Zaprimljen: 22.4.2025.
Odobren za objavu: 23.7.2025.
Izvorni znanstveni rad

PROVJERA ZNANJA O KIBERNETIČKOJ SIGURNOSTI U SREDNJIM ŠKOLAMA POMOĆU DIGITALNOG KVIZA

Ivana Lovrić Senjak[1], Mirko Cobović[2], Žaklina Bender[3], Anita Barišić[4]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: ilovricsenjak@unisb.hr
[2] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: mcobovic@unisb.hr
[3] Gimnazija Požega. Dr. Franje Tuđmana 4A, 34000 Požega, Hrvatska,
ePošta: tajnistvo@gimpoz.hr
[4] Gimnazija Matija Mesić, Naselje Slavonija I 8, 35000 Slavonski Brod, Hrvatska
ePošta: anitaorec2@gmail.com

Sažetak: Ovaj rad istražuje razinu znanja srednjoškolaca o osnovama kibernetičke sigurnosti putem digitalnog kviza. Cilj je bio identificirati područja dobre informiranosti i ona koja zahtijevaju dodatnu edukaciju. U istraživanju je korišten kvantitativni pristup temeljen na strukturiranom digitalnom kvizu, provedenom među 268 učenika iz triju gimnazija, a podaci su analizirani deskriptivnom i korelacijskom statistikom. Rezultati pokazuju visoku ukupnu točnost (87,69 %), s najboljim rezultatima u temama lozinki i digitalnog traga te najslabijima u prepoznavanju osobnih podataka, ransomwarea i 2FA. Nije utvrđena značajna povezanost između točnosti i vremena rješavanja ni između uređaja i uspješnosti. Rad ističe važnost strukturirane edukacije o kibernetičkoj sigurnosti.

Ključne riječi: digitalni kviz, kibernetička sigurnost, gimnazije, obrazovanje, statistička analiza

1. Uvod

Intenzivna izloženost upotrebi digitalnih tehnologija među mladima, zahtijeva pravovremeno obrazovanje o osnovama kibernetičke sigurnosti. Prema izvješću Europske komisije (2022), informatičko obrazovanje u europskim školama postaje ključna komponenta digitalne pismenosti i društvene odgovornosti.
Prema izvješću Europske agencije za kibernetičku sigurnost (ENISA, 2019), Europska unija suočava se s izraženim nedostatkom stručnjaka za kibernetičku sigurnost, što predstavlja izazov za tržište rada i za nacionalnu sigurnost. S naglaskom na visokom obrazovanju, preporuke uključuju ranu implementaciju tema kibernetičke sigurnosti u obrazovni sustav. Analiza školskih kurikuluma u ak.god. 2020/2021 pokazuje da u brojnim državama članicama informatički sadržaji koji obuhvaćaju kibernetičku sigurnost još uvijek nisu sustavno integrirani u sve razine obrazovanja što Navedeno upućuje na potrebu jačeg kurikularnog pristupa u području digitalne sigurnosti u srednjoškolskom uzrastu.

1.1. Prethodna istraživanja

U prethodnim istraživanjima naglašava se važnost uključivanja tema kibernetičke sigurnosti u obrazovni sustav. Jerman Blažič i Jerman Blažič (2022) ističu potrebu za interaktivnim oblicima poučavanja poput edukativnih igara, dok Adams i Makramalla (2015) upozoravaju na neučinkovitost tradicionalnih metoda u području digitalne sigurnosti. Witsenboer i sur. (2022) pokazuju da su nizozemski učenici bolje informirani o lozinkama i

privatnosti, ali slabije razumiju pojmove kao što su phishing i enkripcija. Navedena istraživanja potvrđuju potrebu za ovim radom, koji kroz digitalni kviz procjenjuje znanje hrvatskih srednjoškolaca i identificira područja za dodatnu edukaciju.

