"56. srečanje mladih raziskovalcev Slovenije 2022"

Osnovna šola Janka Padežnika Maribor,

Iztokova 6, 2000 Maribor

BLAZNO RESNO O VARNOSTI NA SPLETU

Raziskovalno področje:

APLIKATIVNI INOVACIJSKI PREDLOGI IN PROJEKTI

Mentorja:

Dejan Peklar,

Ksenija Popošek

Avtorja:

Jošt Hölbl,

Žana Kralj

Maribor, 2022

ZAHVALA

Iskrena hvala mentorjema za vsako vzpodbudno besedo, podporo in navdušenje ob nastajanju naše naloge. Zahvaljujemo se vsem, ki so skrbno izpolnili anketni vprašalnik in izrazili svoje mnenje o uporabi in zlorabah na spletu. Posebna zahvala gre vsem zunanjim strokovnjakom, ki so sodelovali v intervjujih, ter zunanjim strokovnjakom, ki so z nasveti pomagali pri snovanju spletne igre. Vse to je vodilo do realizacije inovacijskega predloga.

VSEBINSKO KAZALO

KAZALO SLIK

KAZALO GRAFOV

KAZALO TABEL

POVZETEK

Uporaba iger v izobraževanju je v uporabi že nekaj desetletij. Z igro podprto poučevanje bo osnovnošolcem približalo obravnavano tematiko in jih pritegnilo k dodatnemu izobraževanju. Takšen način poučevanja bi predstavljal povečanje učinkovitosti učenja. Igrifikacija tako lahko popolnoma spremeni način učenja učencev. Gre za novejši koncept motiviranja, ki izhaja iz sveta informacijskih tehnologij, iger in spletnih igric. Pri pregledu vsebin, ki so obravnavane pri izbirnem predmetu računalništva, spletnih strani, ki mlade učijo o varni uporabi interneta (kot npr. Safe.si), ugotavljamo, da med gradivi ni zaslediti spletne igrice v slovenskem jeziku, ki bi lahko bila uporabljena kot učno gradivo. Tako glede napovedi o širjenju vsebin izobraževanja s področja računalništva in vpeljave teh vsebin v obvezni program predlagamo uporabo z igro podprtega poučevanja, ki bi pomenilo pozitiven doprinos. V ta namen smo preverili zavedanje otrok o varni uporabi spleta, pripravili primer učnega gradiva ter razvili osnovno spletno igro, ki osnovnošolce uči varnega vedenja na spletu.

KLJUČNE BESEDE: spletna varnost, zasebnost, spletne zlorabe, spletne igre, učno gradivo

ABSTRACT

The use of games in education has been in use for several decades. Game-based learning will bring the subject matter closer to primary school children and engage them in further education. This way of teaching would represent an increase in the effectiveness of learning. Gamification can thus completely change the way pupils learn. It is a newer concept of motivation, which comes from the world of information technologies, games and online games. When reviewing the content covered in the Computer Science elective, websites that teach young people about the safe use of the Internet (such as Safe.si), w*e've noticed* that there is no online game in the Slovene language that could be used as teaching material. Thus, in view of the announcements about the expansion of computer science education and the introduction of this content in the compulsory curriculum, *we are of the opinion* that the use of game-based learning would be a positive contribution. To this end, we have tested children's awareness of the use of the Internet, developed example teaching materials and developed a basic online game to teach primary school children safe online behaviour.

KEYWORDS: web security, privacy, web abuses, web game, study material

1. UVOD

Otroci danes veliko prostega časa preživijo pred zasloni, pa naj bo to televizija, računalnik, pametni telefon ali tablica. Uporaba teh tehnologij ima veliko pozitivnih vidikov, vendar je treba vzpostaviti ravnotežje med časom in namenom uporabe sodobne tehnologije. Potrebno se je zavedati, da uporaba interneta za otroke ne pomeni varnega okolja. Na internetu lahko hitro naletimo na različne oblike spletnega nasilja, udeleženi pa smo lahko kot priče, žrtve ali povzročitelji. Spletno nasilje se pojavlja v različnih oblikah, izvajajo ga lahko tako mladi kot starejši, vsaka oblika pa je nedopustna.

Spletno ustrahovanje se dogaja z uporabo digitalnih tehnologij, kot so mobilni telefoni, računalniki in tablice. Lahko se pojavi preko SMS in MMS-sporočil, aplikacij in klepetalnic, preko družbenih omrežij, forumov in iger, kjer si lahko ljudje ogledajo vsebino, sodelujejo pri njej ali jo delijo. Pogosto gre za pošiljanje, objavljanje ali deljenje negativnih in škodljivih vsebin o nekom, s čimer ga spravimo v zadrego ali ga ponižamo. Število udeležencev je lahko pri spletnem nasilju potencialno izjemno številno, žrtev pa ostaja ranljiva, dosegljiva in izpostavljena, zato je spletno nasilje posebej tvegano in škodljivo.

Nekatero spletno ustrahovanje prečka mejo v nezakonito ali kaznivo vedenje. Glede na aktualnost in izrazito škodljivost te oblike medvrstniškega nasilja smo ponudili priložnost ozaveščanja in izobraževanja otrok o varni in odgovorni rabi interneta s pomočjo spletne igre.

Naš cilj je, da bi pripravili igro, s katero bi na igriv način poučili otroke in najstnike o varnosti na spletu.

1.1. Namen in cilj inovacijskega predloga

Vsako spletno nasilje, čeprav je na prvi pogled morda nedolžno in na žrtvi ni videti posledic, pusti posledice. Če vidimo, da je nekdo žrtev nasilja, potem je naša naloga, da ustrezno ukrepamo. Na družabnih omrežjih lahko nasilne komentarje in posameznike prijavimo, če gre za hujše oblike nasilja, je treba o tem obvestiti odrasle, učitelje v šoli ali starše. Ob hujših kaznivih dejanjih (npr. deljenje intimnih fotografij mladoletnih oseb, grožnje, izsiljevanje) je potrebno obvestiti policijo.

S pomočjo anketnega vprašalnika za učence in svetovalne delavce ter intervjuja s kriminalistom in strokovnjakom Točke osveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje Safe.si smo pridobili še dodaten pogum za izdelavo spletne igre, ki bo učence ozaveščala o spletnem nasilju v šoli.

Naš inovacijski predlog bo namenjen ozaveščanju otrok o varni rabi ter nevarnostnih na spletu na igriv način, ki bi ga lahko vključili v šolski proces. Spletna igra bo vsebovala elemente prepoznavanja in razumevanja spletnega nasilja in možnosti izogibanja le-temu. Z računalniškega vidika smo uporabili tehnologije CSS, HTML, JavaScript ter knjižnico Bootstrap. Na tak način smo izdelali vsem dobro poznano igro Vislice, pri kateri igralci ugibajo odgovore na vprašanja, ki so povezana s spletno varnostjo. Hkrati smo se naučili veščin programiranja oziroma jih izpopolnili.

Menimo, da bomo z našo spletno igro pripomogli k temu, da bodo učenci bolje razumeli nevarnosti spletnega nasilja in se bodo lažje izogibali internetnim pastem.

Glede na namen inovacijskega predloga smo si zastavili naslednje hipoteze:

Hipoteza 1: Otroci so zadostno ozaveščeni o nevarnostih na spletu.

Hipoteza 2: Učenci nimajo ustrezno zavarovanih računalnikov.

Hipoteza 3: Več zlorab na spletu se zgodi mlajšim otrokom, saj so manj izkušeni.

Hipoteza 4: Večina otrok se na spletne račune ne prijavlja s svojimi dejanskimi osebnimi podatki.

Hipoteza 5: Izobraževalna igra bo primerna za učence od 5. do 9. razreda.

1.2. Predvidena nova spoznanja

Učno gradivo in spletna igra, ki smo ju pripravili, sta namenjena otrokom in najstnikom, z njima bomo ozaveščali otroke o varni rabi spletnega omrežja.

S pomočjo strokovne literature, spletnih virov, ankete in opravljenega intervjuja smo dobili obsežnejši vpogled v nevarnosti na spletu.

S ciljem, ki smo ga izpostavili, bomo ozaveščali otroke o varni rabi ter nevarnostih na spletu na igriv način, za katerega predlagamo, da se ga vključi v šolski učni program.

2. TEORETIČNI DEL

Ne glede na to, ali smo priče, žrtve ali storilci, lahko na spletu zlahka naletimo na več vrst spletnega nasilja. Spletno nasilje je lahko v različnih oblikah, izvajajo pa ga lahko tako mladi kot starejši. Vedno in v vseh oblikah je obsojanja vredno. Zastraševanje, nadlegovanje in ustrahovanje so primeri spletnega nasilja, ki ga izvaja eden ali več posameznikov nad drugim posameznikom ali skupino (ali na internetu).

Kibernetsko ustrahovanje se med mladimi najpogosteje izvaja kot spletno ustrahovanje oziroma nadlegovanje, vse pa lahko poimenujemo z angleško besedno zvezo *cyberbullying*, ki označuje ustrahovanje z uporabo digitalnih naprav, kot so telefoni, računalniki in tablice. Med drugim se lahko zgodi prek sporočil SMS, MMS, številnih aplikacij in klepetalnic, družabnih omrežij, forumov in iger. Pogosto uporabljeni izrazi so pošiljanje, objavljanje in deljenje.

Ko med brskanjem po družabnih medijih ali komuniciranjem z drugimi naletimo na neprimerno ali nasilno vsebino, lahko postanemo žrtve ali storilci (udeleženci), očividci ali priče. V vsakem primeru gre za grožnjo, ki smo ji nenehno izpostavljeni.

2.1. Vrste spletnega nasilja

Spletno nasilje se izraža na številne načine in po številnih poteh ter komunikacijskih kanalih. Med oblike spletnega nasilja sodijo:

- Žaljiva ali sovražna vsebina, usmerjena proti določeni osebi, ki jo z angleško besedo imenujemo tudi *flaming*.
- Izključitev iz skupin - skupina vrstnikov izključi ali prepove vrstniku, da se pridruži skupini v družbenem omrežju ali aplikaciji za sporočanje. O tem se v skupini razpravlja in se vrstnika obvesti. Razlike so lahko razlog za izključitev.
- Posamezniki ustanavljajo sovražne organizacije in vabijo druge, da se jim pridružijo, z namenom širjenja sovraštva do posameznika ali druge skupine posameznikov.
- Lažni profili - storilec ustvari lažni profil žrtve in v njenem imenu objavlja stvari, ki jo sramotijo ali ponižujejo. Druga možnost je, da s pomočjo izmišljenega profila zavaja ali žali druge in tako očrni zadevnega posameznika.

- Pri intimnih posnetkih storilec objavi gole fotografije ali filme z drugimi, do izsiljevanja pa pride, ko storilec žrtvi grozi z objavo posnetkov, če mu ne pošlje denarja ali več posnetkov.
- Snemanje in objavljanje slik in filmov brez dovoljenja - snemanje fotografij je poseg v zasebnost osebe in se ne sme izvajati brez njenega dovoljenja. Enako velja za deljenje videoposnetkov v družabnih omrežjih ali drugje na internetu. Ne smemo objavljati ali razširjati nikogaršnjih podatkov.
- Prilagoditve fotografij, ki so žaljive - žaljiva sprememba fotografije ali videoposnetka je lahko žaljiva za osebo na fotografiji ali fotografa.
- Ustvarjanje žaljivih slikovnih vsebin, imenovanih tudi *meme,* iz slik in informacij o vrstniku, z namenom žaljenja, zasmehovanja, poniževanja itd.

Kršitev zaupanja se zgodi, ko storilec zasebne informacije o žrtvi, ki mu jih je ta zaupala, objavi na internetu, bodisi odkrito bodisi v zaprti skupini, v pričakovanju, da jih žrtev ne bo delila z drugimi.

O obrekovanju govorimo, kadar nekdo o nekom objavi neresnice (laži) v družabnih medijih, aplikacijah za sporočanje in drugih platformah.

Vdor v profile (račune) je kaznivo dejanje. Gre za kršitev zasebnosti posameznika, ki je primerljiva z vdorom v stanovanje. V ta namen smo pripravili primer učnega gradiva in nabor vprašanj za spletno igro, ki mlade ozavešča o varni rabi gesel. To lahko pripomore k preprečitvi vdorov v posameznikove račune.

Doxing je razkrivanje osebnih podatkov druge osebe brez njenega soglasja.

Objavljanje posnetkov nasilja, na katerih nekdo udari žrtev, drugi to posnamejo in nato posnetek naložijo na mesta, kot je YouTube, da bi žrtev osramotili, je znano kot *happy slapping*.

Pošiljanje nasilnih ali grozljivih fotografij in videoposnetkov - nasilni in grozljivi prizori lahko na prejemnika vplivajo zelo škodljivo, kar se kaže v nočnih morah in strahu.

Pošiljanje verižnih pisem in sporočil - večina poslanih verižnih pisem in sporočil je namenjena strašenju prejemnika. Številne posameznike prestrašijo informacije, tudi če so lažne.

Spletni izzivi - spletni izzivi, pri katerih je oseba izzvana, da naredi nekaj ponižujočega ali celo nevarnega, kar se nato posname in predvaja na spletu. Udeležba pri tem je žal tudi v Sloveniji že terjala smrtno žrtev med mladimi.

Spletno nagovarjanje vključuje približevanje mladim z namenom spolne zlorabe.

Tudi če se zdi, da je zloraba nenamerna in žrtev ni prizadeta, ima vsaka spletna zloraba posledice. Zato je treba spletno agresijo obsoditi. Na prvi pogled se zdi, da številne žrtve trpijo v tišini, vendar v resnici zelo trpijo; tega preprosto nočejo, ne znajo ali ne želijo pokazati. Stiska zaradi spletne agresije lahko preraste v depresijo, izolacijo in samopoškodovanje (celo samomor).

(povzeto po safe.si 10.1.2022)

2.2. Računalniška gesla

Ker ocenjujemo, da so otroci premalo seznanjeni z ukrepi za varno uporabo spleta in bi bilo v bodoče priporočljivo, da postane šolski predmet računalništva v 2. in 3. triadi osnovne šole obvezen, smo pripravili tudi primer učnega gradiva na temo varnosti gesel, ki bi ga lahko učitelji uporabili pri šolskem delu.

Gesla so povezana z varnostjo in predstavljajo na spletu osnovni varnostni mehanizem. Običajno za zaščito uporabljamo klasična gesla, s katerimi se kot uporabniki vsakodnevno srečujemo. Uporabljamo jih za preverjanje e-poštnih predalov, za dostop do družbenih omrežij ali omejitev dostopa do brezžičnih internetnih povezav.

Gesla so zaporedja znakov, lahko vključujejo črke, številke ali posebne znake, kot so pika, vejica ali drugi simboli. Geslo morata poznati tako uporabnik kot sistem, v katerega se uporabnik prijavlja. Uporabnik si lahko po navadi geslo izbere sam ali pa mu ga izda sistem (npr. ponudnik spletne e-pošte). Dolžina gesla in število dovoljenih znakov se razlikujeta glede na sistem. Najmanjšo dolžino gesla določa tudi sistem, v katerem se vodi račun.

Postopek uporabe gesla je preprost: uporabnik v obrazec za prijavo vnese uporabniško ime in geslo, sistem pa preveri, ali se vneseni podatki ujemajo s shranjenimi. Če so podatki pravilni, se uporabniku odobri dostop. Če se podatki ne ujemajo, bo sistem dovolil, da uporabnik z omejenim številom poskusov ponovno vnese uporabniško ime in geslo.

Uporabniško določena gesla so pogosto predvidljiva. Večina uporabnikov jih oblikuje z osebnimi podatki, kot so ime, datum rojstva, imena živali ali družinskih članov in podobno, da bi si jih lažje zapomnili. Takšna gesla so običajno preprosta in jih napadalec zlahka ugiba. V šibkih geslih in geslih, ki si jih je lahko zapomniti, se pogosto uporabljajo zgolj male črke.

Močna gesla so sestavljena iz mešanice naključnih številk, črk in simbolov, ki so razpršeni po celotnem geslu. Gesla morajo biti dolga vsaj osem znakov, priporoča pa se vsaj dvanajst znakov. Daljše kot je geslo, manjša je verjetnost, da bo uvrščeno na seznam gesel, ki jih hekerji uporabljajo za razbijanje gesel.

Ne glede na to, kako dolgo ali raznoliko je geslo, je najpomembnejše, da se ga redno spreminja. Gesla nikoli ne morejo biti popolnoma varna, zato vsako geslo, ne glede na to, kako močno je, nekoč preneha veljati. Kljub temu vas bo močno geslo varovalo veliko dlje kot šibko. Ker je večina gesel šibkih, večina skrbnikov od uporabnikov zahteva, da gesla posodobijo vsakih 60-120 dni.

