ŠOLSKI CENTER VELENJE
ELEKTRO IN RAČUNALNIŠKA ŠOLA
Trg mladosti 3, 3320 Velenje

MLADI RAZISKOVALCI ZA RAZVOJ SAŠA REGIJE

RAZISKOVALNA NALOGA

Ne – Varen klik

Tematsko področje: INTERDISCIPLINARNO (računalništvo, sociologija)

Avtor:
Kristian Muha, 1. letnik

Mentor:
Roman Herlah, mag. inž. inf. in tehnol. kom.

Somentor:
mag. Simon Muha, univ. dipl. inž.

Velenje, 2026

Raziskovalna naloga je bila opravljena na Šolskem centru Velenje, Elektro in računalniški šoli.

Mentor: Roman Herlah, mag. inž. inf. in tehnol. kom.

Somentor: mag. Simon Muha, univ. dipl. inž.

Datum predstavitve: marec 2026

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

ŠD SŠ Šolski center Velenje, šolsko leto 2025/2026

AV MUHA, Kristian

SA HERLAH, Roman / MUHA, Simon

KZ 3320 Velenje, SLO, Vodnikova 3

ZA SŠ Šolski center Velenje

LI 2025

IN NE – VAREN KLIK

TD Raziskovalna naloga

IJ SL

JI sl

KG kibernetska varnost; varna raba interneta; dijaki; gesla; dvofaktorska avtentikacija; spletne prevare; varovanje osebnih podatkov; digitalna pismenost; anonimna anketa; varnostno vedenje

OP 46 str., 30 graf., 2 pril., 18 vir.

AI V sodobnem digitalnem okolju je varna uporaba interneta ključna veščina za mlade uporabnike. Raziskovalna naloga z naslovom Ne-Varen klik se osredotoča na preučevanje znanja, navad in vedenja dijakov elektro-računalniške šole na področju kibernetske varnosti. S pomočjo anonimne ankete med 156 dijaki sem raziskal uporabo gesel, preverjanje varnosti spletnih povezav, uporabo dvofaktorske avtentikacije, zaznavanje spletnih prevar ter varovanje osebnih podatkov. Rezultati kažejo, da dijaki svoje znanje pogosto ocenjujejo kot razmeroma dobro, vendar praktični primeri razkrivajo vrzeli pri prepoznavanju nevarnosti in dosledni uporabi varnostnih ukrepov. Ugotovitve potrjujejo vpliv socialnega in izobraževalnega okolja na varnostno vedenje, pri čemer imajo pomembno vlogo šola, družina in vrstniki. Naloga vključuje tudi predloge za nadaljnje delo, ki zajemajo širitev raziskave na druge šole ter razvoj interaktivnih orodij, izobraževalnih filmov in praktičnih kvizov za spodbujanje odgovorne in varne uporabe interneta med dijaki.

KEY WORDS DOCUMENTATION

ND SŠ Šolski center Velenje 2025/2026

AU MUHA, Kristian

AA HERLAH, Roman / MUHA, Simon

PP 3320 Velenje, SLO, Vodnikova 3

PB SŠ Šolski center Velenje

PY 2025

TI THE UNSAFE CLICK

DT RESEARCH WORK

LA SL

AL sl / en

KG Cybersecurity; safe internet use; students; passwords; two-factor authentication (2FA); online scams; protection of personal data; digital literacy; anonymous survey; security behavior

OP 46 pages, 30 graphs, 2 appendices, 18 sources.

AB In today’s digital environment, safe internet use is a crucial skill for young users. The research paper Ne-Varen klik focuses on examining the knowledge, habits, and behavior of students at the Electro-Computer School regarding cybersecurity. Through an anonymous survey of 156 students, I investigated password practices, verification of secure web connections, use of two-factor authentication, detection of online scams, and protection of personal data. The results show that students often rate their knowledge as relatively good, yet practical scenarios reveal gaps in recognizing threats and consistently applying security measures. The findings also confirm the influence of social and educational environments on cybersecurity behavior, highlighting the role of school, family, and peers. The paper includes suggestions for further work, such as extending the study to other schools, as well as developing interactive tools, educational videos, and practical quizzes to promote responsible and safe internet use among students.

KAZALO VSEBINE

1 UVOD 1

2 PREGLED OBJAV 3

TEMELJNI POJMI KIBERNETSKE VARNOSTI 3
ZAŠČITNI UKREPI ZA VARNO UPORABO INTERNETA 5
VPLIV SOCIALNEGA OKOLJA NA VARNOST MLADIH 7

3. METODOLOGIJA 13

4 REZULTATI 15

5 DISKUSIJA 29

5.1 POTRDITEV HIPOTEZ 29

6 ZAKLJUČEK 40

7 POVZETEK 42

8 SUMMARY 43

9 LITERATURA IN VIRI 44

ZAHVALA 46

PRILOGE 47

KAZALO GRAFOV

GRAF 1: SPOL 15
GRAF 2: IZOBRAŽEVALNI PROGRAM 16
GRAF 3: KATERI LETNIK OBISKUJEŠ 16
GRAF 4: KAKO BI OPISAL/A KRAJ, KJER ŽIVIŠ? 17
GRAF 5: KAKO USTVARJATE SVOJA GESLA ZA SPLETNE RAČUNE? 17
GRAF 6: KJE HRANITE SVOJA GESLA? 18
GRAF 7: ALI UPORABLJATE DVOFAKTORSKO AVTENTIKACIJO (2FA), KJER JE TO MOGOČE? 19
GRAF 8: KATERA OD SPODNJIH POVEZAV JE NAJVARNEJŠA ZA VNOS PODATKOV? 20
GRAF 9: ZAKAJ JE KLIKANJE NA NEZNANE POVEZAVE V E-POŠTI ALI SMS-IH NEVARNO? 21
GRAF 10: SCENARIJ 1 (BANKA): PREJMETE SMS: "ZAZNAN NEPOOBLAŠČEN DOSTOP. POTRDITE IDENTITETO NA 22
GRAF 11: SCENARIJ 2 (FURS): PREJMETE E-POŠTO S PRIPONKO"OBVESTILO_FURS 23
GRAF 12: SCENARIJ 3 (PRIJATELJ): PRIJATELJ VAM NA MESSENGERJU POŠLJE: "O MOJ BOG, POGLEJ TA VIDEO, TI SI NA NJEM! [POVEZAVA]". KAJ STORITE? 24
GRAF 13: KJE STE DOBILI NAJVEČ INFORMACIJ O VARNI RABI INTERNETA? 25
GRAF 14: KAKO BI NA LESTVICI OD 1 DO 10 OCENILI SVOJE DEJANSKO ZNANJE KIBERNETSKE VARNOSTI? 26
GRAF 15: ALI MENITE, DA SO MLADI BOLJ ALI MANJ VARNI NA SPLETU KOT STAREJŠI? 27
GRAF 16: ALI STE ŽE KDAJ DEJANSKO IZGUBILI DOSTOP DO RAČUNA, DENAR ALI PODATKE ZARADI SPLETNE PREVARE? 27
GRAF 17: KATERA OD SPODNJIH POVEZAV JE NAJVARNEJŠA ZA VNOS PODATKOV? 29
GRAF 18: SCENARIJ 1 (BANKA): PREJMETE SMS: "ZAZNAN NEPOOBLAŠČEN DOSTOP. POTRDITE IDENTITETO NA WWW.NLB-VARNOST.COM/PRIJAVA". KAJ STORITE? 30
GRAF 19: SCENARIJ 2 (FURS): PREJMETE E-POŠTO S PRIPONKO "OBVESTILO_FURS_DOLG.ZIP". KAJ STORITE? 30
GRAF 20: SCENARIJ 3 (PRIJATELJ): PRIJATELJ VAM NA MESSENGERJU POŠLJE: "O MOJ BOG, POGLEJ TA VIDEO, TI SI NA NJEM! [POVEZAVA]". KAJ STORITE? 31
GRAF 21: ALI UPORABLJATE DVOFAKTORSKO AVTENTIKACIJO (2FA), KJER JE TO MOGOČE 32
GRAF 22: ZAKAJ JE KLIKANJE NA NEZNANE POVEZAVE V E-POŠTI ALI SMS-IH NEVARNO? 33
GRAF 23: KJE STE DOBILI NAJVEČ INFORMACIJ O VARNI RABI INTERNETA? 34
GRAF 24: MOJI STARŠI SE ZANIMAJO ZA MOJO VARNOST NA SPLETU. 35
GRAF 25: KATERA OD SPODNJIH POVEZAV JE NAJVARNEJŠA ZA VNOS PODATKOV? 36
GRAF 26: ZAKAJ JE KLIKANJE NA NEZNANE POVEZAVE NEVARNO? 36
GRAF 27: SCENARIJ 1 (BANKA): PREJMETE SMS: "ZAZNAN NEPOOBLAŠČEN DOSTOP. POTRDITE IDENTITETO NA WWW.NLB-VARNOST.COM/PRIJAVA". KAJ STORITE? 37
GRAF 28: SCENARIJ 3 (PRIJATELJ): PRIJATELJ VAM NA MESSENGERJU POŠLJE: "O MOJ BOG, POGLEJ TA VIDEO, TI SI NA NJEM! [POVEZAVA]". KAJ STORITE? 38
GRAF 29: KAKO USTVARJATE SVOJA GESLA ZA SPLETNE RAČUNE? 38
GRAF 30: ALI UPORABLJATE DVOFAKTORSKO AVTENTIKACIJO (2FA), KJER JE TO MOGOČE 39

1 UVOD

Internet in digitalne tehnologije so danes nepogrešljiv del vsakdanjega življenja dijakov. Splet uporabljajo za učenje, sporazumevanje, zabavo in ohranjanje stikov, pri tem pa pogosto delijo tudi osebne podatke. Čeprav internet ponuja številne prednosti in omogoča hiter dostop do informacij, prinaša tudi različna tveganja, kot so spletne prevare, kraja osebnih podatkov, zloraba gesel, lažne spletne strani ter dostop do neprimernih ali zavajajočih vsebin. Zaradi pogoste uporabe interneta in še ne povsem razvite kritične presoje so dijaki ena izmed ranljivejših skupin uporabnikov, ki se nevarnosti na spletu pogosto ne zavedajo dovolj ali pa jih podcenjujejo.

Poseben problem predstavlja pomanjkljivo poznavanje osnov kibernetske varnosti. Številni dijaki uporabljajo šibka ali ponavljajoča se gesla, ne preverjajo varnosti spletnih strani, nekritično klikajo na povezave ter ne posvečajo dovolj pozornosti zaščiti svojih osebnih podatkov. Takšno ravnanje jih lahko hitro izpostavi spletnim napadom, kot so phishing, kraja identitete ali zloraba računov, kar ima lahko resne osebne in finančne posledice.

Namen raziskovalne naloge z naslovom Ne-Varen klik je raziskati stopnjo ozaveščenosti dijakov o kibernetski varnosti ter analizirati njihove navade pri uporabi digitalnih storitev. Cilj raziskave je ugotoviti, kako dijaki ustvarjajo in varujejo gesla, ali prepoznajo varne spletne strani, kako ravnajo z osebnimi podatki ter kako pogosto razmišljajo o morebitnih spletnih tveganjih.

Končni cilj naloge ni le analiza stanja, temveč tudi prispevek k večji ozaveščenosti in spremembi vedenja dijakov. Raziskovalna naloga želi spodbuditi razvoj odgovorne, premišljene in varne rabe interneta ter pokazati, da lahko že majhne spremembe v vsakodnevnih navadah pomembno povečajo stopnjo digitalne varnosti.

Hipoteze:

H1: Dijaki imajo težave pri prepoznavanju lažnih spletnih strani in spletnih prevar (scamov).

H2: Stopnja poznavanja osnovnih načel kibernetske varnosti (npr. preverjanje povezav, dvofaktorska avtentikacija, varovanje osebnih podatkov) je med dijaki nizka.

H3: Dijaki, ki se pogosto pogovarjajo o spletni varnosti z družino, vrstniki ali učitelji, kažejo bolj odgovorno vedenje pri uporabi interneta.

H4: Dijaki programa računalniški tehnik bodo v anketi o kibernetski varnosti dosegli boljše rezultate kot dijaki programov tehnik mehatronike, elektro tehnik in tehnik elektronike, kar kaže na vpliv izobraževalnega okolja.

2 PREGLED OBJAV

TEMELJNI POJMI KIBERNETSKE VARNOSTI

Temeljni pojmi kibernetske varnosti predstavljajo osnovo razumevanja zaščite digitalnih sistemov, omrežij in podatkov pred različnimi oblikami kibernetskih napadov ter so ključni za odgovorno in varno rabo interneta.

KIBERNETSKA VARNOST

Kibernetska varnost je zaščita sistemov, omrežij in programov pred digitalnimi napadi. Postaja vse pomembnejša zaradi rasti uporabe interneta.

Učinkovita kibernetska varnost vključuje močna gesla, dvofaktorsko avtentikacijo, varovanje osebnih podatkov in prepoznavanje spletnih groženj. Stroški kršitev varnosti so visoki, zato je znanje uporabnikov ključno za zmanjšanje tveganja in zaščito informacij (Uršič, J., 2022).

KIBERNETSKI NAPADI

Kibernetski napadi so zlonamerna dejanja, ki škodljivo vplivajo na delovanje sistema IKT, digitalno odvisnih podjetij in omrežij. Obstaja tudi kibernetski terorizem, katerega namen je ogroziti elektronske sisteme in povzročiti strah.

Cilj kibernetskih napadov je dostop do občutljivih informacij, njihovo spreminjanje ali uničenje, izsiljevanje denarja ali prekinitev delovanja sistemov. Napadalci postajajo vedno bolj inovativni, zaščita pa je zahtevna, saj je naprav več kot ljudi.

Med najpogostejše načine spada zlonamerna programska oprema, kot so virusi, trojanski konji, vohunska programska oprema, adware in scareware. Drugi napadi vključujejo SQL injection, phishing, Man-in-the-Middle in napade z zavrnitvijo storitve.

Število napadov narašča, tako globalno kot v Sloveniji. Evropska unija sprejema ukrepe za obravnavo izzivov kibernetske varnosti in zaščito pred kibernetskimi grožnjami (Uršič, J., 2022).

SOCIALNI INŽENIRING KOT NAJPOGOSTEJŠA OBLIKA NAPADA

Socialni inženiring je način prevare, kjer prevarant z izkoriščanjem človeških lastnosti manipulira žrtev, da izvede določeno dejanje. Prevarant običajno ne uporablja nasilja, temveč mimikrijo in poskuša pridobiti zasebne informacije.

Ločimo tehnološki in netehnični socialni inženiring. Pri tehnološkem se uporablja računalnik in internet, pri netehničnem pa osebni pristop. Pogoste prevare vključujejo phishing, pharming, smishing in vishing napade.

Cilj je zbiranje uporabniških imen, gesel, dostopa do spletnih bank, spletnih prodajaln, socialnih omrežij ali e-pošte. Posledice vključujejo krajo informacij, denarja ali identitete. Najboljša obramba je previdnost in skeptičnost. (Suša, M., 2014)

NAJPOGOSTEJŠE OBLIKE SOCIALNEGA INŽENIRINGA

Najpogostejše oblike socialnega inženiringa so ribarjenje (phishing), smishing, vishing in pharming.

Ribarjenje (phishing)

Ribarjenje (phishing) je dejavnost, s katero kibernetski kriminalci žrtvam pošiljajo e-poštna sporočila, za katera se zdi, da prihajajo iz zakonitega podjetja, in v njih prosijo za občutljive podatke, v večini primerov so to kreditne kartice.

Lažno predstavljanje oziroma ribarjenje (phishing) je napad socialnega inženiringa, ki se uporablja za krajo podatkov. Napadalci želijo prijavne podatke ali številke kreditnih kartic.

Napadalec se izdaja za zaupanja vredno osebo in zavede žrtev, da odpre e-pošto ali besedilno sporočilo. Prejemnik klikne zlonamerno povezavo, kar lahko privede do namestitve zlonamerne programske opreme, zamrznitve sistema ali razkritja občutljivih podatkov.

Napadi ribarjenja so izpopolnjeni in zrcalijo ciljno spletno mesto, napadalec pa lahko opazuje vse, kar počne žrtev. Posledice so nepooblaščeni nakupi, kraja identitete ali sredstev ter finančna škoda organizacij, zmanjšan tržni delež, ugled in zaupanje potrošnikov (Uršič, J., 2022).

Smishing

Po Shweta in Keatron Evans (2024) je smishing oblika socialnega inženiringa, pri kateri napadalci pošiljajo zavajajoča SMS-sporočila, da bi uporabnike prepričali v razkritje osebnih ali finančnih podatkov ali v prenos zlonamerne programske opreme. Sporočila se pogosto predstavljajo kot poslana s strani bank, dostavnih služb ali drugih zaupanja vrednih organizacij, pri čemer uporabnike nagovarjajo k hitremu ukrepanju. Takšni napadi izkoriščajo psihološke trike in zaupanje v SMS-komunikacijo, zato so zlasti nevarni za uporabnike mobilnih naprav.

Vishing

Vishing je oblika napada, pri kateri napadalci zlorabljajo telefonske klice, da pridobijo občutljive informacije, kot so gesla ali številke kreditnih kartic (Shweta in Keatron Evans, 2024). Napadalci se pogosto predstavljajo kot predstavniki bank, podjetij ali državnih organov in uporabnika nagovarjajo k takojšnjemu ukrepanju. Zaradi psihološkega pritiska in zaupanja uporabnikov v telefonsko komunikacijo je ta metoda še posebej prepričljiva in nevarna.

