

ISTRAŽIVANJE

O DIGITALNOJ BEZBEDNOSTI DECE

U GRADU VRANJU



U okviru projekta "Promocija bezbednosti dece u digitalnom okruženju"
koji realizuje

Organizacija za razvoj i demokratiju Bujanovac, uz finansijsku pomoć
Ministarstva za brigu o porodici i demografiju Republike Srbije



МИНИСТАРСТВО
ЗА БРИГУ О ПОРОДИЦИ
И ДЕМОГРАФИЈУ



Cilj ovog istraživanja je da se sagleda trenutna situacija u vezi sa digitalnom bezbednošću i upotrebom interneta među decom u Gradu Vranju.

Projektom želimo da identifikujemo ključne rizike na koje deca mogu naići u digitalnom okruženju, kao i da prikupimo podatke koji će pomoći u razvoju odgovarajućih smernica za roditelje, obrazovne institucije i lokalnu zajednicu.

Očekuje se da rezultati istraživanja pruže osnovu za dalji razvoj edukativnih programa i preventivnih inicijativa koje će doprineti povećanju digitalne pismenosti i bezbednosti dece, kao i jačanju kapaciteta roditelja i učitelja u zaštiti dece na internetu.

Kroz ovaj projekat, cilj je podići svest o značaju zaštite dece na internetu i omogućiti im bezbednije korišćenje digitalnih platformi.

Istraživanje o digitalnoj bezbednosti dece u Gradu Vranju



1. UVOD

U savremenom dobu, internet je postao nezaobilazni deo svakodnevnog života, kako odraslih, tako i dece. Digitalno okruženje pruža brojne mogućnosti za edukaciju, zabavu i druženje, ali istovremeno nosi i određene rizike, koji su posebno izraženi među mlađim korisnicima. Dok se deca sve više oslanjaju na internet za istraživanje, učenje i komunikaciju, isto tako postaju izložena potencijalnim opasnostima, kao što su neprikladan sadržaj, cyberbullying i kontakt sa nepoznatim osobama.

Cilj ovog istraživanja je da se analiziraju obrasci korišćenja interneta među decom u Gradu Vranju, prepoznaju potencijalni rizici sa kojima se deca suočavaju na internetu i ukaže na ulogu porodice u osiguravanju digitalne bezbednosti. Kroz anketiranje 200 roditelja iz Vranja, istraživanje nastoji da pruži jasnu sliku o tome kako deca koriste internet, koje su najpopularnije platforme, koliko vremena provode online, i kako se roditelji nose sa izazovima digitalne bezbednosti.

Pitanja u anketi biće usmerena na istraživanje učestalosti korišćenja interneta, popularnosti platformi poput YouTube-a, TikTok-a, i Instagrama, kao i na prepoznate opasnosti sa kojima se deca suočavaju. Takođe, biće analizirane mera zaštite koje roditelji preduzimaju, uključujući postavke privatnosti, kontrole vremena provedenog online, i upotrebu jake lozinke.

Očekivani rezultati ovog istraživanja pružiće osnovu za kreiranje smernica koje mogu pomoći roditeljima, obrazovnim institucijama i lokalnoj zajednici u unapređenju digitalne pismenosti i bezbednosti dece. Istraživanje će omogućiti da se identifikuju najveći izazovi sa kojima se roditelji suočavaju i ponudi konkretne preporuke za poboljšanje nadzora nad digitalnim aktivnostima dece. Takođe, pružaće osnovu za razvoj edukativnih programa i inicijativa usmerenih na smanjenje rizika i povećanje sigurnosti u digitalnom okruženju.

Uloga porodice u digitalnoj bezbednosti deca je ključna, jer roditelji igraju centralnu ulogu u postavljanju granica i odgovarajućem nadzoru. Ovaj istraživački rad će takođe ponuditi konkretne preporuke za roditelje, kao što su edukacija o sigurnosnim postavkama, usmeravanje dece ka bezbednijim online sadržajima, i otvorena komunikacija o online iskustvima. Kroz ove aktivnosti, cilj je stvoriti sigurnije i odgovornije digitalno okruženje za decu u Vranju, koje će omogućiti bolje snalaženje u online svetu i smanjiti rizik od negativnih iskustava.

2.METODOLOGIJA

Istraživanje je sprovedeno putem anonimnog upitnika, koji je distribuiran roditeljima sa prebivalištem u Gradu Vranju. Uzorak obuhvata ukupno 200 ispitanika, pri čemu su podaci analizirani prema polu, starosnoj strukturi roditelja, broju dece i njihovim uzrastima. Upitnik sadrži pitanja koja pokrivaju sledeće oblasti:

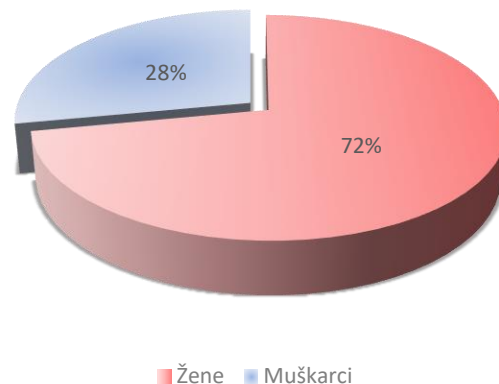
1. Opšti podaci o roditeljima (pol, starost, broj dece).
2. Obrasci korišćenja interneta kod dece (vreme provedeno na internetu, omiljene platforme, vrste sadržaja).
3. Prepoznati rizici i mere bezbednosti (neprijatna iskustva, mere zaštite, poznavanje potencijalnih opasnosti).
4. Uloga porodice u edukaciji i zaštiti dece na internetu.

Podaci su obrađeni kvantitativnim metodama, a rezultati su prikazani kroz tabele i grafikone, uz odgovarajuću analizu i interpretaciju.

3. REZULTATI ISTRAŽIVANJA

3.1. Polna struktura ispitanika

- Žene: 72% (144 ispitanika)
- Muškarci: 28% (56 ispitanika)

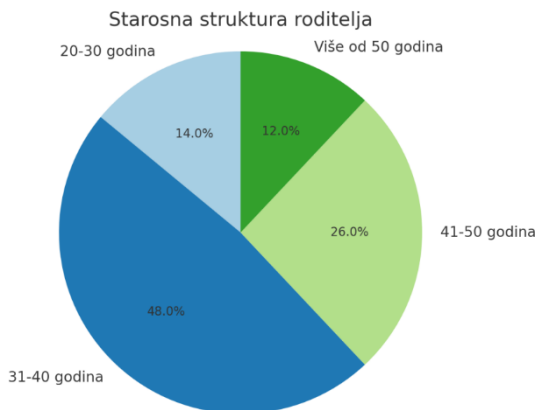


Rezultati istraživanja ukazuju na veću zastupljenost žena (72%) u uzorku, što može biti rezultat njihove veće uključenosti u svakodnevnom nadzoru nad decom. Muškarci čine 28% ispitanika, što sugerise na potrebu za većim angažovanjem očeva u digitalnoj bezbednosti dece.