Varnostni strokovnjaki svarijo pred preprostimi gesli in uporabnikom odsvetujejo uporabo preprostih gesel, ki jih ni težko razvozlati. Priporočeno je, da uporabljamo edinstvena in kompleksna gesla, sestavljena iz najmanj 12 znakov. Uporabniki bi morali gesla tudi redno posodabljati, starega gesla pa ne bi smeli "reciklirati". Za zaščito uporabniških računov je smiselno uporabiti dvofaktorsko overjanje (ang. Two-Factor Authentication - 2FA). Takšna metoda običajno geslo kombinira z enkratnih geslom, ki ga običajno uporabnik prejme preko sporočila SMS ali ga ustvari s pomočjo namenskih aplikacij. (povzeto po https://www.rtvslo.si/zabava-in-slog/zanimivosti/sokantno-najpogostejse-geslo-letosnjega-leta-je-123456/602473, nazadnje obiskano, 17.1.2022)

V omenjenem prispevku so bila predstavljena tudi najpogostejša gesla lanskega leta. Najbolj priljubljena gesla za dostop do uporabniških računov tudi v letu 2021 ostajajo tista najpreprostejša in s tem tudi najranljivejša. Absolutna zmagovalca med gesli sta 123456, ki ni pretirano zahtevno niti za spomin niti za koordinacijo prstov, in qwerty, medtem ko športni navdušenci prisegajo na Liverpool. (povzeto po https://www.rtvslo.si/zabava-in-slog/zanimivosti/sokantno-najpogostejse-geslo-letosnjega-leta-je-123456/602473, nazadnje obiskano, 17.1.2022)

1. - 123456
2. - 123456789
3. - 12345
4. - qwerty
5. - password (geslo)

Slika 1: Pet najbolj priljubljenih gesel leta 2021 (povzeto po https://www.rtvslo.si/zabava-in-slog/zanimivosti/sokantno-najpogostejse-geslo-letosnjega-leta-je-123456/602473).

Tudi številna tuja podjetja redno objavljajo sezname najpogostejših gesel. Mednje sodi podjetje NordPass, ki je objavilo svoj seznam 200 najbolj pogostih gesel v letu 2021. Na tem mestu navajamo samo prvih 15, ki jih prikazuje Tabela 1, preostale pa je mogoče pridobiti na spletnem naslovu https://nordpass.com/most-common-passwords-list/.

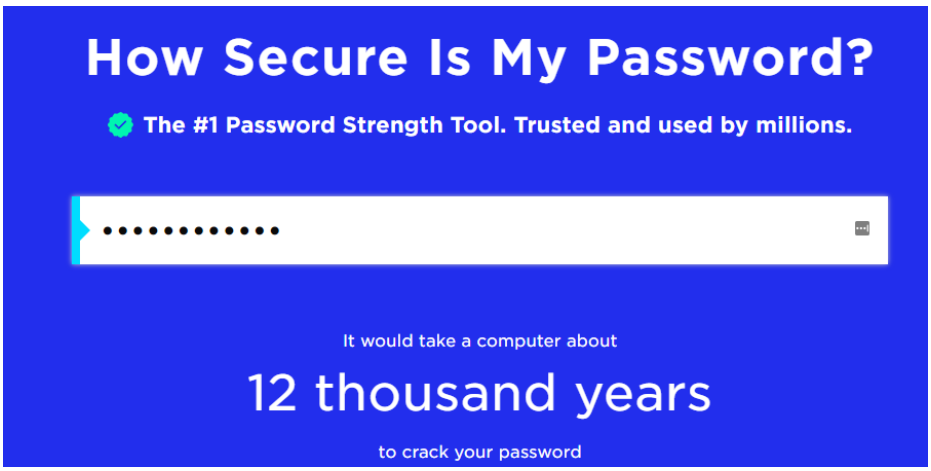
Tabela 1: 15 najbolj pogostih gesel v letu 2021 po raziskave podjetja NordPass, povzeto po https://nordpass.com/most-common-passwords-list/, nazadnje obiskano: 17.1.2022.

#	Geslo	Čas, potreben za razbijanje
1	123456	< 1 sekunde
2	123456789	< 1 sekunde
3	picture1	3 ure
4	password	< 1 sekunde
5	12345678	< 1 sekunde
6	111111	< 1 sekunde
7	123123	< 1 sekunde
8	12345	< 1 sekunde
9	1234567890	< 1 sekunde
10	senha	10 sekund
11	1234567	< 1 sekunde
12	Qwerty	< 1 sekunde
13	abc123	< 1 sekunde
14	Million2	3 ure
15	000000	< 1 sekunde

Geslo je nekaj, kar uporabnik ustvari oz. mora imeti za preverjanje identitete na različnih spletnih računih. Uporabniki pogosto za elemente svojega gesla uporabijo imena bližnjih, hišnih ljubljenčkov, pomembne datume in datume rojstnih dni, priimek. Specialisti priporočajo uporabo močnih gesel, ki vsebujejo velike in male črke, posebno simbole, in so dolga vsaj 10 črk. Takšno geslo mora biti zasnovano tako, da ga noben drug posameznik ne more uganiti. Kot primer navajamo geslo K@iv0=?!s;CK - takšno geslo ima pogosto smisel, ki si ga lahko zapomni ali ve samo kreator tega gesla. (povzeto po W. Stallings, L. Brown: Computer Security – Principles and Practice, 4th Edition, Pearson, Boston, 2018)

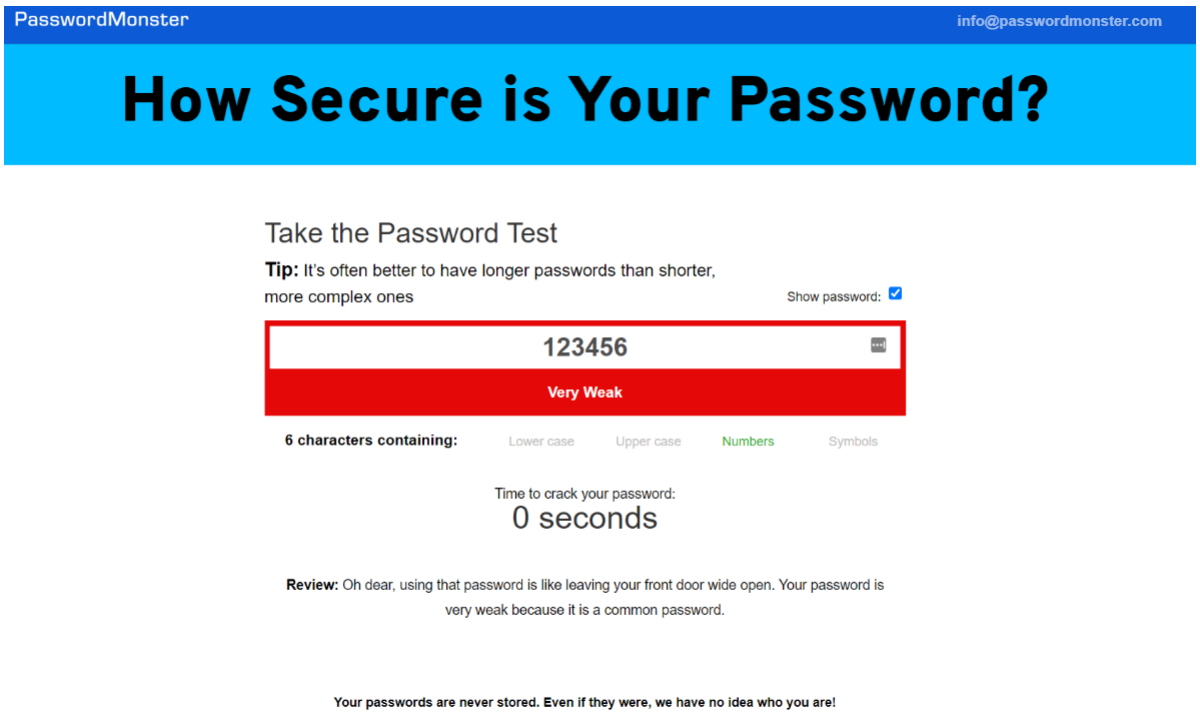
2.2.1. Varna gesla

Uporaba varnih gesel lahko pripomore k boljši varnosti oseb na spletu, tako lahko preprečimo morebitne vdore v uporabniške račune in zlorabo gesel s strani oseb, ki bi šibko geslo zaradi povezave z nami hitro ugotovili. Geslo mora biti močno, a hkrati preprosto, da si ga uporabnik lažje zapomni. Primer takšnega gesla je npr. Vsjk,kjjpm – je močno, vendar si ga lahko uporabnik zapomni z asociacijo »Včeraj sem jedel kremšnite, ki jih je pripravila mama.« V geslu smo uporabili tudi ločila, da ga je še težje uganiti. To težko geslo, ki je hkrati uporabnikom prijazno, je zelo močno. Preizkusili smo ga na spletni strani https://www.passwordmonster.com/, ki omogoča preizkus varnosti gesla, in ugotovljeno je bilo, da gre za varno, močno geslo, za katerega bi tisti, ki bi ga poskušali zlorabiti, porabili 12 tisoč let.



Slika 2: Prvi primer spletne strani, kjer je mogoče preveriti varnosti gesla (povzeto po https://www.passwordmonster.com/)

Priporočamo, da osnovnošolci varnost svojih gesel preizkusijo na spletni strani https://www.passwordmonster.com/. Preizkus je popolnoma enostaven, saj je potrebno geslo vpisati v okvirček, ki nato preveri, koliko let bi bilo potrebnih za ugotovitev tega gesla in kako močno je. Če se izkaže, da je geslo prešibko, lahko ustvarijo novega.



Slika 3: Drugi primer spletne strani, kjer je mogoče preveriti varnosti gesla (povzeto po https://www.passwordmonster.com/)

Varno (močno) ustvarite tako, da spoštujete naslednje napotke:

- dolgo naj bo vsaj 12 znakov,
- vsebovati mora male in velike črke,
- vsebuje številke,
- vključuje posebne znake,
- NE vsebuje osebnih podatkov, kot so datum rojstva, ime hišnega ljubljenčka, vaše ime ali e-poštni naslov.

Pri uporabi gesel na varen način moramo slediti še drugim priporočilom, ki so navedena v nadaljevanju.

(povzeto po https://medium.com/belong-blog/password-101-how-to-create-a-secure-password-8adfbe888d79, nazadnje obiskano dne 17. 1. 2022)

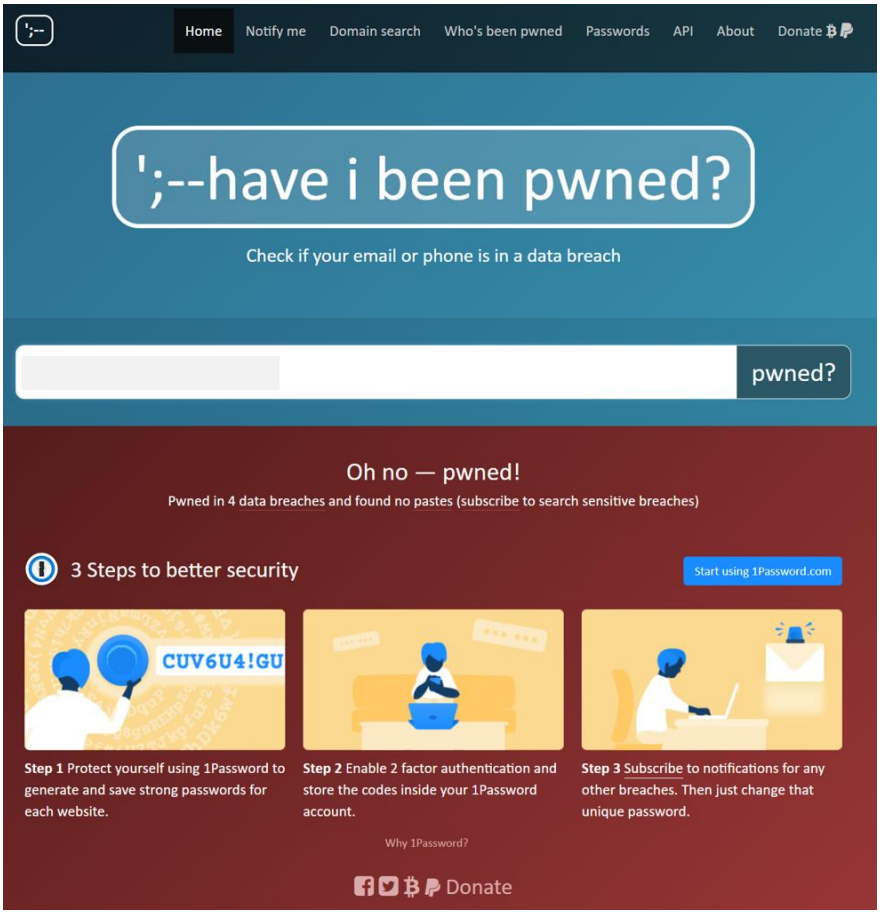
1. Redno spreminjanje gesel

Če geslo uporabljate dlje časa, je možnost, da ga je kdo uganil, večja. Nekatera spletna mesta vas bodo samodejno pozvala k spremembi gesla, če ga niste dolgo spremenili. Vendar je dobro, da svoja gesla za pomembne račune (e-pošta, družbeni mediji) redno spreminjate.

2. Uporaba različnih gesel

Uporaba istega gesla na več spletnih mestih je tvegana. Če so vaše podatke ukradli, na primer, s spletnega mesta družbenih omrežij, vi pa isto geslo uporabljate tudi v aplikaciji za spletno učilnico in elektronsko pošto, ste ranljivi tudi na teh dveh mestih.

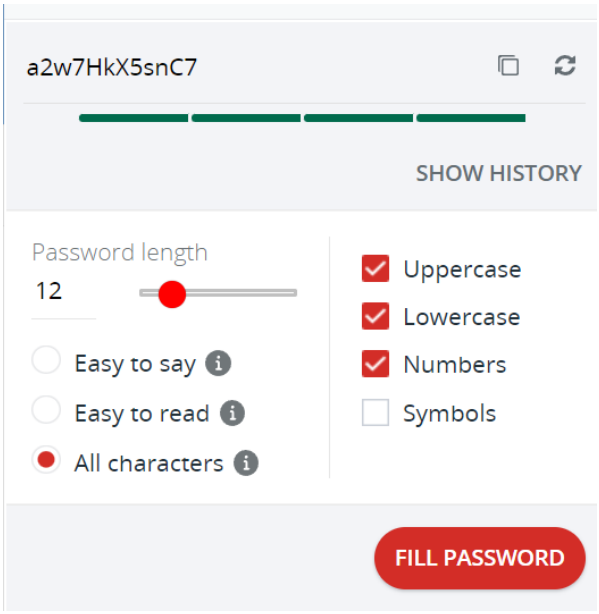
Osnovnošolci lahko preverijo tudi, ali so bili njihovi spletni računi zlorabljeni oz. če so vsi lahko videli njihovo geslo. To lahko preverijo na https://haveibeenpwned.com/, kjer vpišejo svojo e-pošto ali telefonsko številko.



Slika 4: Spletna stran za preverjanje zlorabljenih spletnih računov (https://haveibeenpwned.com/).

Obstajajo aplikacije in programska oprema, ki vas lahko opozorijo, če so bila vaša gesla del kršitve varnosti podatkov. Googlov program Password Manager vas lahko opozori, če ugotovi, da so vaši podatki pricurljali v javnost, Apple pa to funkcijo ponuja v operacijskem sistemu iOS 14 in novejših.

Večina upraviteljev gesel ima možnost ustvarjanja naključnih gesel. Generator naključnih gesel vam lahko pomaga pri ustvarjanju varnega gesla. Uporabnik določi dolžino gesla in vrste znakov, ki jih želi uporabiti, generator pa na podlagi te formule ustvari naključno geslo.



Slika 5: LastPass – generator naključnih gesel.

Gesla, ki jih ustvari človek, so manj varna od računalniških, saj niso naključna. Če si želimo gesla zapomniti, morajo biti močna in enostavna za zapomnitev. Najlažje si zapomnimo gesla, ki so za nas pomembna. Obstaja več metod za sestavo zapletenega gesla, ki si ga je preprosto zapomniti.

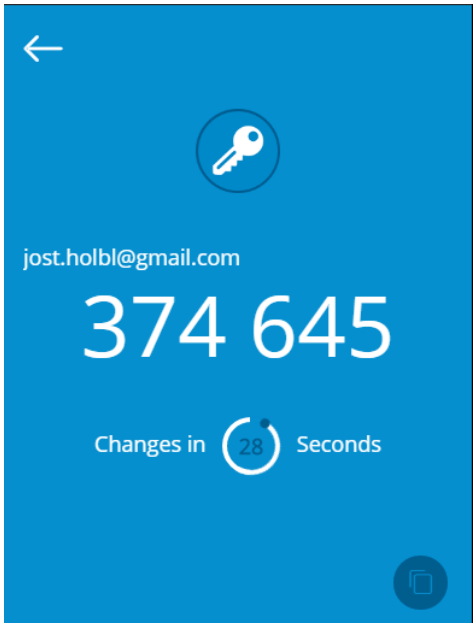
Ena od metod je že bila predstavljena. Tako si na primer za geslo izberemo prve črke verza priljubljene pesmi, kombiniramo velike in majhne črke, dodatno številke in/ali posebne znake. Nikakor pa ne uporabljamo svojega imena, priimka, hišnega ljubljenčka, rojstnega datuma ipd. Z uporabo le-teh smo lahko tarča vdora v spletni račun tudi s strani poznanih oseb, ki bi nam v določenem trenutku želele ponagajati.