Pharming

Pri pharmingu napadalci preusmerijo uporabnika na lažno spletno stran, tudi če je vpisal pravilen URL (Shweta in Keatron Evans, 2024). S tem lahko pridobijo osebne podatke, kot so prijavna imena, gesla ali številke kreditnih kartic. Pharming pogosto deluje skupaj z drugimi oblikami socialnega inženiringa, na primer phishingom, in izkorišča ranljivosti DNS-sistemov ali zlonamerno programsko opremo na napravi uporabnika, zaradi česar je skoraj neopazen za žrtev.

ZAŠČITNI UKREPI ZA VARNO UPORABO INTERNETA

Zaščitni ukrepi so ključni za zmanjšanje tveganj, ki jih prinaša uporaba interneta. Uporabniki, še posebej dijaki, se lahko z različnimi strategijami učinkovito zaščitijo pred krajo podatkov, zlorabo gesel in drugimi spletnimi grožnjami. V tem poglavju so predstavljeni najpomembnejši ukrepi za varno rabo interneta, kot so uporaba močnih gesel, dvofaktorska avtentikacija in varovanje osebnih podatkov.

KAJ JE VARNO GESLO

Varno geslo je kombinacija črk, številk in posebnih znakov, ki je težko uganiti. Močno geslo preprečuje nepooblaščen dostop do spletnih računov in osebnih podatkov. Priporočljivo je, da gesla niso povezana z osebnimi podatki (ime, rojstni datum), so dolga vsaj 12 znakov in jih uporabnik redno menja. Uporaba upraviteljev gesel lahko dodatno poveča varnost (Uršič, 2022).

Poleg tega raziskava Bonneau, Herley, van Oorschot in Stajano (2012) ugotavlja, da so kljub številnim predlogom za nadomestitev gesel tradicionalna gesla še vedno najpogostejša oblika avtentikacije, vendar se uporabniki pogosto soočajo s težavami pri ustvarjanju varnih in zapomnljivih gesel. Zato je uporaba daljših fraz ali kombinacij besed, številk in simbolov učinkovita strategija za povečanje varnosti, hkrati pa ohranja uporabniku prijazno izkušnjo.

DVOFAKTORSKA AVTENTIKACIJA (2FA)

Dvofaktorska avtentikacija je dodaten sloj varnosti, ki zahteva, da uporabnik poleg gesla vnese še en dokaz svoje identitete. Ta lahko vključuje kodo, poslano na mobilni telefon, aplikacijo za generiranje enkratnih gesel ali biometrične podatke, kot je prstni odtis. Uporaba 2FA znatno zmanjša tveganje nepooblaščenega dostopa do spletnih računov, tudi če napadalec pozna geslo (Finderšek, 2024).

Raziskave na področju spletne varnosti kažejo, da dvofaktorska avtentikacija bistveno zmanjšuje verjetnost uspešnega napada, saj napadalci ne morejo pridobiti drugega faktorja tako enostavno kot gesla (Bonneau, 2012). Implementacija 2FA je še posebej priporočljiva pri dostopu do e-poštnih računov, spletnih bančnih storitev in družbenih omrežij, kjer so osebni in finančni podatki še posebej občutljivi.

Poleg tega strokovnjaki priporočajo, da uporabniki ne uporabljajo SMS kot edine metode 2FA, saj so te kode ranljive za napade s prestrezanjem (SIM swap). Bolj varne metode vključujejo uporabo aplikacij za generiranje enkratnih gesel ali fizične varnostne ključe (FIDO Alliance, 2020).

VAROVANJE OSEBNIH PODATKOV

Varstvo osebnih podatkov je ključnega pomena v številnih sektorjih, kjer se obdelujejo občutljivi podatki posameznikov. Različni sektorji imajo specifične zakonodajne zahteve in standarde glede obdelave, shranjevanja in zaščite podatkov. Te podatke je potrebno skrbno zaščititi pred nepooblaščenim dostopom in zlorabo, saj lahko takšne kršitve privedejo do resnih posledic za posameznike (Finderšek, 2024).

Varovanje osebnih podatkov je še posebej pomembno za mlade uporabnike interneta, ki pogosto uporabljajo družbena omrežja, spletne igre in različne aplikacije. Nevarnosti vključujejo krajo identitete, dostop do zasebnih informacij ali zlorabo osebnih podatkov, če jih delijo na nepreverjenih spletnih straneh ali z neznanci.

Mladi pogosto ne razmišljajo o tem, kateri podatki so občutljivi, zato je pomembno, da se zavedajo, da osebnih podatkov, kot so gesla, rojstni datum, številke mobilnega telefona ali lokacija, ne delijo z neznanci ali na javnih platformah. Zaščita osebnih podatkov vključuje tudi uporabo močnih gesel, dvofaktorske avtentikacije in redno preverjanje nastavitev zasebnosti na družbenih omrežjih (Klemenčič, 2021).

Pomembno je, da mladi razvijejo dobre navade pri varovanju svojih podatkov, kot so: neuporaba enakih gesel na več mestih, previdnost pri odpiranju sumljivih povezav in sporočil ter razumevanje, katere informacije je varno deliti. Tako se zmanjša tveganje spletnih prevar, kraje identitete in drugih zlorab (Klemenčič, 2021).

Poleg individualnih ukrepov, kot so močna gesla in dvofaktorska avtentikacija, uporabnikom pomagajo tudi institucionalni viri in izobraževalni programi. V Sloveniji je pomembno vlogo pri ozaveščanju o varni rabi interneta odigral Arnes kot partner nacionalnega projekta Center za varnejši internet – Safe.si. ARNES in Safe.si pripravljata gradiva, delavnice in priporočila za starše in dijake, ki krepijo znanje o prepoznavanju spletnih tveganj, varovanju osebnih podatkov in varni interakciji na spletu. Takšna podpora dopolnjuje posameznikove tehnične ukrepe in spodbuja odgovorno in varno vedenje na spletu (Arnes, n.d.; Safe.si, n.d.).

VPLIV SOCIALNEGA OKOLJA NA VARNOST MLADIH

Varnost mladih na spletu ni odvisna le od tehničnih ukrepov, kot so močna gesla ali dvofaktorska avtentikacija, ampak tudi od socialnega okolja, v katerem odraščajo. Socialno okolje oblikuje navade, znanje in zavedanje o nevarnostih na spletu ter vpliva na vedenje posameznika pri varovanju osebnih podatkov.

DRUŽINA IN NJENA VLOGA

Družina predstavlja primarno okolje socializacije, v katerem otrok oblikuje vrednote, norme in vedenjske vzorce, ki jih kasneje prenaša tudi v digitalni prostor. Sociološke teorije socializacije poudarjajo, da otroci vedenje opazujejo, posnemajo in ponotranjijo skozi vsakodnevne interakcije z družinskimi člani, kar pomembno oblikuje njihov odnos do digitalnih praks, vključno z internetom in varnostnimi navadami (Livingstone & Helsper, 2008).

Družina kot ključni vir učenja o varnosti na spletu

Družina je prvo okolje, kjer se otrok uči pravil in oblikuje svoje vedenjske vzorce, kar velja tudi za uporabo interneta. Po raziskavi Livingstone & Helsper (2008) se najstniki, stari 12–17 let, srečujejo z različnimi spletnimi tveganji. Starši uporabljajo različne strategije, pri čemer dajejo prednost aktivni souporabi in interakciji z otrokom pred tehničnimi omejitvami, kot so filtri ali programska oprema za nadzor (Wisteria, 2025).

Raziskava je pokazala, da starševska omejitev spletnih interakcij med vrstniki lahko zmanjša tveganja, medtem ko druge strategije, kot je široko razširjena aktivna souporaba, niso nujno učinkovite. To poudarja pomen družinske komunikacije in usmerjanja otrok pri uporabi

interneta, ne da bi pri tem omejevali njihovo svobodo pri socialnih interakcijah (Wisteria, 2025).

Kako starši oblikujejo navade otrok na spletu

V slovenskem kontekstu raziskave (Wisteria, 2025) kažejo, da večina staršev spremlja in vodi otroke pri uporabi interneta, pri čemer se nadzor z leti postopoma zmanjšuje. Starši uporabljajo pravila, kot so omejitev časa uporabe interneta, nadzor nad aplikacijami in pogovori o tveganjih. Takšna družinska vloga je ključna za razvoj varnih digitalnih navad, kritičnega razmišljanja in prepoznavanja spletnih nevarnosti.

Poleg neposrednega nadzora je pomemben tudi zgled staršev. Po teoriji socialnega učenja otroci vedenje opazujejo in posnemajo, zlasti kadar gre za osebe, ki jim predstavljajo avtoriteto ali pomembne druge (Bandura, 1971). Če starši odgovorno ravnajo z osebnimi podatki, uporabljajo močna gesla ter so previdni pri deljenju informacij na družbenih omrežjih, otroci takšne vzorce ponotranjijo kot običajen način vedenja. Družinsko okolje tako ne oblikuje le pravil uporabe interneta, temveč tudi širši odnos do zasebnosti, varnosti in odgovornosti v digitalnem prostoru.

Spremljanje uporabe interneta in postavljanje pravil

Sociološko gledano družinska regulacija uporabe interneta ni le tehnični nadzor, temveč del procesa socializacije, kjer otrok uči norme, vrednote in odgovornost. Postavljanje pravil o času uporabe interneta, primernosti vsebin in deljenju osebnih podatkov omogoča otrokom razumevanje meja in sprejemljivega vedenja v digitalnem okolju. Takšna pravila delujejo kot okvir, znotraj katerega otrok razvija samokontrolo, kritično mišljenje in sposobnost prepoznavanja tveganj.

Poleg tega sociološke raziskave poudarjajo, da otroci svoje digitalno vedenje pogosto modelirajo po družinskih vzorcih, torej opazujejo, kako starši uporabljajo internet in kako pristopajo k varovanju osebnih podatkov (Wisteria, 2025). Odprt dialog in skupno dogovarjanje o pravilih prispevata k razumevanju razlogov za omejitve ter spodbujata notranjo motivacijo otrok za odgovorno vedenje, medtem ko stroga prepoved ali pasivni nadzor lahko vodita v prikrito ali tvegano rabo digitalnih tehnologij.

Mednarodne študije prav tako izpostavljajo, da kombinacija jasnih pravil in odprte komunikacije nudi boljše rezultate pri zaščiti otrok pred spletnimi tveganji kot zgolj tehnični

nadzor (Livingstone & Helsper, 2008). S tem družina ne le omejuje nevarnosti, ampak hkrati podpira razvoj digitalne pismenosti, kritičnega mišljenja in samostojnosti pri mladostnikih.

Podpora staršev in digitalna pismenost

Podpora staršev pri razvoju digitalne pismenosti otrok vključuje aktivno spremljanje in usmerjanje otrokove uporabe interneta, pa tudi spodbujanje kritičnega razmišljanja in varnega ravnanja z osebnimi podatki. Starši, ki se aktivno vključujejo v otrokove digitalne aktivnosti, pomagajo otrokom prepoznati spletne nevarnosti, kot so zloraba osebnih podatkov, phishing in neprimerni stiki z neznanci. Takšna podpora omogoča otrokom, da razvijejo samostojnost in odgovorno vedenje na spletu, hkrati pa se učijo pravil in mej, ki jih postavlja družinsko okolje (Wisteria, 2025).

Raziskava Varna raba interneta in starši 2024 kaže, da otroci, katerih starši aktivno podpirajo njihovo digitalno učenje, bolje razumejo spletna tveganja in se znajo pred njimi zaščititi. Starši so ključni pri oblikovanju otrokovega odnosa do interneta, ne le kot prostora za zabavo, temveč tudi kot okolja, kjer je potrebno razvijati varne digitalne navade (Safe.si, 2024).

Pogovori o nevarnostih na spletu

Redni pogovori med starši in otroki o nevarnostih na spletu pomagajo otrokom razviti kritično mišljenje in odgovorno rabo digitalnih vsebin. Družina kot primarno socialno okolje je ključna pri prenosu vrednot in norm, ki veljajo tudi v digitalnem prostoru. S pogovori otroci pridobivajo razumevanje, kako prepoznati nevarnosti, kot so phishing, socialni inženiring ali neprimerni stiki, kot tudi kako ravnati v teh situacijah (Wisteria, 2025).

Safe.si (2024) priporoča, da starši pogovore izvajajo sproti in v kontekstu realnih dogodkov, pri čemer otrokom omogočijo postavljanje vprašanj in izražanje dvomov. Tak pristop ustvarja zaupno okolje, kjer se varnost na spletu dojema kot skupna odgovornost, ne kot kazen. Otroci, ki redno sodelujejo v takšnih pogovorih, razvijejo boljši občutek za tveganja in sposobnost samostojnega odločanja o tem, katere informacije deliti in katere ne.

VPLIV VRSTNIKOV

Vrstniki so ključni pri oblikovanju socialnih in digitalnih vedenj mladih. Otroci in najstniki pogosto prilagajajo svoje navade in interakcije glede na vedenje vrstnikov, kar vključuje uporabo interneta, družbenih omrežij in aplikacij. Vpliv vrstnikov je dvostranski: lahko podpira razvoj varnih digitalnih navad ali pa vodi k tveganim praksam. Razumevanje tega vpliva je ključno za oblikovanje učinkovitih preventivnih strategij (Črnak Meglič, 2017).

Vrstniški vzorci in spletne navade

Mladi se pri oblikovanju svojih spletnih navad pogosto zgledujejo po vrstnikih. Pozitivni vzorci, kot so izmenjava nasvetov o varni uporabi interneta in spodbujanje kritičnega razmišljanja, lahko krepijo digitalno pismenost, medtem ko negativni vzorci, na primer neprevidno deljenje osebnih podatkov, povečujejo tveganja. Razumevanje vrstniških vzorcev omogoča učinkovitejše usmerjanje mladih k odgovornemu vedenju na spletu (Črnak Meglič, 2017).

Posnemanje vedenja vrstnikov

Posnemanje vedenja vrstnikov je naraven del socializacije mladih in vpliva tudi na digitalno vedenje. Če vrstniki izvajajo varne digitalne prakse, se otroci tega naučijo in jih posnemajo, vendar pa lahko hitro prevzamejo tudi tvegane navade. Razumevanje mehanizmov posnemanja je ključno za načrtovanje intervencij, ki spodbujajo varno uporabo interneta v skupinah mladih (Črnak Meglič 2017).

Pritisk vrstnikov na deljenje informacij

Raziskave kažejo, da vrstniki pomembno vplivajo na odločitve mladih glede deljenja informacij in ravnanja na spletu. Socialni pritisk, kot je želja po sprejetju ali posnemanju vrstnikov, lahko vodi k tveganim praksam, kot so prekomerno deljenje osebnih podatkov, sodelovanje v izzivih na družbenih omrežjih ali neprevidno objavljanje vsebin (Črnak Meglič 2017).

ŠOLSKO OKOLJE

Šola je pomembno sekundarno okolje, kjer se otroci in mladostniki učijo družbenih norm, vrednot in vedenjskih vzorcev, ki jih prenašajo tudi v digitalni prostor. V komunikaciji, interakcijah in skupinskih dejavnostih v šoli se oblikujejo pričakovanja glede primernega vedenja znotraj spletnih skupnosti. Tak okvir vpliva na to, kako posamezniki dojemajo družbene standarde, sprejemanje tveganj in odzive na spletne vsebine.

Šolsko okolje kot okvir za oblikovanje digitalnih vedenj

Digitalno vedenje mladih ni le izraz osebnih preferenc, ampak je pogosto povezano tudi s tem, kako šolsko okolje strukturira odnose, kaj od učencev pričakuje in kako spodbuja odgovorno komunikacijo v digitalnem okolju. Vključevanje tematik, povezanih z varnostjo na internetu, v šolske razprave in projekte daje signale o tem, kaj družba preko šolskega sistema šteje za pomembno ter tako oblikuje norme, povezane z varno rabo digitalnih tehnologij (Safe.si, n.d.).

Vpliv učiteljev in šolskih praks na digitalno varnost mladih

Učitelji imajo pomembno vlogo pri oblikovanju vedenjskih vzorcev in ozaveščanju učencev o digitalnih tveganjih. V šolskem vsakdanjem življenju učitelji določajo norme in pričakovanja, ki vplivajo na načine komuniciranja, interakcij in vedenja v digitalnem prostoru.

Safe.si ponuja izobraževanja in priporočila za učitelje in šolske delavce, ki obravnavajo teme, kot so spletno nasilje, e-zlorabe, prepoznavanje nevarnosti in odgovorno ravnanje z informacijami na spletu. Takšna usposabljanja učiteljem omogočajo, da v pouk vključijo odprte razprave o nevarnostih in spodbujajo kritično razmišljanje, refleksijo o spletnih izkušnjah ter razvoj odgovorne rabe interneta med učenci. Ti postopki prispevajo k večji ozaveščenosti in razumevanju spletnih tveganj kot družbenih pojavov, ne le tehničnih izzivov (Safe.si, n.d.).

