

Sigurnost na internetu kod adolescenata



Odgoj danas za sutra:

Premošćivanje jaza između učionice i realnosti

3. međunarodna znanstvena i umjetnička konferencija
Učiteljskoga fakulteta Sveučilišta u Zagrebu Suvremene
teme u odgoju i obrazovanju – STOO4 u suradnji s
Hrvatskom akademijom znanosti i umjetnosti

Ružica Filipović

*Učiteljski fakultet Sveučilišta u Zagrebu, Hrvatska
ruzica.filipovic91@gmail.com*

**Sekcija - Odgoj i obrazovanje za
digitalnu transformaciju**

Broj rada: 43

Kategorija: Izvorni znanstveni rad

Sažetak

Korištenje interneta značajno je poraslo u posljednjih dvadesetak godina, no s tim rastom pojavila se zabrinutost oko problematičnog korištenja interneta koje može uzrokovati psihičke poteškoće. Ovo uključuje aktivnosti poput videoigara, društvenih medija, web-streaminga i online kupovine, a posebno su djeca i adolescenti izloženi rizicima. Cilj ovog istraživanja bio je ispitati razlike, s obzirom na vrstu srednje škole, između stvarnog rizičnog ponašanja adolescenata na internetu i njihove samoprocjene te razinu svijesti o informacijskoj sigurnosti. Istraživanje je provedeno u srednjim školama Sisačko-moslavačke županije na uzorku od 167 učenika prosječne dobi od 16,5 godina, koristeći Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS). Upitnik mjeri rizična ponašanja i svijest o sigurnosti putem 17 varijabli raspoređenih u četiri subskale. Rezultati su pokazali visoku pouzdanost upitnika (Cronbachova alfa = 0,81), a zbog odstupanja podataka od normalne distribucije, korišten je neparametrijski test Mann-Whitney U. Rezultati su pokazali da nema statistički značajnih razlika u rizičnom ponašanju između različitih vrsta srednjih škola, osim u specifičnim područjima kao što su privola za obradu osobnih podataka i provjera prijenosnih medija. Statistički značajna razlika su uočene u svijesti o sigurnosti na internetu, gdje su učenici gimnazijskog smjera pokazali bolje znanje o održavanju zaštite i sigurnosnim praksama. Zaključno, iako učenici imaju pristup edukativnim programima o sigurnosti na internetu unutar školskog sustava, potrebno je dodatno raditi na podizanju svijesti i smanjenju rizičnih ponašanja kod adolescenata.

Ključne riječi:

adolescenti; BKUIS; internet; sigurnost na internetu; rizična ponašanja

Uvod

Korištenje interneta u posljednjih dvadesetak godina uvelike je poraslo u cijelom svijetu (Pettorruso i sur., 2020). Pojam sigurnost na internetu obuhvaća pitanja koja se odnose na fizičku i psihološku dobrobit korisnika Interneta. Istodobno, povećano korištenje interneta izazvalo je zabrinutost zbog njegovog problematičnog korištenja, jer se često povezuje s ozbiljnim psihičkim

tegobama (Aboujaoude, 2010; Spada, 2014). Jedan od aspekata rizika povezanih s internetom je problematično korištenje interneta. Problematično korištenje interneta definira se kao korištenje interneta koje stvara psihološke, socijalne, školske i/ili radne poteškoće u životu osobe (Beard i Wolf, 2001), a ono može uključivati različite oblike neprimjerenog ponašanja, videoigre, korištenje društvenih medija, web-streaming, gledanje pornografije i kupnju. Unatoč tome, koncept problematično korištenja interneta prkosi jasnoj mjerljivoj definiciji i to može odražavati heterogenost i složenost fenomena. Grant i sur. (2014) navode da ostaje nejasno zadovoljavaju li svi oblici problematičnog korištenja interneta iste fiziološke kriterije, kao što su tolerancija i odvikavanje ili čak je li problematično korištenje interneta samostalan poremećaj ili potiče druge oblike ovisnosti. Alternativno, neka ponašanja problematičnog korištenja interneta mogu dijeliti sličnosti s poremećajima povezanim s opsesivno-kompulzivnim poremećajima (npr. opetovano provjeravanje e-pošte ili društvenih medija) ili socijalnim anksioznim poremećajem (npr. pretjerano korištenje društvenih medija kao izbjegavanje društvenog kontakta licem u lice) (Chamberlain i sur., 2018; Ioannidis i sur., 2016).

Budući da problematično korištenje interneta može imati ozbiljne posljedice, važno je razumjeti kako ono utječe na djecu i adolescente, koji su često izloženi specifičnim rizicima tijekom korištenja digitalnih platformi. Núñez-Gómez i sur. (2021) ističu da, s obzirom na to da djeca i adolescenti često konzumiraju sadržaje na internetu i aktivno sudjeluju na društvenim mrežama, potrebno je poznavati rizike kako bi se provela kritička analiza usmjerena na zaštitu i razumijevanje njihove uporabe ovih platformi. Istraživanje koja je provela Livingstone i sur. (2011) u 25 zemalja Europske unije pokazuju kako roditelji podcjenjuju rizike kojima su djeca izložena na internetu te samo 5 % roditelja smatra da je dijete odalo određenu osobnu informaciju, dok u stvarnosti to čini gotovo 50 % djece. Nadalje, samo 7 % roditelja misli kako se njihovo dijete susrelo sa seksualnim komentarima na internetu, a samo 4 % roditelja misli kako je njihovo dijete bilo zlostavljano na internetu dok su izjave djece o navedenim događajima dvostruko su češće. Roditelji najviše podcjenjuju probleme koje doživljava najstarija dobna skupina (Livingstone i Bober, 2006). Prema istraživanju Núñez-Gómez i sur. (2021) provedenom na 1350 djece i adolescenata između 6 i 12 godina koji žive u Španjolskoj, javlja se međugeneracijska napetost između odraslih i djece u korištenju interneta te teškoće u postizanju konsenzusa i kvalitetne podrške pri korištenju interneta. Zaključuju da se djeci moraju dati digitalni alati, kompetencije i sigurnost kako bi ona u potpunosti razvila svoj digitalni identitet. Unatoč tome što roditelji često podcjenjuju rizike s kojima se njihova djeca susreću na internetu, istraživanja pokazuju da je važno pronaći ravnotežu između omogućavanja pristupa digitalnim resursima i zaštite djece od potencijalnih opasnosti. Korištenje interneta pruža brojne prednosti mladima uključujući povećanu društvenu podršku, akademsko obogaćivanje i međukulturalne interakcije širom svijeta, ali postoje i popratni rizici za korištenje interneta (Anderson, 2001; Colley i Maltby, 2008; Goold i sur., 2003; Hunley i sur., 2005; Joiner i sur., 2005). Današnju djecu možemo smatrati djecom „digitalne generacije“ (Despotovic i sur. 2011). Adolescenti također često dijele osobne i identifikacijske informacije o sebi na internetu. Ti detalji mogu uključivati lokaciju njihovog doma, fotografije koje otkrivaju ili opise seksualnog ponašanja i upotrebe supstanci (Back i sur., 2010; Hinduja i Patchin, 2008; Moreno i sur., 2009). Istaknutost i značaj društvenih medija za adolescente, stoga, vjerojatno proizlazi iz sve veće važnosti istraživanja identiteta, samoizražavanja, prijateljstava i prihvaćanja od strane vršnjaka koje se događa tijekom ovog razdoblja (Gerwin, Kaliebe i Daigle, 2018). Razumijevanje odnosa između korištenja društvenih medija i rizičnog ponašanja tijekom adolescencije je ključno (Casey, 2015; Shulman i sur., 2016).