Preporučuje se da se roditeljima omogući obrazovanje o digitalnoj bezbednosti koje uključuje oba roditelja, kako bi zajednički stvorili bezbedno digitalno okruženje za svoju decu. Škole i lokalna zajednica mogu organizovati radionice koje uključuju oba roditelja, čime bi se omogućilo bolje razumevanje i veća saradnja u digitalnoj zaštiti.

3.2. Starosna struktura roditelja

- 20-30 godina: 14% (28 ispitanika)
- 31-40 godina: 48% (96 ispitanika)
- 41-50 godina: 26% (52 ispitanika)
- Više od 50 godina: 12% (24 ispitanika)

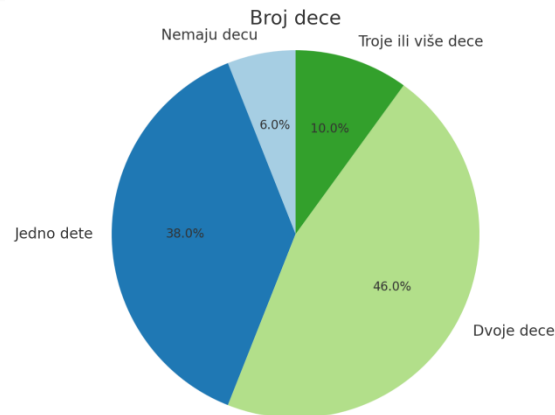


Najveći procenat ispitanika spada u grupu roditelja uzrasta od 31 do 40 godina (50%), što ukazuje na to da su oni u ključnoj životnoj fazi kada imaju decu školskog uzrasta i često koriste internet za obrazovne i zabavne svrhe. Takođe, postojanje manjih procenata roditelja starijih od 50 godina (7%) ukazuje na to da je potrebno dodatno raditi na edukaciji starijih roditelja o digitalnim rizicima.

Za roditelje svih starosnih grupa potrebno je uložiti napore u obrazovanje o digitalnim izazovima. Preporučuje se organizovanje specifičnih edukacija i radionica za starije roditelje, a škole bi mogle implementirati kurseve i predavanja o digitalnoj bezbednosti, dok bi lokalna zajednica trebala podržati takve inicijative.

3.3. Broj dece

- Nemaju decu: 6% (12 ispitanika)
- Jedno dete: 38% (76 ispitanika)
- Dvoje dece: 46% (92 ispitanika)
- Troje ili više dece: 10% (20 ispitanika)

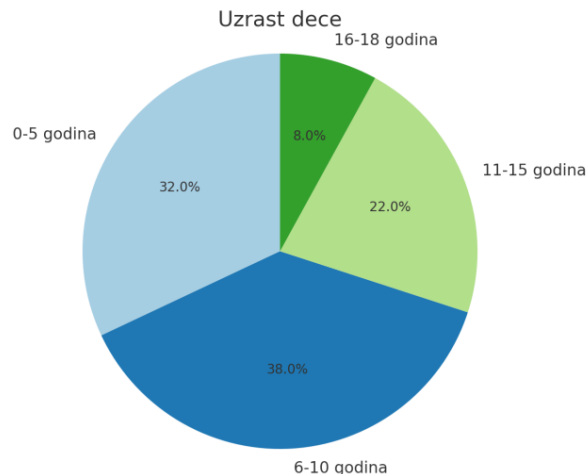


Veći broj ispitanika (46%) ima dvoje dece, a 38% roditelja ima jedno dete. Ovo ukazuje na to da su roditelji sa više dece možda suočeni sa većim izazovima u upravljanju digitalnom pismošću i zaštitom dece na internet

Preporučuje se da roditelji razvijaju strategije zaštite koje uzimaju u obzir specifične potrebe svakog deteta, jer svako dete ima različite digitalne navike i potrebe. Škole bi mogle da implementiraju programe koji obrađuju različite uzraste i nivoe digitalnih veština. Lokalna zajednica može pružiti podršku roditeljima kroz kurseve i materijale za upravljanje digitalnim životima više dece.

3.4.Uzrast dece

- 0-5 godina: 32% (64 roditelja)
- 6-10 godina: 38% (76 roditelja)
- 11-15 godina: 22% (44 roditelja)
- 16-18 godina: 8% (16 roditelja)

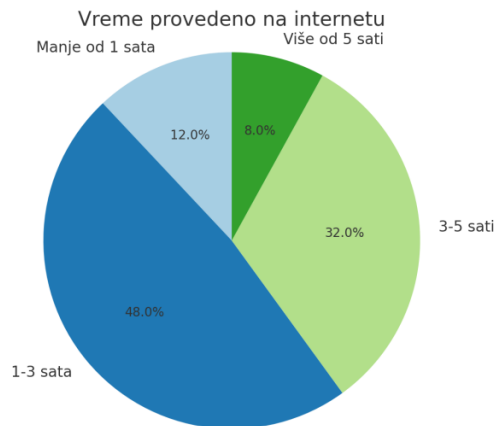


Najveći procenat ispitanika ima decu uzrasta od 6 do 10 godina (39%), što znači da su roditelji ove dece posebno zabrinuti zbog njihove izloženosti internetu. Takođe, 31% roditelja ima decu uzrasta od 0-5 godina, što ukazuje na sve veću digitalnu pismenost već u ranim godinama.

Roditeljima se savetuje da postave jasna pravila o vremenu provedenom online i vrsti sadržaja koji je dozvoljen. Takođe, preporučuje se da se redovno razgovara sa decom o njihovim iskustvima na internetu. Škole bi trebalo da integrišu teme digitalne pismenosti u nastavu, kako bi se razvila svest o sigurnosti na internetu. Lokalna zajednica treba da organizuje edukativne radionice za decu i roditelje, fokusirajući se na prepoznavanje i izbegavanje online rizika.

3.5. Vreme provedeno na internetu

- Manje od 1 sata: 12% (24 roditelja)
- 1-3 sata: 48% (96 roditelja)
- 3-5 sati: 32% (64 roditelja)
- Više od 5 sati: 8% (16 roditelja)

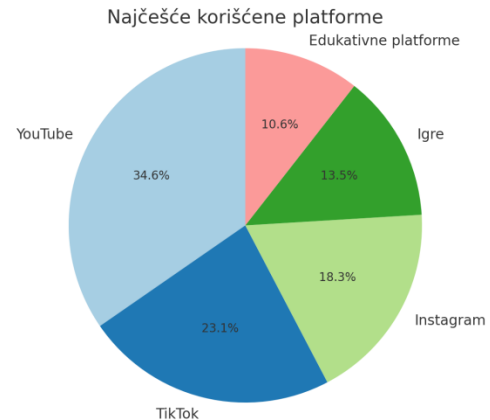


Polovina ispitanika (51%) izjavljuje da deca provode između 1 i 3 sata na internetu dnevno, dok 30% roditelja tvrdi da njihova deca provode između 3 i 5 sati. Ovo ukazuje na značajan broj dece koji provode mnogo vremena online, što može povećati izloženost rizicima poput cyberbullyinga i neprikladnog sadržaja.