SPLETNO OKOLJE IN DRUŽBENA OMREŽJA

Spletno okolje in družbena omrežja predstavljajo pomemben del vsakdanjega življenja mladih. Digitalni prostor ni zgolj tehnično okolje, temveč družbeni prostor, kjer se oblikujejo odnosi, identitete, vrednote in norme. Mladi preko družbenih omrežij vzpostavljajo socialne vezi, izražajo svoja mnenja, gradijo samopodobo in iščejo potrditev vrstnikov.

Posebnost spletnega okolja je v tem, da omogoča hitro širjenje informacij, trajnost objav in večjo izpostavljenost posameznika širši javnosti. Zaradi tega imajo lahko nepremišljene objave dolgoročne posledice. Digitalni prostor tako postaja pomembno okolje socializacije, kjer se oblikujejo vedenjski vzorci in odnos do zasebnosti.

Raziskave, objavljene na Safe.si, kažejo, da mladi pogosto podcenjujejo tveganja, povezana z deljenjem osebnih podatkov, ter da na njihove odločitve vplivajo družbeni trendi, potreba po sprejetosti in pritisk okolja (Safe.si, n.d.).

Deljenje podatkov in ranljivost mladih

Deljenje fotografij, lokacije, osebnih podatkov ali vsakodnevnih aktivnosti je med mladimi postalo del običajne komunikacije. Vendar pa sociološki vidik opozarja, da takšno vedenje ni le individualna odločitev, temveč rezultat družbenih pričakovanj in norm, ki spodbujajo stalno prisotnost na spletu.

Kultura všečkov, komentarjev in delitev ustvarja občutek, da je večja izpostavljenost povezana z večjo socialno vrednostjo. Mladi lahko zato delijo informacije, ki povečujejo njihovo ranljivost, ne da bi se v celoti zavedali dolgoročnih posledic.

Safe.si opozarja, da nepremišljeno deljenje osebnih podatkov povečuje tveganje za krajo identitete, zlorabo fotografij ter različne oblike spletnega nadlegovanja (Safe.si, n.d.). Pomembno je, da mladi razvijejo kritično presojo glede tega, katere informacije so primerne za javno objavo.

Ozaveščenost o spletnih tveganjih in zasebnosti

Spletno okolje mladim omogoča številne priložnosti, hkrati pa jih izpostavlja tveganjem, kot so spletno nadlegovanje, manipulacija, lažne informacije in prevare. Sociološko gledano gre za pojav, kjer digitalna interakcija pogosto poteka brez neposrednega nadzora odraslih, kar povečuje pomen notranjih norm in samoregulacije.

Ozaveščenost o nevarnostih na spletu ni zgolj vprašanje tehničnega znanja, temveč tudi razumevanja družbenih mehanizmov, kot so pritisk vrstnikov, želja po potrditvi in vpliv spletnih skupnosti. Mladi, ki razvijejo kritično mišljenje in razumevanje teh vplivov, so manj ranljivi za manipulacijo in spletne prevare.

Safe.si poudarja pomen pogovorov, izobraževanja in odprte komunikacije kot ključnih dejavnikov pri krepitvi varne in odgovorne rabe interneta (Safe.si, n.d.).

3 METODOLOGIJA

Na začetku izdelave raziskovalne naloge sem opravil pregled obstoječe literature, ki sem jo našel v šolski in mestni knjižnici ter v strokovnih spletnih virih. Preučil sem različne vire s področja kibernetske varnosti, digitalne pismenosti mladih, spletnih prevar ter vpliva izobraževanja na varno uporabo interneta. S tem sem si zagotovil ustrezno teoretično podlago za nadaljnje raziskovanje ter oblikovanje hipotez in anketnega vprašalnika.

Za pridobitev podatkov sem se odločil uporabiti metodo anketiranja. Anketni vprašalnik sem oblikoval v orodju Microsoft Forms, kar mi je omogočilo enostavno zbiranje in avtomatsko obdelavo odgovorov. Po zaključku anketiranja sem zbrane podatke izvozil v program Microsoft Excel, kjer sem jih uredil, analiziral ter pripravil grafikonske prikaze. Obdelane rezultate sem nato vključil in grafično predstavil v programu Microsoft Word.

Anketiranje je potekalo januarja 2026 med dijaki elektro-računalniške šole. V raziskavi je sodelovalo 156 dijakov. Sodelovali so dijaki različnih izobraževalnih programov (tehnik računalništva, tehnik mehatronike, elektrotehnik, elektrikar) ter različnih letnikov. Vprašalnik je bil anonimen, saj sem želel zagotoviti iskrenost odgovorov.

Z anketo sem želel pridobiti podatke o:

- znanju dijakov s področja kibernetske varnosti,
- njihovih navadah pri ustvarjanju in shranjevanju gesel,
- uporabi dvofaktorske avtentikacije,
- sposobnosti prepoznavanja lažnih spletnih strani in phishing poskusov,
- ravnanju v konkretnih varnostnih scenarijih,
- vplivu družine, vrstnikov in šole na njihovo vedenje,
- razlikah v znanju med posameznimi izobraževalnimi programi.

Glavni namen ankete je bil potrditi ali ovreči zastavljene hipoteze.

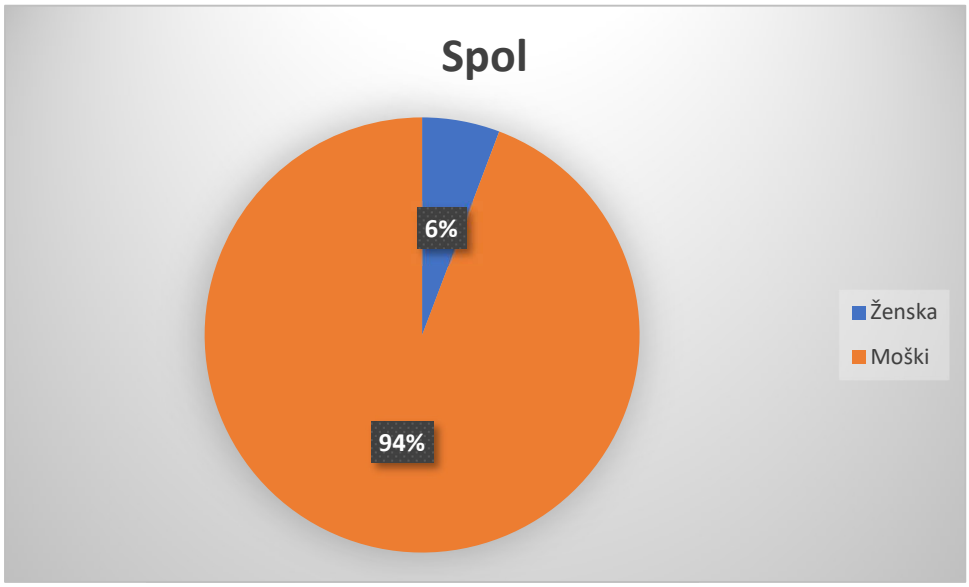
Vprašalnik je zajemal več vsebinskih sklopov. Prvi del je vseboval demografska vprašanja. Drugi del se je nanašal na tehnične vidike varnosti, kot so ustvarjanje in shranjevanje gesel, uporaba dvofaktorske avtentikacije ter prepoznavanje varnih spletnih povezav. Tretji del je vključeval praktične scenarije (banka, FURS, sporočilo prijatelja), s katerimi sem preverjal dejansko sposobnost prepoznavanja spletnih prevar. Zadnji del vprašalnika pa je obravnaval socialne vplive, odnos do varnosti, pogovore o spletni varnosti ter samooceno znanja.

Na ta način sem pridobil celovit vpogled v tehnično znanje dijakov, njihovo dejansko vedenje v konkretnih situacijah ter vpliv socialnega okolja in izobraževalnega programa na njihovo kibernetsko varnost.

4 REZULTATI

V nadaljevanju predstavljam rezultate ankete, ki so prikazani v obliki grafov ter podprti s sprotno analizo in razlago ugotovitev vseh 18 vprašanj, pri čemer so poleg rezultatov podane tudi razlage, kaj posamezni graf prikazuje in kaj lahko iz njega razberemo.

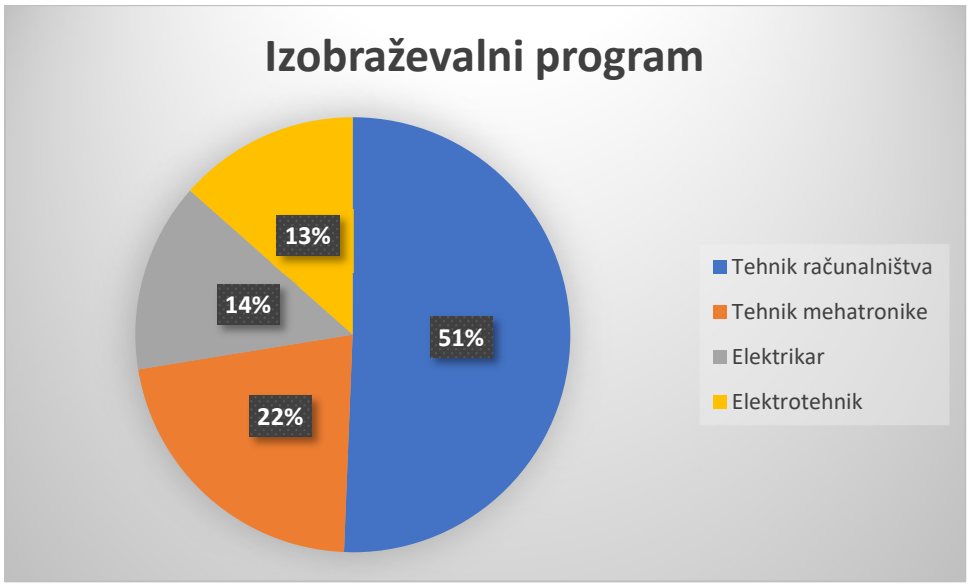
Pri prvem vprašanju, ki se je nanašalo na spol anketirancev, rezultati prikazujejo razmerje med fanti in dekleti, ki so sodelovali v raziskavi. Ta podatek je pomemben za razumevanje strukture vzorca in morebitnih razlik med spoloma pri nadaljnjih vprašanjih.



Graf 1: Spol

Iz grafa je razvidno ali je bil vzorec uravnotežen ali je prevladoval določen spol.

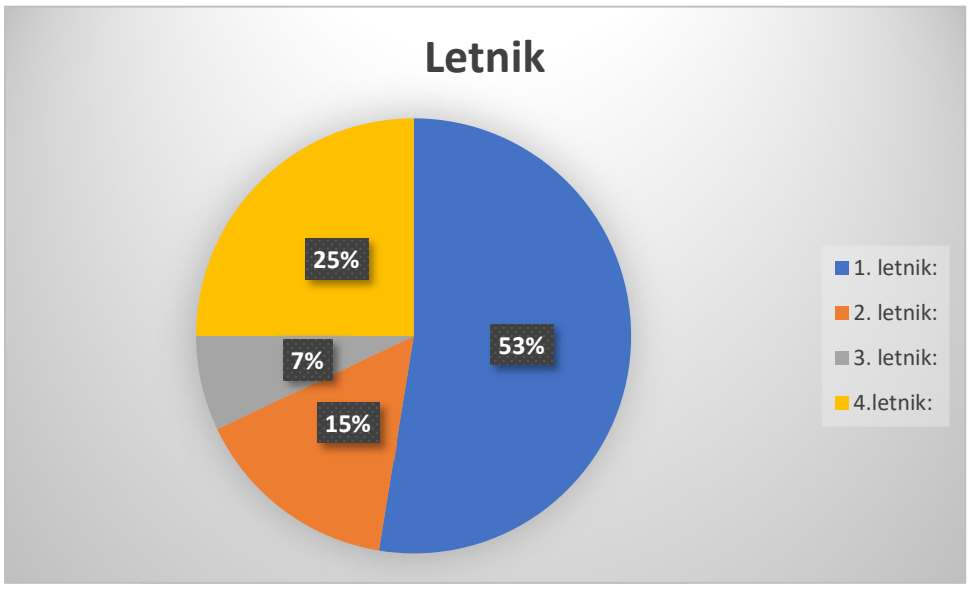
Drugo vprašanje se je nanašalo na program, ki ga dijaki obiskujejo. Rezultati prikazujejo starostno porazdelitev sodelujočih.



Graf 2: Izobraževalni program

Graf pokaže, katera starostna skupina je bila najbolj zastopana, kar je pomembno pri interpretaciji rezultatov, saj se znanje in izkušnje lahko razlikujejo glede na starost.

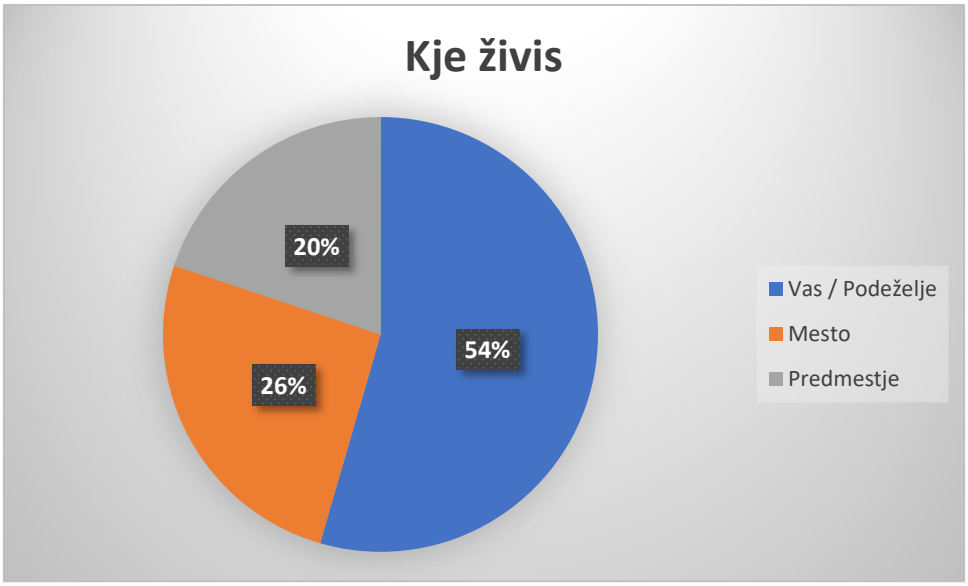
Tretje vprašanje je preverjalo letnik izobraževanja. Rezultati kažejo, iz katerih letnikov prihajajo dijaki.



Graf 3: Kateri letnik obiskuješ

Iz grafa je razvidno, ali so bolj zastopani mlajši ali starejši dijaki, kar lahko vpliva na raven znanja o kibernetski varnosti.

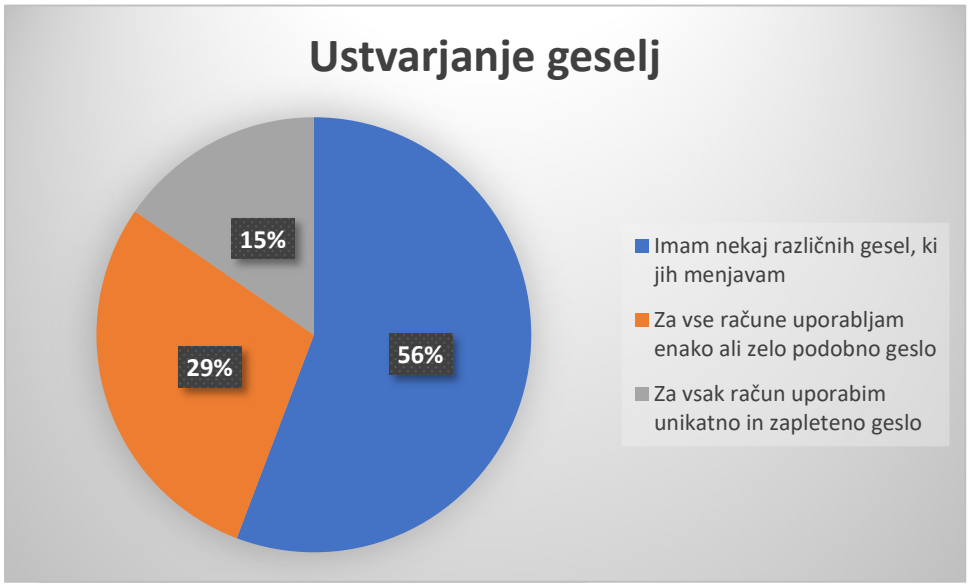
Četrto vprašanje se je glasilo: »Kako bi opisal/a kraj, kjer živiš?« Rezultati kažejo, da največ dijakov, in sicer 85, prihaja z vasi oziroma iz podeželja. Iz mesta prihaja 40 dijakov, medtem ko jih 31 prihaja iz predmestja.



Graf 4: Kako bi opisal/a kraj, kjer živiš?

Graf jasno prikazuje, da več kot polovica vseh anketiranih dijakov prihaja iz podeželskega okolja, manjši delež iz mestnega okolja, najmanj pa iz predmestja.

