Bezbednosne navike i percepcija privatnosti među studentima IT-a

Aksović David 1048/2025,Lazarević Nikola 1043/2025,
Marko Irina 1134/2025, Vučković Ivana 1033/2025,
davidaksovic@outlook.com, nikola9100@gmail.com,
irina.marko@gmail.com, ivanavu00@gmail.com

Decembar 2025

Sažetak

U eri u kojoj sajber kriminal beleži godišnji rast troškova od preko 31%, studenti informacionih tehnologija predstavljaju trenutne ili buduće profesionalce koji će biti odgovorni za bezbednost digitalnih sistema, ali i grupu koja treba da poseduje znanje i navike za zaštitu sopstvenih ličnih podataka. Ovaj rad istražuje stavove 87 studenata IT smerova prema sajber bezbednosti i čuvanju privatnosti, sa ciljem da identifikuje glavne prepreke u usvajanju bezbednosnih navika. Rezultati pokazuju da povećana osvešćenost o bezbednosnim rizicima direktno utiče na primenu temeljnijih bezbednosnih praksi. Analiza bezbednosnih navika pokazuje da studenti preferiraju pasivne zaštitne mere integrisane u aplikacije nad samostalnim konfigurisanjem sistema, pri čemu gotovo polovina (47.1%) nije podesila nijedno bezbednosno podešavanje. Studenti sa iskustvom sajber incidenata pokazuju značajno bolje bezbednosne prakse, što ukazuje da je negativno iskustvo snažan motivator za usvajanje i primenu zaštitnih mera.

Sadržaj

1 Uvod

Razvoj interneta i digitalnih servisa doveo je do toga da se svakodnevne aktivnosti poput komunikacije, rada i finansijskih transakcija oslanjaju na digitalne tehnologije zbog čega su digitalna bezbednost i zaštita privatnosti od velikog značaja. Česta upotreba ovih servisa neretko podrazumeva slanje ličnih i osetljivih podataka, čime se korisnici izlažu različitim bezbednosnim rizicima.

Savremena istraživanja pokazuju da su sajber napadi u poslednjih nekoliko godina ne samo učestaliji, već i tehnički složeniji, što predstavlja dodatni izazov za tradicionalne bezbednosne mehanizme i odbranu organizacija i korisnika [9]. Čak i obrazovne institucije u Srbiji, poput Matematičkog fakulteta u Beogradu, bile su meta phishing napada, što pokazuje da nijedna organizacija nije potpuno imuna na ove pretnje.

Prethodna istraživanja otkrivaju jaz između teorijskog znanja i praktične primene bezbednosnih mera kod univerzitetskih studenata. Rad "Istraživanje svesti univerzitetskih studenata o sajber bezbednosti" [5] pokazuje da studenti poseduju visoku osvešćenost o određenim aspektima sajber bezbednosti, ali im nedostaje adekvatno znanje o samozaštiti, dok se u radu "Svesti o sajber bezbednosti među univerzitetskim studentima: studija slučaja" [2] otkriva nesklad u kojem studenti tvrde da poseduju osnovno bezbednosno znanje, ali nisu usvojili bezbednosne navike, loše upravljaju lozinkama i ne prepoznaju phishing napada. Ključan nalaz ovih studija je odsutnost formalnih programa sajber bezbednosti na univerzitetima. Međutim, većina studija fokusirana je na opštu studentsku populaciju, dok su IT studenti kao specifična grupa nedovoljno istraženi, posebno u kontekstu srpskog obrazovnog sistema.

Ovo istraživanje fokusirano je na studente IT smerova, budući da se od njih očekuje visok nivo informisanosti u oblasti digitalne bezbednosti. Cilj je da se ispita njihovo mišljenje o rizicima i primena bezbednosnih praksi, jer njihove navike sada mogu uticati na spremnost da prepoznaju i izbegnu pretnje, poput phishing napada, u profesionalnom okruženju. Analiza njihovih stavova i ponašanja pruža uvid u nivo informisanosti, prisutne zablude i potencijalne rizike unutar ove populacije.

Anketa je osmišljena da pokaže kako studenti IT smerova zaista funkcionišu u digitalnom svetu - koje mere zaštite koriste, koliko su ih svesni i šta zanemaruju. Prvi deo rada fokusira se na navike studenata u praksi, kako osnovne, tako i napredne, i istražuje faktore koji utiču na njihove odluke. Drugi deo rada posvećen je privatnosti - analizira se kako studenti štite svoje podatke, koliko su svesni praćenja svojih online aktivnosti i koje strategije primenjuju kako bi sačuvali lične informacije.

Rezultati otkrivaju da većina studenata ocenjuje visoko svoje znanje o sajber bezbednosti, ali ne prati većinu bezbednosnih mera. Analiza pokazuje da povećana svest o sajber bezbednosti direktno utiče na broj primenjenih bezbednosnih praksi. Studenti pokazuju veću sklonost ka korišćenju pasivnih bezbednosnih mera nego samostalnom konfigurisanju zaštitnih podešavanja, dok oni koji su bili žrtve incidenata demonstriraju

značajno bolje bezbednosne navike. Kao najveća prepreka identifikovan je nedostatak znanja, pri čemu skoro polovina studenata tokom studija nije imala organizovanu obuku iz digitalne bezbednosti, što ukazuje na potrebu za sistematskom edukacijom budućih IT profesionalaca.

