UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

ANALIZA ZLORAB OSEBNIH PODATKOV

Dejan Hribar

Ljubljana, september 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

ANALIZA ZLORAB OSEBNIH PODATKOV

Kandidat: Dejan Hribar
Vpisna številka: 04039956
Študijski program: Visokošolski strokovni študijski program Uprava prva stopnja

Mentor: viš. pred. dr. Dušan Štrus

Ljubljana, september 2016

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Dejan Hribar, študent visokošolskega strokovnega študijskega programa Uprava prva stopnja, z vpisno številko 04039956, sem avtor diplomskega dela z naslovom: Analiza zlorab osebnih podatkov.

S svojim podpisom zagotavljam, da:

- je priloženo delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil 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 katerimi so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu 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 lektoriral/a: Anže Slana, dipl. slov (un) in dipl. um. zgod (un)

Ljubljana, 4. 9. 2016

Podpis avtorja:

Dejan Hribar

POVZETEK

V diplomski nalogi sem obdelal temo zlorabe osebnih podatkov, ki je vedno pogostejši problem v današnjem življenju. V današnjih časih lahko hekerji pridejo do osebnih podatkov posameznika že s ponarejenim elektronskim sporočilom ter povezavo do spletne strani, ki je zelo podobna originalni. Z vpisom prilaščenih osebnih podatkov na to spletno stran lahko heker z njimi upravlja kakor želi in v primeru, da gre za npr. ponarejeno spletno stran banke, lahko nato upravlja s posameznikovim premoženjem. Prav zaradi takšnih nevarnosti na spletu sem se v diplomski nalogi osredotočil predvsem na varovanje osebnih podatkov pri uporabi interneta, predstavil najpogostejše možnosti zlorab identitete posameznika ter predstavil nekaj načinov, kako se zavarovati pred krajo in zlorabo osebnih podatkov. Raziskal sem, kako ljudje skrbijo in kako skrbno ravnajo s svojimi osebnimi podatki, predvsem pri uporabi interneta. Na podlagi ankete na temo varstva osebnih podatkov sem ugotovil, da ljudje v povprečju slabo skrbijo za svoje osebne podatke in zaščito le-teh, zato sta moj namen in želja ozaveščati ljudi o načinih in možnostih skrbnega ravnanja z osebnimi podatki.

Ključne besede: kraja identitete, osebni podatki, socialni inženiring, varovanje informacij

SUMMARY

THE ANALYSIS OF THE ABUSE OF PERSONAL DATA

In this thesis i processed the information on the subject of abuse of personal data which is an increasingly more common problem in todays life. Nowadays hackers can acess personal data of individuals through a fake e-mail that contains a link to a fake webpage that is very similiar to an original webpage. By entering personal information on this webpage a hacker can manage the information as he wishes and in the case of a fake bank webpage he can then manage your financial assets. Such threats on the internet are the reason why in my thesis i have focused on the protection of personal data online. I have given the most common examples of abuse of individuals identity and also presented a few ways how to counter theft and abuse of personal data. I have researched how people take care and handle their personal information when they use the internet. Based on the survey on the topic of protection of personal data i found out that people on average take very poor care regarding their personal data. Because of this its my intention and wish to raise awareness among people how to carefully handle their personal information.

Key words: Identity theft, personal data, social engineering, protection of information.

KAZALO

KAZALO PONAZORITEV

KAZALO GRAFIKONOV

KAZALO SLIK

1 UVOD

Ker so osebni podatki zelo občutljivi in z njimi neznanci lahko zlorabijo identiteto posameznikov, morajo biti le-ti previdni pri uporabi osebnih podatkov. Mednje spadajo EMŠO, davčna številka, številka zdravstvenega zavarovanja, PIN koda bančne kartice, PIN koda mobilnega telefona, registrska številka vozila itn. Zloraba osebnih podatkov v zadnjih letih zelo narašča, predvsem z vdori v osebne računalnike zaradi vedno spretnejših hekerjev in seveda tudi vedno boljše računalniške ter programske opreme. Zato je priporočljivo, da uporabniki na računalniku ne hranijo občutljivih osebnih podatkov. Prav tako je pomembno, da npr. pred spletnim nakupovanjem preverijo, ali je spletna stran varna za uporabo in vnos osebnih podatkov, da kasneje ne pride do zlorabe le-teh. Marsikateri posameznik in tudi marsikatero podjetje se ne zaveda, da so osebni podatki zelo ranljivi, če niso ustrezno shranjeni oziroma zavarovani. Zato je treba poskrbeti, da se osebni podatki na računalniku zavarujejo z različnimi antivirusnimi programi ter požarnim zidom, če pa so osebni podatki shranjeni v fizični obliki, je treba poskrbeti, da so podatki varni pred ognjem in vodo ter seveda tudi vlomi.

Namen diplomske naloge je proučiti in raziskati varstvo osebnih podatkov ter njihovo zgodovino. Poleg tega želim raziskati, kaj je zloraba osebnih podatkov, kako se pred zlorabo zavarovati, kateri načini zlorabe so najpogostejši, kaj pomenijo določeni izrazi kot so npr. phishing ali pharming.

Cilj diplomske naloge je predstaviti pojem in zgodovino varstva osebnih podatkov, kako se zaščititi pred zlorabo podatkov. Predstaviti želim tudi najpogostejše napake, ki jih storijo ljudje, zaradi katerih na koncu pride do zlorabe osebnih podatkov.

Pri izdelavi diplomske naloge bom uporabil metodo deskripcije, tako da bom opisal določene procese in dejstva ter z njihovo pomočjo prišel do ugotovitev, in metodo kompilacije, s katero bom uporabil izpiske, publikacije in citate drugih avtorjev. Poleg tega bom v raziskovanje vključil tudi anketo, s katero bom ugotavljal, kako ljudje poskrbijo za varnost svojih osebnih podatkov. Za lažjo raziskavo sem si postavil naslednji hipotezi:

- Hipoteza 1: Kraja osebnih podatkov je vedno pogostejši pojav tako v Sloveniji kot tudi na svetu.
- Hipoteza 2: Podjetja dobro skrbijo, da osebni podatki zaposlenih niso ogroženi.