3. Uporaba 2-faktorskega overjanja

Varnost gesel lahko izboljšate s pomočjo 2-faktorsega overjanja (ang. Two-factor authentication - 2FA), če ga spletna stran ali aplikacija podpirata. Tehnologija 2FA poleg gesla za preverjanje identitete uporablja tudi dodatno enkratno številsko geslo, ki ga ustvarimo v namenskih aplikacijah s potrditvijo spletne pošte, SMS-sporočilom ali telefonskim klicem. Tudi najmočnejše geslo se ne more kosati s preverjanjem 2FA, saj to onemogoča zlorabo vaših prijavnih podatkov, tudi če se nekdo uspe do njih dokopati.

Kot primer navedimo aplikacijo Authy, ki jo lahko namestite na vaš pametni telefon in ki omogoča ustvarjanje številskih enkratnih gesel za dodatno varnostno preverjanje (t.i. 2FA). Namestitev prikazuje Slika 6, uporabo aplikacije Slika 7.

Slika 6: Primer namestitve mobilne aplikacije Authy iz trgovine Google Play



Slika 7: Ustvarjanje enkratnega gesla s pomočjo mobilne aplikacije Authy

Slika 8: Primer infografike učnega gradiva za učitelje in učence

3. EMPIRIČNI DEL

3.1. Metode dela – metodologija

Pri izdelavi inovacijskega predloga smo uporabljali naslednje raziskovalne metode:

- metode proučevanja različnih virov in literature,
- metode analize podatkov in njihova interpretacija,
- intervju,
- anketni vprašalnik in
- izdelava spletne igre.

3.2. Metode proučevanja različnih virov in literature

Začetna metoda dela je bila metoda dela s pisnimi viri. Literaturo smo poiskali v šolski knjižnici, Mariborski knjižnici in domači osebni knjižnici. Iz tega razloga smo si veliko pomagali s preverjenimi spletnimi viri, predvsem članki, nekaj pa tudi z diplomskimi ali magistrskimi deli. Zbrane podatke smo prebrali, proučili in se o njih z mentorjema pogovorili. S pomočjo mentorjev smo ugotovitve uskladili, povzeli in zapisali.

3.2.1. Metode analize podatke in njihova interpretacija

Za potrebne raziskave smo anketni vprašalnik vstavili v spletni program 1ka, zaradi predvidene boljše udeležbe pri izpolnitvi anketnega vprašalnika med osnovnošolci smo anketni vprašalnik pripravili v pisni obliki in jim ga razdelili. Interpretirali smo tista vprašanja, ki so povezana s postavljenimi hipotezami, in nekatera med njimi primerjali.

3.2.2. Intervju

V želji dobro raziskati stanje spletnih zlorab in nasilja smo pripravili intervju z gospodom Borutom Zalokarjem, kriminalističnim inšpektorjem, specialistom SKP I., ki zadnjih 11 let dela na področju računalniškega preiskovanja oz. računalniške kriminalitete. Ker smo želeli naš inovacijski predlog oplemenititi, smo mnenje poiskali tudi pri strokovnjakih na Točki osveščanja o varni rabi interneta Safe.si. Intervju smo izpeljali z gospodom Markom Puschnerjem s Fakultete za družbene vede Univerze v Ljubljani.

3.2.3. Anketni vprašalnik

Opravili smo anketo s svetovalnimi delavci na osnovnih šolah v Mariboru prek spletne aplikacije Enka. Anketo je izpolnilo 11 svetovalnih delavcev. Anketa je vsebovala 8 vprašanj zaprtega tipa. Anketni vprašalnik je priložen v prilogi.

Pripravili smo tudi anketni vprašalnik za učence, ki smo ga izvedli v papirnati obliki, in ga razdelili učencem od 6. do 9. razreda. Anketni vprašalnik je izpolnilo 139 učencev. Anketa je vsebovala 13 vprašanj zaprtega tipa in 1 vprašanje odprtega tipa. Anketni vprašalnik je priložen v prilogi.

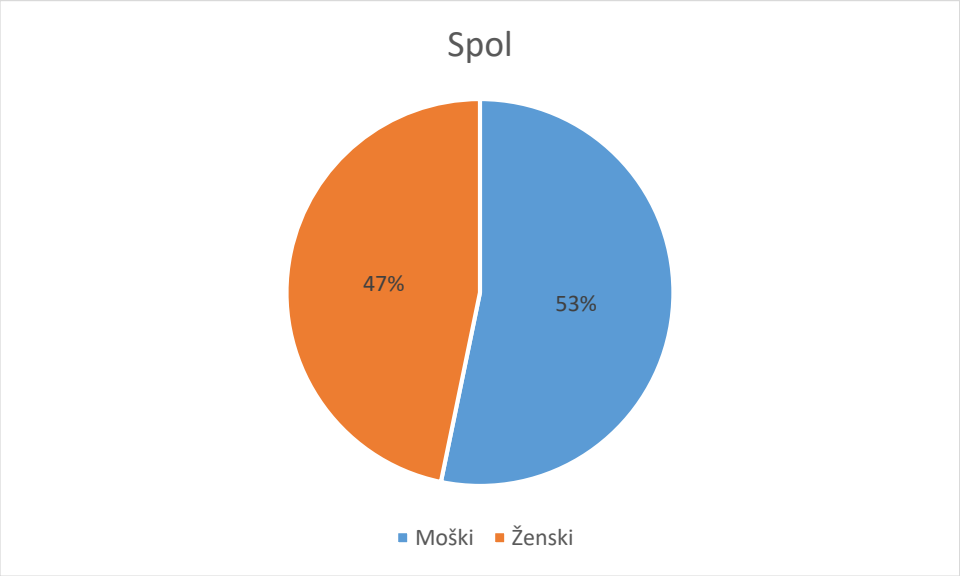
3.2.4. Obdelava podatkov

Pridobljene podatke anketnih vprašalnikov smo obdelali s pomočjo diagramov in dodali interpretacijo rezultatov.

4. OPIS REZULTATOV

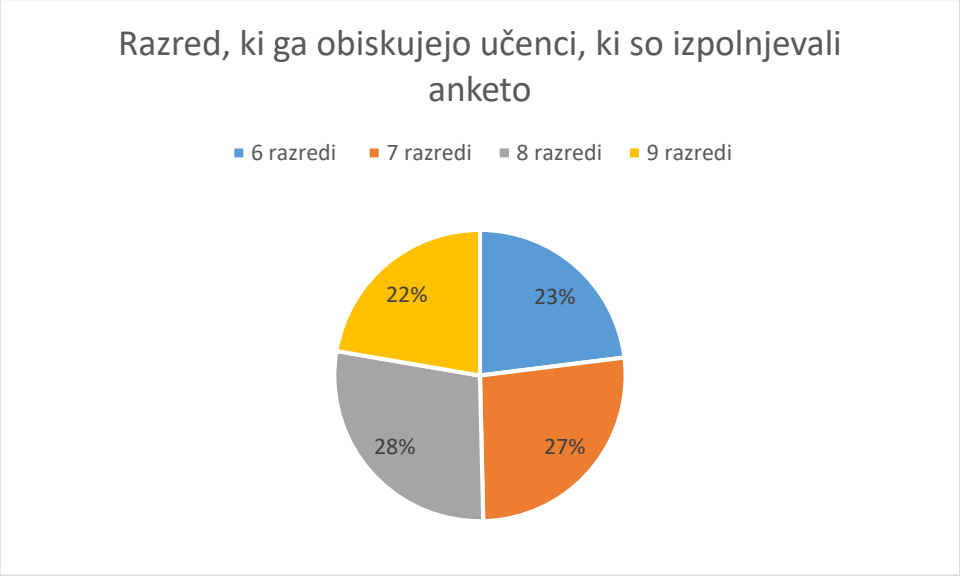
4.1. Rezultati ankete za učence

Graf 1: Spol udeležencev ankete



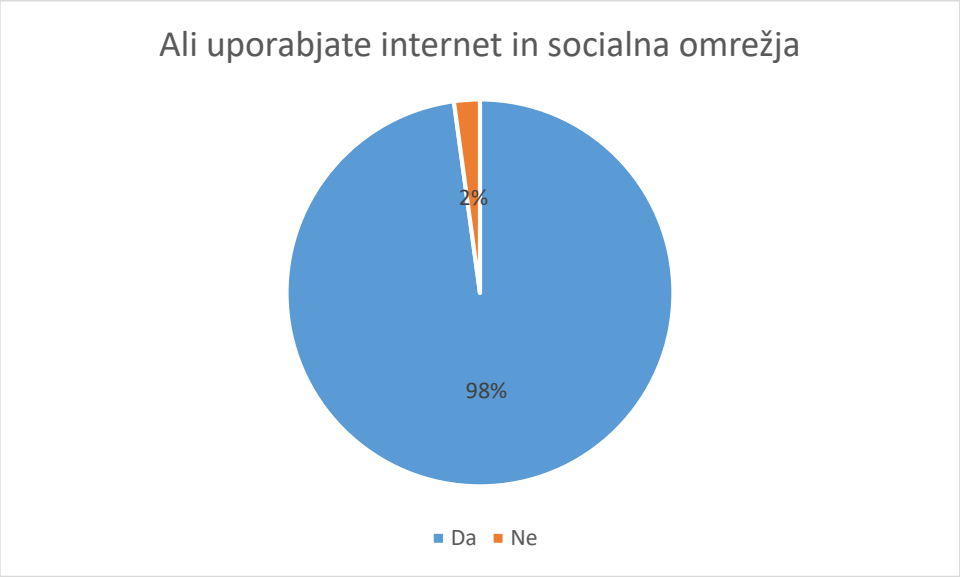
Anketo je reševalno 53 % otrok moškega spola in 47 % ženskega spola.

Graf 2: Razred, ki ga obiskujejo učenci, ki so izpolnjevali anketo



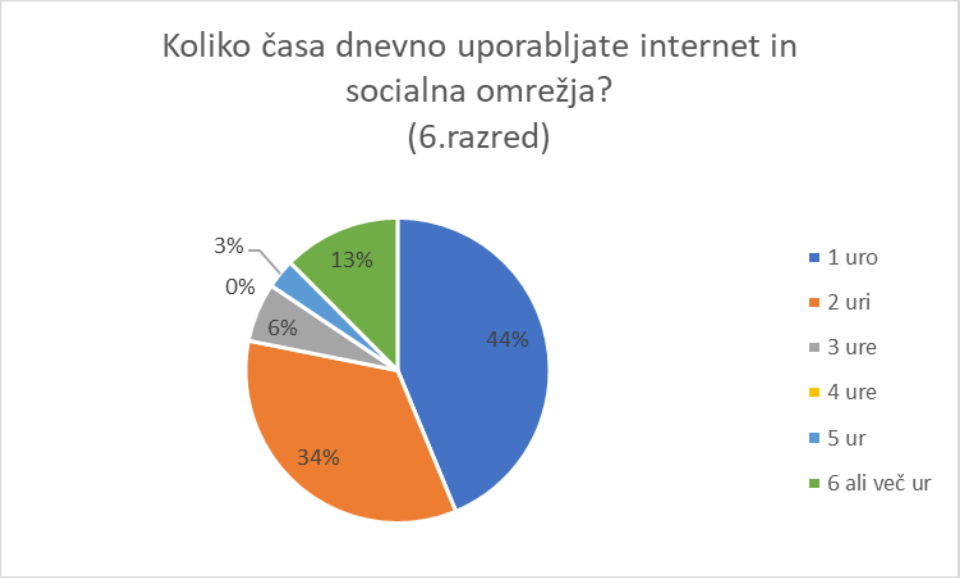
Anketo je reševalo največ učencev iz 8. razreda (28 %) in najmanj iz 9. razreda (22 %).

Graf 3: Ali uporabljate internet in socialna omrežja?



Večina učencev uporablja internet in socialna omrežja.

Graf 4: Koliko časa dnevno uporabljate internet in socialna omrežja?

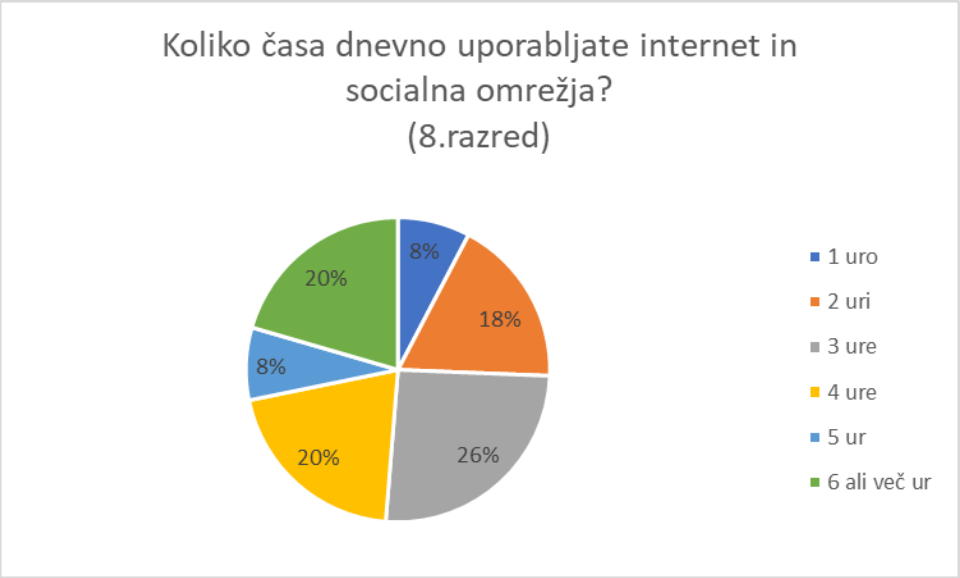


44 % učencev 6. razredov uporablja internet in socialna omrežja eno uro dnevno, 34 % učencev 2 uri dnevno, odstotek tistih, ki internet ali socialna omrežja uporabljajo več kot 6 ur, pa znaša zaskrbljujočih 13 %.

Graf 5: Koliko časa dnevno uporabljate internet in socialna omrežja?

Zaskrbljujoče je, da tudi v 7. razredu opazimo prekomerno uporabo interneta in socialnih omrežij, saj 37 % otrok internet in socialna omrežja uporablja več kot 4 ure.

Graf 6: Koliko časa dnevno uporabljate internet in socialna omrežja? (8. razred)

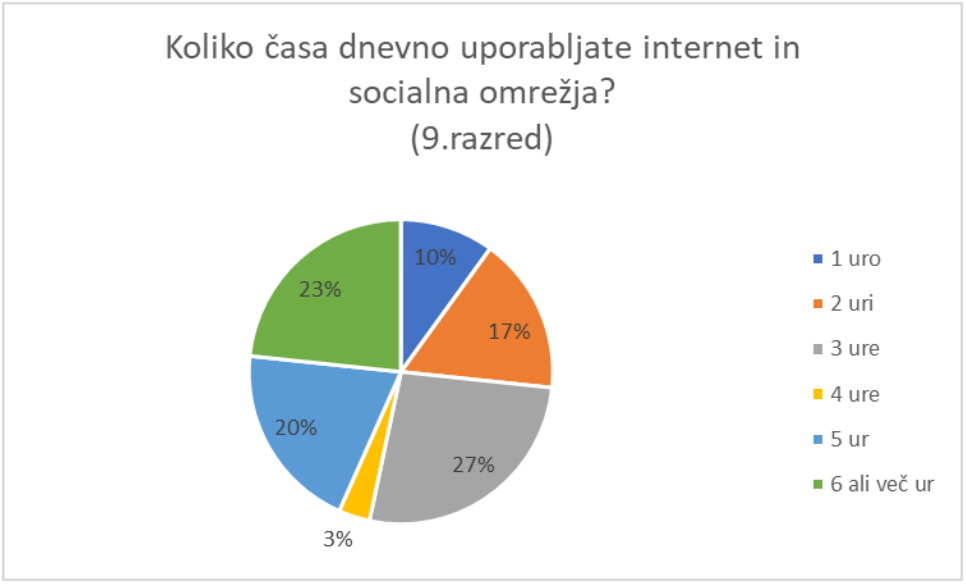


Učenci v 8. razredu prekomerno uporabljajo socialna omrežja in internet - 66 % več kot 4 ure dnevno. Po smernicah WHO ter Točke osveščanja o varni rabi interneta Safe.si je za

mladostnike, stare 13 let, priporočljiva uporaba zgolj 2 uri. Iz grafa razberemo, da učenci 8. razreda prekomerno uporabljajo socialna omrežja in internet.

