel/pametni telefon s pristupom internetu. Njih 125 (78,6 %) ispitanika pristupa internetu putem mobitela/pametnog telefon, 12 ispitanika (7,5 %) putem tableta, 11 (6,9 %) ispitanika pristupa internetu stolnim računalom, igraćom konzolom njih 7 (4,4 %) te njih 4 (2,5 %) pristupa internetu s prijenosnog računala/laptopa.



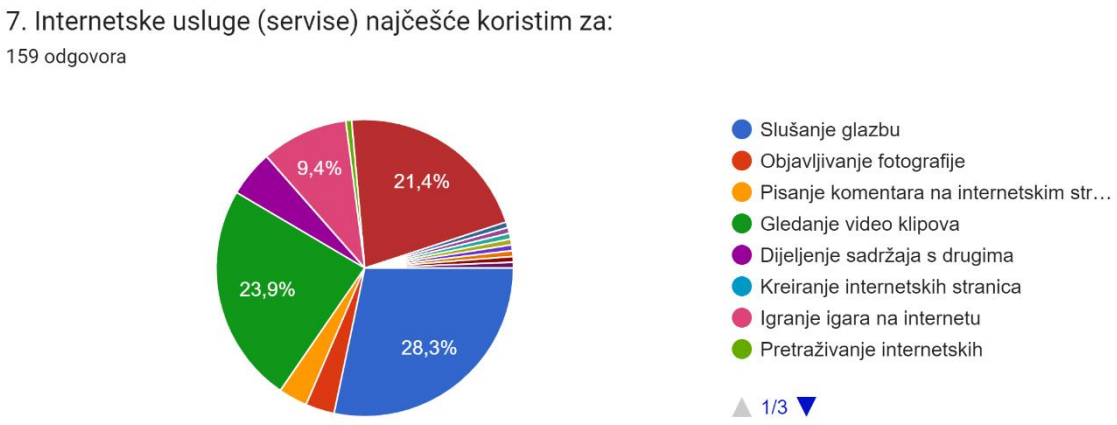
Grafikon 5. Prikaz postotka uređaja kojima ispitanici pristupaju internetu (Izvor: autorica rada)

Bez obzira što je većina ispitanika s područja posebne državne skrbi, Grafikon 6. prikazuje da 150 (94,3 %) ispitanika od ukupno 159 posjeduje vlastiti uređaj s kojim

pristupaju internetu, dok njih 9 (5,7 %) ne posjeduje vlastiti uređaj s kojim pristupaju internetu.

Grafikon 6. Prikaz postotka vlastitog uređaja s kojeg ispitanici pristupaju internetu (Izvor: autorica rada)

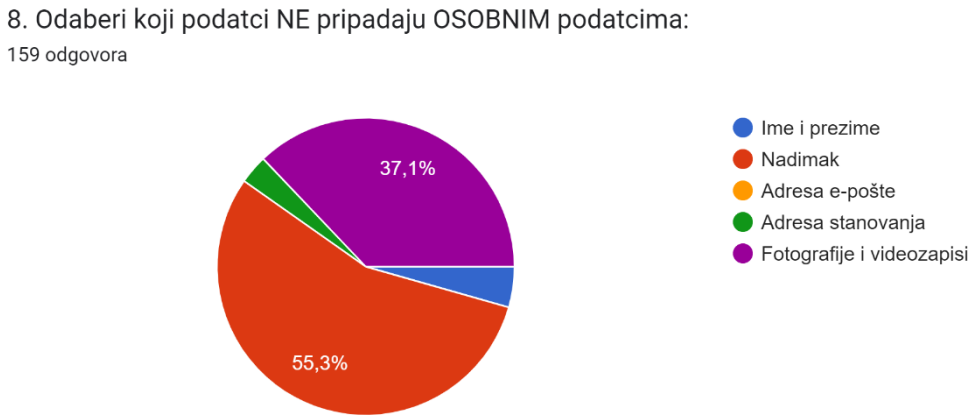
Najveći broj ispitanika njih 45 (28,3 %) najčešće koristi internet za slušanje glazbe, njih 39,9 % svakodnevno koristi internet za slušanje glazbe. Na drugom mjestu je zastupljeno gledanje video klipova, 38 ispitanika (23,9 %). Njih 34 (21,4 %) ispitanika koristi internetske usluge kako bi pristupili društvenim mrežama. 15 (9,4 %) ispitanika od ukupno 159 koristi internetske usluge za igranje igara na internetu. Ostale aktivnosti poput objavljivanja sadržaja, Instagram, pisanje komentara na internetskim stranicama, dijeljenje sadržaja s drugima, kreiranje internetskih stranica, pretraživanje internetskih stranica su zanemarive.



Grafikon 7. Prikaz postotka aktivnosti ispitanika za koje koriste internetske usluge (Izvor: autorica rada)

8.2.2. Rezultati ispitanika o poznavanju zaštite osobnih podataka i sigurnom digitalnom okruženju

Ovim pitanjem provjeravala se opća informatička pismenost ispitanika osnovnoškolske dobe kojima je informatika izborni predmet (sedmi i osmi razred osnovne škole). Od 159 ispitanika njih 88 (55,3 %) navodi točan odgovor, dok 71 ispitanika (44,7 %) navodi netočan odgovor na postavljeno pitanje.



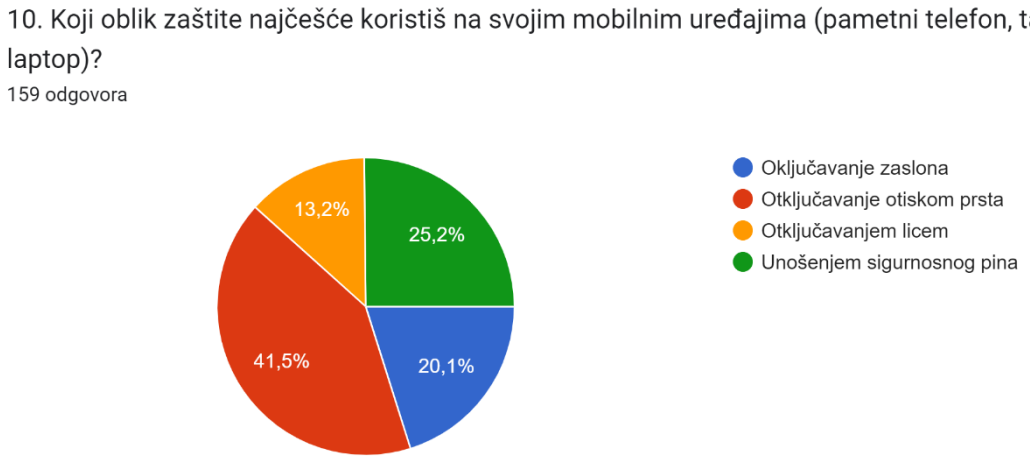
Grafikon 8. Prikaz postotka ispitanika koji prepoznaju osobne podatke (Izvor: autorica rada)

Grafikon 9. prikazuje postotak ispitanika koji ispravno prepoznaju adresu web stranica koja je sigurna za pretraživanje i preuzimanje dokumenata. Njih 93 (58,5 %) ispitanika na postavljeno je pitanje ponudilo ispravan odgovor, dok je njih 66 (41,5 %) na postavljeno pitanje dalo neispravan odgovor.

Grafikon 9. prikaz postotka ispitanika koji ispravno prepoznaju adresu web stranica koja je sigurna za pretraživanje i preuzimanje dokumenata (Izvor: autorica rada)

8.2.3. Rezultati ispitanika o hardverskoj zaštiti digitalnih uređaja

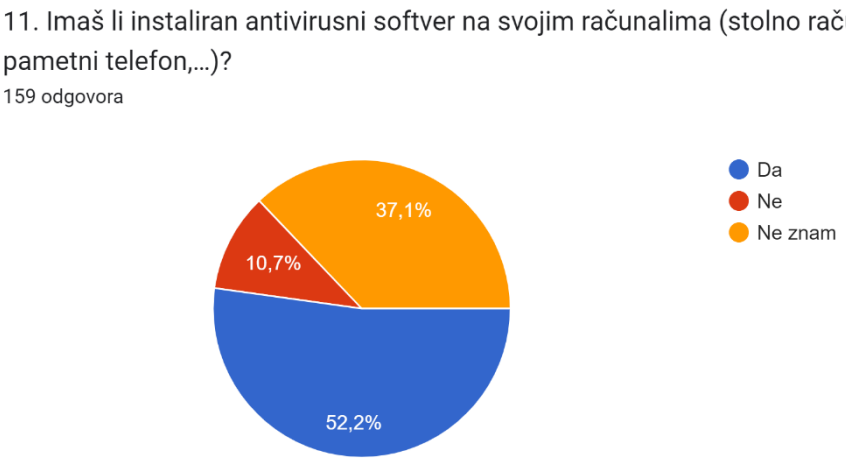
U desetom pitanju ispitivao se koji oblik hardverske zaštite koriste ispitanici na svojim mobilnim uređajima. Njih 66 (41,5 %) koristi otključavanje otiskom prsta, 40 (25,2 %) koristi unos sigurnosnog pina, njih 32 (20,1 %) otključavanje zaslona dok njih 21 (13,2 %) koristi otključavanje licem.