2 VARSTVO OSEBNIH PODATKOV NA INTERNETU

Zasebnost je temelj človeškega dostojanstva in drugih vrednot (svoboda združevanja, svoboda govora), nekateri avtorji pa trdijo, da so vse človekove pravice neke vrste posamični vidiki pravice do zasebnosti (Kovačič, 2016, str. 34). Ta pravica je največkrat določena kot meja, do katere družba lahko vdre v posameznikove zadeve (Banisar, 1999). Je pa zasebnost pojem, ki ni enodimenzionalen. Nekateri avtorji vidijo več dimenzij zasebnosti. Čebulj (1992, str. 7) navaja tri sestavine zasebnosti, in sicer so to zasebnost v prostoru (možnost posameznika, da je sam), zasebnost osebnosti (svoboda misli, opredelitve, izražanja) ter informacijska zasebnost (možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi). Poročilo Privacy and Human Rights 2016 pa loči naslednje vrste zasebnosti, in sicer so to informacijska zasebnost, ki zajema zbiranje in upravljanje z osebnimi podatki in jo poznamo tudi kot varovanje osebnih podatkov, telesna zasebnost, ki pokriva področje, povezano z genetskimi in drugimi preiskavami telesnih tekočin in/ali tkiv ter odprtin, zasebnost komunikacij, ki zagotavlja zasebnost pošte, telefonskih pogovorov in drugih oblik sporazumevanja, in prostorska zasebnost, ki pa omejuje poseganje v zasebnost na delovnem mestu ali doma.

Druženje in komunikacija otrok in najstnikov preko interneta je v zadnjih letih postala ena največjih privlačnosti. Dandanes otroci preživijo preveč časa na internetu. Na spletu se otroci večinoma zadržujejo predvsem zaradi druženja s sovrstniki preko klepetalnic in socialnih omrežij ter igranja iger, nekaj časa pa na spletu porabijo tudi za učenje in iskanje informacij. Žal se starši, ki bi svoje otroke morali ozaveščati o nevarnostih interneta, ne zavedajo, kako nevaren je lahko za otroke. Starši bi morali poskrbeti, da varnost in zasebnost otrok ne bi bili ogroženi in prav je**,** da se starši in bodoči starši zavedajo, kako nevaren je lahko internet. Ker je na spletu mnogo aktivnosti, ki vodijo v razkrivanje osebnih podatkov, je treba poskrbeti, da se mladi naučijo, kako obvarovati svoje osebne podatke.

Mladi se z razkrivanjem osebnih podatkov na spletu srečujejo pogosto, npr. ko:

- izpolnjujejo obrazce ali obiščejo kakšno spletno stran;
- se registrirajo kot uporabniki določene programske opreme, ki jo dobijo prek spleta;
- si ustvarijo račun ali profil za uporabo elektronske pošte, spletnih klepetalnic, socialnih omrežij ipd.;
- svoje podatke delijo pri komunikaciji z drugimi uporabniki storitev.

Še posebej problematične so lahko informacije, ki jih otroci razkrijejo komercialnim ponudnikom storitev. Za uporabo teh storitev se morajo uporabniki po navadi registrirati in običajno tudi izpolniti kakšen obrazec, ki lahko vsebuje tudi vprašanja o osebnih podatkih. Te prakse so na spletu tako pogoste, da lahko pride do situacije, kjer so mladi na to že tako navajeni, da svoje podatke razkrijejo brez pomisleka, da lahko pride do

zlorabe. Še posebej nevarna so spletna mesta za druženje, kjer pri ustvarjanju profila otroci navedejo svoje pravo ime, naslov, datum rojstva in razkrijejo še mnoge informacije o sebi. Običajno se sploh ne zavedajo, da jim ponudnik te storitve ponuja možnosti, kako profil zaščititi pred nepovabljenimi očmi. Tako so njihovi podatki in zasebno življenje vidni prav vsem uporabnikom.

Zaradi hitre rasti pri uporabi informacijsko-komunikacijskih tehnologij prihaja do vedno večjih možnosti zlorab osebnih podatkov. Mednje sodijo:

- ribarjenje podatkov (angl. phishing);
- nezaželena elektronska sporočila (angl. spam);
- otroška pornografija in sovražni govor;
- zlonamerna programska koda (t. i. virusi, črvi, vohunski programi ipd.);
- kraja identitete.

Za zaščito pred zlorabami je najprej treba poskrbeti, da je na računalniku nameščena strojna in programska zaščita, ki jo je treba stalno posodabljati (anti-virusni paketi, požarni zidovi ...), predvsem pa se je treba nevarnosti zavedati in biti še posebej previden pri razkrivanju osebnih podatkov na spletu. (Informacijski pooblaščenec, 2016)

2.1 RIBARJENJE PODATKOV

Izraz ribarjenje podatkov ali po angleško phishing izvira iz angleških besed za geslo (password) in ribarjenje (fishing). Spletni goljufi s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnikov na takšen ali drugačen način želijo izvabiti njihove osebne podatke, kot so: številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila ipd. Pri tem uporabljajo več različnih tehnik, ki spadajo v tako imenovani socialni inženiring, s tem pa poskušajo od uporabnika na prebrisan način pridobiti osebne podatke. Praviloma najprej postavijo lažno spletno stran, podobno originalni, nato pa uporabnika z lažnim elektronskim sporočilom poskušajo pripraviti do obiska te strani ali pa poskušajo pridobiti njegove podatke s takojšnjim odgovorom na elektronsko sporočilo. Za ogoljufanega uporabnika so posledice lahko relativno majhne (npr. odtujitev brezplačne elektronske pošte), lahko pa tudi zelo velike (npr. kraja večjih vsot denarja z bančnih računov). Ogroženost zaradi ribarjenja podatkov se vsako leto povečuje, na svetu namreč dnevno nastane med 100 in 200 novih tovrstnih lažnih strani. (Informacijski pooblaščenec, 2016)

Ker je v Sloveniji med uporabniki interneta več kot 90 % otrok in najstnikov, je zelo pomembno, da se jih seznani z nevarnostmi, ki jih lahko doletijo med brskanjem po internetu. Zato bom v nadaljevanju mladim predstavil nekaj priporočil za obrambo pred phishingom, ki so dostopna tudi na spletni strani Informacijskega pooblaščenca Republike Slovenije.