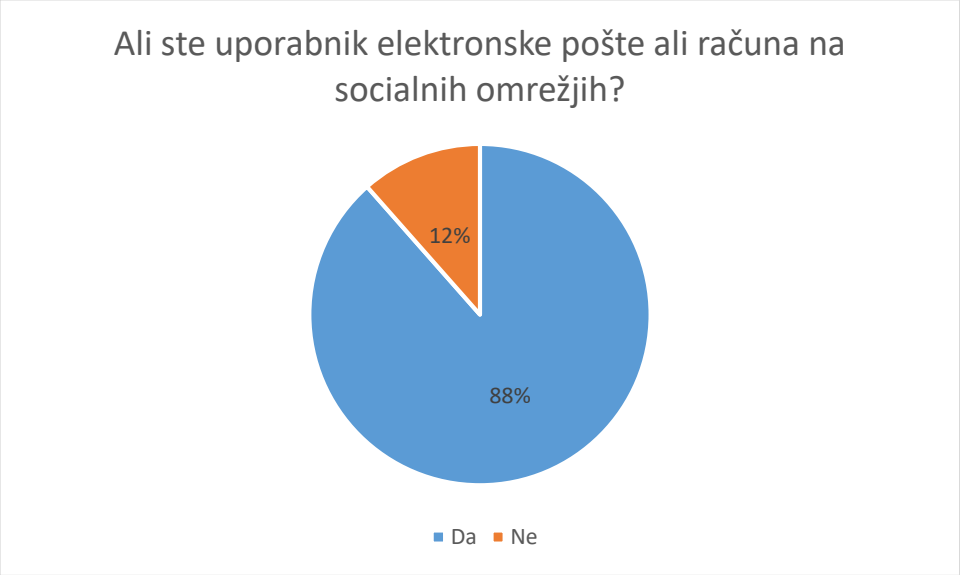
Slika 9: Priporočena dnevna uporaba zaslonov v prostem času
Vir: https://safe.si/sites/default/files/smernice_za_uporabo_zaslonov.pdf

Graf 7: Koliko časa dnevno uporabljate internet in socialna omrežja? (9. razred)



Narašča delež tistih učencev, ki internet in socialna omrežja uporabljajo 6 ur ali več dnevno.

Graf 8: Ali ste uporabnik elektronske pošte ali računa na socialnih omrežjih?

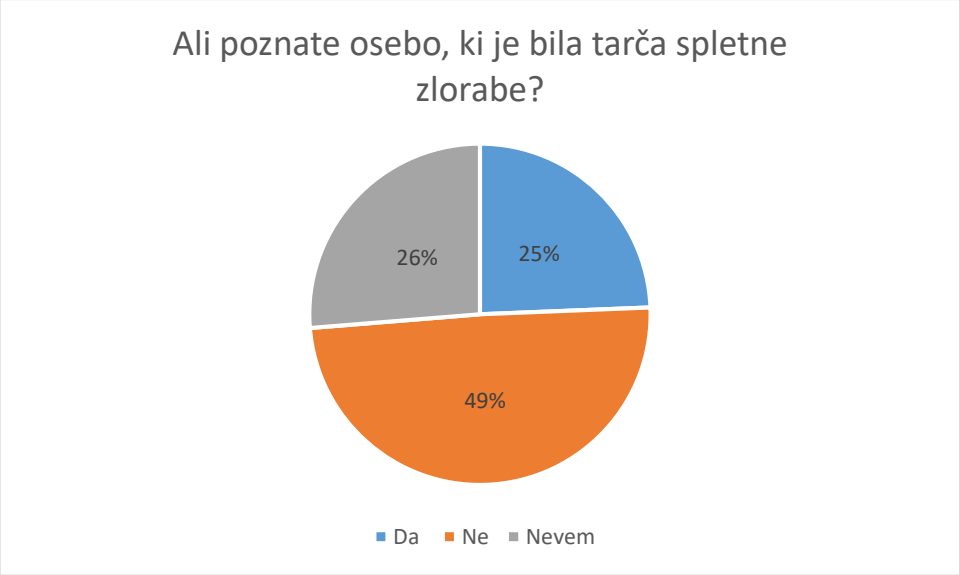


Večina učencev (88 %) uporablja elektronsko pošto in račune na socialnih omrežjih, kar sicer ni presenetljivo.

Graf 9: Ali ste že slišali za spletne zlorabe?

Večina učencev (91 %) je že slišala za spletne zlorabe.

Graf 10: Ali poznate osebo, ki je bila tarča spletne zlorabe?



Največ učencev (49 %) ne pozna osebe, ki je bila tarča spletne zlorabe.

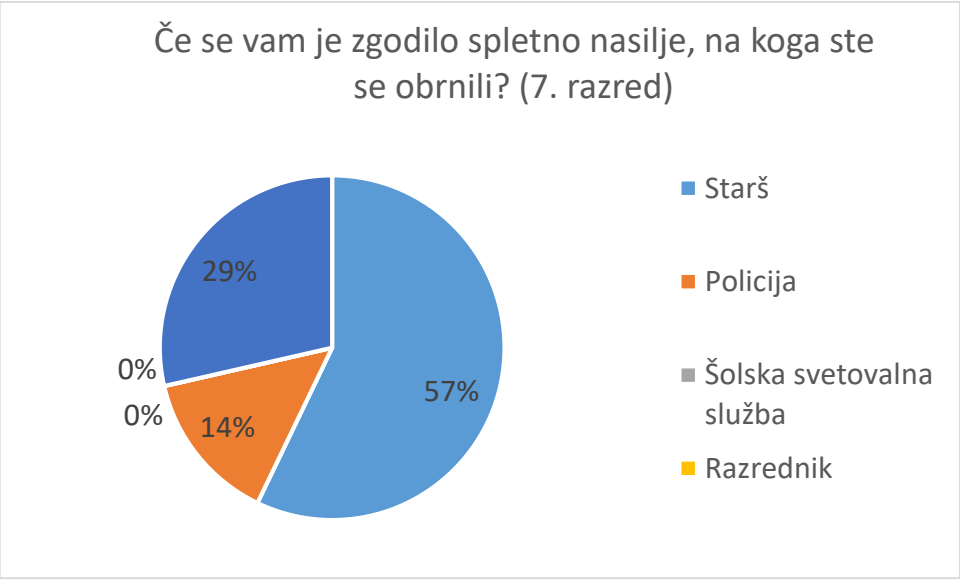
Graf 11: Ali ste že bili žrtev spletnega nasilja?

Največ (78 %) učencev ni bilo žrtev spletnega nasilja. Kar 14 % otrok pa je bila žrtev spletnega nasilja.

Graf 12: Če se vam je zgodilo spletno nasilje, na koga ste se obrnili? (6. razred)

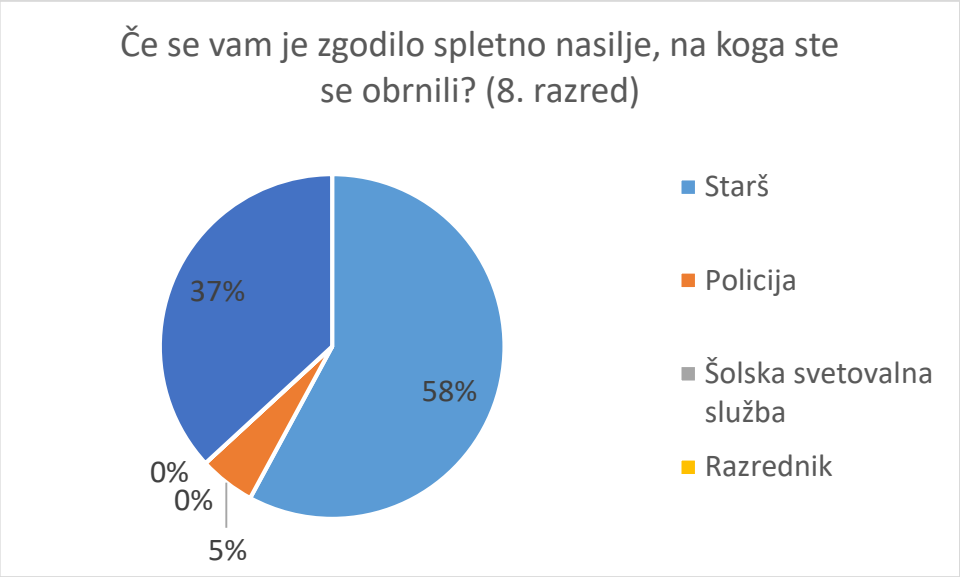
V 6. razredu je največ učencev odgovorilo, da so se obrnili na starše (69 %), nekaj pa jih je odgovorilo, da so se obrnili na šolsko svetovalno službo (23 %).

Graf 13: Če se vam je zgodilo spletno nasilje, na koga ste se obrnili? (7. razred)



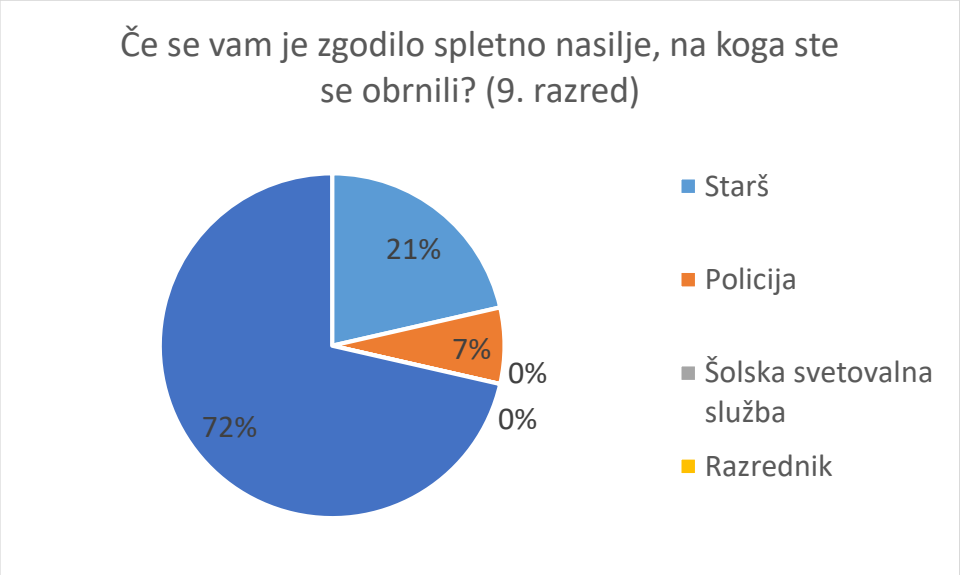
V 7. razredu je največ učencev odgovorilo, da so se obrnili na starše (57 %), nekaj pa tudi, da so se obrnili na policijo (14 %).

Graf 14: Če se vam je zgodilo spletno nasilje, na koga ste se obrnili? (8. razred)



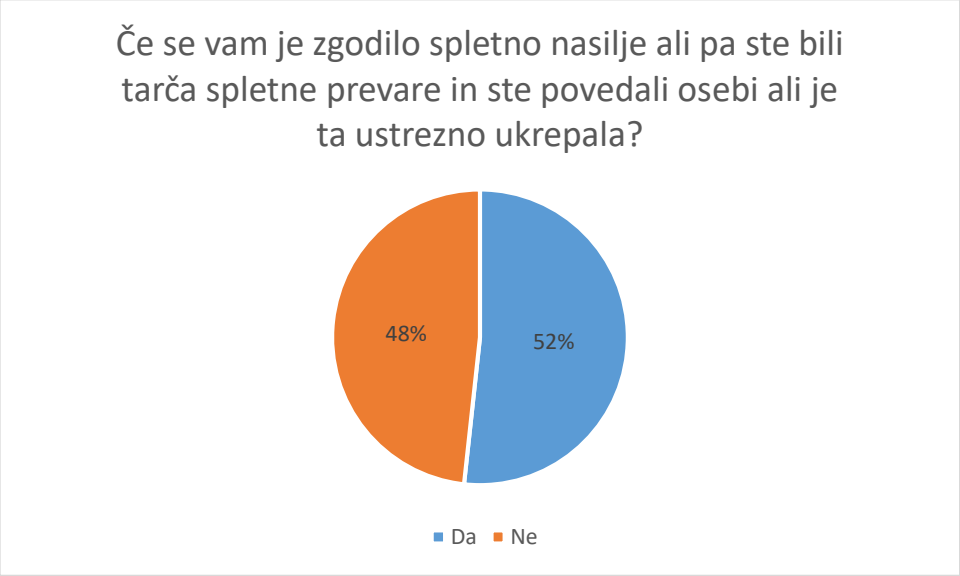
V 8. razredu je večina učencev odgovorila, da so se obrnili na starše (58 %).

Graf 15: Če se vam je zgodilo spletno nasilje, na koga ste se obrnili? (9. razred)



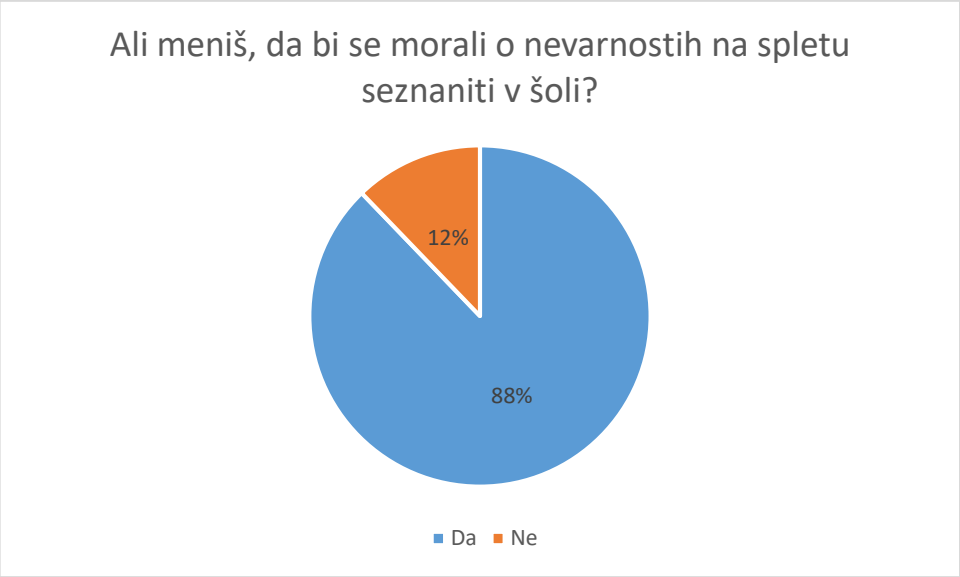
V 9.razredu so učenci odgovorili, da so se obrnili na starše (21 %), nekaj pa tudi na policijo (7 %).

Graf 16: Če se vam je zgodilo spletno nasilje ali pa ste bili tarča spletne prevare in ste povedali osebi, ali je ta ustrezno ukrepala?



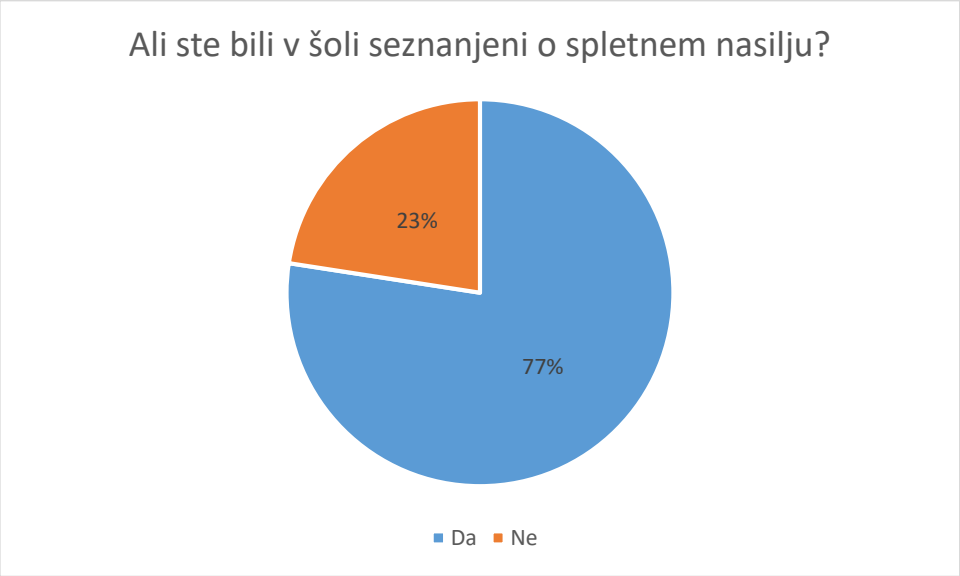
Večina učencev (52 %) meni, da je oseba, ki so ji povedali, da so bili tarča spletne zlorabe, ustrezno ukrepala. Visok je odstotek tistih, ki imajo slabo izkušnjo z osebo, ki so ji zaupali. Navedeno pomeni, da starši nimajo zadostnega znanja za pravilno ukrepanje v teh situacijah.

Graf 17: Ali meniš, da bi se morali o nevarnostih na spletu seznaniti v šoli?