Potrebno je da roditelji postave dnevne limite za vreme koje deca provode na internetu, kako bi se obezbedio balans između online i offline aktivnosti. Škole mogu igrati ključnu ulogu u promovisanju zdravog odnosa prema internetu kroz obrazovne programe koji podstiču fizičku aktivnost. Lokalna zajednica treba da pokrene inicijative koje podstiču decu da se bave vanškolskim aktivnostima, smanjujući vreme provedeno online.

3.6. Najčešće korišćene platforme

- YouTube: 72% (144 roditelja)
- TikTok: 48% (96 roditelja)
- Instagram: 38% (76 roditelja)
- Igre: 28% (56 roditelja)
- Edukativne platforme: 22% (44 roditelja)

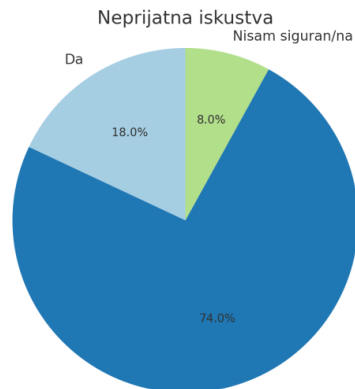


YouTube je najpopularnija platforma među decom (70%), što može značiti da je ovo glavni izvor zabave i edukacije, ali i potencijalno rizična platforma. TikTok i Instagram takođe zauzimaju značajna mesta među najčešće korišćenim platformama (52% i 41%), što može ukazivati na to da deca koriste društvene mreže koje nose specifične rizike, kao što su izloženost neprimerenom sadržaju i cyberbullyingu.

Roditeljima se savetuje da koriste alate za roditeljsku kontrolu na YouTube-u i TikToku i da prate sadržaj koji njihova deca konzumiraju. Takođe, preporučuje se da se deci objašnjavaju rizici od deljenja ličnih podataka na ovim platformama. Škole mogu koristiti ove platforme u obrazovne svrhe, ali bi trebalo da obezbede da se koriste samo bezbedni kanali i sadržaji. Lokalna zajednica može organizovati edukativne kampanje i radionice za decu o sigurnosti na internetu.

3.7. Neprijatna iskustva

- Da: 18% (36 roditelja)
- Ne: 74% (148 roditelja)
- Nisam siguran/na: 8% (16 roditelja)

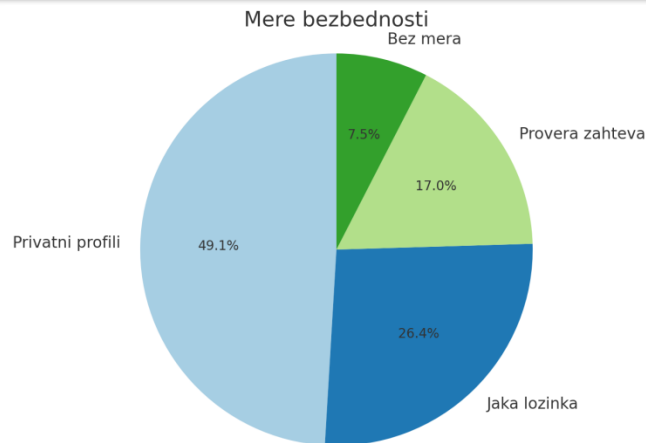


Samo 20% roditelja prijavljuje da je njihovo dete imalo neprijatna iskustva na internetu. Iako ovaj broj nije velik, važno je da se razjasni koji su to problemi sa kojima su se deca suočila, kao što su cyberbullying, neprikladan sadržaj, ili kontakt sa nepoznatim osobama. Ovo je signal za jaču edukaciju i pripremu dece za suočavanje sa digitalnim izazovima.

21% roditelja izjavljuje da su njihova deca imala neprijatna iskustva na internetu. Ovo ukazuje na prisutnost rizika poput cyberbullyinga, neprimerenog sadržaja ili online predatora. Važno je podstaći roditelje da obrate pažnju na ovakve situacije i učine dodatne napore kako bi zaštitili decu.

3.8. Mere bezbednosti

- Privatni profili: 52% (104 roditelja)
- Jaka lozinka: 28% (56 roditelja)
- Provera zahteva: 18% (36 roditelja)
- Bez mera: 8% (16 roditelja)



49% roditelja koristi privatne profile, dok 32% postavlja jake lozinke. Međutim, samo 19% roditelja redovno proverava zahteve koje njihova deca primaju online. Ovi podaci ukazuju na to da je potrebno dodatno educirati roditelje o preventivnim merama zaštite, kao što su proaktivne provere i korišćenje roditeljskih kontrola.

Roditeljima se, na osnovu ovih podataka, savetuje da koriste alate za roditeljsku kontrolu, postave privatnost na svim platformama koje njihova deca koriste i da koriste jake lozinke. Takođe, redovne provere i nadgledanje postavki bezbednosti na uređajima koje deca koriste mogu značajno poboljšati sigurnost. Škole bi mogle obezbediti edukaciju o digitalnoj zaštiti, dok lokalna zajednica treba da podrži roditelje organizovanjem besplatnih kurseva o sigurnosti na internetu.

4. ZAKLJUČCI I PREPORUKE ISTRAŽIVANJA

4.1. Zaključci istraživanja

Zaključci ovog istraživanja su višestruko korisni i omogućavaju dublje razumevanje trenutne situacije u vezi sa digitalnom bezbednošću dece u Gradu Vranju. Na osnovu analize podataka dobijenih od 200 roditelja, možemo izvući nekoliko ključnih tačaka koje se odnose na obrasce korišćenja interneta, prepoznate rizike, kao i meru zaštite koju roditelji primenjuju.



Obrasci korišćenja interneta među decom Istraživanje je pokazalo da je internet postao neizbežan deo života dece u Vranju, što je odraženo u načinu na koji deca koriste internet za različite aktivnosti, kao što su zabava, edukacija i komunikacija. Ovo ukazuje na značajnu transformaciju u načinu života, gde je digitalna tehnologija postala ključna za svakodnevnu interakciju i učenje. Deca uglavnom koriste internet za gledanje video sadržaja, obrazovne resurse i interakciju sa prijateljima putem društvenih mreža. Najpopularnija platforma među decom u Vranju je **YouTube**, koji koristi 72% ispitanih, što ukazuje na njegovu dominantnu ulogu u životima mladih. Na YouTube-u deca ne samo da se zabavljaju, već i pristupaju edukativnim sadržajima koji im pomažu u učenju i istraživanju novih interesa.