2.1.1 PRIPOROČILA ZA OBRAMBO PRED RIBARJENJEM PODATKOV

E-pošta, ki je namenjena ribarjenju podatkov, običajno uporablja imena in znane oblikovne elemente pravih organizacij, poleg tega pa uporablja tudi na videz resnična imena zaposlenih in oddelkov v organizaciji. Ker pa želi tat identitete žrtev čim bolj prepričati v resničnost organizacije, uporablja tudi ime domene, ki je podobna pravemu naslovu domene. Žrtev se mora zavedati, da prave organizacije ne bi grozile z izgubo podatkov, brisanjem računa ali podobnimi škodljivimi posledicami.

Zavedati se je treba, da razne organizacije, predvsem pa banke, uporabnikov ne bodo nagovarjale preko navadne e-pošte, predvsem pa na ta način ne bodo zahtevale osebnih podatkov, kot so uporabniška imena in gesla, oziroma ne bodo pozivale k izvozu digitalnega potrdila. Če uporabnik dvomi v resničnost prejetega sporočila, lahko še vedno uporabi telefon ali drug način komuniciranja z banko in se prepriča, ali je sporočilo verodostojno. Poleg tega pa je priporočljivo, da ne klika na povezave v elektronski pošti, ki se zdijo kot prava povezava do banke, temveč naj raje uporabi zaznamke ali bližnjice, ki jih je predhodno shranil v brskalnik.

Z vstopom na spletno stran naj uporabnik preveri, ali je povezava do spletnega mesta varovana s t. i. varnim http protokolom imenovanim https, v vrstici stanja na dnu okna v brskalniku mora biti prikazana zaklenjena ključavnica. Pri tem je treba biti pozoren na ostala priporočila, saj v primeru, da se na računalniku nahaja nevarna programska oprema, tudi ta korak ne more biti zavarovan pred izgubo podatkov in ostalimi posledicami. Razlika med pravo in lažno stranjo je lahko minimalna, poleg tega pa za nekatere organizacije obstaja poleg prave domene tudi več deset zelo podobnih registriranih domen (npr. spletnabanka.com, spletna-banka.com, login-spletnabanka.com ipd.). Na tem mestu velja opozorilo, da uporabnika v primeru okužbe z nevarnimi trojanskimi konji tudi preverjanje varnosti povezave in zaklenjene ključavnice ne bo obvarovalo pred zlorabo podatkov. Nekateri trojanski konji pravo okno neopazno prekrijejo z lažnim, zato je ključno, da se protivirusne programe redno posodablja. Poskrbeti je treba tudi za redno nameščanje varnostnih popravkov operacijskega sistema ter se izogniti nameščanju programov s sumljivih spletnih mest. Poleg tega pa se velja izogibati odpiranju sporočil neznanih pošiljateljev, predvsem tistih s priponkami izvršljivih programov, kot so npr. .exe ali .bat datoteke.

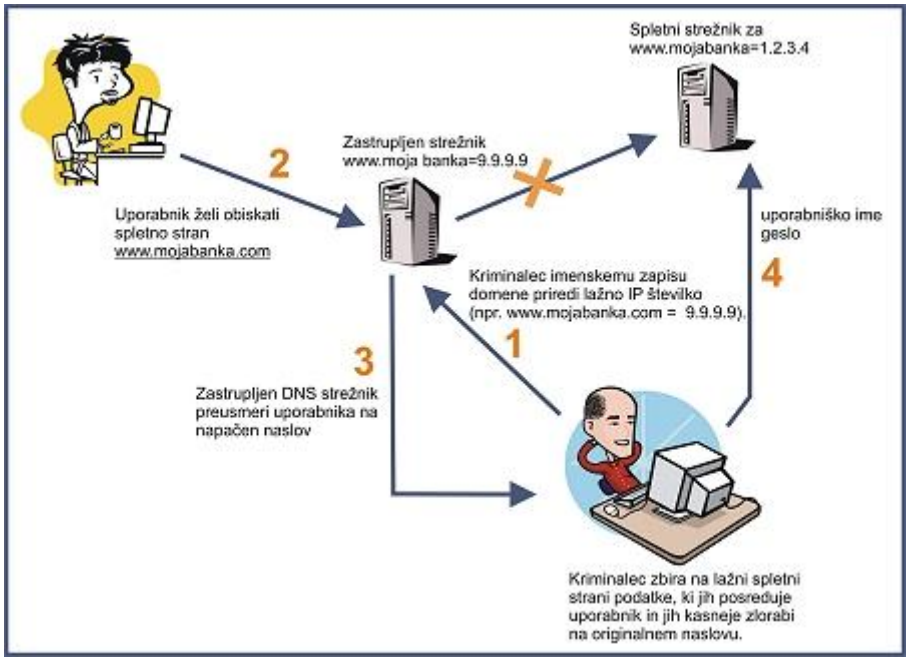
Če uporabnik večkrat nakupuje preko spleta, naj redno preverja bančne izpiske. Pozoren naj bo, da poleg transakcij, ki jih je izvedel, v bančnem izpisku ni navedene še kakšne transakcije, ki je ni izvedel.

Ribarjenje podatkov ni več vezano na angleško govoreči svet, ampak se je v zadnjem času začelo pojavljati tudi v Sloveniji. Ker pa je ribarjenje podatkov resna zadeva, je priporočljivo, da se za spletno brskanje uporablja posodobljene verzije brskalnikov, kot so Internet Explorer, Mozilla Firefox, ipd., saj ti brskalniki že vsebujejo določene tehnologije, ki lahko zaščitijo pred ribarjenjem podatkov.

