UNIVERZA V LJUBLJANI

FAKULTETA ZA UPRAVO

Diplomsko delo

ZAVEDANJE UPORABNIKOV O VARNOSTI OSEBNIH PODATKOV PRI UPORABI INTERNETA

Miranda Ćehić

Ljubljana, avgust 2018

UNIVERZA V LJUBLJANI

FAKULTETA ZA UPRAVO

Diplomsko delo

ZAVEDANJE UPORABNIKOV O VARNOSTI OSEBNIH PODATKOV PRI UPORABI INTERNETA

Kandidatka: Miranda Ćehić
Vpisna številka: 04042659
Študijski program: univerzitetni študijski program Upravljanje javnega sektorja 1. stopnja

Mentor: red. prof. dr. Ljupčo Todorovski

Ljubljana, avgust 2018

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana, Miranda Ćehić, študentka univerzitetnega študijskega programa Upravljanje javnega sektorja 1. stopnja, z vpisno številko 04042659, sem avtorica diplomskega dela z naslovom »Zavedanje uporabnikov o varnosti osebnih podatkov pri uporabi interneta«.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu literature in virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili,
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo, in sem to tudi jasno zapisala v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah, Uradni list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo,
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala Nastja Bojić, dipl. fil. (UN) in dipl. slov. (UN).

Ljubljana, 20. 8. 2018 Miranda Ćehić

POVZETEK

Diplomsko delo obravnava problematiko zavedanja uporabnikov o varnosti osebnih podatkov pri uporabi interneta. Težave se pojavijo pri njihovem deljenju na internetu, ki je nepogrešljivo orodje za pridobivanje in uporabo ogromne količine podatkov, ki so nam na voljo, hkrati pa deljenje le-teh na spletu predstavlja veliko tveganje, saj so večkrat ukradeni in uporabljeni proti volji uporabnika, česar se slednji niti ne zaveda. Najbolj izpostavljena ter ranljiva skupina so otroci, ki se prvič ter posledično brez izkušenj znajdejo na internetu. Pogostost kraje in nezakonite uporabe osebnih podatkov posameznika se sicer zmanjšuje, še vedno pa predstavlja velik svetovni problem pri uporabi interneta. Zakonodaja to področje ureja ter opredeljuje, kaj predstavlja legitimno zahtevo po podatkih in kaj nezakonito poseganje v posameznikovo zasebnost.

Namen diplomskega dela je predstaviti področje varstva podatkov in možne kršitve oziroma zlorabe varnosti na internetu ter podrobneje opredeliti najpogostejše nevarnosti, na katere lahko naleti posameznik, in možne vrste zaščite ter načine varovanja osebnih podatkov. Poleg tega želimo ugotoviti, v kolikšni meri se uporabniki interneta zavedajo nevarnosti zlorab osebnih podatkov.

Med pisanjem diplomskega dela, anketiranjem in pridobivanjem podatkov smo ugotovili, da je delež uporabnikov, ki se niti malo ne zavedajo nevarnosti na internetu, relativno majhen in da so uporabniki pri posredovanju svojih najbolj osebnih podatkov, kot so gesla in podatki o bančnih računih, izjemno previdni in nezaupljivi. To lahko pripišemo temu, da se Slovenija ter EU zavzemata za izobraževanje in splošno ozaveščanje uporabnikov interneta o tovrstnih tveganjih.

Ključne besede: internet, varnost na internetu, uporabnik, zasebnost, osebni podatki.

SUMMARY

USERS' AWARENESS OF THE SECURITY OF PERSONAL DATA WHEN USING THE INTERNET

Diploma thesis addresses the issue of users' awareness of the security of personal data when using the Internet. The problems arise when somebody shares these data on the Internet which is namely an indispensable tool for acquiring and using an enormous amount of data available to us and at the same time the input of personal data and their sharing on the Internet poses a high risk. Data are often stolen and used against the user's will and the user is often not even aware of that. The most exposed and vulnerable group are children who find themselves on the Internet for the first time and consequently without any experience. The frequency of theft and illegal use of personal data is decreasing, but it still represents a major global problem in the use of the Internet. Legislation regulates this area and defines what constitutes a legitimate request for information and what is illegal interference with the privacy of an individual.

The purpose of the diploma thesis is to present the field of data protection and possible violation or abuse of the Internet security, as well as to present in more detail the most common threats that an individual may encounter and possible protection and ways of protecting personal data. With this thesis we want to determine the extend to which the Internet users are aware of the danger of misuse of personal data that remain on the Internet while searching for information and providing services.

While writing the diploma thesis, surveying and retrieving data, we found that the proportion of users who are completely unware of the dangers on the Internet is relatively small and that the users are extremely cautious and mistrustful when providing their most personal information, such as passwords and bank account information. This can be attributed to the fact that Slovenia and the EU are committed to the education and general awareness of Internet users about such risks.

Keywords: Internet, Internet security, user, privacy, personal data.

KAZALO

KAZALO PONAZORITEV

KAZALO GRAFIKONOV

KAZALO TABEL

1 UVOD

Živimo v družbi, v kateri opažamo čedalje večje poudarjanje posameznikove zasebnosti in individualnosti. Zasebnost obravnavamo kot stanje, v katerem je posameznik sam in ga drugi ne motijo. Eden od vidikov zagotavljanja zasebnosti je tudi nadzor nad uporabo lastnih osebnih podatkov. Tako naj bi bil posamezniku zagotovljen nadzor nad lastnimi podatki na način, ki bi omogočal sprejemanje odločitev o njihovem zbiranju ter širjenju, po drugi strani pa smo priča čedalje višji stopnji nadzorovanja. Internet je v novodobni družbi prostor, v katerem se pojavlja vedno več osebnih podatkov, ki jih dostikrat objavi posameznik sam, velikokrat pa se to dogaja brez njegove vednosti in celo v nasprotju z njegovo voljo. S širitvijo uporabe interneta, ki omogoča vedno boljše povezave in storitve, se povečuje tudi nevarnost vdora v zasebnost, posledično pa kraje podatkov. Tako večkrat pride do zlorab osebnih podatkov, kot sta kraja identitete in uporaba tujih podatkov za lastno korist. Najpogostejši primeri so kraje uporabniških imen in gesel, pri katerih največje tveganje predstavljajo podatki o spletnem bančništvu.

Uporabniki internetnih storitev so dostikrat neosveščeni ali pa podcenjujejo tveganje, ki ga prinaša uporaba interneta, saj veliko uporabnikov zavedno širi svoje osebne podatke. Pogosti primeri širjenja se pojavljajo na socialnih omrežjih in v spletnih klepetalnicah, težave pri osveščanju pa v vseh starostnih skupinah. Nezavedanje o nevarnostih na internetu je starostno enakomerno porazdeljeno med otroke in odrasle, med mlajše in starejše uporabnike. Z uvajanjem zavedanja o nevarnostih na internetu v šolski sistem se je stanje pri mlajših generacijah pričelo izboljševati. Splošno tveganje za nevarnosti še vedno ostaja zelo veliko, posledično pa ostaja visok tudi odstotek spletnih zlorab osebnih podatkov, zato je potrebno uporabnike obveščati o teh nevarnostih in jim zagotoviti največjo možno pravno varnost pri uporabi tovrstnih storitev.

Namen diplomskega dela je predstaviti področje varstva osebnih podatkov ter možne kršitve oziroma zlorabe varnosti na internetu. Zanima nas, v kolikšni meri se uporabniki interneta zavedajo možnosti zlorab osebnih podatkov, ki jih puščajo na internetu.

Cilj diplomskega dela je ugotoviti, kako dobro uporabniki poznajo možnosti posega v lastno zasebnost, ko uporabljajo internet, kako dobro poznajo načine preprečitve kraje podatkov ter ali se zavedajo posledic, ki nastanejo zaradi nevednosti ali neustrezne zaščite. Napisano delo je sestavljeno tako, da so najprej predstavljeni osnovni pojmi, ki so pomembni za razumevanje problematike teme, ki jo podajamo, nato pa sledi predstavitev najpogostejših nevarnosti za zaščito podatkov na internetu ter načinov oziroma tehnologij za varovanje in zaščito podatkov.

Osnovna teza dela je trditev, da se posamezniki oziroma uporabniki ne zavedajo nevarnosti, ki jih prinaša uporaba interneta, in s svojimi osebnimi podatki niso previdni.

Na podlagi osnovne teze smo postavili tudi naslednje hipoteze, ki smo jih na koncu potrdili oziroma ovrgli:

H1: Uporabniki interneta se ne zavedajo nevarnosti za zlorabo osebnih podatkov, zato delijo svoje osebne podatke.

H2: Uporabniki, ki se zavedajo nekaterih nevarnosti, svoje osebne podatke vseeno delijo, saj še niso imeli osebne izkušnje z zlorabo osebnih podatkov.

H3: Uporabniki interneta, ki še niso bili v položaju, da bi bili njihovi osebni podatki zlorabljeni, slabše poznajo nasvete za varno uporabo internetnih storitev od tistih, katerih osebni podatki so že bili zlorabljeni.

H4: Uporabniki interneta ne vedo, kam oziroma na koga se obrniti, če bi bili njihovi osebni podatki zlorabljeni.

V diplomskem delu smo z deskriptivno metodo opisali dejstva in odnose področja, ki ga preučujemo. S statistično metodo smo ugotavljali odvisnost posameznih pojavov v določenih trenutkih, jih zbirali ter obdelali. S pomočjo metode klasifikacije smo definirali nekatere pojme, metodo kompilacije smo uporabili pri navedbah in citatih drugih avtorjev, komparativna metoda pa je bila uporabljena za primerjanje naših ugotovitev in rezultatov.

V diplomskem delu smo najprej opredelili osnovne pojme. Predstavili smo napreden razvoj internetnih tehnologij in pojasnili, kaj na internetu predstavljajo osebni podatki, kaj pomeni zasebnost na internetu ter katere so naše pravice do zasebnosti v spletnem svetu.

Nadalje smo predstavili, katere nevarnosti se pojavljajo pri vsakodnevni rabi interneta. V tem poglavju smo še posebej izpostavili piškotke, ribarjenje, farming, viruse in črve, problematiko klepetalnic ter socialnih in brezžičnih omrežij.

V četrtem poglavju smo predstavili načine zaščite oziroma varstva podatkov pred zgoraj naštetimi vsakodnevnimi nevarnostmi uporabe interneta, pri čemer lahko za zaščito največ naredimo ravno uporabniki sami. Izpostavili smo fizično zaščito, možnosti požarnega zidu in uporabo protivirusnih programov, brez katerih si v današnjem času uporabo računalnika težko predstavljamo. Osredotočili smo se tudi na pregledovanje in odstranjevanje piškotkov, kakovostna gesla ter kritičnost pri posredovanju svojih osebnih informacij.

V empiričnem delu smo raziskovali vedenje posameznikov – kako dobro poznajo možnosti kraje ali zlorabe podatkov in če kljub temu občutljive osebne podatke posredujejo ponudnikom internetnih storitev. Ugotavljali smo tudi, kako dobro poznajo tehnologije za

varnost podatkov ter kako pogosto se jih pri uporabi interneta poslužujejo. S pomočjo teh podatkov, ki smo jih pridobili na podlagi anketnega vprašalnika, smo lahko potrdili ali ovrgli zastavljene hipoteze.

2 OPREDELITEV OSNOVNIH POJMOV

2.1 RAZVOJ INFORMACIJSKIH TEHNOLOGIJ

Industrijskima revolucijama iz 18. in 19. stoletja, ki sta rešili agrarno krizo in v svet prinesli tehnološke procese, je v 20. stoletju sledila tretja, informacijska revolucija. Glavna razlika v primerjavi s prvima dvema revolucijama je v tem, da so se informacijske tehnologije (IT) razširile veliko hitreje ter po vsem svetu. Če so imele tehnološke revolucije v preteklosti geografsko omejen razvoj in so se odvijale v počasnem tempu, se je nova revolucija na področju IT razširila po svetu v manj kot dvajsetih letih. Povratna zanka je tako bistveno hitrejša, kot je bila pri predhodnih tehnologijah, saj sta uporabnik in razvijalec tehnologije tu postala eno. Uporabnik je prevzel nadzor nad tehnologijo, in to se lepo odraža pri internetu (Pivec, 2004, str. 26–27).