TikTok i Instagram su takođe značajno prisutni, iako u manjoj meri, sa naglaskom na zabavu i društvenu interakciju. Ove platforme omogućavaju mladima da se povežu sa vršnjacima, izraze kreativnost i prate trendove, ali takođe donose i rizike povezane sa online ponašanjem, kao što su izloženost neprimerenim sadržajima ili cyberbullying.

Podaci o vremenu provedenom na internetu pokazuju ozbiljan trend u digitalnoj angažovanosti dece. 51% roditelja izjavljuje da njihova deca dnevno provode između 1 i 3 sata na internetu, dok 30% dece provodi 3-5 sati dnevno online. Ovi podaci ukazuju na značajnu količinu vremena koju deca provode na internetu, što može biti posledica sveprisutne digitalizacije obrazovnih sistema, društvenih mreža i drugih online sadržaja koji privlače pažnju mladih. Ovo vreme nije samo rezervisano za zabavu, već uključuje i obrazovne aktivnosti, kao i potrebu za komunikacijom sa prijateljima, što je od esencijalne važnosti za njihov socijalni život.

Uzimajući u obzir ove podatke, može se zaključiti da internet ima sveobuhvatan uticaj na svakodnevni život dece. S obzirom na to da deca provode značajan deo svog vremena online, važno je da roditelji, nastavnici i društvo u celini prepoznaju potrebu za odgovornim korišćenjem interneta. Uz kontinuiranu digitalizaciju obrazovnog sistema, važno je da se u nastavi i svakodnevnom životu poveća upotreba interneta u pozitivnom i edukativnom kontekstu. Sa druge strane, roditelji bi trebalo da budu svesni vremena koje deca provode na internetu i da, u meri u kojoj je to moguće, usmere decu ka zdravim i korisnim sadržajima, dok istovremeno razvijaju svest o potencijalnim rizicima.

Takođe, trendovi u korišćenju platformi poput YouTube-a, TikTok-a i Instagrama ukazuju na potrebu za povećanim fokusom na digitalnu pismenost i bezbednost, jer ove platforme, iako korisne, mogu postati izvori opasnosti ako se ne koriste sa odgovarajućim znanjem i pažnjom.

Priznati rizici i neprijatna iskustva Iako internet pruža mnoge prednosti, uključujući lak pristup informacijama, obrazovnim resursima i mogućnostima za društvenu interakciju, istraživanje je pokazalo da nije bez svojih rizika. 21% roditelja prijavilo je da su njihova deca imala neprijatna iskustva na internetu, uključujući izloženost neprikladnom sadržaju i cyberbullying. Ovi podaci jasno ukazuju na to da, iako deca većinu vremena provode na internetu sa ciljem edukacije ili zabave, oni su i dalje izloženi potencijalnim opasnostima koje mogu negativno uticati na njihov emocionalni i psihološki razvoj.

Izloženost neprikladnom sadržaju, poput nasilnih, seksualnih ili uznemirujućih materijala, predstavlja ozbiljan problem koji može imati dugoročne posledice po mentalno zdravlje mladih korisnika interneta. Takođe, cyberbullying, ili digitalno nasilje, postaje sve češći oblik maltretiranja, jer deca često ne shvataju ozbiljnost svojih online postupaka, niti su u potpunosti svesna posledica koje njihov digitalni angažman može imati na druge.

Zanimljivo je da, uprkos ovim rizicima, samo 49% roditelja koristi osnovne mere zaštite na internetu, kao što su privatni profili i jake lozinke, čime se neefikasno štite od potencijalnih pretnji. Ovo ukazuje na zabrinjavajući jaz između svesnosti o rizicima na internetu i konkretnih koraka koje roditelji preduzimaju kako bi zaštitili svoju decu. Iako mnogi roditelji izražavaju zabrinutost zbog sigurnosti svoje dece na internetu, broj roditelja koji aktivno koriste tehnologiju i postavke privatnosti koje nude različite platforme je iznenađujuće nizak.

Ovaj nedostatak proaktivne zaštite može biti rezultat nekoliko faktora, uključujući nedovoljnu edukaciju roditelja o digitalnoj bezbednosti, nesigurnost u korišćenje tehnoloških alata, ili previđanje ozbiljnosti opasnosti koje deca mogu da sretnu na mreži. Nedostatak svesnosti o mogućim posledicama može dovesti do toga da roditelji nisu u potpunosti spremni da prepoznaju opasnosti na internetu ili da ne shvate važnost aktivne kontrole i nadzora.

Kao odgovor na ovaj problem, od esencijalne je važnosti unapređenje edukacije roditelja o sigurnosti na internetu. Roditelji bi trebalo da budu u mogućnosti da prepoznaju i reše potencijalne rizike, kao i da koriste dostupne alate i strategije za zaštitu svojih mališana. Takođe, potrebno je promovisati više zajedničkih inicijativa između obrazovnih i društvenih institucija kako bi se stvorila sigurnija i odgovornija online zajednica, a deca naučila kako da prepoznaju i izbegnu opasnosti, kao i kako da se ponašaju odgovorno na mreži.

Uloga roditelja i mere zaštite Roditelji igraju ključnu ulogu u obezbeđivanju sigurnosti svoje dece na internetu, jer su oni ti koji mogu primeniti odgovarajuće mere zaštite i pružiti potrebnu podršku u navigaciji online sveta. Iako se većina roditelja slaže da je od suštinskog značaja postavljanje sigurnosnih postavki i zaštita privatnosti, istraživanje je pokazalo zabrinjavajući jaz između njihove svesnosti i stvarnog angažmana u nadgledanju aktivnosti dece. Samo 19% roditelja redovno proverava aktivnosti svojih mališana na internetu, što jasno ukazuje na to da, iako roditelji prepoznaju važnost sigurnosti, nisu dovoljno angažovani u njenom svakodnevnom sprovođenju.

Ove informacije ukazuju na ozbiljan problem: iako su roditelji svesni da je internet pun potencijalnih opasnosti, nedovoljno se angažuju u zaštiti svoje dece od tih rizika. Postoji nekoliko razloga zašto roditelji možda ne preduzimaju odgovarajuće mere zaštite, uključujući nedostatak vremena, tehničku nesvesnost o alatima i postavkama privatnosti, kao i verovanje da deca mogu sama upravljati svojim online aktivnostima. Takođe, mnogi roditelji možda nisu dovoljno informisani o najnovijim opasnostima koje vrebaju na internetu, kao što su cyberbullying, neprikladni sadržaji ili pretnje od online predatora.