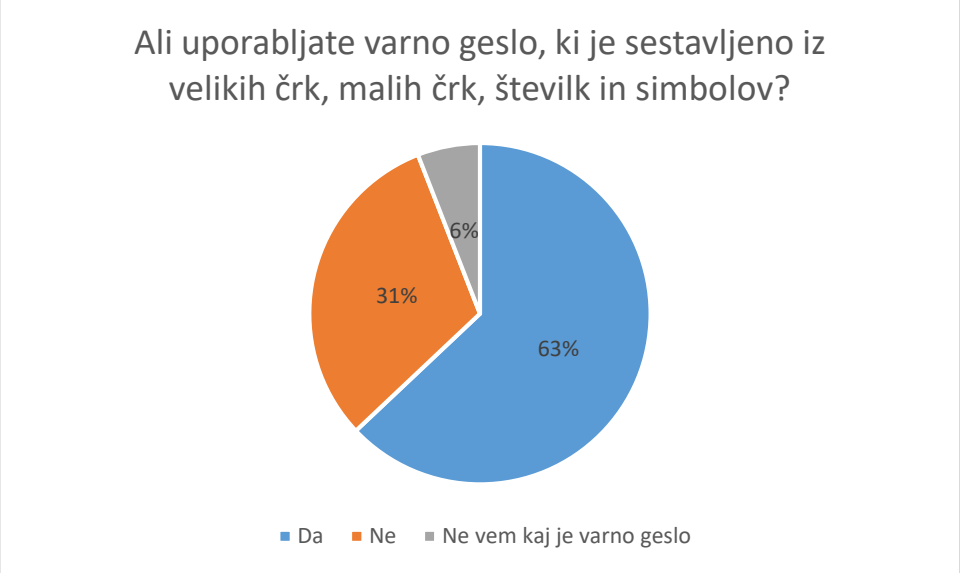
Večina učencev (88 %) meni, da bi se morali o nevarnostih na spletu seznaniti v šoli.

Graf 18: Ali ste bili v šoli seznanjeni o spletnem nasilju?



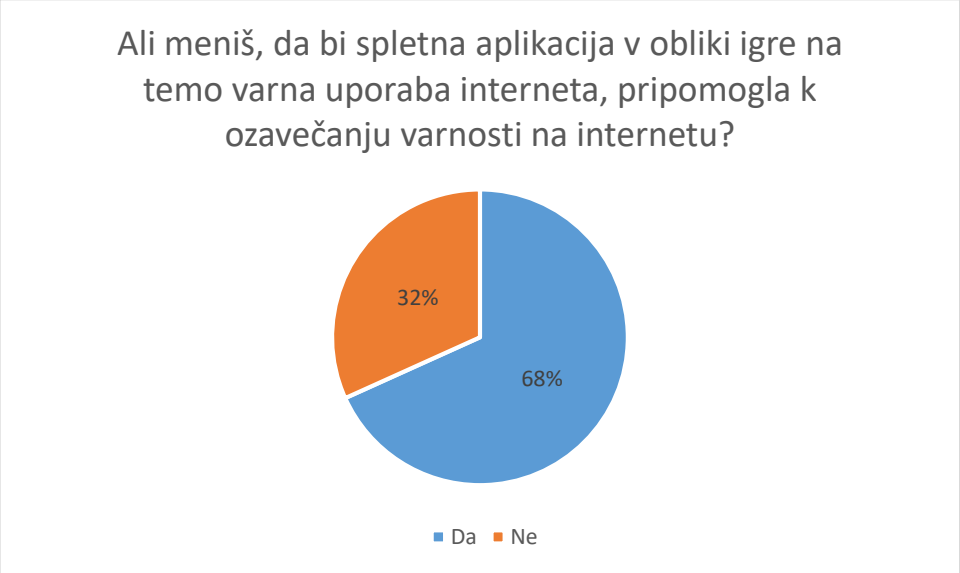
Večina učencev (77 %) je bila o spletnem nasilju seznanjena v šoli. Sama sva bila o spletnem nasilju seznanjena v šoli, in sicer v okviru razrednih ur ter pouku izbirnega predmeta računalništva.

Graf 19: Ali uporabljate varno geslo, ki je sestavljeno iz velikih in malih črk, številk in simbolov?



Večina učencev (63 %) uporablja varno geslo.

Graf 20: Ali meniš, da bi spletna aplikacija v obliki igre na temo varna uporaba interneta pripomogla k ozaveščanju varnosti na internetu?



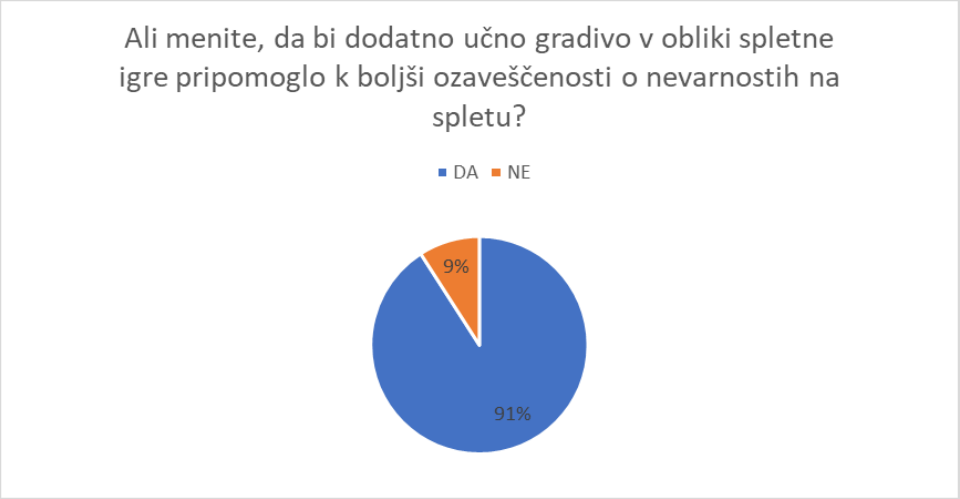
Večina učencev (68 %) meni, da bi spletna aplikacija v obliki igre na temo varna uporaba interneta pripomogla k ozaveščanju varnosti na spletu.

4.2. Rezultati ankete za svetovalne delavce

Graf 21: Ali menite, da so otroci in mladostniki o nevarnostih na spletu zadostno ozaveščeni?

Večina (82 %) anketirancev meni, da otroci niso zadostno ozaveščeni o nevarnostih na spletu, ostali (18 %) pa menijo, da so otroci zadostno ozaveščeni.

Graf 22: Ali menite, da bi dodatno učno gradivo v obliki spletne igre pripomoglo k boljši ozaveščenosti o nevarnostih na spletu?

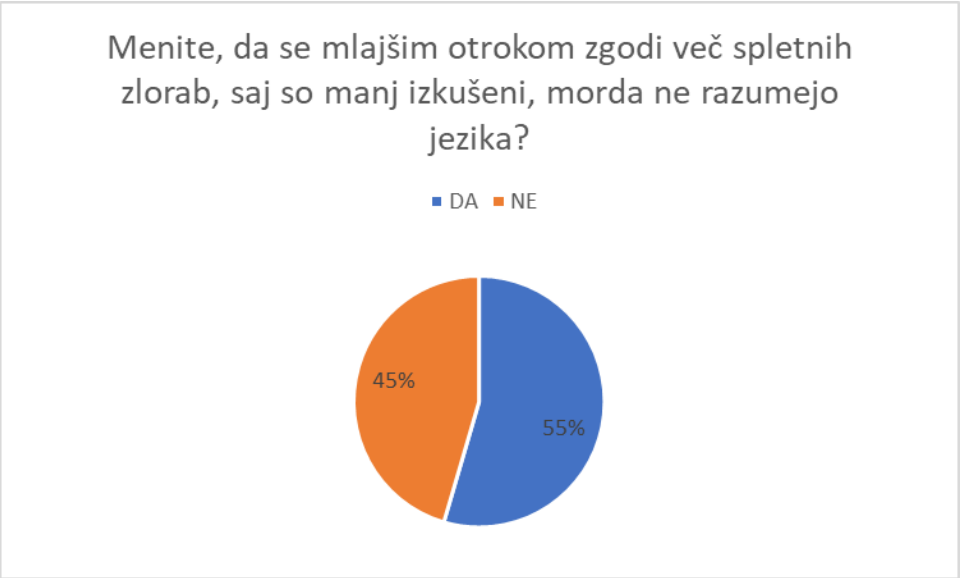


Skoraj vsi (91 %) anketirancev meni, da bi spletna igra pripomogla k boljši ozaveščenosti na spletu.

Graf 23: Katere oblike spletnega nasilja največkrat zaznate?

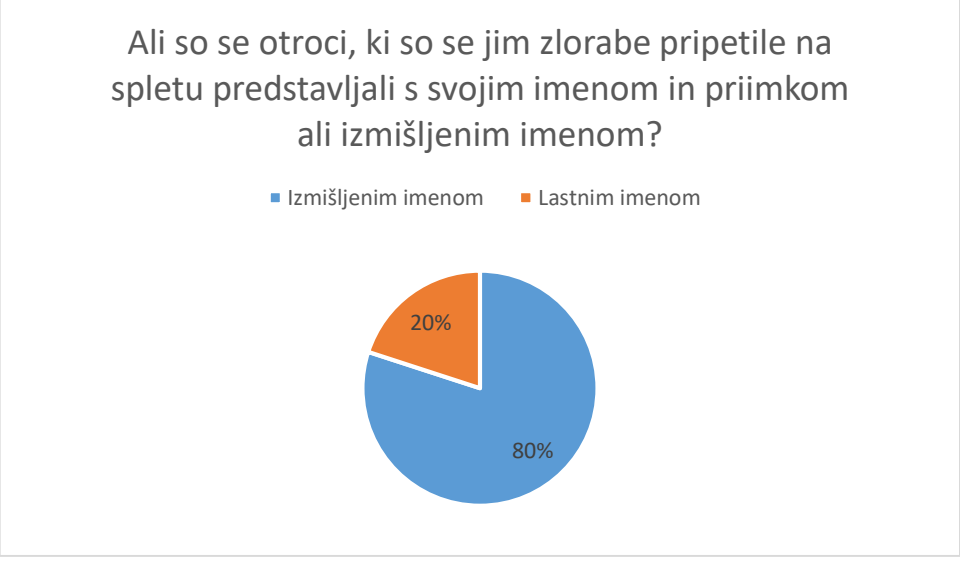
Svetovalni delavci so pri svojem delu največkrat zaznali žaljenje (27 %) kot obliko spletnega nasilja. Nadalje se spletno nasilje pogosto kaže kot izključevanje iz skupin (22 %), kar se pogosto pojavlja tudi v vsakdanjem življenju. Na spletu pa so otroci in mladostniki pogosto izključeni iz pogovorov v skupinah na družbenih omrežjih ter igranja spletnih iger v skupinah. 15 % anketirancev je odgovorilo, da so pogoste oblike spletnega nasilja tudi izzivanja in fotografiranje, snemanje ter objava posnetkov brez dovoljenja. Slednje je še posebej zaskrbljujoče, saj fotografije in posnetki na spletu ostajajo in jih je skoraj nemogoče odstraniti. Redkeje se pojavi ustrahovanje (12 %), v tej starostni skupini se je spletno nasilje v obliki deljenja intimnih posnetkov in izsiljevanje z intimnimi posnetki zaznalo zgolj v 5 %.

Graf 24: Menite, da se mlajšim otrokom zgodi več spletnih zlorab, saj so manj izkušeni, morda ne razumejo jezika?



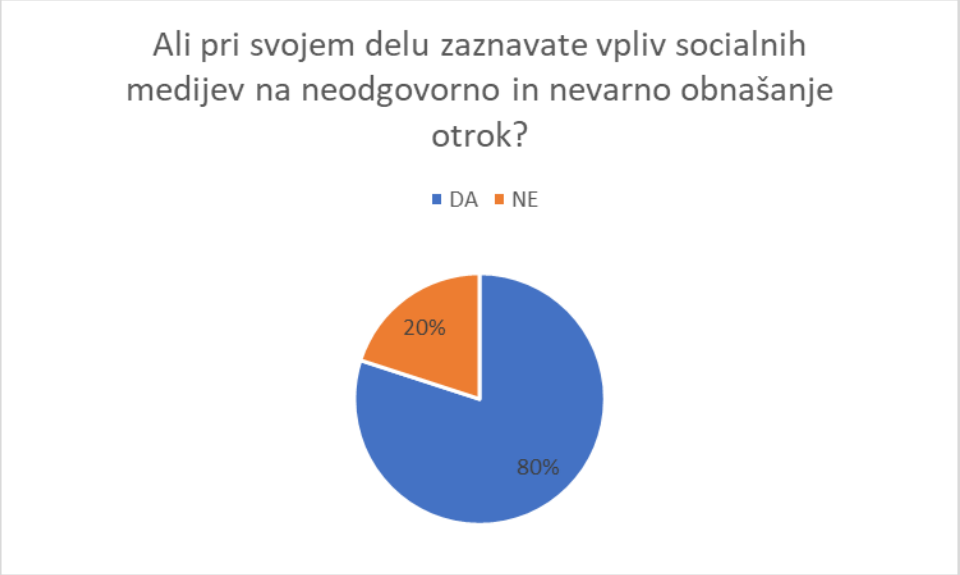
Več anketirancev je odgovorilo z da (55 %), 10 % manj pa jih je odgovorilo z ne (45 %).

Graf 25: Ali so se otroci, ki so se jim zlorabe pripetile na spletu, predstavljali s svojim imenom in priimkom ali izmišljenim imenom?



Anketiranci so odgovorili, da jih je večina uporabljala svoje osebne podatke (80 %), 20 % pa jih je uporabljala izmišljene podatke. Navedeno kaže na pomanjkljivo zavedanje otrok in mladostnikov o varnem obnašanju na spletu.

Graf 26: Ali pri svojem delu zaznavate vpliv socialnih medijev na neodgovorno in nevarno obnašanje otrok?

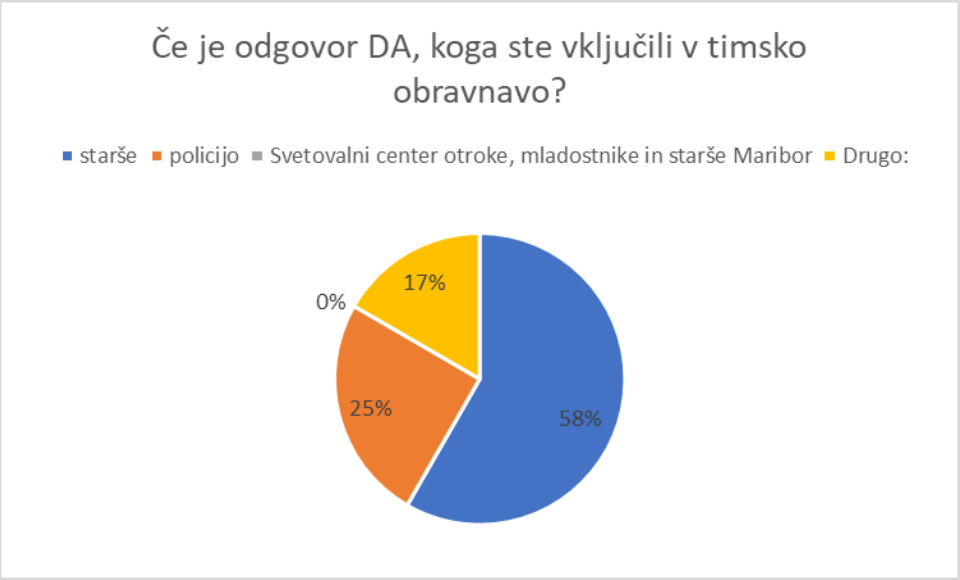


80 % anketirancev je zaznala vpliv socialnih medijev na neodgovorno in nevarno obnašanje otrok na spletu, 20 % anketiranih pa vpliva ni zaznala.

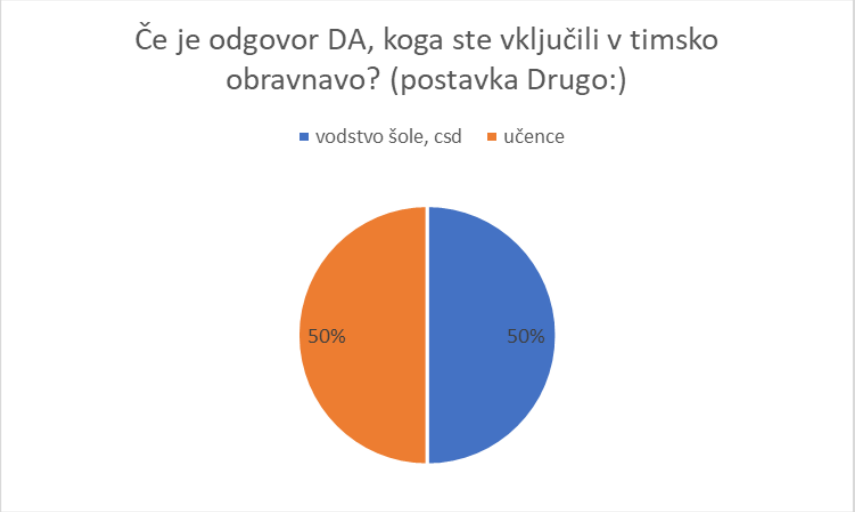
Graf 27: Ali ste v šolskem letu 2020/2021 obravnavali primer spletnega nasilja med učenci?

85 % anketirancev je v šolskem letu 2020/2021 obravnavala primer spletnega nasilja med učenci, 15 % pa jih tega ni obravnavalo.

Graf 28: Če je odgovor DA, koga ste vključili v timsko obravnavo?



Graf 29: Če je odgovor DA, koga ste vključili v timsko obravnavo? (postavka Drugo)



Največ jih je v timsko obravnavo vključilo starše (58 %), manj jih je vključilo policijo (25 %). Strokovni delavci se niso obrnili na Svetovalni center za otroke, mladostnike in starše Maribor. Nekaj (17 %) pa jih je v timsko obravnavo vključilo tudi vodstvo šole in učence.