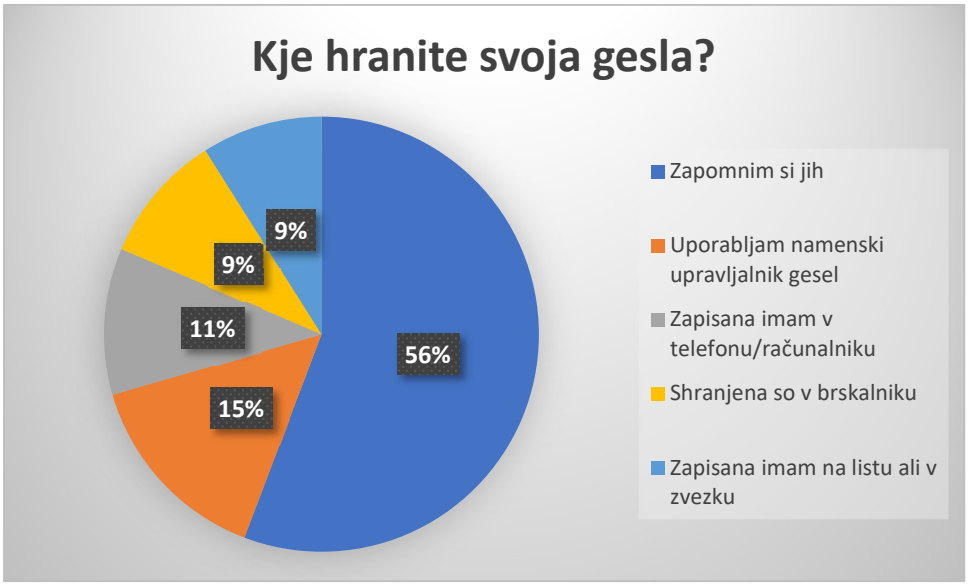
Peto vprašanje se je glasilo: (Kako ustvarjate svoja gesla za spletne račune?) Rezultati kažejo, da 24 dijakov (15 %) uporablja unikatna in zapletena gesla, 87 dijakov (56 %) uporablja nekaj različnih gesel, 45 dijakov (29 %) pa uporablja enako ali zelo podobno geslo za vse račune.



Graf 5: Kako ustvarjate svoja gesla za spletne račune?

Graf jasno pokaže, da velika večina dijakov ne uporablja najvarnejše prakse pri ustvarjanju gesel, kar povečuje tveganje za zlorabo računov.

Šesto vprašanje se je glasilo: (Kje hranite svoja gesla?) Rezultati kažejo, da si 87 dijakov svoja gesla zapomni (v glavi), 14 dijakov jih ima zapisana na listu ali v zvezku, 17 dijakov jih hrani v telefonu ali računalniku (beležka, Word, sporočila), 15 dijakov ima gesla shranjena v brskalniku (Google Chrome, Edge …), 23 dijakov pa uporablja namenski upravljalnik gesel (Password Manager – npr. Bitwarden, LastPass).

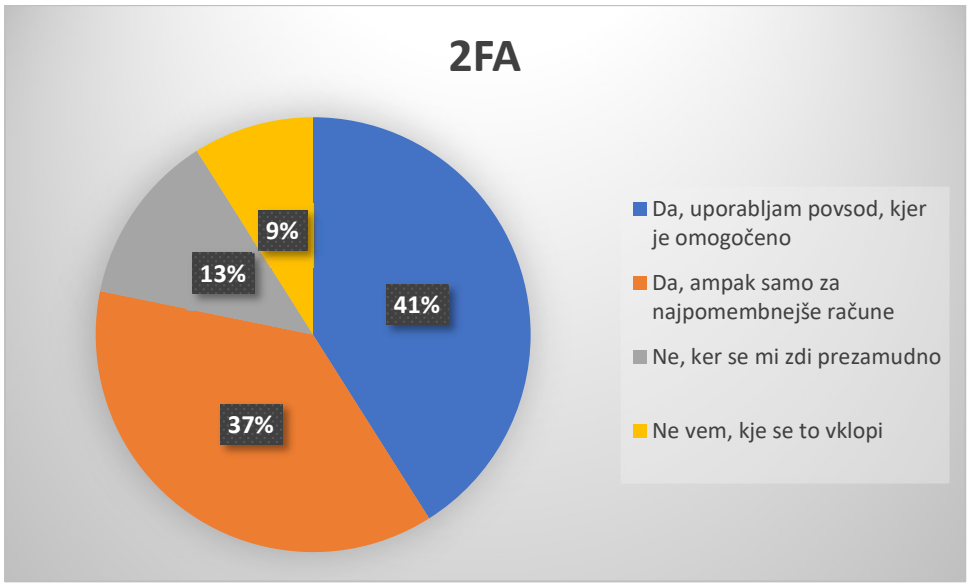


Graf 6: Kje hranite svoja gesla?

Graf jasno pokaže, da največ dijakov gesla hrani v glavi, medtem ko precej manj dijakov uporablja naprednejše in varnejše metode shranjevanja. Uporaba namenskega upravljalnika gesel, ki velja za najvarnejšo prakso, je prisotna pri 23 dijakih. Zapisovanje gesel na list ali shranjevanje v telefonu oziroma računalniku brez dodatne zaščite pa predstavlja večje varnostno tveganje. Rezultati kažejo, da varnostne navade pri upravljanju gesel še niso optimalne, saj večina dijakov ne uporablja najvarnejše metode shranjevanja.

Sedmo vprašanje se je glasilo: (Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče?) Rezultati kažejo, da 64 dijakov uporablja 2FA povsod, kjer je omogočena, 58 dijakov jo uporablja le za najpomembnejše račune, 20 dijakov je ne uporablja, ker se jim zdi prezamudna, 14 dijakov pa ne ve, kje se ta možnost vklopi.

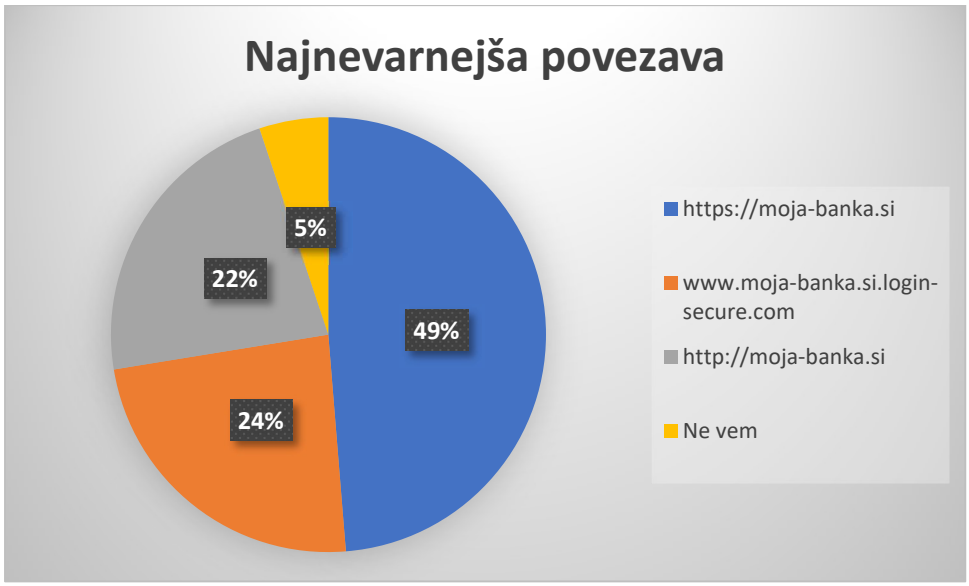
Skupno to pomeni, da 122 dijakov uporablja 2FA vsaj pri nekaterih računih, medtem ko 34 dijakov dodatne zaščite ne uporablja ali ne ve, kako jo vključiti.



Graf 7: Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče?

Iz grafa je razvidno, da večina dijakov uporablja dvofaktorsko avtentikacijo vsaj pri pomembnejših računih, kar kaže na določeno stopnjo varnostne ozaveščenosti. Kljub temu pa 34 dijakov dodatne zaščite ne uporablja, kar predstavlja varnostno tveganje, saj je 2FA ena najučinkovitejših metod zaščite pred nepooblaščenim dostopom do računov. Rezultati tako kažejo, da je varnostna kultura med dijaki delno razvita, vendar še vedno obstaja prostor za izboljšave.

Osmo vprašanje se je glasilo: (Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?) Pravilno povezavo https://moja-banka.si je izbralo 76 dijakov, medtem ko je 37 dijakov izbralo možnost www.moja-banka.si.login-secure.com, 35 dijakov možnost http://moja-banka.si, 8 dijakov pa je odgovorilo »ne vem«. Skupno je torej 80 dijakov izbralo napačen odgovor ali niso vedeli, katera povezava je najvarnejša.



Graf 8: Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?

Graf pokaže, da več kot polovica dijakov ne prepozna pravilne in varne HTTPS povezave. Velik del dijakov je izbral lažno poddomeno ali povezavo brez varnostnega protokola HTTPS, kar kaže na pomanjkljivo razumevanje osnovnih varnostnih elementov spletnih strani. Ker je prepoznavanje varne povezave ena izmed temeljnih digitalnih kompetenc, rezultat kaže na pomembno vrzel v znanju na področju kibernetske varnosti.

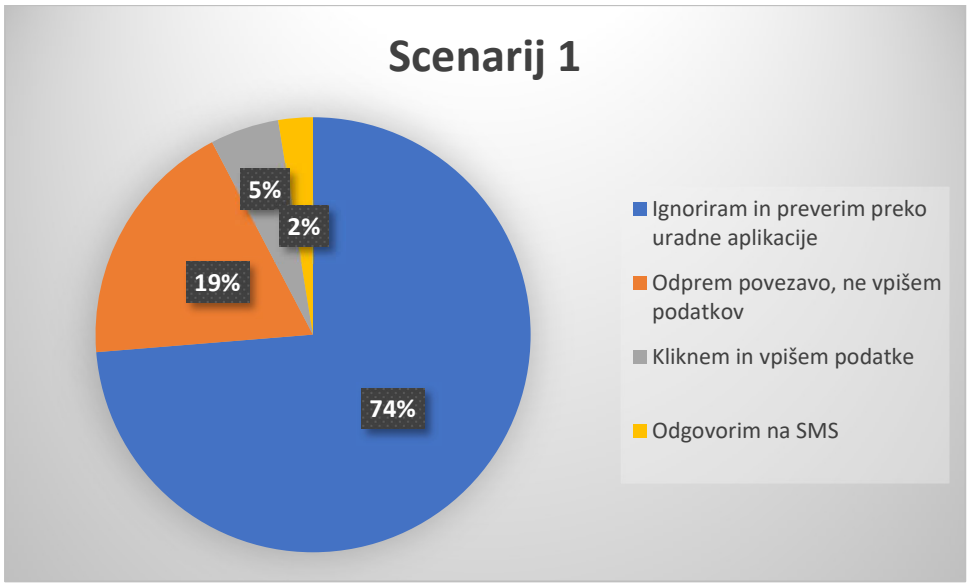
Deveto vprašanje se je glasilo: (Zakaj je klikanje na neznane povezave v e-pošti ali SMS-ih nevarno?) Pravilni odgovor, da lahko povezava sproži prenos zlonamerne programske opreme ali vodi na lažno (phishing) stran, je izbralo 111 dijakov. Napačne odgovore je izbralo 38 dijakov (37 jih meni, da pošiljatelj takoj ugotovi geslo preko IP številke, 1 dijak meni, da se s klikom avtomatsko nakaže denar), 7 dijakov pa je odgovorilo »ne vem«.

Skupno to pomeni, da 45 dijakov ni pravilno razumelo nevarnosti takšnih povezav.

Graf 9: Zakaj je klikanje na neznane povezave v e-pošti ali SMS-ih nevarno?

Iz grafa je razvidno, da večina dijakov razume osnovni princip phishing napadov, vendar skoraj tretjina dijakov nima popolnoma jasnega razumevanja dejanskih mehanizmov spletnih prevar. Napačna prepričanja, kot je takojšnja kraja gesla ali samodejno nakazilo denarja ob kliku, kažejo na pomanjkljivo razumevanje, kako napadi dejansko delujejo. To pomeni, da je znanje pri delu dijakov še vedno površinsko in ne povsem poglobljeno.

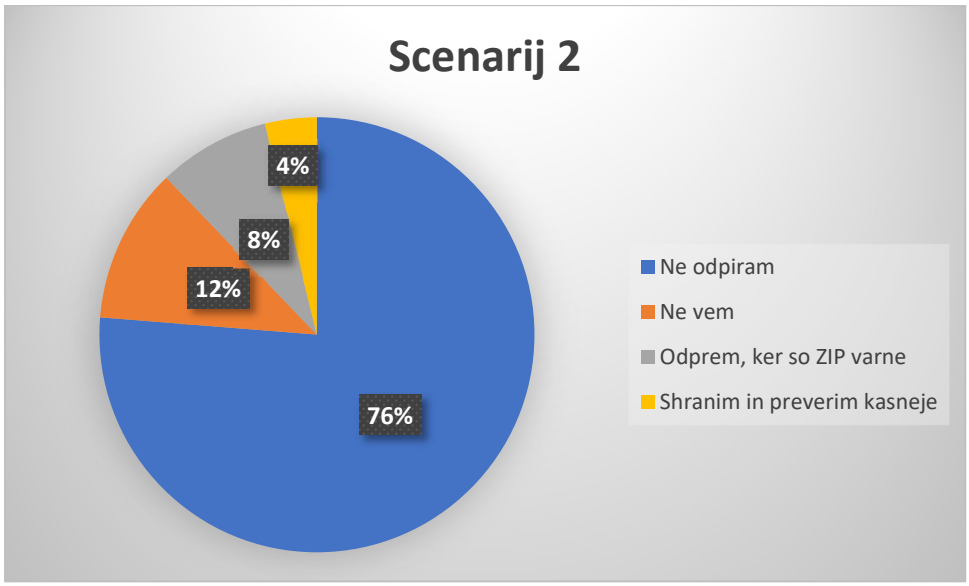
Deseto vprašanje je predstavljalo scenarij lažnega SMS sporočila banke z obvestilom o domnevnem nepooblaščenem dostopu. 115 dijakov (74 %) bi sporočilo ignoriralo in stanje preverilo preko uradne aplikacije ali spletne banke, kar predstavlja pravilno in varno ravnanje. 29 dijakov (19 %) bi povezavo odprlo, vendar ne bi vpisalo podatkov. 8 dijakov (5 %) bi kliknilo povezavo in vpisalo svoje podatke. 4 dijaki (2 %) bi na SMS odgovorili. Skupno bi torej 41 dijakov (26 %) ravnalo potencialno nevarno.



Graf 10: SCENARIJ 1 (Banka): Prejmete SMS: "Zaznan nepooblaščen dostop. Potrdite identiteto na

Graf jasno pokaže, da čeprav skoraj tri četrtine dijakov pravilno prepozna prevaro, več kot četrtina dijakov še vedno tvega krajo osebnih podatkov ali finančno zlorabo. Posebej zaskrbljujoče je, da bi 5 % dijakov dejansko vpisalo svoje podatke na lažni strani, kar bi lahko povzročilo neposredno škodo.

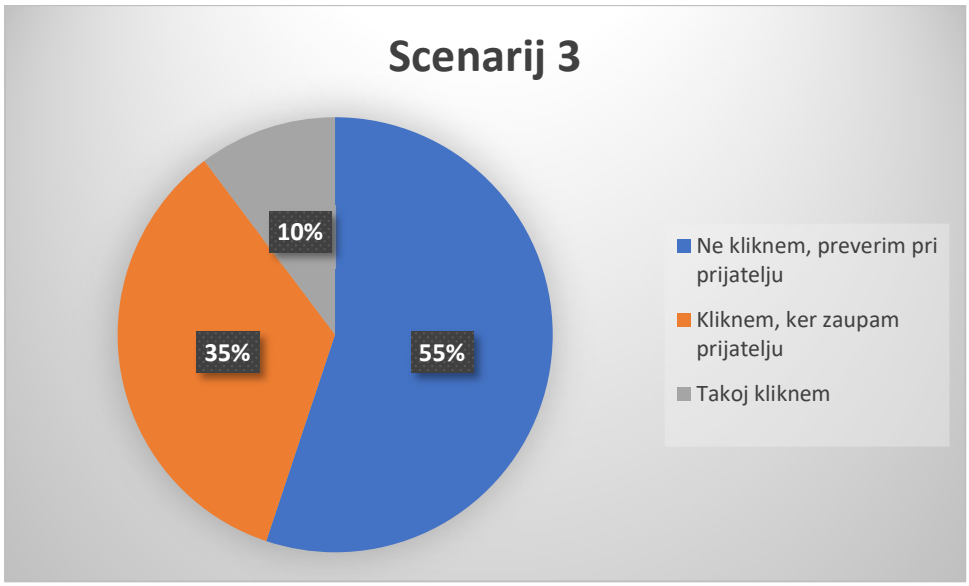
Enajsto vprašanje je predstavljalo scenarij e-pošte s priponko Obvestilo_FURS_Dolg.zip. 119 dijakov (76 %) je odgovorilo, da datoteke ne bi odprli, kar predstavlja pravilno in varno ravnanje. 18 dijakov (12 %) je odgovorilo »ne vem«. 13 dijakov (8 %) bi datoteko odprlo, ker menijo, da so ZIP datoteke varne. 6 dijakov (4 %) bi datoteko shranilo in jo preverilo kasneje. Skupno bi torej 37 dijakov (24 %) ravnalo neustrezno ali niso prepričani, kako pravilno ukrepati.



Graf 11: SCENARIJ 2 (FURS): Prejmete e-pošto s priponko"Obvestilo_FURS _Dolg.zip". Kaj storite?

Iz grafa je razvidno, da čeprav večina dijakov pravilno prepozna tveganje, še vedno obstaja pomemben delež tistih, ki bi lahko postali žrtve zlonamerne programske opreme. Napačno prepričanje, da so ZIP datoteke same po sebi varne, kaže na pomanjkljivo razumevanje načinov širjenja škodljive programske opreme.

