54. srečanje mladih raziskovalcev Slovenije 2020

KDO PREŽI ZA KLIKOM?
SPLETNE PREVARE IN KAKO SE JIM IZOGNITI

Raziskovalno področje: računalništvo ali telekomunikacije

RAZISKOVALNA NALOGA

Mentorja:

Nataša Luković, prof.

Danijel Korpar, prof.

Avtorica:

Jana Zadravec, 8. a

OŠ Ludvika Pliberška Maribor, 2000 Maribor, Lackova cesta 4

Maribor, februar 2020

KAZALA

Kazalo vsebine

Kazalo slik, tabel in grafov

Tabele:

Grafi:

POVZETEK

Ključne besede: spletne prevare, najstniki, lažne spletne trgovine, lažne nagradne igre, Phishing, Deepfake, varno geslo

Čeprav je internet v osnovi dobra stvar, lahko predstavlja veliko nevarnost za njegove uporabnike. Na spletu lahko namreč naletimo na raznovrstne spletne prevare, ki so pogoste tudi zaradi nepravilne uporabe interneta in uporabnikove nepoučenosti o spletnih prevarah. V teoretičnem delu sem povzela razne pisne vire o spletnih prevarah, na katere sem se osredotočila.

Namen moje raziskovalne naloge je bil najprej raziskati, v kolikšni meri so moji vrstniki poučeni o tej vrsti spletnih prevar in kako odreagirajo ob soočenju z njimi. Nato sem jih želela bolje seznaniti s tovrstnimi spletnimi prevarami in jih poučiti o tem, kako spletne prevare ob soočenju z njimi prepoznati ter kako v takšnih situacijah ravnati. Želela sem tudi najti najprimernejši način za seznanjanje najstnikov z nevarnostmi na spletu, saj je zelo težko pritegniti njihovo pozornost. V ta namen sem pripravila dve anketi in predstavitev spletnih prevar. V prvi anketi sem želela preveriti, kako pogosto se učenci srečujejo s spletnimi prevarami, ali jih prepoznajo in ali tudi pravilno odreagirajo v takšni situaciji. Potem sem izvedla predstavitev za vse učence, ki sem jih anketirala o poznavanju spletnih prevar, saj so rezultati pokazali, da z njimi niso dovolj natančno seznanjeni. Učencem sem razdelila tudi letake z opisom spletnih prevar. Nato sem izvedla še drugo anketo, s katero sem želela ugotoviti, ali so učenci po izvedeni predstavitvi bolje poučeni o spletnih prevarah. S tem sem želela preveriti, ali so takšne predstavitve primerna metoda za seznanjanje najstnikov z nevarnostmi spleta.

Iz rezultatov prve ankete sem ugotovila, da večina učencev prepozna večino obravnavanih spletnih prevar že pred soočenjem z njimi in da jih večina tudi pravilno odreagira, če se srečajo z njimi. Učenci se z nekaterimi spletnimi prevarami srečujejo bolj pogosto, z nekaterimi pa skoraj ne. Prav tako nekatere nevarnosti spletnih prevar poznajo bolje kot druge.

Iz rezultatov druge ankete sem sklepala, da so učenci bolje poučeni o vrstah spletnih prevar, ki sem jim jih predstavila. Kljub temu, pa je število učencev, ki spletnih prevar še zmeraj ne poznajo dovolj dobro preveliko. Iz tega razloga sem se odločila ustvariti predstavitveni plakat,

ki je podrobno predstavil nevarnosti in načine zaščite pred obravnavanimi spletnimi prevarami, ki so se mi zdele najbolj pomembne glede na starost anketirancev. Menim, da sta bili izvedba predstavitve in izdelava plakata dobri ideji, saj bosta lahko učencem pomagali, da bodo v prihodnosti postali bolj odgovorni uporabniki spleta. Ker sem ugotovila, da moje metode niso bile dovolj učinkovite, sem na podlagi svojih ugotovitev v zaključku podala idejo, kako bi o nevarnostnih spleta poučili vse učence od 7. do 9. razreda v Sloveniji.

Z raziskovalno nalogo želim predvsem opozoriti na nevarnosti spletnih prevar ter pomagati ljudem, da bi se jim znali izogniti.

ZAHVALA

Iskreno se zahvaljujem mentorjema za usmerjanje in vodenje pri pripravi raziskovalne naloge in lektorici za lektoriranje. Zahvaljujem se tudi vsem sodelujočim v anketi.

1 UVOD

Živimo v času hitrega razvoja tehnologije, v katerem je internet del našega vsakdana. Kljub temu, da je internet v osnovi dobra stvar, saj si lahko z njim veliko pomagamo, pa vsebuje tudi veliko pasti in posledično predstavlja veliko nevarnost za njegove uporabnike. Pride lahko namreč do raznovrstnih spletnih prevar, ki dobivajo vedno večje razsežnosti. Ljudje ne postanejo žrtve različnih vrst spletnih prevar samo zaradi slabih namenov goljufov, ampak je zanje kriva tudi nepravilna uporaba spleta in nepoučenost o spletnih prevarah. Goljufi znajo to s pridom izkoristiti. Dokler se posameznik ne sooči spletno prevaro, se po navadi ne zaveda njene nevarnosti. Tudi sama pred začetkom pisanja raziskovalne naloge nisem veliko razmišljala o takšnih stvareh in nisem bila dovolj pazljiva. Predvidevam, da tako razmišlja večina ljudi. Da bi se izognili spletnim prevaram, se morajo ljudje bolje poučiti o varni uporabi interneta in možnih spletnih prevarah. Na osnovni šoli, ki jo obiskujem, veliko časa posvečamo varni uporabi interneta, saj imamo predavanja. Zato me je ta tema pričela bolj zanimati. O nekaterih pogostih spletnih pasteh so učenci naše šole in predvidevam, da tudi večina uporabnikov spleta že zelo dobro poučeni. Obstaja pa veliko nič manj pogostih spletnih prevar, o katerih ljudje ne vedo veliko. Ministrstvo za notranje zadeve Republike Slovenije skupaj z Interpolom opozarja na najpogostejše vrste finančnih spletnih prevar 21. stoletja in podaja nasvete, kako jih prepoznati in kako se jim izogniti. V raziskovalni nalogi sem se osredotočila na tiste spletne prevare, s katerimi se lahko srečajo tudi najstniki, a so manj znane. Lotila sem se preučevanja naslednjih vrst prevar, in sicer kraje osebnih podatkov in identitete, lažnih nagradnih iger, lažnih spletnih trgovin, spletnega ribarjenja in manipulacije videoposnetkov. Naštete prevare je težko prepoznati, zato je dobro, da se bolje poučimo o njih.

1.1 Cilji

Raziskovalne naloge na temo spletnih prevar sem se lotila, ker sem želela podrobneje raziskati manj znane, a tudi pogoste spletne prevare. Namen moje raziskovalne naloge je ugotoviti, v kolikšni meri so moji vrstniki oz. učenci zadnje triade osnovnih šol poučeni o tej vrsti spletnih prevar. Moja želja je seznaniti vrstnike s tovrstnimi spletnimi prevarami in jih poučiti o tem, kako spletno prevaro prepoznati ter kako v takšni situaciji ravnati. Moja želja je namreč, da bi bili moji vrstniki pri uporabi spleta bolj previdni in da ne bi postali žrtve prevar v prihodnosti. Poleg tega pa bi jih rada tudi opomnila, da vsemu, kar vidijo in slišijo na spletu ni moč verjeti, saj je s sodobno tehnologijo manipulacija podatkov vedno bolj preprosta in dostopna tudi

navadnim uporabnikom. Zavedam pa se tudi tega, da je dandanes zelo težko pritegniti pozornost najstnikov. Zato sem z raziskovalno nalogo želela tudi najti primeren in učinkovit način za seznanjanje najstnikov z nevarnostmi na spletu.

1.2 Hipoteze

Hipoteza 1: Večina učencev spletnih prevar ne prepozna.

Hipoteza 2: Večina učencev napačno odreagira, ko se sooči s spletno prevaro.

Hipoteza 3: Učenci se pogosto srečujejo s spletnimi prevarami.

Hipoteza 4: Večina učencev nima varnih gesel.

Hipoteza 5: Večina učencev ne ve, kaj sta Deepfake in Phishing.

Hipoteza 6: Učenci bodo po predstavitvi brošure veliko bolje poučeni o Deepfake-u, Phishingu in javnih brezplačnih Wi-Fi omrežjih.

2 TEORETIČNI DEL

2.1 Kaj so spletne prevare?

»Na spletu obstaja toliko goljufij kot je uporabnikov spleta. Naivnost in nepoznavanje spleta lahko velikokrat botrujeta, da nasedemo prevari, ki je tako zelo mamljiva, posebej če obljublja denar ali pa zelo poceni storitev ali izdelek.«[1]

Spletne prevare so tip goljufije, ki uporabljajo spletno podporo ali programsko opremo z dostopom do spleta za namerno oškodovanje žrtev in osebnega okoriščanja.[2]

Takšni spletni kriminalni načrti žrtve oškodujejo za veliko denarja in z raznovrstnimi metodami nadlegujejo spletne uporabnike. Gre za prevare, pri katerih lahko gre za prikrivanje informacij ali podajanje napačnih informacij z namenom ukane in pridobivanjem finančnih sredstev, imetja ali dediščine. Pri spletnih prevarah ne gre za eno zločinsko dejanje, ampak obsega niz nezakonitih in prepovedanih dejanj, ki se izvajajo v virtualnem svetu. Kljub temu pa se razlikujejo od kraje, saj v teh primerih žrtve prostovoljno in namenoma posredujejo informacije, denar ali imetje hudodelcem. Od kraje pa se razlikujejo tudi po tem, da so vanje vpleteni začasni in prostorsko ločeni kriminalci.[3]

V današnjem času na spletu naletimo na veliko prevar. V letu 2018 je odzivni center SI-CERT obravnaval 2.431 incidentov, od tega so obravnavali kar 1.372 primerov goljufij, največ do sedaj.[4]

2.2 Veliko hrupa za nič

2.2.1 Lažne nagradne igre

Pri lažnih nagradnih igrah uporabniki po navadi dobijo SMS sporočilo s povezavo, v kateri spletni goljufi v zameno za izpolnjeno anketo obljubljajo bogate darilne bone, najnovejši model

[1] http://www.poslovodno-racunovodstvo.si/sl/spletne-prevare.php (12.11.2019 20:05)
[2] https://ec.europa.eu/anti-fraud/olaf-and-you/report-fraud_sl (13.11.2019 16:27)
[3] https://en.wikipedia.org/wiki/Internet_fraud (13.11.2019 16:39)
[4] https://mariborinfo.com/novica/kronika/lani-so-zabelezili-rekordno-stevilo-spletnih-goljufij-vec-kot-tisoc/268639 (13.11.2019 17:13)

pametnega telefona ali podobne mamljive nagrade. V primeru, da prejmemo takšno SMS sporočilo, je najbolje, da ga ignoriramo in na internetno povezavo ne klikamo.[5]

»Uporabniki so pod pretvezo pridobitve neke želene nagrade zavedeni v vpis podatkov o kreditni kartici. Vpis tako povzroči mesečne stroške za »članarino«, pojavi pa se tudi tveganje za možnost kasnejše zlorabe kreditne kartice. Pogosto so uporabniki zvabljeni tudi v plačljivi SMS-klub, ki jim nakoplje dodatne stroške.«[5]

»V postopku obravnave prijavljenih incidentov strokovnjaki SI-CERT ugotavljajo, da prejeta povezava v SMS sporočilu lahko preusmeri tudi do spletne strani, prek katere se izvede prenos aplikacije za mobilne naprave. Analiza predmetne aplikacije je pokazala, da se v primeru namestitve, mobilna naprava lahko okuži tudi s trojanskim konjem.«[5]

Lažnih nagradnih iger ni težko prepoznati. Če bi nam nekdo v zameno za en klik, 1€ ali našo telefonsko številko želel podariti nagrado v vrednosti 1000€, bi morali podvomiti v verodostojnost takšne ponudbe. Kljub temu na Varni na internetu dobivajo veliko prijav, ker so bili ljudje oškodovani zaradi lažnih nagradnih iger.[5]

2.2.2 Lažni zadetki pri igrah na srečo

Pri lažnih zadetkih na loterijah je precej podobno kot pri lažnih nagradnih igrah. Uporabniki dobijo elektronsko ali SMS sporočilo, v katerem piše, da so zadeli veliko denarno vsoto na loteriji. Če bi odgovorili na takšno sporočilo, bi prevaranti najprej želeli naše osebne podatke za nakazilo denarja. Potem bi od nas zahtevali plačevanje različnih dajatev in stroškov pred prejemom denarne nagrade. Seveda nagrade kljub plačilu ne bi prejeli. Ko prevaranti najdejo žrtev, ki jim denar pošlje, zahtevajo vedno večje zneske denarja. Če kdo nasede takšni spletni prevari, se mu najbolj priporoča, da goljufijo prijavi policiji. Goljufe policija zelo težko najde, saj z žrtvami komunicirajo preko zlorabljenih sistemov in je zato težko izslediti njihovo lokacijo. Po navadi za nakazila denarja uporabljajo Western Union ali Money Gram, pri katerih je izsledite identitete prejemnika veliko težja. Večina goljufov deluje v državah, v katerih

[5] https://www.varninainternetu.si/po-spletu-krozijo-lazne-nagradne-igre-kako-ravnati/ (14.11.2019 16:46)

zakonodaja na področju internetnega kriminala ni urejena. Da gre za loterijsko prevaro, najlažje ugotovimo tako, da del besedila, telefonsko številko ali elektronski naslov pošiljatelja vpišemo v spletni brskalnik. Če je besedilo na povezavi napisano v polomljeni slovenščini (iz Google prevajalnika), gre najverjetneje za spletno prevaro.[6]

2.2.3 Lažne spletne trgovine

»Lažne spletne trgovine imajo z izrazom trgovina le malo skupnega. Gre zgolj za kulise z lepimi slikami, za spletno predstavitvijo pa ne stoji legitimno podjetje. Takšen nakup predstavlja veliko tveganje, saj kupec plačanega blaga ne bo prejel, lahko pride do zlorabe podatkov kreditne kartice ali pa kupi ponarejen izdelek, ki bo na slovenski carini zasežen in uničen. Vedno bolj aktualne so lažne spletne trgovine priljubljenih blagovnih znamk.«[7]

Neverjetna ponudba je prvi znak, da gre za prevaro. Ko določen izdelek v določeni spletni trgovini preveč odstopa v ceni, je to slab znak. Zelo pomembno je tudi, kako smo prišli do oglasa za to spletno trgovino. Veliko bolj verjetno je, da ne gre za prevaro, ko za spletno trgovino izvemo preko televizije, kot pa, če zanjo izvemo preko sporočila, ki nam ga je poslal neznanec. Ko preverjamo, če je spletna trgovina verodostojna, je priporočljivo, da pogledamo komentarje in mnenja ljudi, ki so že imeli izkušnje s to spletno trgovino. Če vidimo veliko negativnih komentarjev, kupovanje tam najverjetneje ni najboljša odločitev. Preden se odločimo za nakup v določeni spletni trgovini, je dobro preveriti, kdo stoji za spletno trgovino. Priporočljivo je pogledati kontaktne podatke podjetja (naslov podjetja, telefonsko številko za pomoč uporabnikom, elektronski naslov) ter vstopiti v kontakt s prodajalcem. Če prodajalec uporablja brezplačen poštni predal, to pomeni, da gre za prevaro. Pozorni moramo biti tudi na način plačila. Če nas spletni trgovec prosi za nakazilo preko sistema Western Union ali MoneyGrama je to zelo jasen znak, da gre za prevaro.[7]

[6] https://www.varninainternetu.si/poskus-loterijske-prevare-preko-sms-sporocil/(14.11.2019 17:57)
[7] https://www.varninainternetu.si/article/lazne-spletne-trgovine/ (23.11.2019 15:03)

2.2.4 Prevare prodajanja po malih oglasih

Večina ljudi ima občutek, da smo kot prodajalci na spletnih oglasnikih povsem varni, ampak temu ni tako. Goljufi nas prevarajo na čisto preprost način. Prepričajo nas, da je denar že nakazan in mi jim pošljemo izdelek. Tako smo pravzaprav dvakratno ogoljufani. Najprej ostanemo brez denarja, potem pa goljufi ta izdelek sami prodajo in zaslužijo.[8]

»Goljufi izkoriščajo najrazličnejše spletne oglasnike (bolha.com, salomon.si, avto.net itd.), da vzpostavijo kontakt s prodajalci, nato pa jim pošljejo lažna potrdila, da je denar že nakazan.«[8]

Goljufi pri spletnih oglasnikih uporabljajo dve vrsti prevar. Pri prvi nas goljufi najprej prepričajo, da so nam denar že nakazali, tako da nam pošljejo lažno potrdilo. Žal to prepozno ugotovimo in izdelek že pošljemo, goljuf pa ga proda naprej. Goljufi se najraje lotijo prevare pri izdelkih, ki se jih da hitro prodati, npr. mobilni telefoni. Prevarantov ni težko prepoznati, saj se sploh ne pogajajo za ceno in so v vseh primerih iz tujine. Če se ne pustimo prevarati, nam velikokrat grozijo, da smo jih okradli in da nas bodo prijavili policiji.[8]

Druga vrsta prevare je še bolj nevarna in lahko povzroči precej večjo finančno škodo. V tem primeru goljufom izdelek, ki ga prodajamo ni tako pomemben. Najpomembnejši znak, da gre za prevaro, je ponudba kupca, da bo nakazal še več denarja, kot je postavljena cena, saj želi, da prodajalec nakaže preplačano vsoto logističnemu podjetju za dostavo. Nadaljnji postopek je podoben postopku prve vrste prevar.[8]

Varno lahko preko spletnih oglasnikov prodajamo tako, da ne pošiljamo izdelka, dokler se popolnoma ne prepričamo, da je denar nakazan, da ne verjamemo lažnim potrdilom, ki nam jih pošlje tujec in da ne verjamemo grožnjam s strani kupca.[8]

2.3 Vem, kdo si

2.3.1 Kaj je kraja osebnih podatkov?

Kraja osebnih podatkov je novejša oblika kriminala, ki se z željo po lahkem zaslužku na tuj račun širi po vsem svetu z velikansko hitrostjo.