2 Metodologija i profil ispitanika

Istraživanje je sprovedeno kroz online anketu na uzorku od 87 studenata informacionih tehnologija različitih nivoa obrazovanja. Uzorak obuhvata studente osnovnih studija (78.2%), master studija (20.7%), i doktorskih studija (1.1%), pri čemu je većina iz oblasti informatike (65.5%) i softverskog inženjerstva (18.4%). Upitnik je sadržao 30 pitanja fokusiranih na percepciju privatnosti, konkretne bezbednosne navike, korišćenje zaštitnih alata, i barijere za primenu zaštitnih praksi.

Značajan broj ispitanika (54.0%) radi pored studija, 34.5% full-time, 14.9% part-time, i 4.6% kao praktikant. Među onima koji rade, 72.3% je zaposleno u IT oblasti, što omogućava analizu uticaja praktičnog iskustva na bezbednosne navike. Raspodela operativnih sistema pokazuje iznad proseka zastupljenost Linux korisnika (35.6%) u poređenju sa opštom populacijom, što ukazuje na tehnički osvešćeniju grupu.

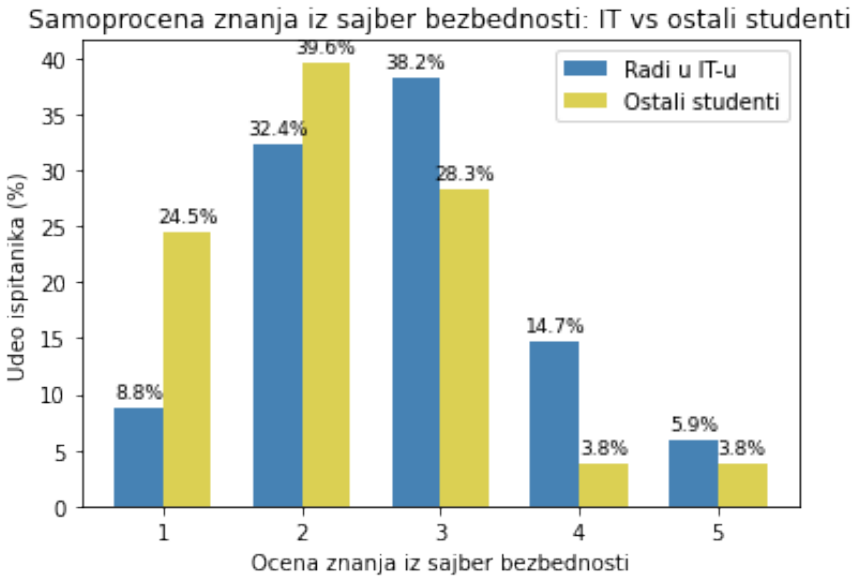
3 Bezbednost

Sajber bezbednost je veoma važna veština za IT stručnjake, jer njihove lične navike u zaštiti podataka direktno utiču na to kako će u budućnosti štititi i održavati bezbednost sistema u kojima rade. Korporativne informacije i tehnološke usluge su ranjive na razne bezbednosne rizike u današnjem informacionom okruženju, uključujući curenje osetljivih podataka i produžene prekide u pristupu e-pošti i internetu, što sve značajno utiče na kontinuitet poslovanja[3]. Bezbednosni rizici se ne odnose isključivo na korporativno okruženje, poznavanje sajber bezbednosti je podjednako važno za zaštitu ličnih podataka, s obzirom da su naši životi duboko digitalni, a osetljive informacije (finansijske, zdravstvene, o identitetu) su konstantno izložene rizicima od krađe, prevare i štete po reputaciju

3.1 Samoocena bezbednosnog znanja

Na pitanje o opštem poznavanju sajber bezbednosti, 16 ispitanika (18.4%) ocenilo je sopstveno znanje ocenom 1, dok je 32 ispitanika (36.8%) dalo ocenu 2. Ocenu 3 dodelilo je 28 ispitanika (32.2%), ocenu 4 svega 7 ispitanika (8.0%), a najvišu ocenu samo 4 ispitanika (4.6%). Ovi rezultati ukazuju da se većina studenata (55.2%) ne oseća kompetentno u oblasti sajber bezbednosti.

Sa prikazanog grafikona uočava se da studenti koji rade u IT sektoru procenjuju svoje znanje iz sajber bezbednosti višim ocenama u poređenju sa studentima koji ne rade u IT-u. Posebno je izražena razlika kod srednjih



Slika 1: Samoprocena znanja o sajber bezbednosti: ljudi koji rade u IT i oni koji ne rade

i viših ocena (3 i 4), koje su znatno zastupljenije među IT studentima, dok su niže ocene češće kod druge grupe.

Kada je reč o poznavanju specifičnih bezbednosnih pretnji (Tabela 1), uočavaju se razlike. Ispitanici su pokazali najveće samopouzdanje u prepoznavanju phishing napada (43.7% ocena 5) i malware-a (26.4% ocena 5), dok su najmanje upoznati sa MITM napadima (37.9% ocena 1) i ransomware-om (33.3% ocena 1).

Tabela 1: Samoprocena poznavanja bezbednosnih pretnji

Ocena	**Phishing**	**Ransomware**	**MITM**	**Social Eng.**	**Malware**
1 (najslabije)	4 (4.6%)	29 (33.3%)	33 (37.9%)	24 (27.6%)	4 (4.6%)
2	5 (5.7%)	16 (18.4%)	9 (10.3%)	15 (17.2%)	6 (6.9%)
3	20 (23.0%)	14 (16.1%)	20 (23.0%)	20 (23.0%)	25 (28.7%)
4	20 (23.0%)	13 (14.9%)	12 (13.8%)	10 (11.5%)	29 (33.3%)
5 (najbolje)	38 (43.7%)	15 (17.2%)	13 (14.9%)	18 (20.7%)	23 (26.4%)

Ovi rezultati ukazuju da ispitanici bolje razumeju pretnje sa kojima se češće susreću u svakodnevnom korišćenju interneta, poput phishing napada i malware-a. S druge strane, slabo poznavanje MITM napada i ransomware-a ukazuje na nedostatak znanja o složenijim oblicima napada iako ove pretnje mogu imati ozbiljne posledice po bezbednost sistema i podataka.