2. Metodologija

U ovom se radu ispituju tri ključna aspekta povezana s razinom znanja srednjoškolaca o kibernetičkoj sigurnosti. Primarno, utvrđuju se tematska područja u kojima učenici pokazuju najvišu razinu informiranosti, kao i ona koja zahtijevaju dodatnu edukaciju. Sekundarno, istražuje se postoji li povezanost između točnosti rješavanja kviza i vremena njegova ispunjavanja. Na kraju, analizira se moguće postojanje razlika u uspješnosti rješavanja kviza s obzirom na vrstu korištenog uređaja, konkretno između korisnika Android i iOS sustava.
U svrhu istraživanja razine znanja o kibernetičkoj sigurnosti među učenicima srednjih škola, provedeno je istraživanje kvantitativne metode temeljene na strukturiranom online kvizu. Alat za izradu i distribuciju kviza bio je Quizizz.

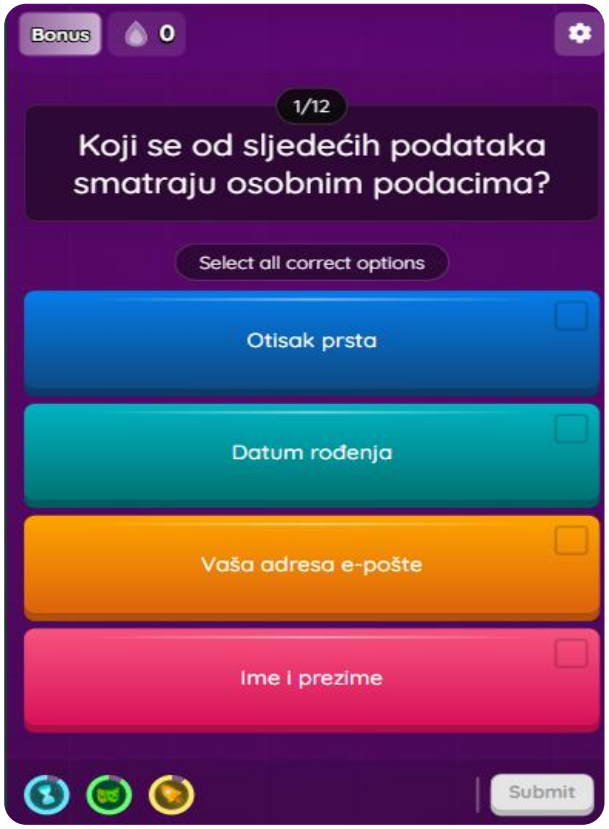
Slika 1: Poster sa QR kodom kviza

Digitalni poster sa QR kodom za pristup kvizu je distribuiran predavačima i suradnicima unutar srednjih škola na području Brodsko-posavske, Požeško-slavonske i Osječko-baranjske županije. Sudjelovanje je bilo anonimno i dobrovoljno. Suradnici škola angažirani u provođenju kviza su bili informirani o svrsi istraživanja i upućeni da savjetuju učenike o mjerama u svrhu anonimnosti. Podaci su prikupljeni u razdoblju 24.03.2025. – 12.04.20205.
Sudionici su bili učenici Gimnazije „Matija Mesić" Slavonski Brod, Gimnazije Požega i I. Gimnazije Osijek. Kvizove su provodili nastavnici i suradnici navedenih škola tijekom nastavnih sati informatike, etike i sata razrednika.
Kviz je sadržavao ukupno 12 pitanja s višestrukim izborom između točnih i netočnih odgovora, podijeljenih u tematske cjeline. Svako od 12 pitanja je sadržavalo četiri ponuđena odgovora, od kojih je za 11 pitanja bio točan samo jedan od ponuđenih odgovora dok su za 1 pitanje bila točna sva četiri ponuđena odgovora. Vrijeme za odgovor je bilo ograničeno na 60 sekundi po pitanju.
Rezultati kviza analizirani su metodama deskriptivne statistike. Za svako pitanje izračunata je učestalost točnih i netočnih odgovora, a ukupni rezultati grupirani su po tematskim područjima s ciljem utvrđivanja koje su teme učenicima najpoznatije, a koje zahtijevaju dodatnu edukaciju. Uz deskriptivne analize, provedene su i korelacijske analize pomoću Pearsonovog i Spearmanovog koeficijenta kako bi se ispitala povezanost između točnosti rješavanja kviza i vremena njegova ispunjavanja. Osim toga, primijenjen je Mann-Whitney U test radi ispitivanja razlika u rezultatima i vremenu rješavanja s obzirom na vrstu korištenog uređaja.