2.2 PHARMING NAPADI

Medtem ko phishing napadi temeljijo predvsem na ponarejenih e-sporočilih, ki na lažne spletne strani privabljajo uporabnike z namenom, da si na protipraven način pridobijo njihove številke kreditnih kartic in ostale zaupne podatke, pa napadalci vse bolj uporabljajo napade brez vabe. Pri pharming napadih gre namreč za neposredne napade na DNS strežnike ali pa na datoteko o gostiteljih (ang. hosts file), ki se nahaja na uporabnikovem računalniku. Posledica tovrstnih napadov je ta, da so uporabniki, ne da bi to sploh vedeli, preusmerjeni na zlonamerne spletne strani (ang. malicious sites), četudi v naslovno vrstico brskalnika pravilno vnesejo URL naslov strani, ki bi jo radi obiskali. Ker pa so lažne strani zelo pogosto popolne kopije originalnih, uporabniki po navadi sploh ne opazijo, da se nahajajo na lažnem naslovu in da se v ozadju dogaja nekaj škodljivega. Napadalci ciljajo ravno na nevednost uporabnikov, saj od njih, ko se enkrat nahajajo na lažni strani, ni težko izvabiti zaupnih podatkov, med katerimi so še posebej zaželene številke kreditnih kartic ter podatki, ki so potrebni za dostop in uporabo e-bančnih storitev. (Skrt, 2016)

Slika 1: Primer pharming napada



Vir: skrt (2005)

2.2.1 DNS STREŽNIKI

Za lažje razumevanje pharming napadov je treba na kratko razložiti delovanje DNS strežnikov, ki skrbijo za pretvarjanje imenskih naslovov domen v specifične internetne IP naslove. DNS strežnike si lahko predstavljamo tudi kot nekakšne telefonske imenike za domene. Ko želi uporabnik obiskati določeno spletno stran, se zahteva po obisku posreduje od njegovega računalnika do najbližjega DNS strežnika, ki poskrbi za prevod spletnega naslova v ustrezen IP naslov, ki je sestavljen iz numeričnega niza (npr.

www.imedomene.com = 1.1.1.1.). Na podlagi uporabnikove zahteve po ogledu določene strani DNS strežnik preusmeri uporabnika na stran, ki jo ta želi obiskati. Če strežnik zahtevka ne more razrešiti, ker nima ustreznega zapisa v pretvorbeni tabeli, posreduje zahtevo do drugega strežnika. Zahtevki potujejo naprej tako dolgo, dokler ne dobijo pravega odgovora in dokler računalnik ne dobi nazaj odgovarjajočega IP naslova spletne strani, ki jo želi obiskati. DNS sistem (domain name system) je bil uveden predvsem zaradi tega, ker si ljudje lažje zapomnimo spletna imena (npr. mojmikro.si) kot pa IP naslove (npr. 193.77.122.36).

Pharming napadi se lahko izvajajo lokalno (na posameznemu računalniku) ali pa neposredno na DNS strežnikih. Medtem ko je za neposredne napade značilno, da prizadenejo vse uporabnike, ki dostopajo do napadenega strežnika, pa je za lokalne napade značilno, da so po eni strani nevarnejši in učinkovitejši od strežniških napadov, po drugi strani pa tudi lažje izvedljivi, saj mora napadalec »le« spremeniti t. i. host datoteko, ki se nahaja na uporabnikovemu računalniku v direktoriju C:WINDOWSsystem32driversetc, in ustvariti lažno spletno stran, na katero bo uporabnik preusmerjen. Napadalci pridejo do host datoteke na daljavo ali pa jo prepišejo s pomočjo različnih virusov ali »trojancev« (kot so npr. Bancos, Banker ali Banbra), ki se jih največkrat dobi prek e-pošte. Hosts datoteka je napadalcem zanimiva predvsem zaradi tega, ker lahko uporabnikovemu računalniku prihrani pot do DNS strežnika, saj lahko vsebuje najpogosteje obiskane IP naslove in njim pripadajoče URL naslove. Če uspe napadalcu prepisati oziroma opremiti host datoteko z lažnimi naslovi, bo uporabnik tudi ob primeru pravilnega vnosa URL naslova preusmerjen na lažno stran, ki jo je ustvaril napadalec.

Neposredni strežniški napadi, ki se realizirajo s kompromitiranjem DNS sistema, so poznani tudi pod imenom DNS poisoning. Ker so tovrstni pharming napadi usmerjeni na strežnik in ne na posamezne uporabnike, lahko v kratkem času dosežejo veliko število žrtev, ki jih preusmerijo na zlonamerne strani. Če je DNS strežnik, ki pretvarja spletne in e-poštne naslove v numerične nize, zastrupljen, pomeni, da vsebuje napačne povezave med imeni domen in pripadajočimi IP številkami. Zaradi tega pride do nepravilnega razreševanja IP naslovov in posledično do preusmeritev uporabnikov na napačne strani kljub pravilno vnesenim URL naslovom. Posledica zastrupitve DNS strežnika je, da se imenskemu zapisu domene priredi lažna IP številka (npr. www.imedomene.com = 9.9.9.9). Če bo po zastrupitvi uporabnik odtipkal naslov www.imedomene.com, bo, ne da bi to sploh vedel, preusmerjen na lažno stran 9.9.9.9, ki bo na videz po vsej verjetnosti popolna kopija originalne strani. Na tej lažni strani bo napadalec od uporabnika skušal izvabiti podatke, ki bi jih lahko kasneje zlorabil na originalni strani.

Najbolj osnovna zaščita pred napadi je uporaba protivirusnih programov s posodobljenimi virusnimi definicijami, ki jih mora uporabljati vsak uporabnik računalnika. Protivirusni programi niso zelo učinkovito sredstvo samo v boju proti virusom, ampak tudi v boju proti pharming napadom, saj lahko preprečijo okužbo računalnika s »trojanci«, ki lahko spremenijo host datoteko. Žal pa si popolne zaščite računalnika tudi z uporabo protivurusnih programov ni mogoče popolnoma zagotoviti, saj se ustrezna orodja za

odstranitev običajno pojavijo šele takrat, ko so virusi, črvi in »trojanci« že nekaj časa v obtoku. Za preventivo pred pharming napadi je zelo priporočljiva tudi uporaba požarnega zidu, ki napadalcem lahko prepreči vstop v računalnik preko nezaščitenih komunikacijskih vrat in s tem spreminjanje sistema oziroma host datoteke. Za preventivo pred pharming napadi pa se lahko poskrbi tudi tako, da se ne odpira sumljivih priponk v poštnih sporočilih in da uporabnik brez predhodnega razmisleka ne klika na povezave v sporočilih, ki naj bi jih posredovale banke, izdajatelji kreditnih kartic ter podjetja, ki se ukvarjajo z elektronskimi plačilnimi storitvami. Če uporabnik dostopa do spletnih strani, kjer posreduje zaupne in občutljive podatke, naj nujno preveri, ali se nahaja na spletni strani, ki uporablja šifriranje podatkov (URL naslov v naslovni vrstici se mora začeti s https://). Če za brskanje po internetu uporablja Internet Explorer se mora v statusni vrstici na spodnji desni strani brskalnika pojaviti ikona z zaklenjeno ključavnico, kar pomeni, da se nahaja na spletni strani, ki uporablja šifriranje. Z dvoklikom na ključavnico je možno tudi preveriti, ali se naslov varnostnega certifikata ujema z naslovom spletnega mesta, kjer se uporabnik trenutno nahaja. (Skrt, 2016)