Grafikon 10. Prikaz postotka oblika hardverske zaštite koriste ispitanici na svojim mobilnim uređajima (Izvor: autorica rada)

8.2.4. Rezultati ispitanika o softverskoj zaštiti osobnih podataka pri korištenju interneta

Grafikon 11. prikazuje u kojoj mjeri ispitanici koriste programsku zaštitu na svojim računalima. 83 ispitanika (52,2 %) ispitanika potvrdilo je da posjeduje antivirusni softver na svojima računalima, 17 (10,7 %) nema instaliran antivirusni program, dok se 59 ispitanika (37,1 %) ispitanika ne zna ima li instaliran antivirusni program na svojim računalima, što dovodi do zaključka da je razina znanja o softverskoj zaštiti učenika osnovnoškolske dobi na nižoj razini.



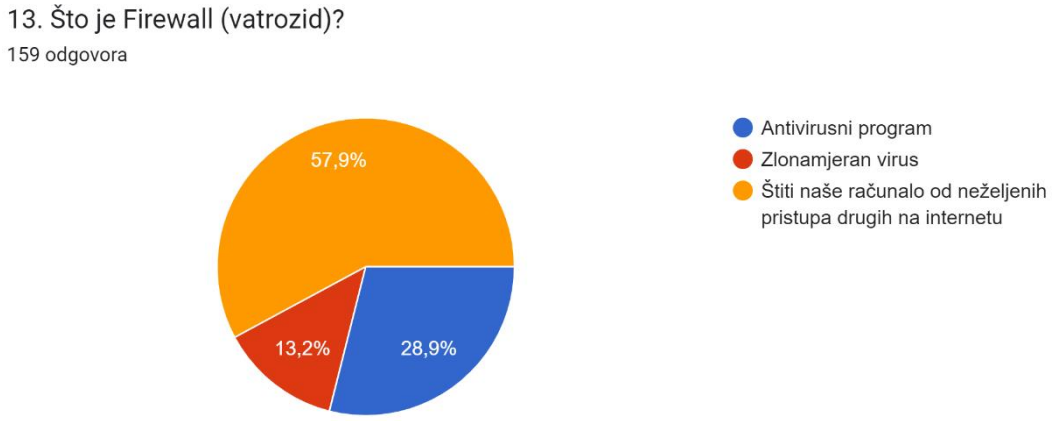
Grafikon 11. Prikaz postotka ispitanika u kojoj mjeri koriste programsku zaštitu na svojim računalima (Izvor: autorica rada)

U dvanaestom pitanju provjeravala se zastupljenost mišljenja ispitanika o važnosti softverske zaštite računala. 135 (84,9 %) ispitanika od ukupno 159 smatra da je antivirusne programe potrebno redovito ažurirati/nadograđivati, dok njih 24 (15,1 %) ispitanika smatra da isto nije potrebno.

Grafikon 12. Prikaz postotka mišljenja ispitanika o programskoj zaštiti (Izvor: autorica rada)

Kroz trinaesto pitanje provjeravao se oblik softverske zaštite digitalnih uređaja, poznaju li ispitanici na koji se način mogu zaštiti digitalni uređaji. Grafikon 13. pokazuje da 92 ispitanika (57,9 %) od ukupno 159 ispitanika primjenjuje i poznaje način na koji

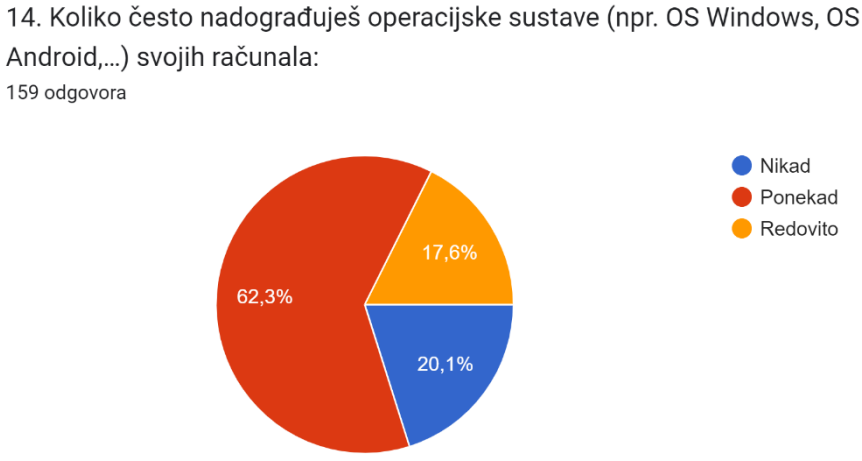
se računalo štiti od neželjenih pristupa na internetu dok je njih 67 (42,1 %) dalo netočan odgovor na postavljeno pitanje.



Grafikon 13. Prikaz postotka poznavanja ispitanika o obliku softverske zaštite računala (Izvor: autorica rada)

8.2.5. Rezultati ispitanika o sigurnosti operacijskih sustava digitalnih uređaja

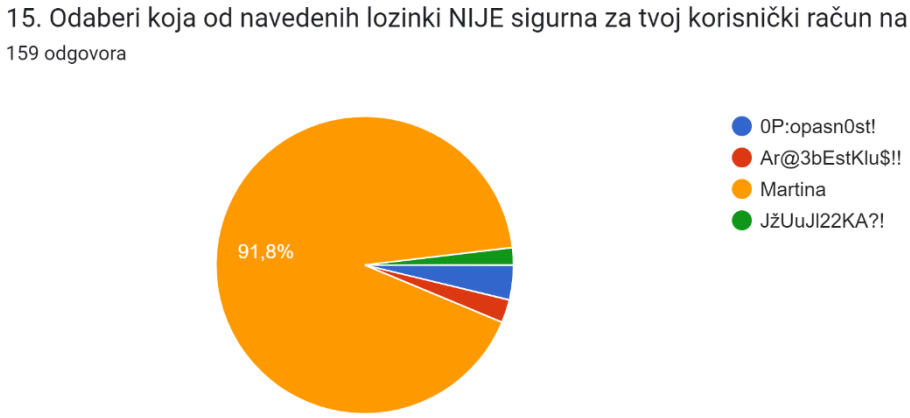
Nadalje, kroz anketni upitnik, u četrnaestom pitanju ispitivala se važnost nadogradnje operacijskih sustava računala. 99 (62,3 %) ispitanika potvrdilo je da svoje operacijske sustave ponekad nadograđuju iz čega se može zaključiti da nadogradnji operacijskih sustava ne pridaju osobitu važnost, njih 32 (20,1 %) isto ne čini nikada dok njih 28 (17,6 %) isto čini redovito.



Grafikon 14. Prikaz postotka koliko često ispitanici nadograđuju operacijske sustave svojih računala (Izvor: autorica rada)

8.2.6. Rezultati ispitanika o zaštiti korisničkih računa na internatskim stranicama i aplikacijama

U petnaestom pitanju provjeravao se oblik zaštite osobnih podataka , znaju li prepoznati te na taj način i sami stvoriti jaku lozinku svojih korisničkih računa. 146 ispitanika (91,8 %) točno je odgovorilo iz čega se može zaključiti, unatoč tome da je Informatika izborni predmet (sedmi i osmi razred osnovne škole), da ispitanici znaju prepoznati koja lozinka nije sigurna za kreiranje korisničkih računa. Njih 13 (8,2 %) netočno je odgovorilo na postavljeno pitanje.