3.2 Percepcija ličnih bezbednosnih sposobnosti

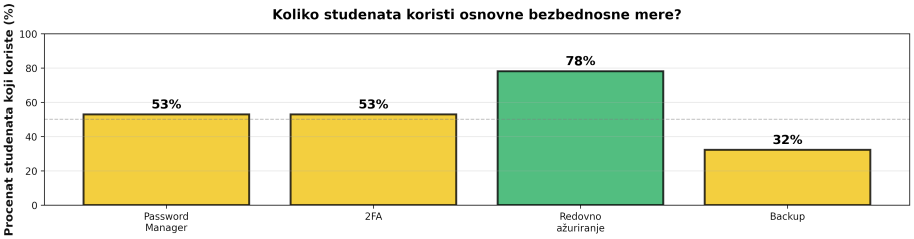
Većina ispitanika pokazala je visoko samopouzdanje u prepoznavanju phishing poruka - 82.8% ocenilo je svoju sposobnost ocenama 4 i 5, dok je dodatnih 10.3% dalo ocenu 3. Ovakav rezultat može biti posledica činjenice da je Matematički fakultet u prethodne dve godine bio česta meta phishing napada, što je studentima pružilo praktično iskustvo u prepoznavanju ovakvih pretnji.

Međutim, situacija je kompleksnija kod zaštite ličnih podataka na internetu. Samo 6.9% ispitanika se oseća potpuno sigurno u ovu sposobnost (ocena 5), dok je 36.8% dalo ocenu 4. Značajan deo ispitanika (33.3%) ocenio je svoju sposobnost sa 3, što ukazuje na izvesnu nesigurnost, dok je čak 23.0% dalo ocene 1 ili 2.

Kada je reč o razumevanju posledica curenja podataka i kompromitovanja naloga, 31.0% studenata ocenilo je svoje razumevanje kao odlično, 27.6% kao vrlo dobro, i 24.1% kao dobro. Međutim, zabrinjavajućih 17.2% studenata ocenilo je svoje razumevanje ovih posledica kao dovoljno (12.6%) ili nedovoljno (4.6%). Kombinacija nesigurnosti u zaštiti ličnih podataka i nedovoljnog razumevanja posledica kompromitovanja naloga ukazuje na važan problem, iako studenti IT-a mogu identifikovati pretnju kada se pojavi, ne razvijaju bezbednosne navike niti u potpunosti razumeju dugoročne posledice zanemarivanja sajber bezbednosti.

3.3 Bezbednosne navike

Savremeni sajber kriminal karakteriše visoka sofisticiranost napada i veliki broj potencijalnih meta, što je posledica tehnološkog razvoja i širenja digitalnih platformi [1]. U takvom okruženju, bezbednosne navike korisnika imaju ključnu ulogu u smanjenju izloženosti sajber pretnjama.



Slika 2: Procenat korišćenja osnovnih bezbednosnih mera

Većina studenata redovno ažurira operativni sistem, bilo da koriste automatsko ažuriranje ili redovno kada dobiju obaveštenje. Polovina (52.8%) ispitanika koristi dvofaktorsku autentifikaciju na svim ili većini važnih naloga, dok 33% samo na nekim nalozima. Skoro polovina studenata (47.1%) ne koristi menadžer lozinki. Samo trećina studenata redovno pravi kopije važnih podataka, dok 26% radi to povremeno.

Analiza primene bezbednosnih praksi otkriva značajne nedostatke. Iako većina studenata izbegava preuzimanje fajlova sa nepouzdanih izvora (67.8%) i koristi ad-blockere (65.5%), svega trećina (32.2%) proverava

HTTPS pre unošenja osetljivih podataka ili se redovno odjavjuje sa naloga. Samo polovina ispitanika koristi privatni režim browsera (47.1%) ili razdvaja email adrese prema nameni (47.1%), što su osnovne mere za zaštitu privatnosti.

Za razliku od relativno visokih stopa primene pasivnih bezbednosnih praksi, samostalno konfigurisanje aktivnih bezbednosnih mera pokazuje niže rezultate. Skoro polovina ispitanika (47.1%) nije samostalno konfigurisala nijedno od navedenih bezbednosnih podešavanja. Najčešće konfigurisana postavka je VPN (32.2%), zatim antivirusni softver (29.9%), dok naprednije mere kao što su firewall (19.5%), šifrovanje diska (17.2%) i bezbednost rutera (12.6%) primenjuje samo manjina studenata.

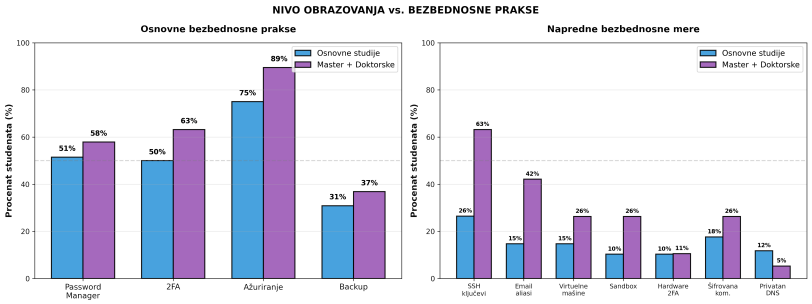
Uočava se obrazac gde su mere koje su integrisane u postojeće aplikacije ili imaju jasne grafičke interfejse (VPN, antivirus) zastupljenije od onih koje zahtevaju viši nivo tehničkog znanja i nisu deo uobičajene korisničke rutine.

