

**Šolski center Celje**  
**Srednja šola za kemijo, elektrotehniko in računalništvo**

# **Varnost na spletu**

## **Raziskovalna naloga**

### **Avtorici:**

Marina Cokan, R-4.a

Sanja Gregorič, R-4.a

### **Mentor:**

dipl.inž. Boštjan Lubej

**Mestna občina Celje, Mladi za Celje**

Celje, marec 2019

## **Zahvala**

Zahvaljujeva se najinemu mentorju profesorju Boštjanu Lubeju, ki naju je pri raziskovanju in pisanju raziskovalne naloge spodbujal, nama dajal nasvete, naju usmerjal.

Zahvaljujeva se tudi šolarjem Osnovne šole Vojnik, ki so z reševanjem ankete pomagali pri raziskavi ter uslužbencem Osnovne šole Vojnik, ki so pomagali pri izvedbi ankete.

## **Povzetek**

*Internet je dandanes zelo pomemben dejavnik v vsakodnevnem življenju ljudi. Uporabljamo ga za komuniciranje, izobraževanje, iskanje spletnih informacij, nekateri za igranje spletnih igrice, prenašanje multimedije.*

*V raziskovalni nalogi sva se ukvarjali s preučevanjem stanja na področju varne uporabe interneta. Najprej si ogledamo nekatere nevarnosti spleta in kako se pred njimi zaščitimo ter njihova tveganja. Sledi poglavje o nevarnosti umetne inteligence. Nadaljevali sva s pregledom rezultatov in ugotovitev raziskave, ki je potekala med učenci OŠ Vojnik. Rezultati kažejo, da se je večina že pogovarjala o varnosti na spletu s starši ali pa so to omenili v šoli. Nekateri posamezniki se spuščajo v veliko nevarnost z objavljanjem osebnih podatkov na spletu in z odpiranjem sporočil neznanih pošiljateljev. Večina učencev bi se v primeru zlorabe obrnila po pomoč k družinskim članom, učiteljem ali pa bi zlorabo prijavili policiji. Pohvalno pa je da ima večina na socialnih omrežjih zaseben ali zaklenjen profil.*

*Najina glavna predloga sta, da bi v šoli potekalo osveščanje o varni rabi interneta in da bi učenci varno uporabljali splet.*

## Vsebina

|        |                                              |    |
|--------|----------------------------------------------|----|
| 1.     | Uvod .....                                   | 1  |
| 2.     | Nevarnosti na spletu in načini zaščite ..... | 2  |
| 2.1.   | Kraja identitete.....                        | 2  |
| 2.2.   | Nadlegovanje in sovražni govor .....         | 3  |
| 2.3.   | Phishing ali ribarjenje.....                 | 4  |
| 2.4.   | Nezakonite in neprimerne vsebine .....       | 4  |
| 2.4.1. | Zavajajoče vsebine .....                     | 4  |
| 2.4.2. | Spletni grooming .....                       | 5  |
| 2.4.3. | Spletno piratstvo .....                      | 5  |
| 3.     | Umetna inteligenca .....                     | 6  |
| 4.     | Socialna omrežja .....                       | 7  |
| 4.1.   | Snapchat.....                                | 7  |
| 4.2.   | Twitter .....                                | 8  |
| 4.3.   | Facebook .....                               | 9  |
| 4.4.   | Instagram .....                              | 9  |
| 5.     | Starši in internet.....                      | 10 |
| 5.1.   | Nasveti za starše.....                       | 11 |
| 6.     | Anketa .....                                 | 13 |
| 7.     | Razprava .....                               | 20 |
| 8.     | Zaključek.....                               | 21 |
| 9.     | Viri in literatura .....                     | 22 |
| 10.    | Priloge .....                                | 23 |

## Kazalo slik

|                                                            |    |
|------------------------------------------------------------|----|
| Slika 1: Zavednost do resničnih podatkov na spletu .....   | 13 |
| Slika 2: Neznani pošiljatelji.....                         | 14 |
| Slika 3: Naprave za dostop do interneta .....              | 14 |
| Slika 4: Za kaj uporabljam internet .....                  | 15 |
| Slika 5: Pogovor s starši o varnosti na spletu .....       | 15 |
| Slika 6: Pozorni na varno rabo interneta.....              | 16 |
| Slika 7: Pomoč, v primeru spletne zlorabe .....            | 16 |
| Slika 8: Vdiranje v profil .....                           | 17 |
| Slika 9: Moč gesel .....                                   | 17 |
| Slika 10: Laganje na spletnih omrežjih.....                | 18 |
| Slika 11: Objavljanje fotografij na spletnih omrežjih..... | 18 |
| Slika 12: Zaseben ali javen profil .....                   | 19 |

### **Ključne besede:**

- **Spletna varnost** – samozaščita pred spletnimi nevarnostmi, zaščita svojih osebnih podatkov
- **Umetna inteligenca (UI)** - posnemanje naravne oz. človeške inteligence, samostojnega učenja s pomočjo strojnega učenja, algoritmov in računalniških sistemov. Simulacija inteligentnega obnašanja z računalniki
- **Nevarnosti interneta** – tveganja pri uporabi interneta. Okužba računalnika z virusi, kraja osebnih podatkov ali identitete, nezaželena ali nelegalne vsebine, spletni napadi, zasvojenost z internetom...
- **Škodljive spletne vsebine** - na splošno lahko rečemo, da so škodljive tiste vsebine, ki so bile ustvarjene z namenom, da žalijo posamezno osebo ali večjo skupino ljudi (spletne strani, ki spodbujajo nasilje, rasizem ...).
- **Kibernetska varnost** - (cyber security) zaščita računalnikov, računalniške opreme in računalniških omrežij; spletna varnost

## 1. Uvod

*»Vsak dan se srečujemo z različnimi metodami komunikacije, v zadnjem času pa se najbolj uveljavlja sporazumevanje preko spleta. Na spletu je mogoče iskati različne informacije, pošiljati in sprejemati elektronsko pošto, pisati spletne dnevnike, igrati igrice, izmenjavati datoteke z drugimi uporabniki, prenašati glasbo, mogoče je tudi izmenjavati mnenja v spletnih klepetalnicah, prek Messengerjev, v forumih in nakupovati preko spleta« (Safe.si, 2019).*

Naloge sva se lotili, ker kot tehniki računalništva pri pouku dajemo ogromen poudarek na varno rabo interneta oz. računalnikov. Zanima naju če so s spletno varnostjo seznanjeni tudi osnovnošolski otroci.

Zanima naju tudi kako na spletno varnost vpliva umetna inteligenca ter kaj so njene prednosti in slabosti.

## 2. Nevarnosti na spletu in načini zaščite

### 2.1. Kraja identitete

Oseba nam ukrade identiteto, ko pridobi naše podatke in se začne predstavljati v našem imenu, zavede naše prijatelje, družinske člane ali sodelavce, si pridobi dostop do naših osebnih informacij, pogovorov, slik. Večina žrtev kraje identitete na spletu izgubi ugled, čast, kraja določenih osebnih podatkov je včasih nepopravljiva.