[8] https://www.varninainternetu.si/prevare-ko-prodajate-prek-malih-oglasov/ (24.11.2019 19:11)

Naše osebne podatke sleparji zbirajo iz družbenih omrežij. Ti podatki lahko goljufom pomagajo pridobiti dostop do naših računov, najeti posojila ali drugače nezakonito poslovati v našem imenu, podatke pa lahko prodajo tudi drugim sleparjem.[9]

Številne spletne storitve in aktivnosti nas spodbujajo, naj na spletu razkrijemo čim več o sebi. Tu so spletne skupnosti, družbena omrežja, galerije slik, video portali, blogi, forumi, klepetalnice, spletne igre ali objave na mobilnih telefonih. Poleg tega se osebni podatki zbirajo tudi s pomočjo t. i. piškotkov. Pogosto se uporabniki ne zavedajo dovolj, da lahko te podatke nekdo zlorabi za svoje koristi. Zato naj vaši osebni podatki, kot so osebno ime, naslov bivanja, telefonska številka, e-poštni naslovi, rojstni podatki itd., raje ostanejo osebni.[9]

2.3.2 Kaj je kraja identitete?

»Pri kraji identitete, neznana oseba pridobi naše osebne podatke in se začne predstavljati v našem imenu. Posledično lahko zavede naše sodelavce ali prijatelje, okrni naš ugled ter si pridobi dostop do naših informacij, dokumentov, slik ali v našem imenu opravlja e-bančne storitve. Kraja identitete na spletu je najpogosteje posledica kraje gesla. Torej neznanec pridobi naše uporabniško ime in geslo in nato dostopa do našega elektronskega predala, Facebook profila ali PayPal računa.«[10]

Neznanec najlažje prevzame našo spletno identiteto, kadar smo sami nepazljivi in po nesreči ali celo namenoma razkrijemo svoja gesla. Pogosti način je tudi Phishing oziroma kraja podatkov, pri katerem nas elektronsko sporočilo pripravi do tega, da razkrijemo svoje uporabniške podatke. Storilec lahko pridobi naša gesla tudi z okužbo računalnika z zlonamerno kodo, ki beleži pritiske tipk. Gre za vrsto virusa, ki napadalcu pošilja shranjena in prestrežena gesla z računalnika.[10]

»Največjo nevarnost na tem področju predstavlja nepooblaščen dostop do našega poštnega predala. Tako lahko nekdo prestreza vso našo elektronsko pošto. Nevarnost je še večja, če so na elektronski naslov vezani tudi uporabniški računi drugih spletnih storitev, npr. Facebooka.

[9] https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/95864-sedem-vrst-spletnih-financnih-prevar-ki-jim-uporabniki-najpogosteje-nasedejo (12.11.2019 18:26)
[10] https://www.varninainternetu.si/article/kraja-identitete-2/ (12.11.2019 20:27)

Tako lahko storilec najprej zamenja geslo za npr. račun Gmail, nato pa še geslo na Facebooku. V tem primeru lahko storilec pride do veliko večje količine informacij, ki jih potem poljubno zlorabi.«[11]

2.3.2.1 Kaj so varna gesla?

Gesla so nizi znakov, ki se uporabljajo za avtentikacijo uporabnikov računalniškega sistema. Živimo v času, ko smo obkroženi z raznimi storitvami, za katere pa potrebujemo varna in učinkovita gesla.[12]

Močno geslo je naša prva obrambna linija, ko se na naše uporabniške račune spravijo nepridipravi, tovrstnih primerov pa je iz dneva v dan več. Ker pa danes potrebujemo več kot le eno geslo, le ta pa morajo biti precej kompleksna, da so tudi varna, kaj hitro naletimo na težavo pomnjenja le teh. Postavljeni smo pred dilemo. Izbrati preprosto geslo, ki bo manj varno in si ga lahko zapomnimo ali pa prepustimo domišljiji prosto pot in ustvarimo kompleksna gesla, a kasneje pogosto iščemo listke z zapisanimi gesli, saj si jih je nemogoče zapomniti. V slednjem primeru si lahko pomagamo z enim od upravljavcev gesel, ki jih je za mobilne naprave na pretek, najbolj praktični so seveda na telefonih, ki jih imamo po navadi pri roki.[12]

Če uporabljamo preprosta gesla, kot so npr. naše ime, ime naših sorodnikov ali hišnih ljubljenčkov, lahka zaporedja številk, datume rojstva itd., je to lahko zelo nevarno, saj so to zelo šibka gesla. Takšna gesla goljufom ne predstavljajo nobene ovire. Še do veliko več podatkov lahko pridejo, če imamo za vse aplikacije in e-naslov enako geslo.[13]

Preprosta gesla goljufi odkrijejo na zelo preprost način. Velikokrat jih ugibajo ali pa si pomagajo s slovarjem. Lahko pa je naš računalnik okužen in se zato goljufu pošiljajo vsa gesla, ki jih mi vpisujemo.[13]

Posledice preprostih gesel so lahko zelo hude. Ko goljufi ugotovijo naše geslo, lahko pridejo do naše e-pošte, spletne banke, poslovnih skrivnosti ter drugih nam pomembnih podatkov.

[11] Nov roparski val: Kraja identitete. V Glamur št. 62 (2002). Stran 48 (13.1.2020 17:10)

[12] https://www.kajkupiti.si/uporabni-nasveti/kako-izbrati-mocno-in-varno-geslo.html (28.11.2019 15:12)
[13] https://www.varninainternetu.si/mocno-geslo/ (28.11.2019 15:56)

Hkrati pa nas lahko hitro postavijo v vlogo lahke tarče in žrtve spletnega kriminala, ki ji lahko nekdo zašifrira datoteke na računalniku, dostopa do njihovih osebnih fotografij, prevzame identiteto na družbenem omrežju ali celo lahko razpolaga z našim denarjem.[13]

Za močna gesla velja nekaj pomembnih pravil:

1. Geslo naj bo dovolj dolgo, po možnosti vsaj 10 znakov, raje pa še več. Vsebuje naj male in velike črke, ločila in posebne znake.
2. Za vsako storitev je treba uporabljati drugo geslo.
3. Primer dobrih gesel, ki si jih je lažje zapomniti, so tudi povezane cele besede.
4. Uporabljati je treba različne stopnje kompleksnosti gesel.
5. Priporočljivo je uporabljati upravljalnik gesel (Password Manager).
6. Gesel nikoli ne smemo razkrivati drugim osebam, sploh pa ne, če to od nas zahtevajo ali pa nas zaprosijo zanje.[13]

2.3.2.2 Kako kreirati močno geslo, ki si ga bomo tudi lahko zapomnili?

Pravzaprav je precej enostavno ustvariti močno geslo. Najbolje je ustvariti geslo, ki bo imelo, vsaj za nas, nek smisel, nek pomen. Pri tem se moramo izogibati najbolj očitnim besedam in znakom, ki so povezani z nami na takšen ali drugačen način in so znane tretjim osebam, ki jim ne zaupamo.[14]

a) Pomagamo si s stavkom, v katerem uporabimo nekaj nepomembnih podatkov.

Primer: ***M**oje **p**rvo **s**tanovanje **je** **b**ilo **n**a **n**aslovu **C**elovška **13, n**ajemnina **je** **z**našala **3**00**€** **n**a **m**esec*. Če to pretvorimo v geslo, tako da uporabimo le prve črke/znake besed dobimo geslo:

- **MpsjbnnC13,njz3€nm**

Dobili smo izjemno močno geslo z 18 znaki, ki vsebuje male in velike črke, simbole, znake in je na prvi pogled povsem naključno generirano.

b) Uporabimo kakšno besedno fraz ali pregovor, ki pa ga moramo nekoliko zamaskirati.

[14] https://www.kajkupiti.si/uporabni-nasveti/kako-izbrati-mocno-in-varno-geslo.html (28.11.2019 16:31)

Primer: ***O**sel **g**re **s**amo **enkrat** **n**a **l**ed*. Uporabimo zopet prve znake besed, besedo enkrat zamenjamo z 1x ter dobimo geslo:

- **Ogs1xnl** ali **053Lgs1xnl**

Primer: ***To be or not to be***. Uporabimo prve znake besed, nekatere črke zamenjamo z znaki, dobimo npr. geslo:

- **2b-or-Not-2b**

Primer: ***Vesel sem, da sem star 30 let***. Uporabimo prevode besed, nekatere črke zamenjamo z znaki, dobimo npr. geslo:

- **Iam:)2b30**

c) Tipkovnico uporabimo kot paleto. Če si zamislimo obliko črke ali druge oblike lahko dobimo izjemno močna gesla, ki jih bomo na tipkovnici hitro našli.

Če uporabimo npr. obliko črke V dobimo npr. geslo: (sledite na tipkovnici):

- **%tgbhu(** ali **5tgbhu8**[14]

2.4 Kaj imate tukaj WI-FI? (Javni računalniki in javna brezplačna omrežja Wi-Fi)

Javni računalniki so pogosti v kampih, kavarnah in knjižnicah ter služijo veliko uporabnikom, zato je veliko večja verjetnost, da so okuženi z virusi. Tako nam lahko goljufi brez težav ukradejo identiteto, saj ne vemo, kaj so počeli na računalniku. Da je računalnik okužen z virusom pomeni, da ima nekdo dostop do vseh podatkov, ki jih vpisujemo, do vseh spletnih strani, ki jih obiščemo, lahko beleži vsako pritisnjeno tipko in gib miške. Zaradi teh nevarnosti se pri uporabi javnih računalnikov močno odsvetuje vpisovanje gesel in prijavljanje v elektronsko pošto, družbena omrežja ipd. Uporaba javnih računalnikov je primerna za prebiranje novic in spremljanje vremenske napovedi.[15]

[15] https://www.varninainternetu.si/top-6-spletne-nevarnosti-za-dopustnike/ (6.12.2019 16:41)

»Na letališčih, v kavarnah in hotelih so pogosto na voljo javna brezžična omrežja (Wi-Fi), ki so brezplačna ali pa so dostopna po zmerni ceni. Ta možnost dostopa je dosti varnejša od javnih računalnikov, saj uporabljamo svoje naprave. Če brezžična dostopna točka ni dovolj zavarovana, lahko pride do prestrezanja omrežnega prometa, kar pomeni, da lahko neznanec spremlja ves naš omrežni promet. Prav posebno previdnost pa zahteva t. i. ad-hoc brezžično omrežje, ki ga ustvari nekdo kar na svojem računalniku. V tem primeru se povežemo neposredno na prenosnik neznanca. Taka omrežja so po navadi prikazana z malce drugačno ikono.« Dobro se je vedno pozanimati, katero je pravo omrežje hotela ali cyber cafeja. Če lahko izbiramo med nešifriranim in šifriranim omrežjem, moramo izbrati šifriranega.[15]

2.5 Si to res ti?

2.5.1 Kaj je manipulacija videoposnetkov ali Deepfake?

Manipulacija posnetkov ali Deepfake je videoposnetek, ki nastane z uporabo umetne inteligence in prikazuje posnetke ljudi, ki počnejo in govorijo reči, ki jih v resnici ne. Deepfake posnetki so lahko zabavni in smešni ali pa tudi škodljivi za ljudi, ki jih prikazujejo. Takšni posnetki so v razmahu, saj obstajajo brezplačne aplikacije, kot sta na primer FakeApp ali DeepFaceLab, ki omogočajo manipulacijo posnetkov amaterjem.[16]

Težava nastane, ker je zelo težko ločiti resnične in umetno narejene, lažne posnetke, kar lahko privede do širjenja napačnih informacij in posledično do nesoglasij, prepirov in osebno prizadetih žrtev. Takšni posnetki lahko uničijo ugled posameznika, vplivajo na rezultate volitev oseb na pomembnih položajih, širijo lažne novice in celo vplivajo na gospodarski trg. Zaradi razsežnosti vpliva takšnih posnetkov in težkega razpoznavanja avtentičnosti, postaja ta problem vse kompleksnejši in bolj nevaren.[16]

[16] https://www.mcafee.com/blogs/consumer/family-safety/sadfishing-deepfakes-tiktok-headlines-you-may-have-missed/ (6.12.2019 17:05)

Prepoznavanje Deepfake tehnologije je zelo velik izziv v današnjem času, saj ima lahko velik negativen vpliv na zaupanje ljudi. Posledice so lahko hude, saj obstaja možnost, da ljudje ne bomo več mogli verjeti in zaupali nikomur drugemu, kakor le še sebi.[17]

Deepfake bo imel tudi pomemben vpliv na pogled ljudi na življenje in svet. Trenutno ga pomembno filtrirajo mediji. Človeški mediji kljub napakam, dajejo vse od sebe, da bi primerno opravili svojo nalogo, kar pa Deepfake spodkopava.[17]

»Podjetje Snapchat je v začetku leta 2016 svojo aplikacijo nadgradilo s filtrom face swap za zamenjavo obraza. Uporabnik je lahko z mobilnim telefonom v živo zamenjal svoj obraz z obrazom nekoga drugega.« Pred časom so morali filmski studii za tovrstne vizualne učinke plačevati milijone in najemati izvrstne montažerje. Danes pa lahko to tehnologijo uporabljajo navadni uporabniki s svojimi pametnimi telefoni.[18]

»Glede na dostopnost podatkov lahko program uporabi prav vsakdo. In tu se začenja tudi ena večjih skrbi. Tehnologija hitro napreduje in ni malo verjetno, da se bo začela izrabljati tudi za potegavščine, ki imajo lahko resne posledice za družbo.« Širiti se bodo začele lažne novice. Če na spletu beremo novice ali gledamo fotografije, jim ne nasedamo kar tako, saj vemo, da lahko gre za photoshop ali lažne novice. Nekaj povsem drugega pa je gledati videoposnetek določene osebe, ki govori in se premika. Temu ljudje brez razmišljanja verjamemo. Na začetku nihče niti pomislil ni, da bi lahko šlo za prevaro, saj je naš organizem narejen tako, da verjamemo temu kar slišimo in vidimo. Raziskovalci univerze Stanford so razvili celo aplikacijo Face2face, ki omogoča prenos obrazne mimike posameznika na obraz osebe na videoposnetku.[18]

V začetku leta 2018 se je pojavila računalniška aplikacija FakeApp. Z njo lahko uporabniki obraz posameznika prestavijo na telo drugega človeka. Nato se ta oseba premika in govori tako kot želi uporabnik. *»Program deluje kot nekakšna naprednejša različica prej omenjenega Snapchata. V program vneseš glavni video, ga povežeš s spletno zbirko fotografij posameznika in po nekaj urah obdelave podatkov dobiš želeni potvorjeni video, ki je pripravljen na deljenje.*

[17] https://radioprvi.rtvslo.si/2019/10/najvecja-zloraba-umetne-inteligence-je-deepfake-tehnologija/ (6.12.2019 19:05)

[18] https://www.dnevnik.si/1042819488/magazin/znanost-in-tehnologija/manipulacija-videoposnetkov-deepfake-posnetki-kot-znanilci-nove-dobe-laznih-novic (6.12.2019 18:13)

Boljša in zajetnejša kot je zbirka fotografij posameznika, pristnejša bo videti animacija obraza. Za zdaj se Deepfake posnetki pojavljajo predvsem kot sredstvo zabave.«[18]

Pretresljive novice so zelo priljubljene na družbenih omrežjih, še posebej pa na Facebooku. Zato strokovnjake zelo skrbi, kako obvladati to situacijo. Težave imajo namreč že s pisano besedo, zato ne vedo, kako naj se lotijo lažnih videoposnetkov.[19]

»Nekatere spletne platforme so že pred časom zagrozile, da bodo odstranile vse takšne ponaredke in blokirale uporabnike, ki so jih objavili. Raziskovalci pa so medtem tudi že razvili prve algoritme za prepoznavanje takšnih izdelkov. Najboljši algoritmi za zdaj ponaredek prepoznajo v 97 odstotkih, kar je veliko, a pri tako občutljivih vsebinah znajo že trije odstotki objavljenih vsebin še vedno močno vplivati na življenja posameznikov.«[19]

2.5.2 Kaj potrebujemo za dober Deepfake videoposnetek?

Eden izmed glavnih sestavin dobrega Deepfake posnetka so fotografije visoke ločljivosti in videoposnetki osebe. V današnjem času ima veliko otrok na svojih pametnih telefonih visoko zmogljive kamere in fotoaparata. Takšne fotografije in posnetki z visoko ločljivostjo so ravno pravšnji za manipulacijo videoposnetkov z zelo realističnimi rezultati.[20]

2.5.3 Nevarnosti uporabe Deepfake tehnologije za najstnike

Glede na porast uporabe različnih spletnih aplikacij za manipulacijo videoposnetkov in spretnost najstnikov pri njihovi uporabi, je le vprašanje časa, kdaj se bo uporaba le-teh spremenila iz zabave v zavajanje z lažnimi posnetki.[21]

Ena izmed zelo priljubljenih dejavnosti otrok in najstnikov današnjega časa je ustvarjanje lastnih fotografij in video vsebin, ki jih pogosto nalagajo na različne strani družbenih medijev, kot so Facebook, Instagram, Snapchat in Tik Tok. S takšnim početjem otroci in najstniki nevede ustvarjajo obsežno knjižnico vsebin, ki jo lahko nato nekdo, ki ga sploh ne poznajo, razčleni in analizira ter ustvari navodila za program umetne inteligence, ki ustvari zmanipuliran video.[21]

---

[19] https://www.dnevnik.si/1042838574/magazin/znanost-in-tehnologija/3d-replike-obrazov-vzbujajo-strah-pred-razmahom-laznih-novic- (6.12.2019 18:32)
[20] https://www.digitaladventures.com/news/2019/8/18/deepfakes-are-here-a-parent-s-guide-to-understanding-the-risks-for-their-kids (6.12.2019 18:48)
[21] https://www.digitaladventures.com/news/2019/8/18/deepfakes-are-here-a-parent-s-guide-to-understanding-the-risks-for-their-kids (6.12.2019 18:59)

To pomeni, da lahko neznanec iz nabora fotografij in posnetkov, ki jih je naivno naložil otrok ali najstnik izbere določene delčke, kot so na primer, obraz, gibanje ali glas in ga vstavi v kakršno koli vrsto posnetka, ki bo prikazoval vsebine, v katerih otrok ali najstnik ni nikoli sodeloval.[21]

V najstniških letih, ko se posameznik še išče in mu največ pomeni mnenje vrstnikov, je nekaj najhujšega, če izgubiš svoj ugled zaradi neresničnih informacij. Toliko huje, če so te dosegljive širšemu krogu ljudi in se širijo preko spleta. Velikokrat za take informacije posameznik ne izve takoj, kasneje to zelo težko zaupa staršem ali odrasli osebi, posledično pa doživlja veliko stisko, ki ima lahko negativen vpliv na njegovo odraščanje in razvoj osebnosti.[21]