Primena naprednih bezbednosnih tehnika dodatno naglašava razliku između teorijskog znanja i praktične primene. SSH ključevi, koje koristi 34.5% ispitanika, predstavljaju izuzetak jer su praktično neophodni za svakodnevni rad sa alatima za kontrolu verzije i serverima. Međutim, tehnike koje nisu direktno neophodne za akademske radove ili rad sa kodom poput virtuelnih mašina za rizične aktivnosti (17.2%), sandbox okruženja (13.8%), ili hardware tokena za autentifikaciju (10.3%) ostaju retko primenjivane uprkos njihovoj efikasnosti. Samo 10.3% studenata redovno proverava da li su njihovi podaci kompromitovani što ponovo potvrđuje hipotezu češće upotrebe pasivnijih mera.

Upravljanje lozinkama predstavlja jednu od ključnih mera zaštite u sajber bezbednosti, a ponašanje korisnika u toj oblasti značajno utiče na nivo njihove lične zaštite. Iako više od polovine ispitanika (54,0%) navodi da izbegava jednostavne kombinacije, gotovo polovina (44.8%) i dalje koristi istu ili sličnu lozinku za više naloga, što predstavlja ozbiljan bezbednosni rizik. Takođe 17.2% studenata bira lako pamtljive lozinke, što može dodatno umanjiti nivo zaštite. Rezultati jasno pokazuju da većina studenata retko menja lozinke na važnim nalozima, 31% nikada osim ako sistem zahteva, 36,8% vrlo retko, a 14,9% povremeno, (10,3%) ispitanika menja lozinku samo kada dobije obaveštenje o curenju podataka. Samo 6,9% ispitanika redovno menja lozinke (svakih 2–3 meseca), što ukazuje na nedovoljnu doslednost u primeni jedne od osnovnih bezbednosnih mera.

Promena lozinke kao primarni odbrambeni mehanizam kod studenata nakon incidenta, ubedljivo najčešća reakcija je promena lozinke (40.23%). Ovo potvrđuje da studenti prepoznaju lozinku kao prvu liniju odbrane, ali takođe ukazuje na to da se promene lozinki često dešavaju reaktivno (tek nakon problema), a ne proaktivno.

Zanimljivo je primetiti da studenti master i doktorskih studija u gotovo svim bezbednosnim navikama postižu bolje rezultate od studenata osnovnih studija. Master i doktorski studenti su spojeni u jednu grupu jer je anketu popunio samo jedan doktorant. Razlika može biti posledica razvijenijih profesionalnih navika, većeg iskustva sa digitalnim alatima ili jednostavno većeg osećaja odgovornosti za zaštitu podataka.



Slika 3: Paralela korišćenja osnovnih bezbednosnih mera studenata osnovnih studija i studenata master i doktorskih studija

3.4 Iskustva sa incidentima

Procenjuje se da će godišnji troškovi sajber kriminala ostvariti +31% projektovani rast na godišnjem nivou u odnosu na 2024. godinu[6]. Ovi trendovi pokazuju da će studenti IT smerova, kao budući profesionalci, snositi značajnu odgovornost za zaštitu i održavanje bezbednosti sistema.

Podaci pokazuju da manje od polovine ispitanika (40,23%) tvrdi da nikada nije bila meta napada. Oko 60% studenata ili je doživelo neki sajber incident, ili nije sigurno da li su bili meta, što ukazuje da su studenti IT-a često izloženi rizicima, uprkos pretpostavljenom tehničkom znanju.

Paradoks visoke stope viktimizacije jeste da studenti koji redovno koriste menadžer lozinki (što je jedna od najvažnijih bezbednosnih praksi) imaju najvišu stopu viktimizacije (52.17%). Studenti koji ne koriste menadžer lozinki imaju značajno nižu stopu viktimizacije (37.93%).

Korišćenje menadžera lozinki	**Stopa viktimizacije**
Redovno koriste	52.17%
Ne koriste	37.93%

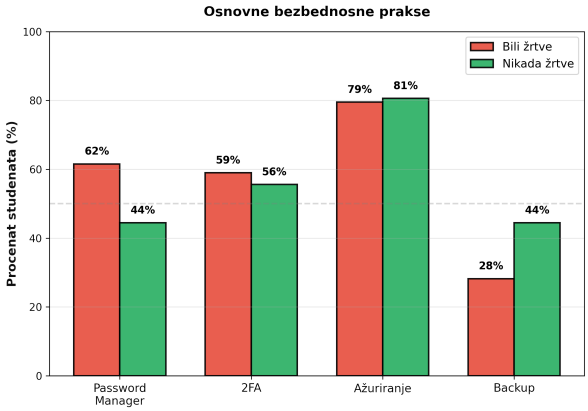
Tabela 2: Prikaz stope viktimizacije u odnosu na korišćenje menadžera lozinki

Možda su studenti koji su već bili žrtve incidenta bili motivisani da počnu redovno da koriste menadžer lozinki.

Prema rezultatima ankete 41.4% studenata nikada nije bila žrtva incidenata, dok 14.9% njih nije sigurno. Većina ostalih studenata bila je žrtva phising napada (20%) ili su im kompromitovani nalozi (18.4%). Njih 14.9%

su bili zaraženi virusom , dok je manji broj njih bio žrtva ransomware napada (4.6%) ili su im ukradeni podaci sa kartice (2.3%).