Kraja identitete predstavlja hud poseg v varstvo osebnih podatkov.

Identiteto nam lahko nekdo ukrade tako, da se prijavi v naš profil in se začne predstavljati v našem imenu. Lahko nas prisili, da sami razkrijemo svoje uporabniško ime in geslo. Naše uporabniške podatke lahko pridobi s posebnimi programi ali virusi. Lahko nam preprosto ukrade slike, ustvari profil z našim imenom in našimi podatki in se začne predstavljati v našem imenu.

Storilcu grozi kazen do treh let zapora, če je oseba finančno oškodovana, pa lahko zahteva odškodnino.

#### **Kako se zaščitimo?**

- Krajo identitete lahko največkrat prijavimo lastnikom spletnih strani.
- Zaščitimo svoje osebne podatke.
- Pogosto spreminjajmo gesla in dodatno zaščitimo svoje račune.
- Kopirajmo osebne dokumente.
- Krajo identitete takoj prijavimo.



## 2.2. Nadlegovanje in sovražni govor

Spletno nadlegovanje obstaja v različnih oblikah, ni pa nujno da ga vedno prepoznamo; včasih celo ignoriramo. Spletno nadlegovanje lahko doseže vse, največkrat pa gre za primer vrstniškega nasilja. Povzročitelji spletnega nasilja so v enaki meri moški in ženske za razliko od tradicionalnega nasilja in nadlegovanja. Povzročitelji lahko svojo identiteto zakrijejo z lažnim imenom, zato se pri zavajanju ali sovražnem govoru ne zadržujejo.

Med spletno nadlegovanje upoštevamo:

- ustrahovanje preko zasebnih sporočil, javnih komentarjev ali klicev;
- obrekovanje na javnih profilih, v komentarjih, na blogih;
- deljenje zasebnih slik, pogovorov, posnetkov;
- pošiljanje nasilnih ali vulgarnih fotografij ali posnetkov;
- objavljanje predelanih oz. preurejenih fotografij, ki osebo ali več oseb žalijo;
- pošiljanje golih ali intimnih fotografij ali posnetkov, prav tako pošiljanje sporočil s spolno vsebino;
- izsiljevanje na kakršen koli način.

Kako se zaščitimo?

- Svojih osebnih podatkov, kot na primer telefonske številke, naslova, gesel, bančnih podatkov itd. ne posredujemo preko spleta, kar pomeni, da jih ne objavljamo, jih ne pošiljamo preko privatnih sporočil, se o njih ne pogovarjamo preko video-klicev, se ne vpisujemo na spletne strani, ki te podatke o nas zahtevajo.
- Ne odpiramo sporočil neznanih pošiljateljev in na njih ne odgovarjamo.
- Ne odgovarjamo na sporočila, ki vsebujejo sovražni govor.
- Blokiram pošiljatelja nezaželenih sporočil, lahko ga tudi prijavimo lastnikom spletne strani.
- Ne pišemo jeznih sporočil, ki jih bomo kasneje obžalovali, raje počakamo in kasneje pravilno odreagiramo.

### 2.3. Phishing ali ribarjenje

Storilec nas poskuša zvabiti, da mu posredujemo svoje uporabniške ali bančne podatke. Ti podatki mu omogočijo dostop do naših spletnih in bančnih storitev.

Kako se zavarujemo?

- Ne odgovarjamo na pisma, ki zahtevajo naše osebne in finančne podatke.
- Pred prijavo na spletne strani, ki upravljajo z našimi financami, spletni naslov vedno vpišemo neposredno v naslovno vrstico.
- Finančnih podatkov ne posredujemo preko spleta.

### 2.4. Nezakonite in neprimerne vsebine

Na splošno lahko rečemo, da so škodljive tiste vsebine, ki prizadenejo čustva določenih ljudi ali določenih skupin ljudi. Podrobneje sva se osredotočili na zavajajoče vsebine, spletni grooming in spletno piratstvo.

#### 2.4.1. Zavajajoče vsebine

To so lažne novice, najpogosteje deljene na socialnih omrežjih. Večina ljudi uporablja socialna omrežja za pregled novic, ne zavedajo pa se, da so na teh straneh objavljene tudi neresnice. Najpogosteje so lažne novice vir zaslužka s prikazovanjem oglasov. Spletne strani se trudijo sproti brisati takšne novice, vendar številne raziskave kažejo da je časovni rok za odstranitev nezakonite vsebine 24 ur, ključno pa je, da se vsebina odstrani že eno uro po objavi, saj se s tem zmanjša škoda lastnika avtorskih pravic.

Kako se zaščitimo?

- Preverimo vire in se prepričamo, da so zanesljivi.
- Če nas tema zanima, se poglobimo, preberemo komentarje.
- Ne verjemimo vsemu, kar preberemo, smo kritični bralci, raziskujemo.
- Ne oblikujemo mnenj na podlagi čustev, saj je namen takih novic, da v nas vzbudijo ekstremna čustva.

#### 2.4.2. Spletni grooming

Navezovanje stika z mladoletnimi osebami z namenom spolne zlorabe imenujemo grooming. Storilec največkrat z mladoletno osebo naveže stik preko socialnih omrežij, začne zasebni pogovor in si pridobi njeno zaupanje, storilec otroku zagotovi, da je njun stik nekaj posebnega, čez čas pa pogovor naveže na spolnost. Spletni grooming lahko vodi v fizične zlorabe otroka.

Tveganja:

- depresija,
- nezaupanje,
- nizka samopodoba,
- osamljenost

#### 2.4.3. Spletno piratstvo

Nepooblaščenno kopiranje in distribuiranje programske opreme, ki je zaščiteno z avtorskimi pravicami, je nezakonito. S tem, ko kupimo programsko opremo, pridobimo tudi licenco za njeno uporabo. V licenci so navedena pravila za uporabo programa, prav tako je zapisano, kolikokrat lahko opremo namestimo. Če naredimo več kopij, kot je dovoljeno, je to spletno piratstvo. Vse bolj popularno je piratstvo glasbe, filmov, iger ...

Tveganja:

- Okužbe: na računalnik lahko prenesemo virus ali nelegalne, neprimerne vsebine.
- Kakovost: nezanesljivo delovanje, slaba kvaliteta.

### 3. Umetna inteligenca

Kamor koli gremo na svetovnem spletu, umetna inteligenca (UI) spremlja in beleži vsak naš klik. S to tehnologijo primerno podprta spletna stran že ob prvem obisku o nas ve ogromno, na primer kje živimo, ali imamo otroke, kakšno je naše finančno stanje, kateri so naši hobije.

Kibernetska varnost je glavna skrb digitalnega sveta in veliko ljudi je še vedno negotovih glede vpliva umetne inteligence. Vse več državnih organov in podjetij že uporablja umetno inteligenco za zaščito podatkov in preprečevanje kibernetskih prestopkov. Z ustrezno programsko opremo umetna inteligenca zdaj upravlja z večjo količino pomembnejših podatkov, ki jih proizvajajo sistemi za kibernetsko varnost brez pomoči ljudi.