Internet je pravzaprav le omrežni protokol, ki deluje po načelu *store and forward*, kar pomeni, da podatke shrani in jih uporabniku posreduje po najhitrejši poti. Dostop do interneta je postal pomemben kazalec razvojnih možnosti posameznih držav oziroma socialnega sloja v družbi, ki pa je v samem začetku svojega razvoja zaradi velikih vložkov v postavitev telekomunikacijske infrastrukture zaobšel revnejše četrti in predmestja. Tako v preteklosti nakup računalnika še ni pomenil možnosti dostopa do interneta. V današnjem času se to seveda drastično spreminja, a ima prekarni razred po večini še vedno dostop do računalnika, medtem ko je dostop do interneta lahko zelo omejen le na javne prostore, v katerih je le-ta na voljo (Pivec, 2004, str. 38).

Internetne tehnologije so tudi v zadnjih dvajsetih letih v vseh gospodarskih panogah povsem spremenile razvoj in delovanje. Brez njih ne moremo, njihova uporaba pa se prične že v osnovnih šolah, saj se otroci informacijske pismenosti učijo praktično hkrati s splošnim znanjem branja in pisanja, kar je z razvojem pametnih telefonov postalo le še izraziteje.

Prva spletna stran v takšni obliki, kot jo poznamo danes, se je na svetovnem spletu pojavila leta 1991. Imenovala se je *World Wide Web Project*, njen namen pa je bil ustvariti neko osnovno stran povezav spletnih informacij. Danes obstaja že več kot milijarda spletnih strani, številka pa z vsakim dnem strmo narašča (Cern, 2017).

2.2 OSEBNI PODATKI

Med obiskovanjem spletnih strani uporabnik na internetnem omrežju pušča sledi osebnih podatkov. Z razvojem IT se je število podatkov, ki jih lahko posredujemo v spletna mesta, drastično povečalo, s tem pa se je povečalo tudi število osebnih podatkov.

Informacijski pooblaščenec Republike Slovenije (IP-RS) osebni podatek definira kot »katerikoli podatek, ki se nanaša na določeno ali določljivo fizično osebo, torej posameznika, ne glede na obliko, v kateri je izražen« (IP-RS, 2017a). Osebni podatki tako predstavljajo širok nabor podatkov, vse od našega imena in priimka do številke transakcijskega računa in številke bančne kartice.

V sodobni družbi smo ob široki uporabi socialnih ter drugih omrežij skoraj vsi aktivni uporabniki interneta, zato je na spletu mogoče najti sledove osnovnih osebnih podatkov skoraj kogarkoli. Pri tem obstaja največ nevarnosti za zlorabo teh podatkov, ki se zbirajo v več gigabajtov velikih datotečnih bazah. Potrebno se je zavedati, da uporabniki interneta te podatke po večini sami vnašamo v baze, včasih tudi z zavedanjem, da se bodo ti podatki nekam shranili in da bodo ostali na internetu. Ko so podatki vneseni, jih praktično ni več mogoče odstraniti oziroma izbrisati iz podatkovne baze, v katero smo jih vnesli.

2.3 ZASEBNOST IN PRAVICA DO ZASEBNOSTI

Zasebnost na spletu se odraža podobno kot zasebnost v vsakdanjem življenju. Je pravica vsakega posameznika in odraža stanje, v katerem je posameznik sam in nanj ne vplivajo zunanji dejavniki, torej ima nadzor nad zbiranjem, uporabo in razširjanjem osebnih podatkov ter informacij.

V današnji družbi smo priča dvema nasprotnima si poloma. Na eni strani vedno bolj poudarjamo posameznikovo individualnost in zasebnost, po drugi strani pa nastaja vedno večja potreba po višji stopnji nadzorovanja. Nadzor in zasebnost sta tesno povezana, a hkrati je nadzor ravno toliko dober, kot je tudi slab. Vpogled v posameznikovo zasebnost se uporablja kot sredstvo za izvajanje družbenega nadzora, zaradi česar ima zasebnost velik pomen pri varnosti držav in njihovih državljanov. Vpogled v zasebnost ne predstavlja problema, dokler ni zlorabljen. To na internetu posamezniku povzroča največjo skrb in posledično rahlo nezaupanje do podajanja vpogleda v svojo zasebnost. A kljub temu posameznik v večini primerov nima izbire, saj če želi uporabiti neko spletno storitev, mora skoraj vedno podati nekaj svojih zasebnih podatkov oziroma na spletu pusti neko sled (Kovačič, 2003, str. 11).

Veliko ljudi ni seznanjenih s tem, katere pravice do svoje zasebnosti imajo ter kateri osebni podatki se lahko oziroma se uporabljajo in na kakšen način. Sorazmerno z naraščanjem IT pravica do zasebnosti predstavlja vse pomembnejšo dobrino, ki jo je potrebno zaščititi.

Pravico do zasebnosti v Sloveniji ureja Zakon o varstvu osebnih podatkov (ZVOP-1) (Uradni list RS, št. 94/07), ki določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečuje neustavne, nezakonite in neupravičene posege v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Temeljni razlog za sprejem tega zakona je bila vsebina

določb Evropske direktive 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Pirc Musar, Prelesnik & Bien Karlovšek, 2006, str. 31).

Zakon postavlja dve načeli: načelo zakonitosti in poštenosti, ki navaja, da se osebni podatki obdelujejo zakonito in pošteno (ZVOP-1, 2. člen), ter načelo sorazmernosti, ki pojasnjuje, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo (ZVOP-1, 3. člen).

Kljub vsej podani zakonodaji in izvajanju nadzora ter kaznovanju kršiteljev še vedno prihaja do kršitev.

3 NEVARNOSTI ZA OSEBNE PODATKE PRI UPORABI INTERNETA

Življenja brez interneta si ljudje v tehnološko razvitih delih sveta praktično ne moremo več predstavljati. Še posebej med mladimi internet postane trend že v osnovni šoli. Tako kot v vsakdanjem življenju nevarnost kraje in zlorabe osebnih podatkov tudi na internetu preži ves čas, ključna razlika pa je, da se nevarnosti na internetu ne zavedamo dovolj dobro oziroma je njihovo poznavanje minimalno. Problematika se še posebej odraža pri osebnih podatkih, ki so glavna tarča hekerjev, zlonamernih programov in virusov, ki jih ustvarijo. Nevarnosti pri vsakodnevni uporabi interneta je tako več, izpostavili pa bomo najpogostejše, ki so hkrati sposobne pridobiti tudi največ osebnih podatkov.

Nevarnosti, ki se pojavljajo pri vsakodnevni rabi interneta, obravnava kibernetska kriminaliteta, ki zajema kriminal, povezan z računalniki in IT. Najpogostejša zločina na področju kibernetske kriminalitete sta ravno vdor in kraja osebnih podatkov (Završnik, 2015, str. 24).

3.1 PIŠKOTKI

Piškotek (ang. *cookie*) je majhna datoteka, ki se shrani na računalniku, ko obiščemo spletno stran. Piškotki vsebujejo različne informacije, ki jih ista spletna stran prebere, ko jo ponovno obiščemo. Piškotki sami po sebi niso škodljivi, saj ne vsebujejo virusov in se uporabljajo za različne namene, kot so košarice v spletnih trgovinah. Na ta način podatki v košarici ostanejo tudi, ko strani s seznamom tega, kar smo že kupili, nimamo odprte. Poleg tega se uporabljajo še za prikaz videov in zemljevidov, z njimi lahko vodimo statistiko obiska strani ter jih uporabimo tudi za prikazovanje oglasov po meri uporabnika spleta. Na vseh modernih spletnih straneh, ki uporabljajo piškotke, se je s 15. 6. 2013 začelo prikazovati pojavno okno, ki pojasni, da spletna stran uporablja piškotke. To zakonodajo, ki regulira uporabo piškotkov, so uvedli kot posledico zlorabe piškotkov, saj so jih nekateri uporabljali za sledenje uporabnikom, s čimer so posegali v zasebnost na spletu (Arh, 2017).

Urad informacijskega pooblaščenca piškotke deli na dobre in slabe, klasificira pa jih po invazivnosti v posameznikovo zasebnost. Deli jih na začasne ali sejne piškotke, trajne ali shranjene piškotke ter lastne in druge piškotke. Zakonodaja vsako vrsto obravnava drugače, kar nekaterim razvijalcem spletnih strani, ki uporabljajo različne vrste piškotkov, povzroča težave pri implementiranju te zakonodaje. Tako morajo po Zakonu o elektronskih komunikacijah (ZEKom-1) in ZVOP-1 obiskovalce spletne strani obvestiti o uporabi piškotkov. V primeru, da so piškotki v posameznikovo zasebnost invazivnejši, pa morajo od obiskovalca spletne strani pridobiti soglasje za njihovo uporabo (IP-RS, 2017c).

3.2 RIBARJENJE

Ribarjenje (ang. *phishing*) je zelo pogosta oblika kibernetskega kriminala. Glavni cilj ribarjenja na internetu je pridobivanje uporabniških imen in gesel s pomočjo e-pošte in lažnih spletnih strani, lahko pa se pridobijo tudi občutljivejši podatki, kot so podatki spletnih bank. V osnovi napadalci naredijo popolno kopijo spletne strani nekega podjetja, najpogostejše tarče kopiranja pa so banke in druge finančne ustanove. S pomočjo skript zagotovijo, da se uporabniku v naslovni vrstici ne prikaže pravi spletni naslov, ki je sicer podoben pravemu naslovu podjetja, nato pa uporabnika preko sporočila, ki ga ta prejme na svoj e-naslov, pozovejo k spremembi podatkov na lažni spletni strani, ki so jo ustvarili (SAFE.SI, 2017).

Sporočila so napisana zelo sofisticirano, saj je njihov namen z uradnimi nazivi prikazati največjo možno legitimnost. Problem uporabnika je, da ga uradnost in občutek pristnosti sporočila zavedeta do te mere, da izpolni, kar je potrebno, ter s tem preko lažne spletne strani, ki je kot povezava do spletnega mesta uporabniku posredovana v e-poštni nabiralnik, svoje osebne podatke posreduje napadalcu. Končni cilj ribarjenja je kraja uporabnikovega denarja s pomočjo njegovih podatkov, zaupanih tretji osebi. Tarča niso le posamezniki, ampak tudi podjetja, kar ne povzroča le velikih denarnih izgub, temveč lahko povzroči tudi izgubo ugleda in verodostojnosti. V povprečju uspe napadalcem z ribarjenjem prepričati 5 % prejemnikov njihovih spletnih sporočil (Skrt, 2014).

3.3 FARMING

Farming (ang. *pharming*) je podobna oblika spletne prevare kot ribarjenje. Nanaša se na enake okoliščine, v katerih se ustvari kopija spletne strani, katere cilj je pridobiti uporabnikove osebne podatke. Glavna razlika med farmingom in ribarjenjem je, da pri farmingu uporabnika ni potrebno zavesti z lažnim spletnim sporočilom in s povezavo do lažnega spletnega mesta, saj se uporabnik neposredno poveže na kopijo spletnega mesta, tudi če je pravilno vnesel povezavo do strani. Tudi pri tej spletni prevari so najpogostejše tarče banke in druge finančne ustanove. Ker farming deluje neposredno na podlagi vnesene povezave do strani, lahko ta vpliva na celotne skupnosti. Napadalec najprej napade obstoječo stran, in sicer tako, da pridobi njeno uradno povezavo do spletne strani, nato pa za vse uporabnike te strani izvede preusmeritev na svojo kopijo strani, s katere potem pridobiva njihove osebne podatke. Na ta način je leta 2004 napadalec iz Nemčije vse uporabnike spletne trgovine eBay preusmeril na lastno kopijo strani ter tako pridobil osebne podatke več tisoč uporabnikov te spletne trgovine (Symantec Corporation, 2017).