Kao odgovor na napad samo 46.7% studenata je analiziralo i preduzelo dodatne mere zaštite, dok je više od pola (62.2%) promenilo lozinku. Neki studenti su kao odgovor aktivirali dvofaktorsku autentifikaciju (35.6%) a 20% njih je prijavilo problem nadležnim institucijama. Čak 13.3% studenata nije preduzelo nikakve mere. Iako je kompromitovanje naloga vodeći incident, samo 12.64% studenata je nakon napada aktiviralo dvofaktorsku autentifikaciju (2FA). Ovo je propuštena prilika za dugoročno osiguravanje naloga, s obzirom na to da je 2FA efikasnija zaštita od ponovnog kompromitovanja nego sama promena lozinke.



Slika 4: Poređenje bezbedonosnih navika studenata koji su bili žrtve sajber napada i onih koji nisu

Slika 4 prikazuje da studenti koji su bili žrtva sajber napada redovno i automatski koriste menadžer lozinki i dvofaktorsku autentifikaciju. Između dve grupe studenata nema razlike u učestalosti ažuriranja ali studenti koji nikada nisu bili žrtve redovnije prave kopije podataka. Rezultati ankete pokazuju da nema značajne razlike u navikama primena naprednih mera između studenata koji su bili žrtva napada i onih koji nisu osim virtuelnih mašina gde je 15% više studenata koji koriste virtuelnu mašinu za rizične aktivnosti.

Tabela 3: Poređenje sigurnosti između studenata koji su bili žrtve incidenata i onih koji nisu

Ocena	**1**	**2**	**3**	**4**	**5**
studenti sa incidentom	5%	21%	36%	26%	13%
studenti bez incidenta	3%	19%	33%	42%	3%

Studenti koji nisu imali iskustvo sa sajber incidentima češće daju više

ocene, što može ukazivati na lažan osećaj sigurnosti, oslanjanje na osnovne mere zaštite i nedostatak svesti o realnim pretnjama. Sa druge strane, studenti koji su bili žrtve incidenata češće biraju srednje ocene, što može ukazivati na realističniju procenu sopstvenog znanja, veću svest o sopstvenim ograničenjima i bolje razumevanje složenosti sajber pretnji nakon negativnog iskustva. Iako studenti bez incidenata u proseku češće daju visoke ocene među studentima koji su bili žrtve sajber incidenata postoji veći procenat onih koji su dali najvišu ocenu (5). Ovaj rezultat može ukazivati na to da su pojedini studenti, nakon pretrpljenog incidenta, unapredili svoje znanje i bezbednosne prakse što je dovelo do povećanog osećaja sigurnosti. Značajan procenat studenata (13.79%) je izjavio da "nisu sigurni" da li su bili žrtve. Ovo je važan podatak jer ukazuje na potencijalnu nemogućnost detekcije suptilnijih napada (npr. spyware ili tiho curenje podataka) čak i kod tehnički pismenije populacije.

4 Privatnost

Digitalna privatnost predstavlja jedan od centralnih izazova savremenog informacionog društva, pri čemu studenti informacionih tehnologija zauzimaju specifičnu poziciju. Naime oni su istovremeno korisnici digitalnih servisa i budući kreatori rešenja koja će oblikovati privatnost ljudima. Njihove lične navike i percepcija privatnosti direktno utiču na profesionalne odluke koje će donositi u karijeri, od implementacije privacy-by-design (PbD) principa do izbora bezbednosnih protokola u korporativnim sistemima [10].

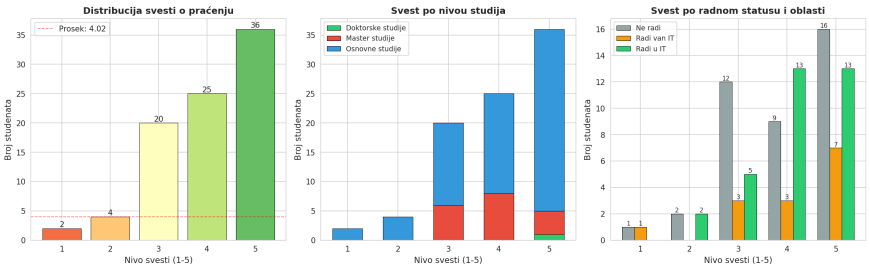
Uprkos formalnom obrazovanju u oblasti informacionih tehnologija, ostaje otvoreno pitanje koliko studenti razumeju koncepte privatnosti i da li to razumevanje prelazi u konkretne bezbednosne navike. Prethodna istraživanja ukazuju na postojanje jaza između teorijskog znanja i praktične primene, što motiviše dalju analizu [12].

4.1 Samoprocena svesti o praćenju online aktivnosti

Ispitanici su na skali od 1 do 5 procenili svoju svest o praćenju online aktivnosti prosečnom ocenom 4.02, pri čemu je 70.1% dalo ocene 4 ili 5, a samo 6.9% ocene 1-2. Ova visoka samoprocena ukazuje da studenti IT-a smatraju da dobro razumeju problem digitalnog praćenja. Istraživanja pokazuju da studenti koji imaju formalno IT obrazovanje pokazuju višu svest o bezbednosnim pretnjama, ali da ta svest često nije u korelaciji sa praktičnom primenom zaštitnih mera [11]. Slika 5 prikazuje ukupnu distribuciju svesti sa razlaganjem po nivou studija i radnom statusu.