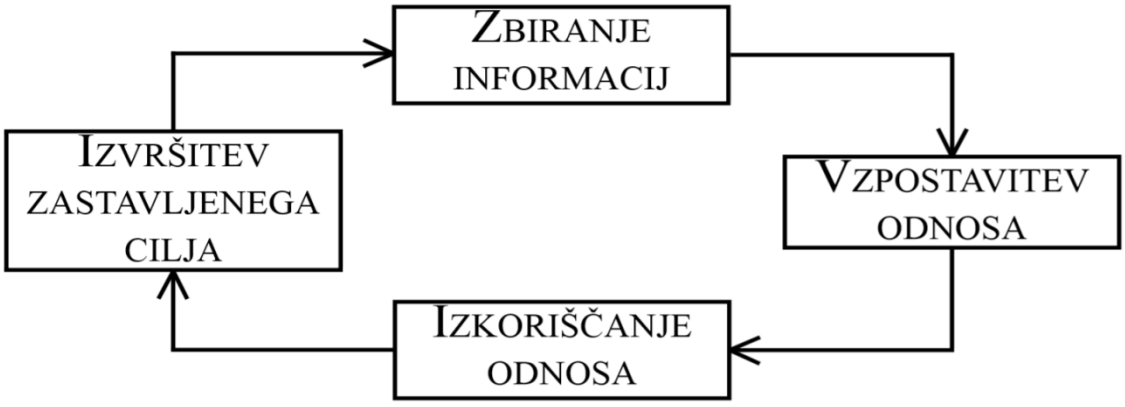
2.3 SOCIALNI INŽENIRING

Socialni inženiring je način prevare, kjer prevarant z izkoriščanjem človekovih lastnosti in s pomočjo manipulacije prepriča žrtev v neko dejanje, ki ga ta sicer običajno ne bi storila. Pri svojem delu socialni inženir uporablja mimikrijo, najpogosteje pa se trudi priti do zasebnih informacij. Socialni inženiring lahko ločimo na netehnični in tehnični. Pri prvem prevaranti uporabljajo osebni pristop, medtem ko se drugega uporablja predvsem v navezi z računalniki in internetom. (Suša, 2009, str. 4)

2.3.1 ŽIVLJENJSKI CIKEL SOCIALNEGA INŽENIRINGA

Napad s pomočjo socialnega inženiringa je sestavljen iz štirih korakov. Vse stopnje so med seboj povezane in so odvisne druga od druge.

Slika 2: Življenjski cikel socialnega inženiringa



Vir: Informacijski pooblaščenec (2009, str. 7)

»Zbiranje informacij je prvi in verjetno najpomembnejši korak v tem življenjskem krogu. Uspeh socialnega inženirja je odvisen predvsem od količine in kakovosti pridobljenih podatkov. Zbirajo se bolj osnovni podatki, kot so telefonske številke, elektronski naslovi ali poštni naslovi, pa tudi bolj osebni podatki, kot so rojstni datum, dekliški priimek, vzdevek ipd. Podatki niso vezani samo na ljudi, ampak tudi na stvari – npr. na arhitekturo informacijskega sistema, poznavanje organizacijskih postopkov v podjetju. Napadalec nato uporabi podatke za vzpostavitev odnosa z žrtvijo.

Druga faza je odvisna predvsem od načina delovanja samega napadalca. Napadalec v tej stopnji poskuša vzpostaviti ter razvijati odnos z žrtvijo. Izkoristi prej pridobljene podatke in odigra določeno vlogo. Prepričljivost odigrane vloge napadalca je odvisna predvsem od kakovosti in količine pridobljenih podatkov ter njegovih igralskih spretnosti. Ljudje smo nagnjeni k tem, da zaupamo informacije tistemu, za katerega menimo, da je zaupanja vreden, to pa napadalec doseže predvsem s poznavanjem oz. posredovanjem podatkov nam. V tej fazi želi socialni inženir prepričati žrtev, da mu lahko zaupa in z njim deli podatke, ki so lahko bolj ali manj zaupni.

Ko napadalec prepriča žrtev, da mu lahko zaupa, in vzpostavi odnos z njo, sledi naslednji korak, v katerem ta odnos in pridobljeno zaupanje izkorišča. Če je napadalec v prejšnjem koraku uspešno prepričal žrtev, da je vreden zaupanja, mu žrtev velikokrat brez zadržkov izda podatke, ki jih želi.

Izvedba zastavljenega cilja je zadnji korak v procesu. Napadalec izkoristi pridobljene podatke za dosego zastavljenega cilja, do katerega ga lahko pripeljejo že same informacije ali pa te napadalec uporabi za pomoč pri vdiranju na tehnični način. Pomembno je poudariti, da življenjski cikel napada s socialnim inženiringom ni končan. Napadalec lahko tako še naprej zbira informacije in s tem ali razširi napad glede na informacijski sistem, uporabi podatke pri drugi žrtvi ali pridobi dodatne podatke, ki mu omogočajo izvesti drug napad. Ker je napadalec že vzpostavil odnos z žrtvijo, ga lahko s pridom izkorišča tudi v drugih situacijah.« (Informacijski pooblaščenec, 2009, str. 7)

2.4 VOHUNSKA PROGRAMSKA OPREMA, ADWARE IN TROJANSKI KONJI

2.4.1 VOHUNSKA PROGRAMSKA OPREMA

Vohunski programi so programi, ki so nameščeni v računalniku z namenom opazovanja, beleženja aktivnosti in dejavnosti uporabnika. S tujko jih imenujemo Spyware. Nekateri vohunski programi lahko celo beležijo in spremljajo udarce tipk in informacije, ki jih uporabnik vnaša na spletna mesta ali v druge programe, ter te informacije uporabijo za ciljno oglaševanje ali krajo identitete. Vohunska programska oprema lahko v spletni brskalnik na primer namesti neželene orodne vrstice, povezave ali priljubljene strani, spremeni privzeto domačo stran ali pogosto prikazuje pojavne oglase in spremeni nastavitve računalnika, običajno brez uporabnikovega soglasja. Nekatera tovrstna programska oprema sploh ne kaže znakov, da je na računalniku, ampak na skrivaj zbira zaupne podatke, na primer spletna mesta, ki jih obiskuje, ali besedilo, ki ga vnaša. Večina vohunske programske opreme se namesti z brezplačno programsko opremo, ki jo

uporabnik prenese, včasih pa se računalnik okuži že, ko obišče neko spletno mesto. (ŠC Celje, 2016)