3.4 VIRUSI IN ČRVI

Virusi in črvi so zlonamerni programi, ki se preko omrežne povezave računalnika z internetom ali pa izključno na uporabnikovem računalniku širijo sami, uporabnik pa se tega širjenja ne zaveda. Vsakršna kopija zlonamernega programa ima tudi možnost nadaljnjega širjenja, kar pomeni, da lahko en zlonamerni program hitro okuži celoten računalnik. Glavna razlika med virusi in črvi je, kako se datoteke zlonamernega programa medsebojno kopirajo in posledično širijo preko lokalnega ali internetnega vira. Najbolj poznani črvi se širijo kot priloge, poslane preko spletne pošte ali pa kot lažne povezave do spletnih mest. Ko uporabnik klikne datoteko ali povezavo, se črv prenese in aktivira. Nato se z lastnimi kopijami takoj prične množiti skozi datotečne sisteme, programe in predele operacijskega sistema. Virusi se delijo glede na metodo, ki jo uporabljajo, da pridejo v uporabnikov računalnik. Delimo jih na datotečne viruse, *boot* in *macro* viruse ter skriptne viruse. Za razliko od črva virus potrebuje nek program oziroma »gostitelja«, preko katerega se prenese, aktivira pa se takrat, ko uporabnik želi zagnati program. Ta se tako ne zažene pravilno, virus pa se prične kopirati in širiti. Cilj virusov in črvov je poškodovanje, posredovanje in brisanje datotek iz računalnika ter oteževanje njegovega delovanja (Kaspersky Lab, 2017a).

3.5 KLEPETALNICE, STRANI ZA ZMENKE IN DRUŽBENA OMREŽJA

Uporabniki interneta na spletu ne iščejo le informacij o stvareh, ki jih zanimajo, ampak internet vedno pogosteje uporabljajo tudi kot obliko komuniciranja z drugimi uporabniki. Tako je spletno komuniciranje postalo zelo pomemben komunikacijski kanal, po katerem ljudje izražajo svoja mnenja, delijo informacije in prepričanja. S tem se je pojavil tudi pojem elektronske demokracije, ki v različnih kontekstih označuje številne stvarne pojave, kot je komuniciranje s političnimi predstavniki ali javno razpravljanje v računalniško posredovanih forumih (Oblak Črnič, 2002).

Ena izmed oblik komuniciranja na spletu, ki postaja tudi vedno večja tržna niša, je komuniciranje v klepetalnicah, na straneh za zmenke in socialnih omrežjih. Veliko uporabnikov interneta na zgoraj omenjenih tipih spletnih mest išče priložnosti za iskanje partnerja. Medtem ko klepetalnice počasi zamirajo, vedno popularnejša postajajo družbena omrežja, ki se razlikujejo od klepetalnic in strani za zmenke. Na socialnih omrežjih uporabniki lahko objavljajo svoja mišljenja in z ostalimi uporabniki delijo svoje osebne izkušnje, mnenja, prepričanja, fotografije, osebne podatke ter na splošno vse, kar počnejo v svojem življenju (Adomaitis, 2017).

Namen klepetalnic in strani za zmenke je, da uporabniki preko ustvarjenega profila, v katerega vnesejo svoje osnovne podatke, v iskanju primernega partnerja komunicirajo z drugimi uporabniki. Vse te strani pa spremlja tudi veliko nevarnosti, ki se jih vsi uporabniki

ne zavedajo, zato je moč zabeležiti veliko primerov kraj in zlorab, ki so z njimi neposredno povezane.

Ena izmed zelo pogostih zlorab je kraja identitete, katere namen je nezakonito odvzeti oziroma kopirati podatke enega izmed uporabnikov in se ostalim uporabnikom predstaviti kot ta oseba. Ti podatki se za namen lažnega predstavljanja lahko zlorabijo na raznih forumih in drugih spletnih mestih, z nezakonitimi dejanji pa se pravo osebo lahko namenoma spravi celo pred organe pregona. Ob zadostni količini podatkov, ki se jih lahko pridobi tudi s pomočjo virusov in drugih že omenjenih metod za krajo osebnih podatkov, pa si napadalec z ukradeno identiteto lahko prisvoji tudi denar in druge morebitne ugodnosti prave osebe. Drugi primer pogostih zlorab na navedenih spletnih mestih je lažno predstavljanje, pri čemer je najpogostejše lažno starostno predstavljanje. Najbolj ogrožena skupina so otroci, ki so slabo ali pa sploh niso seznanjeni z nevarnostmi na internetu. Tretja oseba lahko otroku laže o svoji starosti, kar predstavlja potencialno nevarno okolje, saj lahko vodi v pedofilijo. Če obstaja potencialna nevarnost kriminalnih dejanj, kot so ropi in posilstva, pa so ogroženi tudi odrasli (Adomaitis, 2017).

Širjenje informacij preko družbenih in drugih omrežij predstavlja veliko prednost, hkrati pa tudi nevarnost širjenja lažnih informacij, ki imajo lahko negativne posledice na uporabnikova dejanja, njegovo mišljenje in nadaljnje življenje.

3.6 BREZŽIČNA OMREŽJA

Brezžična omrežja so tako v poslovnih procesih kot tudi v domači uporabi zelo praktična, saj smo z njihovo pomočjo z internetom lahko povezani kjerkoli v bližini oddajnika, ne da bi morali biti priključeni na omrežni kabel. Ker pa je namen brezžičnih omrežij povezovanje več naprav na nek skupni oddajnik, to predstavlja potencialno nevarnost vdora tretje osebe v brezžično omrežje. Ta lahko z vdorom v brezžično omrežje povezavo za brezplačni prenos datotek izkoristi za lastne potrebe ter s tem finančno oškoduje lastnika omrežja. Brezžično omrežje lahko uporabi tudi za kriminalne aktivnosti ter preko njega izvede vdor ali drug kibernetični napad.

Tretja oseba lahko z vdorom pregleduje datoteke in povezave naprav v omrežju ter s tem nezakonito beleži ali celo kopira podatke. Preko omrežja lahko posreduje pornografijo in druge neželene programe ter datoteke, kar bi za podjetje lahko pomenilo izgubo zaupanja in kredibilnosti. Z ustvarjanjem dvojnega zaslona lahko spremlja vsako vnašanje osebnih podatkov in gesel na napravah, povezanih s skupnim omrežjem, te podatke pa lahko potem uporabi za lastne potrebe ali pa jih proda oziroma posreduje konkurenčnim podjetjem (AltiusIT, 2017).

4 NAČINI ZAŠČITE IN VAROVANJA OSEBNIH PODATKOV

Podobno kot pri klasični kriminaliteti je tudi na področju računalniške varnosti napredek varnostnih prijemov močno odvisen od novih oblik načinov in izvedbe kaznivih dejanj. Zaščita računalniškega omrežja je večplasten postopek, zaradi njegove zapletenosti pa se lahko poveča možnost nastanka vrzeli, ki jih napadalci lahko izkoristijo (Verdonik & Bratuša, 2005, str. 191).

Poleg uporabe fizične zaščite, požarnega zidu in protivirusnih programov lahko na področju varovanja osebnih podatkov na internetu največ naredimo uporabniki sami. To dosežemo s pregledovanjem in z odstranjevanjem piškotkov ter generiranjem kakovostnih gesel in s samokritičnostjo pri posredovanju osebnih podatkov (Bogataj Jančič, Makarovič, Toplišek, Klemenčič & Tičar, 2007, str. 24).

4.1 FIZIČNA ZAŠČITA

Tovrstna zaščita je namenjena fizičnemu računalniškemu okolju – od objekta, v katerem je oprema, do samega računalnika in njegovih komponent. Ti ukrepi so primerni za zaščito računalnika pred naravnimi in drugimi nesrečami, morebitno tatvino in namernim poškodovanjem opreme. Fizična zaščita predstavlja osnovo varovanja pred računalniškim kriminalom. Možnost vdora fizično preprečimo s ključavnicami ter preverjanji avtentičnosti, računalnik pa lahko dodatno zavarujemo tudi z videonadzorom in s kontrolnimi točkami do centra sistema. Na teh točkah se mora uporabnik identificirati pri fizični osebi, ki varuje vhod v prostor, ali pa z osebnim dokumentom, magnetno kartico ali drugim dovoljenjem dokazati svojo istovetnost. Uporabnik mora poleg tega oceniti tudi tveganje fizičnega vdora v prostor in kraje podatkov na način, da predvidi možnosti vloma v objekt ter s tem zavaruje kritične točke, kot so prezračevalni jaški. Osebje, ki uporablja prostore, mora biti redno spremljano, njihovo dostopanje do podatkov pa primerno označeno s časovnim žigom in argumentirano. Na ta način lahko preprečimo posredovanje podatkov izven objekta tretjim osebam, ki bi zaposlenim v zameno za podatke lahko plačali ali pa jih izsiljevali. Veliko lahko pripomorejo tudi stopnja motivacije, primerna izobrazba zaposlenih ter prijetno delovno okolje, kar zmanjša tveganje nezadovoljstva in posledično nezakonitega posredovanja podatkov (Verdonik & Bratuša, 2005, str. 191–192).

4.2 POŽARNI ZID, PROTIVIRUSNI PROGRAMI

Požarni zid in protivirusni programi predstavljajo ključni obrambni element pred neželenimi vdori tretjih oseb v omrežje. Čeprav oba, tako požarni zid kot protivirusni program, opravljata podobno nalogo in sledita cilju preprečevanja neželenih vdorov v omrežje ter varovanja podatkov, se med seboj razlikujeta.

Požarni zid deluje, ko je računalnik povezan z omrežjem. S pregledovanjem podatkov, ki gredo iz omrežja v računalnik in nazaj v omrežje, nas ščiti pred vdori tretjih oseb, preprečuje pa tudi pošiljanje podatkov iz računalnika v omrežje brez uporabnikovega privoljenja, kot so gesla, podatki o bančnem računu in drugi osebni podatki. Požarni zid tako v času, ko je priklopljen na omrežje, preveri vse posredovane podatke ter išče zlonamerne programe in poskuse vdora, ki izkazujejo delovanje, ki glede na uporabnikova navodila ni bilo predvideno. Požarni zid ne zagotavlja popolne varnosti na spletu, pač pa predstavlja le prvo obrambno linijo med omrežjem in uporabnikovim računalnikom, zato pri zaščiti pred virusi, neželenimi sporočili, slabo zavarovanimi javnimi omrežji in neželenimi programi, ki bi lahko pridobili ter posredovali uporabnikove osebne podatke, ne bo popolnoma uspešen (BullGuard, 2017).

Zaradi razlogov, navedenih zgoraj, je priporočljiva uporaba protivirusnega programa. Ta pregleduje podatke in programe na uporabnikovem računalniku ter išče viruse in druge neželene programe. Ker lahko izsledi le viruse in neželene programe, ki jih pozna ter jih zna identificirati, je izjemno pomembno njegovo redno posodabljanje. Na ta način lahko protivirusni program redno prejema nove podatke o virusih in drugih neželenih programih ter jih tako identificira kot grožnje in izbriše iz računalnika (OAC Technology, 2012).

Kombinacija požarnega zidu in protivirusnega programa zagotavlja visok nivo varnosti računalnika ter skrbi za redni nadzor podatkov, ki prihajajo in odhajajo iz uporabnikovega računalnika v omrežje.

4.3 PREGLEDOVANJE IN ODSTRANJEVANJE PIŠKOTKOV

Pregledovanje in odstranjevanje neprimernih piškotkov zmanjša tveganje odvzema osebnih in drugih podatkov. Piškotke je mogoče pregledovati preko brskalnikov, ki predstavljajo neposredno povezavo med spletnimi stranmi in računalnikom. V večini brskalnikov je piškotke mogoče najti, pregledovati in upravljati pod možnostmi oziroma orodji, kjer uporabnik izbere zavihek »Zasebnost« in pod nastavitvami ali naprednimi nastavitvami lahko pregleda ter odstrani neželene piškotke. Pregledovanje in odstranjevanje piškotkov se od brskalnika do brskalnika razlikujeta. Možnosti odstranjevanja je najlažje preveriti v navodilih za uporabo brskalnika ali neposredno pri ustvarjalcu brskalnika, saj zaradi odstranitve nekaterih piškotkov lahko pride do nedelovanja nekaterih strani. Pogosti primeri so spletne trgovine in strani, ki uporabljajo orodja za predvajanje večpredstavnostnih vsebin in zemljevide (Microsoft, 2017).