Iako internet može donijeti mnoge koristi, kao što su društvena podrška i obogaćivanje obrazovanja, važno je razumjeti rizike povezane s njegovim korištenjem, posebno u kontekstu adolescenata. U tom smislu, digitalne navike mladih ljudi postaju ključne za očuvanje njihove sigurnosti. Naime, djeca koja provode više vremena na internetu često nisu dovoljno svjesna opasnosti poput izlaganja osobnih podataka, što zahtijeva razvoj digitalnih kompetencija i odgovornosti. Posljednjih godina pojavilo se zlostavljanje putem digitalnih uređaja koristeći internet, koje se često zajednički naziva *cyberbullying*. Odgovarajuća definicija je da je to agresivan, namjeran čin koji izvodi grupa ili pojedinac, koristeći elektroničke oblike kontakta, opetovano i tijekom vremena protiv žrtve koja se ne može lako obraniti (Smith i sur., 2008). *Cyberbullying* ili internetsko nasilje utječe na do trećinu mladih i povezuje se s raznim zdravstvenim problemima, od kojih su neki ozbiljni, kao što su suicidalne misli (Agatston i sur., 2007; Hinduja i Patchin, 2010; Ybarra i sur., 2007). Odnosi se na verbalnu agresiju, neprijateljstvo i druge pokušaje nanošenja štete u online komunikaciji i obuhvaća izraze kao što su *flaming*, *outing*, govor mržnje, online drama i *online* uznemiravanje (Calvete i sur., 2010; Pyżalski, 2012). Može uključivati objavljivanje lažnih profila, distribuciju klevetničkih informacija i internetsko uhođenje (Rivers i Noret, 2010). Osim fizičkih prijetnji i prijetnji domu, obitelji i prijateljstvima, opće je poznato da velik dio internetskog nasilja (poput zlostavljanja licem u lice) ima seksualne komponente, uključujući seksualno uznemiravanje te homofobno i seksističko omalovažavanje (Ehman i Gross, 2019). Govor mržnje i predrasuda je također čest (Henry, 2013). Mrežno zlostavljanje, uznemiravanje, agresija i uhođenje također se pojavljuju u kontekstu adolescentskih veza, među školskim vršnjacima i u vezama započetim na internetu (Rivers i Noret, 2010; Stonard i sur., 2014). Dredge i sur. (2014) navode da su posljedice internetskog nasilja štetnije od tradicionalnog vršnjačkog nasilja zbog sveprisutnog javnog objavljivanja uvredljivih komentara i veće publike koja svjedoči nasilju, anonimnosti zlostavljača, trajnosti i snage pisane riječi ili objavljene fotografije, mogućnosti da se žrtvu zlostavlja neprestano tijekom cijelog dana kao i nemogućnost bijega žrtve.

Osim *cyberbullyinga*, postoje i drugi oblici digitalnih prijetnji koje mogu utjecati na mentalno zdravlje i sigurnost djece i adolescenata, a njihovo razumijevanje ključno je za izradu učinkovitih strategija zaštite. Sigurnost na internetu vrlo je važna za današnju mladež jer provode i do 10 sati dnevno koristeći različite oblike medija (Jones i sur., 2009; Lenhart i sur., 2010; Rideout i sur., 2010). Prema autorima Puri i Sgarma (2016) i Zeng i sur. (2016) što više vremena djeca i adolescenti provode na internetu, osjećaju se usamljenijima. Autori Šolić i Velki (2019) navode kako se dobna granica prvog pristupanja internetu spušta diljem Europe. Prema istraživanju Livingston i sur. (2011) u Danskoj i Švedskoj je prosječna dob sedam godina, dok je u nekim zemljama osam godina (Norveška, Velika Britanija itd.). U nekim zemljama poput Austrije, Turske ili Portugala, je prosječna dob djece koja prvi put pristupaju internetu, deset godina. „Budući da se sve mlađa i mlađa djeca počinju koristiti internetom, internetske sigurnosne kampanje i inicijative moraju biti usmjerene i prilagođene mlađim dobnim skupinama, a istodobno održavati postojeće napore vezane uz sigurnost starije djece“ (Šolić i Velki, 2019). Pojam sigurnost na internetu se također naziva i mrežna sigurnost, digitalna sigurnost ili e-sigurnost, a ovaj koncept povezuje se s rizicima s kojima se pojedinci suočavaju na internetu i načinima na koje se mogu zaštititi od tih rizika (Kimpe i sur., 2019). S obzirom na sveprisutnost interneta u životima kod djece i adolescenata, raste i zabrinutost za njihovu sigurnost na internetu. Pružanje sigurnog okruženja zahtijeva dubinsko razumijevanje vrsta i rasprostranjenosti internetskih rizika s kojima se mladi korisnici interneta suočavaju, kao i najučinkovitijih rješenja za ublažavanje tih rizika (Farrukh i sur., 2014).

Povijesno gledano, sigurnost na internetu, se uglavnom smatrala tehničkim problemom fokusiranim na hardverska i softverska rješenja (Parsons i sur., 2014), ali mnogi autori smatraju da su mnogi sigurnosni problemi uzrokovani upravo ljudski faktorom (Lukasik, 2011; Orshesky, 2003; Sasse i sur., 2001).

S obzirom na to da djeca provode sve više vremena na internetu, istraživanja na nacionalnoj razini pokušavaju utvrditi obrasce digitalnog ponašanja i sigurnosne prijetnje s kojima se mladi susreću u Hrvatskoj. Na razini Republike Hrvatske 2014. godine je provedeno Nacionalno istraživanje o ponašanju korisnika na internetu te znanju o pitanjima sigurnosti i privatnosti na uzorku od 4859 sudionika, od kojih su trećina bili srednjoškolci, trećina studenti i trećina zaposleni odrasli ljudi. Istraživanje je pokazalo kako unatoč znanju, većina ljudi je lakovjerna, ali se i sigurnosno izrazito riskantno ponaša. Većina ljudi je odala svoju lozinku na trik pitanju dobrovoljno (Šolić i Velki, 2019). Prvo hrvatsko istraživanje o digitalnim navikama djece i sigurnosti na internetu provedeno je 2017. godine, a sudjelovalo je 1.017 djece u dobi od 9 do 17 godina te njihovi roditelji, a provedeno je u sklopu projekta *EU (Global) Kids Online*. Utvrđeno je da djeca pristupaju internetu kada žele i trebaju najčešće putem pametnih telefona, ali i dalje više vremena provode družeći se uživo s prijateljima, količina vremena provedenog uz Internet raste s dobi, a djeca koja među svojim Facebook prijateljima imaju svoje roditelje češće posjećuju društvene mreže i komuniciraju s drugima putem aplikacija (Ciboci i sur., 2020).

Tijekom osnovnoškolskog i srednjoškolskog obrazovanja, učenici se susreću s temama sigurnosti na internetu kroz nastavne predmete Hrvatski jezik i Informatika propisane predmetnim kurikulumima koji su utemeljeni na nacionalnom okvirnom kurikulumu. Osim škola, u Republici Hrvatskoj postoji i Nacionalni centar za sigurniji Internet koji svojim djelovanjem želi upozoriti djecu i mlade na rizike i opasnosti svakodnevnog korištenja interneta

Cilj i metode istraživanja

Cilj

S obzirom na mali broj znanstvenih istraživanja o sigurnosti na internetu među djecom i adolescentima u Republici Hrvatskoj, cilj istraživanja je ispitati razlike između stvarnog rizičnog ponašanja adolescenata na internetu i samoprocjene, utvrditi razinu svijesti o informacijskoj sigurnosti i potencijalnim rizicima te analizirati u kojoj se mjeri pridržavaju važnosti sigurnosnih preporuka prilikom korištenja računalnih sustava. Poseban naglasak stavljen je na utjecaj edukacija o sigurnosti na internetu koje učenici pohađaju tijekom svog osnovnoškolskog i srednjoškolskog obrazovanja.

BKUIS

U ovom istraživanju korišten je Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS), koji su razvili i validirali Velki i Šolić (2020). Upitnik sadrži 17 varijabli raspoređenih u četiri subskale: dvije bihevioralne (samoprocjena rizičnog ponašanja i simulacija rizičnog ponašanja) i dvije kognitivne (kognitivni rizik i kognitivna važnost). Bihevioralne skale mjere rizična ponašanja ispitanika, dok kognitivne skale procjenjuju razinu svijesti o rizicima internetske sigurnosti.

Primjeri varijabli uključuju učestalost dijeljenja lozinki i percepciju rizika od krađe novca prilikom korištenja internetskog bankarstva. Rezultati simulacijskih subskala izražavaju se kao zbroj odgovora (0-4), dok se za ostale subskale koristi aritmetička sredina. Rezultati se kreću od 0 (nema rizičnih ponašanja) do 4 (maksimalna rizična ponašanja i visoka svjesnost o rizicima).