Glede na trajnostno naravo spleta, pa se lahko ti trajni digitalni posnetki prikažejo kot prvi rezultati iskanja, ki jih bo ugledala možna bodoča fakulteta ali delodajalec, ko bo vpisal ime posameznika v spletni brskalnik.[21]

Pred kratkim smo lahko videli, kako mogočna je lahko ta tehnologija, ko so po spletu zaokrožile aplikacije, ki so prikazale, kakšni bomo videti, ko bomo starejši. Aplikacija namreč uporabi knjižnico posnetkov v naši napravi in ustvari podobo postaranega posameznika. Z uporabo te aplikacije pa posameznik prispeva podobe v obsežno knjižnico podob, pri čemer se odpove svojim pravicam do posnetkov in zasebnosti, v zameno za privilegij ogleda svojega možnega videza v obdobju starosti.[21]

2.5.4 Kako se zaščititi pred manipulacijo videoposnetkov?

Kljub dejstvu, da je ta napredna tehnologija šele v povojih, se moramo zavedati njenih nevarnosti. Prvotnega pomena je, da postanejo otroci in najstniki bolj občutljivi in pozorni pri deljenju fotografij in posnetkov samih sebe z drugimi. Večje kot je število fotografij in posnetkov, lažje je vzeti vsebino in jo umetno spojiti na načine, ki jih nihče ne bi pričakoval.[22]

Prav tako je pomembno, da smo pazljivi na virtualne sledi, ki jih puščamo na določenih spletnih straneh. Preveriti je treba, ali gre za dobro znane spletne strani s primerno varnostjo zasebnosti

[22] https://www.digitaladventures.com/news/2019/8/18/deepfakes-are-here-a-parent-s-guide-to-understanding-the-risks-for-their-kids (6.12.2019 19:43)

ali pa za mobilne aplikacije, katerih namen je zbiranje fotografij za potencialno škodoželjno uporabo v prihodnosti.[22]
Otroke in najstnike je treba tudi poučiti o možnostih, ki jih ponujajo vse novodobne tehnologije. Zavedati se morajo, da se za zabavno uporabo in kratkočasenjem z nalaganjem fotografij in posnetkov na družbena omrežja lahko skriva tudi veliko tveganje, kateremu se izpostavljajo, če niso dovolj previdni.[22]

Namesto širokega objavljanja z namenom pridobivanja všečkov in delitev, je mogoče mnogo bolje deliti svoje zasebne fotografije in videe s skupino prijateljev ali družino, ki ji lahko zaupamo. Z zmanjševanjem obsega deljenja vsebin se lahko najbolje zaščitimo pred zlorabo tistih, ki nimajo najboljših namenov.[22]

Potrebno je skrbno varovati svoj nabor fotografij in posnetkov. Vzeti si je treba čas in posodabljati svoje podatke pri na aplikacijah ter večkrat preverjati politiko zasebnosti, še posebej pri aplikacijah, ki uporabljajo kamero in mikrofon. Prav tako je treba biti previden pri gledanju posnetkov in klikanju na povezave in spletne strani, ki niso varne.[22]

Na koncu pa obstaja še najboljši način preprečevanja zlorabe lastnih podatkov in sicer tako, da mladi pričnejo z uporabo spleta šele, ko so dovolj stari. Otroci in najstniki velikokrat nekontrolirano uporabljajo splet in možnosti, ki jim ponuja, brez da bi starši nadzorovali njihovo početje. Sami še niso dovolj zreli in poučeni, da bi znali sami razsoditi katero početje je pravilno in katero neprimerno.[22]

Pri otrocih in najstnikih bo v času odraščanja vedno obstajala dovzetnost za ustrahovanje in zbadanje. Toliko huje, če se kot žrtev pojaviš ti sam. Nihče si ne sme zatiskati oči in biti prepričan, da se njemu kaj takega ne more zgoditi.[22]

2.5.5 Kako prepoznati zmanipuliran posnetek?

Opaziti, da gre za Deepfake video ni lahko. Pozorni moramo biti na podrobnosti, kot so mežikanje z očmi, sence ali robovi, ki niso videti pravilni, ton kože, ki se ne ujema in premikanje ustnic, ki ni popolnoma v skladu z besedami govorca.

2.6 Kaj je spletno ribarjenje ali Phishing?

»Spletno ribarjenje ali Phishing je spletna prevara, pri kateri gre za krajo podatkov s pomočjo lažnega predstavljanja, ki storilcu omogoča dostop do spletnih storitev v našem imenu in v skrajnem primeru tudi krajo našega denarja. S Phishing prevaro spletni goljuf pridobi osebna uporabniška imena in gesla za dostop do storitev kot so elektronska pošta, Facebook ali PayPal. Tipična Phishing prevara se prične z elektronskim sporočilom, ki naj bi bilo od ponudnika spletne storitve. Obvestijo nas, da se moramo zaradi preverjanja podatkov ali dodatnih ugodnosti prijaviti in ponovno vnesti svoje podatke. V sporočilu se nahaja tudi povezava, na katero naj bi kliknili, vendar nas vodi na lažno spletno stran, ki je zelo podobna, morda skoraj identična strani legitimnega ponudnika.«[23]

»Cilj napadalcev je prevzem nadzora nad uporabniškimi računi. Ko pridobijo podatke, lahko zamenjajo geslo in s tem lastniku računa preprečijo dostop. Potem njegov račun uporabljajo za objavljanje lažnih oglasov in goljufanje kupcev.«[23]

Phishing prevare so zelo pogoste na uporabniškem portalu Avto.net. Ta je začel močno oteževati ustvarjanje lažnih oglasov. Zato so goljufi iznašli drug način. Po phishing kraji podatkov poskušajo pridobiti gesla preverjenih, legitimnih uporabnikov in pod njihovimi profili objavljati lažne oglase. Na ta način tudi precej povečajo možnost uspeha goljufije.[23]

2.6.1 Kako prepoznati Phishing sporočilo?

Ko se znajdemo na Phishing spletni strani, se od nas pričakuje, da tam ponovno vpišemo svoje osebne podatke in geslo. Če na tisti spletni strani podatke vpišemo, jih pravzaprav posredujemo goljufu.[24]

Čeprav je Phishing v osnovi namenjen kraji podatkov za dostop do spletnega bančništva, imajo vrednost tudi drugi podatki, ki se nam morebiti ne zdijo tako pomembni. To so lahko uporabniško ime ali geslo za dostop do poštnega predala. Velika večina spletnih storitev od nas zahteva registracijo, kjer si izberemo ime in določimo geslo za dostop do storitve. Če geslo pozabimo, dobimo sporočilo s podatki za nastavitev novega gesla na naš elektronski naslov. Če

[23] https://www.varninainternetu.si/kraja-podatkov-phishing-na-avto-net/ 1(12.11.2019 20:46)

[24] Darinka Meško. Spletne goljufije. V Poslovno računovodstvo(2015). Stran 85-99 (9.12.2019 19:22)

ima torej goljuf dostop do našega poštnega predala, lahko v našem imenu dostopa tudi do storitev, pri katerih smo svoj elektronski naslov navedli pri registraciji.[24]

Obstaja pa nekaj zelo jasnih znakov s pomočjo katerih lahko ugotovimo, da smo žrtve Phishing prevare še preden nam prinese hude posledice:

1. Elektronsko sporočilo, ki smo ga prejeli, od nas zahteva, da zaradi preverjanja podatkov ali dodatnih ugodnosti ponovno vnesemo osebne podatke. Če se to zgodi, zagotovo vemo, da gre za prevaro, saj banka tega nikoli ne bi naredila.
2. Prejeli smo flag obvestilo. To je obvestilo banke v polomljeni slovenščini.
3. Sprememba uporabniškega imena in gesla za dostop do poštnega predala sta posredovana po elektronski pošti.
4. Lažna spletna stran je zelo podobna spletni strani naše banke.
5. URL naslov se začne s http, namesto s https. Naša banka bo vedno uporabljala varno povezavo, ki jo ponazarja sličica sklenjenega ključa ali ključavnice v spodnjem levem kotu ali URL vrstici.[24]

2.6.2 Kaj storiti v primeru, da smo geslo in osebne podatke na Phishing strani vpisali?

V primeru, da smo geslo in osebne podatke na Phishing strani vpisali, moramo čim prej spremeniti geslo. Če enako geslo uporabljamo tudi za kakšno drugo storitev, ga moramo zamenjati tudi tam. Dejansko bi morali za vsako storitev uporabljati drugo geslo.[25]

»Če so bili izdani podatki o kreditni, debetni ali bančni kartici, je potrebno čim prej prijaviti krajo teh podatkov izdajatelju kartice. Večina izdajateljev ima brezplačno telefonsko številko in 24-urno storitev za ukrepanje v takšnih primerih. Potrebno je preklicati račun in odpreti novega. Uporabnik mora natančno preveriti izpiske bančnih računov in kreditnih kartic. O vsaki sumljivi transakciji je potrebno čimprej obvestiti izdajatelja kartice. Če smo na lažni spletni strani dali svoje osebne identifikacijske podatke, kot so ime, priimek, davčna številka, EMŠO številka ali druge podatke za ugotavljanje istovetnosti, obstaja sum kraje identitete. Kraja identitete je kaznivo dejanje, za katerega je zagrožena zaporna kazen od treh mesecev

[25] https://www.varninainternetu.si/kraja-podatkov-phishing-na-avto-net/ (12.1.2020 12:53)

do treh let. Za pregon je potrebno vložiti pisno ali ustno ovadbo na pristojno državno tožilstvo ali policijo. Obvestiti je potrebno tudi izdajatelja kartic.«[26]

3 METODE DELA

3.1 Opredelitev raziskovalnega problema

Svoje raziskovalno delo sem pričela z opredelitvijo raziskovalnega problema. Nepoznavanje nevarnosti spletnih prevar s strani najstnikov ima lahko velik negativen vpliv na njihov zdrav osebnostni razvoj, v primeru, da pride do zlorabe. Ob pregledu in študiranju različnih slovenskih in tujih člankov na temo spletnih prevar, sem ugotovila, da je tema zelo obsežna in da jo bom le stežka raziskovala, če si postavim problem preširoko.

3.2 Zbiranje informacij (metoda analize in sinteze)

Moje raziskovalno delo se je pričelo z zbiranjem informacij o obstoječih spletnih prevarah. Ugotovila sem, da jih obstaja ogromno in da o nekaterih še nikoli nisem slišala. Nato sem se osredotočila na tiste spletne prevare, ki lahko ogrozijo najstnike. Na podlagi prebranega sem nato zapisala teoretični del. Iz zbranih podatkov pa sem prišla do nekih sklepov in predvidevanj, na podlagi katerih sem si nato zastavila cilje raziskovalne naloge.

3.3 Opredelitev hipotez in izbira metode dela

Osredotočila sem se predvsem na vprašanje, koliko so najstniki seznanjeni s spletnimi prevarami, s katerimi se lahko med uporabo spleta srečajo in ali znajo v takšnih primerih pravilno odreagirati. Ob pregledu literature sem postavila nekaj domnev o najstnikih na naši šoli in njihovem odnosu do spletnih prevar. Zastavila sem si šest hipotez, ki sem jih nato poskusila dokazati ali ovreči. Po postavitvi hipotez sem se odločila za metodo anketiranja, saj sem na tak način prišla do informacij, ki sem jih potrebovala za preverjanje hipotez.

3.4 Zbiranje podatkov (metoda anketiranja)

V namen raziskave sem sestavila dva anketna vprašalnika. Pri je vseboval 18 vprašanj, drugi pa 13 vprašanj. Za izdelavo ankete sem uporabila brezplačno odprtokodno aplikacijo za spletno

[26] file:///C:/Users/Anita/Downloads/Phising%20-%20Kako%20se%20izogniti%20prevari%20(1).pdf (12.1.2020 13:09)

anketiranje 1KA. Učenci so na vprašanja odgovorili med razredno uro v računalniški učilnici. Izpolnjene vprašalnike sem nato analizirala.

Slika 1:Učenci med reševanjem ankete

3.4.1 Opis eksperimentalne skupine

V okviru raziskovalne naloge sem izvedla dve anketi med učenci naše šole, starimi od 12 do 15 let.

Tabela 1: Število in spol anketirancev v prvi anketi

Število anketirancev (prva anketa)	
Število fantov	79
Število deklet	80
Skupaj	159

Tabela 2: Število in spol anketirancev v drugi anketi

Število anketirancev (druga anketa)	
Število fantov	75
Število deklet	66
Skupaj	141

3.4.2 Potek pridobivanja podatkov in predstavitev spletnih prevar

Najprej sem izvedla prvo anketo. Po analizi rezultatov prve ankete, sem izvedla predstavitve učencem 7., 8. in 9. razreda naše šole. Predstavitve so potekale med razrednimi urami, razdelila

sem jim tudi letake. Predstavila sem jim spletne prevare, o katerih sem v anketnih vprašalnikih spraševala in za katere sem ugotovila, da jih ne poznajo preveč dobro. To so: nevarnosti javnih brezplačnih brezžičnih oz. Wi-Fi omrežij, spletno ribarjenje in manipulacija video posnetkov.

Slika 2: Letak o spletnih prevarah 1. stran

Slika 3:Letak o spletnih prevarah 2. stran

3.4.3 Primerjanje rezultatov (metoda anketiranja in primerjalna metoda)

Izvedla sem še drugo anketo, ki je ponovno spraševala o poznavanju spletnih prevar, ki lahko ogrožajo najstnike. Analizirala sem rezultate, nato pa še primerjala rezultate prvega in drugega vprašalnika med seboj.

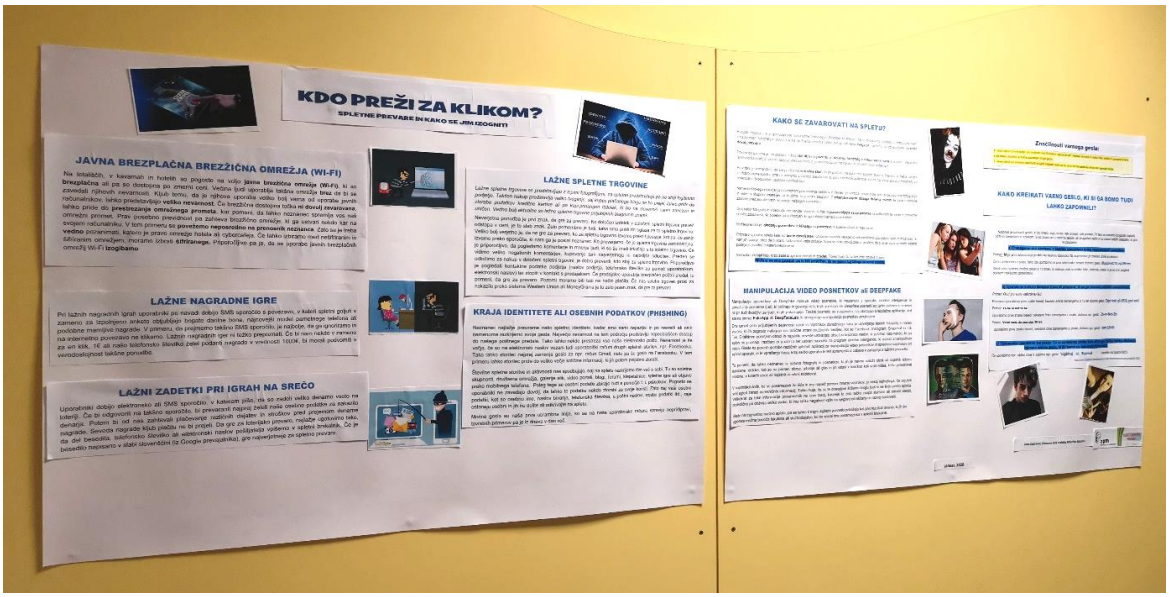
3.5 Analiza rezultatov (induktivno – deduktivna metoda)

Na podlagi deleža učencev, ki so bili nekega mnenja, sem sklepala na mnenje vse populacije najstnikov. Poudariti želim, da pridobljeni podatki niso verodostojni za natančno sklepanje, saj na podlagi tako majhnega vzorca ne moremo sklepati na celotno populacijo.

3.6 Zaključki

Na podlagi analize rezultatov sem nato potrdila oz. ovrgla svoje hipoteze ter prišla do ideje za rešitev zastavljenega raziskovalnega problema.

Slika 4:Predstavitev letaka o spletnih prevarah pri razredni uri



Slika 5:Plakata o spletnih prevarah

4 REZULTATI

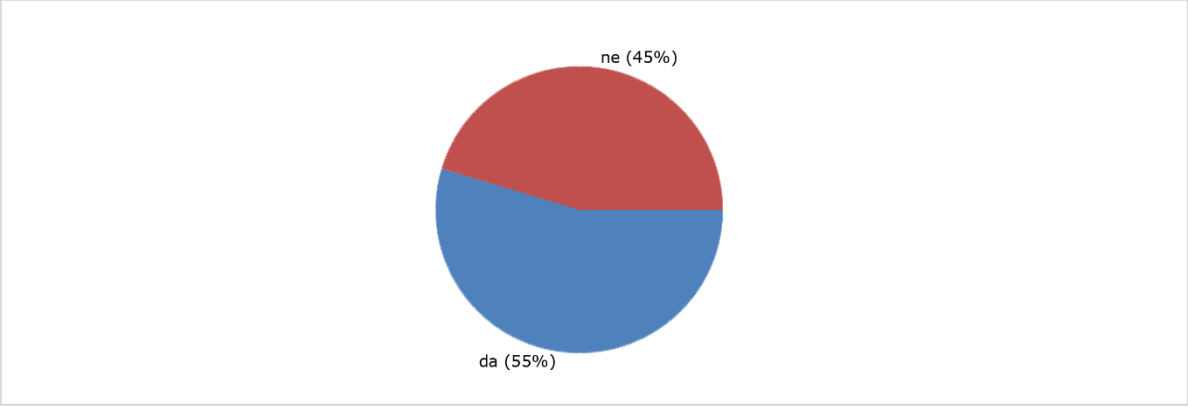
4.1 Vzorec in zbiranje podatkov

Anketiranje sem izvedla meseca decembra 2019. Ankete so izpolnjevali učenci od 7. do 9. razreda. Anketa je bila anonimna in so jo anketiranci izpolnjevali samostojno. V nadaljevanju so prikazani rezultati ankete. Predstavljeni so samo rezultati, ki so se mi zdeli najzanimivejši in so me pripeljali do novih spoznanj.