4.4 KAKOVOSTNA GESLA IN KRITIČNOST PRI POSREDOVANJU INFORMACIJ

Delovanja in uporabe sodobnih računalniških in informacijskih sistemov, elektronske pošte, socialnih omrežij in raznih forumov si ne predstavljamo več brez gesel. Čeprav poznamo

veliko metod overjanja, kot so pametne kartice, prevladujoč dostop do podatkov ostaja uporaba uporabniškega imena in gesla. Večina uporabnikov uporablja preprosta gesla, ki si jih je lahko zapomniti in ki jih je mogoče hitro vnesti, zaznati pa je tudi pogosto uporabo istih gesel za več različnih uporabniških računov. Uporaba lahkih gesel vdiralcu v račun skozi generatorje močno olajša delo, zato je uporaba močnih gesel pomemben element na področju varovanja osebnih podatkov, na katerem lahko uporabniki največ naredijo sami. Uporabnik geslo vnese takrat, ko želi dostopiti do določenega zavarovanega vira. Tipičen uporabnik se vsak dan sreča z večjim številom gesel, ki jih uporablja v vsakodnevnem življenju. Sem spadajo predvsem gesla bančnih kartic, telefona, računalnika in drugih informacijskih sistemov (Hölbl, 2007).

Geslo lahko definiramo kot niz znakov, ki predstavljajo poljubne črke, številke, ločila in druge ter posebne znake. Dobra in močna gesla so daljša in sestavljena iz čim večjega števila različnih znakov. Med najšibkejša gesla spadajo besede, kot sta »geslo« (ang. *password*) in »administrator« (ang. *admin*), ter kopija uporabniškega imena. Med šibka gesla se uvrščajo še polnopomenske besede, kot so osebna imena in imena krajev, odsvetovana pa je tudi uporaba zaporedij črk na tipkovnici ter izključno številk v vrstnem redu. Med močna gesla spadajo vsi sestavki znakov, ki so daljši od šestih znakov in jih ni mogoče najti v slovarju. Priporočeni sta uporaba vsaj treh do štirih različnih znakov ter kombinacija velikih in malih črk, na voljo pa je tudi veliko spletnih orodij, ki svetujejo, preverjajo in ocenjujejo kakovost vnesenega gesla (Hölbl, 2007).

Pri posredovanju informacij je vedno potrebno upoštevati načelo previdnosti ter biti pozoren na morebitne spremembe redno obiskovanih in novih spletnih mest. Svetovano je redno preverjanje in spreminjanje gesel uporabniških računov vsaj enkrat mesečno. Spletne nakupe je priporočljivo opravljati izključno na straneh, ki imajo navedeno jasno politiko o varovanju osebnih podatkov, ki je skladna z veljavno zakonodajo. Uporabnik mora biti pozoren na neželeno pošto in se v primeru dvoma o morebitni prejeti pošti pozanimati pri pristojnem vodstvu podjetja, ki zahteva vnos osebnih podatkov. Pošto, katere pošiljatelj nam ni poznan ali pri kateri ni jasno razvidno, kdo jo pošilja in kakšen je njen namen, moramo odpirati s previdnostjo. Odsvetovano je vsakršno prenašanje datotek, katerih vir oziroma namen ni znan. Poleg tega se je vedno potrebno vprašati, ali določena spletna stran resnično potrebuje zahtevane informacije, priporočljivo pa je tudi, da stran preverimo za morebitne pretekle prevare (Stay Smart Online, 2017).

5 EMPIRIČNA ANALIZA ZAVEDANJA UPORABNIKOV INTERNETA O NEVARNOSTIH ZA OSEBNE PODATKE

V tem delu diplomske naloge smo raziskovali védenje posameznikov – kako dobro poznajo možnosti kraje ali zlorabe podatkov in ali kljub temu občutljive osebne podatke posredujejo ponudnikom internetnih storitev ter kako dobro poznajo tehnologije za varnost podatkov in kako pogosto se jih poslužujejo pri uporabi interneta.

Uporabili smo metodo anketnega vprašalnika, v katerega smo poskusili zajeti najrazličnejše profile anketirancev, tako mlade kot stare, zaposlene in nezaposlene. Podatke, potrebne za potrditev ali zavrnitev hipotez, smo pridobili z anketnimi vprašalniki.

5.1 HIPOTEZE

Osnovna teza dela je trditev, da se posamezniki oziroma uporabniki ne zavedajo nevarnosti, ki jih prinaša uporaba interneta, in s svojimi osebnimi podatki niso previdni. Preverjali smo hipoteze, katerih potrditev ali zavrnitev nam je pomagala pri potrditvi osnovne teze. Zastavili smo si naslednje štiri hipoteze:

H1: Uporabniki interneta se ne zavedajo nevarnosti za zlorabo osebnih podatkov, zato delijo svoje osebne podatke.

H2: Uporabniki, ki se zavedajo nekaterih nevarnosti, svoje osebne podatke vseeno delijo, saj še niso imeli osebne izkušnje z zlorabo osebnih podatkov.

H3: Uporabniki interneta, ki še niso bili v položaju, da bi bili njihovi osebni podatki zlorabljeni, slabše poznajo nasvete za varno uporabo internetnih storitev od tistih, katerih osebni podatki so že bili zlorabljeni.

H4: Uporabniki interneta ne vedo, kam oziroma na koga se obrniti, če bi bili njihovi osebni podatki zlorabljeni.

5.2 METODOLOGIJA

Za preverjanje zastavljenih hipotez smo uporabili metodo anketiranja uporabnikov interneta. V anketo smo poskusili zajeti najrazličnejše profile anketirancev, tako mlade kot stare, zaposlene in nezaposlene. Za izvedbo ankete, ki je bila anonimna, smo uporabili spletni portal 1ka. Anketni vprašalnik smo sestavili iz niza desetih vprašanj, ki so se neposredno navezovala na podane hipoteze, ter treh splošnih vprašanj, v katerih smo anketirance povprašali po spolu, starostni skupini in doseženi formalni izobrazbi. Delovni

naslov anketnega vprašalnika je bil »Zloraba osebnih podatkov na internetu«. Na podlagi podanih hipotez smo anketirancem zastavili vprašanja, ki se nahajajo v prilogi 1.

5.3 PREDSTAVITEV REZULTATOV IN ANALIZA

Vprašalnik je bil sestavljen iz niza desetih vprašanj, s pomočjo katerih smo na podlagi podanih hipotez ugotavljali, ali se uporabniki interneta zavedajo nevarnosti, ki jih prinaša uporaba interneta, in ali so s svojimi osebnimi podatki previdni. Anketirancem smo za potrebe statistike zastavili tudi tri osnovna vprašanja o njihovem spolu, starostni skupini in dokončani formalni izobrazbi. Vprašalnik smo poslali v izpolnjevanje vsem starostnim skupinam, ki imajo osnovno znanje računalniške pismenosti, nahajal pa se je na spletu in bil izdelan ter deljen preko spletnega portala 1ka. V izpolnjevanje vprašalnika so bili pozvani prijatelji in svojci ter širša javnost, predvsem uporabniki družbenih omrežij, na katerih prihaja do največjih zlorab osebnih podatkov.

Anketo smo izvajali v aprilu in maju 2017, natančneje od 15. aprila do 23. maja 2017. V tem času je v anketi sodelovalo 100 anketirancev, na podlagi podanega anketnega vprašalnika pa je bilo skupaj veljavnih 37 odgovorov. Število slednjih je za tehtno preverjanje zastavljenih hipotez majhno. Zaradi omejenega nabora uporabnikov družbenih omrežij, ki so bili v času izvajanja ankete dostopni, je bilo naslovljeno manjše število anketirancev. Kljub majhnemu številu odgovorov, ki ne daje utemeljene podlage za preverjanje hipotez, smo z izvajanjem ankete nadaljevali. Sklepali smo, da bi bila s ponovnim anketiranjem za izid, ki bi bil negotov oziroma enak prejšnjemu (v tem primeru majhen delež veljavnih odgovorov), porabljena prevelika količina časa. Zastavljeni vprašalnik je kljub omejenosti opravljene analize uporaben tudi za nadaljnje raziskovanje na področju ozaveščenosti uporabnikov pri uporabi interneta.

5.3.1 Spol

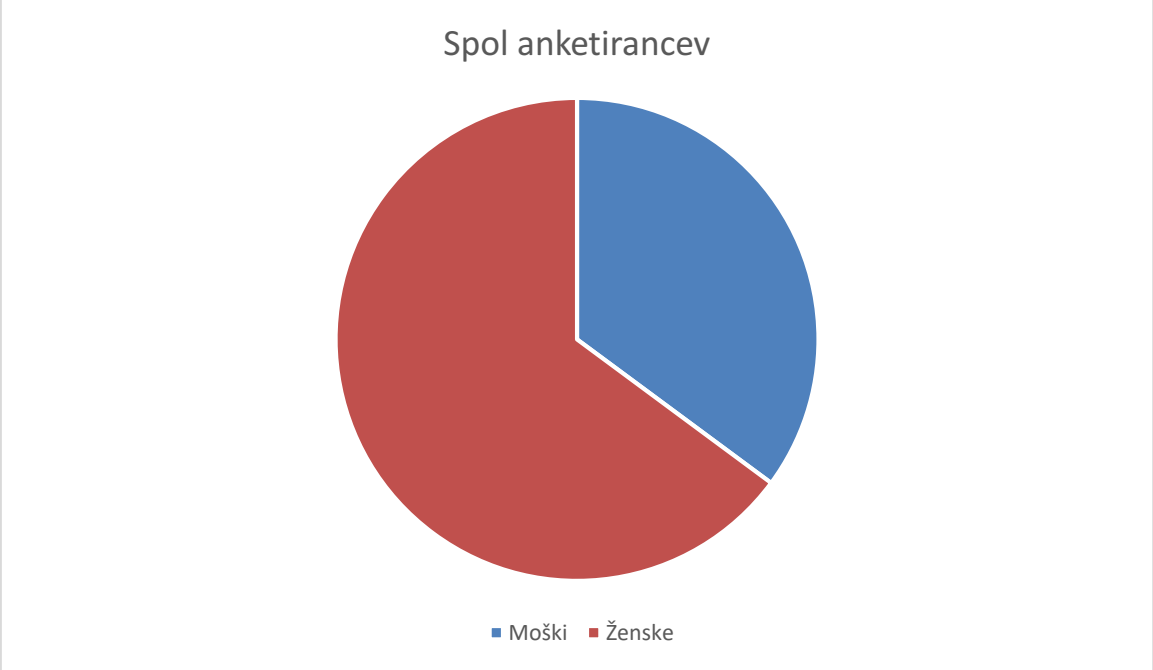
V anketi je sodelovalo 24 žensk in 13 moških, kar pomeni, da je bil delež žensk v anketi 65-odstotni, torej več kot dvotretjinski.

Tabela 1: Delež anketirancev glede na spol

XSPOL	Spol?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Moški.)	13	35 %	35 %
	2 (Ženski.)	24	65 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 1: Delež anketirancev glede na spol (N = 37)



Vir: lasten, tabela 1

Iz grafikona je razvidno, da večinski del anketiranih predstavljajo ženske.

5.3.2 Starost

V anketi je sodelovalo 34 oseb, ki so stare med 21 in 40 let, kar predstavlja 92 % vseh anketiranih, 2 osebi, ki sta stari med 41 in 60 let, ter 1 oseba, ki je stara 61 let ali več.