Uzorak

U istraživanju je sudjelovalo 167 učenika srednjih škola, od čega 57 iz gimnazija i 110 iz strukovnih škola s prosječnom dobi od 16,5 godina. Korišten je izvorni faktorski model, a koeficijent pouzdanosti tipa Cronbachov alpha, za svih 17 varijabli, iznosio je 0,81, što ukazuje na visoku pouzdanost varijabli ($KMO=0,787$, $\chi^2=1709,383$, $df=190$, $p<0,001$) (Tablica 1).

Tablica 1

Prikaz KMO i Bralettovog testa zakrivljenosti

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,787
Bartlett's Test of Sphericity	Approx. Chi-Square	1709,383
	df	190
	Sig.	<,001

Normalnost distribucije podataka provjerena je Kolmogorov-Smirnov testom, koji je pokazao značajno odstupanje od normalne distribucije (Tablica 2) (Steinskog i sur., 2007). Analiza distribucije podataka dodatno potvrđuje ova odstupanja, što je vidljivo iz vrijednosti skewnessa (asimetrije) i kurtosisa (zašiljenosti). Prema kriterijima, ako skewness prelazi ± 1 , distribucija je značajno asimetrična, dok vrijednosti kurtosisa veće od ± 3 ukazuju na odstupanja u zašiljenosti distribucije. U ovom istraživanju, kod više varijabli, poput "Obavijest od suradnika" (skewness = -2,895, kurtosis = 6,460), "Daje lozinku" (skewness = -2,556, kurtosis = 6,009) i "Posuđuje debitnu/kreditnu karticu" (skewness = -4,219, kurtosis = 19,961), jasno je vidljivo značajno odstupanje od normalne distribucije. S obzirom na to da test Kolmogorov-Smirnov potvrđuje ova odstupanja, za daljnju analizu podataka korišten je neparametrijski test Mann-Whitney U, budući da on ne zahtijeva pretpostavku normalnosti distribucije i prikladniji je za analizu ovakvih podataka.

Tablica 2

Deskriptivna statistika i odstupanje od normalne distribucije

	N	Min	Max	Mean	Std. Dev.	Skewness	Std. Error (Skew.)	Kurtosis	Std. Error (Kurt.)
Obavijest od suradnika	167	1	2	1,91	0,287	-2,895	0,188	6,460	0,374
Besplatni antivirus	167	1	4	1,86	0,394	-0,585	0,188	5,909	0,374
Promotivni materijali	167	1	3	1,89	0,311	-2,553	0,188	4,570	0,374

Privola za obradu osobnih podatak a	167	1	3	1,39	0,600	1,285	0,188	0,622	0,374
Posuđuj e podatke	167	2	5	4,44	0,825	-1,358	0,188	0,986	0,374
Daje lozinku	167	2	5	4,72	0,676	-2,556	0,188	6,009	0,374
Razdvaj a privatn o od služben og	167	1	5	4,00	1,349	-1,133	0,188	0,006	0,374
Dozvolj ava kolega ma	167	1	5	4,43	0,908	-1,697	0,188	2,644	0,374
Posuđuj e debitnu/ kreditn u karticu	167	3	5	4,81	0,617	-4,219	0,188	19,961	0,374
Otkriva PIN	167	3	5	4,83	0,658	-4,542	0,188	21,675	0,374
Radi sigurno sne kopije	167	1	5	3,65	1,146	-0,746	0,188	-0,044	0,374
Održava nje zaštite	167	1	5	2,43	1,282	0,554	0,188	-0,922	0,374
Odjavlji vanje	167	1	5	2,72	1,431	0,282	0,188	-1,327	0,374
Provjer avanje prijenos nih medija	167	1	5	2,53	1,260	0,537	0,188	-0,765	0,374
Povrem eno mijenja nje lozinke	167	2	5	2,90	1,228	0,066	0,188	-0,998	0,374

Krađa identite ta	167	1	5	2,09	1,330	0,953	0,188	-0,459	0,374
Krađa novaca	167	1	5	2,02	1,439	1,148	0,188	-0,207	0,374
Hakiranje osobnog računa	167	1	5	2,01	1,329	1,148	0,188	-0,376	0,374
Gubitak privatnih fotografija	167	1	5	2,41	1,394	0,566	0,188	-1,036	0,374
Zloupotreba kreditne ili debitne kartice	167	1	5	1,93	1,459	1,270	0,188	-0,023	0,374

Postupak

Istraživanje je provedeno od ožujka do svibnja 2024. u srednjim školama Sisačko-moslavačke županije, a empirijski podatci su prikupljeni putem anketnog upitnika (Matijević i sur., 2016). Upitnik je izrađen u Microsoft Formsu, uz prethodno pribavljene potrebne suglasnosti za sudjelovanje. Učenici su imali su mogućnost odustati od istraživanja u bilo kojem trenutku. Upitnik je ispunjavan online uz jasne upute, a rezultati su obrađeni statističkim programom IBM SPSS 20 (Brownlow, 2004).

Rezultati

U istraživanju su postavljene četiri hipoteze. Prva hipoteza ispituje razliku između vrsta srednjih škola u procjeni rizičnog online učeničkog ponašanja na simulacijskoj skali te predviđa da postoji statistički značajna razlika između gimnazija i strukovnih škola. S obzirom na to da učenici gimnazija, prema svom kurikulumu, imaju više nastavnih predmeta koji ih podučavaju o sigurnosti na internetu, očekuje se da će njihovi rezultati na simulacijskom testu pokazati nižu razinu rizičnog ponašanja u odnosu na učenike strukovnih škola, čiji programi ne uključuju toliko sadržaja vezanih uz digitalnu sigurnost.

Tablica 3

Usporedba dvije grupe na simulacijskoj skali rizičnog online ponašanja

	Obavijest od suradnika	Besplatni antivirus	Promotivni materijali	Privola za obradu osobnih podataka
--	------------------------	---------------------	-----------------------	------------------------------------

Mann-Whitney U	2978,0000	3072,000	3121,000	2486,000
Wilcoxon W	4631,000	4725,000	9228,000	4139,000
Z	-1,070	-,338	-,075	-2,659
Asymp. Sig. (2-tailed)	,285	,735	,940	,008

a. Grouping Variable: Smjer srednje škole

Na osnovu prikazanih rezultata iz tablica za Mann-Whitney U test (Tablica 3), p-vrijednosti (Asymp. Sig.) su sljedeće: obavijest od suradnika ($p = 0,285$), besplatni antivirus ($p = 0,735$), promotivni materijali ($p = 0,940$), privola za obradu osobnih podataka ($p = 0,008$). U varijablama obavijest od suradnika, besplatni antivirus i promotivni materijali nije utvrđena statistički značajna razlika između gimnazija i strukovnih škola na simulacijskoj skali u procjeni rizičnog ponašanja, time se hipoteza ne može potvrditi. S druge strane, u varijabli privola za obradu osobnih podataka, gdje je p-vrijednost manja od 0.05, postoji statistički značajna razlika, što upućuje na to da vrsta srednje škole može imati različit utjecaj na pojedine aspekte rizičnog online ponašanja. Međutim, s obzirom na cjelokupne rezultate Mann-Whitney U testa, hipoteza se ne može potvrditi jer nije utvrđena statistički značajna razlika između gimnazija i strukovnih škola u procjeni rizičnog online ponašanja na simulacijskoj skali.

Druga hipoteza predviđa postojanje statistički značajna razlike između vrsta srednjih škola u učeničkoj samoprocjeni rizičnog online ponašanja. Prema Panaderu i sur. (2016), samoprocjena se odnosi na širok raspon mehanizama i tehnika pomoću kojih učenici opisuju (tj. procjenjuju) i eventualno dodjeljuju zasluge ili vrijednosti (tj. procjenjuju) kvalitetu vlastitih procesa učenja i proizvoda. Samoevaluacija zahtijeva od učenika da u određenim vremenskim intervalima ocjenjuju vlastito ponašanje (Shapiro i Cole, 1994). Očekuje se da će učenici četverogodišnjih srednjih škola (gimnazija) imati višu razinu samoprocjene rizičnog online ponašanja u usporedbi s učenicima strukovnih škola, pri čemu bi njihova samoprocjena mogla odstupati u odnosu na rezultate simulacijske skale. Jedan od najučinkovitijih pristupa povećanju sigurnosti na internetu među digitalnim građanima jest obrazovanje (Onyancha, 2015; Sharma i sur., 2015; Whittier, 2013). Shui Ng (2020) u svojem pregledu istraživanja ističe važnost edukacije u poboljšanju *online* ponašanja (Dhir i sur., 2016; Hur i sur., 2009; Ncube i Dube, 2016).