4.1.1 Rezultati prvega anketnega vprašalnika

1. **Si že kdaj dobil/a sporočilo, v katerem je pisalo, da si zmagal/a na nagradni igri ali zadel/a na loteriji?**

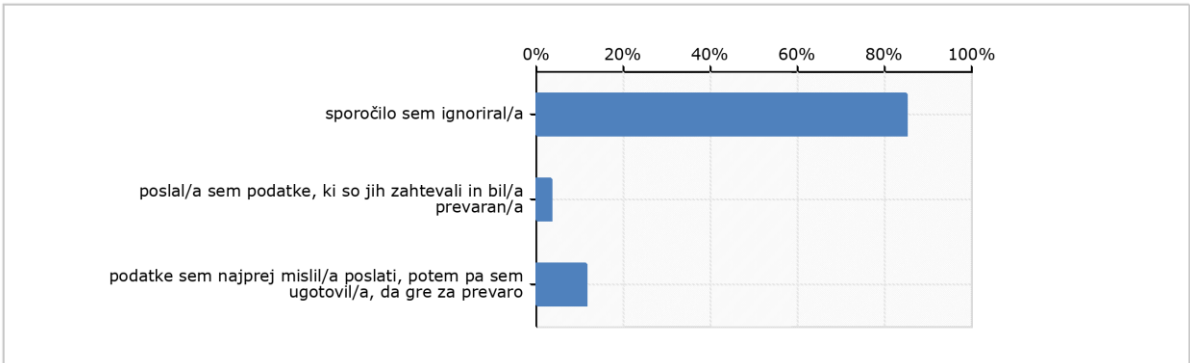
Graf 1:Si že kdaj dobil/a sporočilo, v katerem je pisalo, da si zmagal/a v nagradni igri ali zadel/a na loteriji? (n = 159)



Iz grafikona lahko razberemo, da je 55% odstotkov anketirancev že prejelo sporočilo, v katerem je pisalo, da so zmagali v nagradni igri ali zadeli na loteriji. Takšen rezultat sem tudi pričakovala, saj sem predvidevala, da se je večina učencev že srečala s to spletno prevaro.

2. **Kako si odreagiral/a, ko si prejel/a takšno sporočilo?**

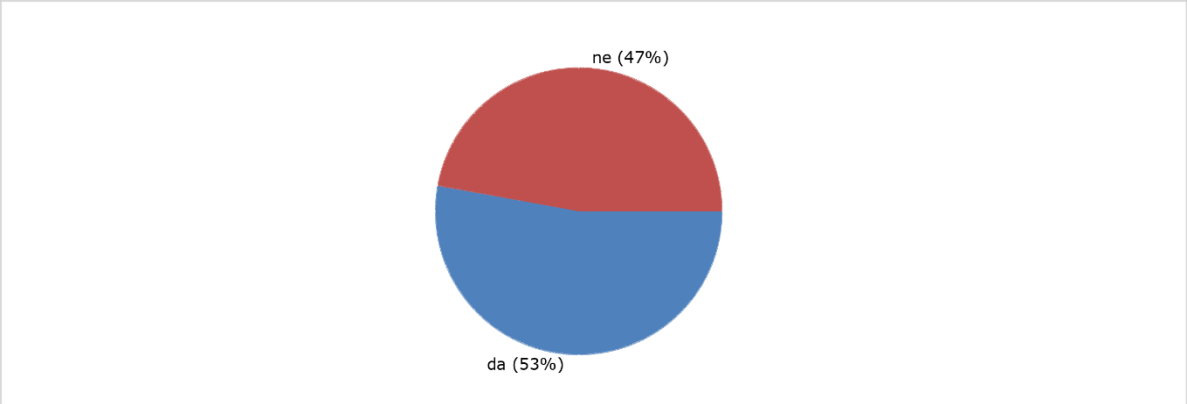
Graf 2: Kako si odreagiral/a, ko si prejel/a takšno sporočilo? (n = 87)



Na to vprašanje so odgovarjali le tisti anketiranci, ki so že prejeli sporočilo o zmagi pri nagradnih igrah. Iz grafa 2 je razvidno, da je 85% anketirancev sporočilo ignoriralo, 3% anketirancev so poslali podatke, ki so jih zahtevali v sporočilu in bili prevarani. 6% anketirancev pa je najprej razmišljajo o pošiljanju podatkov, potem pa so ugotovili, da gre za prevaro in tega niso storili. Pričakovala sem, da bo večina učencev označila drugi odgovor, saj sem mislila, da večina ne odreagira pravilno ob soočenju s to spletno prevaro.

3. **Si že kdaj, ko si nakupoval/a v spletni trgovini pomislil/a, da gre morda za prevaro?**

Graf 3: Si že kdaj, ko si nakupoval/a v spletni trgovini pomislil/a, da gre morda za prevaro? (n = 159)

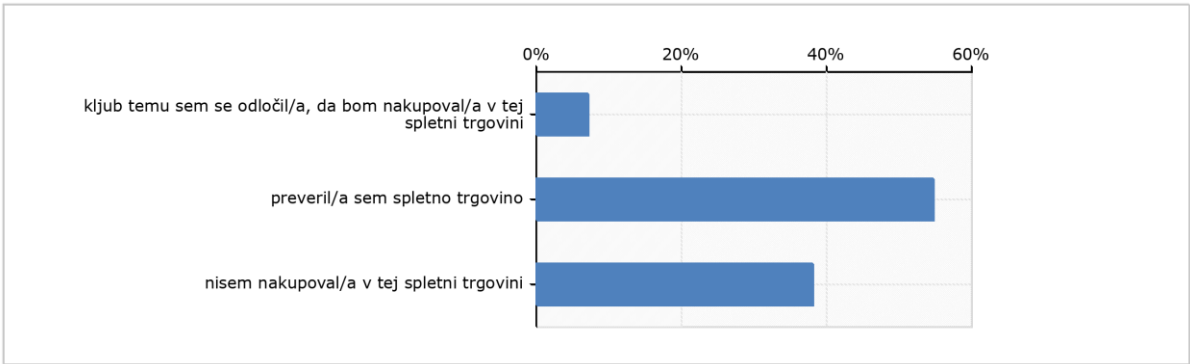


Iz grafa 3 je razvidno, da je 53% anketirancev, ki so nakupovali v spletni trgovini pomislilo, da

gre morda za prevaro, 47% pa o prevari ni razmišljalo. Vem, da veliko mojih sošolcev nakupuje po spletu, vendar si nisem mislila, da večina razmišlja o morebitni prevari.

4. Kaj si storil/a v tem primeru?

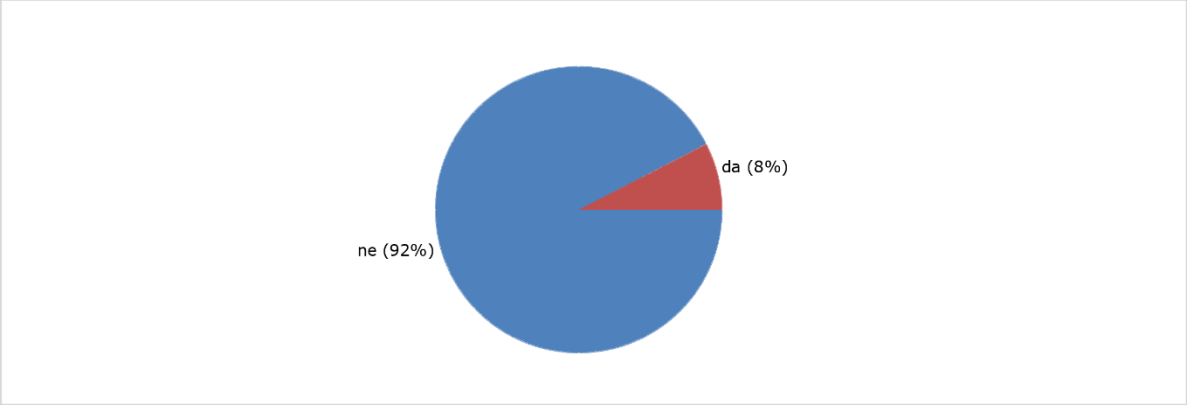
Graf 4:Kaj si storil/a v tem primeru? (n = 84)



Na to vprašanje so odgovarjali le tisti anketiranci, ki so ob nakupovanju po spletu pomislili, da gre za prevaro. 7% anketirancev se je kljub temu odločilo, da bodo nakupovali v tisti spletni trgovini. 55% anketirancev je spletno trgovino najprej preverilo. 38% anketirancev pa se za nakup v tisti spletni trgovini ni odločilo. Odgovori tega vprašanja so me zelo presenetili, saj si nisem mislila, da kar 93% učencev v primeru razmišljanja o spletni prevari pravilno odreagira.

5. Si bil/a kdaj prevaran/a pri prodajanju preko malih oglasov (npr. bolha)?

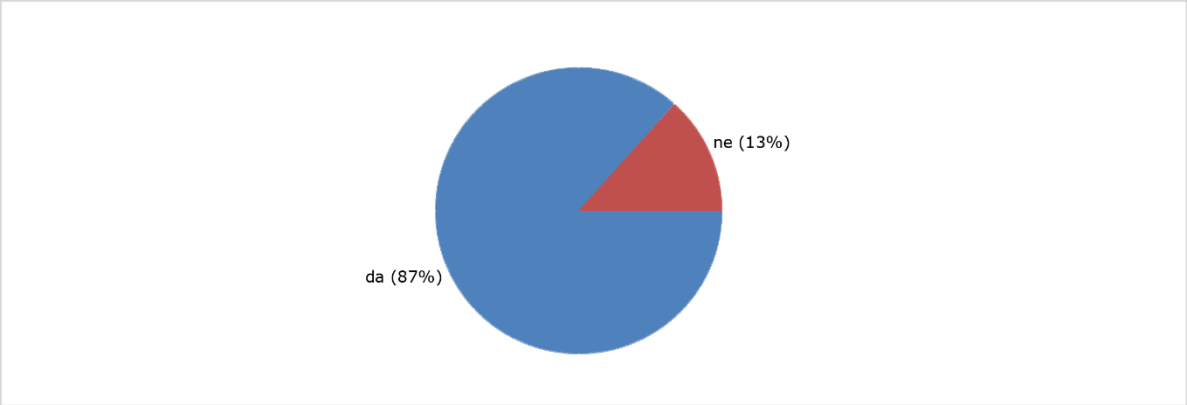
Graf 5: Si bil/a kdaj prevaran/a pri prodajanju preko malih oglasov (npr. bolha)? (n = 159)



Graf 5 prikazuje, da je bilo 8% anketirancev že prevaranih pri prodaji preko malih oglasov. 92% odstotkov anketirancev pa takšne izkušnje še ni imelo. Rezultat me ne preseneča, saj se zavedam, da najstniki še nimajo veliko izkušenj s prodajo preko malih oglasov. Kljub temu, se mi zdi zanimivo, da pa se je nekaj učencev že srečalo s to prevaro, saj tega nisem pričakovala.

6. **Meniš, da so tvoja gesla varna?**

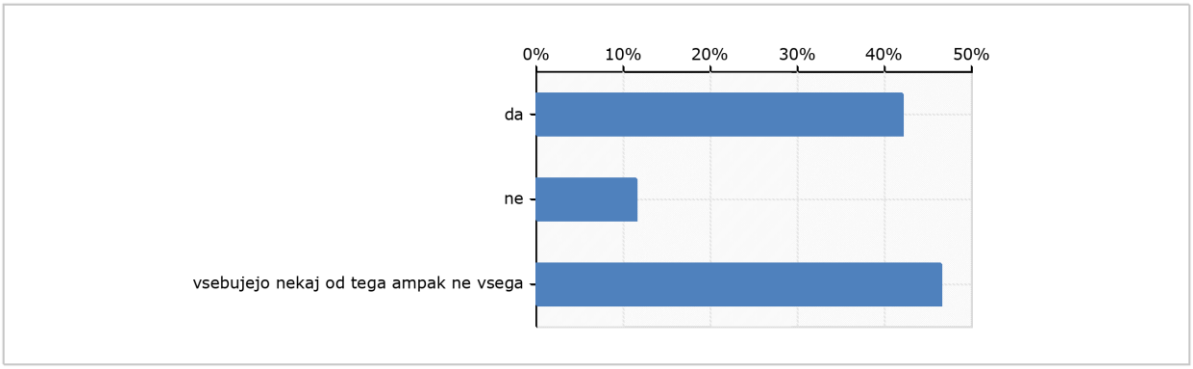
Graf 6:Meniš, da so tvoja gesla varna? (n = 157)



Od tega vprašanja dalje sta anketo zapustila 2 anketiranca in se je zato je število vzorca zmanjšalo na 157. Nad rezultati, ki so razvidni iz grafa 6, sem najbolj presenečena. Kar 87% anketirancev meni, da so njihova gesla varna.

7. **Ali tvoja gesla vsebujejo velike in male črke, številke in znake ter niso preveč očitna (ne vsebujejo tvojega imena, priimka ipd.)?**

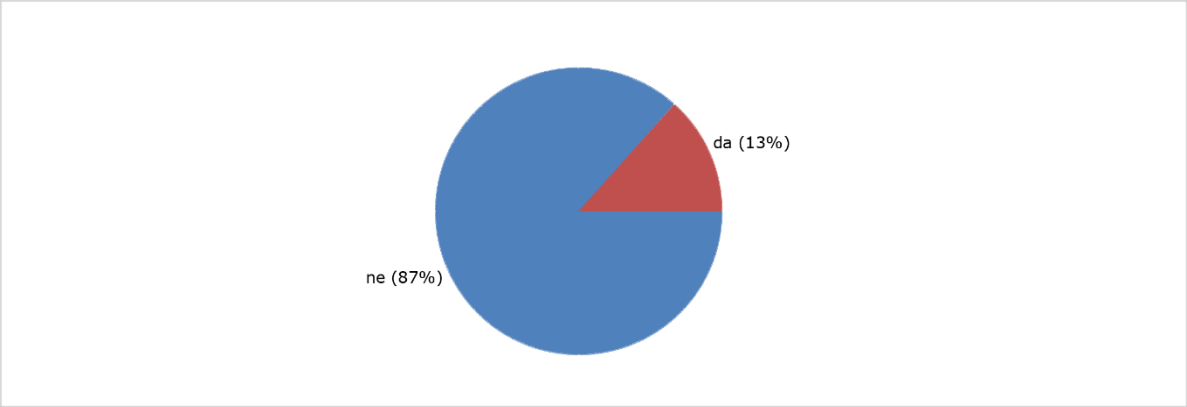
Graf 7: Ali tvoja gesla vsebujejo velike in male črke, številke in znake ter niso preveč očitna (ne vsebujejo tvojega imena, priimka ipd.)? (n = 157)



Iz grafa 7 lahko razberemo, da ima 42% anketirancev varna gesla, 46% anketirancev nima dovolj močnih gesel in 11% anketirancev uporablja šibka gesla. Iz grafa 6 lahko razberemo, da večina učencev misli, da so njihova gesla varna. Iz grafa 7 pa lahko razberemo, da temu ni tako. Razlog je, da najverjetneje učenci ne vedo, kaj je varno geslo.

8. Ali so ti že kdaj ukradli geslo (npr. vdrli v tvoj profil na družabnem omrežju)?

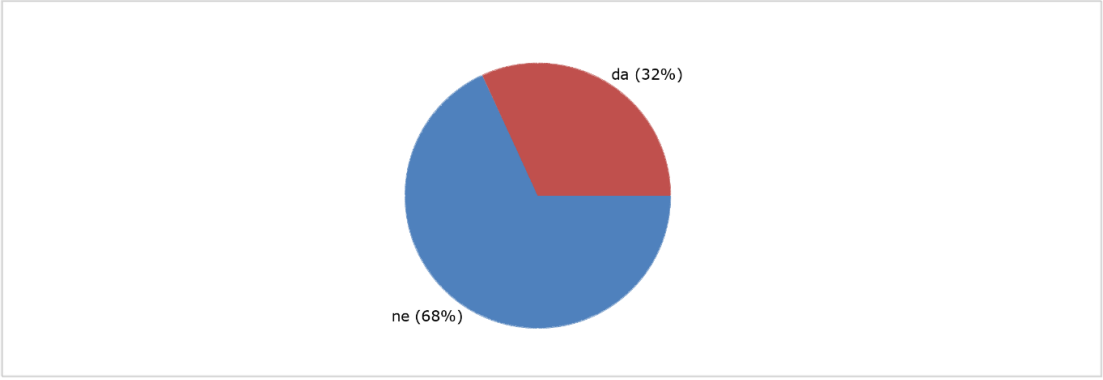
Graf 8:Ali so ti že kdaj ukradli geslo (npr. vdrli v tvoj profil na družabnem omrežju)? (n = 157)



Iz grafa 8 je razvidno, da ima 13% anketirancev že izkušnjo z ukradenim geslom, 87% pa ne. Število učencev s šibkimi gesli je zelo podobno številu učencev, kar pa še ne pomeni, da ki jim je že bilo ukradeno geslo. To pomeni, da slaba gesla res predstavljajo veliko nevarnost. Morda pa vseeno ni tako nevarno, če določeno geslo ne vsebuje vseh sestavnih delov varnega gesla (npr. ne vsebuje velikih črk).

9. Ali kdaj uporabljaš javne računalnike (v kavarnah, knjižnicah ipd.)?

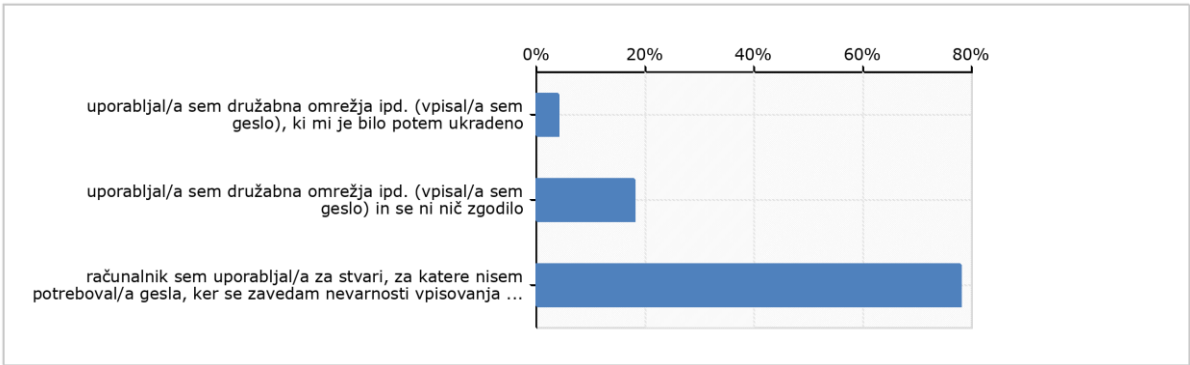
Graf 9: Ali kdaj uporabljaš javne računalnike (v kavarnah, knjižnicah ipd.)? (n = 157)



Iz grafa 9 je razvidno, da 32% anketirancev kdaj uporablja javne računalnike, 68% pa ne. Verjetno javnih računalnikov ne uporablja zelo veliko učencev, ker sploh pridejo v stik z njimi, saj imajo na razpolago svoje računalnike in druge mobilne naprave.