Tabela 2: Delež anketirancev glede na starost

XSTAR2a4	V katero starostno skupino spadate?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Do 20 let.)	0	0 %	0 %
	2 (21–40 let.)	34	92 %	92 %
	3 (41–60 let.)	2	5 %	97 %
	4 (61 let ali več.)	1	3 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

5.3.3 Najvišja dosežena formalna izobrazba

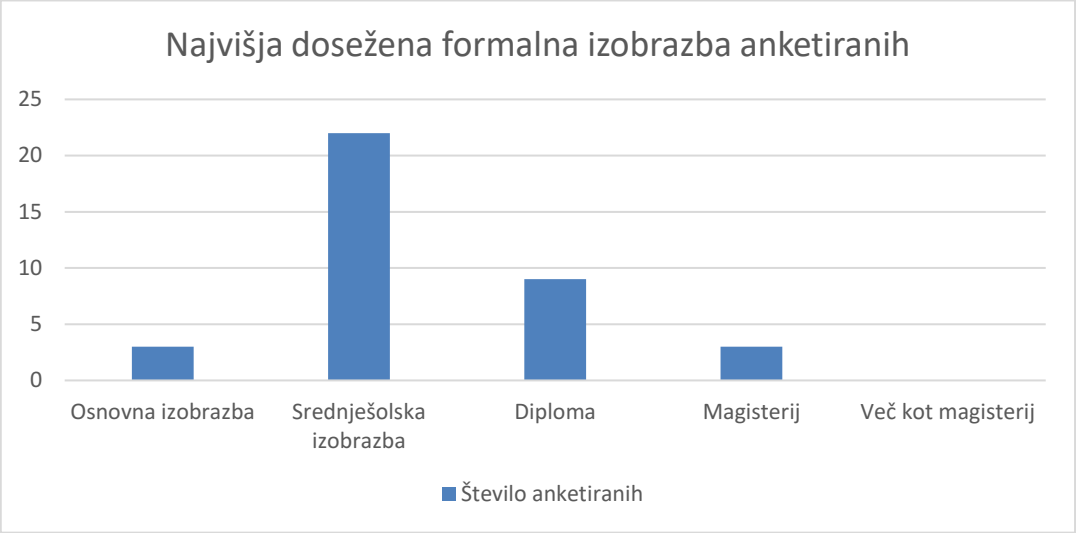
3 anketiranci so imeli osnovno oziroma osnovnošolsko izobrazbo, srednješolsko izobrazbo je imelo 22 vprašanih, opravljeno diplomo 9, magisterij pa so imeli 3 anketirani.

Tabela 3: Delež anketirancev glede na najvišjo doseženo formalno izobrazbo

XIZ1a2	Katera je vaša najvišja dosežena formalna izobrazba?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Osnovna izobrazba.)	3	8 %	8 %
	2 (Srednješolska izobrazba.)	22	59 %	68 %
	3 (Diploma.)	9	24 %	92 %
	4 (Magisterij.)	3	8 %	100 %
	5 (Več kot magisterij.)	0	0 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 2: Delež anketirancev glede na najvišjo doseženo formalno izobrazbo



Vir: lasten, tabela 3

Iz stolpčnega diagrama lahko razberemo, da ima v tej anketi največ anketiranih doseženo srednješolsko izobrazbo.

5.3.4 Q1: Ali ste pripravljeni deliti svoje osebne podatke z neznanci?

Na vprašanje o deljenju svojih osebnih podatkov je 84 % anketirancev dejalo, da svojih osebnih podatkov niso pripravljeni deliti z neznanci. 3 vprašani so odgovorili, da so to pripravljeni storiti delno.

Tabela 4: Prikaz pripravljenosti delitve osebnih podatkov vprašanih z neznanci

Q1	Ali ste pripravljeni deliti svoje osebne podatke z neznanci?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Da.)	0	0 %	0 %
	2 (Ne.)	31	84 %	84 %
	3 (Delno.)	6	16 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 3: Pripravljenost delitve osebnih podatkov vprašanih z neznanci

Vir: lasten, tabela 4

Iz grafikona je razvidno, da večina vprašanih svojih osebnih podatkov ni pripravljena deliti z neznanci.

5.3.5 Q2: Ali ste pripravljeni deliti svoje osebne podatke s prijatelji?

Na to vprašanje je 15 vprašanih odgovorilo, da so svoje osebne podatke pripravljeni deliti s prijatelji, 4 so izrazili mnenje, da tega niso pripravljeni storiti, 18 pa jih je dejalo, da bi to naredili delno.

Tabela 5: Prikaz odgovorov o pripravljenosti delitve osebnih podatkov anketiranih s prijatelji

Q2	Ali ste pripravljeni deliti svoje osebne podatke s prijatelji?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Da.)	15	41 %	41 %
	2 (Ne.)	4	11 %	51 %
	3 (Delno.)	18	49 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 4: Pripravljenost deljenja osebnih podatkov vprašanih s prijatelji

Vir: lasten, tabela 5

Iz grafikona je razvidno, da je večina vprašanih svoje osebne podatke pripravljena le delno deliti s svojimi prijatelji.

5.3.6 Q3: Ali ste posebej pozorni pri deljenju osebnih podatkov s prijatelji preko interneta?

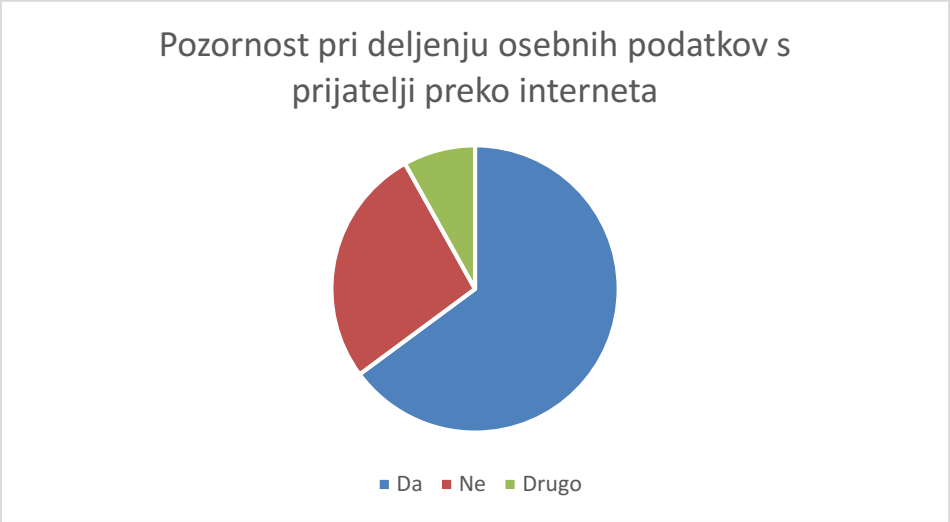
24 vprašanih je odgovorilo, da so pri deljenju osebnih podatkov s prijatelji preko interneta posebej pozorni, 10 jih je odgovorilo, da niso, 3 pa so označili »Drugo:«. Med slednjimi je prvi navedel, da svojih osebnih podatkov preko interneta ne deli, drugi je dejal, da svoje podatke deli včasih, tretji pa, da je odvisno, katere osebne podatke preko interneta deli s prijatelji.

Tabela 6: Prikaz odgovorov o pozornosti pri deljenju osebnih podatkov s prijatelji preko interneta

Q3	Ali ste posebej pozorni pri deljenju osebnih podatkov s prijatelji preko interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Da.)	24	65 %	65 %
	2 (Ne.)	10	27 %	92 %
	3 (Drugo:)	3	8 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 5: Pozornost pri deljenju osebnih podatkov s prijatelji preko interneta



Vir: lasten, tabela 6

Iz grafikona lahko razberemo, da je večina vprašanih pri deljenju osebnih podatkov s prijatelji preko interneta pozorna.

5.3.7 Q4: Ali mislite, da lahko brezskrbno delite svoje osebne podatke preko interneta?

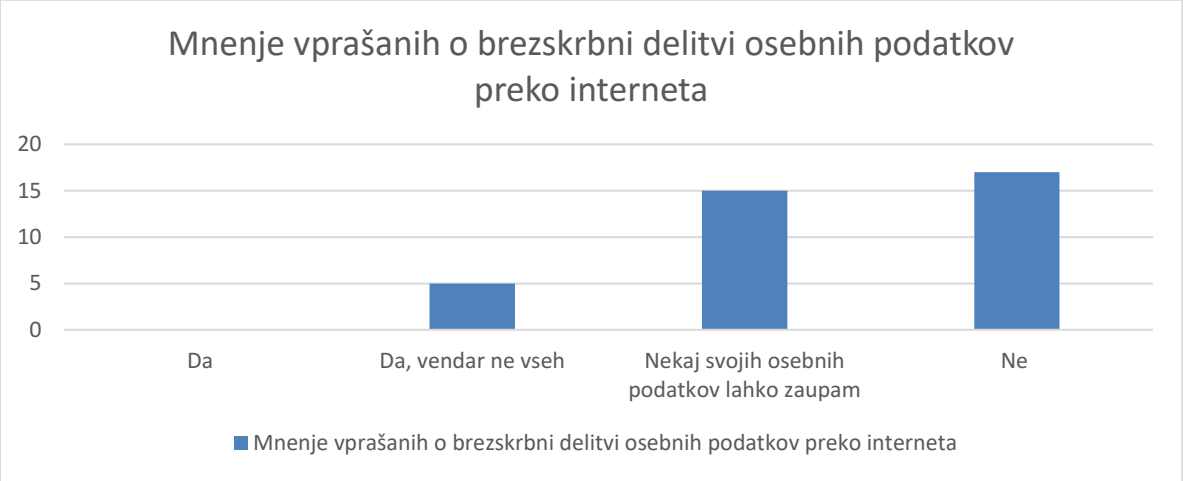
Nihče od vprašanih ne misli, da lahko svoje podatke brezskrbno deli preko interneta. Da, vendar ne vseh, je odgovorilo 5 vprašanih, 15 jih je dejalo, da nekaj svojih podatkov lahko zaupajo, ter 17, da svojih osebnih podatkov ne morejo brezskrbno deliti preko interneta.

Tabela 7: Prikaz odgovorov glede brezskrbne delitve osebnih podatkov vprašanih preko interneta

Q4	Ali mislite, da lahko brezskrbno delite svoje osebne podatke preko interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Da.)	0	0 %	0 %
	2 (Da, vendar ne vseh.)	5	14 %	14 %
	3 (Nekaj svojih osebnih podatkov lahko zaupam.)	15	41 %	54 %
	4 (Ne.)	17	46 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 6: Mnenje vprašanih o brezskrbni delitvi osebnih podatkov preko interneta



Vir: lasten, tabela 7

Iz stolpčnega diagrama lahko razberemo, da je večina vprašanih mnenja, da svojih osebnih podatkov preko interneta ne more brezskrbno deliti ali pa jih lahko deli le delno.

5.3.8 Q5: Katere svoje osebne podatke razkrivate oz. delite preko interneta?

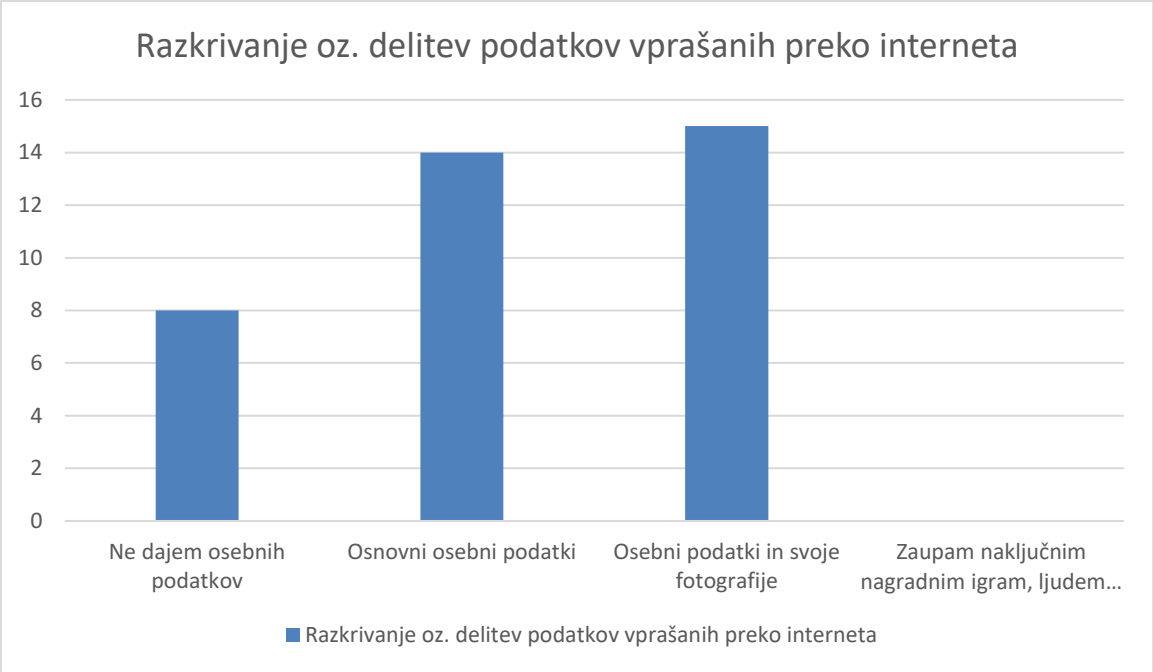
Na vprašanje, katere izmed svojih osebnih podatkov razkrivajo oziroma delijo preko interneta, je 8 vprašanih odgovorilo, da osebnih podatkov sploh ne dajejo. Da delijo svoje osnovne osebne podatke (ime, priimek, starost, kraj bivanja), je odgovorilo 14 vprašanih, da razkrivajo oziroma delijo svoje osebne podatke in fotografije, pa je potrdilo 15 vprašanih, ki z 41 % predstavljajo večino. Nihče od vprašanih pa svojih osebnih podatkov ne razkriva oziroma ne deli v naključnih nagradnih igrah in z ljudmi, ki jih povprašujejo po številki bančnega računa.