Tablica 4

Samoprocjena rizičnog ponašanja po vrsti srednje škole

	Posuđuje podatke	Daje lozinku	Razdvaja privatno od službenog	Dozvoljava kolegama	Posuđuje debitnu/kreditnu karticu	Otkriva PIN	Rai sigurnosne kopije
Mann-Whitney U	2969,500	3065,000	2753,000	2954,500	3016,000	3046,500	2461,000
Wilcoxon W	9074,500	4718,000	4406,000	9059,500	9121,000	9151,500	4114,000
Z	-,645	-,354	-1,420	-,718	-,729	-,602	-2,371
Asymp. Sig. (2-tailed)	,519	,724	,156	,473	,466	,547	,018

Rezultati Mann-Whitney U testa (Tablica 4) pokazuju da su za većinu varijabli osim *Radi sigurnosne kopije*, p-vrijednosti veće od konvencionalnog praga statističke značajnosti od 0,05 (npr. $p = 0,519$, $p = 0,724$, $p = 0,156$, itd.). To znači da nema dovoljno dokaza koji bi potvrdili hipotezu o postojanju statistički značajne razlike u samoprocjeni rizičnog online ponašanja između učenika gimnazija i strukovnih škola. Slijedom toga, hipoteza nije potvrđena. Iako hipoteza nije potvrđena, obrazovni sustav i dalje treba razvijati strategije za edukaciju učenika o sigurnom *online* ponašanju, neovisno o vrsti srednje škole. Cilj je povećati njihovu svijest i razviti sigurne digitalne navike, čime bi se unaprijedila njihova sposobnost prepoznavanja i izbjegavanja potencijalnih rizika na internetu.

Treća hipoteza predviđa postojanje statistički značajne razlike između vrsta srednjih škola u samoprocjeni svijesti učenika o informacijskoj sigurnosti. Škola ima ključnu ulogu u kritičkom digitalnom opismenjavanju učenika i odgovornost ne samo za njihovu edukaciju o sigurnom korištenju interneta već i za informiranje roditelja o dječjem online iskustvu kod kuće. Cilj obrazovanja o sigurnosti na internetu jest osvijestiti korisnike o potencijalnim rizicima povezanim s upotrebom digitalnih alata, uključujući društvene mreže, online igre, e-poštu i razne komunikacijske platforme. Iako postoji značajan broj istraživanja o internetskoj sigurnosti, manje je radova koji se bave konkretnim mjerama koje škole mogu poduzeti za jačanje svijesti o sigurnosti na internetu (Franke i Brynielsson, 2014; Dong i sur., 2015; Kruse i sur., 2017; Mellado i sur., 2010; Rahim i sur., 2015). Uvidom u kurikulare nastavnih predmeta Hrvatski jezik, Informatika ili tehničkih smjerova (poput tehničar za računalstvo), očekuje se da će učenici četverogodišnjih srednjih škola, koji imaju navedene nastavne predmete, imati veće spoznaje o sigurnosti na internetu od učenika strukovnih škola, gdje su ovi predmeti manje zastupljeni ili ih nemaju uopće tijekom srednjoškolskog obrazovanja.

Tablica 5

Samoprocjena razine svjesnosti o važnosti korištenja računalnih sustava i interneta

	Krađa identiteta	Krađa novaca	Hakiranje osobnog računa	Gubitak privatnih fotografija	Zloupotreba kreditne ili debitne kartice
Mann-Whitney U	2483,500	2589,500	2656,000	3135,000	2836,500
Wilcoxon W	4136,500	4242,500	4279,000	9240,000	4489,500
Z	-2,354	-2,042	-1,881	,000	-1,177
Asymp. Sig. (2-tailed)	,019	,041	,060	1,000	,239

Na temelju statističkih rezultata Mann-Whitney U testa i Wilcoxon W testa (Tablica 5), može se zaključiti da postoji statistički značajna razlika u percepciji prijetnji informacijske sigurnosti između učenika različitih vrsta srednjih škola, ali samo za određene varijable. Učenici koji pohađaju škole s naglaskom na IKT ili informatiku pokazuju veću svijest o sigurnosti na internetu u usporedbi s učenicima strukovnih škola, gdje su informatički predmeti manje zastupljeni ili ih uopće nema. Z-vrijednosti, koje su negativne za varijable poput Krađe identiteta ($Z = -2,354$) i Krađe novca ($Z = -$

2,042), ukazuju na statistički značajnu razliku u rangovima između tih skupina. Međutim, za varijable poput Hakiranja osobnog računa, Gubitka privatnih fotografija i Zloupotrebe kreditne ili debitne kartice, p-vrijednosti su veće od 0,05, što znači da te razlike nisu statistički značajne. Dakle, iako se u tekstu navodi postojanje statistički značajnih razlika, ove razlike su statistički značajne samo za varijable u kojima je p-vrijednost manja od 0,05. Ovi nalazi potvrđuju hipotezu da je inkluzija predmeta o sigurnosti na internetu u kurikulum srednjih škola ključna za podizanje svijesti i zaštitu mladih od online prijetnji, s naglaskom na varijable koje su statistički značajne. Ovi rezultati naglašavaju važnost obrazovanja o sigurnosti na internetu u obrazovnom sustavu, no treba imati na umu da nisu sve varijable pokazale značajnu razliku.

Četvrta hipoteza predviđa da postoji statistički značajna razlika u vrsti srednje škole u samoprocjeni svjesnosti potencijalnih rizika kod učenika. Internet je imao značajan pozitivan utjecaj na živote ljudi, ali je također donio brojne izazove, uključujući: *cyberbullying*, online prijevare, rasno zlostavljanje, pornografiju i online kockanja. Nedostatak svijesti i digitalne pismenosti često čini korisnike ranjivima na ove prijetnje. Prema istraživanjima, razina svijesti o sigurnosti na internetu i dalje je niska ili umjerena. Stoga je ključno od najranije dobi razvijati znanja i vještine potrebne za sigurno digitalno okruženje (Rahman i sur., 2020). Rezultati provedenog istraživanja pokazuju da postoji statistički značajna razlika u samoprocjeni svjesnosti potencijalnih rizika među učenicima iz različitih srednjih škola za većinu mjerenih varijabli čime se hipoteza potvrđuje. Ovi nalazi dodatno naglašavaju važnost sustavnog obrazovanja o internetskoj sigurnosti, ne samo u adolescentskoj dobi već i kroz rane stupnjeve obrazovanja.

Tablica 6

Samoprocjena razine svjesnosti potencijalnih rizika

	Održavanje zaštite	Odjavljivanje	Provjeravanje prijenosnih medijai	Povremeno mijenjanje lozinki
Mann-Whitney U	2062,500	2494,500	2365,500	2783,000
Wilcoxon W	3715,500	4147,500	4018,500	4436,000
Z	-3,760	-2,220	-2,686	-1,220
Asymp. Sig. (2-tailed)	<,001	,026	,007	,223

. Grouping Variable: Smjer srednje škole

Rezultati Mann-Whitney U testa (Tablica 6) pokazali su statistički značajnu razliku u percepciji važnosti određenih sigurnosnih praksi među učenicima različitih vrsta srednjih škola. Najznačajnija razlika utvrđena je kod varijable održavanje zaštite (Asymp. Sig. < 0,001), što ukazuje na to da učenici iz gimnazija i strukovnih škola imaju različite stavove o važnosti kontinuiranog osiguravanja digitalne sigurnosti. Također, značajna razlika pronađena je i kod varijable provjeravanje prijenosnih medija (Asymp. Sig. = 0,007), što sugerira da učenici iz različitih škola različito percipiraju potrebu za provjerom sigurnosti eksternih uređaja i medija. Statistički značajna razlika zabilježena je i kod varijable odjavljivanje (Asymp. Sig. = 0,026), iako manje izražena u odnosu na prethodne varijable. S druge strane, kod varijable povremeno mijenjanje lozinki nije pronađena statistički značajna razlika (Asymp. Sig. = 0,223), što sugerira da učenici bez obzira na vrstu srednje škole imaju slične stavove o važnosti ove sigurnosne prakse. Dobiveni rezultati potvrđuju

da obrazovni pristup, dostupnost tehnoloških resursa te socio-ekonomski i kulturni čimbenici mogu utjecati na svijest učenika o sigurnosti na internetu. Učenici koji pohađaju škole s izraženijim naglaskom na IKT pokazuju veću svijest o sigurnosnim praksama, dok učenici iz škola u kojima su takvi sadržaji manje zastupljeni ili ih nema uopće rjeđe percipiraju važnost određenih sigurnosnih mjera. Ovi nalazi upućuju na potrebu za unaprjeđenjem obrazovnih programa iz područja internetske sigurnosti u svim vrstama srednjih škola, s ciljem razvijanja boljih sigurnosnih navika kod mladih i smanjenja njihove izloženosti digitalnim prijetnjama.