4.2 Primena alata i tehnologija za zaštitu privatnosti

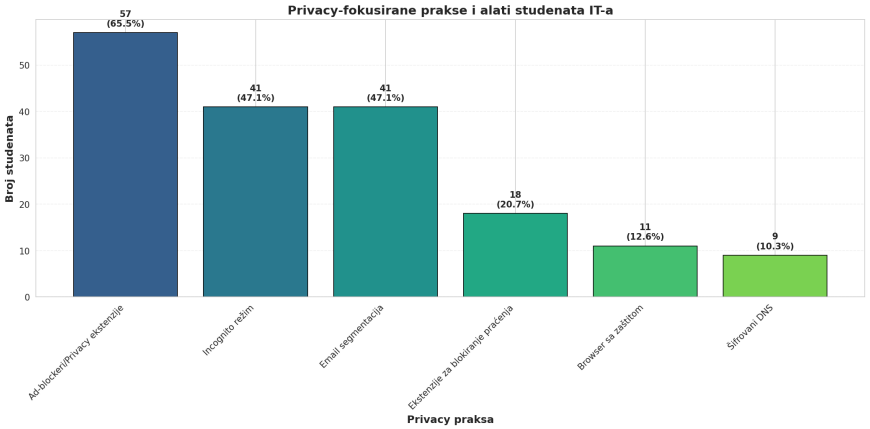
Praktična primena zaštitnih mera, međutim, značajno zaostaje za samoprocenom. Manje od polovine studenata (41.4%) aktivno koriste VPN, pri čemu je raspodela sledeća: 48.3% ne koristi, 26.4% koristi povremeno,



Slika 5: Samoprocena svesti o praćenju online aktivnosti

a samo 11.5% koristi redovno. Zabrinjavajuće je da 8.0% ispitanika nije upoznato sa konceptom VPN-a.

Kada je reč o drugim alatima, situacija je nešto bolja (Slika 6). Naime, 65.5% studenata koristi ad-blockere i privacy ekstenzije, dok 47.1% implementira segmentaciju email adresa, što predstavlja naprednu praksu koja se retko viđa. Međutim, samo 20.7% koristi naprednije alate za blokiranje praćenja, uprkos tome što su ekstenzije poput uBlock Origin i Privacy Badger besplatne, open-source, i dostupne direktno iz pretraživača.



Slika 6: Učestalost primene alata i praksi fokusiranih na privatnost

4.3 Pristanak i transparentnost

4.3.1 Uslovi korišćenja

Čitanje uslova korišćenja predstavlja kritičnu slabost. Samo 10.3% ispitanika redovno čita uslove pre prihvatanja, dok 42.5% nikada ih ne čita, a 47.1% čita ponekad. To znači da gotovo 90% studenata prihvata uslove bez razumevanja šta odobravaju, što je posebno problematično kod budućih IT profesionalaca koji će biti odgovorni za kreiranje i implementaciju

privacy politika. Ova praksa nije iznenađujuća. Naime, prosečnom korisniku bi bilo potrebno približno 76 radnih dana godišnje da pročita sve uslove servisa koje koristi, a kompleksnost teksta često zahteva ekspertizu [7].

4.3.2 Upravljanje kolačićima

Suprotno tome, upravljanje kolačićima pokazuje pozitivne rezultate (Slika 7). Naime, 75.9% studenata odbija sve osim neophodnih kolačića, dok dodatnih 19.5% blokira third-party kolačiće kroz podešavanja pregledača. Međutim, implementacija GDPR direktive iz 2018. godine, koja zahteva eksplicitni pristanak, dovela je do pojave "dark patterns" tehnika koje guraju korisnike ka opciji "Prihvati sve" kroz istaknuto dugme, dok opcija odbijanja zahteva navigaciju kroz više nivoa menija [8].

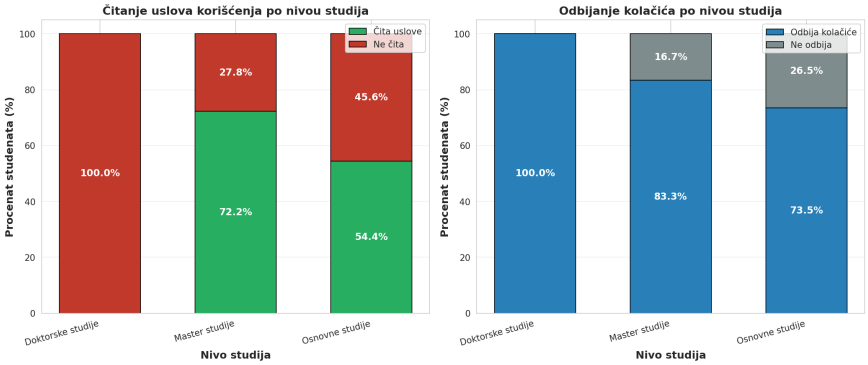
4.3.3 Dozvole aplikacija

Dodatni aspekt informisanog pristanka odnosi se na dozvole mobilnih i desktop aplikacija (Slika 8). Analiza pokazuje da 18.4% studenata uvek proverava dozvole pre instalacije, dok 24.1% često proverava, što ukazuje na razumnu opreznost. Međutim, 27.6% retko ili nikada ne proverava dozvole, što predstavlja rizično ponašanje jer aplikacije mogu zahtevati pristup podacima koji nisu neophodni za njihovu funkcionalnost. Nedavne analize Android aplikacija pokazuju da preko 80% traži dozvole koje prevazilaze osnovnu funkcionalnost, koristeći strategiju "permission creep" gde svaka nova verzija zahteva dodatne pristupe [4].