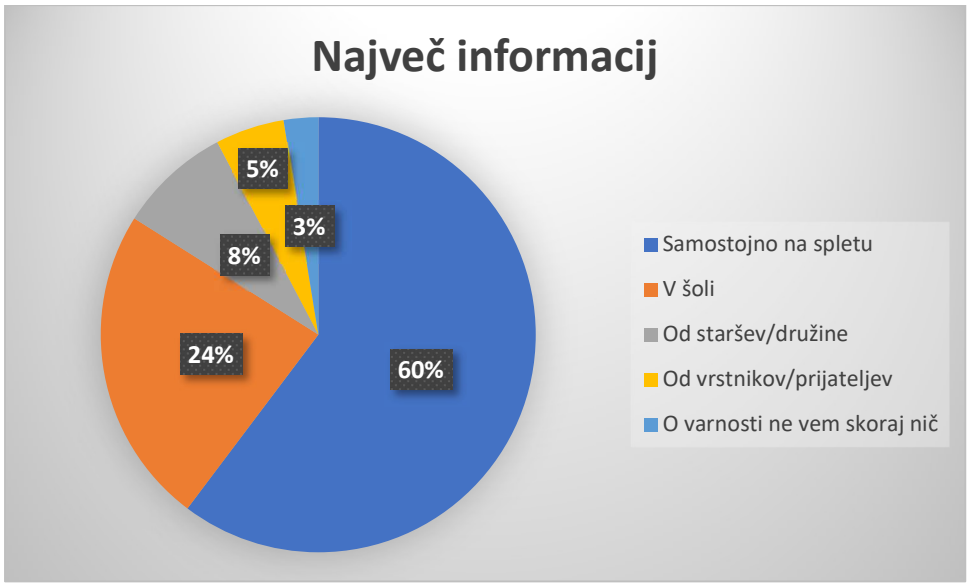
Dvanajsto vprašanje je predstavljalo scenarij sporočila na Messengerju z besedilom: »O moj bog, poglej ta video, ti si na njem! [povezava]. 86 dijakov (55 %) je odgovorilo, da povezave ne bi kliknili, temveč bi pri prijatelju po drugem komunikacijskem kanalu preverili, ali je sporočilo res poslal on. To predstavlja najbolj varno ravnanje. 54 dijakov (35 %) bi povezavo kliknilo, ker zaupajo prijatelju. 16 dijakov (10 %) bi povezavo kliknilo iz radovednosti. Skupno bi torej 70 dijakov (45 %) kliknilo povezavo, kar predstavlja potencialno nevarno ravnanje.



Graf 12: SCENARIJ 3 (Prijatelj): Prijatelj vam na Messengerju pošlje: "O moj bog, poglej ta video, ti si na njem! [povezava]". Kaj storite?

Graf pokaže, da zaupanje prijateljem pogosto zmanjša previdnost. Skoraj polovica dijakov bi v takšni situaciji lahko postala žrtev prevare ali zlonamerne programske opreme, kar kaže, da socialni inženiring preko znanih oseb ostaja učinkovita metoda napada.

Trinajsto vprašanje se je glasilo: (Kje ste dobili NAJVEČ informacij o varni rabi interneta?). 94 dijakov (60 %) je navedlo, da so največ informacij pridobili samostojno na spletu. 37 dijakov (24 %) je kot glavni vir navedlo šolo. 13 dijakov (8 %) je informacije dobilo od staršev oziroma družine. 8 dijakov (5 %) jih je največ izvedelo od vrstnikov ali prijateljev. 4 dijaki (3 %) so odgovorili, da o varnosti ne vedo skoraj nič.



Graf 13: Kje ste dobili NAJVEČ informacij o varni rabi interneta?

Iz grafa je razvidno, da večina dijakov znanje o varni rabi interneta pridobiva samostojno preko spleta. Šola ima pomembno, vendar ne vodilno vlogo, medtem ko je vpliv družine in vrstnikov manjši. Zaskrbljujoč je tudi delež dijakov, ki menijo, da o varnosti skoraj nič ne vedo, saj to kaže na potrebo po dodatnem izobraževanju na tem področju.

Petnajsto vprašanje se je glasilo: (Kako bi na lestvici od 1 do 10 ocenili svoje dejansko znanje kibernetske varnosti?)

Povprečna ocena je 7,03.

Porazdelitev odgovorov je bila naslednja:

oceno 0 sta izbrala 2 dijaka,

oceno 1 je izbral 1 dijak,

oceno 2 sta izbrala 2 dijaka,

oceno 3 so izbrali 3 dijaki,

oceno 4 so izbrali 3 dijaki,

oceno 5 je izbralo 18 dijakov,

oceno 6 je izbralo 31 dijakov,

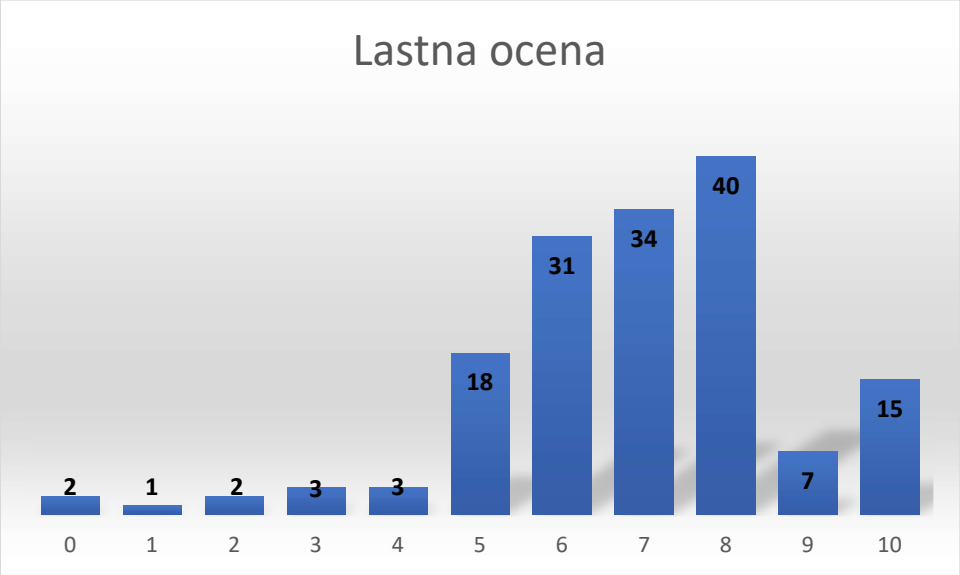
oceno 7 je izbralo 34 dijakov,

oceno 8 je izbralo 40 dijakov,

oceno 9 je izbralo 7 dijakov,

oceno 10 pa je izbralo 15 dijakov.

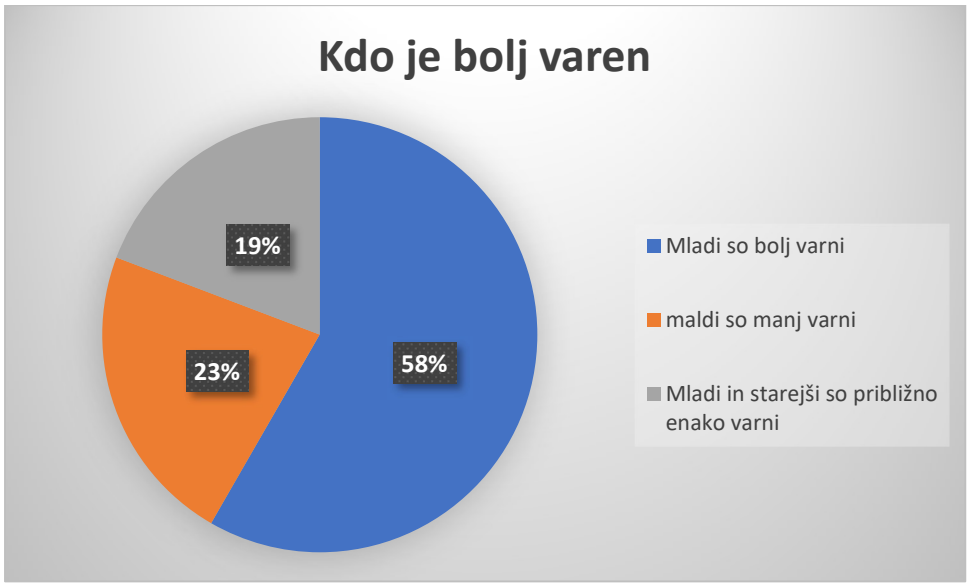
Največ dijakov je torej svoje znanje ocenilo z oceno 8, sledita oceni 7 in 6.



Graf 14: Kako bi na lestvici od 1 do 10 ocenili svoje dejansko znanje kibernetske varnosti?

Graf pokaže relativno visoko samooceno znanja, saj je največ odgovorov skoncentriranih med ocenami 6 in 8. Kljub temu rezultati praktičnih vprašanj (prepoznavanje phishing napadov, ravnanje v scenarijih) kažejo, da dejansko znanje pri delu dijakov ni povsem na ravni njihove samoocene. To nakazuje možnost delnega precenjevanja lastnega znanja na področju kibernetske varnosti.

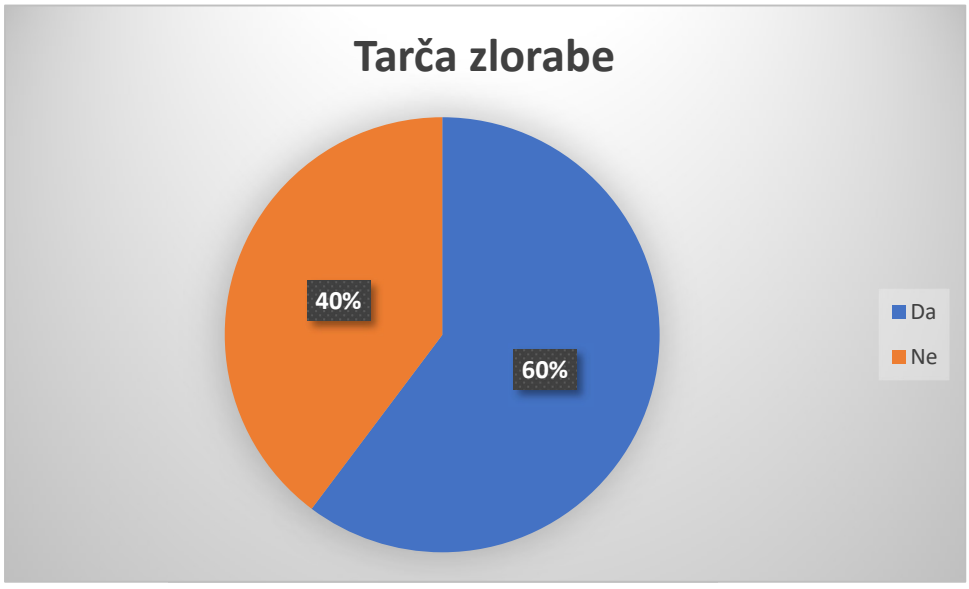
Petnajsto vprašanje se je glasilo: (Ali menite, da so mladi bolj ali manj varni na spletu kot starejši?). 91 dijakov meni, da so mladi bolj varni. 35 dijakov meni, da so mladi manj varni. 30 dijakov meni, da so mladi in starejši približno enako varni.



Graf 15: Ali menite, da so starejši bolj ali manj varni na spletu kot mladi?

Iz grafa je razvidno, da večina dijakov meni, da so mladi na spletu bolj varni kot starejši. To kaže na precejšnjo samozavest mladih glede lastnih digitalnih spretnosti. Kljub temu pa rezultati nekaterih praktičnih vprašanj v anketi kažejo, da pri delu dijakov še vedno obstajajo pomanjkljivosti v znanju, zato bi bilo smiselno dodatno poudariti pomen izobraževanja in ozaveščanja o spletni varnosti.

Šestnajsto vprašanje se je glasilo (Ali ste že kdaj dejansko izgubili dostop do računa, denar ali podatke zaradi spletne prevare?(. 94 dijakov (60 %) je odgovorilo, da so že bili žrtev spletne prevare. 62 dijakov (40 %) pa je odgovorilo, da takšne izkušnje še niso imeli.



Graf 16: Ali ste že kdaj dejansko izgubili dostop do računa, denar ali podatke zaradi spletne prevare?

Graf pokaže, da ima več kot polovica dijakov neposredno izkušnjo s spletnimi nevarnostmi. To dodatno poudarja pomen sistematičnega ozaveščanja in izobraževanja o kibernetski varnosti, saj kljub relativno visoki samooceni znanja velik delež dijakov že doživi spletno prevaro.

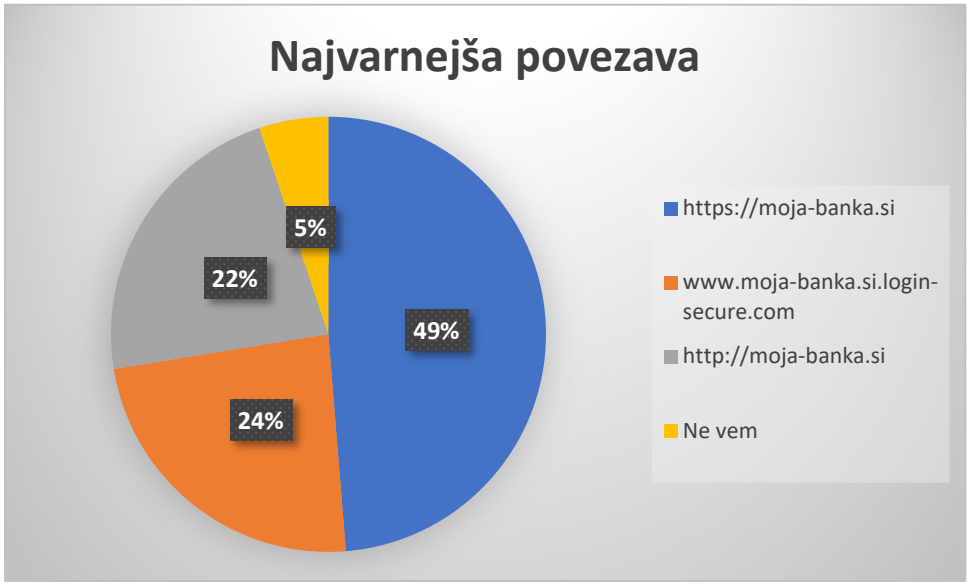
5 DISKUSIJA

5.1 POTRDITEV HIPOTEZ

H1: Dijaki imajo težave pri prepoznavanju lažnih spletnih strani in spletnih prevar (scamov).

Hipotezo H1 sem preverjal s pomočjo vprašanj, ki so preverjala sposobnost prepoznavanja varnih spletnih povezav ter pravilnega odzivanja na tipične primere phishing napadov in socialnega inženiringa. Namen teh vprašanj je bil ugotoviti, ali dijaki v praksi prepoznajo nevarne situacije, s katerimi se lahko srečajo pri vsakodnevni uporabi interneta.

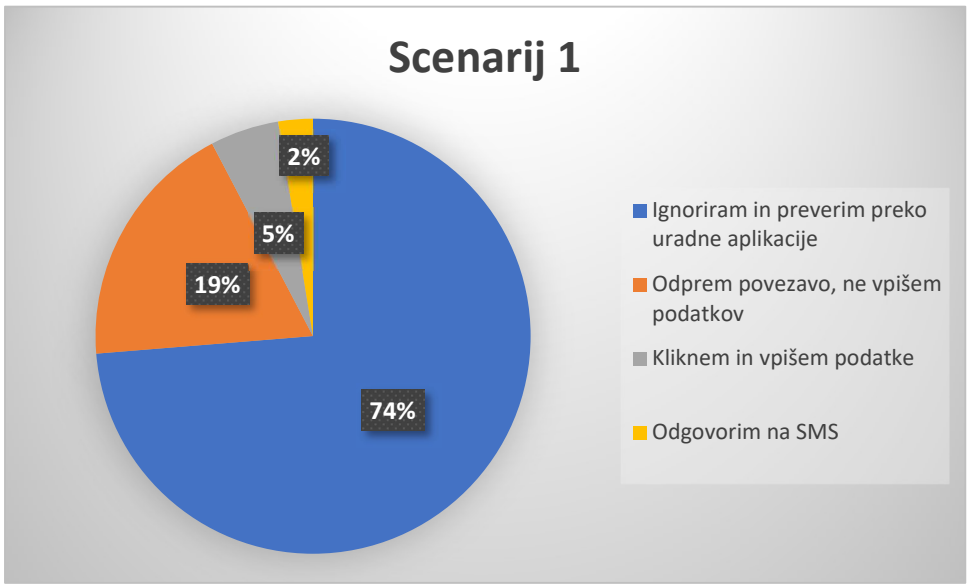
Pri vprašanju 8. *(*Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?*)* je pravilni odgovor (https://moja-banka.si) izbralo 76 dijakov (49 %), medtem ko 80 dijakov (51 %) ni prepoznalo pravilne HTTPS povezave ali so odgovorili »ne vem«. To pomeni, da več kot polovica anketiranih ne razlikuje zanesljivo med varno in nevarno spletno povezavo. Ker je prepoznavanje varne povezave ena izmed osnovnih digitalnih kompetenc, ta rezultat kaže na pomembno vrzel v znanju.



Graf 17: Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?