10. Za kaj si uporabljal/a takšen računalnik?

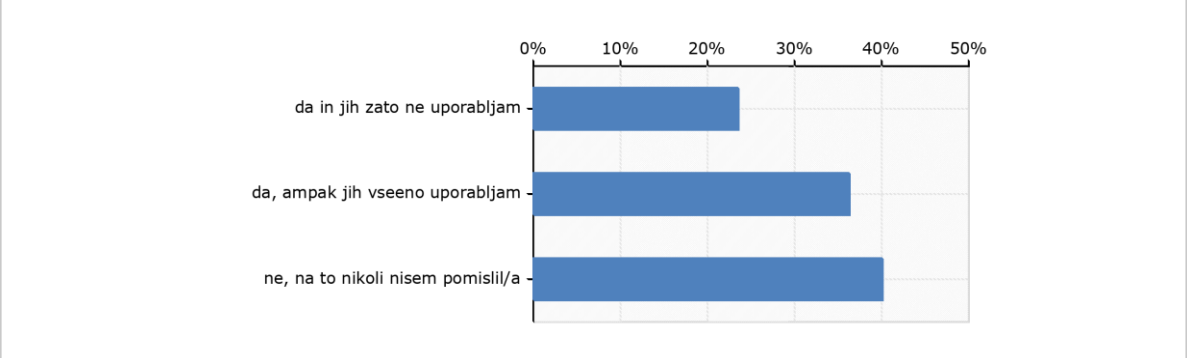
Graf 10: Za kaj si uporabljal/a takšen računalnik? (n = 50)



Na to vprašanje so odgovarjali le tisti, ki kdaj uporabljajo javne računalnike. Iz grafa 10 lahko razberemo, da je le 4% anketirancev (2 anketiranca) na javnem računalniku uporabljalo družbena omrežja, pri čemer so vpisali svoje geslo, ki jim je bilo potem ukradeno. 18% anketirancev kljub vpisu gesla na javnem računalniku ni imelo slabih izkušenj. 78% anketirancev pa je javni računalnik uporabljalo za stvari, za katere niso potrebovali gesla, ker se zavedajo nevarnosti vpisovanja gesel v javni računalnik. Morda je znanje učencev na tem področju boljše zaradi različnih šolskih predavanj, ki smo jih imeli.

11. Se zavedaš, da je lahko uporaba javnih brezplačnih Wi-Fi omrežij nevarna?

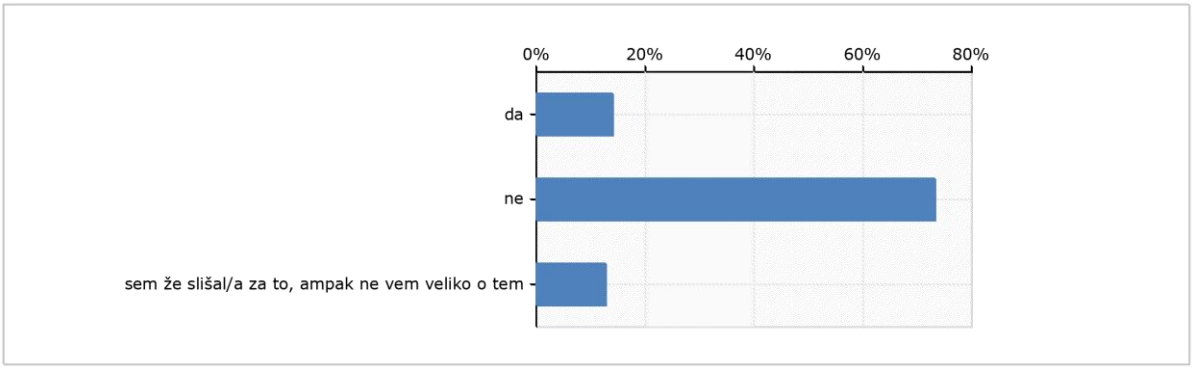
Graf 11: Se zavedaš, da je lahko uporaba javnih brezplačnih Wi-Fi omrežij nevarna? (n = 157)



Iz grafa 11 je razvidno, da se 24% anketirancev zaveda nevarnosti uporabe javnih brezplačnih Wi-Fi omrežij in jih zato ne uporablja. 36% anketirancev se zaveda nevarnosti uporabe Wi-Fi omrežij, ampak jih vseeno uporablja. 40% anketirancev pa o nevarnostih uporabe Wi-Fi omrežij ni nikoli razmišljala. Predvidevam, da je takšen rezultat, ker jih nihče nikoli ni obvestil o tej nevarnosti, morda pa uporabniki s tem še niso imeli slabih izkušenj.

12. Ali veš kaj je Deepfake?

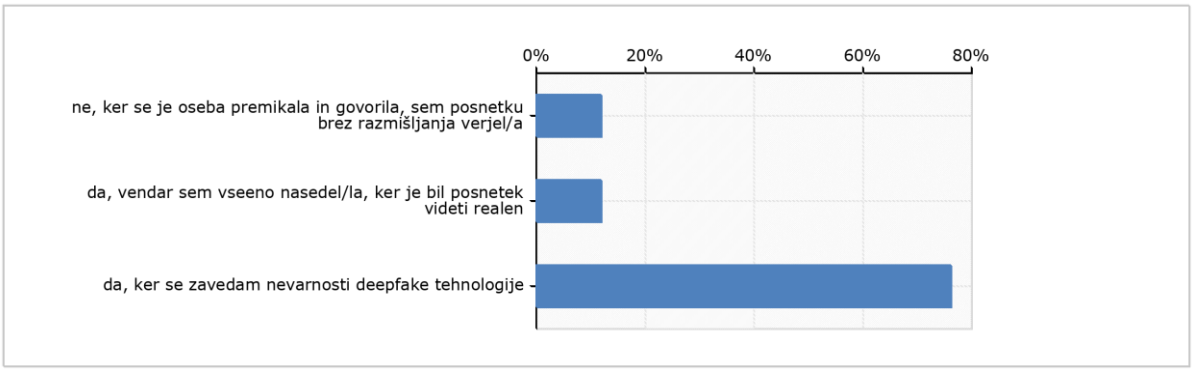
Graf 12: Ali veš kaj je Deepfake? (n = 157)



Iz grafa 12 lahko razberemo, da je 14% anketirancev že slišalo o Deepfake posnetkih in vedo, kaj to je. 13% anketirancev je že slišalo za Deepfake, ampak ne vedo veliko o njem. 73% anketirancev še ni slišalo za Deepfake, kar me ne čudi, saj je to precej nova stvar.

13. Ali si ob ogledu določenega posnetka na družabnem omrežju ali internetu dvomil/a o njegovi resničnosti?

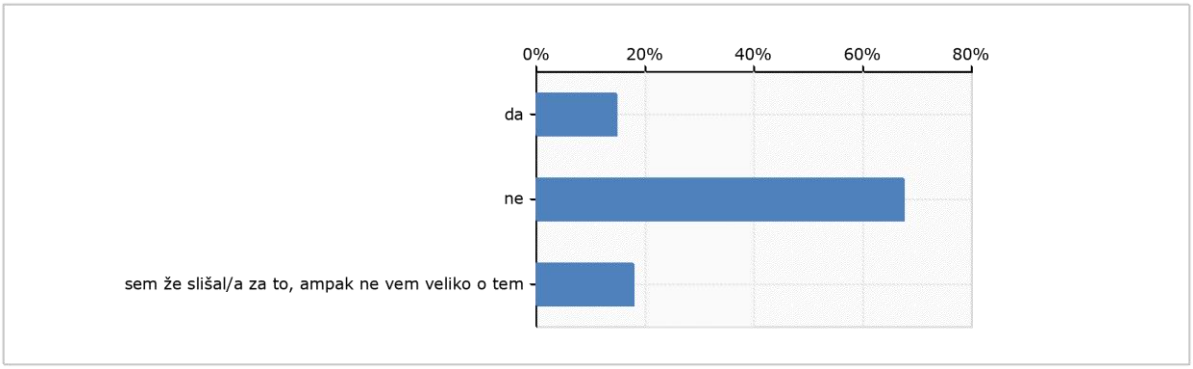
Graf 13: Ali si kdaj ob ogledu določenega posnetka na družabnem omrežju ali internetu dvomil/a o njegovi resničnosti? (n = 42)



Na to so odgovarjali samo tisti anketiranci, ki so že kdaj slišali za Deepfake tehnologijo. 12% anketirancev ni dvomilo o resničnosti določenega posnetka na družbenem omrežju ali spletu, ker se je oseba premikala in govorila. 12% anketirancev je dvomilo o resničnosti posnetka, vendar so vseeno nasedli, ker je bil posnetek videti realen. 67% anketirancev je dvomilo o resničnosti posnetka, ker se zavedajo nevarnosti Deepfake tehnologije. Če poznaš tehnologijo, je večja verjetnost, da prepoznaš Deepfake kot če sploh ne veš, da obstaja. Zato je zelo pomembno, da so ljudje seznanjeni z novimi tehnologijami.

14. Ali veš kaj je Phishing?

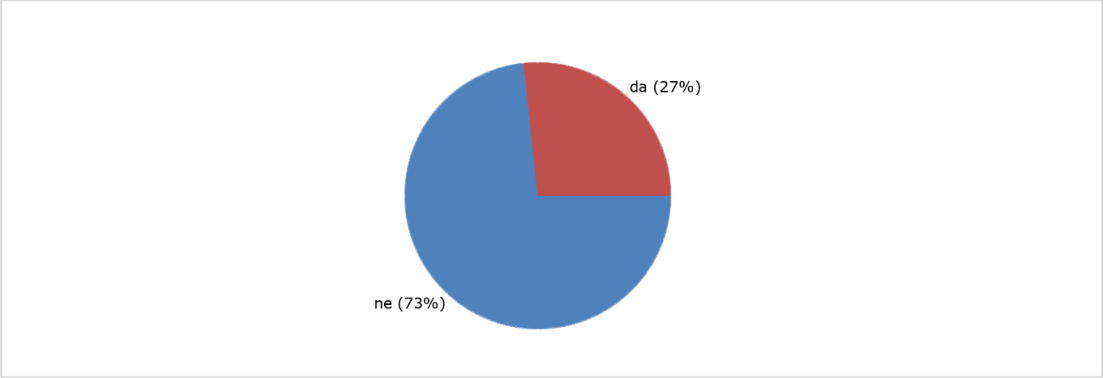
Graf 14: Ali veš kaj je Phishing? (n = 157)



Iz grafa 14 lahko razberemo, da 15% anketirancev ve, kaj je spletno ribarjenje oz. Phishing. 68% anketirancev za Phishing še ni slišalo. 18% anketirancev pa je za Phishing že slišalo, ampak ne vedo veliko o njem. To pomeni, da so učenci premalo poučeni o nekaterih spletnih prevarah, ki pa niso nič manj pogoste. Takšen rezultat sem tudi pričakovala.

15. Ali si kdaj prejel/a elektronsko sporočilo, ki bi naj bilo poslano od ponudnika spletne storitve, v katerem te ta prosi za ponovni vpis gesla in osebnih podatkov na določeni spletni strani?

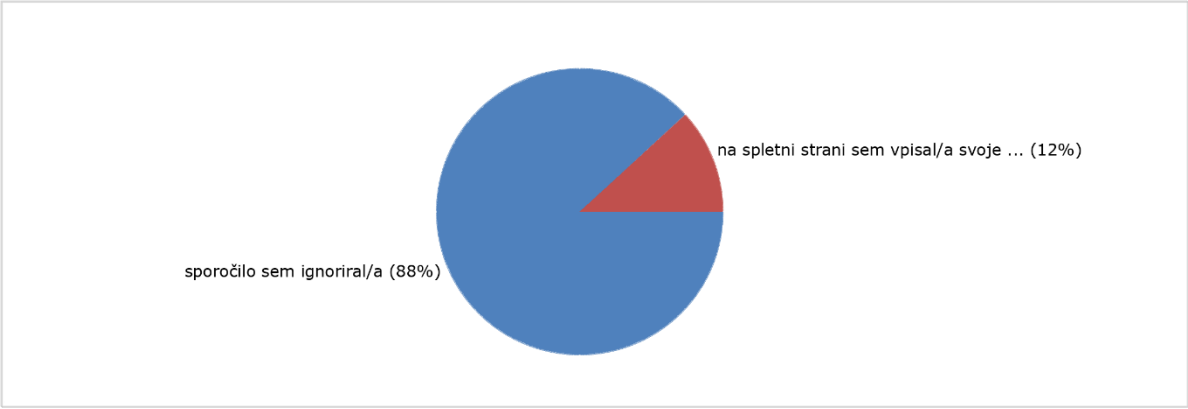
Graf 15: Ali si kdaj prejel/a elektronsko sporočilo, ki bi naj bilo poslano od ponudnika spletne storitve, v katerem te ta prosi za ponovni vpis gesla in osebnih podatkov na določeni spletni strani? (n = 157)



Iz grafa 15 je razvidno, da se je 27% anketirancev že srečalo z zahtevo po ponovnem vpisu gesla na določeni spletni strani. 73% odstotkov anketirancev se s tem še ni srečalo. Ta rezultat me je zelo presenetil, saj sem mislila, da se ni noben učenec še ni srečal s Phishing prevaro ali pa da se jih je zelo malo.

16. Kaj si storil/a v te primeru?

Graf 16: Kaj si storil/a v tem primeru? (n = 42)



Na to vprašanje so odgovorili le anketiranci, ki so že kdaj dobili elektronsko sporočilo z zahtevo po ponovnem vpisu gesla. 12% jih je na spletni strani vpisalo svoje osebne podatke in geslo. 88% anketirancev pa je sporočilo ignoriralo. Presenetilo me je, da je večina učencev pravilno odreagirala. Morda je tako zaradi dobre poučenosti o lažnih nagradnih igrah, saj učenci vedo, da morajo sporočila s sumljivo vsebino ignorirati.

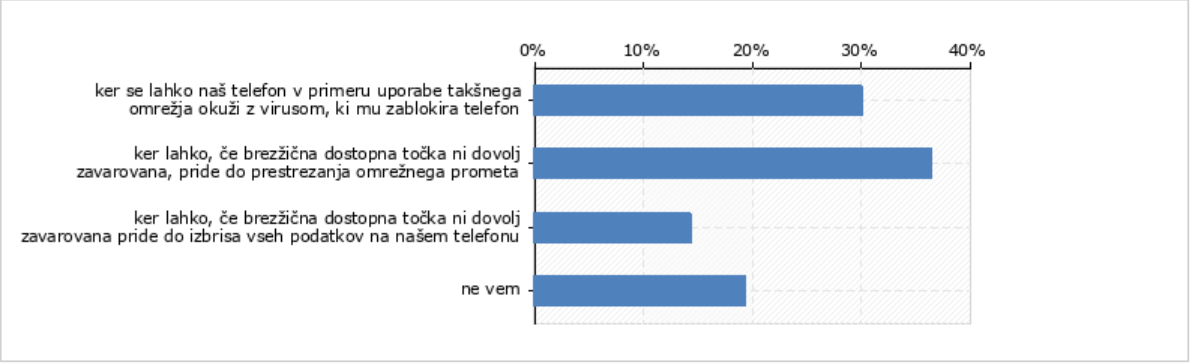
4.2 Zbiranje podatkov (metoda anketiranja)

Anketiranje sem izvedla meseca januarja 2020. Anketo sem izvedla, ker sem želela ugotoviti, če so učenci po predstavitvi, ki sem jo izvedla, bolj poučeni o nekaterih vrstah spletnih prevar. Ankete so izpolnili učenci od 7. do 9. razreda. Anketa je bila anonimna in so jo anketiranci izpolnjevali samostojno. V nadaljevanju so prikazani rezultati druge ankete.

4.2.1 Rezultati drugega anketnega vprašalnika

1. **Zakaj je uporaba javnih brezplačnih brezžičnih Wi-Fi omrežij lahko nevarna?**

Graf 17: Zakaj je uporaba javnih brezplačnih brezžičnih Wi-Fi omrežja lahko nevarna? (n = 140)

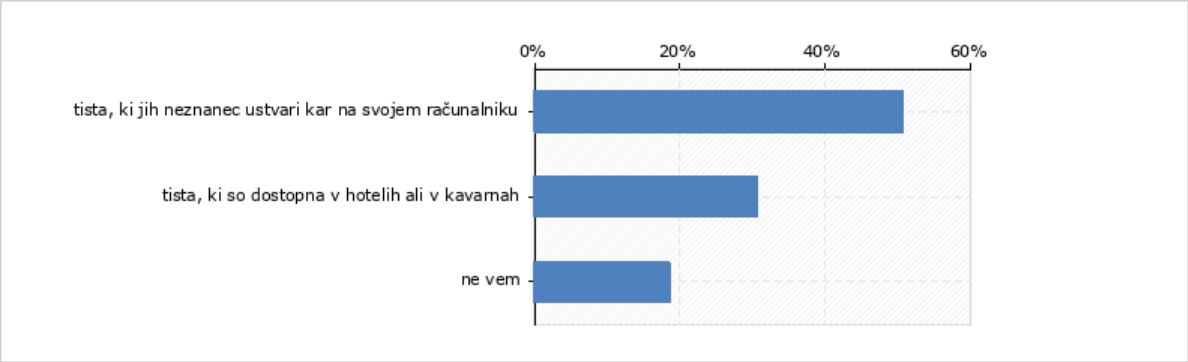


Od tega vprašanja dalje je 1 anketiranec zapustil anketo in je zato 140 anketirancev obravnavanih kot celota. 36% odstotkov anketirancev je izbralo drugi, pravilen odgovor. 45% anketirancev je izbralo napačen odgovor. 19% anketirancev pa ni vedelo odgovora na to vprašanje. Ta rezultat me je zelo presenetil, saj sem bila prepričana, da bodo učenci po moji

predstavitvi bolje seznanjeni z nevarnostmi uporabe brezplačnih Wi-Fi omrežij. Razlog za takšen rezultat je mogoče tudi to, da vrstniki niso bili dovolj pozorni pri poslušanju predstavitve.