4.3. Intervju s predstavnikom PU Maribor

Intervju smo opravili s predstavnikom policijske uprave Maribor Borutom Zalokarjem, kriminalističnim inšpektorjem specialistom SKP I., ki zadnjih 11 let dela na področju računalniškega preiskovanja oz. računalniške kriminalitete.

Veliko nevarnosti na spletu preži na najstnike, vendar je tudi veliko društev, združenj, zavodov, ki poskušajo pomagati otrokom in najstnikom, da se lažje znajdejo. Otroci imajo toliko izkušenj, kolikor jih skozi življenje pridobijo, in so pri vsakem otroku drugačne. V Sloveniji nimamo uzakonjenega kaznivega dejanja, ki bi neposredno obravnavalo medvrstniško nasilje na spletu. Kadar se dogodek preko spleta prijavi policiji, se v postopku raziskave ugotavlja elemente obstoječih kaznivih dejanj, ki so predpisana v kazenskem zakoniku ali pa v določenih zakonih, ki obravnavajo prekrške, zato se medvrstniško nasilje, ki ga obravnava policija, kaže skozi različna kazniva dejanja. Najhujša oblika posledice medvrstniškega nasilja je samomor. Ker policija statističnih podatkov o medvrstniškem nasilju ne vodi, je težko povedati, je pa razumljivo, da so otroci oz. najstniki manj izkušeni z dogajanjem na spletu, komunikacijo preko spleta in so manj seznanjeni z vsemi pastmi, ki jih internet premore. Zlorabe, ki se dogajajo otrokom na spletu, so pogosto posledica objave pravih podatkov, ki jih otroci zaradi neizkušenosti vpisujejo v razne spletne portale. Socialni/družbeni mediji močno vplivajo na neodgovorno ravnanje odraslih, zato težko rečemo, da ne vpliva na neodgovorno in nevarno obnašanje otrok oz. najstnikov. Izkazal je naklonjenost dodatnemu izobraževanju otrok in mladostnikom s področja računalništva, vpeljavi igre v učni proces, saj bi to povečalo varno obnašanje otrok na spletu.

4.4. Intervju s Točko osveščanja o varni rabi interneta Safe.si.

Intervju s predstavnikom Točke osveščanja o varni rabi interneta Safe.si, Markom Puschnerjem, s Fakultete za družbene vede Univerze v Ljubljani.

Osveščanje o varni rabi interneta je nikoli dokončano delo. Neprestano prihajajo nove generacije, ki nimajo ustreznih znanj in jih je treba informirati. Opažamo pa, da je ozaveščenost v višjih razredih osnovne šole in v srednjih šolah vedno boljša, kar je posledica vedno bolj zgodnjega ozaveščanja in vseh ozaveščevalnih aktivnosti, ki jih slovenske šole izvajajo. Ker pa se pojavljajo vedno nove oblike tveganj na spletu, je

ozaveščanje ves čas potrebno. Najpogostejše oblike spletnega nasilja med osnovnošolci: širjenje neresničnih govoric, prejemanje sporočil z neprimerno vsebino, žaljivi ali nesramni komentarji o videzu žrtve, prejemanje sporočil, ki povzročajo strah, grožnje, deljenje posnetkov, ki niso namenjeni javnosti. Mlajši otroci so bolj izpostavljeni tveganju za spletno nasilje in spletne zlorabe, ker so manj vešči uporabe interneta, vendar imajo običajno omejen dostop do interneta in so pod večjim nadzorom staršev. Ocenjujemo, da so najbolj izpostavljeni spletnim zlorabam predvsem mlajši najstniki, ker so intenzivni uporabniki interneta. Na Safe.si opažamo, da se zlorabe dogajajo ne glede na to, ali se žrtev predstavlja z imenom in priimkom ali izmišljenim imenom. Družbena omrežja, kot vodilne platforme za takšne vsebine, imajo zelo velik vpliv na to in so posredno kriva za marsikateri tragični dogodek.

5. PREDSTAVITEV SPLETNE IGRE ZA OTROKE

5.1. Namen spletne igre

Uporaba iger v izobraževanju je v uporabi že nekaj desetletij. Z igro podprto poučevanje (ang. game-based learning) bo osnovnošolcem približalo obravnavano tematiko in jih pritegnilo k dodatnemu izobraževanju. Takšen način poučevanja bi predstavljal povečanje učinkovitosti učenja. Igrifikacija tako lahko popolnoma spremeni način učenja učencev. Gre za novejši koncept motiviranja, ki izhaja iz sveta informacijskih tehnologij, iger in spletnih igric. (povzeto po : Becker, K. (2018). What's the difference between serious games, educational games, and game-based learning? nazadnje obiskano dne 28.1.2022 http://minkhollow.ca/beckerblog/2018/02/03/whats-the-differencebetween-serious-games-educational-games-and-game-based-learning/comment-page-1/)

5.2. Analiza obstoječega stanja

Pri pregledu vsebin, ki so obravnavane pri izbirnem predmetu računalništva, spletnih strani, ki mlade učijo o varni uporabi interneta (kot npr. Safe.si), ugotavljamo, da med gradivi ni zaslediti spletne igrice v slovenskem jeziku, ki bi lahko bila uporabljena kot učno gradivo za tematiko varne uporabe interneta. Tako glede napovedi o širjenju vsebin izobraževanja s področja računalništva in vpeljave teh vsebin v obvezni program predlagamo uporabo z igro podprtega poučevanja, ki bi pomenilo pozitiven doprinos. V ta namen smo razvili osnovno spletno igro, ki osnovnošolce uči varnega vedenja na spletu.

5.3. Uporabljene tehnologije in orodja

V tem poglavju bomo na kratko predstavili tehnologije, ki smo jih uporabili pri snovanju naše spletne igre.

5.3.1. Označevalni jezik HTML

HTML je kratica za Hypertext Markup Language in je jezik, ki ga zna brati spletni brskalnik. Namenjen je ustvarjanju besedila in vsebine v brskalniku. Jezik je sestavljen iz sestavnih delov, ki jih imenujemo oznake. Te določajo elemente in so berljive tudi ljudem.

Vendar je njihov glavni namen, da jih zna prebrati in prikazati spletni brskalnik. Kot primer navedimo oznako <p>, ki označuje odstavek, ali oznako <img>, ki označuje sliko. Dokumenti HTML so shranjeni v datotekah s končnico .html.

Pri razvoju spletna igre smo uporabili elemente, ki jih opisujemo v nadaljevanju.

Glava dokumenta HTML (oznaka `<head>`) je del, ki se ob nalaganju strani ne prikaže v spletnem brskalniku, a vsebuje podatke, kot so <title>, ki označuje naslov strani, povezave do oblikovnih predlog CSS (za potrebe oblikovanja dokumentov HTML) in druge metapodatke. Znotraj elementa `<head>` pogosto umestimo element `<meta>`, ki določa metapodatke o dokumentu HTML. Metapodatki so podatki o podatkih. Običajno se uporabljajo za določitev nabora znakov, opisa strani, ključnih besed, avtorja dokumenta in nastavitev prikaza. Metapodatki niso prikazani na strani, vendar jih je mogoče strojno razčleniti. Metapodatke uporabljajo brskalniki za namene kako prikazati vsebino ali ponovno naložiti stran, iskalniki v obliki ključnih besed in druge spletne storitve. HTML-element `<link>` je namenjen definiranju povezav, s katerimi lahko v dokument dodamo povezavo do zunanjih spletnih virov ali vključujemo zunanje gradnike v HTML. V okviru spletne igre smo na tak način vključili knjižnico Bootstrap ter oblikovno predlogo CSS.

Kot že omenjeno, HTML-element `<title>` določa naslov dokumenta, ki je prikazan v naslovni vrstici brskalnika ali zavihku strani. Vsebuje samo besedilo, medtem kot se oznake znotraj elementa ne upoštevajo. Element `<body>` predstavlja vsebino dokumenta in je lahko samo en v dokumentu. Element `<main>` predstavlja prevladujočo vsebino znotraj elementa `<body>`. Glavno vsebinsko področje sestavlja vsebina, ki je neposredno povezana z osrednjo temo dokumenta. Element je splošni vsebnik za vsebino. Na vsebino ali postavitev ne vpliva, dokler ni na kakršenkoli način oblikovan s pomočjo oblikovne predloge CSS. HTML določa naslove v spletnem dokumentu z uporabo šestih naslovnih elementov `<h1>` do `<h6>`. Besedilna vsebina elementa `<h1>` ima večjo velikost pisave kot druge oznake naslovov. Velikost pisave se od oznak `<h1>` do `<h6>` zmanjšuje. Element `<p>` predstavlja odstavek, ki je običajno blok besedila, od sosednjih blokov ločen s praznimi vrsticami. Odstavki v HTML-dokumentu so v splošnem lahko tudi druge strukture, kot so slike ali obrazci. Element `<button>` predstavlja gumb, ki ga je mogoče klikniti in se lahko, na primer, uporablja za pošiljanje obrazcev. Videz gumbov

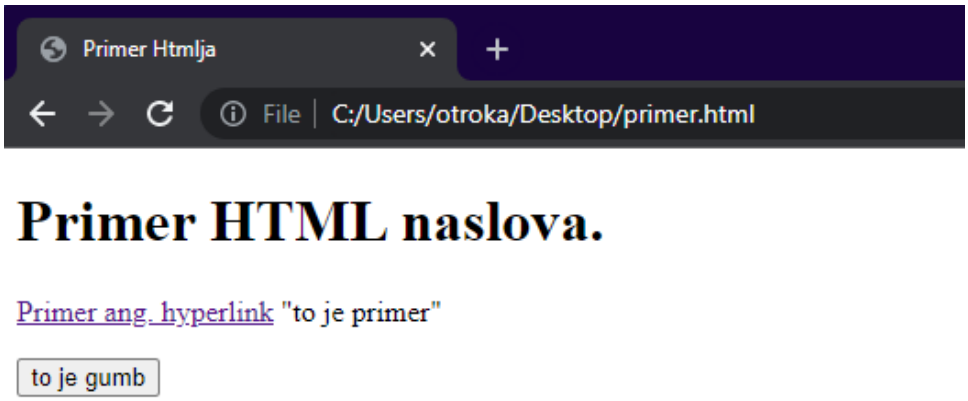
lahko spremenimo s predlogo CSS. Prav tako lahko določenim elementom HTML dodajamo t. i. atribute.

Spodaj je naveden primer HTML-dokumenta z vsemi opisanimi elementi (Programska koda 1).

```
<!DOCTYPE html>
<html>

    <head>

        <meta charset="utf-8">

        <!-- to je komentar v HTML dokumentu-->

        <link href="https://www.google.com">

        <link rel="stylesheet" href="oblikovanje.css">

        <title> Primer Htmlja </title>

    </head>

    <body>

        <main>

            <div>

                <h1>

                    Primer HTML naslova.

                </h1>

                <p>

                    "to je primer"

                </p>

                <button type="button">to je gumb</button>

            </div>

        </main>

    </body>

</html>
```

Programska koda 1: Primer osnovnega HTML-dokumenta

Ko zgoraj naveden dokument odpremo v brskalniku, izgleda tako:



Slika 10: Izgled preprostega HTML-dokumenta v brskalniku.

Atribut `class` se pogosto uporablja za usmerjanje na ime razreda v oblikovni predlogi CSS. Uporablja se lahko tudi v programskem jeziku Javascript za dostop do elementov z določenim imenom razreda, torej atributa `class`, in njihovo obdelavo. Podobno vlogo igra tudi atribut `id`, ki določa edinstven identifikator elementa HTML. Vrednost atributa `id` mora biti edinstvena v določenem dokumentu HTML. Uporablja se za usmerjanje na določeno definicijo oblike znotraj oblikovne predloge CSS. Atribut `id` lahko uporablja tudi JavaScript za dostop do elementa, ki ima določen `id` in njegovo spreminjanje. Primer uporabe atributov prikazuje Programska koda 2.

(povzeto po https://www.w3schools.com/html/html_intro.asp, nazadnje obiskano 28. 1. 2022)

```
<div class="text-center">
        <div id="vprasanje-ena">
          Primer vprašanja 2
        </div>
        <div id="vprasanje-dva">
          Primer vprašanja 1
        </div>
</div>
```

Programska koda 2: Primeri uporabe atributov v HTML dokumentu

5.3.2. Označevalni jezik CSS

CSS je kratica za (ang. Cascading Style Sheets) in je jezik, ki dopolnjuje vsebino v jeziku HTML, za lepšo in bolj privlačno predstavitev. To izvedemo tako, da HTML-datoteko povežemo z datoteko CSS. Vanjo lahko, na primer, vpišemo barvo in vrsto pisave določenih delov, kot so naslovi in odstavki.

```
<link rel="stylesheet" href="oblikovanje.css">
```

Programska koda 3: Vključevanje oblikovne predloge CSS

Spodnja oblikovna predloga CSS v prvem razdelku definira, da je HTML-element `<h1>` druge barve, ki jo definiramo s pomočjo lastnosti `color`. V tem primeru je element modre barve. Prav tako je za element `<p>`, ki označuje besedilne odstavke, definirano, da so ležeče pisani, zelo veliki in rumene barve. Zadnja definira lastnost se nanaša na vse gumbe na spletni strani oz. HTML-elemente `<button>`. Za te elemente je definirana barva ozadja (temno oranžna), neviden rob gumba, barva besedila, sredinska poravnava in velikost pisave (16 točk).

```
h1 {
    color: blue;
    ;
}
p {
    font-style: italic;
    font-size: xx-large;
    color: yellow;
}
button {
    background-color: darkorange;
    border: none;
    color: white;
```

```
    text-align: center;
    font-size: 16px;
}
```

Programska koda 4: Primer oblikovne predloge CSS

V spletni igri smo uporabili knjižnico Bootstrap za oblikovanje.

5.3.3. Javascript

Javascript je programski jezik, s katerim smo izdelali našo spletno igro. Javascript je najbolj priljubljen oziroma uporabljen programski jezik, ki je enostaven za uporabo in prijazen uporabnikom, lahko sodeluje s HTML-kodo in s tem poživi stran z dinamičnem izvajanjem. V naši spletni igro smo, na primer, z Javascriptom dodali gumb, ki začne novo igro. Javascript je eden od treh programskih jezikov, za katere je priporočljivo, da se jih izdelovalci spletni strani naučijo. Je brezplačen in ga ni potrebno naložiti, saj ga zna izvajati vsak spletni brskalnik, ki se nahaja na računalnikih, mobilnih telefonih in tabličnih računalnikih.

Javascript vsebuje različne gradnike. Med osnove štejemo spremenljivke ter polja. Spremenljivke definiramo z besedo let. Spodaj je naveden primer:

```
let avto = renault;
```

Polja pa so spremenljivke, ki lahko imajo več vrednosti. Navedimo primer polja:

```
let = ['jože', 'ana', 'janez', 'marjetka']
```

V naši spletni igri smo uporabili tudi Javascriptove zanke, kot je zanka for, ki ponavlja del kode, dokler se ne doseže logični pogoj.

Pogojni stavek `if-else`

Prav tako smo uporabili pogojne stavke tipa `if-else` To izvede določeno kodo le, ko je določen pogoj izpolnjen. Ponovno navajamo primer spodaj:

```
if (x = y)
{
   alert('x je enako y')
```

```
}
```

Pogoj else je dodatek pogoju if. Če se pogoj if ne izpolni, se izvede kod pod izrazom else, kot je zapisano v spodnjem primeru:

```
if (x = y)
{
   alert('x = y')
}
else
{
   alert('x /= y')
}
```

V naši igri smo uporabili tudi programske zanke. Te ponavljajo določen sklop programske kode, dokler ni izpolnjen določen pogoj. Ti pogoji vključujejo logični vrednosti `true` ali `false`. Vsaka znanka ima začetek, med izvajanjem pa se določene spremenljivke spreminjajo znotraj zanke. Ko je pogoj izpolnjen, se lahko izvajanje programske kode nadaljuje za zanko.

Zanka `while`

Je najpreprostejša oblike zanke in jo zapišemo tako:

```
while (pogoj)
{
stavek/stavki
}
```

JavaScript najprej preveri pogoj, ki mora biti zapisan v oklepajih, in če je ta izpolnjen, izvrši stavek, ki sledi. Nato ponovno preveri pogoj, in če je ta še vedno izpolnjen, izvrši stavek še enkrat in ponovno preveri pogoj. Ko pogoj ni več izpolnjen, nadaljuje s stavkom, ki sledi zanki. V primeru, da pogoj že pri prvem preverjanju ni izpolnjen, se stavek v zanki sploh ne izvrši. V primeru zanke `while` pogosto uvedemo pomožno spremenljivko, s katero štejemo, kolikokrat se zanka izvrši. To spremenljivko imenujejo tudi števec.