Rasprava

Rezultati ovog istraživanja ukazuju na značajne razlike u samoprocjeni rizičnog ponašanja adolescenata na internetu među učenicima gimnazija i strukovnih škola, što je u skladu s prethodnim istraživanjima koja sugeriraju da vrsta obrazovne institucije može oblikovati percepciju i ponašanje učenika u digitalnom okruženju (Livingstone i sur., 2011; Núñez-Gómez i sur., 2021). Na primjer, učenici gimnazija, koji su obično izloženi korištenju digitalnih tehnologija kroz informatiku, pokazuju višu razinu svijesti o sigurnosnim rizicima na internetu. S druge strane, učenici strukovnih škola, koji mogu biti manje izloženi temama vezanim uz digitalnu pismenost u školama, često iskazuju nižu svijest o potrebnim sigurnosnim mjerama, poput redovite promjene lozinki ili provjere sigurnosti prijenosnih uređaja. Ovi rezultati potvrđuju teoretske okvire koji problematično korištenje interneta i sigurnost na mreži promatraju kroz bihevioralne i kognitivne dimenzije (Beard i Wolf, 2001; Velki i Šolić, 2020), dok konkretni primjeri ukazuju na to da obrazovni pristupi u različitim vrstama škola mogu značajno oblikovati studentske digitalne navike.

Hipoteza 1, koja je istraživala razlike između gimnazija i strukovnih škola u procjeni rizičnog online ponašanja, nije potvrđena, osim za varijablu privole za obradu osobnih podataka. To sugerira da su učenici iz obje vrste škola izjednačeni u samoprocjeni rizičnog ponašanja na internetu, no razlika u percepciji privatnosti i upravljanju osobnim podacima ukazuje na specifične obrazovne razlike u pristupu sigurnosti na internetu. Učenici gimnazija pokazuju višu razinu svijesti o zaštiti svojih podataka, dok učenici strukovnih škola možda nisu dovoljno educirani o važnosti privatnosti, što se očituje u nižoj razini privole za obradu osobnih podataka. Hipoteza 2, koja se bavila razlikama između vrsta srednjih škola u samoprocjeni rizičnog ponašanja, nije potvrđena, osim u slučaju provjere prijenosnih medija, gdje je zabilježena statistički značajna razlika. Učenici gimnazija su češće prijavljivali korištenje antivirusnog softvera i redovito ažuriranje postavki privatnosti na društvenim mrežama, dok učenici strukovnih škola rjeđe poduzimaju ovakve korake. Ovi podaci sugeriraju da se teorijski okvir problematično korištenja interneta može primijeniti i unutar različitih obrazovnih sustava, s naglaskom na specifične razlike u praksama vezanim uz digitalnu sigurnost. Razlike u obrazovnim programima između gimnazija i strukovnih škola mogu igrati ključnu ulogu u oblikovanju tih sigurnosnih navika. Hipoteza 3, koja je istraživala razlike u samoprocjeni svijesti o potencijalnim rizicima između učenika različitih vrsta srednjih škola, potvrđena je. Mann-Whitney test ukazao je na statistički značajne razlike između gimnazija i strukovnih škola za varijable održavanja zaštite i provjere prijenosnih medija. Ovi rezultati jasno naglašavaju utjecaj obrazovnog pristupa i kurikula na percepciju sigurnosti na internetu među učenicima. Učenici gimnazija, koji su češće izloženi obrazovnim programima koji uključuju digitalnu pismenost i sigurnost na internetu, pokazuju bolju svijest o rizicima, kao što su održavanje zaštite na uređajima i provjera sigurnosti prijenosnih medija. Nasuprot tome, učenici strukovnih škola pokazuju manju sklonost poduzimanju zaštitnih mjera, što ukazuje na potrebu za jačim obrazovnim intervencijama u tim institucijama. Hipoteza 4, koja je također istraživala razlike u samoprocjeni svjesnosti o potencijalnim rizicima, potvrđena je. Mann-Whitney test ponovno je pokazao statistički značajne razlike između gimnazija i strukovnih škola za varijable održavanja zaštite i provjere prijenosnih medija. Ovi nalazi ponovo podcrtavaju važnost uključivanja edukativnih programa o kibernetičkoj

sigurnosti u školski kurikulum kako bi se ojačala svijest i praksa učenika u digitalnom okruženju. Učenici koji su prošli obrazovne programe o sigurnosti na internetu, koji su specifično dizajnirani u gimnazijama, pokazuju veće razumijevanje sigurnosnih praksi, što može značajno smanjiti rizike povezane s nesigurnim ponašanjem na internetu.

Ovi rezultati također ukazuju na važnost obrazovnih programa koji se bave sigurnošću na internetu. Rezultati se slažu s prethodnim istraživanjima koja potvrđuju potrebu za integracijom edukacija o sigurnosti na internetu u školski kurikulum (Livingstone i sur., 2011; Velki i Šolić, 2020). Iako su samoprocjene rizičnih ponašanja među učenicima gimnazija i strukovnih škola slične, specifične digitalne navike, kao što su provjera prijenosnih medija i održavanje zaštite, mogu biti pod utjecajem različitih obrazovnih pristupa i iskustava. Na primjer, obrazovni programi u gimnazijama koji uključuju tematiku digitalne sigurnosti i kritičkog razmišljanja o medijima mogu pomoći učenicima u razvijanju većih vještina zaštite svojih podataka, dok bi slični programi u strukovnim školama mogli smanjiti nesklad između samoprocjene i stvarnog ponašanja. Obrazovni programi koji fokusiraju na podizanje svijesti o rizicima internetskog ponašanja mogu znatno smanjiti nesklad između samoprocjene i stvarnog ponašanja učenika.

Rezultati također sugeriraju da se svijest o rizicima i digitalnoj sigurnosti razvija kroz formalno obrazovanje. Na primjer, učenici gimnazija koji su redovito izloženi kurikulumu koji uključuje sigurnost na internetu često bolje razumiju važnost zaštite privatnosti, dok učenici strukovnih škola, koji možda nemaju istu količinu obrazovanja o digitalnim prijetnjama, mogu biti skloniji rizičnim ponašanjima. Razlike u kurikulumu između gimnazija i strukovnih škola mogu značajno utjecati na percepciju i ponašanje učenika u digitalnom prostoru, osobito u kontekstu varijabli poput održavanja zaštite i provjere prijenosnih medija. Na primjer, učenici koji su uključeni u obrazovne aktivnosti usmjerene na sigurnost na internetu, poput radionica o zaštiti privatnosti, izvještavanju o prijetnjama i korištenju sigurnosnih postavki na društvenim mrežama, pokazali su značajno veću spremnost na implementaciju tih sigurnosnih mjera u svakodnevnom online ponašanju. Ovi nalazi naglašavaju važnost kontinuiranog obrazovanja o sigurnosti na internetu, koje bi trebalo postati sastavni dio obrazovnih programa, kako bi se smanjio nesklad između samoprocjene i stvarnog ponašanja učenika u digitalnom okruženju (Spada, 2014; Velki i Šolić, 2020).