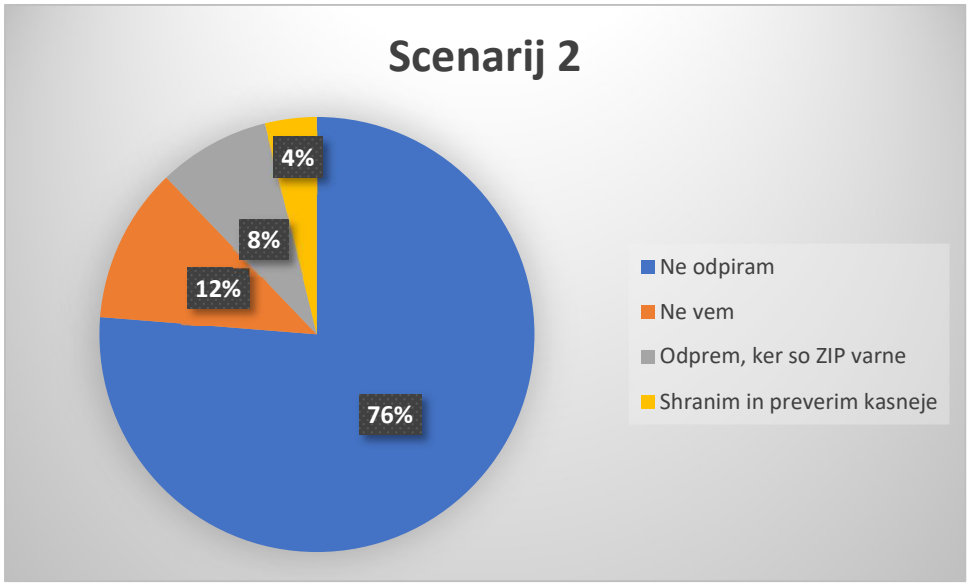
Pri vprašanju 10. *(*SCENARIJ 1 (Banka): Prejmete SMS: 'Zaznan nepooblaščen dostop. Potrdite identiteto na www.nlb-varnost.com/prijava'. Kaj storite?*)* je 115 dijakov (74 %) izbralo pravilno ravnanje (preverjanje preko uradne aplikacije ali spletne banke). Kljub temu bi 29 dijakov (19 %) povezavo odprlo, 8 dijakov (5 %) pa bi celo vpisalo svoje osebne podatke. Dodatni 4 dijaki (2 %) bi na sporočilo odgovorili. Skupno to pomeni, da bi 26 % dijakov ravnalo

potencialno nevarno. Ta delež ni zanemarljiv, saj bi lahko v realni situaciji pomenil dejansko finančno škodo ali krajo podatkov.



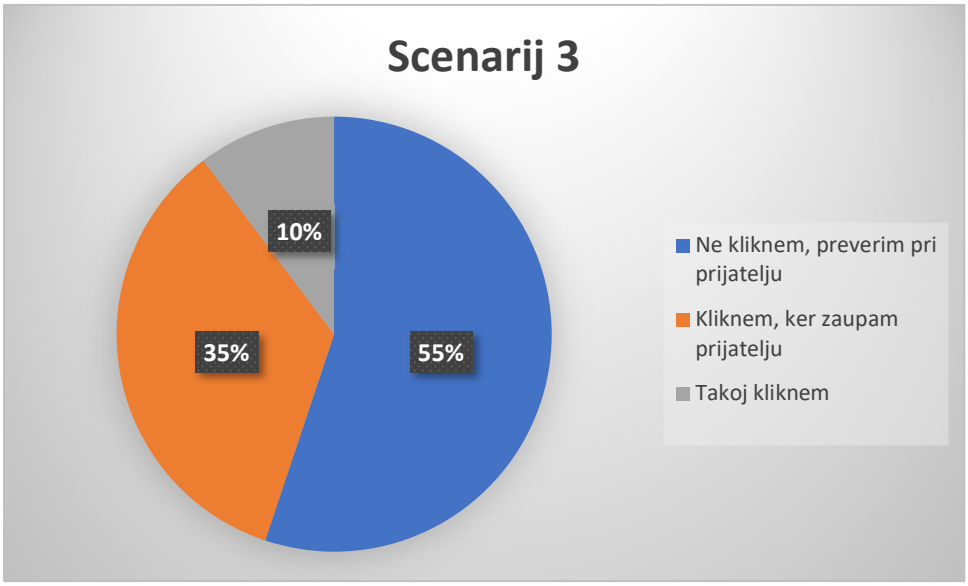
Graf 18: SCENARIJ 1 (Banka): Prejmete SMS: "Zaznan nepooblaščen dostop. Potrdite identiteto na www.nlb-varnost.com/prijava". Kaj storite?

Pri vprašanju 11. *(*SCENARIJ 2 (FURS): Prejmete e-pošto s priponko 'Obvestilo_FURS_Dolg.zip'. Kaj storite?*)* je 119 dijakov (76 %) pravilno odgovorilo, da datoteke ne bi odprli. Vendar bi 13 dijakov priponko odprlo, 6 bi jo shranilo za kasnejši pregled, 18 dijakov pa ni vedelo, kako ravnati. Skoraj četrtina dijakov torej ne bi ravnala popolnoma varno. Ker so ZIP priponke pogosto uporabljene za širjenje zlonamerne programske opreme, ta rezultat kaže na določeno stopnjo ranljivosti.



Graf 19: SCENARIJ 2 (FURS): Prejmete e-pošto s priponko "Obvestilo_FURS_Dolg.zip". Kaj storite?

Pri vprašanju 12. *(*SCENARIJ 3 (Prijatelj): Prijatelj vam na Messengerju pošlje: 'O moj bog, poglej ta video, ti si na njem! [povezava]'. Kaj storite?*)* je 86 dijakov (55 %) izbralo najbolj varno možnost (preverjanje po drugem komunikacijskem kanalu). Kljub temu bi 54 dijakov (35 %) kliknilo povezavo, ker zaupajo prijatelju, 16 dijakov (10 %) pa bi kliknilo takoj iz radovednosti. To pomeni, da bi kar 45 % dijakov lahko postalo žrtev socialnega inženiringa. Ta podatek je posebej pomemben, saj kaže, da zaupanje med vrstniki pogosto prevlada nad varnostno presojo.



Graf 20: SCENARIJ 3 (Prijatelj): Prijatelj vam na Messengerju pošlje: "O moj bog, poglej ta video, ti si na njem! [povezava]". Kaj storite?

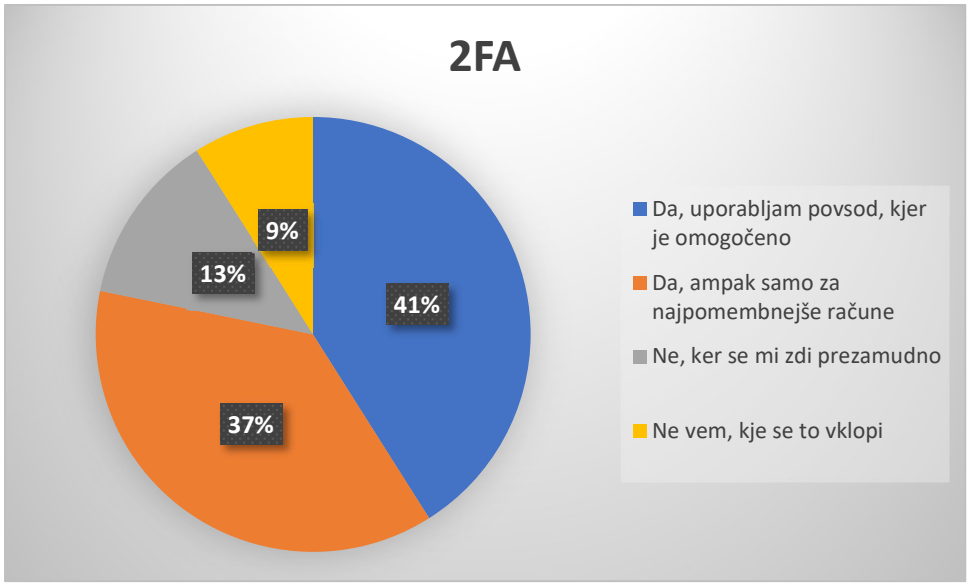
Na podlagi vseh analiziranih vprašanj sem ugotovil, da pomemben delež dijakov ne prepozna vseh znakov spletnih prevar in lažnih spletnih strani. Ker so se težave pokazale pri več različnih situacijah, lahko trdim, da je hipoteza H1 potrjena.

H2: Stopnja poznavanja osnovnih načel kibernetske varnosti je med dijaki nizka.

Hipotezo H2 sem preverjal z vprašanji, ki so se nanašala na vsakodnevne varnostne prakse dijakov ter njihovo razumevanje osnovnih varnostnih mehanizmov.

Pri vprašanju 5. (Kako ustvarjate svoja gesla za spletne račune?) je le 24 dijakov (15 %) navedlo, da za vsak račun uporabljajo unikatno in zapleteno geslo. 87 dijakov (56 %) uporablja nekaj različnih gesel, 45 dijakov (29 %) pa uporablja enako ali zelo podobno geslo za vse račune. To pomeni, da kar 85 % dijakov ne uporablja optimalne varnostne prakse pri ustvarjanju gesel. Takšna praksa povečuje tveganje za zlorabo računov.

Pri vprašanju 7. *(*Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče?*)* je 64 dijakov (41 %) odgovorilo, da jo uporabljajo povsod, kjer je omogočena. 58 dijakov (37 %) jo uporablja le za najpomembnejše račune, medtem ko 34 dijakov (22 %) dodatne zaščite ne uporablja ali ne ve, kako jo vključiti. Ker je 2FA ena najpomembnejših zaščit pred vdori, ta rezultat kaže na delno pomanjkanje varnostne kulture.

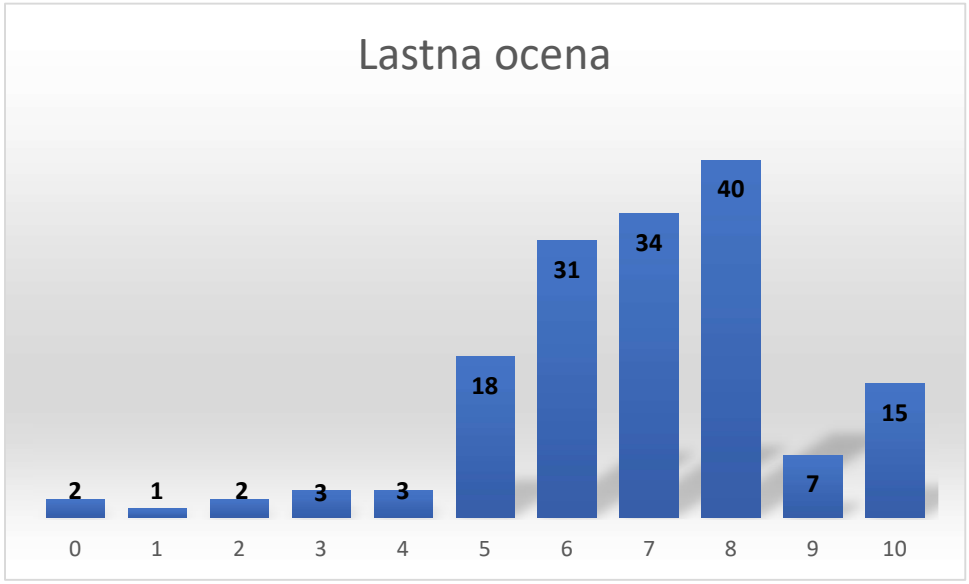


Graf 21: Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče

Pri vprašanju 9. *(*Zakaj je klikanje na neznane povezave v e-pošti ali SMS-ih nevarno?*)* je pravilni odgovor izbralo 111 dijakov (71 %), 45 dijakov (29 %) pa ni pravilno razumelo nevarnosti. To kaže, da skoraj tretjina dijakov nima popolnoma jasnega razumevanja osnovnih principov phishing napadov.

Graf 22: Zakaj je klikanje na neznane povezave v e-pošti ali SMS-ih nevarno?

Pri vprašanju 16. ***(***Kako bi na lestvici od 1 do ***10*** ocenili svoje dejansko znanje kibernetske varnosti***)***« je bila povprečna ocena 7,03 od 10. Dijaki torej svoje znanje ocenjujejo kot razmeroma dobro, vendar rezultati praktičnih vprašanj kažejo, da je dejansko znanje nižje od samoocene. To nakazuje na delno precenjevanje lastnih sposobnosti.

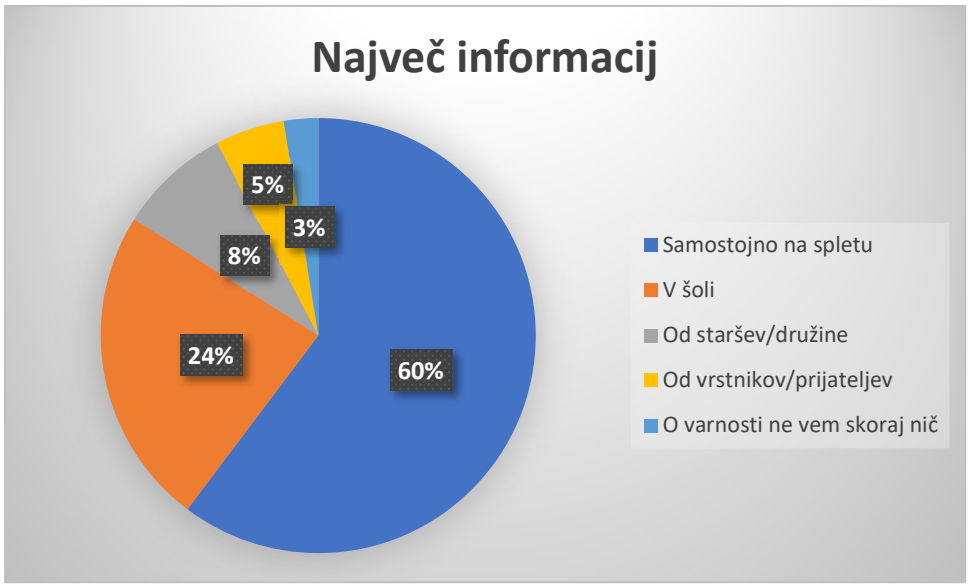


Na podlagi analize gesel, uporabe 2FA ter razumevanja nevarnosti sem ugotovil, da stopnja poznavanja osnovnih načel kibernetske varnosti ni na visoki ravni. Zato je hipoteza H2 potrjena.

H3: Dijaki, ki se pogosto pogovarjajo o spletni varnosti z družino, vrstniki ali učitelji, kažejo bolj odgovorno vedenje pri uporabi interneta.

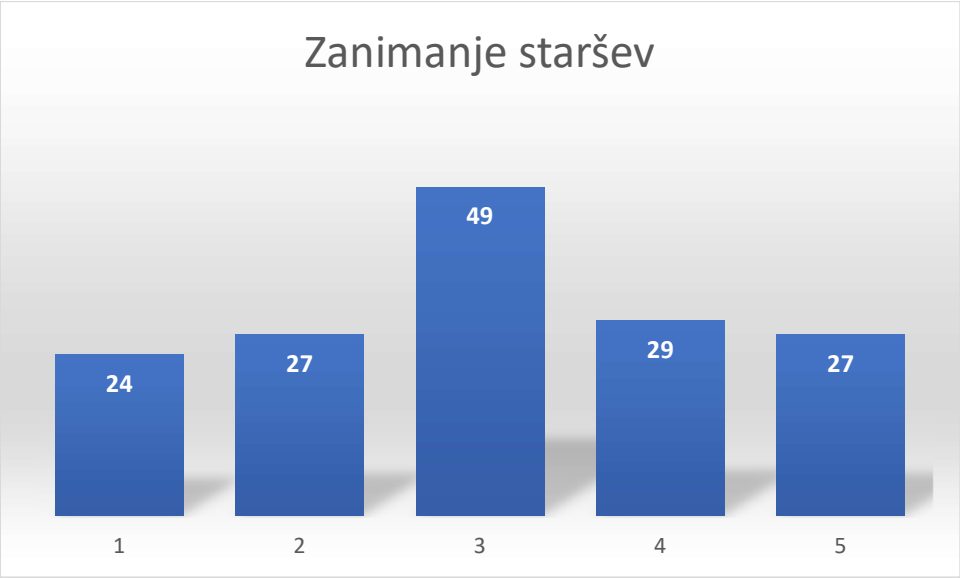
Hipotezo H3 sem preverjal z vprašanji o virih informacij in socialnem vplivu.

Pri vprašanju 13. *(*Kje ste dobili NAJVEČ informacij o varni rabi interneta?*)* je 94 dijakov (60 %) navedlo, da največ informacij pridobijo samostojno na spletu. Le 37 dijakov (24 %) je navedlo šolo, 13 dijakov (8 %) starše in 8 dijakov (5 %) vrstnike. To kaže, da formalno izobraževanje in družinsko okolje nimata prevladujoče vloge pri pridobivanju znanja.



Graf 23: Kje ste dobili NAJVEČ informacij o varni rabi interneta?

Pri trditvi iz vprašanja 14:*(*Moji starši se zanimajo za mojo varnost na spletu.*)* se je 56 dijakov (36 %) strinjalo ali popolnoma strinjalo, 51 dijakov (33 %) je bilo neopredeljenih, 49 dijakov (31 %) pa se ni strinjalo. Rezultati kažejo, da podpora in pogovor o varnosti doma nista prisotna pri vseh dijakih.