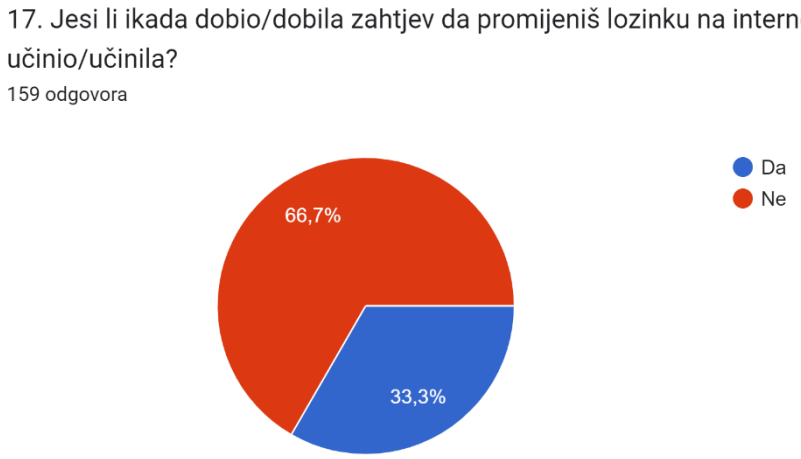


Grafikon 15. Prikaz postotka ispitanika koji prepoznaju sigurne lozinke za kreiranje korisničkih računa (Izvor: autorica rada)

Grafikon 16. prikazuje koliko često ispitanici mijenjaju lozinke svojih korisničkih računa. 77 (48,4 %) ispitanika izjasnilo se da isto radi ponekad, 63 (39,6 %) nikada dok njih 19 (11,9 %) redovito mijenja lozinku svojih korisničkih računa.

Grafikon 16. Prikaz postotka koliko često ispitanici mijenjaju lozinke svojih korisničkih računa (Izvor: autorica rada)

Kroz anketni upitnik ispitivalo se jesu li ispitanici ikada bili izloženi nekom od oblika zlouporabe njihovih korisničkih računa, 106 (66,7 %) ispitanika od ukupno 159 nije nikada dobilo zahtjev za promjenu lozinke na internetskoj stranici dok je njih 53 (33,3 %) potvrdilo da su bili izloženi nekom od oblika zlouporabe njihovih osobnih podataka.



Grafikon 17. Prikaz postotka ispitanika koji su dobili zahtjev za promjenom lozinke na internetskim stranicama na kojima imaju kreiran korisnički račun (Izvor: autorica rada)

Rezultati dobiveni u osamnaestom pitanju prikazani su u Tablici 3.. Ispitanici su odabirali u kojoj se mjeri navedene tvrdnje odnose na njih, navedenim tvrdnjama ispitivalo se u kojoj su mjeri i na koji način bili izloženi nekom od oblika kibernetičkih napada te na koji način štite svoje korisničke račune prilikom korištenja interneta. Njih 48 (30,1 %) redovito provjerava adresu pošiljatelja prije otvaranja e-pošte, njih 71 (44,6 %) isto čini redovito dok njih 40 (25,1 %) isto ne čini nikada iz čega se može zaključiti da većina ispitanika osnovnoškolske dobi brine o sigurnosti svojih osobnih podataka. 51 (32,2 %) ispitanika navodi da redovito čita „Izjavu o pravima i odgovornosti“ prilikom kreiranja korisničkih računa na internetskim stranicama, njih 58 (36,4 %) isto čini ponekad, njih 50 (31,4 %) nikada.

Sljedeća se tvrdnja odnosila na phishing kao jedan od oblika kibernetičkih napada, 108 (67,9 %) ispitanika izjasnilo se da nikada ne unosi lozinku na mrežne stranice slijedeći poveznice od nepoznatih pošiljatelja, njih 31 (19, 4 %) isto čini ponekad te njih 20 (12,5 %) isto čini redovito, većina ispitanika, dakle, štiti svoje osobne podatke te ih ne dijeli s nepoznatim osobama.

Posljednja se tvrdnja odnosi na informacije o postavkama privatnosti prilikom pristupanja aplikacijama i internetskim stranicama. 52 ispitanika (32,7 %) redovito čita informacije o postavkama privatnosti, 65 (40,8 %) isto čini ponekad te 42 (26, 4 %) isto ne čini nikada.

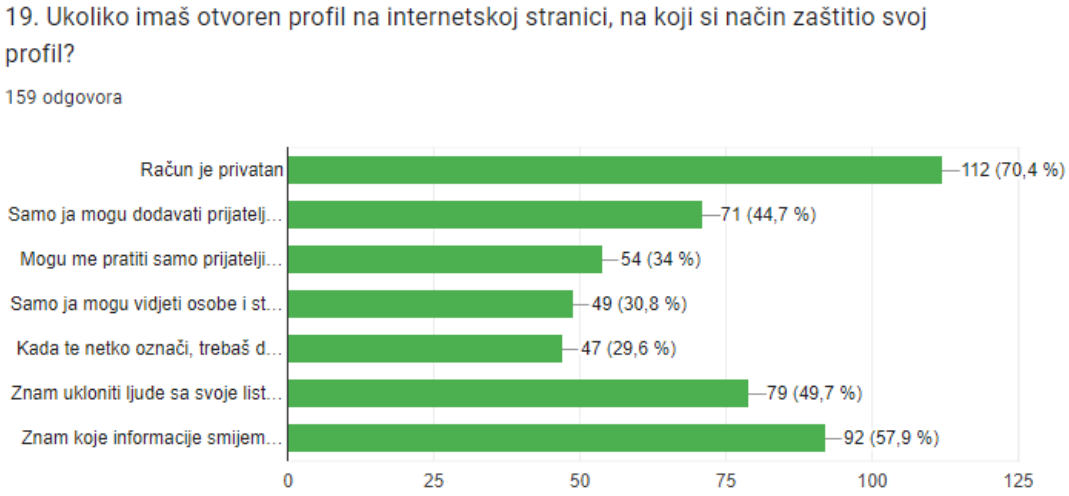
Tablica 4. Prikaz postotka ispitanika o navedenim tvrdnjama

Tvrdnje	**Ispitanici**		
	Nikada	Ponekad	Redovito
Kada sam u mogućnosti uvijek provjeravam adresu pošiljatelja prije otvaranja moje e-pošte.	40 (25,1 %)	71 (44,6 %)	48 (30,1 %)
Na internetskim stranicama na kojima kreiram svoj profil, najprije uvijek pročitam „Izjavu o pravima i odgovornosti“.	50 (31,4 %)	58 (36,4 %)	51 (32,2 %)
Unosim svoju lozinku na mrežnu stranicu slijedeći poveznicu koju sam dobio/dobila e-poštom od nepoznatog pošiljatelja.	108 (67,9 %)	31 (19,4 %)	20 (12,5 %)
Gotovo uvijek čitam informacije o postavkama privatnosti kada pristupam aplikacijama i stranicama na internetu.	42 (26,4 %)	65 (40,8 %)	52 (32,7 %)

(Izvor: autorica rada)

Nadalje, u devetnaestom pitanju provjeravalo se na koji su način ispitanici zaštitili svoj profil na internetskoj stranici. Njih 112 (70,4 %) imaju kreiran, privatan račun na internetskim stranicama, 92 (57,9 %) ispitanika zna koje informacije smiju dijeliti na internetu, 79 (49,7 %) znaju ukloniti ljude sa svojih lista pratitelja, 71 (44,7 %) ispitanika imaju uključenu mogućnost odabira prijatelja na vlastite liste prijatelja, njih 54 (34 %) imaju mogućnost da samo oni mogu dodavati prijatelje na svoje liste prijatelja, 49 (30,8 %) ispitanika su uključili mogućnost da samo oni mogu vidjeti osobe i stranice koje

prate na internetskim stranicama dok njih 47 (29,6 %) u postavkama privatnosti uključili su opciju dopuštenja da se nešto objavi na njihovim profilima od strane drugih osoba.