2. Katera brezžična omrežja zahtevajo posebno previdnost?

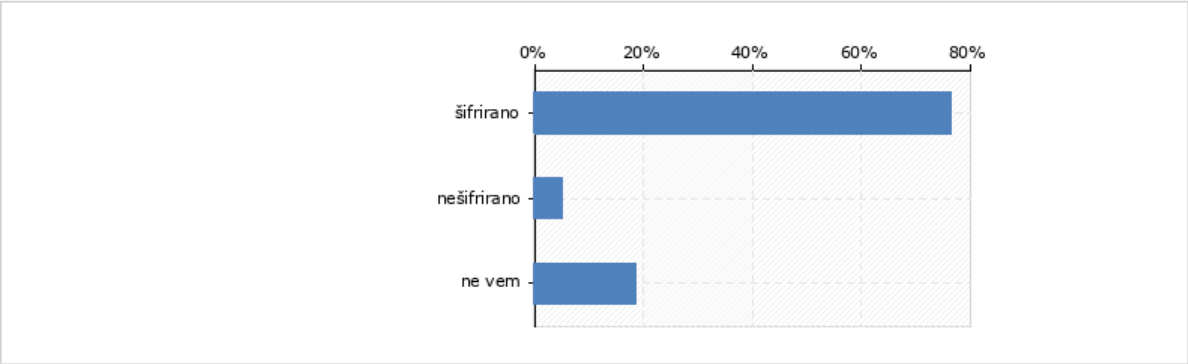
Graf 18: Katera brezžična omrežja zahtevajo posebno previdnost? (n = 140)



Iz grafa 18 lahko razberemo, da je 51% anketirancev izbralo prvi odgovor, kar pomeni, da vedo, da morajo biti posebej previdni pri uporabi omrežij, ki jih nekdo ustvari na svojem računalniku. 31% anketirancev je izbralo drugi odgovor, ki je nepravilen, 19% anketirancev pa ni poznalo pravilnega odgovora na vprašanje.

3. Katero brezžično omrežje moramo izbrati, če lahko izbiramo med šifriranim in nešifriranim?

Graf 19: Katero brezžično omrežje moramo izbrati, če lahko izbiramo med šifriranim in nešifriranim? (n = 140)

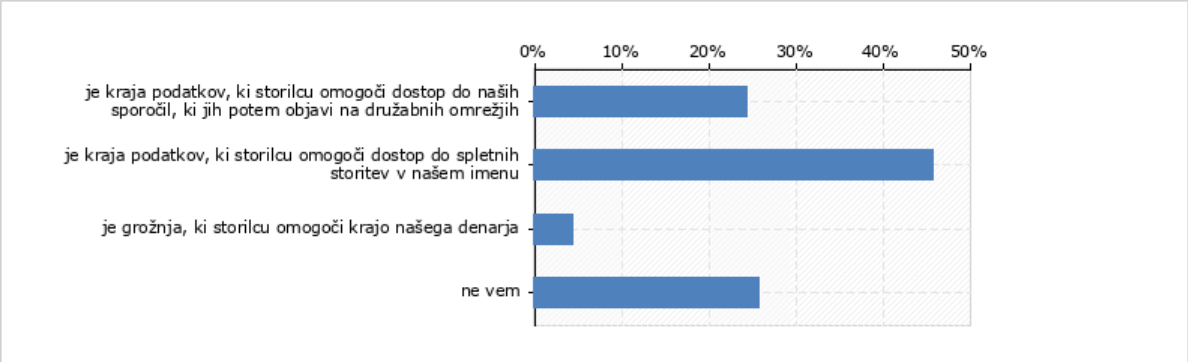


Iz grafa 19 je razvidno, da je 76% anketirancev izbralo prvi odgovor, kar pomeni, da vedo, da

je treba izbirati šifrirana omrežja. 5% anketirancev je izbralo drugi odgovor, ki je nepravilen. 19% anketirancev ni poznalo pravilnega odgovora na vprašanje. Predvidevam, da je večina učencev izbrala pravilen odgovor, ker je bil odgovor precej logičen.

4. Kaj je Phishing?

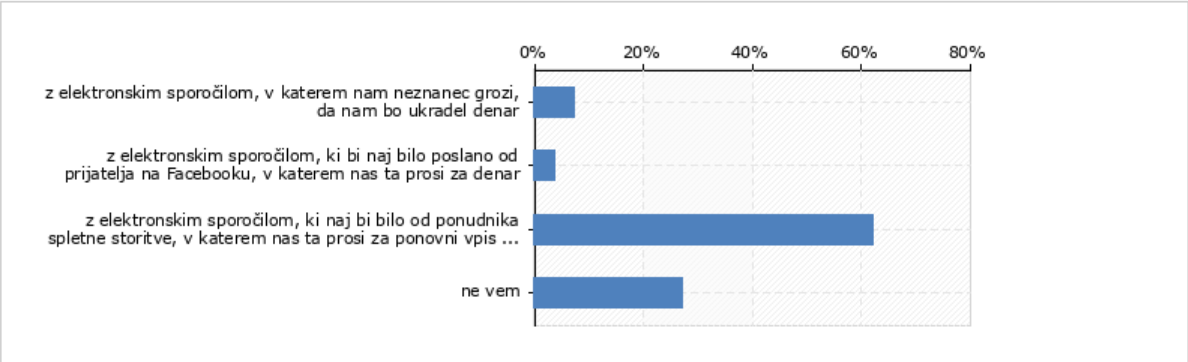
Graf 20: Kaj je Phishing? (n = 140)



Iz grafa 20 je razvidno, da je 46% anketirancev izbralo drugi, pravilen odgovor in da so vedeli, kaj je Phishing. 28% anketirancev je izbralo prvi ali tretji odgovor, ki sta nepravilna. 26% anketirancev ni poznalo odgovora na vprašanje. Pričakovala sem več pravilnih odgovorov. Ugotavljam, da najstniki slabo poslušajo oz. mogoče jaz Phishing prevare nisem dovolj natančno predstavila.

5. Kako se začne tipična Phishing prevara?

Graf 21: Kako se začne tipična Phishing prevara? (n = 140)

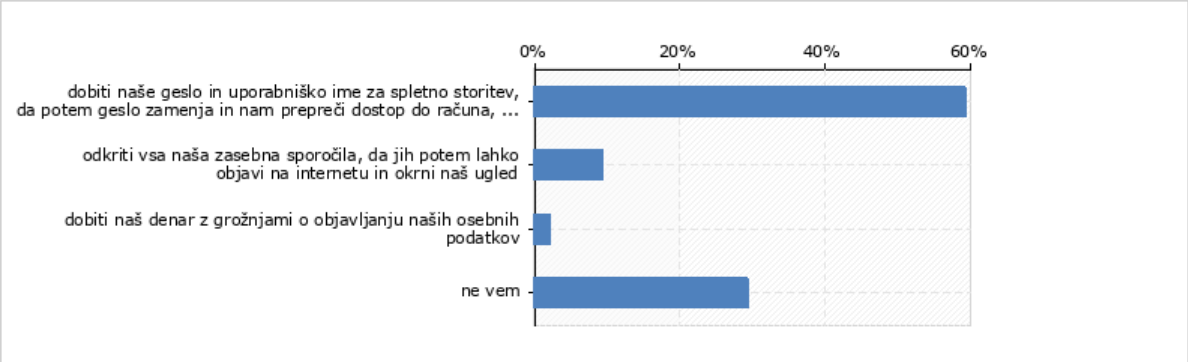


Iz grafa 21 je razvidno, da je 62% anketirancev označilo tretji, pravilen odgovor in da vedo,

kako se prične tipična Phishing prevara. 11 % anketirancev je označilo nepravilna odgovora in 27% anketirancev je označilo, da ne poznajo odgovora na vprašanje. Predvidevam, da so anketiranci izbrali pravilen odgovor, ker se jim je zdel najbolj verjeten oz. logičen.

6. Kaj je cilj storilca Phishing prevare?

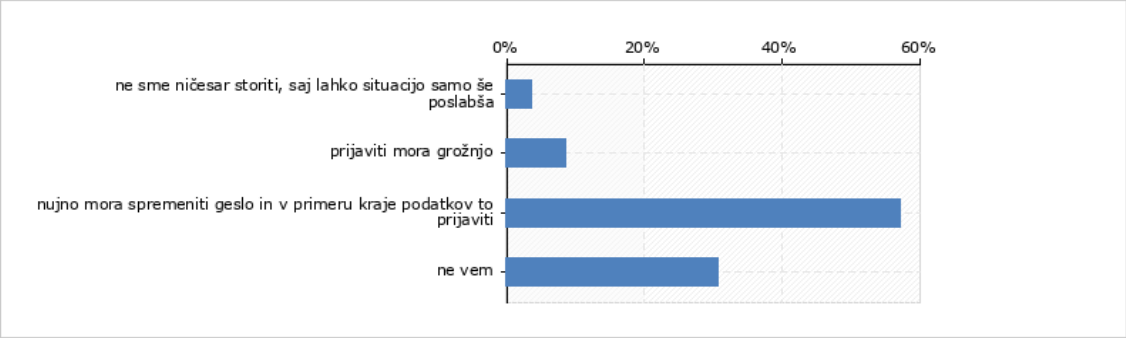
Graf 22: Kaj je cilj storilca Phishing prevare? (n = 140)



Iz grafa 22 lahko razberemo, da 59% anketirancev pozna cilje storilcev Phishinga. 11% anketirancev ne pozna resničnega cilja Phishinga in 29 % anketirancev ni poznalo pravega odgovora na vprašanje.

7. Kaj mora oseba storiti v primeru, da je vpisala geslo in osebne podatke na Phishing strani?

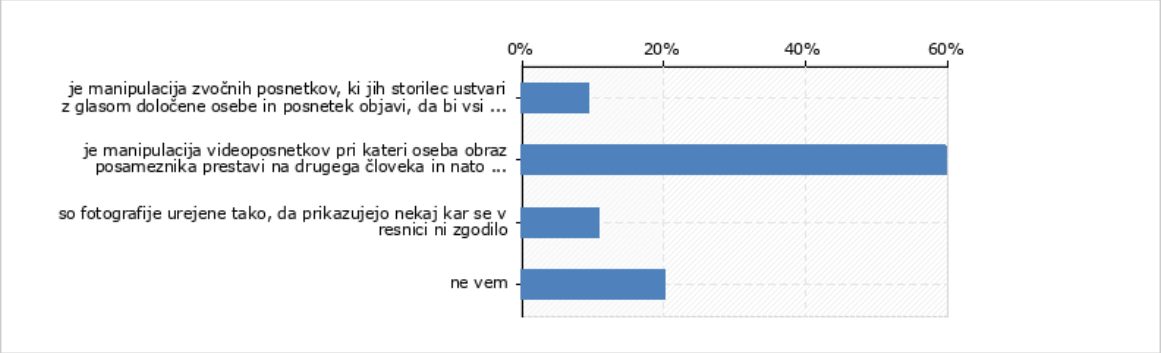
Graf 23: Kaj mora oseba v storiti v primeru, da je vpisala geslo in osebne podatke na Phishing strani? (n = 140)



Iz grafa 23 je razvidno, da se 57% anketirancev zaveda, kaj je potrebno storiti v primeru, da so vpisali osebne podatke in geslo na Phishing strani. 13% anketirancev ne bi ustrezno ravnalo v primeru, da bi prišlo do vpisa osebnih podatkov in gesla na Phishing strani. 31% anketirancev pa ne bi vedelo, kako odreagirati.

8. Kaj je Deepfake?

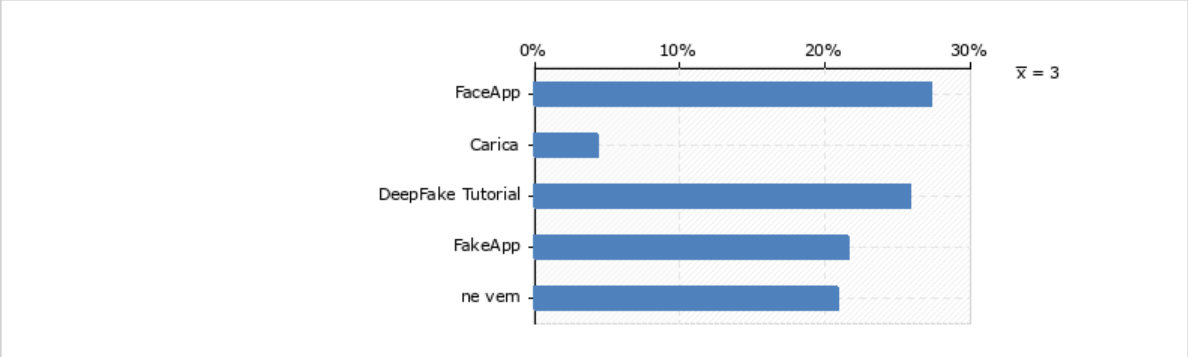
Graf 24: Kaj je Deepfake? (n = 139)



Od tega vprašanja dalje je anketo zapustil 1 anketiranec in je zato 139 anketirancev obravnavanih kot celota. Iz grafa 24 je razvidno, da je 60% anketirancev poznalo pomen izraza Deepfake. 20 % anketirancev je izbralo napačna odgovora, 20% anketirancev pa ni poznalo pomena izraza Deepfake. Ta odgovor me ni presenetil, saj je bilo med predstavitvijo spletnih prevar očitno, da najstnike ta spletna prevara najbolj zanima. Predvidevam, da je razlog za to njihov vsesplošen interes za ustvarjanje video vsebin. Presenetilo me je dejstvo, da so vsi želeli izvedeti več o aplikaciji FakeApp, da bi se lahko tudi sami preizkusili v ustvarjanju Deepfake posnetkov.

9. Kako se imenuje najbolj znana aplikacija za ustvarjanje Deepfake posnetkov?

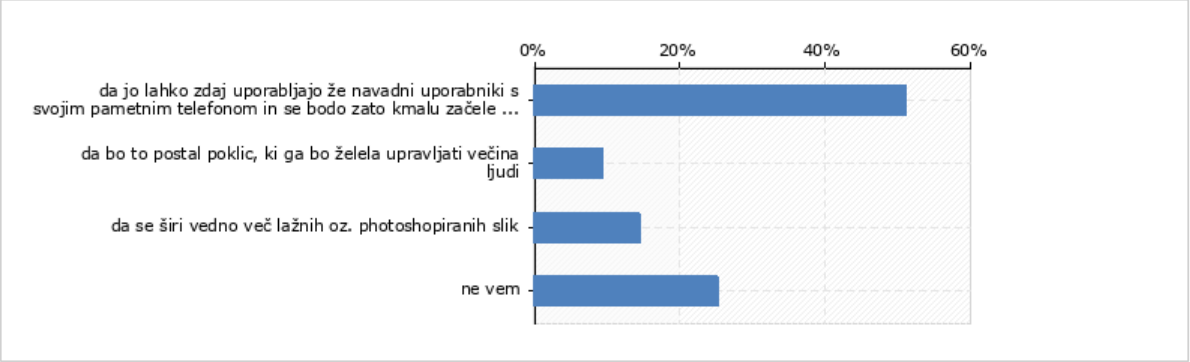
Graf 25: Kako se imenuje najbolj znana aplikacija za ustvarjanje Deepfake posnetkov? (n = 139)



Iz grafa 25 je razvidno, da si je le 22% odstotkov anketirancev zapomnilo ime najbolj znane aplikacije za manipulacijo videoposnetkov.

10. Kaj je najbolj zaskrbljujoče glede Deepfake tehnologije?

Graf 26: Kaj je najbolj zaskrbljujoče glede Deepfake tehnologije? (n = 139)

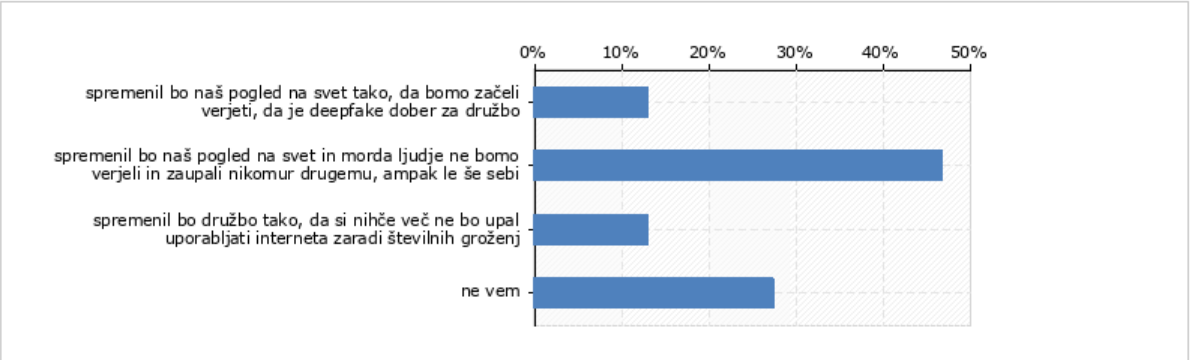


Iz grafa 26 lahko razberemo, da se 52% anketirancev zaveda resnične nevarnosti Deepfake tehnologije. 23% anketirancev je izbralo napačen odgovor in 25% anketirancev odgovora na vprašanje ni poznalo.

Ob odgovoru na vprašanje 9 in 10 sem se vprašala, kako natančno najstniki sploh poslušajo in koliko od slišanega si zapomnijo.

11. Kakšne bodo predvidene posledice Deepfaka?

Graf 27: Kakšne bodo predvidevane posledice Deepfaka? (n = 139)



Iz grafa 27 se da razbrati, da se 47% anketirancev zaveda razsežnosti vpliva Deepfake tehnologije. Presenečena sem bila nad 13% anketirancev, ki menijo, da bodo ljudje verjeli, da je ta tehnologija dobra za družbo. Upam, da ta odgovor ni posledica mišljenja, da se učencem zdi ta tehnologija pozitivna stvar. 27% anketirancev ni poznalo odgovora na vprašanje.

5 ANALIZA HIPOTEZ

Hipoteza 1: Večina učencev spletnih prevar ne prepozna.