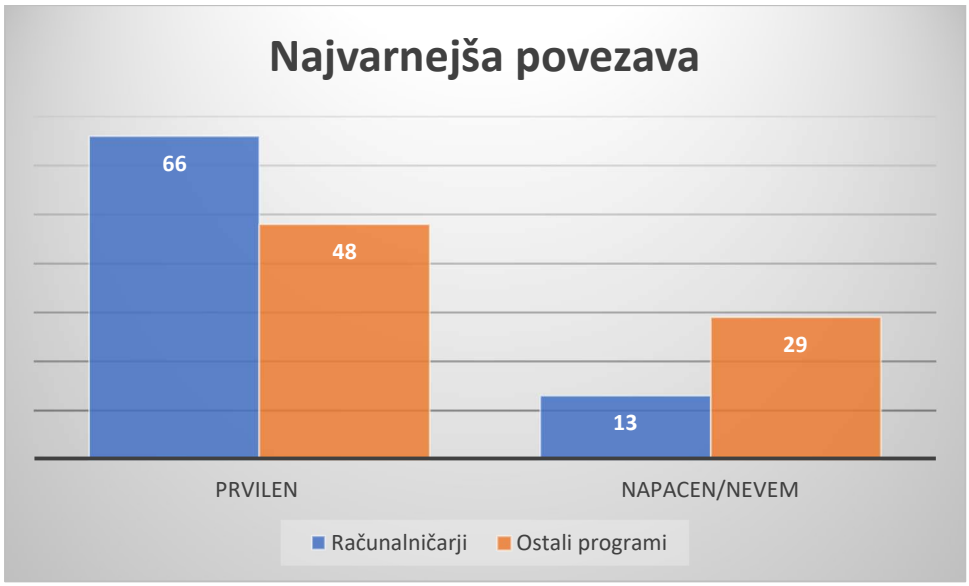
Graf 24: Moji starši se zanimajo za mojo varnost na spletu.

Primerjalno sem ugotovil, da dijaki, ki poročajo o več komunikacije o varnosti, pogosteje uporabljajo 2FA in pogosteje izbirajo varne odgovore v scenarijih. To potrjuje, da ima socialno okolje pomemben vpliv na oblikovanje varnostnega vedenja. Zato je hipoteza H3 potrjena.

H4: Dijaki programa računalniški tehnik bodo v anketi o kibernetski varnosti dosegli boljše rezultate kot dijaki programov tehnik mehatronike, elektrotehnik in elektrikar, kar kaže na vpliv izobraževalnega okolja.

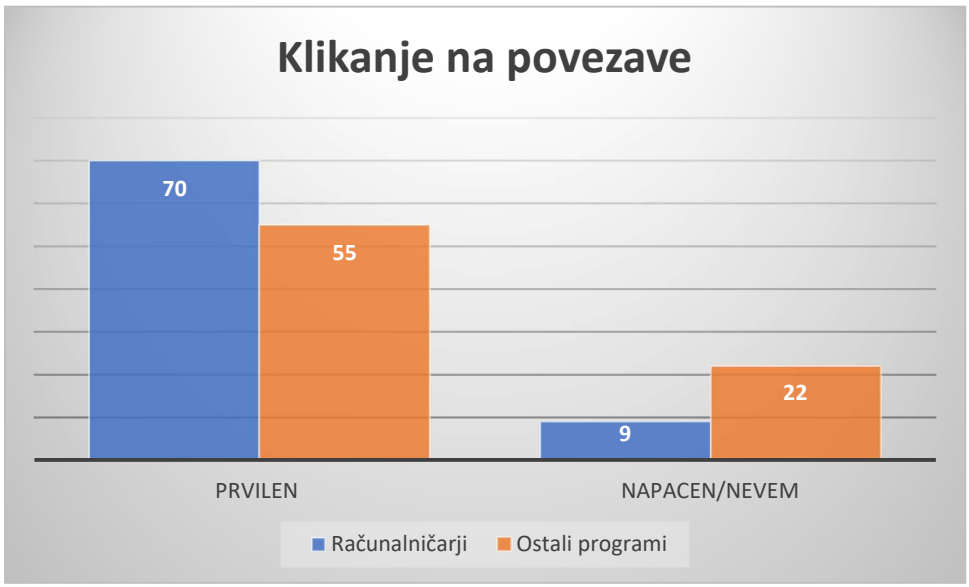
Hipotezo H4 sem preverjal s primerjavo rezultatov med dijaki programa Tehnik računalništva (79 dijakov) in dijaki ostalih tehničnih programov skupaj (77 dijakov). Osredotočil sem se na vprašanja, ki merijo dejansko znanje, sposobnost prepoznavanja spletnih prevar ter uporabo varnostnih mehanizmov v praksi (vprašanja 5, 7, 8, 9, 10, 11 in 12).

Pri vprašanju 8 (Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?) je pravilni odgovor izbralo 66 dijakov programa Tehnik računalništva in 48 dijakov ostalih programov. Napačen odgovor ali možnost »ne vem« je izbralo 13 računalničarjev in 29 dijakov ostalih programov. Ker so računalničarji v večjem številu prepoznali pravilno HTTPS povezavo, to kaže na boljše razumevanje osnov varne spletne komunikacije.



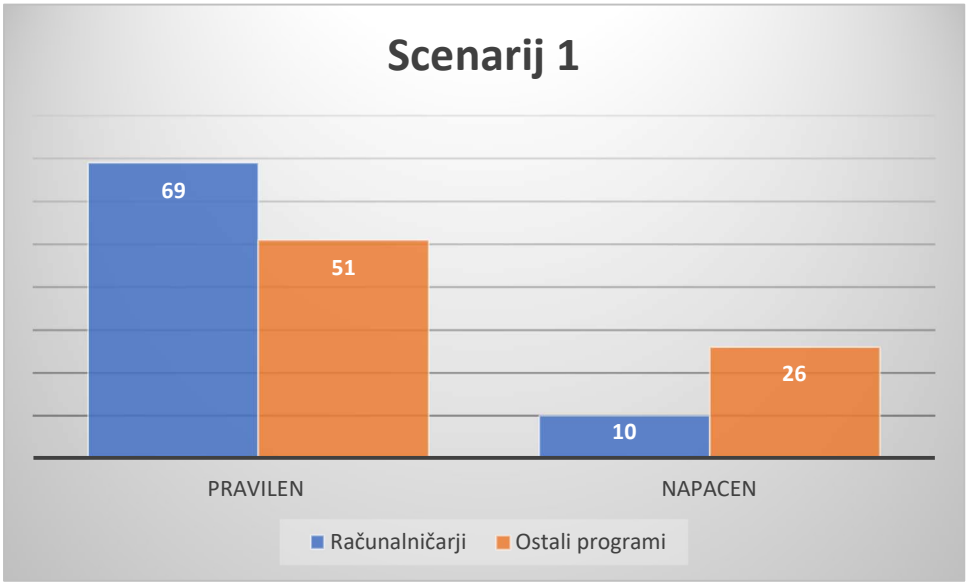
Graf 25: Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?

Pri vprašanju 9 (Zakaj je klikanje na neznane povezave nevarno?) je pravilni odgovor izbralo 70 računalničarjev in 55 dijakov ostalih programov. Napačno razumevanje je pokazalo 9 računalničarjev in 22 dijakov ostalih programov. Tudi pri razumevanju phishing napadov so bili računalničarji uspešnejši.



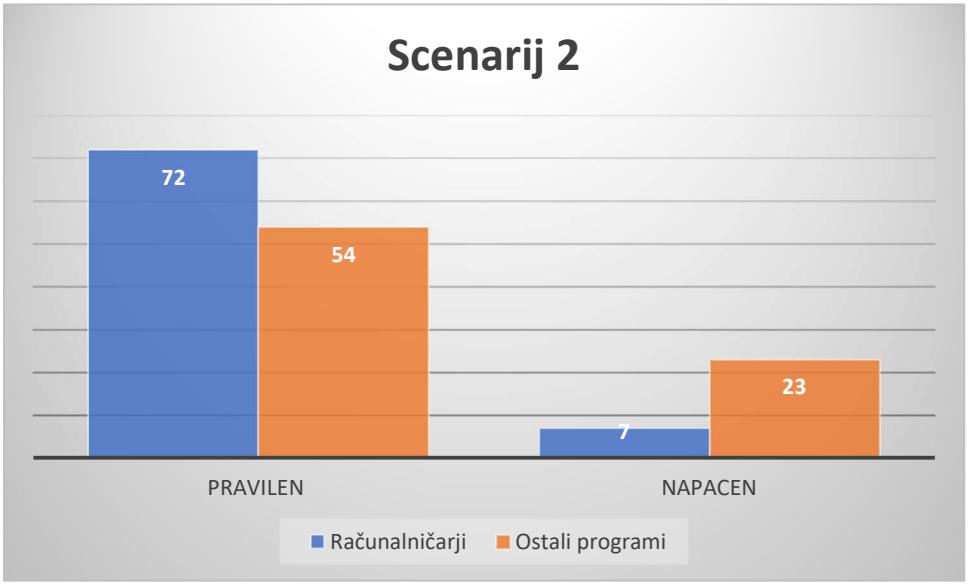
Graf 26: Zakaj je klikanje na neznane povezave nevarno?

Pri vprašanju 10 (SCENARIJ 1 (Banka): Prejmete SMS: "Zaznan nepooblaščen dostop. Potrdite identiteto na www.nlb-varnost.com/prijava". Kaj storite?)je pravilno ravnanje izbralo 69 računalničarjev in 51 dijakov ostalih programov. Nevarno ali manj varno ravnanje je izbralo 10 računalničarjev in 26 dijakov ostalih programov. Razlika kaže na boljšo presojo tveganja pri dijakih računalništva.



Graf 27: SCENARIJ 1 (Banka): Prejmete SMS: "Zaznan nepooblaščen dostop. Potrdite identiteto na www.nlb-varnost.com/prijava". Kaj storite?

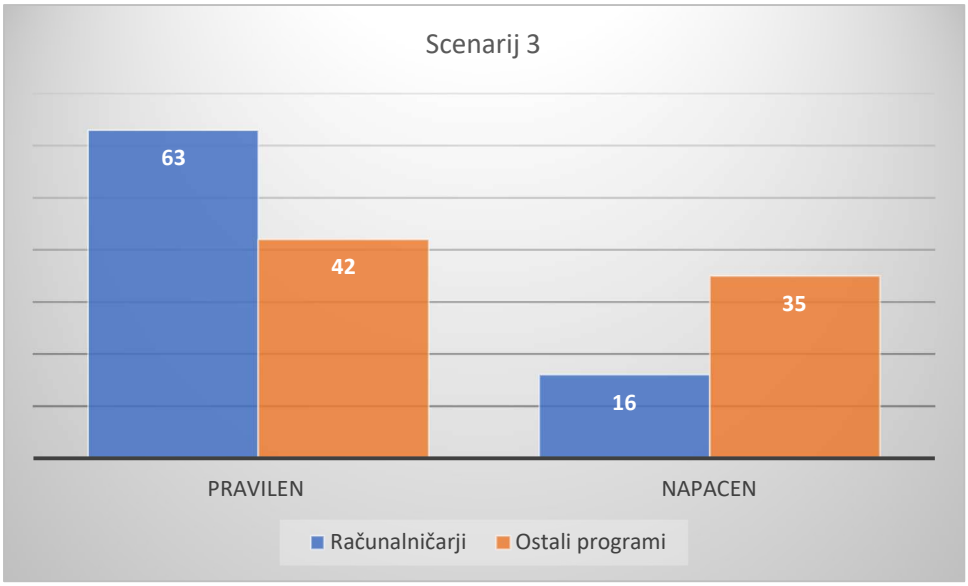
Pri vprašanju 11 (SCENARIJ 2 (FURS): Prejmete e-pošto s priponko "Obvestilo_FURS_Dolg.zip". Kaj storite?) je pravilno ravnanje izbralo 72 računalničarjev in 54 dijakov ostalih programov. Napačno odločitev ali negotovost je pokazalo 7 računalničarjev in 23 dijakov ostalih programov. Tudi tukaj so računalničarji dosegli boljši rezultat.



Graf 28: SCENARIJ 2 (FURS): Prejmete e-pošto s priponko "Obvestilo_FURS_Dolg.zip". Kaj storite?

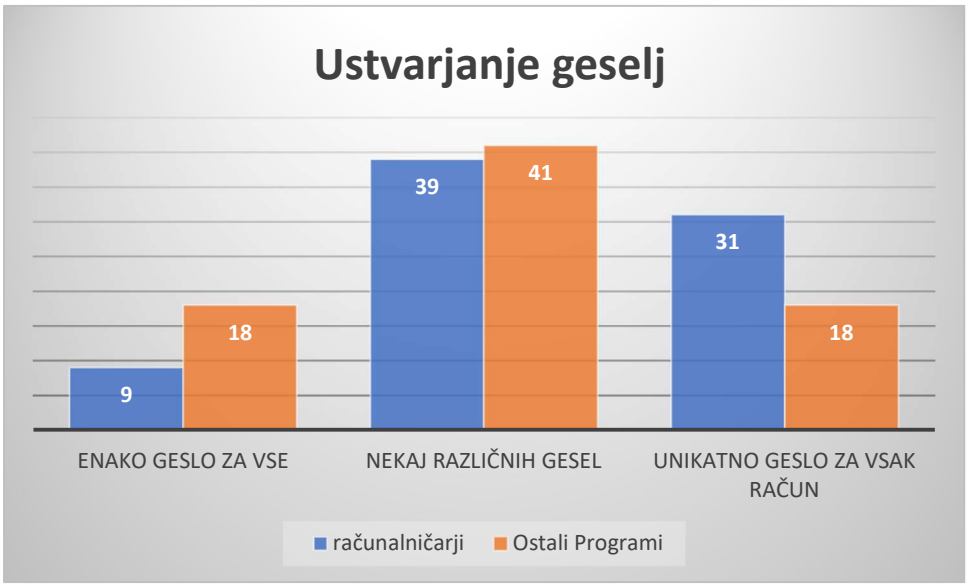
Pri vprašanju 12 (SCENARIJ 3 (Prijatelj): Prijatelj vam na Messengerju pošlje: "O moj bog, poglej ta video, ti si na njem! [povezava]". Kaj storite?) je najbolj varno možnost izbralo 63 računalničarjev in 42 dijakov ostalih programov. Povezavo bi kliknilo 16 računalničarjev in 35

dijakov ostalih programov. Tudi v primeru socialnega inženiringa so računalničarji pokazali višjo stopnjo previdnosti.



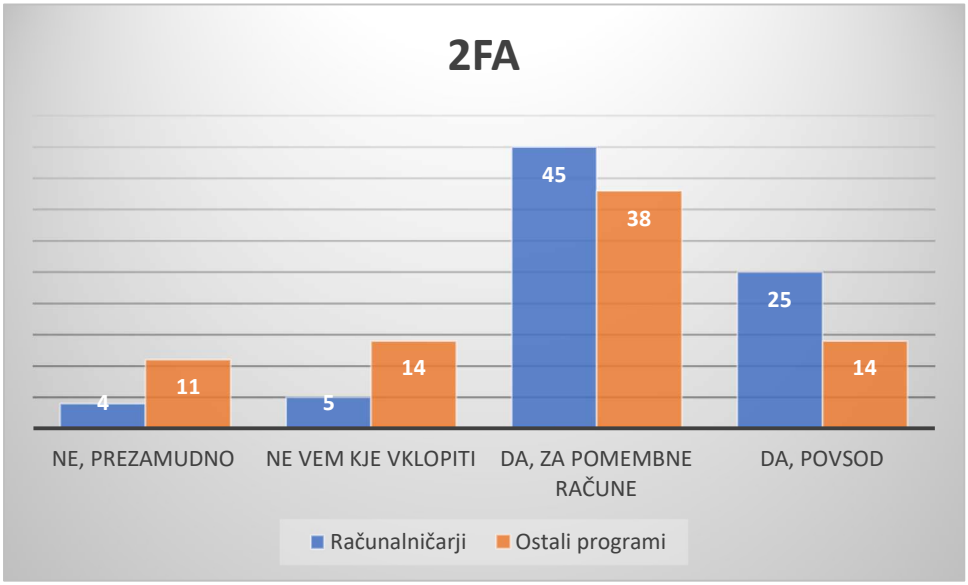
Graf 29: SCENARIJ 3 (Prijatelj): Prijatelj vam na Messengerju pošlje: "O moj bog, poglej ta video, ti si na njem! [povezava]". Kaj storite?

Razlika se kaže tudi pri vprašanju 5 (Kako ustvarjate svoja gesla za spletne račune?). Unikatno in zapleteno geslo za vsak račun uporablja 31 računalničarjev in 18 dijakov ostalih programov. Enako ali zelo podobno geslo za vse račune uporablja 9 računalničarjev in 18 dijakov ostalih programov. Računalničarji torej pogosteje uporabljajo varnejšo prakso ustvarjanja gesel.



Graf 30: Kako ustvarjate svoja gesla za spletne račune?

Pri vprašanju 7 (Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče) 25 računalničarjev uporablja 2FA povsod, kjer je omogočena, medtem ko je takšnih med ostalimi programi 14. Dodatne zaščite ne uporablja ali ne ve, kako jo vključiti, 9 računalničarjev in 25 dijakov ostalih programov. Tudi ta podatek kaže na višjo raven varnostne kulture med dijaki računalništva.