Nedostatak redovnog nadzora može dovesti do toga da deca postanu izložena opasnostima koje roditelji nisu uočili, čime se povećava rizik od negativnih posledica po njihovo mentalno zdravlje i sigurnost. Deca mogu postati žrtve nasilja, manipulacije ili eksploatacije, a roditelji često nisu u mogućnosti da prepoznaju te prijetnje na vreme, što još više pogoršava situaciju.

Zato je ključno obrazovanje roditelja o metodama zaštite na internetu i o tome kako da koriste sigurnosne alate i nadzorne tehnike. Roditelji moraju biti informisani o različitim opcijama zaštite koje nude društvene mreže, aplikacije i uređaji, uključujući postavljanje privatnosti, filtriranje sadržaja, i praćenje aktivnosti na mreži. Takođe, važno je razvijati i podsticati komunikaciju između roditelja i dece o sigurnosti na internetu, kako bi deca bila svesna opasnosti i naučila kako da se ponašaju odgovorno na mreži.

Pored toga, važno je uključiti se u aktivni nadzor nad internet aktivnostima dece. Redovno proveravanje i razgovor o tome šta deca rade na internetu mogu značajno smanjiti rizik od izlaganja neprimerenom sadržaju ili opasnim situacijama. Roditelji ne treba da shvataju svoj nadzor kao oblik kontrole, već kao odgovornost za zaštitu dobrobiti svog deteta.

Kroz zajedničke inicijative i obrazovne programe koji se fokusiraju na digitalnu pismenost i bezbednost, roditelji mogu postati bolji mentori i zaštitnici za svoju decu u online svetu. Edukacija i angažman roditelja nisu samo potrebni kako bi deca bila sigurnija, već i da bi roditelji razvili svest o tome kako se tehnologija brzo menja, kao i o tome šta sve deca mogu da naiđu na internetu.

Demografski faktori i obrazovne potrebe istraživanje je takođe pokazalo značajnu demografsku karakteristiku roditelja u Vranju: najveći broj roditelja je u uzrastu između 31 i 40 godina, a većina njih ima dvoje dece. Ovi podaci imaju ključnu ulogu u razumevanju kako roditelji pristupaju pitanjima digitalne bezbednosti, jer porodice sa više dece mogu biti suočene sa specifičnim izazovima u obezbeđivanju sigurnosti na internetu za svako svoje dete, naročito kada se radi o deci različitih uzrasta i sa različitim potrebama.

Roditelji koji imaju više od jednog deteta često moraju balansirati između različitih faza razvoja dece, što uključuje različite potrebe u pogledu digitalne bezbednosti. Na primer, mlađa deca (od 6 do 10 godina), koja čine najveću grupu korisnika interneta, zahtevaju posebnu pažnju. U ovoj uzrasnoj grupi, deca su često radoznala i sklona istraživanju sadržaja na internetu, ali im nedostaje sposobnost da prepoznaju opasnosti i neprikladan sadržaj. Roditelji u ovoj grupi treba da budu posebno oprezni u postavljanju pravila korišćenja interneta, kao i u obezbeđivanju tehničkih alata koji mogu ograničiti pristup neprimerenom sadržaju.

S obzirom na to da deca različitih uzrasta koriste internet na različite načine, roditeljima je teško da postavе univerzalne smernice koje će odgovarati svim njihovim potomcima. Na primer, dok starija deca (11 do 14

godina) mogu biti više zainteresovana za društvene mreže i aplikacije kao što su TikTok, Instagram i YouTube, mlađa deca uglavnom koriste internet za igre i obrazovne aktivnosti. Takođe, starija deca imaju veću sposobnost da se nose sa online izazovima, kao što su cyberbullying i online komunikacija sa vršnjacima, ali im i dalje trebaju odgovarajući nadzor i edukacija o tome kako da se ponašaju odgovorno u digitalnom svetu.

S obzirom na ove različite potrebe i izazove, roditelji sa više dece trebaju imati strategiju koja se prilagođava uzrastu svakog deteta, kao i koristiti različite alate i tehnike zaštite koje će biti efikasne za svaku starosnu grupu. Na primer, roditelji mogu koristiti parental control aplikacije za mlađu decu, dok se za stariju decu mogu koristiti razgovori o sigurnosti na internetu i usmeravanje prema odgovornim online praksama.

Ovaj demografski profil takođe ukazuje na potrebu za obrazovnim programima koji su specifični za roditelje sa više dece, kao i za one koji imaju decu različitih uzrasta. Programi koji se bave digitalnom pismenošću i bezbednošću na internetu mogu pružiti roditeljima praktične smernice o tome kako da prepoznaju i reše specifične probleme koji se javljaju u porodicama sa više dece.

Kroz ovakve inicijative, roditelji mogu postati sigurniji u svom pristupu internetu, osiguravajući da njihova deca budu zaštićena od digitalnih opasnosti, bez obzira na to koliko godina imaju ili kako koriste internet.

Kultura sigurnosti na internetu Iako je očigledno da većina roditelja prepoznaje rizike koji dolaze sa internetom, istraživanje je pokazalo da i dalje postoji značajan jaz između toga što roditelji razumeju i onoga što zaista preduzimaju u praksi u pogledu implementacije sigurnosnih mera. Naime, samo 32% roditelja koristi jake lozinke, što je osnovna zaštita od neovlašćenog pristupa njihovim i dečjim nalozima na internetu. Ovaj podatak jasno ukazuje na to da je sigurnost korisničkih naloga još uvek zanemarena, a lozinke često ne pružaju adekvatnu zaštitu, što povećava rizik od hakovanja i krađe ličnih podataka.

Još zabrinjavajući je podatak da samo 19% roditelja redovno proverava aktivnosti svoje dece na internetu. Iako mnogi roditelji prepoznaju opasnosti kao što su cyberbullying, izloženost neprikladnom sadržaju i interakcija sa nepoznatim osobama, malo roditelja se zaista angažuje u preventivnom nadzoru ili se bavi proaktivnim postavljanjem sigurnosnih postavki. Nedostatak takvog angažovanja može dovesti do toga da deca postanu ranjiva na digitalne pretnje, jer roditelji nisu u mogućnosti da na vreme identifikuju potencijalne rizike ili prepoznaju neprikladan sadržaj.

Ovaj nesklad između razumevanja i delovanja ukazuje na potrebu za povećanjem svesti među roditeljima o efikasnijim metodama zaštite na internetu. Takođe, postoji jasna potreba za edukacijom roditelja o praktikama i alatima zaštite koji mogu značajno poboljšati sigurnost na internetu, kao što su aparati za roditeljsku kontrolu, praćenje online aktivnosti i postavljanje ograničenja za pristup određenim sadržajima.