Prvo hipotezo zavrnem, saj je prva anketa prikazala, da večina učencev spletne prevare prepozna že pred soočenjem in večina tudi pravilno odreagira. Pri 4. vprašanju je 85% vseh učencev, ki so odgovorili na to vprašanje, ignoriralo sporočilo, v katerem je pisalo, da so zmagali na nagradni igri ali zadeli na loteriji. Po tem lahko sklepamo, da so spletno prevaro prepoznali takoj ob prejemu sporočila. Pri 5. vprašanju je 53% anketirancev med nakupovanjem v neznani spletni trgovini pomislilo, da gre za prevaro, kar pomeni, da je več kot pol učencev prepoznalo prevaro in pravilno odreagiralo. To je možno videti tudi pri naslednjem vprašanju, saj je 55% vseh učencev, ki so odgovorili na to vprašanje ob dvomu glede spletne trgovine, trgovino preverilo, 38% učencev pa ni nakupovalo v tej spletni trgovini. Pri 15. vprašanju je 76% učencev, ki so odgovorili na to vpašanje, ob ogledu določenega posnetka na družbenem omrežju ali spletu dvomilo o njegovi resničnosti, ker se zavedajo nevarnosti Deepfake tehnologije. Pri 18. vprašanju je 88% vseh učencev, ki so odgovorili na to vprašanje, ob prejemu elektronskega sporočila, ki bi naj bilo poslano od ponudnika spletne storitve, v katerem jih ta prosi za ponovni vpis osebnih podatkov in gesla na določeni spletni strani, sporočilo ignoriralo. Sklepam, da je večina učencev spletno prevaro prepoznalo.

Hipoteza 2: Večina učencev napačno odreagira, ko se sooči s spletno prevaro.

To hipotezo zavrnem, saj lahko iz rezultatov prve ankete sklepamo, da večina učencev pravilno odreagira ob soočenju s spletno prevaro. Pri 4. vprašanju je 85% vseh učencev, ki so odgovorili na to vprašanje, sporočilo v katerem je pisalo, da so zmagali na nagradni igri ali zadeli na loteriji ignoriralo. Pri 6. vprašanju je 55% vseh učencev, ki so odgovorili na to vprašanje, ob dvomu glede spletne trgovine, trgovino preverilo, 38% učencev pa ni nakupovalo v tej spletni trgovini. Pri 12. vprašanju je 78% vseh učencev, ki so odgovorili na to vprašanje, računalnik uporabljalo za stvari, za katere niso potrebovali gesla, ker se zavedajo nevarnosti vpisovanja gesel v javni računalnik. Pri 15. vprašanju je 76% vseh učencev, ki so odgovorili na to vprašanje, ob ogledu določenega posnetka na družbenem omrežju ali spletu dvomilo o njegovi resničnosti, ker se zavedajo nevarnosti Deepfake tehnologije. Pri 18. vprašanju je 88% vseh učencev, ki so

odgovorili na to vprašanje, ob prejemu elektronskega sporočila, ki bi naj bilo poslano od ponudnika spletne storitve, v katerem jih ta prosi za ponovni vpis osebnih podatkov in gesla na določeni spletni strani, sporočilo ignoriralo. Po tem lahko sklepamo, da so dobro poučeni o prevarah, s katerimi se pogosto srečujejo in tudi vedo kako odreagirati v takšni situaciji.

Hipoteza 3: Učenci se pogosto srečujejo s spletnimi prevarami.

To hipotezo delno potrdim in delno zavrnem. Iz rezultatov prve ankete je razvidno, da se večina učencev z nekaterimi prevarami srečuje pogosto, z drugimi pa nikoli. Pri 3. vprašanju je 55% učencev označilo, da so že dobili sporočilo v katerem je pisalo, da so zmagali pri nagradni igri ali zadeli na loteriji. Pri 7. vprašanju je samo 8% učencev označilo, da so že bili prevarani pri prodajanju preko malih oglasov, kar 92% pa je označilo da ne. Pri 10. vprašanju je le 13% učencev označilo, da so jim že kdaj ukradli geslo, 87% pa je označilo, da jim ga niso. Pri 17. vprašanju je 27% učencev označilo, da so kdaj prejeli elektronsko sporočilo, ki bi naj bilo poslano od ponudnika spletne storitve, v katerem jih je ta prosil za ponovni vpis gesla in osebnih podatkov na določeni spletni strani. 73% učencev pa je označilo, da takšnega sporočila še niso prejeli. Iz pridobljenih podatkov lahko sklepam, da se učenci pogosto srečujejo s prevaro lažnih nagradnih iger ter loterijsko prevaro. Manj učencev pa se je srečalo s prevaro pri prodajanju preko malih oglasov, krajo gesla ali Phishing sporočilom.

Hipoteza 4: Večina učencev nima varnih gesel.

Četrto hipotezo lahko na podlagi rezultatov prve ankete delno potrdim in delno zavrnem. Pri 8. vprašanju je 87% učencev označilo, da misli, da so njihova gesla varna, 13% pa jih je označilo da tega ne misli. Pri 9. vprašanju je 42% učencev označilo, da njihova gesla vsebujejo velike in male črke, številke in znake ter da niso preveč očitna, 11% pa je označilo, da njihova gesla tega ne vsebujejo. Če bi gledala samo ta dva odgovora, bi sklepala, da ima večina učencev varna gesla. Vendar pa je bilo pri 9. vprašanju možno označiti še en odgovor, ki ga je označilo 46% učencev in sicer, da njihova gesla vsebujejo nekaj od tega, ampak ne vsega. Varno geslo pa mora vsebovati vse lastnosti navedene v 9. vprašanju. To torej pomeni, da 46% učencev nima dovolj varnih gesel, kar je več kot 42%, ki pa varna gesla ima.

Hipoteza 5: Večina učencev ne ve, kaj sta Deepfake in Phishing.

Peto hipotezo lahko glede na rezultate prve ankete potrdim. Pri 14. vprašanju je kar 73% učencev označilo, da ne vedo, kaj je Deepfake in še nikoli niso niti slišali zanj. Pri 16. vprašanju je 68% učencev označilo, da ne vedo, kaj je Phishing in še nikoli niso slišali zanj. Po tem lahko sklepam, da večina učencev ne ve, kaj sta Deepfake in Phishing.

Hipoteza 6: Učenci bodo po predstavitvi letaka veliko bolje poučeni o Deepfake-u, Phishingu in javnih brezplačnih Wi-Fi omrežjih.

Glede na rezultate druge ankete, šesto hipotezo potrjujem. Pri 3. vprašanju druge ankete je sicer le 36% učencev vedelo, zakaj je uporaba javnih brezžičnih omrežij lahko nevarna. Nevarnost brezžičnih omrežij, ki jih neznanec ustvari na svojem računalniku je poznalo 51% učencev. Da je potrebno izbirati šifrirana brezžična omrežja je vedelo 76% učencev. Ti odgovori kažejo na dejstvo, da so se učenci večinoma dojeli, da je uporaba brezplačnih Wi-Fi omrežij lahko nevarna, vendar ne poznajo še dovolj dobro razlogov zakaj oz. še ne poznajo možnih negativnih posledic. 46% učencev je po predstavitvi vedelo, kaj je Phishing, 62% jih je tudi vedelo, kako se tipična Phishing prevara prične, 59% jih je poznalo cilj takšne prevare in 57% odstotkov bi vedelo, kako odreagirati v primeru, da so vpisali svoje osebne podatke ali geslo. Res je, da je po predstavitvi več učencev poznalo to prevaro, vendar menim, da je število učencev prenizko in da lahko sklepam, da jih veliko del te prevare ne pozna dovolj dobro. Pri poznavanju Deepfake tehnologije lahko iz rezultatov druge ankete sklepam, da so se učenci najbolj seznanili z Deepfake tehnologijo, predvidevam da zato, ker jim je glede na njihovo uporabo spleta najbliže oz. jim je bil ta del predstavitve najbolj zanimiv. Kljub temu se je pokazalo, da si podrobnih podatkov pri predstavitvi le niso zapomnili, saj si je le 22% odstotkov učencev zapomnilo ime aplikacije FakeApp. To kaže na dejstvo, da ena predstavitev mogoče ni dovolj, da se učencem vtisne v spomin oz. da si zapomnijo vse pomembne informacije. Vsekakor pa lahko glede na odgovore v zvezi z DeepFake tehnologijo sklepam, da so učenci ozavestili dejstvo, da predstavlja nevarnost in da ne moremo verjeti vsemu, kar vidimo in slišimo v medijih oz. na spletu. Kljub temu, da je število učencev, ki o teh vrstah spletnih prevar niso dovolj dobro poučeni še vedno preveliko, menim, da so učenci veliko bolje poučeni o Deepfake-u, Phishingu in javnih brezplačnih Wi-Fi omrežjih.

6 RAZPRAVA

Ko sem izvedla prvo anketo in pridobila želene podatke, sem preverila resničnost prvih petih hipotez. Zavedam se, da je moj eksperimentalni vzorec veliko premajhen, da bi lahko na podlagi pridobljenih rezultatov podajala pomembne ugotovitve. Prav tako obstaja kar nekaj dejavnikov, ki so lahko vplivali na učence v času izvedbe anketnih vprašalnikov in so rezultati morebiti zaradi tega manj zanesljivi. Takšni dejavniki so zgodnja jutranja ura, ko sem izvajala anketo in predstavitev spletnih prevar. Najstniki so namreč zgodaj zjutraj manj osredotočeni in niso pripravljeni za resno delo. Poleg tega imajo različen odnos do reševanja anket v zvezi z raziskovalnimi nalogami. V času izvedbe anket in predstavitve je bilo tudi veliko manjkajočih učencev zaradi gripe, kar je lahko vplivalo na dejstvo, da v obeh eksperimentalnih vzorcih niso bili isti učenci in da so nekateri pri predstavitvi spletnih prevar manjkali. Že zaradi teh dejstev ne morem natančno sklepati iz rezultatov, ki sem jih pridobila z anketnimi vprašalniki. Ugotovila sem tudi, da vrstnike najbolj zanima Deepfake tehnologija, čemer botruje dejstvo, da najstniki v svojem prostem času ustvarjajo veliko fotografij in video vsebin in se jim zdi ta tehnologija zelo zanimiva. Upam, da s svojo raziskovalno nalogo nisem koga spodbudila k ustvarjanju Deepfake posnetkov z namenom škodovanja komu drugemu, saj so bili zelo zainteresirani za aplikacijo FakeApp. Glede pridobljenih rezultatov v zvezi s šesto hipotezo oz. seznanjanjem vrstnikov z nevarnostmi spleta, nisem bila preveč zadovoljna. Upala sem na boljše rezultate oz. da bodo vrstniki po predstavitvi s spletnimi prevarami bolje seznanjeni. Ob pogovoru o varnih geslih sem ugotovila tudi, da se najstniki ne obremenjujejo preveč z gesli, saj so prepričani, da jim ne bo nihče ukradel gesla in se z njim okoristil. Ker je bila moja primarna želja v raziskovalni nalogi, da vrstnike čim bolje seznanim z nevarnostmi spletnih prevar, sem se odločila, da izdelam plakat, ki sem ga pritrdila na dobro vidno mesto na šolskem hodniku, kjer ga bodo lahko videli vsi učenci in učitelji ter delavci naše šole, kakor tudi starši, ki prihajajo v šolo. To se mi je zdelo zelo pomembno, saj si bodo ljudje verjetno vzeli več časa in si plakat podrobno pogledali. Nanj sem vključila kratek opis nevarnosti, ki jih predstavljata nakup po spletu in lažne nagradne igre. Opisala sem pomembnost močnih gesel in načine, kako si generirati močno geslo. Vključila pa sem tudi nevarnosti Deepfake tehnologije s poudarkom nevarnosti nalaganja osebnih vsebin na splet. To se mi je ob zaključevanju moje raziskovalne naloge zdelo zelo pomembno. Plakat sem pritrdila tudi na nekaterih drugih osnovnih šolah v Mariboru in okolici. Upam, da mi bo uspelo vsaj nekaj vrstnikov ozavestiti o nevarnostih spletnih prevar in doseči, da bodo bolj previdni pri uporabi spleta ter si bodo mogoče kreirali

bolj varna gesla. S tem bodo postali bolj odgovorni uporabniki spleta tudi ko odrastejo. Ugotovila sem tudi, da predstavitev in plakat nista bila dovolj učinkovita pri seznanjanju najstnikov z nevarnostmi na spletu. To tudi ni rešitev, ki bi pomagala večjemu številu najstnikov. Zato sem podala idejo za rešitev raziskovalnega problema v zaključku.

7 DRUŽBENA ODGOVORNOST

Spletne prevare so realnost današnjega časa in se jim v prihodnosti ne bo moč izogniti. Glede na priporočila Ocene ogroženosti zaradi internetnega organiziranega kriminala v EU (IOCTA) za leto 2018 je najučinkovitejša zaščita pred socialnim inženiringom ozaveščanje potencialnih žrtev, med katerimi se ob vsaki uporabi spleta lahko znajdemo tudi sami. Z ozaveščanjem splošne javnosti o tem, kako prepoznati različne načine zavajanja, lahko zaščitimo uporabnike in njihov denar.

Evropski center za boj proti kibernetski kriminaliteti pri Europolu in Združenje evropskih bank ter njuni partnerji iz javnega in zasebnega sektorja so leta 2018 pričeli s kampanjo ozaveščanja o spletnih prevarah z naslovom **Klikni in se poslovi od svojega denarja** – spletne prevare 21. stoletja (#CyberScams). Gonilo tega vseevropskega prizadevanja bo preventivna kampanja, ki bo potekala preko družbenih medijev in s pomočjo organov odkrivanja in pregona, združenj bank in finančnih ustanov.

Preventivnim dejavnostim na tem področju bi morali posvetiti več časa tudi v osnovnih šolah. Kljub temu, da temu na naši šoli posvečamo veliko časa, saj imamo velikokrat delavnice na to temo in sodelujemo s centrom za varnejši internet Safe.si, menim, da se najstniki še zmeraj ne zavedajo vseh nevarnosti, ki prežijo nanje na spletu. Mladostniki so namreč ena izmed najranljivejših družbenih skupin, saj se njihova osebnost še ni izoblikovala in so najbolj dojemljivi za zunanje vplive pri oblikovanju lastnih mnenj in stališč do novosti, s katerimi se srečujejo. Nad novostmi se hitro navdušijo, nimajo pa še dovolj izkušenj, da bi bili dovolj pozorni na morebitne pasti, ki jih te novosti prinašajo.

S svojo raziskovalno nalogo sem ravno iz tega razloga želela opozoriti na nevarnosti, ki jih za družbo predstavlja množična uporaba spleta in z njim povezane spletne prevare. Nekateri ljudje se namreč s pomočjo le-teh okoriščajo in posledično škodujejo drugim. V težavah se znajdejo tisti, ki o pasteh na spletu niso dovolj poučeni. Če bodo mladostniki bolje seznanjeni in poučeni o spletnih prevarah, jih bodo lažje prepoznali in redkeje postali njihove žrtve. Kasneje bodo kot odrasle osebe tudi bolj odgovorni uporabniki spleta in bodo pripravljeni spletne prevare, na katere bodo naleteli, prijaviti pristojnim organom.

Dobro bi bilo, da bi se mladi začeli bolj zavedati, kakšno škodo lahko goljufi s spletnimi prevarami povzročajo drugim ljudem in ozavestili, da takšna dejanja ne sodijo v sodobno

družbo, v kateri želimo sobivati v sožitju. Upam, da bo ta ozaveščenost pripomogla tudi k zmanjševanju števila goljufov in spletnih prevar v prihodnosti.

8 ZAKLJUČEK

Z raziskovalno nalogo sem ugotovila, da se učenci tretje triade osnovne šole zavedajo nevarnosti uporabe spleta in možnih spletnih prevar, vendar niso dovolj seznanjeni s posameznimi vrstami nevarnosti in možnimi posledicami. Prišla sem do zaključka, da kljub temu, da se v šoli veliko pogovarjamo o internetni varnosti, se učenci ne zavedajo dejstva, da so s svojo nepazljivo uporabo vsakodnevno potencialne žrtve spletnih prevar.

Digitalna pismenost je prvi korak, ki ga lahko naredimo pri zaščiti pred spletnimi prevarami in manipulacijo lastnih življenj. To bi moral biti del modernega starševstva in izobraževalnega sistema. Najpomembnejše je, da se naučimo oceniti informacije in ponudbe, ki se pojavljajo na spletu, še posebej z naraščajočim porastom umetne inteligence. Potrebno si je privzgojiti tudi spletno odgovornost in etičnost pri oblikovanju zavajajočih spletnih vsebin in s tem zmanjšati število spletnih goljufov.

Glede na hiter razvoj tehnologije in s tem povezanega hitro spreminjajočega se načina življenja se mi zdi nujno potrebna tudi sprememba v šolskem sistemu, ki ne bi ponujal predmeta računalništvo le kot interesno dejavnost ali izbirni predmet, ampak bi ta postal del rednega šolskega programa. Tako bi lahko otroci in najstniki dobili možnost spoznavanja vsestranske uporabe spleta in ga ne bi uporabljali le za zabavo in preživljanje prostega časa. Na naši šoli imamo že vrsto let predavanja o nevarnostih spleta, a ta niso primerna za najstnike, saj ne pritegnejo dovolj njihove pozornosti. V teh predavanjih tudi opozarjajo samo na določene nevarnosti spleta, o drugih pa sploh ne govorijo. Menim, da bi morali najstnike seznaniti z nevarnostmi spleta na drugačen način in da bi jih morali seznaniti z vsemi nevarnosti, ne samo z nekaterimi. Zato sem razmislila in s pomočjo metod dela (predstavitev, deljenje letakov in druga anketa) dobila idejo, kako bi lahko seznanili najstnike s spletnimi prevarami na bolj zanimiv način. Lahko bi se npr. enkrat letno za zadnjo triado po vseh osnovnih šolah v Sloveniji, organiziral dan dejavnosti na temo *Nevarnosti na spletu*. Vseboval bi krajše predavanje, ki bi nujno moralo vključevati zanimivo Power Point predstavitev z veliko slikovnega materiala, animacijami ter obvezno z video vsebinami. Nato bi se učenci razdelili v nekaj manjših skupin. Bilo bi več delavnic. Na vsaki bi učenci spoznali eno spletno prevaro s pomočjo ugank in videoposnetkov (uganke bi lahko reševali tudi s pomočjo kakšne aplikacije). Ko bi vse skupine obiskale vse delavnice, bi lahko preverili svoje znanje s pomočjo kviza Kahoot ali s kakšnim drugim kvizom ali igro. Če bi potem želeli preveriti ali je tak način seznanjanja za najstnike

primeren, bi lahko njihov napredek znanja preverjali s pomočjo ankete in potem naredili raziskavo med vsemi šolami.