Tabela 8: Prikaz odgovorov o razkrivanju oziroma delitvi vrst podatkov preko interneta

Q5	Katere svoje osebne podatke razkrivate oz. delite preko interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Ne dajem osebnih podatkov.)	8	22 %	22 %
	2 (Osebni podatki (ime, priimek, starost, kraj bivanja).)	14	38 %	59 %
	3 (Osebni podatki in svoje fotografije.)	15	41 %	100 %
	4 (Zaupam naključnim nagradnim igram, ljudem, ki me kontaktirajo, dam tudi številko osebnega računa.)	0	0 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 7: Razkrivanje oziroma delitev podatkov vprašanih preko interneta



Vir: lasten, tabela 8

Iz stolpčnega diagrama lahko razberemo, da večina vprašanih zaupa svoje osnovne osebne podatke (ime in priimek, starost, kraj bivanja), 15 vprašanih pa poleg navedenih osnovnih osebnih podatkov razkriva oziroma deli tudi svoje fotografije.

5.3.9 Q6: Komu zaupate svoja gesla?

Na vprašanje o zaupanju gesel je 23 vprašanih odgovorilo, da svoja gesla skrbno izbirajo, zato so zahtevna, in jih ne zaupajo nikomur. 10 jih je odgovorilo, da so njihova gesla

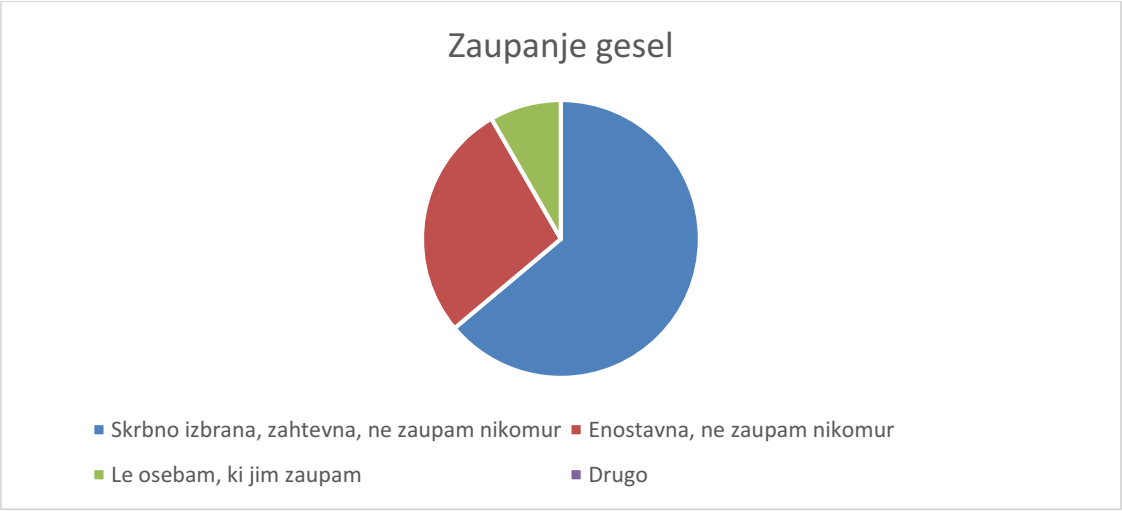
enostavna in jih prav tako ne zaupajo nikomur, 3 pa so dejali, da gesla delijo le z osebami, ki jim zaupajo.

Tabela 9: Prikaz odgovorov vprašanih o zaupanju gesel

Q6	Komu zaupate svoja gesla?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Gesla skrbno izbiram, so zahtevna in jih ne zaupam nikomur.)	23	62 %	62 %
	2 (Gesla so enostavna in jih ne zaupam nikomur.)	10	27 %	92 %
	3 (Gesla zaupam le osebam, ki jim zaupam.)	3	8 %	100 %
	4 (Drugo:)	0	0 %	100 %
Veljavni	Skupaj	36	97 %	

Vir: priloga 1

Grafikon 8: Zaupanje gesel anketiranih



Vir: lasten, tabela 9

Iz grafikona lahko razberemo, da večina vprašanih gesla izbira skrbno, zato so zahtevna, in jih ne zaupa nikomur.

5.3.10 Q7: Ali so bili vaši osebni podatki kdaj zlorabljeni preko računalniških omrežij oziroma interneta?

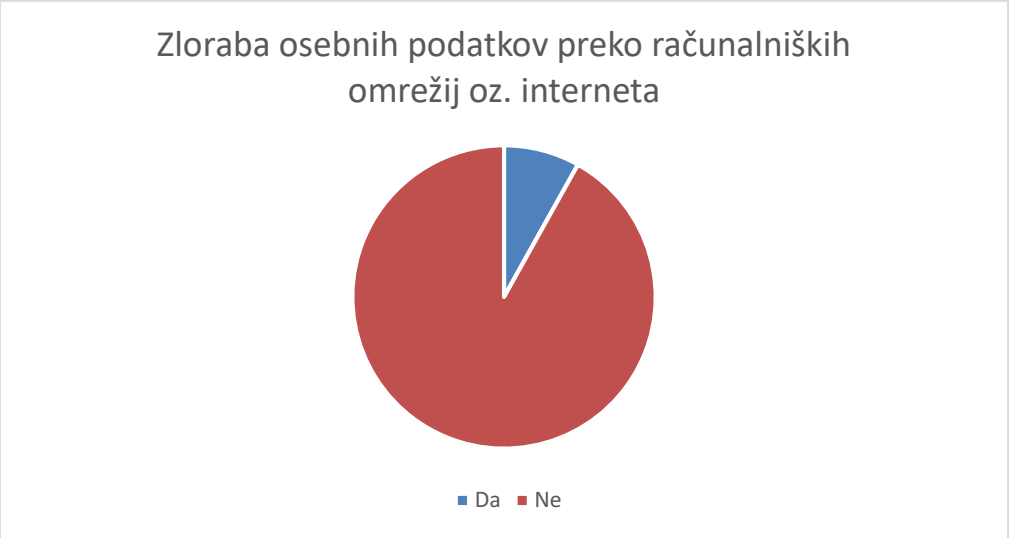
Na vprašanje o primeru zlorabe osebnih podatkov so 3 osebe odgovorile, da so bili njihovi osebni podatki v preteklosti že zlorabljeni preko računalniških omrežij oziroma interneta, ter 34, da se jim to še ni zgodilo.

Tabela 10: Prikaz odgovorov na vprašanje o zlorabi osebnih podatkov anketiranih preko računalniških omrežij oziroma interneta

Q7	Ali so bili vaši osebni podatki kdaj zlorabljeni preko računalniških omrežij oziroma interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Da.)	3	8 %	8 %
	2 (Ne.)	34	92 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 9: Zloraba podatkov vprašanih preko računalniških omrežij oziroma interneta



Vir: lasten, tabela 10

Iz grafikona lahko jasno razberemo, da večina vprašanih še ni doživela zlorabe svojih osebnih podatkov preko računalniških omrežij oziroma interneta.

5.3.11 Q8: Ali poznate osebo, katere osebni podatki so bili že kdaj zlorabljeni preko interneta?

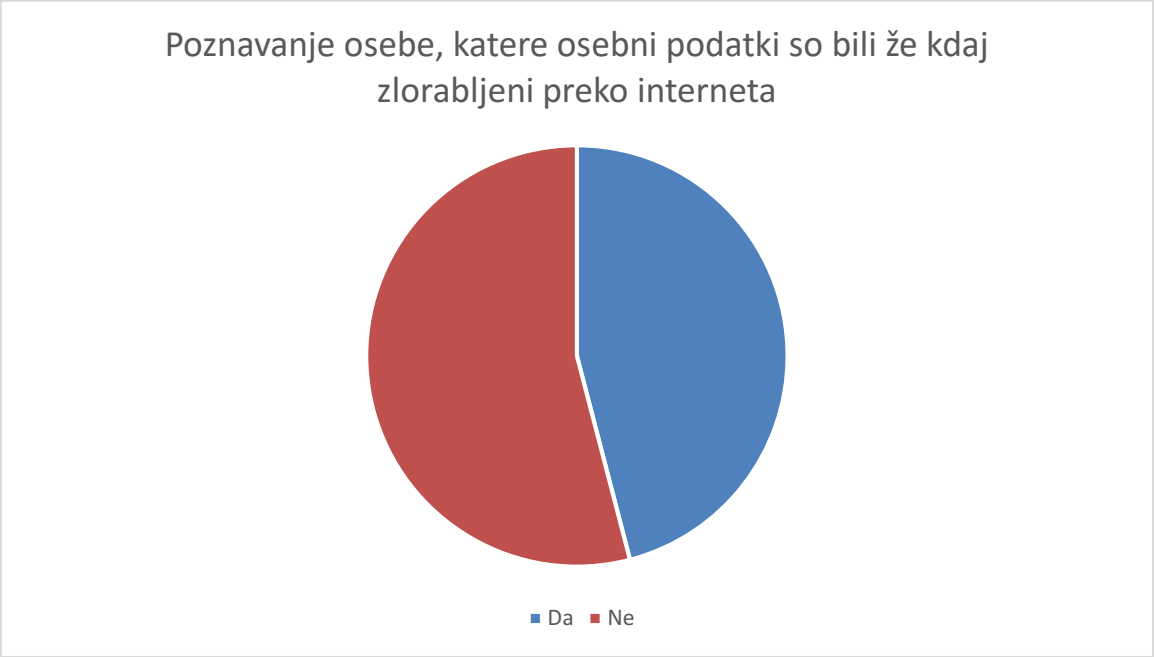
Na vprašanje, ali poznajo osebo, katere osebni podatki so bili v preteklosti že zlorabljeni preko interneta, je 17 vprašanih odgovorilo, da jo poznajo, ter 20, da takšne osebe ne poznajo.

Tabela 11: Prikaz odgovorov na vprašanje o poznavanju osebe, katere osebni podatki so bili v preteklosti že zlorabljeni preko interneta

Q8	Ali poznate osebo, katere osebni podatki so bili že kdaj zlorabljeni preko interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Da.)	17	46 %	46 %
	2 (Ne.)	20	54 %	100 %
Veljavni	Skupaj	37	100 %	

Vir: priloga 1

Grafikon 10: Poznavanje osebe, katere osebni podatki so bili že kdaj zlorabljeni preko interneta



Vir: lasten, tabela 11

Iz podanega grafikona lahko razberemo, da skoraj vsaka druga oseba, vprašana v tej anketi, pozna vsaj eno osebo, katere osebni podatki so v preteklosti že bili zlorabljeni preko interneta.