Grafikon 18. Prikaz postotka načina na koji su ispitanici zaštitili profil na internetskim stranicama (Izvor: autorica rada)

9. ZAKLJUČAK

Za izradu diplomskog rada izrađen je i proveden anketni upitnik. Anketni upitnik proveden je u dvije osnovne škole, na području grada Slavonskog Broda te na području općine Bebrina, a u njemu je sudjelovalo ukupno 159 učenika petih, šestih, sedmih i osmih razreda osnovne škole. Analizom rezultata istraživanja zaključilo se da je opća informatička razina učenika na nižoj razini i da se uvelike mora učenike učiti i podizati svijest o važnosti kibernetičke sigurnosti prilikom korištenja interneta.

Internet je danas prisutan u svim sferama društva kao i razvojnim fazama pojedinca što potvrđuje i provedena anketa. Njih 76,1 % ispitanika, većinski dio, potvrđuje da redovito pristupa internetu. 34,6 % ispitanika provodi na internetu 2-3 sata dnevno, što je u granicama tolerancije što potvrđuje istraživanje EUKidsOnline iz 2020. godine provedeno na razini Republike Hrvatske, 31,4 % dnevno provode na internetu 4-5 sati, što je zabrinjavajući podatak uz ostale dnevne obveze ispitanika koji su osnovnoškolske dobi. 6-7 sati dnevno na internetu provodi 10,7 % ispitanika, 9,4 % ispitanika provodi manje od sat, 5,7 % 8-9 sati, a najmanji broj ispitanika 5 % provodi 10 i više sati dnevno na internetu.

U usporedbi s istraživanjem EUKidsOnline iz 2020. godine provedenim na nacionalnoj razini uočava se da rezultati provedenog istraživanja odgovaraju rezultatima nacionalnog istraživanja. Tako najveći broj ispitanika 28,3 % najčešće koristi internet za slušanje glazbe, što odgovara rezultatima nacionalnog istraživanja prema kojem najveći postotak ispitanika, njih 39,9 % svakodnevno koristi internet za slušanje glazbe. Na drugom mjestu u oba istraživanja zastupljeno je gledanje video klipova, 23,9 %, a u nacionalnom istraživanju 33,4 %. 21,4 % ispitanika koristi internetske usluge kako bi pristupili društvenim mrežama, dok ova teza nije ispitana u nacionalnom istraživanju. Iznenađuje činjenica 9,4 % ispitanika od ukupno 159 koristi internetske usluge za igranje igara na internetu, dok na nacionalnoj razini postotak je veći te iznosi 26,5 %. Ostale aktivnosti poput objavljivanja sadržaja, Instagram, pisanje komentara na internetskim stranicama, dijeljenje sadržaja s drugima, kreiranje internetskih stranica, pretraživanje internetskih stranica su zanemarive.

Anketnim upitnikom provjeravala se opća informatička pismenost učenika osnovnoškolske dobi. Na pitanje o osobnim podatcima, što pripada osobnim podatcima, 55,3% ispitanika navodi točan odgovor što dovodi do zaključka da je opća informatička pismenost učenika na nižoj razini. Ta činjenica potvrđena je i u nastavku

analize istraživanja, 58,5 % ispitanika zna prepoznati adresu web stranice koja je sigurna za pretraživanje i preuzimanje dokumenta.

Analizom rezultata istraživanja utvrđena je i razina hardverske i programske zaštite koju učenici osnovnoškolske dobi koriste na svojim računalima. Ispitanici koriste jedan od oblika hardverske zaštite na svojim mobilnim uređajima kako bi onemogućili nepoznatim osobama pristup svojim osobnim podatcima. 52,2 % ispitanika potvrdilo je da posjeduje antivirusni softver na svojim računalima dok njih 37,1 % ne zna ima li isti na svojim računalima. Ispitanici, njih 84,9 %, smatra da je antivirusne programe potrebno redovito ažurirati/nadograđivati. 57,9% ispitanika poznaje na koji se način računalo može štiti od neželjenih pristupa na internetu iz čega se može zaključiti da učenici osnovnoškolske dobi ne poznaju dovoljno načine i mjere hardverske i softverske zaštite svojih računala.

Iako se većina ispitanika izjašnjava da su redoviti korisnici interneta, analiza rezultata istraživanja potvrđuje činjenicu da učenici osnovnoškolske dobi nisu dovoljno upoznati o zaštiti svojih korisničkih računa na internetskim stranicama i aplikacijama. 39,6 % ispitanika izjasnilo je kako nikada ne mijenja lozinku svojih korisničkih računa unatoč činjenici da je njih čak 33,3 % ispitanika bilo izloženo nekom od oblika zlouporabe svojih osobnih podataka.

Nadalje, analiza rezultata istraživanja pokazuje da ispitanici štite svoje osobne podatke te ih ne dijele s nepoznatim osobama. 67,9 % ispitanika izjasnilo se da nikada ne unose lozinku sljedeći poveznicu koju su dobili od nepoznatih pošiljatelja, 30,1 % ispitanika redovito provjerava adresu pošiljatelja prilikom otvaranja e-pošte. Prije kreiranja profila na internetskim stranicama, 32,2 % ispitanika čita „Izjavu o pravima i odgovornosti“, dok njih 32,7 % čita informacije o postavkama privatnosti kada pristupa aplikacijama i internetskim stranicama.

Dakle, unatoč tome, što većina ispitanika osnovnoškolske dobi poznaje i brine o zaštiti svojih osobnih podataka prilikom korištenja internata, važno je istaknuti da je, obzirom na dobivene rezultate, potrebno podizati svijest te educirati učenike osnovnoškolske dobi o kibernetičkoj sigurnosti.

Provedeno istraživanje jasan je pokazatelj da je opća informatička pismenost kao i razina poznavanja načina i mjera hardverske i softverske zaštite računala učenika osnovnoškolske dobi na nižoj razini stoga je važno uvesti informatiku kao obvezan nastavni predmet u sve razrede osnovne škole, od prvoga do osmoga razreda osnovne škole.

LITERATURA

Članci, istraživanja, internetski izvori:

- Agencija za zaštitu osobnih podataka: *Što je krađa identiteta?,* URL: https://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi
- Alton, L. (2017): *The 4 Most Secure Forms of Online Communication*, Isaca.org, URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/the-4-most-secure-forms-of-online-communication
- A. Ramakić, Z. Bundalo (2013.), *Softversko-hardverska zaštita podatka u računarskim sistemima*,URL: https://tfb.ba/repozitorij/2/RIM/RIM2013/rim2013_057%20C%20-%20101%20-%20Ramakic%20Adnan_pdf_59.pdf
- Asanka Gamagedora Arachchilage N. (2014.): *Security Awareness of Compter users: A phishing threat avoidance perspective*, URL: https://www.sciencedirect.com/science/article/abs/pii/S0747563214003331
- Aufderheide, P. (1993): *A Report of the National Leadership Conference on Media Literacy*.Maryland. Washington, D.C.: The Aspen Institute, URL: https://files.eric.ed.gov/fulltext/ED365294.pdf
- Azop.hr: *Djelatnost agencije*, URL: https://azop.hr/djelatnost-agencije
- Azop.hr: *Djelatnosti i ustrojstvo agencije*, URL: http://azop.hr/djelatnost-agencije
- CARNet (2010): *Napredne tehnike socijalnog inženjeringa NCERT-PUBDOC-2010-02-292*, URL: https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-02-292.pdf
- Carnet.hr: *Sigurnost na internetu*, URL: https://www.carnet.hr/wp-content/uploads/2019/09/Sigurnost-na-Internetu-1.pdf
- Carnet.hr (2004.), *Sustav za prevenciju neovlaštenog pristupa*, URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-08-86.pdf
- Cert.hr (2016.): *Mali pojmovnik kibernetičke sigurnosti*, URL: https://www.cert.hr/wp-content/uploads/2009/07/Pojmovnik.pdf
- Ciboci, L., Ćosić Pregrad, I., Kanižaj, I., Potočnik, D., Vinković, D. (2020.): *Nacionalno istraživanje o sigurnosti djece na internetu – EU Kids online*, URL: http://hrkids.online/prez/EUKidsOnlineHRfinal.pdf
- Cis.hr (2011.), *Zaštita mreže – vatrozid*, URL: https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html
- Družin, I. (2018): *Zaštita osobnih podataka u informacijskom društvu* [završni rad]. Zagreb: Sveučilište u Zagrebu, URL: http://darhiv.ffzg.unizg.hr/id/eprint/10579/1/Druzin_zavrsni.pdf?fbclid=IwAR0mBsOjaAUI24C7XRc4Jfwnxj0CFTJXnKFQ_A3E5UwOJaPPWHyEZ7w9yII