Zanka `for`

Je najpogosteje uporabljana zanka v JavaScriptu. Je zelo uporabna struktura, saj lahko sproti vodi število ponovitev stavka znotraj sebe.

```
for ([zacetni izraz]; [pogoj]; [spreminjanje spremenljivke])
{
stavek/stavki
}
```

Oglati oklepaji pomenijo, da je element lahko prisoten, ni pa nujno. Prvi del običajno določa začetno vrednost spremenljivke. Pogoj - enake vrste pogoj, kot smo ga videli pri stavkih `if`. Definira pogoj, ki poskrbi za izvajanje ali prekinitev pogoja in tako preprečuje brezkončno ponavljanje zanke. Na zadnjem mestu je stavek, ki se izvede vedno, ko je pogoj še izpolnjen.

Spreminjanje elementov HTML

V okviru naloge smo tudi uporabili dostop do elementov HTML s pomočjo Javascripta. Kot primer navedimo ukaz `document.getElementById("opis-vprasanje-test").style.display = "block"`, ki dostopa do elementa z `id`-jem `opis-vprasanje-test`, in ta element HTML prikaže kot blok, kar pomeni, da zajema celoten zaslon. Atribut `id` mora biti unikaten za vsak element HTML. Kot drugi primer navedimo ukaz `document.getElementsByClassName("kos-cloveka")`, ki dostopa do elementa z atributov `class`-jem `kos-cloveka`. Atribut `class` pa pripada skupini elementov HTML, ki jim določimo razred. Kot zadnji primer uporabe spreminjanja HTML-ja z Javascriptom navedimo `napacneCrkeDiv.innerHTML`, ki elementu z id-jem `napacneCrkeDiv` določi vrednost znotraj HTML-značk. V tem primeru elementu `<div>`.

5.3.4. Bootstrap

V kolikor opazite, da se spletna stran prikazuje drugače na mobilnem telefonu ali tabličnem računalniku kot na računalniku in celotna vsebina na tabličnem računalniku ali mobilnem telefonu ni v celoti ni vidna oziroma berljiva, snovalcem spletne strani svetujemo uporabo sistema Bootstrap. Ta bo poskrbel za enako velikost, obliko in vidno vsebino spletne strani na vseh napravah.

Bootstrap je brezplačna, odprtokodna knjižnica, kar pomeni, da si lahko vsi ogledajo njegovo izvorno kodo. Je sistem za oblikovanje in le-to olajša – podobno kot CSS.

Razvijalcem pomaga predvsem z vnaprej določenimi razredi in drugimi postavitvami. Sistem Bootstrap omogoča ustvarjanje in upravljanje več prikazov za različne velikosti zaslonov (tablica, telefon, računalnik, televizor). Z njim je omogočeno hitrejše snovanje - v našem primeru - spletne igrice. Nam je omogočil tudi olepšavo igrice v smislu barvne sheme, centriranja besedila, dodajanja šolskega logotipa in podobno.

Bootstrap smo v kodo HTML povezali s HTML-jevo značko `<link>`.

```
<link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstr
ap.min.css" rel="stylesheet" integrity="sha384
1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3"
crossorigin="anonymous">
```

Programska koda 5: Vključevanje knjižnice Bootstrap v dokument HTML

5.4. Načrtovanje in predstavitev spletne igre

K učnemu gradivu, ki smo ga pripravili na temo varnosti gesel, za popestritev dodajamo tudi spletno igro na to temo. Izdelava spletne igre se je začela z idejo. Zamislili smo si koncept igre »vislic«, ki bi otrokom pomagala pri učenju varne uporabe spleta. Odločili smo se za uporabo tehnologij HTML in CSS ter spletnega programskega jezika JavaScript in pripadajoče knjižnice Bootstrap.

Najprej smo izdelali osnovni koncept igre, ki še ni vseboval tudi učne snovi (vprašanja in odgovori). Nato smo dodali vsebinsko del igre, ki vključuje vprašanja in pripadajoče odgovore.

Spletna igra deluje tako, da igralec pritiska črke na tipkovnici in igra s pomočjo JavaScripta 'posluša', kaj je uporabnik pritisnil oziroma katero črko je vnesel. Ko vnese pravilno črko, le-to zamenja s podčrtaji, napačno ugibane črke pa vpiše v kvadrat za napačne črke ter nariše del možica. Igra se konča, ko je možic dokončno narisan ali pa je igralec pravilno uganil vse črke in ni več podčrtajev.

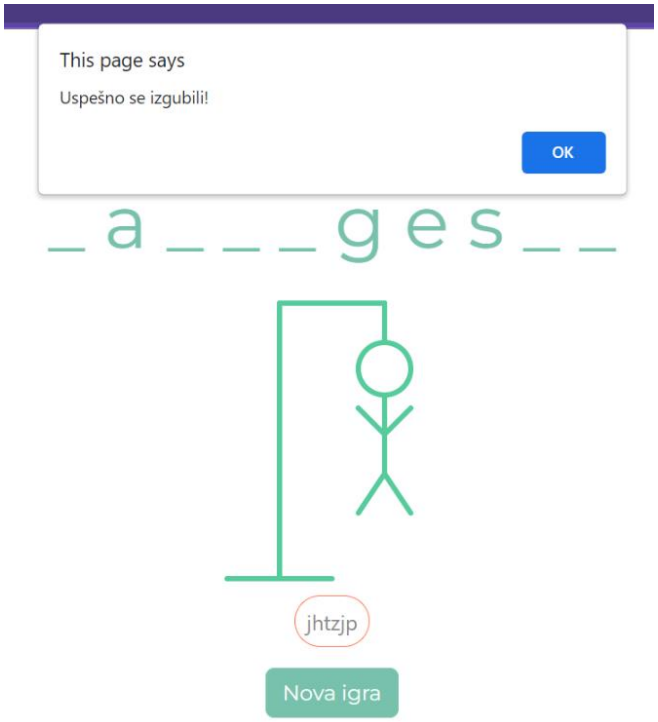
Koda JavaScripta se začne tako, da se spremenljivka `besede` nastavi na besede, ki so možne za ugibanje. Nato koda pogleda dolžino besede in izriše toliko podčrtajev, kot je potrebno. Glede na besedo, ki je v spremenljivki `besede`, izpiše vprašanje nad podčrtaji. Pogleda, ali je v besedi presledek, in na mestu, kjer je presledek, izriše presledek in ne podčrtaja. Nato 'posluša' črke, ki jih vnaša uporabnik. Začetek igre prikazuje Slika 11.

Slika 11: Začetek igre

Če je vnesena črka v besedi, zamenja podčrtaj s to črko. Če črke ni v besedi, pa ugibano črko doda med napačne črke, ki so shranjene v spremenljivki `napacneCrke`. Igra spremlja, ali se v ugibani besedi še nahajajo podčrtaji in kako daleč je možic izrisan, kar je prikazano na Slika 12.

Slika 12: Vpisovanje črk

Če je možic dokončno narisan, je igra izbuljena (Slika 13).



Slika 13: Konec igre v primeru, ko igralec izgubi

Če pa v besedi več ni podčrtajev (je torej v celoti izpisana), pa je igra dobljena in igralcu se še dodatno izpišejo poučne vsebine o ugibani besedi pod sliko možica, kar je prikazano na Slika 14. Ko igralec igro zmaga ali izgubi, se mu tudi izpiše opozorilno okno (angl. alert box), ki igralca o tem obvesti.

Slika 14: Konec igre, v primeru, ko igralec zmaga.

6. RAZPRAVA

6.1. Vrednotenje hipotez

V razpravi bomo analizirali dane hipoteze. Hipoteze bomo potrdili, ovrgli ali le delno potrdili.

Hipoteza 1: Otroci so zadostno ozaveščeni o nevarnostih na spletu.

Hipotezo lahko **ovržemo**, saj je iz ankete za socialne delavce oziroma iz Grafa 1 razvidno, da je večina (82 %) anketirancev menila, da otroci niso zadostno ozaveščeni o nevarnostih na spletu.

Prav tako lahko iz rezultatov ankete, opravljene med učenci, ugotovimo, da je bila večina učencev o nevarnostih na spletu sicer poučena tudi v šolskem okolju (Graf 12), glede na število spletnih zlorab, ki jih obravnavata tudi policija in Točke osveščanja o varni rabi interneta Safe.si, pa ozaveščenost ni zadostna, da bi mlade v večji meri obvarovala pred nevarnostmi na spletu.

Hipoteza 2: Menimo, da učenci nimajo ustrezno zavarovanih računalnikov.

Hipotezo lahko **ovržemo**, saj iz ankete, opravljene med učenci, oziroma iz Grafa 13 izhaja, da večina (63 %) učencev za zaščito spletnih računov uporablja varno geslo. Pripravljeno učno gradivo in spletna igra bi tako lahko pripomogla k višjemu odstotku otrok, ki bi za zaščito uporabljali varno geslo.

Hipoteza 3: Več zlorab na spletu se zgodi mlajšim otrokom, saj so manj izkušeni.

Hipotezo lahko **delno potrdimo,** saj je iz ankete za socialne delavce oziroma iz Grafa 4 razvidno, da večina (55 %) anketirancev meni, da se več zlorab zgodi mlajšim otrokom. Hkrati pa je le 10 % manj anketirancev odgovorilo z ne, zato te hipoteze ne moremo v celoti potrditi.

Hipoteza 4: Večina otrok se na spletne račune ne prijavlja s svojimi dejanskimi osebnimi podatki.

Hipotezo lahko **ovržemo**, saj je iz ankete za socialne delavce oziroma iz Grafa 5 razvidno, da je večina (80 %) anketirancev odgovorila, da so se otroci, ki so se jim zgodile spletne zlorabe na spletu, prijavljali s svojimi osebnimi podatki. Navedeno nam je potrdil tudi

predstavnik policije, gospod Borut Zalokar, kriminalistični inšpektor specialist, ki zadnjih 11 let dela na področju računalniškega preiskovanja oziroma računalniške kriminalitete. Navedel je da so zlorabe, ki se dogajajo otrokom na spletu, pogosto posledica objave pravih podatkov, ki jih otroci zaradi neizkušenosti vpisujejo v razne spletne portale.

Hipoteza 5: Menimo, da bo izobraževalna igra primerna za učence od 5. do 9. razreda.

Hipotezo lahko **potrdimo**, saj je iz ankete za socialne delavce oziroma iz Grafa 2 razvidno, da so skoraj vsi anketiranci (91 %) mnenja, da bi spletna igra pripomogla k boljši ozaveščenosti na spletu. Uporabi iger v izobraževanju so naklonjeni tudi otroci in mladostniki. Večina učencev (68 %) meni, da bi spletna aplikacija v obliki igre na temo varna uporaba interneta pripomogla k ozaveščanju varnosti na spletu.

6.2. Samoevalvacija raziskovalnih metod in raziskovalnega dela

Menimo, da smo pri svojem raziskovalnem delu uporabili veliko raznolikih metod. Literaturo smo uporabljali predvsem pri iskanju podatkov o spletnem nasilju s pomočjo raziskav Točke osveščanja o varni rabi interneta Safe.si. Aktualne podatke smo pridobili z intervjujem s strokovnjakom, kriminalistom za področje spletnega nasilja ter v najnovejših raziskavah na spletu.

Za spoznavanje dejanskega stanja smo izvedli anketi med učenci naše šole in svetovalnimi delavci mariborskih osnovnih šol. Pridobljene podatke smo obdelali in prikazali z grafi.

Za programiranje naše spletne igre smo uporabili brezplačne računalniške programe. Uporabili smo Javascript, CSS, HTML in Bootstrap.

Še posebej smo ponosni na naš izdelek v obliki spletne igre, ki je v slovenskem prostoru unikaten in nam lasten. Menimo, da je izdelek uporaben za učence vseh vzgojno-izobraževalnih obdobij, še posebej za učence od drugega razreda naprej.

Spletno nasilje predstavlja neveščim uporabnikom veliko nevarnost, zato predlagamo vsem, ki se ukvarjajo z mladimi, preizkus in uporabo naše spletne igre, saj ta predstavlja preventivno dejavnost.

7. SKLEP

Pereč problem zlorab in nevarnosti na spletu nas je motiviral, da smo želeli področje bolje spoznati. Podali smo predlog, za katerega menimo, da bi lahko stanje izboljšal na inovativen način, s pomočjo lastne spletne igre, ki bi učence osveščala o varni uporabi interneta.

Pri svojem raziskovalnem delu smo uporabili metodo proučevanja različnih virov in literature, s katero smo pridobili ustrezno predznanje na področju raziskave in informacij o trenutnih načinih izobraževanja o varni rabi interneta. To smo predstavili v teoretičnem delu naloge. V empiričnem delu naloge smo s pomočjo anketnih vprašalnikov, intervjujev ter kasneje metode analize podatkov in njihove interpretacije pridobili veliko informacij o stanju spletnega nasilja in zlorab. Na podlagi ugotovitev smo kot inovacijski predlog razvili lastno spletno igro »vislice«, in sicer s pomočjo tehnologij HTML, CSS in Javascript. Kot nam je znano, je to prva takšna igra v slovenskem jeziku.

S pomočjo anketnih vprašalnikov med učenci in svetovalnimi delavci smo prišli do številnih ugotovitev glede uporabe interneta, socialnih omrežij ter zlorab in spletnega nasilja. Rezultati vprašalnikov so pokazali, da večina otrok ni dovolj ozaveščena o nevarnostih na spletu in o tem, kako se je pri nevarnostih mogoče ustrezno zavarovati. Veliko otrok uporablja družbena omrežja in elektronsko pošto. Problem predstavlja prekomerna uporaba socialnih omrežij in interneta v 3. triadi osnovne šole. Rezultati vprašalnika med učenci naše osnove šole kažejo, da je bilo med njimi le majhno število žrtev spletnega nasilja. Po drugi strani rezultati, pridobljeni s strani svetovalnih delavcev več osnovnih šol, kažejo bolj zaskrbljujoče stanje, saj je bilo zaznanih veliko zlorab na internetu in spletnega nasilja. Mednje sodijo izključevanje iz skupin, žaljenje in izzivanje, nedovoljeno snemanje ter fotografiranje. Prav tako so pogosto zaznali vpliv socialnih medijev na nevarno in neodgovorno obnašanje učencev. Iz intervjujev s predstavnikov PU Maribor ter predstavnikom točke osveščanja o varni rabi interneta Safe.si, ki smo ju izvedli v sklopu naloge, smo dobili potrditev, da so pogost problem predvsem zlorabe posredovanih podatkov uporabnikov.

Iz anketnega vprašalnika je razvidno, da bi se učenci v primeru spletnega nasilja v večini primerov obrnili na starše ali šolsko svetovalno službo.

Večina svetovalnih delavcev meni, da učenci niso zadostno ozaveščeni o nevarnostih na spletu. Tudi ti menijo, da bi se želeli v šoli bolje izobraziti o varni rabi interneta, spletnem nasilju in zlorabah. Oba intervjuvanca in večina svetovalnih delavcev meni, da bi bila naša predlagana spletna igra inovativen način za dvig ozaveščenosti o varni rabi interneta, pripomogla bi k izboljšanju trenutnega stanja in bi jo lahko vpeljali v proces izobraževanja otrok že v šoli, pa tudi širše.

Zaključimo lahko, da bi naš predlog uporabe učnega gradiva, ki bi ga učitelji lahko uporabili v razredu in ga kombinirali z našo spletno igro, pripomogel k večji osveščenosti o varni rabi interneta in s tem zmanjšal število zlorab in nasilja na spletu. V nalogi smo predstavili proces načrtovanja spletne igre ter uporabljene tehnologije. Naš predlog predstavlja nov pristop k izobraževanju otrok s spletnimi igrami v slovenskem prostoru. Predstavljena spletna igra bo dosegljiva za vse potencialne uporabnike na spletni strani naše šole po naših zagovorih.

8. DRUŽBENA ODGOVORNOST

Nevarnost na spletu se zadnja leta pojavlja pogosto in v različnih oblikah. Potrebno se je zavedati, da je splet postal nevarno družbeno okolje za različne vrste starostnih skupin, zato smo pripravili spletno igro, s katero bomo na igriv in poučen način ozaveščali otroke in najstnike o nevarnostih na spletu.

Vsak droben prispevek k razumevanju nevarnosti na spletu pomeni zavedanje in prevzemanje odgovornosti za razvoj družbe in medsebojnih odnosov. Učenje in doživljanje le-tega bi moral vsebovati vsak šolski kurikulum.

Menimo, da bi s pomočjo spletne igre otroci pridobili nova spoznanja, in s tem upamo, da bi preprečili oz. omogočili manj zlorab na spletu.

9. VIRI IN LITERATURA

Knjižni viri:

1. Burnett, M., in Kleiman, D., Perfect passwords: selection, protection, authentication, Syngress, 2006.
2. Pfleeger, C. P., in Pfleeger, S. L., *Security in computing, 4th Edition*, Prentice Hall, 2006.