Algoritmi s samostojnim učenjem ugotavljajo odstopanje od običajnih vzorcev. Umetna inteligenca najprej preveri, kakšno je normalo obnašanje sistema, nato primerja odstopanja in sistem pregleda za napade. Tako zaznavanje težav štejemo med nenadzorovane učne algoritme.

Drugi pristop je uporaba nadzorovanih algoritmov, za katere je bila umetna inteligenca usposobljena. Primer takšnega nadzora je odkrivanje napredne zlonamerne programske opreme.

Ker se kompleksnost kibernetskih napadov povečuje, UI zagotavlja takojšnje vpogled, ki se pomagajo boriti skozi tisoč dnevnih opozoril, kar drastično zmanjša odzivni čas na napade (60-krat hitreje).

Umetna inteligenca se uči tako, da obdela milijarde podatkov iz različnih virov kot so novice, objave na socialnih omrežjih in blogi. S strojnim učenjem izboljšuje razumevanje kibernetskih napadov, groženj in tveganj.

Hakerji pa seveda lahko uporabijo umetno inteligenco kot orožje za napad.

Ker umetna inteligenca dodaja vrednost tudi varnostnim sektorjem družb in posameznikov, širi več moči tudi v napačne roke. Da bi UI v bližnji prihodnosti dali več pooblastil v varnostne namene, moramo biti prepričani, da ostanejo samo pri pravih ljudeh.

## 4. Socialna omrežja

### 4.1. Snapchat

Snapchat je ena izmed zelo priljubljenih aplikacij, ki jo uporabljajo najstniki. Omogoča pošiljanje fotografij in videoposnetkov, prav tako pa lahko klepetamo s prijatelji.

Aplikacijo lahko brezplačno prenesemo in brezplačno pošiljamo fotografije in videoposnetke. Snapchat se od drugih aplikacij razlikuje po tem, da sporočila in slike oziroma videoposnetki po določenem času izginejo. Imamo možnost, da določimo kako dolgo bo slika vidna (od 0 do 10 sekund). Po izteku časa slika izgine s telefona. Aplikacija omogoča tudi klepet, pri katerem sporočila prav tako izginejo ko oba uporabnika zapustita okno za klepet.

Nobena aplikacija pa ni popolna, tudi Snapchat ne. Obstajajo tveganja kot je na primer občutek, da je Snapchat varen. Ker slike, videoposnetki in klepet izginejo, uporabniki mislijo, da lahko preko Snapchata pošiljajo karkoli, kar pa čisto ne drži. Vsak pametni telefon ima opcijo narediti sliko zaslona, zato si lahko prejemnik prav vsako sliko, ki jo prejme, shrani. Snapchat je sicer uvedel možnost, ki pošlje obvestilo pošiljatelju, da je prejemnik naredil sliko zaslona, ampak se je tudi temu mogoče izogniti tako, da posname sliko z drugim telefonom.

Za varno uporabo Snapchata je priporočeno, da pošiljate fotografije in videoposnetke samo svojim prijateljem, čeprav ima Snapchat na voljo možnost pošiljanja komurkoli. Prav tako je zaželeno, da ogled vaše zgodbe (angl. story) dovolite samo vašim prijateljem. Najbolj pomembno pa je, da ne pošiljamo nikakršnih fotografij in videoposnetkov, ki so na kakršne koli način sporni.

## 4.2. Twitter

Twitter je družabno omrežje, ki temelji na t.i. mikrobloganju, kjer ljudje izražajo svoja mnenja, čustva, občutke ter komunicirajo drug z drugim preko tako imenovanih tvitov (angl. tweet). Tviti so omejeni na 280 znakov, kar jih naredi enostavne za branje. Vaš tvit lahko vidijo vsi vaši sledilci (angl. follower). Do Twitterja se, da dostopati preko računalnika ali preko aplikacije Twitter.

Twitter je zelo enostaven za uporabo. Najprej si ustvarite brezplačen profil in že lahko objavite svoj prvi tvit. Vsi vaši sledilci bodo vaš tvit videli in ga bodo lahko všečkali (angl. like) ali delili (angl. retweet), kar pomeni, da je vaš tweet objavil nekdo drug, vaše uporabniško ime pa je še vseeno vidno pod njegovim.

V prvi vrsti je Twitter družabno omrežje, namenjeno komuniciranju med uporabniki. Med drugimi je tudi nekakšen amaterski novičarski portal, saj ljudje z vsega sveta pišejo, kaj se jim trenutno dogaja oziroma kaj se dogaja na njihovem koncu sveta. Priljubljen je tudi kot oglaševalsko orodje, saj ima ogromno uporabnikov, ki samo listajo po njem. Izjemno priljubljen je tudi med zvezdniki in politiki, da izražajo svoja mnenja in stališča.

Kot vsa družbena omrežja a tudi Twitter predstavlja določeno tveganje. Na prvem mestu bi bilo spletno ustrahovanje, ki je v zadnjem letu postal velik problem. Predvsem to velja, ko nas ljudje »napadejo« zaradi izražanja našega mnenja preko tvitov. Ampak namen Twitterja je prav ta, da izražamo svoje mnenje in včasih se najde tudi kakšen posameznik, ki gre z besedami predaleč. Prav tako moramo biti na Twitterju pazljivi na lažne novice (angl. fake news). Te se širijo zelo hitro, nas pa lahko tudi zelo hitro zavedejo. Še posebej moramo biti pazljivi, da teh novic ne delimo.

Twitter je javno dostopen, ima pa tudi nekaj možnosti s katerimi lahko naredimo naš račun popolnoma zaseben. To pomeni, da nam mora vsak uporabnik, ki želi videti naše tvite najprej poslati prošnjo, ki jo odobrimo ali zavrnemo.

### 4.3. Facebook

Facebook je družabno omrežje, ki ga je ustanovil Mark Zuckerberg, ko je leta 2004 študiral na Harvardu. Odkar je bil ustanovljen je postal zelo popularno družabno omrežje, ki je namenjeno ljudem vseh starosti.

Uporabnikom omogoča, da si ustvarijo brezplačen profil, ki jim potem omogoča objavljanje slik, mnenj, videoposnetkov, anket in drugih vsebin. Facebook tudi omogoča kreiranje skupin za različne stvari, kot so ljubitelji različnih nadaljevk, filmov, glasbe in drugo. Kadar se želimo povezati s kakšno osebo, ji pošljemo prošnjo za prijateljstvo, ki jo nato ta oseba odobri ali zavrne. Če oseba prošnjo sprejme, lahko z njo komuniciramo preko Facebookovega klepeta, ki se mu reče messenger, lahko všečkamo ter komentiramo njegove objave, prav tako pa ga lahko označimo (angl. tag) v različnih objavah.