- eBizMBA (2017): Top 15 most popular social networking sites, URL: http://www.ebizmba.com/articles/social-networking-websites
- Eduvizija.hr.: *Opasnosti na internetu*, URL: http://www.eduvizija.hr/portal/sadrzaj/opasnosti-na-internetu
- Element.hr: *Početak interneta i nastanak weba*, URL: https://element.hr/artikli/file/1259
- Enciklopedija.hr (2021.) Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, URL: https://www.enciklopedija.hr/natuknica.aspx?id=68380
- Europska komisija, *Što su osobni podaci?,* URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr
- Essau, C.A., Conradt,J. (2006): *Agresivnost u djece i mladeži*. Jastrebarsko: Naklada Slap
- Europski parlament: *Zaštita osobnih podataka*, URL: https://www.europarl.europa.eu/factsheets/en/home
- Filozofski fakultet Sveučilišta u Zagrebu: *Informatizacija i sociokulturni razvoj*, URL: http://dzs.ffzg.unizg.hr/text/Uvod%20u%20informacijske%20znanosti/pog11.htm
- Grbavac, J., Grbavac, V. (2014): „Pojava društvenih mreža kao globalnog komunikacijskog fenomena.“ *Media, culture and public relations* 5(2): 206.-219.
- Hakom.hr (2018): *06. veljače obilježava se Dan sigurnijeg interneta. Potpisana prva „Povelja o sigurnosti djece na internetu*. URL: https://www.hakom.hr/UserDocsImages/2018/dokumenti/Press%20release%20Potpisivanje%20Povelje%20o%20sigurnosti%20djece%20na%20internetu.pdf
- Hajdarović, M. (2006): *Povijesni razvoj interneta*. URL: http://povijest.net/2018/?p=2374
- Haralambos, M., Heald, R. (1989): *Uvod u sociologiju.* Zagreb: Globus
- Hendrix M., Al-Sherbat A., Bloom V. (2016*.): Game Based Cyber securty Training: are Serious Games suitable for cyber securty training?*, URL: http://nectar.northampton.ac.uk/8279/7/Hendrix_etal_IJSG_2016_Game_based_cyber_security_training_are_serious_games_suitable_for_cyber_security_training.pdf
- Hodak Kodžoman, I., Velki, T. i Cakić, L. (2013): „Izloženost djece starije školske dobi elektroničkom nasilju.“ *Život i škola*; 30(59): 110-128.
- Hr.encyclopedia-titanica.com: *Značenje računalne sigurnosti (što je, pojam i definicija)*, URL: https://hr.encyclopedia-titanica.com/significado-de-seguridad-informtica
- Informatika.buzdo.com: *ECDL – European Computer Driving Licence*, URL: https://informatika.buzdo.com/pojmovi/ecdl.htm

- Jezikoslovac.com: *Informatizacija-značenje i definicija*, URL: https://jezikoslovac.com/word/ggu
- Kaportal.net.hr (2011): *Tko nije informatički pismen praktički je nepismen*, URL: https://kaportal.net.hr/nekategorizirano/3774035/tko-nije-informaticki-pismen-prakticki-je-nepismen-ecdl-u-kz-proslo-tristo-polaznika/
- Kaspersky.com (2022.): *What is Cyber Security?*, URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
- Kucaljudskihprava.hr (2019): *Privatnost kao ljudsko pravo*, URL: https://www.kucaljudskihprava.hr/2019/12/18/privatnost-kao-ljudsko-pravo/
- Leiner, B. M. et al. (2009): *Brief History of the Internet*. URL: https://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf
- Madden M., Lenhart A., Cortesi S., Gasser U., Duggan M., Smith A., Beaton M. (2013.): *Teens, Social Media and Privacy*, URL: https://assets.pewresearch.org/wp-content/uploads/sites/14/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf
- Ministarstvo za demografiju, obitelj, mlade i socijalnu politiku (2017): *Nacionalna strategija zaštite od nasilja u obitelji za razdoblje od 2017.do 2020. godine*. URL: https://mdomsp.gov.hr/UserDocsImages/Vijesti2017/Nacionalna%20strategija%20zastite%20od%20nasilja%20u%20obitelji%20za%20razdoblje%20do%202017.%20do%202022.%20godine.pdf
- Ministarstvo socijalne politike i mladih (2014*): Nacionalna strategija za prava djece u RH za razdoblje od 2014. – 2020. godine.*, URL: https://mdomsp.gov.hr/userdocsimages/arhiva/files/91286/NACIONALNA%20STRATEGIJA%20ZA%20PRAVA%20DJECE%20U%20RHZA%20RAZDOBLJE%20OD%202014.%20DO%202020.%20GODINE.pdf
- Ministarstvo obitelji, branitelja i međugeneracijske solidarnosti (2004): *Protokol o postupanju u slučajevima nasilja među djecom i mladima*. URL: https://mzo.gov.hr/UserDocsImages/dokumenti/Dokumenti-ZakonskiPodzakonski-Akti/Predskolski/Protokol%20o%20postupanju%20u%20slučaju%20nasilja%20među%20djecom%20i%20mladima%20-%20Ministarstvo%20za%20demografiju,%20obitelj,%20mlade%20i%20socijalnu%20politiku.pdf
- Mup.gov.hr (2015.) *Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Strategije*, URL: https://mup.gov.hr/UserDocsImages//dokumenti/kiberneticka_sigurnost//Sa%C5%BEetak%20Nacionalne%20strategije%20kiberneti%C4%8Dke%20sigurnosti.pdf
- MUP KS: *Zaštitimo se od cyber kriminala*, URL: http://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala

- Orehovački T., Babić S. (2015.): *Inspecting Quality of Games Designed for Learning Programming*, URL: https://link.springer.com/chapter/10.1007/978-3-319-20609-7_58
- Orehovački T., Etinger D., Babić S. (2017.): *Perceived security and privacy of cloud computing applications used in educational ecosystem*, URL: https://ieeexplore.ieee.org/abstract/document/7973516
- Ortega, R., Mora – Merchan, J., Jäger, T. (2007): „Acting against school bullying and violence“. *The role of media, local authorities and the Internet,* URL: https://iamnotscared.pixel-online.org/data/database/publications/618_Acting_against_school_bullying_and_violence.pdf
- Poliklinika za zaštitu djece i mladih Grada Zagreba (2014.): *Istraživanje o iskustvima i ponašanjima djece na internetu i društvenoj mreži Facebook*, URL: https://www.poliklinika-djeca.hr/istrazivanja/istrazivanje-o-iskustvima-i-ponasanjima-djece-na-internetu-i-na-drustvenoj-mrezi-facebook-2/
- Poliklinika za zaštitu djece i mladih Grada Zagreba i Hrabri telefon (2010.): *Istraživanje i korištenju interneta, mobitela i drugih tehnologija*, URL: https://www.poliklinika-djeca.hr/istrazivanja/istrazivanje-o-koristenju-interneta-mobitela-i-drugih-tehnologija/
- Politička akademija BiH: *Računalni kriminalitet – Prijetnje i posljedice na političke i ekonomske odnose*, URL: http://www.academia.edu/17744563/Ra%C4%8Dunalni_kriminalitet_Prijetnje_i_posljedice_na_politi%C4%8Dke_i_ekonomske_odnose
- Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F. (2010.): *The Importance of Cybersecurity Education in School*, URL: http://www.ijiet.org/vol10/1393-JR419.pdf
- Schneider Fred B. (2013.): *Cybersecurity Education in Universities*, URL: https://ieeexplore.ieee.org/abstract/document/6573305
- SciTechBlog (2010): *Facebook fixes security bug in chat program*, URL: https://scitech.blogs.cnn.com/2010/05/05/blog-finds-possible-security-flaw-in-facebook-chat/
- Sites.google.com: *Usluge interneta*, URL: https://sites.google.com/site/sveointernetu/home/usluge-interneta
- Službena stranica Grada Rijeka: *Deklaracija o pravima djeteta*. URL: https://www.rijeka.hr/teme-za-gradane/obitelj-i-drustvena-skrb/djeca-i-mladi/sigurnost-i-zastita-prava-djece-i-mladih/deklaracija-pravima-djeteta/
- Skolazazivot.hr: *Eksperimentalne škole*, URL: https://skolazazivot.hr/o-projektu/eksperimentalne-skole/