3. Rezultati i rasprava

Rezultati kviza prikazuju različite razine poznavanja temeljnih pojmova kibernetičke sigurnosti među učenicima srednjih škola. Kviz je riješilo 268 učenika sa ukupno zabilježeno 297

pristupa. Izuzeti su svi prazni i polovični zapisi kao i višestruki pokušaji rješavanja kviza zabilježeni na osnovi sesija.
Od ukupno 297 zapisa o pristupu kvizu, iz obrade je izuzeto ukupno 9,76% zapisa. S obzirom na svaku školu zasebno izuzeto je nominalno 9 od 95, tj. 9,47% zapisa iz Gimnazija „Matija Mesić" Slavonski Brod; zatim, nominalno 12 od 163, 7,36% iz Gimnazija Požega i nominalno 8 od 39, 20,51% iz I. Gimnazija Osijek. U obradu je ukupno uzeto 268 zapisa.
Rezultati ovog istraživanja se djelomično podudaraju sa prethodnim nalazima (Witsenboera, Sijtsme i Scheelea 2022), koji su utvrdili da nizozemski srednjoškolci pokazuju osnovno razumijevanje lozinki i privatnosti i slabije rezultate na temama poput phishinga i enkripcije. U našem slučaju, samo 57,84% ispitanih je uspješno prepoznalo sve navedene tipove osobnih podataka.
Ovakav rezultat se djelomično može pripisati činjenici kako je pitanje o prepoznavanju osobnih podataka, prvo od dvanest pitanja – ujedno bilo i jedino pitanje u kojemu su svi navedeni odgovori bili točni što je moguće navelo ispitanike da pretpostave da je barem jedan od navdenih odgovora netočan. Međutim, više od polovice ispitanika je pokazalo nepobitno znanje o raspoznavanju vrsta osobnih podataka.
Od četiri ponuđena odgovora, vidljiva na slici 2, najproblematičniji tip podataka za raspoznavanje je bila E-mail adresa koja je ostala neidentificirana kao osobni podatak u 67,26% od 113 netočnih odgovora na ovo pitanje, zatim otisak prsta u 56,64% odgovora, datum rođenja u 28,32% te ime i prezime u 27,43% netočnih odgovora.



Slika 2: Pitanje o osobnim podacima

Tablica 1. Uspješnost po tematskim cjelinama

Ukupno	Netočno	Točno	Točno %	Pitanja iz tematske cjeline
268	2	266	99,25%	Stvaranje sigurnih lozinki
268	5	263	98,13%	Razumijevanje digitalnog traga
268	7	261	97,39%	Postupanje sa sumnjivim e-mailovima
268	12	256	95,52%	Privatnost na društvenim mrežama
268	13	255	95,15%	Rizici ponovne upotrebe lozinki
268	17	251	93,66%	Važnost ažuriranja uređaja
268	18	250	93,28%	Digitalna higijena i sigurnosne navike
268	34	234	87,31%	Razumijevanje enkripcije
268	40	228	85,07%	Prepoznavanje phishing poruka
268	63	205	76,49%	Prepoznavanje ransomware prijetnji
268	72	196	73,13%	Razumijevanje dvofaktorske autentifikacije
268	113	155	57,84%	Prepoznavanje osobnih podataka

3.1. Ukupna uspješnost

Prosječna točnost rješavanja kviza iznosila je 87,69%, što ukazuje na zadovoljavajuću razinu znanja o osnovnim pojmovima teme digitalne sigurnosti. Najveća koncentracija točnih odgovora zabilježena je kod pitanja vezanih uz odabir najsigurnije forme lozinke i razumijevanje digitalnog traga, dok su najlošiji rezultati postignuti u temama koje se odnose na prepoznavanje vrsta osobnih podataka, dvofaktorsku autentifikaciju i poznavanje pojma ransomwarea.