2.4.2 ZAŠČITA PRED VOHUNSKIMI VIRUSI

Za zaščito pred vohunsko programsko opremo je najbolje, da uporabnik uporabi protivohunski program. V Windows sistemu je vgrajen protivohunski program, imenovan Windows Defender. Ta opozori, ko se vohunska programska oprema poskuša namestiti v računalnik. Prav tako lahko pregleda računalnik, v njem poišče že obstoječo vohunsko programsko opremo in jo odstrani. Ker vohunska oprema nastaja vsak dan, je treba Windows Defender redno posodabljati, da lahko odkriva najnovejše grožnje vohunske programske opreme ter ščiti pred njimi. (ŠC Celje , 2016)

2.4.3 ADWARE

Adware ali advertisement software je programska oprema, ki zlorablja računalnik za predvajanje oglaševalskih sporočil. Nekateri programi tudi zbirajo informacije o uporabnikovih brskalnih navadah. Na podlagi teh informacij nato predvajajo oglasna sporočila. Adware program se običajno namesti ob nameščanju kakšnega drugega brezplačnega ali nelegalnega programa. (Flibo, 2016)

2.4.4 TROJANSKI KONJI

Trojanski konji so računalniški programi, ki ustvarjajo vtis uporabne programske opreme, vendar v resnici lahko močno ogrozijo računalnik in povzročijo precej škode. Trojanski konji se začnejo širiti, ko uporabniki odprejo program, za katerega verjamejo, da prihaja iz pristnega vira (uporaba t. i. socialnega inženiringa). Trojanski konji se lahko skrivajo v programski opremi, ki je prenesena brezplačno. Zato naj se uporabnik poskuša izogniti nalaganju programske opreme iz vira, ki mu ne zaupa, posodobitve in popravke programske opreme pa vedno prenaša le z uradnega spletnega mesta proizvajalca. (SI-CERT, 2016)

2.5 VIRUSI IN ČRVI

Računalniški virusi so programi, ki imajo sposobnost, da se sami širijo preko drugih programov ali dokumentov na računalniku. Računalniški program je v tem primeru gostitelj virusa. Širjenje računalniškega virusa zelo spominja na biološki virus, ki pa se širi tako, da okuži celice. Od tod prihaja izraz okužba računalnika z virusom. Pogosto se zgodi, da se med viruse šteje tudi druge zlonamerne programe, kot so npr. trojanski konji in črvi. Uporabnike takšne pomote zmedejo, kar pa pripelje do varovanja računalnika le pred določenimi tipi zlonamernih programov**,** žal pa so zato bolj dovzetni za ostale vrste zlonamernih programov. K sreči je večina virusov le nadležnih, čeprav so ustvarjeni z namenom uničevanja podatkov. Nekateri so narejeni tako, da se sprožijo šele po tem, ko mine določen čas od prvotne okužbe računalnika ali pa ko se okuži zadostno število drugih računalnikov. Večina virusov je kljub temu usmerjena v lastno nekontrolirano

reprodukcijo, kar troši računalniška sredstva, kot so procesorska moč, pomnilnik ali količina trdega diska.

Z virusi se bojujemo s pomočjo protivirusnih programov, požarnimi zidovi in pravočasnimi popravki programja. Danes ti programi niso več namenjeni samo boju proti virusom, ampak služijo tudi preprečevanju prisotnosti vohunskega programja.

Črv je prav tako kot virus zasnovan z namenom širjenja v druge računalnike, vendar to naredi samodejno, tako da prevzame nadzor nad računalniškimi funkcijami za prenos datotek in podatkov. Ko se črv naseli v vašem sistemu, lahko potuje sam. Nevaren je prav zaradi izjemne sposobnosti hitrega širjenja: svoje kopije lahko na primer pošlje na vse naslove, ki jih ima uporabnik v adresarju, računalniki naslovnikov pa bi naredili enako, kar povzroči učinek domin. Velik omrežni promet, ki je posledica širjenja črva, lahko upočasni poslovna omrežja in celo internet kot celoto. Ko se pojavijo novi črvi, se razširijo zelo hitro in zasitijo omrežja, zato je treba včasih do dvakrat dlje čakati na ogled posameznih spletnih strani. (FRI, 2016)

2.6 SMISHING, VISHING IN SPOOFING

Smishing je pojav, ko je žrtev na sporno spletno stran zvabljena s pomočjo poziva v obliki SMS sporočila. V pozivu prejemnika obvestijo, da se je včlanil v plačljiv klub, v izogib stroškom pa se lahko odjavi z vstopom na spletno stran**,** katere povezava je bila napisana v sporočilu.

Vishing tehnika je tehnika, kjer hekerji za krajo osebnih podatkov žrtve izkoriščajo mobilne telefone. Da je vishing tehnika uspešna, je treba vzporedno uporabiti tudi spoofing tehniko. Preko spoofing tehnike heker žrtvi pošlje e-sporočilo, ki je identično pravim spletnim stranem. V e-sporočilu je žrtev pozvana, da pokliče na določeno in v sporočilu navedeno telefonsko številko, klic pa heker spremeni na avtomatski odzivnik, ki od žrtve zahteva osebne podatke. Obstaja tudi možnost, da v tej tehniki hekerji žrtev pokličejo sami na stacionarni ali mobilni telefon. (Perič, 2014, str. 84)

Spoofing je beseda, ki v varnosti omrežja pomeni prevara. Spoofing attack pa po slovensko pomeni napad s prevaro, v katerem se ena oseba oziroma program uspešno pretvarja za drugo. To naredi s poneverjanjem podatkov. Možna posledica uspešnega napada je, da oseba oz. program pridobi zaupne podatke na nelegalen način.