Facebook ima za uporabo določeno minimalno starost 13 let. V primeru, da se mlajša oseba vseeno registrira na Facebook in se to odkrije, je Facebook odgovoren, da takoj, ko dobi obvestilo, izbriše profil te osebe. Profil na Facebooku je mogoče nastaviti na javnega, kar pomeni, da si lahko vaš profil ogleda vsak, ki ima Facebook profil, če ga nastavite profil zasebno, si lahko vaš profil ogleda samo tisti, ki vam je poslal prošnjo za prijateljstvo in ste jo vi odobrili. Facebook nevarno družbeno omrežje predvsem za najstnike, ki objavljajo preveč podatkov o sebi.

### 4.4. Instagram

Instagram je družabno omrežje, ki si ga lasti Facebook. Uporabnikom omogoča deljenje fotografij ali videoposnetkov, katerim lahko dodajo opis. Ko na Instagram objavimo sliko ali videoposnetek, je ta viden na našem profilu, ki je prav tako brezplačen.

Instagram je predvsem mobilna aplikacija, saj lahko slike objavljamo neposredno iz naše galerije slik. Do njega lahko seveda dostopamo tudi preko računalnika, ampak tam lahko samo všečkamo in komentiramo objave drugih uporabnikov.

Uporabniški profil na Instagramu prav tako kot Facebook omogoča nastavitve javnega in zasebnega računa, ki ga nastavimo v nastavitvah.

## 5. Starši in internet

Za starše je skoraj nemogoče ves čas spremljati otrokovo početje, ko je ta na računalniku oz. internetu. Pogosto so starši še vedno v službi, ko njihovi otroci pridejo domov iz šole. Poleg tega so otroci navihani in nekateri izkoristijo vsak trenutek nepozornosti njihovih staršev za hitro računalniško igro ali klepet s prijatelji. Namesto da bi spali, pozno v noč klepetajo s prijatelji, gledajo posnetke ali igrajo igre. V takšnih trenutkih pride prav programska oprema, ki omejuje možnost uporabe računalnika ali interneta. Pametno je, da otrokom zvečer vzamemo telefon in jim ga zjutraj vrnemo.

Za otroke v starosti od dveh do treh let ni priporočljivo, da imajo stik z napravami z zasloni. V tem času se začnejo intenzivno razvijati možgani, vid in globinska zaznava; zasloni ne omogočajo globinske zaznave in so zato škodljivi.

V obdobju primarne socializacije se otroci učijo od staršev s pomočjo posnemanja, kar pomeni tudi odnos staršev do računalnika in telefona.

Predšolske otroke lahko z zabavnimi učnimi programi in igrami spodbudimo k učenju. Najbolj priporočljivi so interaktivni učni programi, ki spodbujajo otroka h govoru, na primer posnemanje živali, petje pesmi, poimenovanje predmetov s pomočjo slik ali posnetkov ... Programe za učenje lahko namestimo na računalnik in se izognemo povezavi na internet, ali pa otroka spodbujamo k samostojnem iskanju vsebin in ga postopoma učimo o delovanju internetnih strani. Seznanimo ga tudi z računalniškimi komponentami.

Preden otroka seznanimo z internetom, je smiselno, da nastavimo programe za filtriranje vsebine. S spletnimi filtri otroku preprečimo dostop do prepovedanih ali nevarnih vsebin, kot so na primer spletne strani s sovražno, nasilno ali pornografsko vsebino, prepovejo pa lahko tudi dostop do klepetalnice. Ne smemo pozabiti, da spletni filtri ne nudijo popolne zaščite.

Šolarji začnejo uporabljati računalnik in internet za pomoč pri pouku. Otroku pomagajmo pri iskanju informacij za domače naloge in šolske projekte. Pomagajmo mu pri ustvarjanju lastnega elektronskega naslova. Zdaj je čas za družinski dogovor o rabi interneta, nastavimo lahko tudi časovne omejitve, pri katerih se računalnik sam ugasne in zakleni.



Mladostnikom internet predstavlja komunikacijsko središče, kjer si lahko s prijatelji, pa tudi z neznanci, izmenjajo informacije, zato jim moramo razložiti, da smo pripravljeni pomagati v primeru nadlegovanja ali groženj preko spleta. Po drugi strani pa ne smemo postaviti pretiranih omejitev, saj se bo mladostnik počutil prikrajšanega in se nam začeli upirati.

### 5.1. Nasveti za starše

Spletna stran [safe.si](https://safe.si/starsi/10-naj-nasvetov-za-starse) nudi zelo dobre nasvete za starše, učitelje, mlajše otroke in mladostnike, prav tako kot pomoč pri napadih ali spletnem nadlegovanju. Spodaj so navedeni koristni nasveti za starše, ki sva jih našli na spletnem naslovu <https://safe.si/starsi/10-naj-nasvetov-za-starse>.

1. Zaščitite svoj računalnik in mobilno napravo s požarnim zidom in protivirusnim programom, ki ga redno posodablajte. Če tega ne zmorete sami, poiščite pomoč.
2. Računalnik postavite v dnevni prostor in skupaj s svojimi otroki raziskujte internet. Pustite jim, da vas tudi oni naučijo česa o novih tehnologijah.
3. Določite družinska pravila, koliko prostega časa na dan ali na teden lahko otroci preživijo na internetu oz. z mobilno napravo.
4. Naj prepoved interneta ne bo način reševanja morebitnih težav. Z otroki vzpostavite dialog o tem, kaj počnejo na spletu. Otroci naj zaupajo svojim občutkom – če jim je zaradi česar koli na internetu neprijetno, naj vam o tem povedo.
5. Otroci naj na internetu ne objavljajo svojega naslova, telefonske številke, naslova elektronske pošte, šole, ki jo obiskujejo, in drugih osebnih informacij. Kjer se da, naj uporabljajo vzdevek, ki ne razkriva njihove identitete.
6. Nadlegovanje, trpinčenje preko spleta in drugih tehnologij je nedopustno. Naučite svoje otroke, da pravila lepega obnašanja veljajo tudi na spletu. Učite jih, da je razlika med tem, kaj je prav in kaj ne, na internetu enaka kot v resničnem življenju.

7. Otroke poučite, da sta posedovanje in uporaba piratskih kopij računalniških programov, filmov in glasbe nezakonita. Pojasnite jim, da je nezakonito presnemavanje rezultatov dela drugih ljudi povsem enako, kot če bi nekaj ukradli v trgovini.
8. Otroke učite, da ni nujno, da vse, kar preberejo ali vidijo na internetu, tudi drži. Spodbujajte jih, naj vas, če niso prepričani, vprašajo in preverijo še druge vire.
9. Otrokom prepovejte, da bi se brez vaše vednosti sestajali s »prijatelji« z interneta. Pojasnite jim, da internetni prijatelji morda niso to, za kar se izdajajo.
10. Zavedajte se, da noben filter za neprimerne vsebine ni 100-odstoten. Filtri so morda primerna rešitev za mlajše otroke, pri večjih pa se ni priporočljivo zanašati nanje. Otrok bo slej ko prej naletel na določene vsebine (pri prijatelju, v knjižnici) in morda je bolje, da ste takrat poleg.