U cilju dublje evaluacije odnosa između vremena potrebnog za rješavanje kviza i razine točnosti odgovora, provedena je korelacijska analiza. Izračunata su dva koeficijenta korelacije: Pearsonov koeficijent za ispitivanje linearne povezanosti te Spearmanov koeficijent za monotoni odnos između varijabli.

Rezultati analize pokazali su da je Pearsonova korelacija iznosila 0,012, dok je Spearmanova korelacija iznosila 0,015. Oba su koeficijenta vrlo blizu nuli, što upućuje na izostanak značajne linearne i monotone povezanosti između točnosti rješavanja kviza i ukupnog vremena potrebnog za njegovo ispunjavanje. Drugim riječima, brzina odgovaranja učenika nije bila presudan faktor za uspješnost.

Također je uzet u obzir i tip uređaja u odnosu na brzinu rješavanja te je korišten neparametrijski test (Mann-Whitney U) jer je tip uređaja kategorička varijabla. Utvrđeno da nema statistički značajne razlike u vremenu rješavanja između korisnika Android i iOS uređaja ($p > 0.05$) ondosno $p=0.951$.

Mann-Whitney U test je korišten i pri analizi korelacije točnosti i tipa uređaja. Rezultati analize po tipu uređaja ukazuju na blagu razliku u točnosti između korisnika Android i iOS uređaja. Kao što je prikazano u Tablici 2., sudionici koji su pristupili kvizu putem Android uređaja postigli su višu prosječnu točnost (83,84 %) i viši medijan točnosti (93 %), u usporedbi s korisnicima iOS uređaja, čija je prosječna točnost iznosila 79,94 %, a medijan 80 %. Raspon točnosti bio je širi kod iOS korisnika (33 % – 100 %) nego kod Android korisnika (47 % – 100 %), što ukazuje na veću varijabilnost rezultata unutar te skupine.

Kako bi se ispitala statistička značajnost ove razlike, proveden je Mann-Whitney U test, koji je prikladan za usporedbu dviju nezavisnih skupina kada se ne može pretpostaviti normalna distribucija. Rezultati testa pokazali su da razlika nije statistički značajna ($U=9820,5$; $p= 0,075$), iako se može uočiti trend u korist Android korisnika. Stoga se razlike u postotku točnih odgovora po tipu uređaja ne mogu tumačiti kao sustavne, ali rezultati mogu poslužiti kao polazište za buduća istraživanja o utjecaju korisničkog sučelja, veličine zaslona ili operacijskog sustava na izvedbu u digitalnim obrazovnim alatima.

Za buduća istraživanja preporučuje se detaljnija analiza potencijalnog utjecaja tehničkih čimbenika, poput veličine zaslona, responzivnosti sučelja i brzine prikaza kviza na različitim operacijskim sustavima, s ciljem boljeg razumijevanja kako tehnološki aspekti mogu oblikovati izvedbu učenika u digitalnim edukacijskim okruženjima.