5.3.12 Q9: Na koga ste se obrnili, ko so bili vaši osebni podatki zlorabljeni preko interneta?

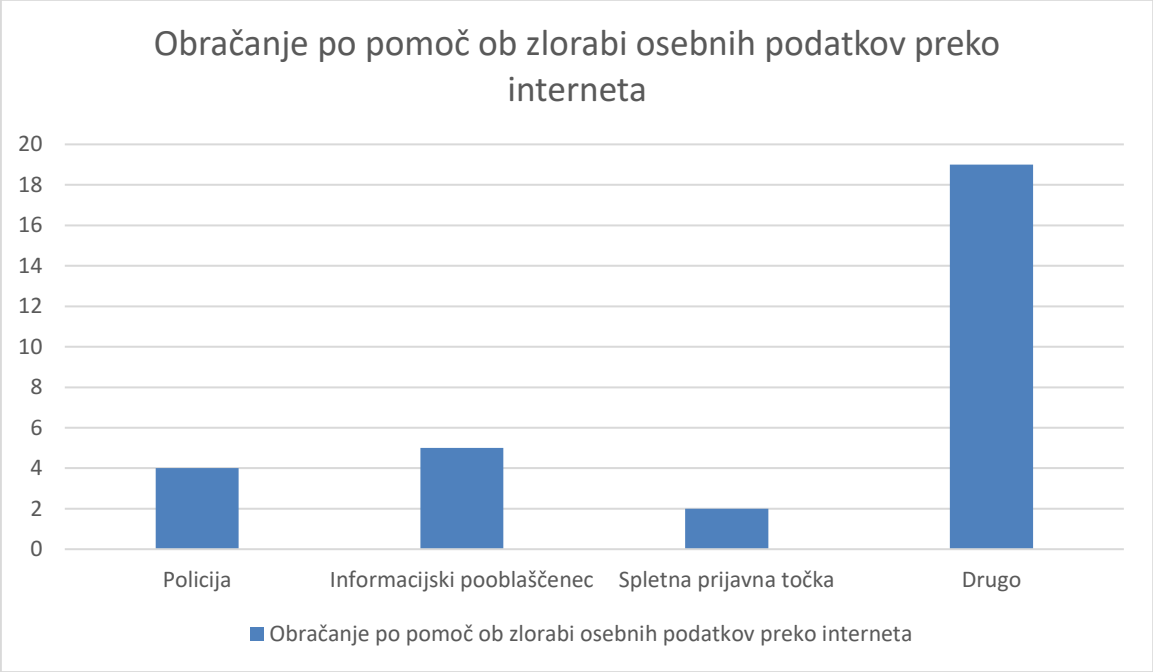
Na vprašanje, na koga so se uporabniki, katerih podatki so bili zlorabljeni, obrnili, so 4 odgovorili, da na policijo, in sicer s kazensko oziroma odškodninsko ovadbo, 5 se jih je obrnilo na informacijskega pooblaščenca in 2 na spletno prijavno točko. Od 19 odgovorov, označenih kot »Drugo:«, je bilo mogoče ovrednotiti 9 odgovorov. 6 vprašanih je pod to točko pojasnilo, da še nikoli niso imeli takšne izkušnje oziroma da njihovi podatki še nikoli niso bili zlorabljeni, 2 sta zlorabo podatkov uredila sama, 1 pa se ni obrnil na nikogar.

Tabela 12: Prikaz odgovorov na vprašanje o obračanju po pomoč ob zlorabi osebnih podatkov preko interneta

Q9	Na koga ste se obrnili, ko so bili vaši osebni podatki zlorabljeni preko interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Na policijo, kazenska ovadba, odškodninska ovadba.)	4	11 %	11 %
	2 (Na informacijskega pooblaščenca.)	5	14 %	30 %
	3 (Spletna prijavna točka.)	2	5 %	37 %
	4 (Drugo:)	19	51 %	100 %
Veljavni	Skupaj	30	81 %	

Vir: priloga 1

Grafikon 11: Obračanje vprašanih po pomoč ob zlorabi osebnih podatkov preko interneta



Vir: lasten, tabela 12

Zaradi prevladujočega odgovora, označenega kot »Drugo:«, in pojasnil, v katerih navajajo, da po večini težav z osebnimi podatki niso imeli, iz grafikona ni moč razbrati uporabnih podatkov.

5.3.13 Q10: Na koga bi se obrnili, če bi bili vaši osebni podatki zlorabljeni preko interneta?

Na vprašanje o tem, na koga bi se obrnili v primeru, da bi bili njihovi osebni podatki zlorabljeni preko interneta, je 19 vprašanih odgovorilo, da bi se obrnili na policijo s

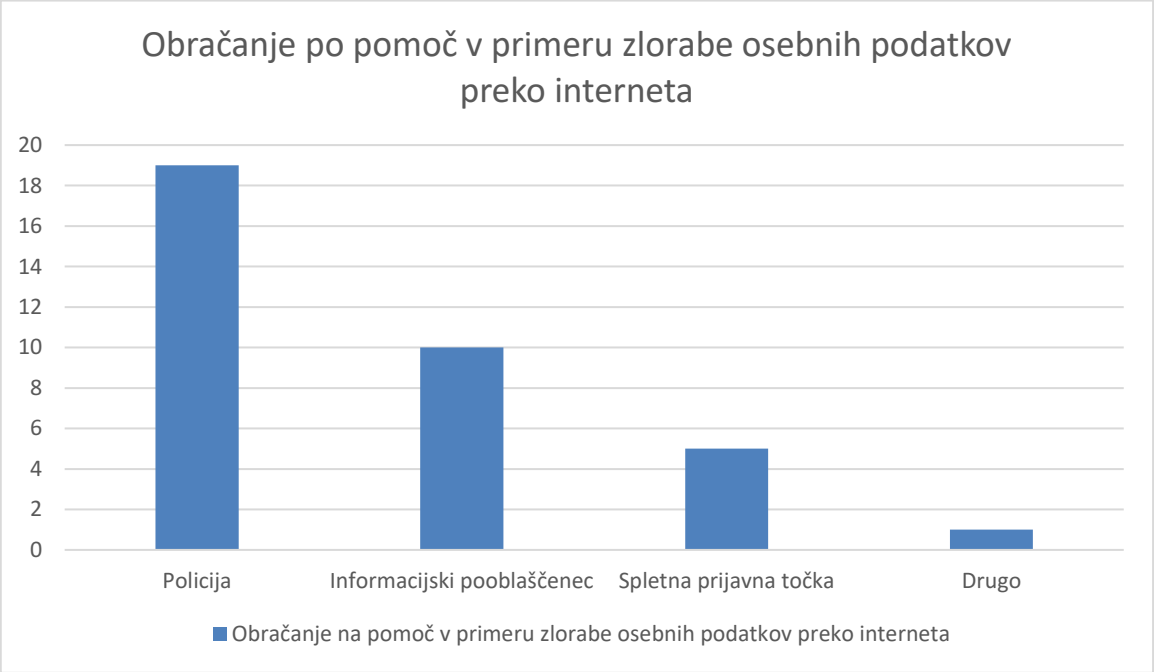
kazensko oziroma odškodninsko ovadbo. 10 jih je odgovorilo, da bi se obrnili na informacijskega pooblaščenca, 5 pa na spletno prijavno točko. Odgovor pod opcijo »Drugo:« glede na postavljeno vprašanje ni bil veljaven.

Tabela 13: Prikaz odgovorov na hipotetično vprašanje, na koga bi se obrnili, če bi bili njihovi osebni podatki zlorabljeni preko interneta

Q10	Na koga bi se obrnili, če bi bili vaši osebni podatki zlorabljeni preko interneta?			
	Odgovori	Frekvenca	Odstotek	Kumulativa
	1 (Na policijo, kazenska ovadba, odškodninska ovadba.)	19	51 %	51 %
	2 (Na informacijskega pooblaščenca.)	10	27 %	83 %
	3 (Spletna prijavna točka.)	5	14 %	97 %
	4 (Drugo:)	1	3 %	100 %
Veljavni	Skupaj	35	95 %	

Vir: priloga 1

Grafikon 12: Obračanje po pomoč v primeru zlorabe osebnih podatkov vprašanih preko interneta



Vir: lasten, tabela 13

Grafikon prikazuje, da bi se v primeru zlorabe osebnih podatkov preko interneta vprašani v večini obrnili na policijo ali na informacijskega pooblaščenca.

5.4 PREVERJANJE HIPOTEZ

Na podlagi podanih in analiziranih rezultatov lahko sedaj preverimo hipoteze, predpostavljene na podlagi osnovne teze.

Hipoteza H1 navaja: Uporabniki interneta se ne zavedajo nevarnosti za zlorabo osebnih podatkov, zato delijo svoje osebne podatke.

Na podlagi v anketi pridobljenih rezultatov ugotavljamo, da je večina uporabnikov pri deljenju osebnih podatkov na internetu dokaj previdna, ko gre za deljenje podatkov, kot so podatki o bančnem računu, kot je razvidno iz tabele 8. Večina uporabnikov brez težav deli osnovne osebne podatke, kot so ime, priimek, starost in kraj bivanja, več kot tretjina vprašanih pa na internetu deli tudi svoje fotografije, kar prav tako lahko vidimo v tabeli 8. Ugotavljamo, da se uporabniki interneta vendarle zavedajo nekaterih nevarnosti za zlorabo osebnih podatkov, saj nihče od vprašanih svojih osebnih podatkov ni bil pripravljen brez oklevanja zaupati neznanim osebam. Na podlagi pridobljenih rezultatov hipotezo H1 lahko potrdimo.

Hipoteza H2 navaja: Uporabniki, ki se zavedajo nekaterih nevarnosti, svoje osebne podatke vseeno delijo, saj še niso imeli osebne izkušnje z zlorabo osebnih podatkov.

Na podlagi v anketi pridobljenih rezultatov ugotavljamo, da se večina uporabnikov zaveda nekaterih nevarnosti na internetu in izraža nezaupanje, kar lahko sklepamo na podlagi podatkov v tabeli 4. Kljub temu več kot dve tretjini vprašanih deli svoje osnovne osebne podatke, kot je razvidno iz tabele 8. Na vprašanje, ali so že bili žrtve kraje osebnih podatkov na internetu, je večina vprašanih odgovorila, da se jim to še ni zgodilo. Iz tega lahko sklepamo, da svoje osebne podatke objavljajo, ker še niso bili žrtve zlorabe svojih osebnih podatkov na internetu. Na podlagi pridobljenih podatkov hipotezo H2 lahko potrdimo.

Hipoteza H3 navaja: Uporabniki interneta, ki še niso bili v položaju, da bi bili njihovi osebni podatki zlorabljeni, slabše poznajo nasvete za varno uporabo internetnih storitev od tistih, katerih osebni podatki so že bili zlorabljeni.

Na podlagi podatkov, ki se nahajajo v tabeli 11, ugotavljamo, da večina uporabnikov še ni bila v položaju, da bi bili njihovi osebni podatki zlorabljeni. Ker so na zastavljeno vprašanje o žrtvah zlorabe osebnih podatkov na internetu pritrdilno odgovorili le 3 vprašani, lahko na podlagi ostalih odgovorov sklepamo, da vprašani varnostnih nasvetov za uporabo internetnih storitev ne poznajo tako dobro kot tisti, katerih podatki so že bili zlorabljeni. Zato na podlagi pridobljenih podatkov hipotezo H3 lahko potrdimo.

Hipoteza H4 navaja: Uporabniki interneta ne vedo, kam oziroma na koga se obrniti, če bi bili njihovi osebni podatki zlorabljeni.

Na podlagi v anketi pridobljenih rezultatov, ki jih prikazuje tabela 13, ugotavljamo, da večina uporabnikov ve, kam oziroma na koga se obrniti, če bi prišlo do zlorabe podatkov. Zato na podlagi pridobljenih podatkov hipotezo H4 lahko ovržemo.

Osnovna teza navaja, da se posamezniki oziroma uporabniki ne zavedajo nevarnosti, ki jih prinaša uporaba interneta, in s svojimi osebnimi podatki niso previdni. Ugotavljamo, da se kljub manjšemu zavedanju nevarnosti na internetu uporabniki, ki so sodelovali v anketi, držijo načela previdnosti ter nezaupljivosti, saj nihče od vprašanih svojih osebnih podatkov ne bi zaupal neznani osebi. Osnovno tezo zato na podlagi pridobljenih podatkov lahko le delno potrdimo.

Zaradi omejenosti števila veljavnih odgovorov so sklepi, ki smo jih sprejeli, veljavni le za vzorec anketirancev, ki so se na anketo odzvali z veljavnimi odgovori. Za preverjanje splošne veljavnosti hipotez bi bilo v prihodnje potrebno opraviti empirično raziskavo na večjem vzorcu anketirancev.