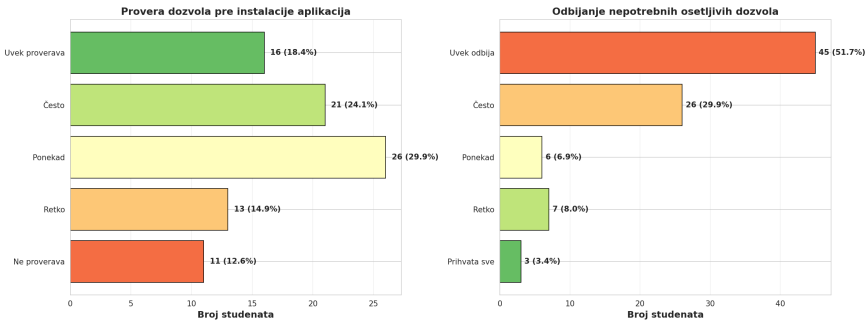
Kod upravljanja osetljivim dozvolama (kamera, mikrofon, lokacija), većina studenata (51.7%) uvek odbija nepotrebne zahteve, dok 29.9% često odbija. Samo 3.4% prihvata sve što aplikacija traži bez evaluacije neophodnosti. Ovi podaci pokazuju da su studenti generalno oprezni prema osetljivim dozvolama, ali ne proveravaju rutinski sve dozvole prilikom instalacije, što može biti posledica zamora (permission fatigue). Prethodno navedeno podrazumeva da korisnici automatski, bez detaljnog pregleda, prihvataju dugačke liste dozvola.

4.4 Rizično ponašanje

Dodatni kontekst pruža analiza korišćenja javnih računara i tuđih uređaja. Većina studenata pokazuje oprezno ponašanje. Prosečna ocena za pristup email-u na javnim računarima iznosi 2.1/5, za online kupovinu 1.8/5, dok je za bankarstvo najniža sa 1.4/5. Ovi podaci ukazuju da studenti intuitivno prepoznaju rizike korišćenja javnih uređaja i izbegavaju takvo ponašanje, posebno za osetljive aktivnosti poput bankarstva. Nizak nivo korišćenja javnih uređaja delimično objašnjava nisku stopu upotrebe VPN-a jer studenti možda ne osećaju potrebu za VPN-om jer uglavnom koriste lične uređaje u kontrolisanim okruženjima.



Slika 7: Stratifikacija po nivou obrazovanja: procenat studenata koji čitaju uslove korišćenja (levo) i odbijaju kolačiće (desno)



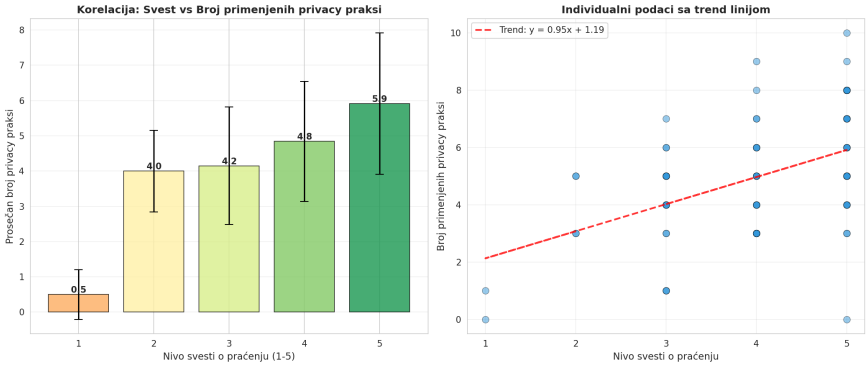
Slika 8: Provera i odbijanje dozvola aplikacija: levi panel prikazuje učestalost provere dozvola pre instalacije, dok desni panel pokazuje ponašanje prema osetljivim dozvolama (kamera, mikrofon, lokacija)

4.5 Odnos svesti i primene mera zaštite privatnosti

Najznačajniji nalaz odnosi se na odnos između svesti i ukupnog broja primenjenih mera za zaštitu privatnosti. Koeficijent korelacije od 0.474 pokazuje pozitivnu, umerenu korelaciju. Međutim, najinteresantniji detalj je nelinearan obrazac rasta. Studenti sa najnižom svešću (nivo 1) primenjuju prosečno samo 0.5 praksi. Prelazak na nivo 2 donosi dramatičan skok na 4.0 prakse. Ovo je kritična tačka transformacije gde student prelazi sa nesvesnosti problema na razumevanje i aktivnu primenu zaštitnih mera.

Nakon ovog inicijalnog skoka, rast postaje postepen. Odnosno, nivo 3 donosi 4.2 prakse, nivo 4 dovodi do 4.8, dok najviši nivo (nivo 5) rezultuje sa 5.9 praksi. Grafikon 9 ilustruje ovaj obrazac, prikazujući kako drastičan početni skok prelazi u linearan trend. Najveći potencijal za intervenciju javlja se kod studenata sa najnižom svešću, gde jedan, dobro oblikovan i

konkretan, edukativni program može postići značajno povećanje u primeni praksi.



Slika 9: Korelacija između nivoa svesti o praćenju i broja primenjenih privacy praksi. Levi panel prikazuje prosečne vrednosti sa standardnom devijacijom, dok desni panel pokazuje individualne podatke sa trend linijom.

5 Zaključak

Većina ispitanika (48.3%) navodi da tokom studija uopšte nisu imali priliku da se upoznaju sa sadržajima o digitalnoj bezbednosti, dok se deo studenata seća samo delimičnog obuhvatanja tema (16.1%). Manje od četvrtine studenata (21.8%) imalo je mogućnost da kroz formalne obrazovne sadržaje stekne znanje o sajber bezbednosti, bilo kroz obavezne ili izborne kurseve i radionice. Ovi rezultati ukazuju na značajan prostor za unapređenje obrazovnog pristupa sajber bezbednosti u okviru studijskih programa ali i važnost samostalnog zanimanja za zaštitu privatnosti.