- Središnji državni ured za razvoj digitalnog društva (2022.): *Kibernetička sigurnost*, URL: https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436
- Tesla.carner.hr - Nacionalni portal za učenje na daljinu: *Uvod u Internet*. URL: https://tesla.carnet.hr/mod/book/view.php?id=5428&chapterid=883
- Tuđman, M., Boras, D., Dovedan, Z. (1993): *Uvod u informacijske znanosti*. Zagreb: Školska knjiga, URL: http://dzs.ffzg.unizg.hr/text/Uvod%20u%20informacijske%20znanosti/
- Vlada Republike Hrvatske (2015.): *Nacionalna strategija kibernetičke sigurnosti*, URL: https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kibernetic ke%20sigurnosti%20(2015.).pdf?vel=491670
- Vlada RH (2004): *Program aktivnosti za sprječavanje nasilja među djecom i mladima*. URL: http://os-akzrinski-retkovci.skole.hr/upload/os-akzrinski-retkovci/images/static3/879/attachment/PROGRAM_aktivnosti_za_sprjecavanje_nasilja_medju_djecom_i_mladima_2004.pdf
- Zalessky I., Furnell S. (2020.): *Digital Education: The Cyberrisks of the online classroom*, URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/03172621/education_report_04092020.pdf
- Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 126/12, 94/13, 152/14, 07/17, 68/18, 98/19, 64/20)
- Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)
- Zavod za sigurnost informacijskih sustava (2016.): *Nacionalna taksonomija računalno-sigurnosnih incidenata*, URL: https://www.cert.hr/wp-content/uploads/2018/06/Nacionalna-taksonomija-ra%C4%8Dunalno-sigurnosnih-incidenata.pdf
- Žele, A.: *Agresija psihologija – definicija agresivno ponašanje i nasilna komunikacija*, URL: https://gorila.jutarnji.hr/vijestigorila/gorilopedija/lifestyle/obrazovanje_i_psihologija/agresija_psihologija_definicija_agresivno_ponasanje_i_nasilna_komunikacija/

Knjige i radovi:

- Bachmair, B., Bazalgette, C. (2007): „The European Charter for Media Literacy: Meaning and Potential.“ *Research in Comparative and International Education*; 2(1): 80.-87.
- Bašić, J. (2012): *Prevencija poremećaja u ponašanju u školi.* Velika Gorica:: Tiskara

- Bauer, T.A. (2005): „Medijska etika kao pitanje komunikacijske kulture.“, str.45.-77., u: Zgrabljić Rotar, N. (ur.): *Medijska pismenost i civilno društvo.* Sarajevo: MediaCentar
- Bedić, B., Filipović, M. (2014):. "Klikni za sigurnost" – spriječimo nasilje, gradimo kulturu mira i nenasilja. Zagreb: Ambidekster Klub
- Bilić, V., Buljak Flander, G., Hrpka, H. (2012): *Nasilje nad djecom i među djecom*. Zagreb: Naklada Slap
- Boban, V. (2003): *Počela govorne komunikacije*. Zagreb: Dan
- Bošković, T. (2017): *Medijska pismenost i suvremeno društvo* [diplomski rad]. Rijeka: Filozofski fakultet Sveučilišta u Rijeci
- Boyd, D. M., Ellison, N. B. (2007): „Social Network Sites: Definition, History, and Scholarship.“ *Journal of Computer-Mediated Communication* 13(1): 210.-230.
- Breslauer, N., Gregorić, M. (2016): „Utjecaj suvremenih informacijskih tehnologija na učinkovitost poduzetničkih projekata.“ *Zbornik radova Međimurskog veleučilišta u Čakovcu*; 6(2): 49.-57.
- Cajner Mraović, I., Gosarić, S., Kikić, S. (2019): „Povezanost školske klime s postupanjem učenika i razlozima za nepostupanje u situacijama nasilja na društvenim mrežama.“ *Napredak: Časopis za interdisciplinarna istraživanja u odgoju i obrazovanju*; 160(3-4): 241.-263.
- Ćurković, L. (2021): *Sociološke teorije devijantnosti*. Završni rad. Osijek: Filozofski fakultet Sveučilišae J. J. Strossmayera u Osijeku
- Demunter, C. (2006): „How skilled are Europeans in using computers and Internet?“. *Eurostat: Statistics in Focus*; 17
- Dragičević, D. (2004): *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb: Informatorov biro sustav
- Dragičević, D. (2015): *Pravna informatika i pravo informacijskih tehnologija*. Zagreb: Narodne Novine
- Ivić, P. (2015): *Uloga informacijske tehnologije u poslovanju banaka s posebnim osvrtom na Erste&Steiermarkische banku* [diplomski rad], Zagreb: Ekonomski fakultet Sveučilišta u Zagrebu
- Jakovac Baier A., Hebrang Grgić, I. (2015): „Informacijska (ne)pismenost: istraživanje mladih korisnika knjižnica u Vukovaru.“ *Knjižničarstvo*, Glasnik Društva knjižničarstva Slavonije i Baranje; 19(1-2): 27.-46.
- Jokić A., Koljenik D., Faletar Tanacković S., B.Badurina B. (2016): „Vještine informacijske i informatičke pismenosti studenata informacijskih znanosti u Osijeku: pilot-istraživanje.“ *Vjesnik bibliotekara Hrvatske* 59(3-4): 63-92.

- Jurić, Lj. (2015): *Strategije za promicanje medijske pismenosti u Hrvatskoj* [završni rad]. Koprivnica: Sveučilište Sjever
- Keresteš, G. (2007): „Dječja agresivnost - što pokazuju rezultati istraživanja provedenih u našoj zemlji?“ u: Kolesarić, V. (ur.): *Psihologija i nasilje u suvremenom društvu*, Zbornik radova Psihologija i nasilje u suvremenom društvu znanstveno-stručnog skupa. Osijek: Filozofski fakultet Sveučilišta J. J. Strossmayera u Osijeku
- Kladar, D. (2018.) Kako se pripremiti za GDPR, Zagreb: Forum poslovni mediji
- Kregar, J., Sekulić, D., Ravlić, D., Grubišić, K. (2008): *Uvod u sociologiju*, Zagreb: Pravni fakultet Zagreb
- Kupres Đorđević, E. (2016): *Uloga društvenih mreža u suvremenom poslovanju*. Pula: Fakultet ekonomije i turizma Sveučilišta Jurja Dobrile u Puli
- Kušić, S. (2010): „Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike facebook generacije.“ *Život i škola: časopis za teoriju i praksu odgoja i obrazovanja* 56(24): 103.-125.
- Labaš, D. (2015): „Medijska pismenost: preduvjet za odgovorne medije.“ *Knjižničar/Knjižničarka: e-časopis Knjižničarskog društva Rijeka*; 6(6): 22.-32.
- Lamza-Maronić, M., Glavaš, J. (2008): *Poslovno komuniciranje*. Osijek: Studio HS internet d.o.o.; EFOS
- Laniado, N., Pietra, G. (2005): *Naše dijete, videoigre, Internet i televizija: što učiniti ako ga hipnotiziraju?*. Rijeka: Studio TiM
- Mandarić, V. (2012): „Novi mediji i rizično ponašanje djece i mladih.“ *Bogoslovska smotra*; 82(1): 131.-149.
- Mangold, G. W., Faulds, D. J. (2009): „Social media: The newhybrid element of the promotionmix,“ *Business Horizonts* 53(4): 357.-365.
- Masterman, L. (1985): *Teaching the Media,* London: Routledge
- Masterson, J., Apel, K. (2004): *Jezik i govor - od rođenja do 6. godine.* Lekenik: Ostvarenje d.o.o.
- Mataušić, J.M. (2007): „Komunikacijske znanosti: znanstvene grane i nazivlje.*“* U: Matušić, J.M.: *Zbornik radova Znanstvenog kolokvija, Hrvatski studiji,* 3.svibnja 2006. Zagreb: Hrvatski studiji
- Matusina, M. (2017): *Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka* [diplomski rad]. Zagreb: Sveučilište u Zagrebu
- McQuade, S. C., Colt, J. P., Meyer, B. B. (2009*): Cyber Bullying: Protecting Kids and Adults from Online Bullies.* Westport. Conn: Praeger Publishers
- Mecanović, I., Zima, P. (2007): *Uvod u pravo informacija.* Osijek: Pravni fakultet Sveučilišta J.J.Strossmayera u Osijeku