Tablica 2. Rezultati analize točnosti po tipu uređaja

Tip uređaja	Broj sudionika	Prosječna točnost	Medijan točnosti	Raspon točnosti
Android	149	83,84 %	93 %	47 % – 100 %
iOS	119	79,94 %	80 %	33 % – 100 %

3.2. Obrasci razumijevanja

Rezultati ukazuju na to da forma pitanja s višestrukim točnim odgovorima može utjecati na uspješnost odgovaranja, što sugerira postojanje kognitivne pristranosti među učenicima. Naime, značajan broj učenika nije prepoznao sve osobne podatke, iako su svi ponuđeni odgovori bili točni. Takva pristranost, gdje učenici sumnjaju u mogućnost da su svi odgovori točni, može se povezati s iskustvom iz školskog konteksta gdje se rijetko koristi ta struktura pitanja. Buduće obrazovne strategije mogle bi uključivati eksplicitno upoznavanje učenika s različitim vrstama ispitnih formata kako bi se minimizirao utjecaj pretpostavki na točnost odgovora.

4. Zaključak

Doprinos rada očituje se u primjeni digitalnog kviza kao suvremenog alata za evaluaciju znanja o kibernetičkoj sigurnosti među srednjoškolcima u Hrvatskoj, što predstavlja empirijski utemeljenu osnovu za razvoj obrazovnih strategija u području digitalne sigurnosti. Istraživanje je pokazalo da srednjoškolci posjeduju zadovoljavajuću razinu znanja o osnovnim konceptima kibernetičke sigurnosti. Najbolje rezultate učenici su postigli u temama koje se odnose na stvaranje sigurnih lozinki i razumijevanje digitalnog traga, dok su slabiji rezultati zabilježeni kod pitanja prepoznavanja osobnih podataka, dvofaktorsku autentifikaciju i ransomware. Rezultati upućuju na potrebu za edukacijom u tehnički zahtjevnijim aspektima digitalne sigurnosti.
Analize su pokazale da ne postoji značajna povezanost između vremena rješavanja kviza i točnosti odgovora, kao ni između tipa uređaja i uspješnosti. Zapaženo je da su učenici iskazali nižu uspješnost na pitanju koje je sadržavalo višestruke točne odgovore, što može ukazivati na prisutnost kognitivne pristranosti uvjetovane iskustvom sa tradicionalnim evaluacijskim formama.

Dobiveni rezultati potvrđuju važnost ranog i strukturiranog uključivanja tema kibernetičke sigurnosti u srednjoškolski kurikulum, uz primjenu suvremenih i interaktivnih obrazovnih alata poput digitalnih kvizova. Nadalje, predložena su buduća istraživanja koja bi mogla ispitati utjecaj tehničkih čimbenika i različitih formata pitanja na učenikovu izvedbu, čime bi se doprinijelo oblikovanju učinkovitijih obrazovnih strategija u području digitalne sigurnosti.

5. Literatura

Adams, M., & Makramalla, M. (2017). Cybersecurity skills training: An attacker-centric gamified approach. Technology Innovation Management Review, 7(4), 12–18. https://timreview.ca/article/861

ENISA. (2020). Cybersecurity skills development in EU. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

European Commission: European Education and Culture Executive Agency. (2022). Informatics education at school in Europe. Publications Office of the European Union. https://data.europa.eu/doi/10.2797/268406

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity. Sustainability, 14(8), 4763. https://doi.org/10.3390/su14084763

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186, 104536. https://doi.org/10.1016/j.compedu.2022.104536

ASSESSING CYBERSECURITY KNOWLEDGE AMONG HIGH SCHOOL STUDENTS USING A DIGITAL QUIZ

Abstract: This paper examines the level of cybersecurity knowledge among high school students using a digital quiz. The aim was to identify areas of strong awareness as well as those requiring additional education. A quantitative approach was employed, based on a structured digital quiz conducted among 268 students from three grammar schools, with data analyzed using descriptive and correlational statistics. The results indicate a high overall accuracy rate (87.69%), with the highest scores in topics related to password security and digital footprints, and the lowest in identifying personal data, ransomware, and two-factor authentication (2FA). No significant correlations were found between accuracy and completion time, nor between device type and performance. The study highlights the importance of structured cybersecurity education in secondary schools.

Keywords: Cybersecurity, Digital assessment, Educational measurement, Grammar schools, Statistical analysis