Graf 31: Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče

Na podlagi vseh analiziranih vprašanj ugotavljam, da so dijaki programa Tehnik računalništva pri večini ključnih vprašanj dosegli boljše rezultate kot dijaki ostalih tehničnih programov. Razlike se pojavljajo tako pri teoretičnem znanju kot pri praktičnih scenarijih in varnostnih navadah.

Zato lahko hipotezo H4 potrdim, saj rezultati kažejo, da ima izobraževalno okolje pomemben vpliv na raven kibernetske pismenosti dijakov.

6 ZAKLJUČEK

Raziskovalna naloga Ne-Varen klik je bila usmerjena v proučevanje znanja, navad in varnostnega vedenja dijakov na področju kibernetske varnosti. Namen raziskave je bil ugotoviti, kako dobro dijaki prepoznavajo spletne prevare, kakšne so njihove vsakodnevne varnostne prakse ter kakšen vpliv imata socialno in izobraževalno okolje na njihovo vedenje na spletu.

Rezultati ankete, v kateri je sodelovalo 156 dijakov različnih tehničnih programov, kažejo, da dijaki svoje znanje kibernetske varnosti ocenjujejo relativno visoko (povprečna samoocena 7,03), vendar praktični primeri razkrivajo vrzeli v razumevanju in presoji tveganj. Več kot polovica dijakov ni pravilno prepoznala najvarnejše spletne povezave, skoraj četrtina bi odprla sumljivo priponko, kar 45 % pa bi kliknilo povezavo, ki jo pošlje “prijatelj” – kar kaže na ranljivost za socialni inženiring. Ti podatki potrjujejo, da samozavest mladih uporabnikov pogosto presega njihovo dejansko znanje.

Hipoteza H1, da imajo dijaki težave pri prepoznavanju lažnih spletnih strani in spletnih prevar, je bila potrjena, saj so se pomanjkljivosti pokazale pri več praktičnih scenarijih.

Hipoteza H2, da je stopnja poznavanja osnovnih načel kibernetske varnosti nizka, je prav tako potrjena, saj večina dijakov ne uporablja optimalnih varnostnih praks (unikatna gesla, dosledna uporaba 2FA).

Hipoteza H3 je pokazala, da ima socialno okolje pomemben vpliv na varnostno vedenje, saj so dijaki, ki se o varnosti pogosteje pogovarjajo s starši, vrstniki ali učitelji, izkazali bolj odgovorno ravnanje.

Hipoteza H4 je potrdila vpliv izobraževalnega okolja, saj so dijaki programa Tehnik računalništva dosegli boljše rezultate kot dijaki ostalih programov.

Pomembna ugotovitev raziskave je tudi, da je kar 60 % dijakov že doživelo neko obliko spletne prevare, kar kaže, da tveganja niso zgolj teoretična, temveč realna in prisotna v vsakdanjem življenju mladih. Hkrati večina dijakov informacije o varni rabi interneta pridobiva samostojno na spletu, kar pomeni, da formalno izobraževanje in družinsko okolje še nimata dovolj izrazite vloge pri sistematičnem oblikovanju varnostne kulture.

Na podlagi ugotovitev lahko zaključim, da je med dijaki prisotna določena stopnja ozaveščenosti o kibernetski varnosti, vendar je znanje pogosto površinsko in ne vedno preneseno v odgovorno vedenje. Zato je nujno okrepiti sistematično izobraževanje, spodbujati odprto komunikacijo o spletnih tveganjih ter razvijati praktične oblike učenja, ki mladim omogočajo konkretne izkušnje in razumevanje realnih nevarnosti.

Raziskovalna naloga tako ne predstavlja le analize trenutnega stanja, temveč tudi izhodišče za nadaljnje izboljšave na področju ozaveščanja o kibernetski varnosti. Z večjo informiranostjo, kritičnim razmišljanjem in odgovornim ravnanjem lahko dijaki bistveno zmanjšajo svojo ranljivost ter postanejo varnejši in samozavestnejši uporabniki digitalnega okolja.

7 POVZETEK

Način, kako mladi uporabljajo internet in se soočajo s spletnimi tveganji, ni zgolj tehnično vprašanje, temveč odraža širše družbene vzorce, digitalno kulturo ter vpliv izobraževanja na oblikovanje odgovornega vedenja. Raziskovalna naloga proučuje stopnjo poznavanja osnov kibernetske varnosti med dijaki elektro-računalniške šole ter njihove digitalne navade in vedenjske vzorce pri uporabi interneta.

S pomočjo anonimne ankete sem zbral in analiziral podatke o znanju, ravnanju in odnosu dijakov do kibernetske varnosti. Raziskava je zajemala področja ustvarjanja in shranjevanja gesel, uporabo dvofaktorske avtentikacije, prepoznavanje varnih spletnih povezav, odzivanje na phishing napade ter varovanje osebnih podatkov. Rezultati so pokazali, da dijaki svoje znanje pogosto ocenjujejo kot razmeroma dobro, vendar praktični primeri razkrivajo pomanjkljivosti pri prepoznavanju spletnih prevar in dosledni uporabi varnostnih ukrepov.

Raziskava vključuje tudi širši družbeni vidik, saj analizira vpliv digitalne kulture mladih, socialnega okolja in izobraževalnega programa na oblikovanje varnega ali tveganega vedenja na spletu. Ugotovitve kažejo, da imajo pomembno vlogo tako šola kot družina ter vrstniki, pri čemer se kot ključni dejavnik izkaže tudi izobraževalno okolje.

Namen naloge je ugotoviti, kako stopnja ozaveščenosti in družbeni dejavniki vplivajo na spletno vedenje dijakov ter kako lahko ciljno usmerjeno ozaveščanje prispeva k bolj odgovorni in varni uporabi interneta. Naloga tako združuje tehnične in družbene vidike kibernetske varnosti ter poudarja potrebo po celostnem pristopu k razumevanju in zmanjševanju spletnih tveganj med mladimi.

8 SUMMARY

The way young people use the internet and confront online risks is not merely a technical issue, but also reflects broader social patterns, digital culture, and the influence of education on the development of responsible behavior. This research project examines the level of basic cybersecurity knowledge among students of a technical secondary school specializing in electrical engineering and computer science, as well as their digital habits and behavioral patterns in internet use.

Through an anonymous survey, data were collected and analyzed regarding students' knowledge, behavior, and attitudes toward cybersecurity. The research covered areas such as password creation and storage practices, the use of two-factor authentication, recognition of secure website connections, responses to phishing attacks, and the protection of personal data. The results show that students often assess their knowledge as relatively good; however, practical scenarios reveal deficiencies in recognizing online scams and consistently applying security measures.

The study also incorporates a broader social perspective by analyzing the influence of youth digital culture, social environment, and educational programs on the formation of safe or risky online behavior. The findings indicate that school, family, and peers all play an important role, with the educational environment emerging as a particularly significant factor.

The aim of the research is to determine how awareness levels and social factors influence students' online behavior and how targeted awareness-raising initiatives can contribute to more responsible and secure internet use. The project combines technical and social aspects of cybersecurity and highlights the need for a comprehensive approach to understanding and reducing online risks among young people.

9 LITERATURA IN VIRI

1. Arnes. (n.d.). Sodelovanje v projektu Center za varnejši internet – Safe.si. https://safe.si/center-za-varnejsi-internet/o-centru (pridobljeno 13. 1. 2026).
2. Bandura, A. (1971). Social Learning Theory. Stanford University. General Learning Press, New York, USA.
3. Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy (pp. 553–567). IEEE. https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf (pridobljeno 9. 1. 2026).
4. Črnak Meglič, A., & Kobal Tomc, B. (2017). Položaj otrok v Sloveniji danes: situacijska analiza. Inštitut RS za socialno varstvo. Ljubljana.
5. Finderšek, N. (2024). Varovanje osebnih podatkov v šolstvu. Diplomsko delo. Univerza v Ljubljani, Fakulteta za upravo. Ljubljana.
6. FIDO Alliance. (2020). FIDO2: Passwordless, phishing-resistant authentication standards. https://fidoalliance.org/fido2 (pridobljeno 9. 1. 2026).
7. Klemenčič, M. (2021). Digitalna pismenost mladih in varovanje osebnih podatkov. Pedagoški inštitut. Ljubljana.
8. Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet use. Journal of Broadcasting & Electronic Media. https://www.tandfonline.com/doi/abs/10.1080/08838150802437396 (pridobljeno 13. 1. 2026).
9. Safe.si. (2020). Priporočila za šole in učitelje pri izobraževanju na daljavo – varnostni vidik. Center za varnejši internet. https://safe.si/ucitelji/priporocila-za-sole-in-ucitelje-pri-izobrazevanju-na-daljavo-varnostni-vidik
10. Safe.si. (n.d.). Družbena omrežja in varnost. Center za varnejši internet. https://safe.si (pridobljeno 6. 2. 2026).
11. Safe.si. (n.d.). Izobraževanja za strokovne delavce šol. Center za varnejši internet. https://safe.si/delavnice-in-predavanja/izobrazevanja-za-strokovne-delavce-sol (pridobljeno 6. 2. 2026).
12. Safe.si. (n.d.). Mladi. Center za varnejši internet. https://safe.si/mladi

13. Safe.si. (n.d.). Učitelji. Center za varnejši internet. https://safe.si/ucitelji (pridobljeno 6. 2. 2026).
14. Safe.si. (n.d.). Varna in odgovorna raba interneta v učilnici. Center za varnejši internet. https://safe.si/dopolnilna/varna-in-odgovorna-raba-interneta-ucilnici (pridobljeno 6. 2. 2026).
15. Shweta, Main. K. (2024, May 29). What is smishing? Definition, examples & protection. Forbes Advisor. https://www.forbes.com/advisor/in/business/what-is-smishing/(pridobljeno 9. 1. 2026).
16. Suša, M. (2009). Socialni inžiniring na internetu. Diplomsko delo. Univerza v Ljubljani, Fakulteta za družbene vede. Ljubljana.
17. Uršič, J. (2022). Kibernetska varnost v zdravstvu. Diplomsko delo. Univerza v Ljubljani, Fakulteta za elektrotehniko, računalništvo in informatiko. Ljubljana.
18. Wisteria, A., Vehovar, V., Petek, A., Praček, A., & Brečko, B. (2025). Varna raba interneta in starši 2024. Analiza anketne raziskave, 1KA panel. Center za družboslovno informatiko, Fakulteta za družbene vede, Univerza v Ljubljani. Ljubljana.

.

ZAHVALA

Iskreno se zahvaljujem svojemu mentorju Romanu Herlahu za strokovno vodenje, usmerjanje in podporo pri nastajanju raziskovalne naloge.

Zahvaljujem se tudi somentorju Simonu Muhi za pomoč in konstruktivne predloge.

Posebna zahvala gre Nataši Meh Peer za skrbno lektoriranje besedila ter Vlasti Leban za lektoriranje angleškega povzetka.

Vsem učencem, ki so izpolnili anketo ter učiteljem, ki so dovolili, da sem z izvajanjem ankete motil pouk, se prav tako iskreno zahvaljujem.

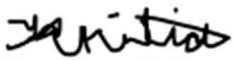
PRILOGE

IZJAVA

Izjavljamo, da smo pri pripravi raziskovalne naloge upoštevali etična načela in smernice v skladu z veljavnimi pravnimi akti raziskovalnega področja.

Podpisani:

Avtor: Kristian Muha



Mentor: Roman Herlah

1. Spol:

- Moški
- Ženska

2. Kateri izobraževalni program obiskujete?

- Tehnik računalništva
- Tehnik mehatronike
- Elektrotehnik
- Elektrikar

Kateri letnik obiskujete:

- 1.letnik
- 2.letnik
- 3.letnik
- 4.letnik

4. Kako bi opisal/a kraj, kjer živiš?

- Mesto (živim v mestnem središču ali blokovskem naselju)
- Predmestje (okolica mesta, hiše blizu mesta)
- Vas / Podeželje (manjši kraj, kmetija)

5. Kako ustvarjate svoja gesla za spletne račune?

- Za vse račune uporabljam enako ali zelo podobno geslo.
- Imam nekaj različnih gesel, ki jih menjavam.
- Za vsak račun uporabim unikatno in zapleteno geslo.

6. Kje hranite svoja gesla?

- Zapomnim si jih (v glavi).

- Zapisana imam na listu ali v zvezku.
- Zapisana imam v telefonu/računalniku (beležka, Word, sporočila).
- Shranjena so v brskalniku (Google Chrome, Edge ...).
- Uporabljam namenski upravljalnik gesel (Password Manager - npr. Bitwarden, LastPass).

7. Ali uporabljate dvofaktorsko avtentikacijo (2FA), kjer je to mogoče (npr. potrditev s SMS ali aplikacijo)?

- Ne, ker se mi zdi prezamudno.
- Ne vem, kje se to vklopi.
- Da, ampak samo za najpomembnejše račune (npr. banka, email).
- Da, uporabljam povsod, kjer je omogočeno.

8. Katera od spodnjih povezav je NAJVARNEJŠA za vnos podatkov?

- http://moja-banka.si
- https://moja-banka.si
- www.moja-banka.si.login-secure.com
- Ne vem.

9. Zakaj je klikanje na neznane povezave v e-pošti ali SMS-ih nevarno? *(Izberite najbolj točen odgovor)*

- Ker lahko sprožijo prenos zlonamerne programske opreme ali vodijo na lažno (phishing) stran.
- Ker lahko pošiljatelj vidi mojo IP številko in takoj ugotovi moje geslo.
- Ker s klikom pošiljatelju avtomatsko nakažem denar.
- Ne vem.

10. SCENARIJ 1 (Banka): Prejmete SMS: "Zaznan nepooblaščen dostop. Potrdite identiteto na www.nlb-varnost.com/prijava". Kaj storite?

- Kliknem povezavo in vpišem podatke, da preprečim blokado računa.
- Povezavo odprem, da vidim, kako izgleda stran, podatkov pa ne vpišem.

- Sporočilo ignoriram, povezave ne klikam. Stanje preverim izključno preko uradne aplikacije ali spletne banke.
- Odgovorim na SMS in vprašam, če je to res.

11. SCENARIJ 2 (FURS): Prejmete e-pošto s priponko "Obvestilo_FURS_Dolg.zip". Kaj storite?

- Odprem datoteko, saj so ZIP datoteke stisnjene in zato varne.
- Datoteke ne odpiram. Državne ustanove običajno ne pošiljajo ZIP priponk in terjatev po e-pošti.
- Datoteko shranim na disk in jo preverim kasneje.
- Ne vem.

12. SCENARIJ 3 (Prijatelj): Prijatelj vam na Messengerju pošlje: "O moj bog, poglej ta video, ti si na njem! [povezava]". Kaj storite?

- Takoj kliknem, ker me zanima.
- Kliknem, ker zaupam prijatelju.
- Ne kliknem. Prijatelja po drugem kanalu (npr. SMS, v živo) vprašam, če je to res poslal on, saj gre verjetno za virus.

13. Kje ste dobili NAJVEČ informacij o varni rabi interneta? *(Izberite en odgovor)*

- V šoli (pri pouku, krožkih).
- Od staršev/družine.
- Samostojno na spletu (YouTube, članki, forumi).
- Od vrstnikov/prijateljev.
- O varnosti ne vem skoraj nič.

14. Ocenite strinjanje s spodnjimi trditvami (1 - Sploh se ne strinjam, 5 - Popolnoma se strinjam):

Trditev	1	2	3	4	5
Moji starši se zanimajo za mojo varnost na spletu.	O	O	O	O	O

S prijatelji se pogosto pogovarjamo o varnosti na spletu.	O	O	O	O	O
V moji družbi velja prepričanje, da se nam na spletu ne more nič zgoditi.	O	O	O	O	O
Če bi postal/a žrtev prevare, bi to povedal/a staršem ali učiteljem.	O	O	O	O	O
Šola mi je dala dovolj praktičnega znanja za zaščito na spletu.	O	O	O	O	O
Deljenje fotografij, videoposnetkov ali osebnih informacij na družbenih omrežjih ne vpliva na varnost na internetu.	O	O	O	O	O
Pri uporabi interneta se počutim popolnoma varno in suvereno.	O	O	O	O	O
Povsem zaupam spletni vsebini, ki jo delijo prijatelji ali znane osebe.	O	O	O	O	O
Z preventivnim lastnim vedenjem se bistveno zmanjšuje tveganje za varnostne incidente v digitalnem okolju.	O	O	O	O	O
Vsaj 1-krat mesečno se udeležim šolskih ali zunanjih delavnic o varni rabi interneta.	O	O	O	O	O
Pripravljen/a bi bil/a žrtvovati nekaj udobja (npr. daljša prijava) za večjo varnost.	O	O	O	O	O

15. Kako bi na lestvici od 1 do 5 ocenili svoje dejansko znanje kibernetske varnosti?

1 (Zelo slabo) - 5 (Odlično)

16. Ali menite, da so starejši bolj ali manj varni na spletu kot mladi?

- Bolj varni, ker tehnologijo bolje poznamo.
- Manj varni, ker smo bolj brezskrbni in več časa preživimo na spletu.
- Enako varni.

17. Ali ste že kdaj dejansko izgubili dostop do računa, denar ali podatke zaradi spletne prevare?

- Da

- Ne
- Nisem prepričan/a