Zaključak

Rezultati ovog istraživanja ukazuju na statistički značajnu razliku između učenika gimnazija i strukovnih škola u svijesti o specifičnim aspektima informacijske sigurnosti, kao što su održavanje zaštite i provjera prijenosnih medija. Ovi nalazi sugeriraju da obrazovni pristup i kurikulumi mogu imati ključnu ulogu u oblikovanju percepcije sigurnosnih rizika među učenicima. Stoga, uključivanje edukativnih programa o kibernetičkoj sigurnosti u školske kurikulume može značajno unaprijediti svijest i praksu učenika u digitalnom okruženju, čime bi se smanjio nesklad između samoprocjene i stvarnog ponašanja.

Iako nisu sve hipoteze u istraživanju bile potvrđene, rezultati naglašavaju složenost faktora koji utječu na percepciju i svijest o sigurnosti na internetu među srednjoškolcima. Razlike između gimnazija i strukovnih škola ukazuju na to da obrazovni pristupi u različitim vrstama škola oblikuju specifične navike i stavove učenika prema digitalnoj sigurnosti. Potreba za daljnjim istraživanjima, koja će uzeti u obzir širi spektar varijabli i konteksta školovanja, postaje očita. Buduća istraživanja trebaju uključiti čimbenike poput socijalno-ekonomskog statusa, dostupnosti tehnologije kod kuće i kulturnih specifičnosti, koji također mogu značajno utjecati na digitalne navike učenika.

Zaključci ovog istraživanja pružaju nove uvide u percepciju sigurnosnih rizika među učenicima srednjih škola, ističući važnost vrste obrazovne institucije i kurikuluma kao ključnih

faktora u oblikovanju njihove percepcije i ponašanja u digitalnom okruženju. Korištenje kvantitativne analize, konkretno Mann-Whitney U testa, omogućilo je objektivno ispitivanje razlika u percepciji sigurnosnih rizika. Ovi nalazi pružaju konkretne smjernice za daljnji razvoj i prilagodbu obrazovnih programa o kibernetičkoj sigurnosti u srednjim školama, s ciljem povećanja sigurnosti i smanjenja rizičnih ponašanja među učenicima.

Istraživanje doprinosi razumijevanju složenosti percepcije sigurnosnih rizika u digitalnom okruženju među srednjoškolcima. Rezultati ukazuju na potrebu za daljnjim teorijskim i praktičnim smjernicama za razvoj obrazovnih strategija koje će adresirati specifične izazove u oblikovanju digitalnih navika i povećanju svijesti o sigurnosti među mladima.

Preporuke za buduće istraživanje uključuju proširenje uzorka na različite geografske regije i tipove škola kako bi se omogućila šira generalizacija rezultata. Također, preporuča se kombiniranje kvantitativnih i kvalitativnih metoda, što bi omogućilo dublje razumijevanje iskustava i stavova učenika. Razvoj sveobuhvatnijih mjera za procjenu percepcije rizika, koje će obuhvatiti različite aspekte digitalne sigurnosti, kao i uključivanje relevantnih kontekstualnih faktora poput socijalno-ekonomskog statusa, moglo bi dodatno obogatiti rezultate.

Dodatno, provedba longitudinalnih istraživanja koja bi pratila promjene u percepciji i ponašanju učenika kroz vrijeme mogla bi omogućiti dublje uvide u dinamiku razvoja digitalnih navika. Evaluacija učinkovitosti obrazovnih programa o kibernetičkoj sigurnosti, kroz praćenje njihovog utjecaja na sigurnosnu praksu učenika, također bi pružila dragocjene informacije za usmjeravanje budućih obrazovnih politika i strategija.

Literatura

- Aboujaoude, E. (2010). Problematic Internet use: An overview. *World Psychiatry*, 9(2), 85–90. <https://doi.org/10.1002/j.2051-5545.2010.tb00278.x>
- Agatston, P. W., Kowalski, R., i Limber, S. (2007). Students' Perspectives on Cyber Bullying. *Journal of Adolescent Health*, 41(6), S59–S60. <https://doi.org/10.1016/j.jadohealth.2007.09.003>
- Anderson, K. J. (2001). Internet Use Among College Students: An Exploratory Study. *Journal of American College Health*, 50(1), 21–26. <https://doi.org/10.1080/07448480109595707>
- Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., i Gosling, S. D. (2010). Facebook Profiles Reflect Actual Personality, Not Self-Idealization. *Psychological Science*, 21(3), 372–374. <https://doi.org/10.1177/0956797609360756>
- Beard, K. W., i Wolf, E. M. (2001). Modification in the Proposed Diagnostic Criteria for Internet Addiction. *CyberPsychology & Behavior*, 4(3), 377–383. <https://doi.org/10.1089/109493101300210286>
- Board, N. E. (2017b). Spring 2017. *Cornell International Affairs Review*, 10(2). <https://doi.org/10.37513/ciar.v10i2.495>
- Brownlow, P. R. H., i McMurray Charlotte, I. (2004). *SPSS Explained*. Routledge. <https://doi.org/10.4324/9780203642597>
- Calvete, E., Orue, I., Estévez, A., Villardón, L., i Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior*, 26(5), 1128–1135. <https://doi.org/10.1016/j.chb.2010.03.017>
- Casey, B. J. (2015). Beyond Simple Models of Self-Control to Circuit-Based Accounts of Adolescent

Behavior. *Annual Review of Psychology*, 66(1), 295–319. <https://doi.org/10.1146/annurev-psych-010814-015156>

- Ciboci, L., Ćosić Pregrad, I., Kanižaj, I., Potočnik, D., i Vinković, D. (2020). Istraživanje o sigurnosti djece na internetu: *HR Kids Online*. Pribavljeno veljača 12, 2024. <http://hrkids.online/prez/EUKidsOnlineHRfinal.pdf>.
- Ciboci, L., Kanižaj, I., i Labaš, D. (2018). *Razvoj medijske pismenosti: Sigurnost djece na internetu i elektroničke medije: Nastavni materijali za osnovne škole za učenike od 5. - 8. razreda*. Agencija za elektroničke medije i Unicef. Pribavljeno Veljača 12, 2024, s <https://www.medijskapismenost.hr/wp-content/uploads/2018/04/elektronicko-nasilje.pdf>.
- Chamberlain, S. R., Ioannidis, K., i Grant, J. E. (2018). The impact of comorbid impulsive/compulsive disorders in problematic Internet use. *Journal of Behavioral Addictions*, 7(2), 269–275. <https://doi.org/10.1556/2006.7.2018.30>
- Colley, A., i Maltby, J. (2008). Impact of the Internet on our lives: Male and female personal perspectives. *Computers in Human Behavior*, 24(5), 2005–2013. <https://doi.org/10.1016/j.chb.2007.09.002>
- CSI (2024) Centar za sigurniji Internet, <https://csi.hr/onama/> . Pribavljeno Veljača 12, 2024
- Despotovic, Z. O., Hossfeld T. O., Kellerer, W. O., Lehrieder, F. R., Oechsner, S. I. i Michel, M. A. (2011). Mitigating Unfairness In Locality-Aware Peer-To-Peer Networks. *International Journal Of Network Management*, 21 (1), 3-20.
- Dhir, A., Chen, S., i Nieminen, M. (2016). Psychometric validation of the compulsive internet use scale: Relationship with adolescents' demographics, ICT accessibility, and problematic ICT use. *Social Science Computer Review*, 34(2), 197-214. <https://doi.org/10.1177/0894439315572575>
- Dredge, R., Gleeson, J. F. M. i De la Piedad Garcia, X. (2014). Risk Factors Associated with Impact Severity of Cyberbullying Victimization: A Qualitative Study of Adolescent Online Social Networking. *Cyberpsychology, Behavior, and Social Networking*, 17(5), 287-291.
- Ehman, A. C., i Gross, A. M. (2019). Sexual cyberbullying: Review, critique, & future directions. *Aggression and Violent Behavior*, 44, 80–87. <https://doi.org/10.1016/j.avb.2018.11.001>
- Farrukh, A., Sadwick, R., i Villasenor, J. (2014). Youth Internet Safety: Risks, Responses, and Research Recommendations. *Center for Technology Innovation at Brookings*. Washington DC.
- Franke, U. i Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature, *Computers & Security*, vol. 46, pp. 18-31.
- Gerwin, R., Kaliebe, K., i Daigle, M. (2018). The Interplay Between Digital Media Use and Development. *Child and Adolescent Psychiatric Clinics of North America*, 27(2), 345–355. <https://doi.org/10.1016/j.chc.2017.11.002>
- Goold, P. C., Ward, M., i Carlin, E. M. (2003). Can the Internet be used to improve sexual health awareness in web-wise young people? *Journal of Family Planning and Reproductive Health Care*, 29(1), 28–30. <https://doi.org/10.1783/147118903101196864>
- Grant, J. E., Atmaca, M., Fineberg, N. A., Fontenelle, L. F., Matsunaga, H., Janardhan Reddy, Y. C., Simpson, H. B., Thomsen, P. H., Van Den Heuvel, O. A., Veale, D., Woods, D. W., i Stein, D. J. (2014). Impulse control disorders and “behavioural addictions” in the ICD-11. *World Psychiatry*, 13(2), 125–127. <https://doi.org/10.1002/wps.20115>