Kada su u pitanju prepreke za primenu bezbednosnih mera, studenti najčešće ističu nedostatak znanja (64.4%), ali i nedostatak vremena (36.8%), osećaj da im se "neće ništa loše desiti" (33.3%) i percepciju da nisu dovoljno "značajne mete" (36.8%). Dodatni komentari ispitanika ukazuju i na izazove kao što su finansijski troškovi, prisustvo veštačke inteligencije u svakodnevnim alatima, kao i osećaj da su određene mere komplikovane ili usporavaju rad.

Rezultati pokazuju da studenti IT smerova imaju osnovno tehničko znanje, ali većina tokom studija nije dobila organizovanu obuku iz oblasti digitalne bezbednosti. Jedan od problema je jasan a to je da nedostaje sistematska edukacija o bezbednosnim rizicima. Zato je neophodno razviti svest o sajber pretnjama i posledicama kompromitovanja informacija, kao i razumevanje načina na koji mogu zaštititi svoju bezbednost i privatnost u svakodnevnom korišćenju digitalnih tehnologija i motivisati izgradnju bezbednosnih navika.

6 Preporuke za unapređenje sajber bezbednosti studenata

1. **Implementirati menadžer lozinki i jedinstvene lozinke**
   Korišćenje istih ili sličnih lozinki za više naloga predstavlja ozbiljan bezbednosni rizik. Menadžeri lozinki omogućavaju jednostavno korišćenje jakih, jedinstvenih lozinki za svaki nalog bez potrebe za njihovim pamćenjem. Izbegavajte lako pamtljive kombinacije i proaktivno menjajte lozinke na važnim nalozima, ne samo kada sistem to zahteva.

2. **Aktivirati dvofaktorsku autentifikaciju na svim važnim nalozima**
   Dvofaktorska autentifikacija predstavlja dodatni sloj zaštite koji značajno pojačava sigurnost naloga čak i ako dođe do kompromitovanja lozinke. Važno je implementirati je proaktivno na svim kritičnim nalozima (email, bankarstvo, društvene mreže), a ne tek nakon što dođe do kompromitovanja naloga.

3. **Redovno praviti backup važnih podataka**
   Automatsko pravljenje sigurnosnih kopija može spasiti značajne količine podataka u slučaju ransomware napada, hardverskog kvara ili gubitka uređaja. Ova navika je jednako važna kao i prevencija napada.

4. **Primenjivati osnovne bezbednosne prakse dosledno**
   Uvek proveravajte HTTPS pre unošenja osetljivih podataka, odjavljivajte se sa naloga nakon korišćenja, koristite privatni režim browsera za osetljive aktivnosti i segmentirajte email adrese prema nameni. Dosledno sprovođenje ovih osnovnih praksi značajno smanjuje izloženost rizicima.

5. **Konfigurisati osnovne bezbednosne mere**
   Ne oslanjajte se samo na podrazumevana podešavanja sistema. Uložite vreme da samostalno konfigurišete VPN, antivirusni softver, firewall, šifrovanje diska i bezbednosna podešavanja rutera. Ove mere nisu tehnički zahtevne, ali značajno povećavaju nivo zaštite.

6. **Razviti proaktivan pristup bezbednosti**
   Ne čekajte incident da biste preduzeli mere zaštite. Redovno ažurirajte operativni sistem i aplikacije, periodično proveravajte da li su vaši podaci kompromitovani na servisima poput “Have I Been Pwned”, i analizirajte potencijalne ranjivosti u svom digitalnom ponašanju pre nego što postanu problem.

7. **Razumeti posledice curenja podataka i kompromitovanja naloga**
   Važno je u potpunosti razumeti dugoročne posledice zanemarivanja sajber bezbednosti - od finansijskih gubitaka i krađe identiteta do štete po reputaciju. Ovo razumevanje je ključno za razvoj trajnih bezbednosnih navika, a ne samo reaktivnih odgovora na incidente.

Literatura

[1] Ömer Aslan i dr. "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions". U: *Electronics* (2023.).

[2] Adamu Abdullahi Gabra i dr. "Cyber Security Awareness Among University Students: A Case Study". U: *Science Proceedings Series* 2 (2020.).

[3] Diptiben Ghelani. "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review". U: *Authorea* (2022.).

[4] Mohammad Hatamian, Juan Serna i Kai Rannenberg. "Revealing the unrevealed: Mining smartphone users privacy perception on app markets". U: *Computers Security* 112 (2022.), str. 102513.

[5] Fariza Khalid i dr. "An Investigation of University Students' Awareness on Cyber Security". U: *International Journal of Engineering & Technology* (2018.).

[6] Mohammed Khalil. "Cybersecurity Statistics 2025: Breach Costs, Ransomware AI Threats". U: *Deepstike* (2025.).

[7] Aleecia M. McDonald i Lorrie Faith Cranor. "The cost of reading privacy policies". U: *I/S: A Journal of Law and Policy for the Information Society* 4.3 (2008.), str. 540–565.

[8] Midas Nouwens i dr. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence". U: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 2020., str. 1–13.

[9] Yang-Im Lee Peter R. J. Trim. "Advances in Cybersecurity: Challenges and Solutions". U: *Applied Sciences 14, no. 10: 4300* (2024.).

[10] Charles P. Pfleeger i Shari Lawrence Pfleeger. *Security in Computing*. 4. izdanje. Prentice Hall, 2008.

[11] Martina A. Sasse i Michelle P. Steves. "Making security usable: Are we really making progress?" U: *IEEE Security Privacy* 18.2 (2020.), str. 7–11.

[12] Michael E. Whitman i Herbert J. Mattord. *Principles of Information Security*. 7. izdanje. Cengage Learning, 2021.