## 6. Anketa

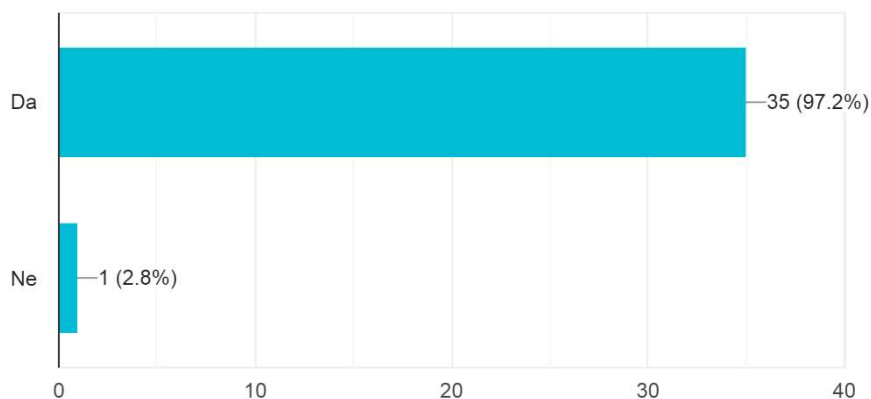
V raziskovalni nalogi sva se odločili, da bova izvedli anketo o tem, koliko o varnosti na spletu vedo osnovnošolci. Anketo sva izvedli na Osnovni Šoli Vojnik. Anketirali sva po en razred iz vsakega triletja in dobili 36 odgovorov, ki so prikazani v nadaljevanju.

Po uvodnem nagovoru in zahvali za sodelovanje sva anketirancem postavili 12 vprašanj.

Rezultate ankete sva predstavili v že narejenih grafih iz google forms.

### 1. Zavedam se, da stvari, ki jih preberem na spletu, niso vedno resnične.

36 responses

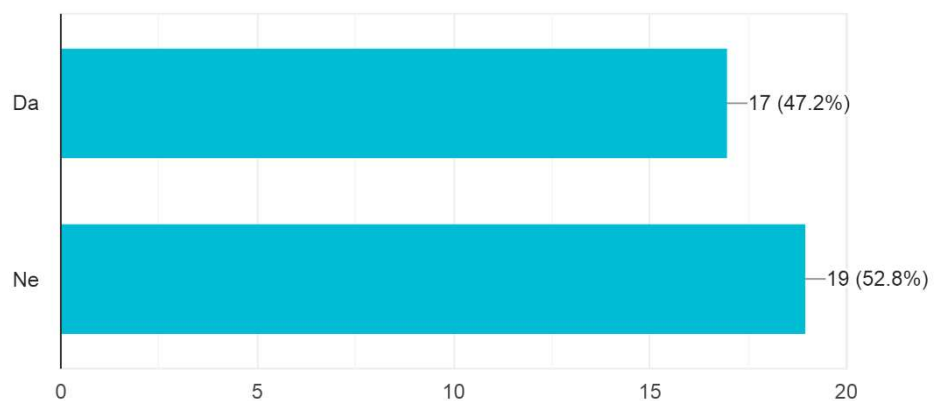


Slika 1: Zavednost do resničnih podatkov na spletu

Na trditev, ali se zavedam, da stvari, ki jih preberem na spletu, niso vedno resnične, je 97.2 % anketirancev odgovorilo z odgovorom DA, medtem ko jih je z odgovor NE odgovorilo 2.8 %.

## 2. Sporočil neznanih pošiljateljev ne odpiram.

36 responses

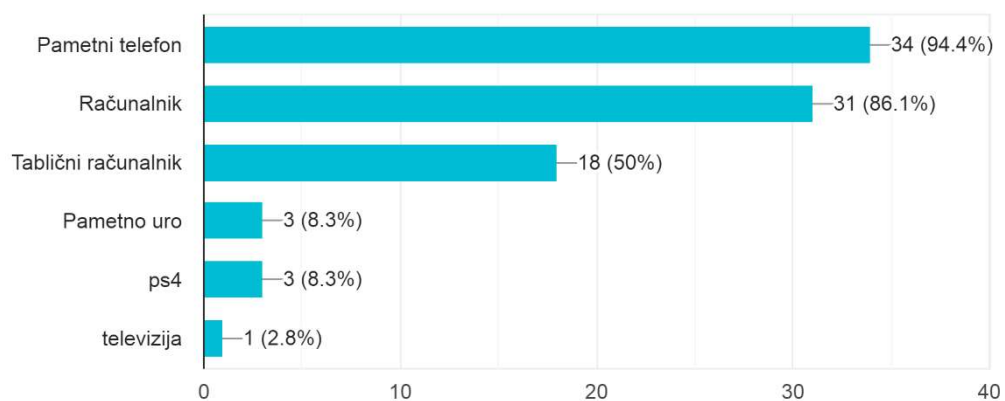


Slika 2: Neznani pošiljatelji

Na trditev, da sporočil neznanih pošiljateljev ne odpirajo, je 47.2 % anketirancev odgovorilo z odgovorom DA, medtem ko jih je z NE odgovorilo 52.8 %.

## 3. Katere naprave uporabljaš za dostop do interneta? (obkljukaj)

36 responses

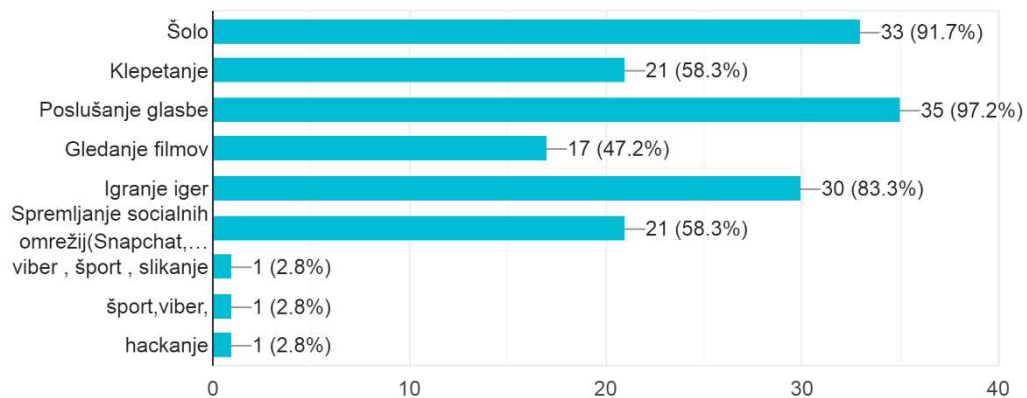


Slika 3: Naprave za dostop do interneta

Na vprašanje katere naprave uporabljaš za dostop do interneta je 94.4 % odgovorilo pametni telefon, 86.1 % računalnik, 50 % tablični računalnik, 8.3 % pametno uro in ps4 ter 2.8 % televizijo.