- Henry, J. S. (2012). Bias-Based Cyberbullying: The Next Hate Crime Frontier? *Social Science Research Network*.
https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2331371_code2128509.pdf?abstractid=2331371&mirid=1&type=2
- Hinduja, S., i Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, 31(1), 125–146.
<https://doi.org/10.1016/j.adolescence.2007.05.004>
- Hinduja, S., i Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, 14(3), 206–221. <https://doi.org/10.1080/13811118.2010.494133>
- Hunley, S., Evans, J., Delgado-Hachey, M., Krise, J., Rich, T., i Schell, C. (2005). Adolescent Computer Use and Academic Achievement. *Adolescence*, 40, 307–318.
- Hur, J. H., Kim, K. Y., Song, J. B., i Lee, T. W. (2009). The narrative approach to teach information and communication ethics education in elementary school. *Proceedings of the 17th International Conference on Computers in Education*, Volume 6 (pp. 960-964). Hong Kong: Asia-Pacific Society for Computers in Education.
- Ioannidis, K., Chamberlain, S. R., Treder, M. S., Kiraly, F., Leppink, E. W., Redden, S. A., Stein, D. J., Lochner, C., i Grant, J. E. (2016). Problematic internet use (PIU): Associations with the impulsive-compulsive spectrum. An application of machine learning in psychiatry. *Journal of Psychiatric Research*, 83, 94–102. <https://doi.org/10.1016/j.jpsychires.2016.08.010>
- Joiner, R., Gavin, J., Duffield, J., Brosnan, M., Crook, C., Durndell, A., Maras, P., Miller, J., Scott, A. J., i Lovatt, P. (2005). Gender, Internet Identification, and Internet Anxiety: Correlates of Internet Use. *CyberPsychology & Behavior*, 8(4), 371–378. <https://doi.org/10.1089/cpb.2005.8.371>
- Jones, S., Johnson-Yale, C., Millermaier, S., i Pérez, F. S. (2009). U.S. College Students' Internet Use: Race, Gender and Digital Divides. *Journal of Computer-Mediated Communication*, 14(2), 244–264. <https://doi.org/10.1111/j.1083-6101.2009.01439.x>
- Kruse, C. S., Frederick, B., Jacobson, T., i Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. <https://doi.org/10.3233/thc-161263>
- Kimpe, L., Walrave, M., Ponnet, K., i Van Ouytsel, J. (2019). *Internet Safety*. 1–11. <https://doi.org/10.1002/9781118978238.ieml0093>
- Lei, M., i Lomax, R. G. (2005). The Effect of Varying Degrees of Nonnormality in Structural Equation Modeling. *Structural Equation Modeling*, 12(1), 1–27.
https://doi.org/10.1207/s15328007sem1201_1
- Lenhart, A., Purcell, K., Smith, A., i Zickuhr, K. (2010). Social Media & Mobile Internet Use Among Teens and Young Adults. Pew Internet and American Life Project.
- Letica, I. B., Tokić, I. S., Duvnjak, I., Grgić, K., Pakšić, B. H., Horvat, I., Ilakovac, V., Kralik, K., Nenadić, K., Romstein, K., Ružić, V., Šincek, D., Šolić, K., Velki, T., Vojković, G., i Vuković, M. (2019). *Izazovi digitalnog svijeta*. Pribavljeno Veljača, 5, 2024, s <https://repozitorij.foozos.hr/islandora/object/foozos%3A988>.
- Livingstone, S. i Bober, M. (2006). Regulating the internet at home: Contrasting the

perspectives of children and parents. U: D. Buckingham i R. Willett (Ur.), *Digital Generations* (str. 93-113). Mahwah, NJ: Erlbaum.

Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The

perspective of European children. Full Findings. LSE, London: *EU Kids Online*.

Lukasik, S. J. (2011). Protecting Users of the Cyber Common. *Communications of the ACM*, 54, 54-61.

Matijević, M., Bilić, V. i Opić, S. (2016). *Pedagogija za učitelje i nastavnike*. Školska knjiga.

Mellado, D. i sur.(2017). A systematic review of security requirements engineering, *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 153-165, 2010. A. V. Herrera, M. Ron, and C. Rabadão, National cyber-security policies oriented to BYOD (bring your own device): Systematic review, in Proc. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-4.

Medijska pismenost. (2017). Koji su sve oblici elektroni?kog nasilja - Medijska pismenost. *Medijska pismenost- Pribavljeno Velja?a 5, 2024*, s <https://www.medijskapismenost.hr/oblici-obiljezja-elektronickog-nasilja/>.

Mevojšek M. (2003). *Uvod u metode znanstvenog istraživanja*. Naklada Slap

Ministarstvo znanosti, obrazovanja i športa RH. (2011). *Nacionalni okvirni kurikulum*. Ministarstvo znanosti, obrazovanja i športa RH. Pribavljeno Veljača 12, 2024, s http://mzos.hr/datoteke/Nacionalni_okvirni_kurikulum.pdf.

Ministarstvo znanosti i obrazovanja. (2018). *Okvir nacionalnoga kurikuluma*.

Ministarstvo znanosti i obrazovanja. Pribavljeno Veljača 12, 2024, s

<https://shorturl.at/ntvzM>.

Mishna, F. i sur., (2011). Interventions to prevent and reduce cyber abuse of youth: A systematic review,|| *Research on Social Work Practice*, vol. 21, no. 1, pp. 5-14.

Moreno, M. A., Parks, M. R., Zimmerman, F. J., Brito, T. E., i Christakis, D. A. (2009). Display of Health

Risk Behaviors on MySpace by Adolescents. *ARCH PEDIATR AOLESC MED*, 163(1).

Narodne novine. (2019, siječanj). *Odluka o donošenju kurikuluma za nastavni predmet Hrvatski jezik*

za osnovne škole i gimnazije u Republici Hrvatskoj. Zagreb, Republika Hrvatska. Pribavljeno Veljača 10, 2024, s

https://narodne-novine.nn.hr/clanci/sluzbeni/2019_01_10_215.html .

Narodne novine. (2019, siječanj). *Odluka o donošenju kurikuluma za nastavni predmet Informatike za osnovne škole i gimnazije u Republici Hrvatskoj*. Zagreb, Republika Hrvatska. Pribavljeno Veljača 10, 2024, s

Odluka o donošenju kurikuluma za nastavni predmet Informatike za osnovne škole i gimnazije u Republici Hrvatskoj (nn.hr).

Narodne novine. (2019, siječanj). *Odluka o donošenju kurikuluma za nastavni predmet Hrvatski jezik za srednje strukovne škole na razini 4.2 u Republici Hrvatskoj*. Zagreb,

Republika Hrvatska. Pribavljeno Veljača 10, 2024, s

https://narodne-novine.nn.hr/clanci/sluzbeni/2019_01_10_214.html.