6 ZAKLJUČEK

Na podlagi pridobljenih podatkov smo ugotovili, da nihče od vprašanih v anketi svojih osebnih podatkov ni pripravljen deliti z neznanimi osebami, kar kaže na vsaj delno zavedanje o nevarnostih, ki prežijo na uporabnike interneta. Še vedno pa je več kot polovica anketirancev svoje podatke pripravljena deliti s prijatelji, pri čemer se z vdorom v računalnik uporabnika ali njegovega prijatelja tretje osebe lahko škodoželjno okoristijo s posredovanjem ali zlonamerno uporabo osebnih podatkov. Čeprav osebne podatke delijo s prijatelji, je 65 % odstotkov vprašanih pri deljenju vseeno pozornih, kar odraža upoštevanje načela previdnosti tudi pri posredovanju osebnih podatkov bližnjim. Poleg tega je 46 % vprašanih odgovorilo, da se ne strinjajo s tem, da lahko svoje osebne podatke na internetu brezskrbno delijo, 41 % pa, da lahko zaupajo le del svojih osebnih podatkov, kar kaže na prisotnost zavedanja, da moramo biti pri deljenju svojih osebnih podatkov na internetu previdni. 78 % vprašanih je odgovorilo, da razkrivajo oziroma delijo svoje osnovne osebne podatke, kot so ime, priimek, starost in kraj bivanja. Od tega jih je 41 % potrdilo tudi, da delijo svoje fotografije, kar predstavlja manjše zavedanje o možnostih kraje in zlorabe objavljenih fotografij. Prav tako se posredovanje osnovnih osebnih podatkov večini ne zdi preveč tvegano, spletni portali pa večinoma zahtevajo tudi te podatke, zato uporabnik, če želi uporabljati stran, ki zahteva osnovne osebne podatke, zelo pogosto nima izbire. 62 % vprašanih je odgovorilo, da svoja gesla skrbno izbirajo ter jih ne zaupajo nikomur. Opažamo, da je največje zavedanje o varovanju osebnih podatkov na internetu ravno pri geslih, ki so po navadi skrbno izbrana in jih uporabniki drugim ne zaupajo zlahka, niti bližnjim ne. V tej anketi je delež oseb z zlorabljenimi osebnimi podatki 8-odstotni, kar pomeni, da vdorov ter zlorab osebnih podatkov ni tako veliko. Moramo pa upoštevati, da število uporabnikov interneta z leti narašča, s čimer se povečuje tudi tveganje za obstoječe ter razvoj novih nevarnosti. 51 % vprašanih bi se v primeru zlorabe osebnih podatkov na internetu obrnilo na policijo, razen enega vprašanega pa bi se ostali obrnili na informacijskega pooblaščenca ali na spletno prijavno točko.

Varovanje osebnih podatkov na internetu razvijalcem IT predstavlja velik izziv in hkrati razkol med tem, kolikšen nadzor nad uporabniki in pridobivanjem osebnih podatkov je kot posledica potrebe po nadzorovanju ljudi zaradi njihove varnosti še označen za primernega ter kaj je prekomerno poseganje v zasebnost. Zavedanje uporabnikov o nevarnostih na internetu je z razvojem IT močno napredovalo, s tem pa so se pričela pojavljati tudi nova tveganja, ki jih osebe s primernim tehničnim znanjem želijo nezakonito izkoristiti za lastne potrebe ali druge interese. S povečanjem zavedanja o nevarnostih, ki prežijo na internetu, je delež deljenih osebnih podatkov neznanim osebam postal praktično ničeln, še vedno pa je v povprečju približno 5-odstotni delež vseh uporabnikov spletnih storitev žrtev različnih zlonamernih programov, katerih namen je uporabniku nezakonito odvzeti podatke ali pa

mu škodovati. Z ozaveščanjem uporabnikov o nevarnostih na internetu se s pomočjo različnih programov pričenja že v osnovnih šolah. Na ta način se bo otroke skozi učne procese seznanilo s prepoznavanjem in zavedanjem nevarnosti, še preden bodo lahko postali žrtve zlorab na svetovnem spletu. S podporo države in Evropske unije pa bo s pomočjo različnih projektov o zavedanju uporabnikov in odkrivanju načinov za zmanjševanje tveganja zadostno zavedanje lahko pozitivno vplivalo tudi na zmanjšanje kibernetskega kriminala.

Število veljavnih odgovorov v opravljeni anketi je bilo za tehtno preverjanje zastavljenih hipotez majhno. Zaradi omejenega nabora uporabnikov družbenih omrežij, ki so bili v času izvajanja ankete dostopni, je bilo naslovljeno manjše število anketirancev, vendar smo kljub majhnemu številu odgovorov, ki ne daje utemeljene podlage za preverjanje hipotez, nadaljevali z izvajanjem ankete. Sklepali smo, da bi bila s ponovnim anketiranjem za izid, ki bi bil negotov oziroma enak prejšnjemu (v tem primeru majhen delež veljavnih odgovorov), porabljena prevelika količina časa. Zaradi omejenosti števila veljavnih odgovorov so sklepi, ki smo jih sprejeli, veljavni le za vzorec anketirancev, ki so se na anketo odzvali z veljavnimi odgovori. Za preverjanje splošne veljavnosti hipotez bi bilo v prihodnje potrebno opraviti empirično raziskavo na večjem vzorcu anketirancev, hkrati pa ugotavljamo, da je zastavljeni vprašalnik uporaben tudi za nadaljnje raziskovanje na področju ozaveščenosti uporabnikov pri uporabi interneta.

LITERATURA IN VIRI

LITERATURA

Bogataj Jančič, M., Makarovič, B., Toplišek, J., Klemenčič, G., & Tičar, K. (2007). *Pravni vodnik po internetu*. Ljubljana: GV založba.

Goldberg, I., Wagner, D., & Brewer, E. (1997). Privacy-enhancing technologies for the Internet. V *COMPCON '97: Proceedings of the 42nd IEEE International Computer Conference* (str. 103–110). Berkeley: Univesity of California.

Horniak, V. (2004). *Privacy of Communications – Ethics and Technology* (magistrsko delo). Västerås: Mälardalen University, Department of Computer Science and Engineering.

Jerše, A. (2009). *Varstvo osebnih podatkov in dostop do informacij javnega značaja*. Ljubljana: Dashöfer.

Kovačič, M. (2003). *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.

Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.

Kovačič, M., Modic, D., Rusjan, M., Selinšek, L., Šavnik, J., & Završnik, A. (2010). *Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Križaj, F. (1989). *Osebne svoboščine in zasebnost v »informacijski družbi«*. Ljubljana: Gospodarski vestnik.

Mednarodna konferenca Človeku prijazna, tehnološko popolna, informacijska družba. (2001). *Telekomunikacije 01 telecommunications: razkrij svojo digitalno substanco: zbornik predavanj*. Ljubljana: Inštitut za telekomunikacije.

Mišič, K. & Pirc Musar, N. (2007). *Samo ti odločaš: komu lahko zaupam osebne podatke in kdaj?*. Ljubljana: Informacijski pooblaščenec.

Možina, D. (2002). Se Evropa odreka zasebnosti v korist varnosti?: nova direktiva EU o varstvu zasebnosti pri elektronskih komunikacijah. *Pravna praksa*, *21* (43), 17–19.

Oblak Črnič, T. (2002). Podobe elektronske demokracije. *Teorija in praksa, 39* (2). 155–169.

Pirc Musar, N., Prelesnik, M., & Bien Karlovšek, S. (2006). *Vstop v zasebnost prepovedan!: varstvo osebnih podatkov*. Ljubljana: Informacijski pooblaščenec.

Pivec, F. (2004). *Informacijska družba*. Maribor: Subkulturni azil.

Slovenija. (2006). *Predpisi s področja prava varstva osebnih podatkov in dostopa do informacij javnega značaja*. Ljubljana: GV založba.

Verdonik, I. & Bratuša, T. (2005). *Hekerski vdori in zaščita*. Ljubljana: Pasadena.

Završnik, A. (2015). *Kibernetska kriminaliteta*. Ljubljana: IUS Software, GV založba: Inštitut za kriminologijo pri Pravni fakulteti.

VIRI

Adomaitis, M. B. (17. 11. 2017). Online Social Networking Dangers [online]. Pridobljeno 17. 11. 2017 s http://socialnetworking.lovetoknow.com/Online_Social_Networking_Dangers

AltiusIT. (17. 11. 2017). Top 10 Wireless Network Risks [online]. Pridobljeno 17. 11. 2017 s http://www.altiusit.com/files/blog/Top10WirelessNetworkRisks.htm

Arh, A. (20. 11. 2017). Kaj so piškotki in kako delujejo? [online]. Pridobljeno 20. 11. 2017 s http://piskotki.net/kaj-so-piskotki-in-kako-delujejo/

BullGuard. (18. 11. 2017). Firewall, Internet Security, Anti Virus Protection – BullGuard [online]. Pridobljeno 18. 11. 2017 s https://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/firewall-protection.aspx

Carabott, E. (24. 6. 2010). Do you know the dangers of wireless networks? [online]. Pridobljeno 17. 11. 2017 s https://techtalk.gfi.com/do-you-know-the-dangers-of-wireless-networks/

Cern. (18. 11. 2017). World Wide Web (W3) [online]. Pridobljeno 18. 11. 2017 s http://info.cern.ch/hypertext/WWW/TheProject.html

Hölbl, M. (2007). Gesla in napadi nanje. *Monitor, 17* (6). Pridobljeno 20. 11. 2017 s http://www.monitor.si/clanek/gesla-in-napadi-nanje/122762/

Informacijski pooblaščenec Republike Slovenije. (2007). Zakon o varstvu osebnih podatkov. Uradni list RS, št. 94/07 – uradno prečiščeno besedilo. Pridobljeno 20. 11. 2017 s https://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebnih-podatkov/

Informacijski pooblaščenec Republike Slovenije. (20. 11. 2017a). Odgovori na pogosta vprašanja s področja varstva osebnih podatkov [online]. Pridobljeno 20. 11. 2017 s https://www.ip-rs.si/varstvo-osebnih-podatkov/pogosta-vprasanja/#cb301

Informacijski pooblaščenec Republike Slovenije. (20. 11. 2017b). Pravice posameznika [online]. Pridobljeno 20. 11. 2017 s https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/

Informacijski pooblaščenec Republike Slovenije. (20. 11. 2017c). Smernice o uporabi piškotkov na spletnih straneh [online]. Pridobljeno 20. 11. 2017 s https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_uporabi_piskotkov.pdf

Internet Live Stats. (17. 11. 2017). Total number of Websites [online]. Pridobljeno 17. 11. 2018 s http://www.internetlivestats.com/total-number-of-websites/#screenshots

Kaspersky Lab. (22. 11. 2017a). Viruses and worms [online]. Pridobljeno 22. 11. 2017 s https://securelist.com/threats/viruses-and-worms/

Kaspersky Lab. (22. 11. 2017b). What is a Computer Virus or a Computer Worm? [online]. Pridobljeno 22. 11. 2017 s https://www.kaspersky.com/resource-center/threats/viruses-worms

Microsoft. (20. 11. 2017). Delete and manage cookies [online]. Pridobljeno 20. 11. 2017 s https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies

National Research Council. (1999). 7 Development of the Internet and the World Wide Web. V *Funding a Revolution: Government Support for Computing Research* (str. 169–183). Washington, DC: The National Academies Press. Pridobljeno 19. 11. 2017 s https://www.nap.edu/read/6323/chapter/9

OAC Technology. (30. 7. 2012). What's the difference between firewall and antivirus? [online]. Pridobljeno 18. 11. 2017 s http://www.oactechnology.com/it-blog/whats-the-difference-between-firewall-and-antivirus/

SAFE.SI. (20. 11. 2017). Ribarjenje – kaj je to? [online]. Pridobljeno 20. 11. 2017 s http://old.safe.si/c/1001/Ribarjenje/?preid=1234

Skrt, R. (30. 12. 2014). Phishing napadi – internetna ribičija [online]. Pridobljeno 20. 11. 2017 s http://www.nasvet.com/phishing/

Stay Smart Online. (17. 11. 2017). Personal information and privacy [online]. Pridobljeno 17. 11. 2017 s https://www.staysmartonline.gov.au/protect-yourself/protect-your-stuff/personal-information-and-privacy

Symantec Corporation. (20. 11. 2017). pharming [online]. Pridobljeno 20. 11. 2017 s https://us.norton.com/cybercrime-pharming

PRILOGE

PRILOGA 1: ANKETNI VPRAŠALNIK