- Miliša, Z., Zloković, J. (2008): *Odgoj i manipuliranje u obitelji i medijima*. Zagreb: Markom
- Nadrljanski, Đ. (2006): „Informatička pismenost informatizacija obrazovanja.“ *Informatologija;* 39 (4): 262. – 266.
- Obiteljski zakon (NN 103/15, 98/19)
- Opća uredba o zaštiti podataka (SL EU L119)
- Oblak, T. (2002): „Internet kao medij i normalizacija kibernetskog prostora.“ *Medijska istraživanja* 8(1): 61.-76.
- Olweus, D. (1998): *Nasilje među djecom u školi*. Zagreb: Školska knjiga
- Onyemauche, J. (2021): *Deviant behaviours in school: Implication for counselling.* Nigeria: National Opet University of Nigeria
- Palmer, A., Koenig, L.N. (2008): „An experiental, socialnetwork-based approach to direct marketing“. International Journal of Direct Marketing 3(3): 162.-176.
- Pašica, A., Turza-Bogdan, T. (2020): „O medijima i govorno-jezičnome razvoju djece s roditeljskog motrišta.“ *Hrvatski: časopis za teoriju i praksu nastave hrvatskoga jezika, književnosti, govornoga i pismenoga izražavanja te medijske kulture* 18(1-2): 73.-92.,
- Pašica, A. (2019): *Utjecaj medija na razvoj govora djeteta*. Zagreb: Učiteljski fakultet Sveučilišta u Zagrebu
- Paul, S., Smith, P. K., Blumberg, H. H. (2012): „Comparing student perceptions of coping strategies and school interventions in managing bullying and cyberbullying incidents“. *Pastoral Care in Education;* 30(2): 127-146.
- Pelc, M. (2002): *Pismo, knjiga, slika: uvod u povijest informacijske kulture*. Zagreb: Golden marketing
- Peruško, Z. (2008): *Mediji, kultura i civilno društvo,* Zagreb: Hrvatsko sociološko društvo
- Potter, J. (2011): *Medijska pismenost.* Beograd: Multimedia,Clio
- Potter, J.W. (2001): *Media Literacy*. London: SAGE Publications
- Pötinger, I. (2004): *Medienbildung im Dopelpack- Wie Schule und Jugendhilfe einander ergänzen können*, Bielefeld, GMK
- Povelja Europske unije o temeljnim pravima (2016/C, 202/02)
- Pregrad, J., Tomić Latinac, M., Mikulić, M. i Šeparović, N. (2011): *Iskustva i stavovi djece, roditelja i učitelja prema elektroničkim medijima: Izvještaj o rezultatima istraživanja provedenog među djecom, učiteljima i roditeljima u sklopu programa prevencije elektroničkog nasilja "Prekini lanac".* Zagreb: Ured UNICEF-a za Hrvatsku
- Prpić, I. (2006): „Vršnjačko nasilje među djevojčicama.“ *Ljetopis socijalnog rada* 13(2): 315.-330.

- Reardon, K.K. (1998): *Interpersonalna komunikacija: gdje se misli susreću*. Zagreb: Alinea
- Roberts, D,, Foehr, U. (2008): *Trends in Media Use*. New Jersey: Centre for the Future of Children
- Schneier, B. (2015): *Data and Goliath*, W. W. Norton & Company, New York, London
- Srića V., Spremić M. (2000): *Informacijskom tehnologijom do poslovnog uspjeha*. Zagreb: Sinergija nakladništvo
- Stepanić, L. (2019): „Vršnjačko nasilje i preventivni programi.“ *Varaždinski učitelj: digitalni stručni časopis za odgoj i obrazovanje* 2(2): 67.-77.
- Šimundić, S., Franjić, S., Vdovjak, K. (2012): „HOAX.“ *Zbornik radova pravnog fakulteta u Splitu*; 49(3): 459.-480.
- Špiranec, S. (2003): „Informacijska pismenost-ključ za cjeloživotno učenje.“ Edupoint; 3(17)
- Šušnjara, S. (2013): „Izloženost djece nasilju putem različitih medija.“ *Suvremena pitanja* 15: 77.-90.
- Tolić, M. (2008): „Aktualnost medijskih kompetencija u suvremenoj pedagogiji.“ *Acta Iadertina*; 5(1): 1.-13.
- Ustav RH (NN 56/90,…05/14)
- Varga, M., Šimović, V. i Milković, M. (2012.): Zaštita elektroničkih informacija, Varaždin
- Velki, T. (2012): „Uloga nekih obiteljskih čimbenika u pojavi nasilja nad djecom“. *Psihologijske teme* 21 (1): 26-60.
- Vrkić Dimić J. (2014): “Suvremeni oblici pismenosti.” *Školski vjesnik*; 63(3): 381-394.
- Vučić, Đ. (2015): *Kvantitativne i kvalitativne odlike medijske pismenosti u kontekstu masovnog komuniciranja* [završni rad]. Koprivnica: Sveučilište Sjever
- Willard, N. E. (2007): *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. Champaign, IL: Research Press
- World Health Organization (2002): *World report on violence and health*. Geneva: World Health Organization
- Zgrabljić Rotar, N. (2011): „Masovni mediji i digitalna kultura.“ U: *Digitalno doba, Masovni mediji i digitalna kultura.* Zadar: Sveučilište u Zadru
- Zgrabljić Rotar, N. (2005): „Mediji - Medijska pismenost, medijski sadržaji i medijski utjecaji“, str.9.-45. u: Zgrabljić Rotar, N. (ur.): *Medijska pismenost i civilno društvo*, Sarajevo: MediaCentar
- Zovkić, D. (2015): *Nasilje putem interneta* [završni rad]. Osijek: Filozofski fakultet Sveučilišta u Osijeku

- Žarković Palijan, T. (2004): Z*načajke osobnosti alkoholičara počinitelja i nepočinitelja kaznih djela* [doktorska disertacija]. Zagreb: Medicinski fakultet Sveučilišta u Zagrebu
- Žilić, M., Janković, J. (2016): „Nasilje.“ *Socijalne teme: Časopis za pitanja socijalnog rada i srodnih znanosti* 1(3): 67-87.
- Žuran, K., Ivanišin, M. (2013): „Media Literacy in Times of Media Divides.“ *Medijske studije*; 4(8): 3.-15.

POPIS SLIKA

Slika 1. Najveće stranice za društveno umrežavanje prema sveukupnoj posjećenosti (Izvor: eBizMBA (2017): Top 15 most popular social networking sites, URL: http://www.ebizmba.com/articles/social-networking-websites).....25

POPIS TABLICA

Tablica 1. Pregled najvažnijih godina/događaja za razvoj Interneta (Izvor: Izrada autorice prema: Hajdarović, M. (2006): *Povijesni razvoj interneta*. URL: http://povijest.net/2018/?p=2374).....23
Tablica 2. Razine školskih preventivnih programa i aktivnosti kojima se prevenira nasilje (Izvor: Bašić, J. (2012): *Prevencija poremećaja u ponašanju u školi.* Velika Gorica:: Tiskara 11.-22.)……45
Tablica 3. Sigurnost djece na internetu – prikaz istraživanja (Izvor: autorica rada temeljem dosadašnjih istraživanja i rezultatima istih)……50
Tablica 4. Prikaz postotka ispitanika o navedenim tvrdnjama (Izvor: autorica rada)..67