#### 4. Internet uporabljam za (obkljukaj):

36 responses

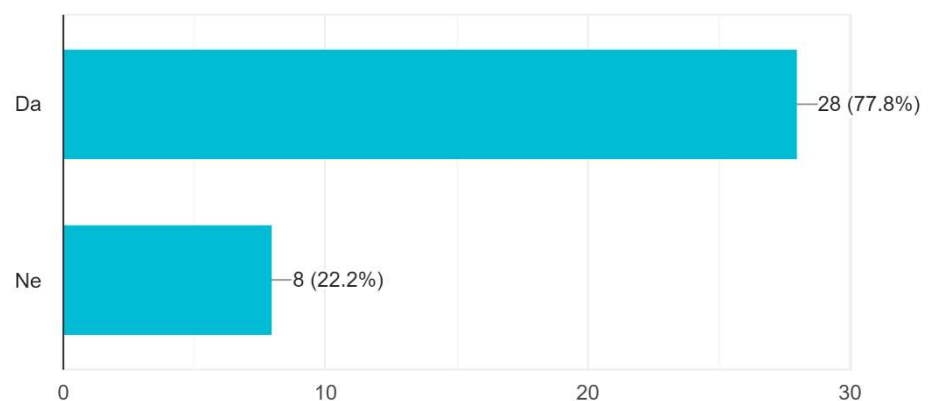


Slika 4: Za kaj uporabljam internet

pri izbiri za kaj uporabljamo internet je 91.7 % anketirancev odgovorilo za šolo, 58.3 % za klepetanje, 97.2 % za poslušanje glasbe, 47.2 % za gledanje filmov, 83.3 % za igranje iger, 58.3 % za spremljanje socialnih omrežij in 2.8 % za viber, šport, slikanje in hackanje.

#### 5. Ali si se s starši kdaj pogovarjal o varnosti na spletu?

36 responses

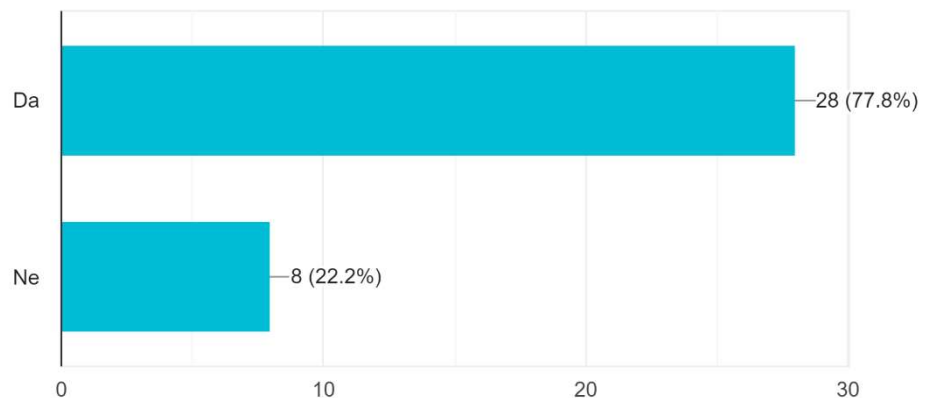


Slika 5: Pogovor s starši o varnosti na spletu

Na vprašanje, ali se s starši kdaj pogovarjal o varnosti na spletu, je 77.8 % anketirancev odgovorilo z odgovorom DA, 22.2 % pa jih je odgovorilo NE.

## 6. Ali ste pri pouku oziroma razrednih urah pozorni na varno rabo interneta?

36 responses

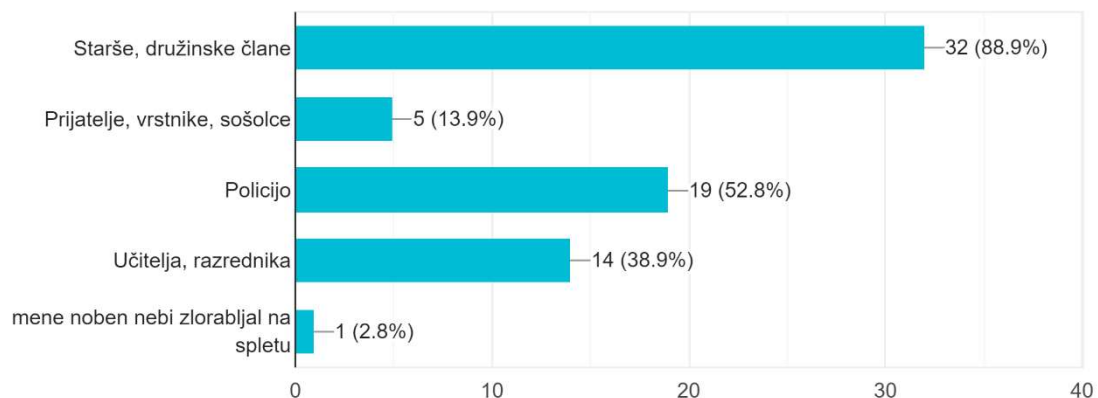


Slika 6: Pozorni na varno rabo interneta

Na vprašanje, ali ste pri pouku oziroma razrednih urah pozorni na varno rabo interneta, je 77.8 % anketirancev odgovorilo z odgovorom DA, 22.2 % pa jih je odgovorilo NE.

## 7. Koga bi v primeru spletne zlorabe prosili za pomoč?

36 responses

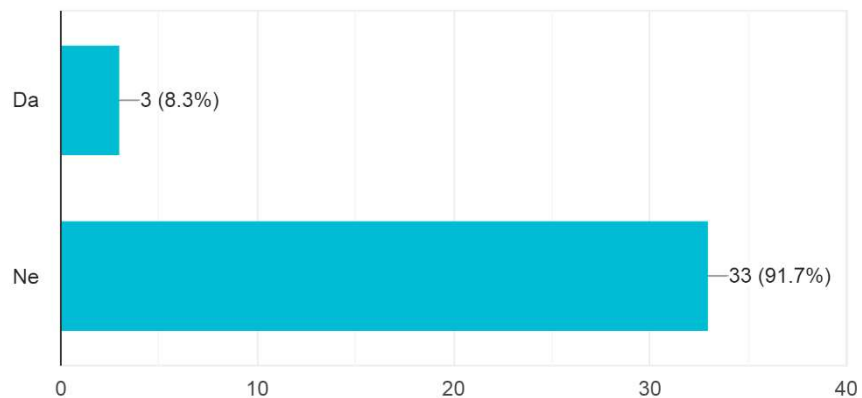


Slika 7: Pomoč, v primeru spletne zlorabe

Na vprašanje, koga bi v primeru spletne zlorabe prosili za pomoč, je 88.9 % anketirancev izbralo starše, 13.9 % prijatelje, vrstnike ali sošolce, 52.8 % policijo, 38.9% učitelja ali razrednika, 2.8% je odgovorilo, da jih nihče na spletu ne bi zlorabljal.