Med več zvrstmi spoofinga je najbolj pogost e-mail spoofing. To je nelegalna aktivnost uporabe tujih e-poštnih naslovov za pošiljanje sporočil. Gre za eno najlažjih metod spoofinga. Vsak ljubiteljski programer php-ja zna na primer ustvariti skripta, ki s strežnika pošlje e-sporočilo na poljuben naslov, pri čemer je pošiljatelj v vrstici »FROM« lahko kdorkoli. To lahko izkoriščajo spammerji. Ustvarijo lahko skripta, ki pošilja sporočila v tujem imenu. V praksi bo laik v svojem poštnem odjemalcu odprl sporočilo spammerja, misleč da ga je poslal nekdo drug. Množično pošiljanje e-pošte na tak način spammerje običajno postavi na črne liste poštnih strežnikov. (Presentia d.o.o., 2008)

2.7 NEŽELENA ELEKTRONSKA SPOROČILA (SPAM)

Spam oz. nezaželena elektronska pošta so vsa nezaželena elektronska sporočila, ki jih avtorji pošiljajo v e-poštne predale številnih uporabnikov v komercialne namene. Na internetu je mogoče najti na tisoče elektronskih naslovov, ki spletnim trgovcem predstavljajo možnost dodatnega oglaševanja, ki se mu ne morejo upreti. Majhni stroški pošiljanja elektronske pošte pa pošiljatelje nezaželenih sporočil spodbujajo k ustvarjanju vedno daljših seznamov prejemnikov tovrstnih sporočil. (Telekom, 2016)

2.8 ZASEBNOST NA DRUŽABNIH OMREŽJIH

Na družabnih omrežjih obstaja veliko nevarnosti, ki se jih ne zavedamo, zato se je pred njimi treba ustrezno zavarovati. Zelo pomembno je, da uporabniki ustrezno nastavijo nastavitve zasebnosti. Pri npr. Facebooku je zasebnost mogoče urejati v zavihkih nastavitve računa in nastavitve zasebnosti.

Nastavitve si lahko po želji nastavi vsak uporabnik sam. Treba si je vzeti le nekaj časa in se posvetiti opravilu, ki se na prvi pogled ne zdi pomembno. Velika večina uporabnikov primarno nastavljenih nastavitev zasebnosti sploh ne spremeni. Treba je vedeti, da se brez ustreznih nastavitev zasebnosti svoje osebne informacije podarja celemu svetu, ne samo svojim prijateljem. V naslednjih nekaj točkah bom predstavil nastavitve zasebnosti trenutno še vedno najbolj priljubljenega družbenega omrežja Facebook.

Na Facebooku uporabnik lahko ustvari skupino, katere člani so njegovi prijatelji (sošolci, znanci idr.). Vsaki tovrstni skupini lahko nastavi drugačne varnostne nastavitve. Nastavi lahko, kdo dostopa do slik, ki jih je objavil, lahko pa tudi nastavi, kdo lahko dostopa do njegovih osebnih podatkov. Obstaja še mnogo drugih varnostnih nastavitev na profilu družabnega omrežja. V nastavitvah zasebnosti je med drugim mogoče tudi urediti, kdo lahko vidi seznam prijateljev in kdo ne.

Na Facebooku posameznega uporabnika lahko na objavljenih slikah označi vsakdo. Tudi za to obstajajo varnostni ukrepi. V orodni vrstici na zgornjem delu posamezne slike je mogoče ostalim uporabnikom onemogočiti označevanje posameznikovih objavljenih slik na Facebook profilu. Na Facebooku so najbolj priljubljene slike, ki jih uporabniki objavljajo. Dostop do njih ima vsak, kdor ima dostop do njihovega Facebook profila. Če uporabnik ne želi vsesplošnega vpogleda v objavljene slike na svojem Facebook profilu, lahko v nastavitvah albumov uredi, kdo bo do njih lahko dostopal in kdo ne.

Če uporabnik ne želi, da bi bili njegovi kontaktni podatki na Facebooku vidni vsem, to lahko prepreči z ureditvijo le-teh. V zavihku s kontaktnimi podatki na posameznem uporabniškem profilu je mogoče s klikom na ukaz »uredi« urejati posamezen podatek. Uporabnik lahko za vsakega posebej regulira, komu od ostalih uporabnikov socialnega omrežja bo viden in komu ne. Ostalim lahko onemogoči vpogled v kontakte, ki so mu blizu (npr. elektronska pošta).

Če se zgodbe o uporabniku pojavljajo v novicah (News feed) njegovih prijateljev, lahko pri določenih objavah včasih pride tudi do neprijetnih situacij. Eno takih predstavlja sprememba stanja razmerja oz. stanu, ko po propadu zveze uporabnik objavi, da je (zopet) samski. Objavo pa vidijo vsi v svojih novicah. Temu se je mogoče izogniti tako, da se v nastavitvah zasebnosti klikne na »novice in zid« (news feed and wall privacy page), kjer se odstrani kljukico pri dejavnosti »change relationship status«.

Pri objavi zgodb iz aplikacij so stvari bolj zapletene, saj uporabnik sam namešča aplikacije na svoj profil. Aplikacije pa imajo vse pravice, da same objavljajo komentarje v uporabnikovem imenu. To tudi potrdi s klikom ob nameščanju posamezne aplikacije. Edina rešitev pri tem je previdnost pri dodajanju aplikacij na posamezen profil.

Iz Facebookovih rezultatov iskanj se uporabnik lahko odstrani tako, da pri nastavljanju zasebnosti izbere možnost »iskane« (Search Privacy Settings Page) in pri nastavljanju vidnosti izbere ukaz »samo prijatelji« ter shrani spremembe. Po ureditvi uporabnika v iskalniku razen prijateljev ne more najti nihče drug. Ta način uporabniku onemogoča, da bi ga ostali dodajali kot prijatelje, zato mora morebitne prijatelje poiskati sam in jih zaprositi za prijateljstvo.