- Ncube, L. S., i Dube, L. (2016). Cyberbullying a desecration of information ethics: Perceptions of post high school youth in a rural community. *Journal of Information, Communication and Ethics in Society*, 14(4), 313-322. <https://doi.org/10.1108/JICES-04-2016-0009>
- Núñez-Gómez, P., Larrañaga, K. P., Rangel, C., i Ortega-Mohedano, F. (2021). Critical Analysis of the Risks in the Use of the Internet and Social Networks in Childhood and Adolescence. *Frontiers in Psychology*, 12. <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.683384>
- Onyancha, O. B. (2015). An informetrics view of the relationship between internet ethics, computer ethics and cyberethics. *Library Hi Tech*, 33(3), 387-408. <https://doi.org/10.1108/LHT-04-2015-0033>
- Orshesky, C. (2003). Beyond technology - The human factor in business systems. *Journal of Business Strategy*, 24, 4, 43-47.
- Panadero, E., G.T.L. Brown, and J.-W. Strijbos. 2016. 'The Future of Student Self-Assessment: A Review of Known Unknowns and Potential Directions'. *Educational Psychology Review* 28 (4): 803-830. doi:10.1007/s10648-015-9350-2.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., i Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, 22(4), 334-345. <https://doi.org/10.1108/IMCS-10-2013-0078>
- Pettorruso, M., Valle, S., Cavic, E., Martinotti, G., Di Giannantonio, M., i Grant, J. E. (2020). Problematic Internet use (PIU), personality profiles and emotion dysregulation in a cohort of young adults: Trajectories from risky behaviors to addiction. *Psychiatry Research*, 289, 113036. <https://doi.org/10.1016/j.psychres.2020.113036>
- Puri, A. i Sharma, R. (2016). Internet usage, depression, social isolation and loneliness amongst adolescents. *Indian Journal of Health & Wellbeing*, 7(10), 996-1003.
- Pyżalski, J. (2012). From cyberbullying to electronic aggression: Typology of the phenomenon. *Emotional and Behavioural Difficulties*, 17(3-4), 305-317. <https://doi.org/10.1080/13632752.2012.704319>
- Rahim, N. H. A. i sur., (2015). A systematic review of approaches to assessing cybersecurity awareness, Kybernetes.
- Rahman, N. a. A., Sairi, I. H., Zizi, N. a. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5), 378-382. <https://doi.org/10.18178/ijiet.2020.10.5.1393>
- Rideout VJ, Foehr UG, Roberts D: Generation M2: Media in the lives of 8 to 18 year olds. *Menlo Park: Kaiser Family Foundation*; 2010. 21.
- Rivers, I., i Noret, N. (2010). 'I h8 u': Findings from a five-year study of text and email bullying. *British Educational Research Journal*, 36(4), 643-671. <https://doi.org/10.1080/01411920903071918>
- Sasse, M. A., Brostoffand, S. i Weirich, D. (2001). Transforming the 'weakest link' - a human/

computer interaction approach to usable and effective security. *BT Technology Journal*, 19, 122-131.

Shapiro, E. S., i Cole, C. L. (1994). Behavior change in the classroom. New York, NY: Guilford Press

Sharma, M., Mittal, S., i Verma, A. (2015). Cyber ethics in security application in the modern era of Internet. *IITM Journal of Management and IT*, 6(1), 140-143. <https://iitmjp.ac.in/wp-content/uploads/2017/06/ITConference-2015.pdf#page=140>

Shui Ng, W. (2020). A Self-assessment Approach to Adolescents' Cyberethics Education. *Journal of Information Technology Education: Research*, 19, 555-570. <https://doi.org/10.28945/4623>

Shulman, E. P., Smith, A. R., Silva, K., Icenogle, G., Duell, N., Chein, J., i Steinberg, L. (2016). The dual

systems model: Review, reappraisal, and reaffirmation. *Developmental Cognitive Neuroscience*, 17, 103-117. <https://doi.org/10.1016/j.dcn.2015.12.010>

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. i Tippett, N. (2008).Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, 49(4), 376-385

Solic, K., Velki, T., Fosic, I., i Vukovic, M. (2024). Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire. *Acta Polytechnica Hungarica*, 21(4), 49-68. <https://doi.org/10.12700/APH.21.4.2024.4.3>

Spada, M. M. (2014). An overview of problematic Internet use. *Addictive Behaviors*, 39(1), 3-6. <https://doi.org/10.1016/j.addbeh.2013.09.007>

Steinskog, D. J., Tjøstheim, D. B., & Kvamstø, N. G. (2007). A cautionary note on the use of the Kolmogorov-Smirnov test for normality. *Monthly Weather Review*, 135(3), 1151-1157. <https://doi.org/10.1175/mwr3326.1>

Stonard, K. E., Bowen, E., Lawrence, T. R., i Price, S. A. (2014). The relevance of technology to the nature, prevalence and impact of Adolescent Dating Violence and Abuse: A research synthesis. *Aggression and Violent Behavior*, 19(4), 390-417. <https://doi.org/10.1016/j.avb.2014.06.005>

Sun, P., Unger, J. B., Palmer, P. H., Gallaher, P., Chou, C.-P., Baezconde-Garbanati, L., Sussman, S., i Johnson, C. A. (2005). Internet Accessibility and Usage among Urban Adolescents in Southern California: Implications for Web-Based Health Research. *CyberPsychology & Behavior*, 8(5), 441-453. <https://doi.org/10.1089/cpb.2005.8.441>

Taber, K. S. (2017). The use of Cronbach's Alpha when developing and reporting research instruments in science education. *Research in Science Education*, 48(6), 1273-1296. <https://doi.org/10.1007/s11165-016-9602-2>

Tavakol, M., & Wetzel, A. (2020). Factor Analysis: a means for theory and instrument development in support of construct validity. *International Journal of Medical Education*, 11, 245-247. <https://doi.org/10.5116/ijme.5f96.0f4a>

Ybarra, M. L., Espelage, D. L., i Mitchell, K. J. (2007). The Co-occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration: Associations with Psychosocial Indicators. *Journal of Adolescent Health*, 41(6), S31-S41. <https://doi.org/10.1016/j.jadohealth.2007.09.010>

- Velki, T., i Šolić, K. (2020). Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti. *Policija i sigurnost*, 29(4), 341–355. <https://hrcak.srce.hr/249659>
- Whittier, D. B. (2013). Cyberethics: Envisioning character education in cyberspace. *Peabody Journal of Education*, 88(2), 225-242. <https://doi.org/10.1080/0161956X.2013.775882>
- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.* (2018). Pribavljeno Veljača 12, 2024, s https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html.
- Zheng, X. i Zhao, W. (2015). Relationship between Internet altruistic behavior and hope of middle-school students: The mediating role of self-efficacy and self-esteem. *Psychological Development and Education*, 31(4), 428–436.



**Teaching (Today for) Tomorrow:
Bridging the Gap between the Classroom and
Reality**

3rd International Scientific and Art Conference
Faculty of Teacher Education, University of Zagreb in
cooperation with the Croatian Academy of Sciences and
Arts

Internet safety in adolescents

Abstract

Internet use has increased significantly over the past twenty years, but with this growth has come concerns about problematic internet use that can cause psychological problems. This includes activities such as video games, social media, web streaming and online shopping, and children and young people are particularly at risk. The aim of this study was to investigate the differences between young people's actual risk behavior online and their self-assessment and awareness of information security, according to school type. The research was conducted in secondary schools in Sisak-Moslavina County on a sample of 167 students with an average age of 16.5 years, using the Behavioral Cognitive Internet Safety Questionnaire (BKUIS). The questionnaire measures risk behavior and safety awareness using 17 questions divided into four subscales. The results showed a high reliability of the questionnaire (Cronbach's alpha = 0.81), and due to the deviation of the data from the normal distribution, the non-parametric Mann-Whitney U-test was used. The results showed that there are no statistically significant differences in risk behaviors between the different types of high schools, except in certain areas such as consent to process personal data and portable media review. A statistically significant difference was found in online safety awareness, with high school students showing better knowledge of maintaining protection and safety practices. In summary, while students have access to Internet safety education programs within the school system, more needs to be done to raise awareness and reduce risky behavior among youth.

Key words:

adolescents; BKUIS; Internet; Internet security; risky behaviors

Revizija #4

Stvoreno 8 svibnja 2025 11:49:26 od Martina Gajšek

Ažurirano 21 svibnja 2025 07:34:19 od Martina Gajšek