Osim toga, istraživanje sugeriše da roditelji nisu u dovoljnoj meri informisani o postojećim tehnologijama i strategijama za zaštitu dece na internetu. Na primer, mnogi roditelji nisu svesni naprednih sigurnosnih alata kao što su aplikacije za praćenje i filtriranje sadržaja ili tehnike za zaštitu privatnosti kao što su korišćenje VPN-a ili anonimnih internet pregledača.

Aktivna participacija roditelja u digitalnim aktivnostima svoje dece takođe zahteva otvoreni dijalog o sigurnosnim pitanjima. U tom kontekstu, od esencijalnog je značaja da se razvije kultura komunikacije između roditelja i dece o tome šta je sigurno, a šta nije na internetu. Roditeljski nadzor ne bi trebao biti shvaćen kao preterana kontrola, već kao partnerstvo u edukaciji i zaštiti dece od mogućih opasnosti.

Povećanje roditeljske svesti o digitalnoj bezbednosti treba da bude prioritet u budućim inicijativama. To uključuje organizovanje obuka i radionica za roditelje, distribuciju edukativnih materijala i razvoj platformi koje bi omogućile roditeljima da se lakše upoznaju sa osnovama internet sigurnosti i metodama preventivnog nadzora.

U zaključku, ključni izazov leži u tome što roditelji, uprkos razumevanju opasnosti, često ne primenjuju dovoljan broj sigurnosnih mera. Samo povećana edukacija i podrška roditeljima mogu doprineti stvaranju sigurnijeg digitalnog okruženja za decu u Vranju.

4.2. Preporuke za dalji rad

Na osnovu utvrđenih zaključaka, preporučuje se da roditelji u Vranju unaprede svoju edukaciju o digitalnoj bezbednosti, jer je očigledno da, iako prepoznaju opasnosti, nisu dovoljno informisani o konkretnim merama zaštite. S obzirom na to da su deca sve više izložena digitalnom svetu, roditelji treba da budu aktivno uključeni u nadgledanje i oblikovanje digitalnih navika svoje dece.

Preporučuje se organizovanje edukativnih radionica za roditelje, koje bi se fokusirale na ključne aspekte digitalne bezbednosti, kao što su sigurnost na internetu, postavljanje privatnih postavki na društvenim mrežama, prepoznavanje potencijalnih online prijetnji, kao i kako prepoznati i reagovati na opasne situacije poput cyberbullying-a ili izlaganja neprimerenom sadržaju. Edukacija treba da bude interaktivna, sa konkretnim primerima i alatima koje roditelji mogu primeniti u svakodnevnom životu.

Takođe, roditeljima se preporučuje da razviju proaktivan pristup prema digitalnim aktivnostima svoje dece. To podrazumeva redovno proveravanje sa kim se njihova deca povezuju online, koje platforme koriste i šta je sadržaj kojem su izloženi. Važno je da roditelji postave jasna pravila korišćenja interneta, kao i da budu u stalnom dijalogu sa decom o tome šta rade na internetu, sa posebnim naglaskom na to kako da se ponašaju u digitalnom okruženju i kako da prepoznaju potencijalno opasne situacije.

Uz to, roditelji treba da nauče kako da koriste alatke i postavke zaštite koje nude različite platforme i aplikacije, kao što su postavljanje privatnosti na društvenim mrežama, upotreba roditeljskih kontrola, kao i kreiranje sigurnih lozinki. Preporučuje se i korišćenje edukativnih aplikacija i resursa koji mogu pomoći

roditeljima da bolje razumeju kako tehnologija utiče na decu i kako da ih zaštite. Ovaj sveobuhvatan pristup može značajno doprineti smanjenju rizika i povećanju digitalne pismenosti među roditeljima i deci.

Edukacija o digitalnoj bezbednosti treba da postane sastavni deo školskih programa, kako bi deca od najranijeg uzrasta razvila odgovoran i kritički pristup prema svom ponašanju na internetu. S obzirom na to da je internet neizbežan deo života savremenih generacija, deca moraju naučiti kako da prepoznaju i reše potencijalne opasnosti koje vrebaju online. Programi edukacije treba da obuhvate teme kao što su sigurnost na internetu, zaštita ličnih podataka, prevencija cyberbullying-a, razumevanje posledica deljenja neprimerenog sadržaja, kao i etičko ponašanje u digitalnim interakcijama. Ovi programi bi trebali biti prilagođeni uzrastu dece, sa posebnim akcentom na razvoj digitalne pismenosti, koja je danas ključna za snalaženje u savremenom društvu.

Škole treba da organizuju interaktivne radionice i edukativne sesije za roditelje i decu, kako bi svi učesnici postali svesni potencijalnih opasnosti i kako da preduprede rizične situacije. Radionice za roditelje mogu se fokusirati na upoznavanje sa alatima i postavkama zaštite, savete o tome kako da prate aktivnosti svoje dece na internetu, kao i kako da usmere svoju decu ka sigurnim i edukativnim sadržajima. S obzirom na to da mnogi roditelji nisu u potpunosti upoznati sa svim rizicima i tehnologijama koje deca koriste, ove radionice mogu biti ključne za povećanje njihove svesti i angažmana u zaštiti digitalne bezbednosti.

Takođe, predlaže se uključivanje stručnjaka iz oblasti digitalne sigurnosti u obrazovni sistem, koji će deci i roditeljima pružiti potrebne savete, informacije i alate za sigurnije kretanje kroz digitalni svet. Stručnjaci mogu održavati edukativne seminare, kreirati priručnike, kao i obezbediti konkretne primere na temelju stvarnih situacija sa interneta. Pored toga, stručnjaci mogu pomoći učiteljima i roditeljima da pravilno

interpretiraju nove tehnologije, kao i da postave efikasne strategije za prevenciju potencijalnih online opasnosti. Ovaj multidisciplinarni pristup je ključan za obezbeđivanje sigurne i obrazovane online zajednice, u kojoj će deca biti odgovorna, svesna rizika i sposobna da se zaštite na internetu.

Lokalna zajednica igra ključnu ulogu u organizaciji edukativnih programa i kampanja koje se bave temom digitalne bezbednosti, jer je njen angažman od esencijalnog značaja za kreiranje sigurnog okruženja za decu i roditelje. Preporučuje se da opštinske vlasti aktivno investiraju u besplatne kurseve i radionice za roditelje i decu, kako bi se povećala svest o digitalnim opasnostima i razvile veštine za zaštitu dece na internetu. Ovi kursevi mogu pokriti osnovne aspekte digitalne bezbednosti, kao što su postavljanje privatnih postavki, prepoznavanje opasnosti na internetu, kao i edukacija o digitalnom identitetu i zaštiti ličnih podataka. Besplatne edukativne inicijative su ključne, jer omogućavaju pristup svim roditeljima, bez obzira na njihov socijalno-ekonomski status, i osiguravaju da svi imaju iste šanse da postanu odgovorni korisnici interneta.