## 8. Ali si kdaj poskusil komu vdreti v profil?

36 responses

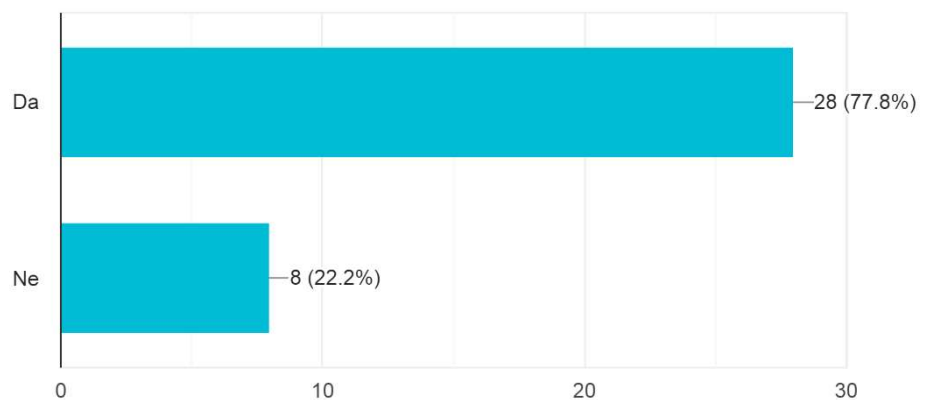


Slika 8: Vdiranje v profil

Na vprašanje, ali si kdaj poskusil komu vdreti v profil, je 8.3 % anketirancev odgovorilo z odgovorom DA, 91.7 % pa jih je to zanikalo.

## 9. Ali poskrbiš, da so tvoja gesla dovolj močna?

36 responses

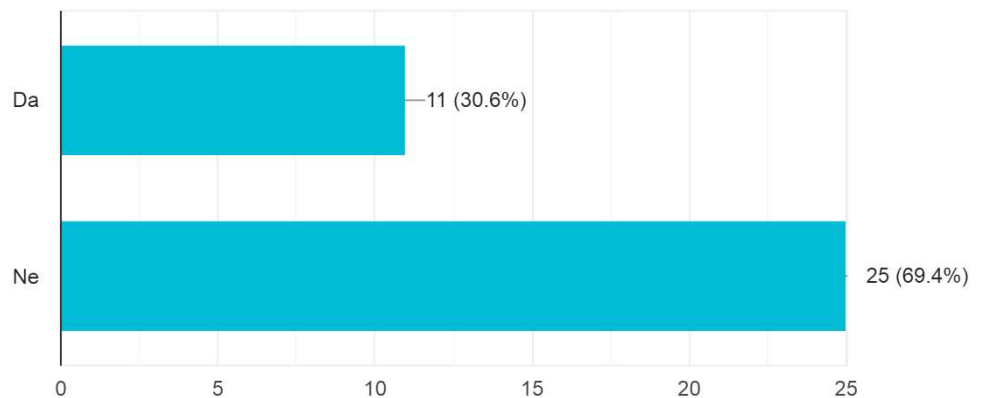


Slika 9: Moč gesel

Na vprašanje, ali poskrbiš, da so tvoja gesla dovolj močna, je 77.8 % anketirancev odgovorilo z odgovorom DA, medtem ko jih je z NE odgovorilo 22.2 %.

#### 10. Ali na socialnih omrežjih kdaj lažeš o svoji starosti/imenu/izgledu?

36 responses

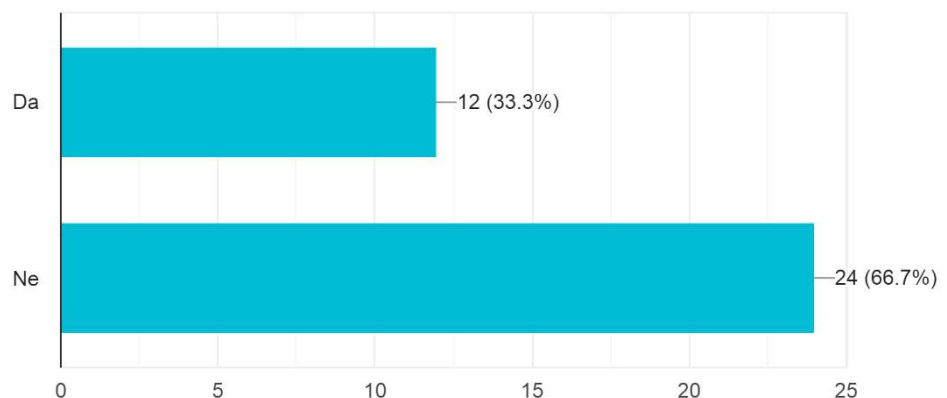


Slika 10: Laganje na spletnih omrežjih

Na vprašanje, ali na socialnih omrežjih kdaj lažeš o svoji starosti/imenu/izgledu, je 30.6% anketirancev odgovorilo z odgovorom DA, 69.4% jih je odgovorilo z NE.

#### 11. Ali na socialnih omrežjih objavljaš svoje fotografije?

36 responses



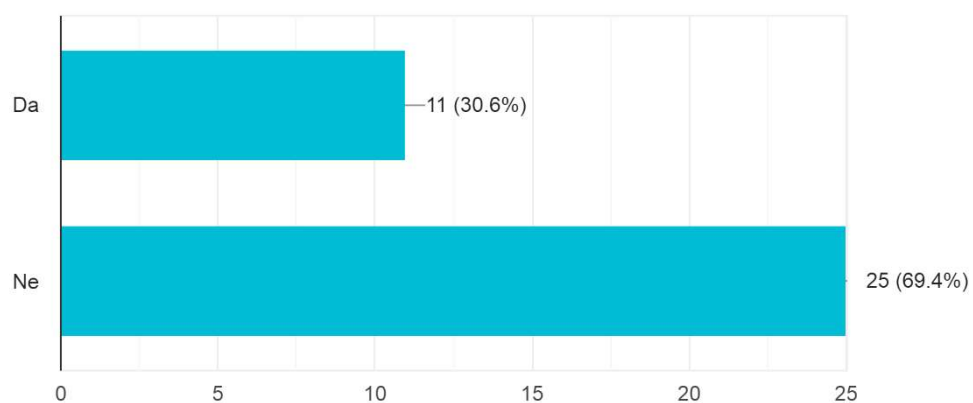
Slika 11: Objavljanje fotografij na spletnih omrežjih

Na vprašanje, ali na socialnih omrežjih objavljaš svoje fotografije, je 33.3 % anketirancev odgovorilo z odgovorom DA, z NE pa jih je odgovorilo 66.7 %.



## 12. Ali je tvoj profil javen?

36 responses



Slika 12: Zaseben ali javen profil

Na vprašanje, ali je tvoj profil javen, je 30.6 % anketirancev odgovorilo z odgovorom DA, 69.4 % pa z NE.

## 7. Razprava

Namen raziskave je bilo raziskovanje nevarnosti in načinov varnosti na spletu, izvedeti več o umetni inteligenci in socialnih omrežjih ter ugotoviti koliko mladi vedo o varnosti na spletu.