Ob prebiranju literature in podrobnejšem spoznavanju raznih spletnih goljufij in spletnih aplikacij, sem naletela tudi na pojem 'Sadfishing' ali žalostno ribarjenje. V prihodnje bi bilo zanimivo raziskati povezavo med vsebinami, ki jo nalagajo najstniki na splet, razlogi za deljenje osebnih vsebin in njihovo samopodobo, počutjem ter odnosi z vrstniki.

9 VIRI IN LITERATURA

9.1 Pisni in elektronski viri

(1) http://www.poslovodno-racunovodstvo.si/sl/spletne-prevare.php (12.11.2019 20:05)

(2) https://ec.europa.eu/anti-fraud/olaf-and-you/report-fraud_sl (13.11.2019 16:27)

(3) https://en.wikipedia.org/wiki/Internet_fraud (13.11.2019 16:39)

(4) https://mariborinfo.com/novica/kronika/lani-so-zabelezili-rekordno-stevilo-spletnih-goljufij-vec-kot-tisoc/268639 (13.11.2019 17:13)

(5) https://www.varninainternetu.si/po-spletu-krozijo-lazne-nagradne-igre-kako-ravnati/ (14.11.2019 16:46)

(6) https://www.varninainternetu.si/poskus-loterijske-prevare-preko-sms-sporocil/(14.11.2019 17:57)

(7) https://www.varninainternetu.si/article/lazne-spletne-trgovine/ (23.11.2019 15:03)

(8) https://www.varninainternetu.si/prevare-ko-prodajate-prek-malih-oglasov/ (24.11.2019 19:11)

(9) https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/95864-sedem-vrst-spletnih-financnih-prevar-ki-jim-uporabniki-najpogosteje-nasedejo (12.11.2019 18:26)

(10) https://www.varninainternetu.si/article/kraja-identitete-2/ (12.11.2019 20:27)

(11) Nov roparski val: Kraja identitete. V Glamur št. 62 (2002). Stran 48 (13.1.2020 17:10)

(12) https://www.kajkupiti.si/uporabni-nasveti/kako-izbrati-mocno-in-varno-geslo.html (28.11.2019 15:12)

(13) https://www.varninainternetu.si/mocno-geslo/ (28.11.2019 15:56)

(14) https://www.kajkupiti.si/uporabni-nasveti/kako-izbrati-mocno-in-varno-geslo.html (28.11.2019 16:31)

(15) https://www.varninainternetu.si/top-6-spletne-nevarnosti-za-dopustnike/ (6.12.2019 16:41)

(16) https://www.mcafee.com/blogs/consumer/family-safety/sadfishing-deepfakes-tiktok-headlines-you-may-have-missed/ (6.12.2019 17:05)

(17) https://radioprvi.rtvslo.si/2019/10/najvecja-zloraba-umetne-inteligence-je-deepfake-tehnologija/ (6.12.2019 19:05)

(18) https://www.dnevnik.si/1042819488/magazin/znanost-in-tehnologija/manipulacija-videoposnetkov-deepfake-posnetki-kot-znanilci-nove-dobe-laznih-novic (6.12.2019 18:13)

(19) https://www.dnevnik.si/1042838574/magazin/znanost-in-tehnologija/3d-replike-obrazov-vzbujajo-strah-pred-razmahom-laznih-novic- (6.12.2019 18:32)

(20) https://www.digitaladventures.com/news/2019/8/18/deepfakes-are-here-a-parent-s-guide-to-understanding-the-risks-for-their-kids (6.12.2019 18:48)

(21) https://www.digitaladventures.com/news/2019/8/18/deepfakes-are-here-a-parent-s-guide-to-understanding-the-risks-for-their-kids (6.12.2019 18:59)

(22) https://www.digitaladventures.com/news/2019/8/18/deepfakes-are-here-a-parent-s-guide-to-understanding-the-risks-for-their-kids (6.12.2019 19:43)

(23) https://www.varninainternetu.si/kraja-podatkov-phishing-na-avto-net/_1(12.11.2019 20:46)

(24) Darinka Meško. Spletne goljufije. V Poslovno računovodstvo(2015). Stran 85-99 (9.12.2019 19:22)

(25) https://www.varninainternetu.si/kraja-podatkov-phishing-na-avto-net/ (12.1.2020 12:53)

(26) file:///C:/Users/Anita/Downloads/Phising%20-%20Kako%20se%20izogniti%20prevari%20(1).pdf (12.1.2020 13:09)

10 PRILOGE

10.1 Priloga 1: Prvi anketni vprašalnik za učence o spletnih prevarah

Pozdravljen/a!
Sem učenka 8. razreda in pripravljam raziskovalno nalogo o spletnih prevarah. Prosim te za sodelovanje v anketi, ki ti bo vzela nekaj minut časa, tvoji odgovori pa mi bodo v veliko pomoč pri izdelavi naloge. Anketa je anonimna.

Q1 - Spol:

◯ moški
◯ ženski

Q2 - Razred:

◯ 7. razred
◯ 8. razred
◯ 9. razred

Q3 - Si že kdaj dobil/a sporočilo v katerem je pisalo, da si zmagal/a v nagradni igri ali zadel/a na loteriji?

◯ da
◯ ne

Q4 - Kako si odreagiral/a, ko si prejel/a takšno sporočilo?

◯ sporočilo sem ignoriral/a
◯ poslal/a sem podatke, ki so jih zahtevali in bil/a prevaran/a
◯ podatke sem najprej mislil/a poslati, potem pa sem ugotovil/a, da gre za prevaro

Q5 - Si že kdaj, ko si nakupoval/a v spletni trgovini pomislil/a, da gre morda za prevaro?

◯ da
◯ ne

Q6 - Kaj si storil/a v tem primeru?

◯ kljub temu sem se odločil/a, da bom nakupoval/a v tej spletni trgovini
◯ preveril/a sem spletno trgovino
◯ nisem nakupoval/a v tej spletni trgovini

Q7 - Si bil/a kdaj prevaran/a pri prodajanju preko malih oglasov (npr. bolha)?

◯ da
◯ ne

Q8 - Meniš, da so tvoja gesla varna?

◯ da
◯ ne

Q9 - Ali tvoja gesla vsebujejo velike in male črke, številke in znake ter niso preveč očitna (ne vsebujejo tvojega imena, priimka ipd.)?

◯ da
◯ ne
◯ vsebujejo nekaj od tega ampak ne vsega

Q10 - Ali so ti že kdaj ukradli geslo (npr. vdrli v tvoj profil na družabnem omrežju)?

◯ da
◯ ne

Q11 - Ali kdaj uporabljaš javne računalnike (v kavarnah, knjižnicah ipd.)?

◯ da
◯ ne

Q12 - Za kaj si uporabljal/a takšen računalnik?

◯ uporabljal/a sem družabna omrežja ipd. (vpisal/a sem geslo), ki mi je bilo potem ukradeno
◯ uporabljal/a sem družabna omrežja ipd. (vpisal/a sem geslo) in se ni nič zgodilo
◯ računalnik sem uporabljal/a za stvari, za katere nisem potreboval/a gesla, ker se zavedam nevarnosti vpisovanja gesel v javni računalnik

Q13 - Se zavedaš, da je lahko uporaba brezplačnih Wi-Fi omrežij nevarna?

◯ da in jih zato ne uporabljam
◯ da, ampak jih vseeno uporabljam
◯ ne, na to nikoli nisem pomislil/a

Q14 - Ali veš kaj je deepfake?

◯ da
◯ ne
◯ sem že slišal/a za to, ampak ne vem veliko o tem

Q15 - Ali si kdaj ob ogledu določenega posnetka na družabnem omrežju ali internetu dvomil/a o njegovi resničnosti?

◯ ne, ker se je oseba premikala in govorila, sem posnetku brez razmišljanja verjel/a
◯ da, vendar sem vseeno nasedel/la, ker je bil posnetek videti realen
◯ da, ker se zavedam nevarnosti deepfake tehnologije

Q16 - Ali veš kaj je phishing?

◯ da
◯ ne
◯ sem že slišal/a za to, ampak ne vem veliko o tem

Q17 - Ali si kdaj prejel/a elektronsko sporočilo, ki bi naj bilo poslano od ponudnika spletne storitve, v katerem te ta prosi za ponovni vpis gesla in osebnih podatkov na določeni spletni strani?

◯ da
◯ ne

Q18 - Kaj si storil/a v tem primeru?

◯ na spletni strani sem vpisal/a svoje osebne podatke in geslo
◯ sporočilo sem ignoriral/a

10.2 Priloga 2: Drugi anketni vprašalnik za učence o spletnih prevarah

Pozdravljen/a!
Sem učenka 8. razreda in pripravljam raziskovalno nalogo o spletnih prevarah. To je moja druga anketa, s katero bi rada preverila, ali ste učenci bolj poučeni o nekaterih vrstah spletnih prevar, po predstavitvi, ki sem jo izvedla. Zato vas prosim za sodelovanje v anketi, ki mi bo zelo pomagala pri izdelavi naloge. Anketa je anonimna.

Q1 - Spol:

◯ moški
◯ ženski

Q2 - Razred:

◯ 7. razred
◯ 8. razred
◯ 9. razred

Q3 - Zakaj je uporaba javnih brezplačnih brezžičnih Wi-Fi omrežja lahko nevarna?

◯ ker se lahko naš telefon v primeru uporabe takšnega omrežja okuži z virusom, ki mu zablokira telefon
◯ ker lahko, če brezžična dostopna točka ni dovolj zavarovana, pride do prestrezanja omrežnega prometa
◯ ker lahko, če brezžična dostopna točka ni dovolj zavarovana pride do izbrisa vseh podatkov na našem telefonu
◯ ne vem

Q4 - Kakšna brezžična omrežja zahtevajo posebno previdnost?

◯ takšna, ki jih neznanec ustvari kar na svojem računalniku
◯ takšna, ki so dostopna v hotelih ali v kavarnah
◯ ne vem

Q5 - Katero brezžično omrežje moramo izbrati, če lahko izbiramo med šifriranim in nešifriranim?

◯ šifrirano
◯ nešifrirano
◯ ne vem

Q6 - Kaj je phishing?

◯ je kraja podatkov, ki storilcu omogoči dostop do naših sporočil, ki jih potem objavi na družabnih omrežjih
◯ je kraja podatkov, ki storilcu omogoči dostop do spletnih storitev v našem imenu
◯ je grožnja, ki storilcu omogoči krajo našega denarja
◯ ne vem

Q7 - Kako se začne tipična phishing prevara?

◯ z elektronskim sporočilom, v katerem nam neznanec grozi, da nam bo ukradel denar
◯ z elektronskim sporočilom, ki bi naj bilo poslano od prijatelja na Facebooku, v katerem nas ta prosi za denar
◯ z elektronskim sporočilom, ki naj bi bilo od ponudnika spletne storitve, v katerem nas ta prosi za ponovni vpis gesla in osebnih podatkov na določeni spletni strani zaradi preverjanja podatkov ali dodatnih ugodnosti
◯ ne vem

Q8 - Kaj je cilj storilca phishing prevare?

◯ dobiti naše geslo in uporabniško ime za spletno storitev, da potem geslo zamenja in nam prepreči dostop do računa, sam naš račun potem uporabi za objavljanje lažnih oglasov in goljufanje kupcev
◯ odkriti vsa naša zasebna sporočila, da jih potem lahko objavi na internetu in okrni naš ugled
◯ dobiti naš denar z grožnjami o objavljanju naših osebnih podatkov
◯ ne vem

Q9 - Kaj mora oseba v storiti v primeru, da je vpisala geslo in osebne podatke na phishing strani?

◯ ne sme ničesar storiti, saj lahko situacijo samo še poslabša
◯ prijaviti mora grožnjo
◯ nujno mora spremeniti geslo in v primeru kraje podatkov to prijaviti
◯ ne vem

Q10 - Kaj je deepfake?

◯ je manipulacija zvočnih posnetkov, ki jih storilec ustvari z glasom določene osebe in posnetek objavi, da bi vsi mislili, da je tista oseba res tisto rekla, čeprav tega v resnici ni storila
◯ je manipulacija videoposnetkov pri kateri lahko oseba obraz posameznika prestavi na drugega človeka in nato videoposnetek zmontira tako, da se ta oseba premika in govori tako kot on/ona hoče
◯ so fotografije urejene tako, da prikazujejo nekaj kar se v resnici ni zgodilo

◯ ne vem

Q11 - Kako se imenuje najbolj znana aplikacija za ustvarjanje deepfake posnetkov?

◯ FaceApp
◯ Carica
◯ DeepFake Tutorial
◯ FakeApp
◯ ne vem

Q12 - Kaj je najbolj zaskrbljujoče glede deepfake tehnologije?

◯ da jo lahko zdaj uporabljajo že navadni uporabniki s svojim pametnim telefonom in se bodo zato kmalu začele širiti lažne novice
◯ da bo to postal poklic, ki ga bo želela upravljati večina ljudi
◯ da se širi vedno več lažnih oz. photoshopiranih slik
◯ ne vem

Q13 - Kakšne bodo predvidevane posledice deepfaka?

◯ spremenil bo naš pogled na svet tako, da bomo začeli verjeti, da je deepfake dober za družbo
◯ spremenil bo naš pogled na svet in je tudi mogoče, da ljudje ne bomo verjeli in zaupali nobenemu drugemu, ampak le še sebi
◯ spremenil bo družbo tako, da si nihče več ne bo upal uporabljati tehnologije zaradi številnih groženj
◯ ne vem

10.3 Priloga 3: Letak za učence o spletnih prevarah

JAVNA BREZPLAČNA BREZŽIČNA OMREŽJA (WI-FI)

Na letališčih, v kavarnah in hotelih so pogosto na voljo **javna brezžična omrežja (Wi-Fi)**, ki so **brezplačna** ali pa so dostopna po zmerni ceni. Večina ljudi uporablja takšna omrežja **brez,** da bi se zavedali njihovih nevarnosti. Kljub temu, da je njihova uporaba veliko bolj varna od uporabe javnih računalnikov, lahko predstavljajo **veliko nevarnost**. Če brezžična dostopna točka **ni dovolj zavarovana**, lahko pride do **prestrezanja omrežnega prometa**. To pomeni, da lahko neznanec spremlja ves naš omrežni promet. Prav posebno previdnost pa zahteva brezžično omrežje, ki ga ustvari nekdo kar na svojem računalniku. V tem primeru se **povežemo neposredno na prenosnik neznanca**. Zato se je treba **vedno** pozanimati, katero je pravo omrežje hotela ali cybercafeja. Če lahko izbiramo med nešifriranim in šifriranim omrežjem, moramo izbrati **šifriranega.** Priporočljivo pa je, da se uporabe javnih brezplačnih omrežij Wi-Fi **izogibamo**.

PHISHING ALI RIBARJENJE

S tem imenom poimenujemo **krajo podatkov**, ki storilcu omogoči dostop do spletnih storitev v našem imenu in v skrajnem primeru tudi krajo našega denarja. S phishing prevaro spletni goljuf pridobi **osebna uporabniška imena in gesla** za dostop do storitev, kot so elektronska pošta, Facebook ali PayPal. Tipična phishing prevara se prične z **elektronskim sporočilom**, ki naj bi bilo od ponudnika spletne storitve. Obvestijo nas, da se moramo zaradi preverjanja podatkov ali dodatnih ugodnosti **prijaviti in ponovno vnesti svoje podatke**. V sporočilu se nahaja tudi povezava na katero naj bi kliknili, vendar nas vodi na **lažno spletno stran**, ki je **zelo podobna**, morda skoraj identična strani legitimnega ponudnika. Cilj napadalcev je prevzem nadzora nad uporabniškimi računi. Ko pridobijo podatke, lahko **zamenjajo geslo** in s tem lastniku računa **preprečijo dostop**. Potem njegov račun uporabljajo za objavljanje lažnih oglasov in goljufanje kupcev. V primeru, da smo osebne podatke in geslo na phishing strani vpisali, moramo nujno **spremeniti geslo** in v primeru kraje podatkov to **prijaviti.**

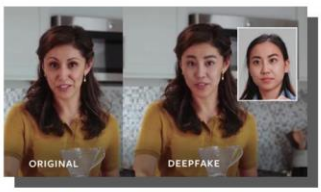
DEEPFAKE

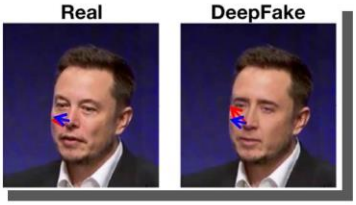
V zadnjih dveh letih so se na spletu pojavili videoposnetki, imenovani **deepfake**. Gre za **nameščanje obrazov** zvezdnikov na tuja telesa. Ker je tehnologija že zelo razvita in učinkovita, se vse pogosteje pojavljajo tudi skrbi pred povsem novo ravnjo **lažnih novic**.

V začetku leta 2018 se je pojavila računalniška aplikacija **FakeApp**. Z njo lahko uporabniki obraz posameznika prestavijo na telo drugega človeka. Nato se ta oseba **premika in govori,** tako kot oni hočejo. V program je treba vnesti le glavni video, ga povezati s spletno zbirko fotografij posameznika in po nekaj urah obdelave podatkov dobimo želeni potvorjeni video, ki je pripravljen na deljenje. Nedavno tega so filmski studii morali za tovrstne vizualne učinke plačevati milijone in najemati izvrstne montažerje. Danes pa lahko to tehnologijo uporabljajo **navadni uporabniki** s svojim pametnim telefonom. Za zdaj se deepfake posnetki pojavljajo predvsem kot sredstvo zabave. Glede na dostopnost podatkov lahko program uporabi prav vsakdo. Tu pa se začenja tudi ena večjih skrbi. Tehnologija hitro napreduje in ni malo verjetno, da se bo kmalu pričela izrabljati tudi za potegavščine, ki imajo lahko **resne posledice** za družbo.

Strokovnjake zelo skrbi, kako obvladati to situacijo. Težave imajo namreč že s pisano besedo, zato ne vedo, kako naj se lotijo lažnih videoposnetkov.

Prepoznavanje deepfake tehnologije je zelo **velik izziv,** zato obstaja možnost, da bodo ljudje zaradi takšnih posnetkov izgubili zaupanje v medije in ne bodo **zaupali nobenemu** drugemu, ampak le še **sebi**. Deepfake bo **spremenil** pa bo tudi naš **pogled nas svet.**





10.4 Priloga 4: Plakata o spletnih prevarah