Pored toga, lokalna zajednica može podržati inicijative koje promovišu sigurnost na internetu i angažovanje na prevenciji digitalnih pretnji. Opštinske vlasti mogu sarađivati sa školama, organizacijama i stručnjacima za digitalnu sigurnost kako bi organizovale kampanje koje će podići svest o problemima kao što su cyberbullying, online predatori, i zaštita privatnosti na internetu. Kampanje mogu biti sprovedene kroz različite medije (npr. plakate, bilborde, lokalne novine, i društvene mreže), kao i kroz organizovane javne događaje, koji će omogućiti građanima da se informišu o sigurnosnim praksama na internetu.

Lokalna zajednica takođe može obezbediti resurse i savete roditeljima kako bi im pomogla da postave odgovarajuće sigurnosne mere u svojim domovima. Ovo može uključivati besplatne savete o tome kako koristiti roditeljske kontrole, kako da se povežu sa sigurnosnim alatima dostupnim na internetu, kao i kako

da razviju pravila za korišćenje tehnologije u porodici. Lokalne organizacije mogu pružiti i konkretne materijale, kao što su vodiči ili priručnici, koji roditeljima olakšavaju implementaciju digitalnih sigurnosnih praksi u svakodnevnom životu. Na ovaj način, zajednica može osigurati da svi članovi porodice, od roditelja do dece, budu bolje informisani o digitalnoj bezbednosti i razviju odgovorne navike u online svetu.

Osim toga, lokalne vlasti mogu saradivati sa školama u izradi lokalnih politika zaštite na internetu koje bi uključivale konkretne smernice i protokole za zaštitu dece u digitalnom okruženju, a takođe mogu obezbediti sredstva za pružanje tehničke podrške roditeljima i nastavnicima, kako bi svi bili u mogućnosti da efikasno zaštite decu od digitalnih pretnji. Angažman lokalne zajednice u ovom procesu je ključan za stvaranje holističkog pristupa u očuvanju digitalne bezbednosti, kao i za izgradnju otpornog društva koje je svesno potencijalnih opasnosti u digitalnom svetu.

5.Zaključci sa fokus grupa na temu bezbednosti na internetu

Fokus grupa 1: Mladi (15-18 godina)

Pitanja postavljena učesnicima:

1. Kako se osećate u vezi sa zaštitom privatnosti na internetu?
2. Koje su najčešće opasnosti sa kojima ste se susreli na društvenim mrežama?
3. Kako se štitite od cyberbullyinga?
4. Da li koristite zaštitu kao što su dvostruka autentifikacija ili jakih lozinki?
5. Kako biste reagovali na sumnjivu poruku ili zahtev za prijateljstvo od nepoznate osobe?

Odgovori učesnika:

<i>Privatnost</i>	Mnogi su naglasili da postavljaju stroga pravila o tome šta deli sa drugima na mreži. Neki su istakli da je važno postaviti naloge kao privatne, dok su drugi rekli da koriste anonimnost na internetu, kako bi zaštitili svoje podatke.
<i>Opasnosti</i>	Učesnici su pominjali najčešće opasnosti kao što su prevara i cyberbullying. Iako su svest o tim opasnostima imali, većina njih nije bila u potpunosti sigurna kako da prepozna i izbegne malveri i lažne ponude.
<i>Zaštita</i>	Većina mladih učesnika koristi dvostruku autentifikaciju na društvenim mrežama, a neki su naglasili kako je važno postaviti jake lozinke i koristiti različite lozinke za različite naloge.
<i>Reakcija na sumnjive zahteve</i>	Većina je rekla da nikada ne bi prihvatila prijateljstvo od nepoznate osobe, i da bi ignorisali sumnjive poruke.

Zaključci iz prve fokus grupe:

- Mladi ljudi su svesni osnovnih rizika na internetu, ali im je potrebna dodatna edukacija o prepoznavanju sofisticiranijih prevara i zaštiti od malvera.
- Preporučuje se povećanje edukacije o cyberbullyingu i odgovornom ponašanju na društvenim mrežama.
- Iako koriste sigurnosne alate kao što su dvostruka autentifikacija i jake lozinke, učesnici su izrazili potrebu za boljim razumevanjem zaštite svojih podataka.

Fokus grupa 2: Stariji učesnici (30-50 godina)

Pitanja postavljena učesnicima:

1. Kako se ponašate kada koristite društvene mreže i internet u svakodnevnim situacijama?
2. Da li koristite online bankarstvo i kako se zaštitite pri korišćenju ovih usluga?
3. Kako se zaštitite od virusa i malvera na vašim uređajima?
4. Šta mislite o upotrebi antivirusnih programa i redovnom ažuriranju softvera?
5. Koje korake preduzimate kada sumnjate na prevaru ili zlonameran e-mail?

Odgovori učesnika:

Ponašanje na internetu	Stariji učesnici ističu da se trude da budu oprezni u pogledu privatnosti na internetu, ali se suočavaju sa problemima u razumevanju tehničkih aspekata zaštite. Mnogi koriste društvene mreže, ali su postavili stroga pravila za deljenje ličnih podataka.
Online bankarstvo	Učesnici su istakli da koriste online bankarstvo, ali se strogo pridržavaju sigurnosnih protokola, kao što je proveravanje HTTPS oznaka na stranicama i nikada ne unose podatke na nesigurnim sajtovima.
Zaštita od virusa i malvera	Većina starijih učesnika koristi antivirusne programe i smatraju da su oni ključni za bezbednost njihovih uređaja. Takođe, smatraju redovno ažuriranje softvera vrlo važnim.
Reakcija na prevaru	Ako dobiju sumnjiv e-mail ili poruku, većina njih prvo proverava izvor i nikada ne klikće na sumnjive linkove. Mnogi se konsultuju sa stručnjacima za IT sigurnost pre nego što preduzmu bilo kakvu akciju.

Zaključci iz druge fokus grupe:

- Stariji ljudi su generalno svesni rizika na internetu i koriste zaštitu kao što su antivirusni programi i sigurnosne protokole za online bankarstvo. Međutim, i dalje postoji potreba za dodatnim obrazovanjem o prepoznavanju sofisticiranijih online prevara.
- Veliki broj učesnika ne koristi društvene mreže u potpunosti, zbog straha od gubitka privatnosti, ali se sve više upoznaju sa osnovnim sigurnosnim merama.
- Učesnici ove fokus grupe često upotrebljavaju Internet i računare za osnovne svakodnevne aktivnosti, pa je važna njihova edukacija o tome kako se zaštititi od potencijalnih prijetnji na internetu.