POPIS GRAFIKONA

Grafikon 1. Prikaz postotka ispitanika obzirom na razred koji pohađaju (Izvor: autorica rada) ..……..55
Grafikon 2. Prikaz postotka ispitanika s obzirom na spol (Izvor: autorica rada)…….55
Grafikon 3. Prikaz postotka učestalosti pristupa ispitanika internetu (Izvor: autorica rada) ..……..56
Grafikon 4. Prikaz postotka vremena koje ispitanici provode na internetu(Izvor: autorica rada) ……57
Grafikon 5. Prikaz postotka uređaja kojima ispitanici pristupaju internetu (Izvor: autorica rada) ……57
Grafikon 6. Prikaz postotka vlastitog uređaja s kojeg ispitanici pristupaju internetu (Izvor: autorica rada) ……58
Grafikon 7. Prikaz postotka aktivnosti ispitanika za koje koriste internetske usluge (Izvor: autorica rada)……..58
Grafikon 8. Prikaz postotka ispitanika koji prepoznaju osobne podatke (Izvor: autorica rada) ..……..59
Grafikon 9. prikaz postotka ispitanika koji ispravno prepoznaju adresu web stranica koja je sigurna za pretraživanje i preuzimanje dokumenata (Izvor: autorica rada)……..……..59
Grafikon 10. Prikaz postotka oblika hardverske zaštite koriste ispitanici na svojim mobilnim uređajima (Izvor: autorica rada) ……..60
Grafikon 11. Prikaz postotka ispitanika u kojoj mjeri koriste programsku zaštitu na svojim računalima (Izvor: autorica rada) ……61
Grafikon 12. Prikaz postotka mišljenja ispitanika o programskoj zaštiti (Izvor: autorica rada) ……61
Grafikon 13. Prikaz postotka poznavanja ispitanika o obliku softverske zaštite računala (Izvor: autorica rada) ……62
Grafikon 14. Prikaz postotka koliko često ispitanici nadograđuju operacijske sustave svojih računala (Izvor: autorica rada) ……..62
Grafikon 15. Prikaz postotka ispitanika koji prepoznaju sigurne lozinke za kreiranje korisničkih računa (Izvor: autorica rada) ……63
Grafikon 16. Prikaz postotka koliko često ispitanici mijenjaju lozinke svojih korisničkih računa (Izvor: autorica rada) ……63

Grafikon 17. Prikaz postotka ispitanika koji su dobili zahtjev za promjenom lozinke na internetskim stranicama na kojima imaju kreiran korisnički račun (Izvor: autorica rada)……64
Grafikon 18. Prikaz postotka načina na koji su ispitanici zaštitili profil na internetskim stranicama (Izvor: autorica rada)……66

PRILOG 1.

ANKETNI UPITNIK KORIŠTEN U ISTRAŽIVANJU
SIGURNOST DJECE NA INTERNETU - ZAŠTITA OSOBNIH PODATAKA

Dragi učenici,

ispred vas se nalazi anonimna anketa čiji je cilj istražiti na koji način i u kojoj mjeri upotrebljavate softversku i hardversku računalnu zaštitu prilikom korištenja interneta. Anketa se provodi u svrhu izrade diplomskog rada čiji je naziv „Sigurnost djece na internetu – zaštita osobnih podataka“ na Fakultetu Informatike Sveučilišta Jurja Dobrile u Puli. Vaši će se odgovori koristiti isključivo u znanstvene svrhe. Istraživanje ne nosi rizik korištenja i objave vaših osobnih podataka.

Srdačan pozdrav,

Gordana Vukoje

e-mail: gvukoje@student.unipu.hr

ZAOKRUŽITE ODGOVOR KOJI SE ODNOSI NA VAS:

1. U koji razred ideš?
   a) Peti
   b) Šesti
   c) Sedmi
   d) Osmi

2. Spol:
   a) Muški
   b) Ženski

3. Koliko često pristupaš internetu?
   a) Nikad
   b) Ponekad
   c) Redovito

4. Koliko vremena dnevno provodiš na internetu?
   a) Manje od 1 sata
   b) 1 sat
   c) 2 – 3 sata
   d) 4 - 5 sati
   e) 6 - 7 sati
   f) 8 – 9 sati
   g) 10 i više sati

5. S kojeg uređaja najčešće pristupaš internetu?
   a) Mobitel/pametni telefon

b) Stolno računalo
c) Prijenosno računalo/laptop
d) Tablet
e) Igraća konzola

6. Imaš li vlastiti uređaj s kojeg pristupaš internetu?
   a) Da
   b) Ne

7. Internetske usluge (servise) najčešće koristim za:
   a) Slušanje glazbe
   b) Objavljivanje fotografije
   c) Pisanje komentara na internetskim stranicama
   d) Gledanje video klipova
   e) Dijeljenje sadržaja s drugima
   f) Kreiranje internetskih stranica
   g) Igranje igara na internetu
   h) Pretraživanje internetskih
   i) Pristup društvenim mrežama
   j) Ostalo

8. Odaberi koji podatci NE pripadaju OSOBNIM podatcima:
   a) Ime i prezime
   b) Nadimak
   c) Adresa e-pošte
   d) Adresa stanovanja
   e) Fotografije i videozapisi

9. Po čemu prepoznaješ adresu web stranice koja je sigurna za pretraživanje i preuzimanje dokumenata:
   a) Počinje sa https://
   b) Ima znak malog zaključanog lokota
   c) Počinje sa http://
   d) Ima znak ⓘ

10. Koji oblik zaštite najčešće koristiš na svojim mobilnim uređajima (pametni telefon, tablet, laptop)?
    a) Otključavanje zaslona
    b) Otključavanje otiskom prsta
    c) Otključavanjem licem
    d) Unošenjem sigurnosnog pina

11. Imaš li instaliran antivirusni softver na svojim računalima (stolno računalo, laptop, tablet, pametni telefon,…)?
    a) Da
    b) Ne
    c) Ne znam

12. Smatraš li da je antivirusne programe potrebno redovito ažurirati/nadograđivati?
    a) Da
    b) Ne

13. Što je Firewall (vatrozid)?
    a) Antivirusni program
    b) Zlonamjeran virus
    c) Štiti naše računalo od neželjenih pristupa drugih na internetu

14. Koliko često nadograđuješ operacijske sustave (npr. OS Windows, OS Mac, OS Linux, Android,…) svojih računala:
    a) Nikad
    b) Ponekad
    c) Redovito

15. Odaberi koja od navedenih lozinki NIJE sigurna za tvoj korisnički račun na internetu:
    a) 0P:opasn0st!
    b) Ar@3bEstKlu$!!
    c) Martina
    d) JžUuJl22KA?!

16. Koliko često mijenjaš lozinku svojih korisničkih računa na internetu?
    a) Nikad
    b) Ponekad
    c) Redovito

17. Jesi li ikada dobio/dobila zahtjev da promijeniš lozinku na internetskoj stranici, a da to nisi učinio/učinila?
    a) Da
    b) Ne

18. Označite za sljedeće tvrdnje u kojoj se mjeri odnose na vas:

    Kada sam u mogućnosti, uvijek provjeravam adresu pošiljatelja prije otvaranja moje e-pošte:
    a) Nikad
    b) Ponekad
    c) Redovito

    Unosim svoju lozinku na mrežnu stranicu slijedeći poveznicu koju sam dobio/dobila e- poštom od nepoznatog pošiljatelja
    a) Nikad
    b) Ponekad
    c) Redovito

Na internetskim stranicama na kojima kreiram svoj profil, najprije uvijek pročitam „Izjavu o pravima i odgovornosti“:

a) Nikad
b) Ponekad
c) Redovito

Gotovo uvijek čitam informacije o postavkama privatnosti kada pristupam aplikacijama i stranicama na internetu:

a) Nikad
b) Ponekad
c) Redovito

19. Ukoliko imaš otvoren profil na internetskoj stranici, na koji si način zaštitio svoj profil?

a) Račun je privatan
b) Samo ja mogu dodavati prijatelje na svoju listu prijatelja
c) Mogu me pratiti samo prijatelji na mojoj listi
d) Samo ja mogu vidjeti osobe i stranice koju pratim
e) Kada te netko označi, trebaš dati dopuštenje da se objava može vidjeti na tvom profilu
f) Znam ukloniti ljude sa svoje liste pratitelja
g) Znam koje informacije smijem dijeliti, a koje ne smijem dijeliti na internetu

PRILOG 2.

SUGLASNOST ZA PROVEDBU ISTRAŽIVANJA

Molim Vas da odobrite provođenje istraživanja u kojem bi sudjelovali učenici Vaše škole. Cilj istraživanja je na koji način i u kojoj mjeri učenici upotrebljavaju softversku i hardversku zaštitu prilikom korištenja interneta. Istraživanje se provodi u svrhu izrade diplomskog rada čiji je naziv „Sigurnost djece na internetu – Zaštita osobnih podataka“ na Fakultetu Informatike Sveučilišta Jurja Dobrile u Puli. Odgovori prikupljeni dobivenim istraživanje koristit će se isključivo u znanstvene svrhe.

_____ _____

Potpis studentice Potpis ravnateljice