Spletni viri :

1. safe.si (nazadnje obiskano 10.1.2022)
2. https://www.rtvslo.si/zabava-in-slog/zanimivosti/sokantno-najpogostejse-geslo-letosnjega-leta-je-123456/602473 (nazadnje obiskano, 17.1.2022)
3. https://www.rtvslo.si/zabava-in-slog/zanimivosti/sokantno-najpogostejse-geslo-letosnjega-leta-je-123456/602473, nazadnje obiskano, 17.1.2022).
4. https://nordpass.com/most-common-passwords-list/ (nazadnje obiskano: 17.1.2022)
5. https://www.passwordmonster.com/ 8nazadnje obiskano 29. 1. 2022)
6. povzeto po https://www.passwordmonster.com/ (nazadnje obiskano 17. 1. 2022)
7. https://medium.com/belong-blog/password-101-how-to-create-a-secure-password-8adfbe888d79 (nazadnje obiskano 17. 1. 2022)
8. https://www.w3schools.com/html/html_intro.asp (nazadnje obiskano 28.1.2022)
9. https://www.stopbullying.gov/cyberbullying/what-is-it (nazadnje obiskano 17.1.2022)
10. https://www.unicef.org/end-violence/how-to-stop-cyberbullying (nazadnje obiskano 17.1.2022)
11. https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/spletno-nasilje-in-spolne-zlorabe-otrok-na-internetu/medvrstnisko-nasilje-na-spletu (nazadnje obiskano 15.1.2022)

10. PRILOGE

10.1. Priloga 1: Anketa za učence

Spol

1. Ženski
2. Moški

Kateri razred obiskujete?

6. razred

7. razred

8. razred

9. razred

Ali uporabljate internet in socialna omrežja?

1. Da
2. Ne

Koliko časa dnevno uporabljate internet in socialna omrežja?

1. Ura
2. Uri
3. Ure
4. ure
5. ur
6. ali več ur

Ali ste uporabnik elektronske pošte ali računa na socialnih omrežjih?

1. Da

2. Ne

Ali ste že slišali za spletne zlorabe?

1. Sem že prej vedel/a zanje
2. Nisem, prvič slišim zanje

Ali poznate osebo, ki je bila tarča spletne zlorabe (spletno nadlegovanje, kraja identitete, zloraba gesla, ipd.)?

1. Da
2. Ne
3. Ne vem

Ali ste že bili žrtev spletnega nasilja ?

1. Da
2. Ne
3. Ne vem

Če se vam je zgodilo spletno nasilje na koga ste se obrnili?

1. Starš
2. Policija
3. Šolska svetovalna služba
4. Razrednik
5. Drugo: _____

Če se vam je zgodilo spletno nasilje ali pa ste bili tarča spletne prevare in ste povedali osebi ali je ta ustrezno ukrepala?

1. Da
2. Ne

Ali meniš, da bi se morali o nevarnostih na spletu seznaniti v šoli?

1. Da
2. Ne

Ali ste bili v šoli seznanjeni o spletnem nasilju?

1. Da
2. Ne

Ali uporabljate varno geslo, ki je sestavljeno iz velikih črk, malih črk, številk in simbolov (npr. JjK34@/%FDgs)?

1. Da
2. Ne
3. Ne vem kaj je varno geslo

Ali meniš, da bi vam spletna aplikacija v obliki igre na temo varna uporaba interneta, pripomogla k ozaveščanju varnosti na internetu?

1. Da
2. Ne

10.2. Priloga 2: Anketa za strokovne delavce

Ali menite, da so otroci in mladostniki o nevarnostih na spletu zadostno ozaveščeni?

DA NE

Ali menite, da bi dodatno učno gradivo v obliki spletne igre pripomoglo k boljši ozaveščenosti o nevarnostih na spletu?

DA NE

Katere oblike spletnega nasilja največkrat zaznate?

- Ustrahovanje
- Izzivanje
- Žaljenje
- Izključevanje iz skupin
- Deljenje intimnih posnetkov in izsiljevanje z intimnimi posnetki
- Fotografiranje in snemanje ter objavljanje posnetkov brez dovoljenja
- Izsiljevanje
- Spletni izzivi

Menite, da se mlajšim otrokom zgodi več spletnih zlorab, saj so manj izkušeni, morda ne razumejo jezika?

DA NE

Ali so se otroci, ki so se jim zlorabe pripetile na spletu predstavljali s svojim imenom in priimkom ali izmišljenim imenom?

DA NE

Ali pri svojem delu zaznavate vpliv socialnih medijev na neodgovorno in nevarno obnašanje otrok?

DA NE

Ali ste v šolskem letu 2020/2021 obravnavale primer spletnega nasilja med učenci?

DA NE

Če je odgovor da, koga ste vključili v timsko obravnavo?

- Starše,
- Policija
- Svetovalni center otroke, mladostnike in starše Maribor
- Drugo: _____

10.3. Priloga 3: Intervju z gospodom Borutom Zalokarjem

Gospod Borut Zalokar kriminalistični inšpektor specialist SKP I., ki zadnjih 11 let dela na področju računalniškega preiskovanja oz. računalniške kriminalitete.

Intervju je bil opravljen 13. 12. 2021.

1. Ali menite, da so otroci in mladostniki o nevarnostih na spletu zadostno ozaveščeni?

Veliko nevarnosti na spletu preži na najstnike, vendar je tudi veliko društev, združenj, zavodov, ki poskušajo pomagat otrokom in najstnikom, da se lažje znajdejo. Otroci imajo toliko izkušen koliko jih skozi življenje pridobijo in so pri vsakem otroku drugačne. So odvisno od vsakega posameznika (ozaveščenost o nevarnostih na spletu).

Zavedati se moramo, da je najšibkejši člen vedno posameznik in je njegova ranljivost odvisna od njegove ozaveščenosti.

2. Ali menite, da bi dodatno učno gradivo v obliki spletne igre pripomoglo k boljši ozaveščenosti o nevarnostih na spletu?

Absolutno, ker otroci skozi igro spoznavajo življenje, zaradi tega je tudi spletna igra dober pripomoček k ozaveščenosti. Za igrico bi lahko bile besede npr. ustrahovanje, zloraba, žalitev, kraja identitete, snemanje nasilja, zasmehovanje, izločanje iz skupine, pošiljanje obdelanih slik.

Dodatek k programu, ko nekdo besedo zadene, se napiše pojasnitev te besede.

3. Katere oblike spletnega nasilja največkrat zaznate?

Spletno nasilje policija obravnava takrat, kadar je pri tem zaznati elemente kaznivega dejanja ali prekrška. V Sloveniji nimamo kaznivega dejanja, ki bi neposredno obravnavalo med vrstniško nasilje na spletu. Kadar se dogodek preko spleta prijavi policiji, se v postopku raziskave ugotavlja elemente obstoječih kaznivih dejanj, ki so predpisana v kazenskem zakoniku ali pa v določenih zakonih, ki obravnavajo prekrške.

Zato se med vrstniško nasilje, ki ga obravnava policija, kaže skozi kazniva dejanja grožnje, neopravičenega slikovnega snemanja, zlorabe osebnih podatkov, izsiljevanja, napadov oz. zlorab informacijskega sistema, nasilništva, javnega spodbujanja sovraštva, nasilja ali nestrpnosti, in druga kazniva dejanja, ki so odvisna glede na življenjsko okoliščino dogodka ali nekega dejanja, ki pa ima lahko tudi znake prekrška. Zaradi tega nimamo točnih statističnih podatkov, ker jih konkretno za tako imenovano med vrstniško nasilje ne vodijo (evidence ne vodijo). Ocenjujejo, da je približno med 50 in 120 primerov letno. Najhujša oblika posledice med vrstniškega nasilja je samomor.

4.Menite, da se mlajšim otrokom zgodi več spletnih zlorab, saj so manj izkušeni, morda ne razumejo jezika?

Ker policija statističnih podatkov o med vrstniškem nasilju ne vodi, je težko povedati, je pa razumljivo, da so otroci oz. najstniki manj izkušeni z dogajanjem na spletu, komunikacijo preko spleta, in so manj seznanjeni z vsemi pastmi, ki jih internet premore. Pojem spletnih zlorab je širši pojem od med vrstniškega nasilja na spletu. V pasti interneta, kot so prijave v spletne portale, ki zahtevajo plačilo ali osebne podatke otroka, so najstniki in otroci pri tem bolj ogroženi zaradi pomanjkanja lastnih izkušenj.

5. Ali so se otroci, ki so se jim zlorabe pripetile na spletu predstavljali s svojim imenom in priimkom ali izmišljenim imenom?

Žal tega podatka nimam. Zlorabe, ki se dogajajo otrokom na spletu, so pogosto posledica objave pravih podatkov, ki jih otroci zaradi neizkušenj vpisujejo v razne spletne portale. Pogosto pa tisti najstniki, ki poskušajo izvajat med vrstniško nasilje, lahko uporabljajo izmišljanja imena in se skrivajo za sicer zakonitimi možnostmi interneta. Pri tem sem pogosto zaznava uporaba žalitev, ustrahovanja in drugih oblik prej omenjenega med vrstniškega nasilja. Storilec na ta način poskuša pridobiti nek status med vrstniki, da si upa, da ni mevža ali podobno.

6. Ali pri svojem delu zaznavate vpliv socialnih medijev na neodgovorno in nevarno obnašanje otrok?

Socialni/družbeni mediji močno vplivajo na neodgovorno ravnanje že odraslih, zato težko rečemo, da ne vpliva na negovorno in nevarno obnašanje otrok oz. najstnikov. Lahko si predstavljamo, da to ni njihov osnovni namen družbenih medijev, da bo nekdo na ta način drugega nadlegoval, zasmehoval, žalil, vendar posamezniki kljub temu to pogosto izkoriščajo oz. zlorabijo zato, da postavijo negativno komunikacijo z drugim, ga poskušajo očrniti pred drugimi.

Za obdobje korone ni konkretnih podatkov, lahko pa se naslonimo na odgovor, kam spada in koliko je nasilja v povprečju. Stopnja kaznivih dejanj, ki se izvršijo preko spleta, se je sicer povečala, vendar v kontekstu med vrstniškega nasilja pa je to podatek, ki ga je gospod dal že v prejšnjih odgovorih.

Osebo, ki izvaja nasilje, lahko tudi opozorimo, naj tega ne počne, če pa želimo pomagati, moramo paziti, da se ne znajdemo v tveganem položaju, v katerem bi lahko bili izpostavljeni fizični zlorabi ali nasilju. V takem primeru se moramo vedno obrniti na odraslo osebo.

Pred nasilnežem se nikoli ne zatečemo k nasilju. Več nasilja je skoraj vedno posledica nasilja. Posamezniki, ki so nasilni, pogosto sami potrebujejo pomoč. Nasilnežu lahko resnično omogočimo, da dobi pomoč, če ga razkrijemo.

10.4. Priloga 4: Izvorna koda spletna igre

izvorna koda JavaScript

```
// Seznam besed
let besede = ["varno_geslo","ana","test","zelopametno"];

// Izbira naključne besede iz seznama
let nakljucnoStevilo = Math.floor(Math.random() * besede.length);
let izbranaBeseda = besede[nakljucnoStevilo];
console.log(izbranaBeseda);
if(izbranaBeseda == "varno_geslo"){
  document.getElementById("opis-vprasanje-joze").style.display      =
"block";
}
if(izbranaBeseda == "ana"){
  document.getElementById("opis-vprasanje-ana").style.display       =
"block";
}
if(izbranaBeseda == "test"){
  document.getElementById("opis-vprasanje-test").style.display      =
"block";
}


let napacneCrke = [];

let podcrtajiDiv = document.getElementById("odgovor");

let napacneCrkeDiv = document.getElementById("napacneCrke");

let kosCloveka = document.getElementsByClassName("kos-cloveka");


// Ustvarjanje podčrtajev
let podcrtaji = [];
let ustvariPodcrtaje = () => {
    for (let i = 0; i < izbranaBeseda.length; i++) {
        if(izbranaBeseda[i] != '_') {
            podcrtaji.push('_');
        }
        else {
            podcrtaji.push(' ');
        }
    }
    return podcrtaji;
}
podcrtajiDiv.innerHTML = ustvariPodcrtaje().join(' ');
function sleep (time) {
  return new Promise((resolve) => setTimeout(resolve, time));
}

// Poslušaj tipkovnico
```

```
document.addEventListener('keypress', (event) => {
    let keyCode = event.keyCode;
    let keyWord = String.fromCharCode(keyCode);
    // Preveri, ali je uporabnik vpisal pravilno črko
    if(izbranaBeseda.indexOf(keyWord) > -1) {
        // Dodamo v seznam pravilnih črk

        // Zamenjaj podčrtaj z pravilno črko
        var indexOccurence = izbranaBeseda.indexOf(keyWord, 0);
        podcrtaji[indexOccurence] = keyWord;
        while(indexOccurence >= 0) {
            indexOccurence      =      izbranaBeseda.indexOf(keyWord,
indexOccurence + 1);
            podcrtaji[indexOccurence] = keyWord;
        }
        podcrtajiDiv.innerHTML = podcrtaji.join(' ');


        // Preveri, če je uporabnik že zadel vse črke
        if(podcrtaji.join('') == izbranaBeseda) {

          if(izbranaBeseda == "varno_geslo"){
            document.getElementById("opis-besede-
joze").style.display = "block";
          }
          if(izbranaBeseda == "ana"){
            document.getElementById("opis-besede-ana").style.display
= "block";
          }
          if(izbranaBeseda == "test"){
            document.getElementById("opis-besede-
test").style.display = "block";
          }

          sleep(100).then(() => {
            alert('Uspešno ste zmagali!');
          });

        }
    }
    else {
        // Če uporabnik vpiše napačno črko
        napacneCrke.push(keyWord);
        napacneCrkeDiv.innerHTML = napacneCrke.join('');
        kosCloveka[napacneCrke.length-1].style.display = "block";
        if(napacneCrke.length>=kosCloveka.length){
          sleep(100).then(() => {
            alert('Uspešno se izgubili!');
            location.reload();
          });
        }
    }
});
```

Izvorna koda HTML z vključeno oblikovno predlogo CSS ter knjižnico

```
<!DOCTYPE html>
<html lang="sl" dir="ltr">
  <head>
    <meta charset="utf-8">
    <meta   name="viewport"   content="width=device-width,   initial-
scale=1">
    <title>Ugibanje besed</title>
    <link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstra
p.min.css"            rel="stylesheet"            integrity="sha384-
1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3"
crossorigin="anonymous">
    <link                                              rel="stylesheet"
href="https://bootswatch.com/5/minty/bootstrap.min.css">
    <style media="screen">
    body {
    }
    .figure-container {
      fill: transparent;
      stroke: #56cc9d!important;
      stroke-width: 4px;
      stroke-linecap: round;
    }
    .kos-cloveka {
      display: none;
    }

    #opis-besede-joze,  #opis-besede-ana,  #opis-besede-test,  #opis-
vprasanje-joze, #opis-vprasanje-ana, #opis-vprasanje-test {
      display: none;
    }
    </style>
  </head>
  <body>
    <main class="container my-4">
      <div class="text-center">
         <h3>Ugibanje besed</h3>
        <img src="logo.png" alt="">
        <div id="opis-vprasanje-joze">
          Kako lahko zaščitiomo naše spletne račune ?
        </div>
        <div id="opis-vprasanje-ana">
          Blab bla vprasanje ana bla
        </div>
        <div id="opis-vprasanje-test">
          Blab bla vprasanje test bla
        </div> </div>

      <h1       class="text-center       display-4       text-primary"
id="odgovor"></h1>
```

```
      <div class="text-center">
        <svg height="250" width="200" class="figure-container">
              <!-- stojalo -->
              <line x1="60" y1="20" x2="140" y2="20"></line>
              <line x1="140" y1="20" x2="140" y2="50"></line>
              <line x1="60" y1="20" x2="60" y2="230"></line>
              <line x1="20" y1="230" x2="100" y2="230"></line>
              <!-- glava -->
              <circle    cx="140"    cy="70"    r="20"    class="kos-
cloveka"></circle>
              <!-- telo -->
              <line  x1="140"  y1="90"  x2="140"  y2="150"  class="kos-
cloveka"></line>
              <!-- roke -->
              <line  x1="140"  y1="120"  x2="120"  y2="100"  class="kos-
cloveka"></line>
              <line  x1="140"  y1="120"  x2="160"  y2="100"  class="kos-
cloveka"></line>
              <!-- noge -->
              <line  x1="140"  y1="150"  x2="120"  y2="180"  class="kos-
cloveka"></line>
              <line  x1="140"  y1="150"  x2="160"  y2="180"  class="kos-
cloveka"></line>
          </svg>
      </div>
      <div  class="text-center">  <span  class="border  rounded-pill
border-danger my-4 p-2" id="napacneCrke"></span> </div>
      <div class="text-center">
        <div id="opis-besede-joze">
          dolgo naj bo vsaj 12 znakov,

          vsebovati mora male in velike črke,

          vsebuje številke,

          vključuje posebne znake,

          NE vsebuje osebnih podatkov, kot so datum rojstva, ime
hišnega ljubljenčka, vaše ime ali e-poštni naslov.
        </div>
        <div id="opis-besede-ana">
          Blab bla ana bla
        </div>
        <div id="opis-besede-test">
          Blab bla test bla
        </div>
      </div>
```

```
      <div class="text-center">
        <button    type="button"    class="btn    btn-primary    mt-4"
onClick="window.location.reload();">Nova igra</button>
      </div>


    </main>
    <script
src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.
bundle.min.js"                                          integrity="sha384-
ka7Sk0Gln4gmtz2MlQnikT1wXgYsOg+OMhuP+IlRH9sENBO0LRn5q+8nbTov4+1p"
crossorigin="anonymous"></script>
    <script src="script.js" charset="utf-8"></script>


  </body>
</html>
```