Opšti zaključci sa obe fokus grupe:

1. Svest o bezbednosti na internetu: Iako su mladi i stariji učesnici svesni osnovnih opasnosti na internetu, postoji značajna razlika u nivou razumevanja naprednijih prijetnji, kao što su sofisticirane prevare, malveri i napadi na online bankarstvo. Mladi su skloniji korišćenju modernih sigurnosnih alata kao što su dvostruka autentifikacija, dok stariji učesnici više koriste osnovne antivirusne programe.
2. Obrazovanje o sigurnosti: Potrebno je sprovesti dodatne edukacije, kako za mlade, tako i za starije korisnike, o prepoznavanju i zaštiti od naprednih prevara, lažnih sajtova i phishing napada.
3. Zajednički izazovi: I u jednoj i u drugoj grupi postoji potreba za većim razumevanjem tehničkih aspekata zaštite, kao što su postavke privatnosti na društvenim mrežama, identifikacija sigurnih sajtova i pravilna zaštita lozinkama.
4. Zaštita ličnih podataka: Učesnici obe grupe su saglasni da je zaštita privatnosti ključna i da je potrebno biti oprezan sa deljenjem ličnih informacija na internetu.

6.Izjave sa fokus grupa za bezbednost na netu

Mladji učesnici:

1. Jovana, 17 godina:

"Često koristim društvene mreže, ali sam postala mnogo opreznija otkako sam čula o svim prevarama koje se događaju online. Znam da nikada ne bih trebalo da delimo lične informacije ili da prihvatim prijateljstvo sa nekim koga ne poznajem."

"Mislim da je važno postaviti privatnost na visok nivo. Nemam ništa protiv deljenja slika, ali samo sa ljudima kojima verujem."

2. Marko, 16 godina:

"Nikada ne klikćem na linkove koje ne prepoznam. Mnoge pretrage na internetu mogu biti lažne i da vas navode na stranice koje preteče vašim uređajima. Prošle godine sam imao problem sa virusima zbog jedne takve greške."

"Koristim dva faktora autentifikacije na svim nalogima jer mislim da je to najbolji način da se zaštitim."

3. Teodora, 18 godina:

"Društvene mreže mogu biti super, ali takođe mogu biti i opasne ako ne postaviš jasne granice. Moja prijateljica je imala loše iskustvo sa nekim ko ju je maltretirao na internetu, pa sada pazimo šta postavljamo i kome šaljemo poruke."

"Savete koje sam dobila o cyberbullyingu pomažu mi da budem pažljivija prema onome što pišem i kako se ponašam online."

4. Nikola, 15 godina:

"Na internetu sam puno naučio o bezbednosti i o tome kako prepoznati rizične situacije. Nikada ne bih razmenjivao lozinke ili šifre sa nekim. Slučajevi hakovanja su mi došli do ušiju i sad se trudim da budem oprezniji."

"Bitno je da se postavi privatnost na svim aplikacijama koje koristim. Tako ne moram da brinem o tome ko može da vidi moje slike ili informacije."

5. Ana, 17 godina:

"Online je lako da se neko pretvara da je neko drugi, pa mi je jasno da je potrebno biti oprezan. Ako me neko ne poznaje, ne šaljem mu ništa lično, ni slike, ni informacije."

"Svi moji prijatelji znaju da ne klikću na sumnjive linkove, jer postoji mnogo virusa i malvera koji mogu da unište uređaje. Moj savet je uvek da proverimo svaki link pre nego što nešto otvorimo."

Stariji učesnici:

6. Marija, 30 godina:

"Kao roditelj, trudim se da edukujem svoju decu o bezbednosti na internetu. Smatram da je važno da znaju da sve što postavite na mreži može biti trajno. Takođe im stalno skrećem pažnju na opasnosti od cyberbullyinga."

"Odrasli ljudi, uključujući nas, takođe moraju biti oprezni sa internetom. Hakeri koriste društvene mreže da bi došli do ličnih informacija, i to je nešto što ne smemo da zanemarimo."

7. Ivan, 45 godina:

"Kada koristim internet za online kupovinu ili bankarske usluge, uvek proverim sigurnost stranice, tražim HTTPS i ne unosim podatke na sajtovima koji izgledaju sumnjivo."

"Zaštita od online prevara postala je ključna. Koristim antivirusne programe, a takođe redovno ažuriram softver na svim uređajima kako bih se zaštitio od potencijalnih napada."

8. Jelena, 39 godina:

"Sa svim ovim novim tehnologijama, veoma je lako da neko upadne u vaše lične podatke. Mislim da bi svi, uključujući decu i mlade, trebali biti educirani o važnosti postavljanja jakih lozinki i zaštite privatnosti na internetu."

"Moj savet za mlade je da nikada ne prihvataju prijateljstva online od nepoznatih osoba. Takođe, važno je znati kako prepoznati prevarante i kako se nositi sa nepoželjnim porukama."

9. Stefan, 52 godine:

"Nedavno sam bio meta prevara, neko je pokušao da mi ukrade lične podatke putem e-maila. Od tada sam postao mnogo pažljiviji u vezi sa svim vezama koje imam na internetu, bilo da su to društvene mreže, e-mailovi ili online kupovina."

"Verujem da je edukacija o sigurnosti na internetu nešto što bi trebalo da bude obavezno. Mladi ljudi treba da znaju kako da zaštite sebe i svoje podatke od raznih online prijetnji."

10. Dragana, 40 godina:

"Priznajem da se nisam mnogo bavila pitanjem bezbednosti na internetu dok nisam imala iskustva sa virusima na svom računaru. Od tada sam postavila sve potrebne zaštite na svim uređajima. U porodici imamo pravilo da se svi informišemo o novim opasnostima na internetu."

"Mladi moraju da shvate da internet nije uvek bezbedno mesto. Savetujem im da uvek paze šta postavljaju, a posebno ko može videti njihove informacije. Privatnost je ključna."

SADRŽAJ

1.UVOD.....	4
2.METODOLOGIJA	6
3. REZULTATI ISTRAŽIVANJA	7
3.1.Polna struktura ispitanika	7
3.2.Starosna struktura roditelja	8
3.3.Broj dece.....	9
3.4.Uzrast dece	10
3.5.Vreme provedeno na internetu.....	11
3.6. Najčešće korišćene platforme	12

3.7. Neprijatna iskustva	13
3.8. Mere bezbednosti.....	14
4. ZAKLJUČCI I PREPORUKE ISTRAŽIVANJA	15
4.1. Zaključci istraživanja.....	15
4.2. Preporuke za dalji rad	24
5. Zaključci sa fokus grupa na temu bezbednosti na internetu	28
Fokus grupa 1: Mladi (15-18 godina).....	28
Fokus grupa 2: Stariji učesnici (30-50 godina).....	31
6. Izjave sa fokus grupa za bezbednost na netu	35