Glavni hipotezi sta bili, da ima večina mladih javen profil in da večina mladih ni dovolj izobražena o tem. Ugotovili sva, da mladi vedo veliko o varnosti na spletu, kar sva ugotovili s pomočjo ankete, ki sva jo izvedli na OŠ Vojnik. Velika večina anketirancev je odgovorila, da nimajo javnega profila zaradi česar je tudi ta hipoteza ovržena. Prav tako pa sva odkrili, da mladi vedo veliko o varnosti na spletu, kot na primer, da imajo dovolj močno geslo, da na spletu ne lažejo o svojih podatkih. Zaradi tega sva tudi ovrgli drugo hipotezo.

## 8. Zaključek

V prvem delu raziskovalne naloge sva opisali nevarnosti spleta, varnostna tveganja in načine za zaščito. V nadaljevanju sva opisali vpliv umetne inteligence na kibernetško varnost in izpostavili njene prednosti in slabosti. Zatem sva se osredotočili na specifična socialna omrežja, in sicer Facebook, Snapchat, Twitter in Instagram. Spletna omrežja so opisana, predstavljena so tveganja njihove uporabe, predstavljeni pa so tudi nasveti za njihovo varno uporabo. V tretjem delu sva s pomočjo ankete, opravljeni na OŠ Vojnik, pridobili podatke o uporabi spleta pri mladih. Ugotovili sva da se vsi učenci ne zavedajo da vse izjave na spletu niso resnične, veliko anketirancev odpira sporočila neznancev, kar je zaskrbljujoče. Večina anketirancev dostopa do spleta preko pametnih telefonov ali računalnikov. Izvedeli sva, da se je večina že pogovarjala o varnosti na spletu s starši ali pa so to omenili v šoli. v primeru zlorabe bi večina obvestila člane družine, učitelje ali pa bi direktno obvestili policijo. Ne dajejo prevelike pozornosti zaščiti, določeni se na svojih profilih lažejo o svoji starosti. Pohvalno pa je da ima večina na socialnih omrežjih zaseben ali zaklenjen profil.

Na koncu sva navedli še nasvete za starše, ki lahko pomagajo pri računalniški oz. spletni vzgoji otrok. Nasveti za vzgojo so opisani tudi po obdobjih odraščanja do adolescence.

Za raziskovalno naloga sva našli največ materiala na spleti saj obstaja veliko slovenskih spletnih strani, ki se osredotočajo pa spletno varnosti. Tudi anketo so osnovnošolci reševali na računalnikih.

## 9. Viri in literatura

- [1] *Arnes*. (5. 3 2019). Pridobljeno iz Arnes: <https://www.arnes.si/storitve/varnost/>
- [2] *Forbes*. (16. 1 2019). Pridobljeno iz Forbes: <https://www.forbes.com/insights-intelai/ai-issue-1/>
- [3] *Safe.si*. (2019). Pridobljeno iz Safe.si: <http://www.safe.si/>
- [4] *Safe.si*. (27. 2 2019). *Safe.si*. Pridobljeno iz Safe.si: <https://safe.si/nasveti/druzabna-omrezja>
- [5] *Varni na internetu.si*. (10. 1 2019). Pridobljeno iz Varni na internetu.si: <https://www.varninainternetu.si/>
- [6] *Varnost na spletu.si*. (2. 2 2019). Pridobljeno iz Varnost na spletu.si: <https://www.varnostnaspletu.si/splosni-napotki-za-varno-rabo-interneta/>

## 10. Priloge

- Anketa - Varnost na internetu
- Izjava

## Varnost na internetu

V okviru raziskave, ki jo opravljam za maturitetno nalogo z naslovom »Varnost na internetu« bom ugotavljala koliko ste izobraženi o varnosti na internetu. Anketiranje je anonimno, kar pomeni, da se imena nikjer ne bodo uporabljala, rezultati pa bodo uporabljeni samo za namen raziskave.

\* Required

1. 1. Zavedam se, da stvari, ki jih preberem na spletu, niso vedno resnične. \*

*Check all that apply.*

- ☐ Da  
☐ Ne

2. 2. Sporočil neznanih pošiljateljev ne odpiram. \*

*Check all that apply.*

- ☐ Da  
☐ Ne

3. 3. Katere naprave uporabljaš za dostop do interneta? (obkljukaj) \*

*Check all that apply.*

- ☐ Pametni telefon  
☐ Računalnik  
☐ Tablični računalnik  
☐ Pametno uro  
☐ Other: \_\_\_\_\_

4. 4. Internet uporabljam za (obkljukaj): \*

*Check all that apply.*

- ☐ Šolo  
☐ Klepetanje  
☐ Poslušanje glasbe  
☐ Gledanje filmov  
☐ Igranje iger  
☐ Spremljanje socialnih omrežij(Snapchat, Instagram, Facebook...)  
☐ Other: \_\_\_\_\_

5. 5. Ali si se s starši kdaj pogovarjal o varnosti na spletu? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

6. 6. Ali ste pri pouku oziroma razrednih urah pozorni na varno rabo interneta? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

7. 7. Koga bi v primeru spletne zlorabe prosili za pomoč? \*

*Check all that apply.*

- ☐ Starše, družinske člane  
☐ Prijatelje, vrstnike, sošolce  
☐ Policojo  
☐ Učitelja, razrednika  
☐ Other: \_\_\_\_\_

8. 8. Ali si kdaj poskusil komu vdreti v profil? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

9. 9. Ali poskrbiš, da so tvoja gesla dovolj močna? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

10. 10. Ali na socialnih omrežjih kdaj lažeš o svoji starosti/imenu/izgledu? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

11. 11. Ali na socialnih omrežjih objavljaš svoje fotografije? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

12. 12. Ali je tvoj profil javen? \*

*Check all that apply.*

- ☐ Da  
☐ Ne

### IZJAVA\*

Mentor Boštjan Lubej v skladu z 2. in 17. členom Pravilnika raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje, zagotavljam, da je v raziskovalni nalogi z naslovom Varnost na spletu, katere avtorja sta Marina Cokan, Sanja Gregorič:

- besedilo v tiskani in elektronski obliki istovetno,
- pri raziskovanju uporabljeno gradivo navedeno v seznamu uporabljene literature,
- da je za objavo fotografij v nalogi pridobljeno avtorjevo dovoljenje in je hranjeno v šolskem arhivu,
- da sme Osrednja knjižnica Celje objaviti raziskovalno nalogo v polnem besedilu na knjižničnih portalih z navedbo, da je raziskovalna naloga nastala v okviru projekta Mladi za Celje,
- da je raziskovalno nalogo dovoljeno uporabiti za izobraževalne in raziskovalne namene s povzemanjem misli, idej, konceptov oziroma besedil iz naloge ob upoštevanju avtorstva in korektnem citiranju,
- da smo seznanjeni z razpisni pogoji projekta Mladi za Celje.

Celje, 8.3.2019



Podpis mentorja

Podpis odgovorne osebe

### POJASNILO

V skladu z 2. in 17. členom Pravilnika raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje je potrebno podpisano izjavo mentorja (-ice) in odgovorne osebe šole vključiti v izvod za knjižnico, dovoljenje za objavo avtorja (-ice) fotografskega gradiva, katerega ni avtor (-ica) raziskovalne naloge, pa hrani šola v svojem arhivu.