V primeru da kdo od uporabnikovih prijateljev ali znancev na zid njegovega Facebook profila objavi vsebino, ki bi ga spravila v zadrego, se lahko temu izogne tako, da v nastavitvah zasebnosti določi, kdo lahko objavlja in kdo lahko vidi objave na njegovem zidu. Te objave lahko vidijo vsi prijatelji in znanci, ki jih ima shranjene v svojem Facebook profilu, zato se je treba prej pripraviti, da ne pride do nerodnih situacij. Vsak uporabnik spletnega socialnega omrežja Facebook, zlasti mladi, bi se moral zavedati posledic izpostavljanja svoje zasebnost na spletu. Samo poznavanje nevarnosti ni dovolj, treba je tudi poznati posledice in primerno ukrepati proti le-tem. (Murn, 2015)

2.9 PROTIPRAVNO OBJAVLJENI OSEBNI PODATKI NA SPLETNI STRANI

Da so osebni podatki objavljeni protipravno, morajo biti po Zakonu o varstvu osebnih podatkov (8. in 9. člen) izpolnjeni trije pogoji. Prvi je, da so predmet zlorabe varovani osebni podatki oz. vsi podatki, iz katerih je posameznik določljiv. Drugi je, da posameznik za objavo ni podal osebne privolitve ali da za to ne obstaja podlaga v zakonu. Zadnji pogoj pa je, da so osebni podatki del zbirke ali namenjeni vključitvi vanjo, npr. če bi upravljavec foruma na forumu objavljal osebne podatke.

Poleg zgoraj naštetih pogojev je pomembno tudi to, kako je uporabnik pridobil osebne podatke. Če jih je pridobil z vdorom v računalniško zbirko podatkov, gre za kaznivo dejanje in v takšnem primeru lahko oseba, katere osebni podatki so bili zlorabljeni, poda prijavo na policijo ali državno tožilstvo. Če pa je uporabnik pridobil osebne podatke od upravljavca foruma, se v takem primeru poda prijavo informacijskemu pooblaščencu.

Za umik sporne objave je najbolje, da se uporabnik foruma obrne na upravljavca foruma. Kot izhaja iz določb Zakona o elektronskem poslovanju na trgu upravljavec foruma ne odgovarja za objavljene vsebine, če zanje ne ve. Vendar pa mora po opozorilu na

protipravno vsebino le-to umakniti, v nasprotnem primeru pa lahko odgovarja za posledice objave, saj se ne more izgovarjati, da za sporno objavo ni vedel.

Če se upravljavec foruma na poziv za umik vsebine ne odzove oz. ga zavrne, pa se lahko uporabnik foruma obrne na gostitelja spletne strani. Gostitelj strani, tako kot upravljavec foruma, sicer ni odgovoren za vsebino na spletni strani, ki jo gosti. Vendar pa se po opozorilu na protipravno vsebino ne more več šteti, da ni vedel za sporno vsebino. Zato lahko gostitelj, ki sporne vsebine na zahtevo ne umakne, odgovarja za posledice objave.

Če uporabnik še vedno ni dosegel umika sporne vsebine, lahko od sodišča zahteva, da upravljavcu foruma naloži ustavitev ali preprečitev kršitve ter odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih. Uporabnik foruma poda tudi zahtevo za prenehanje s kršitvami osebnostnih pravic. Sodišče lahko odredi prenehanje dejanja, preprečitev takšnega dejanja oz. odstranitev njegovih posledic.

Ko je z ravnanjem druge osebe prišlo do občutnega posega v zasebnost uporabnika foruma in mu je s tem nastala škoda, lahko uporabnik foruma vloži odškodninsko tožbo pred pristojnim sodiščem in zahteva odškodnino. (Havliček, 2012)

V primerih, ko uporabnik predvideva, da sodišče ni odločilo v korist uporabnika, čeprav so vsi dokazi kazali njemu v prid, pa se lahko obrne tudi na Informacijskega pooblaščenca, ki lahko izvršuje inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov. Poleg tega ima Informacijski pooblaščenec tudi pristojnosti, da odloča o pritožbi zoper odločbo, s katero je organ zavrnil ali zavrgel zahtevo ali kako drugače kršil pravico do dostopa ali ponovne uporabe informacij javnega značaja. V drugi stopnji postopka je pristojen tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja in na njegovi podlagi izdanih predpisov. Informacijski pooblaščenec lahko odloča tudi o pritožbi posameznika, takrat ko upravljavec osebnih podatkov ne ugodi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki. Informacijski pooblaščenec je kot prekrškovni organ pristojen tudi za nadzor nad izvajanjem Zakona o Informacijskem pooblaščencu, Zakona o dostopu do informacij javnega značaja v okviru pritožbenega postopka in Zakona o varstvu osebnih podatkov. (ZInfP, 2. čl. in ZDIJZ, 32. čl.)

2.9.1 KAKO SE IZOGNITI ZLORABI OSEBNIH PODATKOV

Da bi se zmanjšala možnost zlorabe osebnih podatkov, naj pri registraciji uporabnik vpiše le podatke, ki so resnično potrebni. Pri izbiri gesla naj bo pazljiv in naj upošteva varnostne nasvete ter geslo redno menja. Pri uporabi foruma naj uporablja vzdevek, iz katerega ni razvidno, kdo je uporabnik foruma. Na forumu naj neznancem ne sporoča osebnih podatkov in ne pošilja svojih fotografij. Pomembno je tudi, da se zaveda, da se na forumu še vedno pogovarja z ljudmi in ne z računalniki. Uporabnik foruma naj bi spoštoval pravila obnašanja in naj se ne zanaša na svojo anonimnost. (Havliček, 2012)

3 KRAJA IDENTITETE

Kraja identitete je kaznivo dejanje, kjer se storilci izdajajo za drugo osebo, običajno zaradi finančnih goljufij. V današnji družbi mora posameznik velikokrat posredovati delčke informacij o sebi, kot so davčna številka, EMŠO, podpis, ime, naslov, telefonske številke in celo bančne podatke o kreditni kartici. Če ima storilec dostop do vseh teh osebnih podatkov, lahko v imenu žrtve izvede finančne transakcije, najame posojilo, nakupi blago za večjo količino denarja, vzame hipoteko na žrtvino hišo itd.

Kraja identitete pomeni posebno vrsto hudega posega v varstvo osebnih podatkov. Kraja identitete se ne nanaša le na premoženjski vidik, ampak posega v osebnost žrtve. Zabeleženi so tudi primeri, ko je bila posameznikom odvzeta prostost zaradi suma storitve kaznivega dejanja.

S pomočjo različnih načinov pridobitve osebnih podatkov se lahko storilec začne izdajati za nekoga drugega in v njegovem imenu vstopa v različna pravna razmerja. Kraja identitete ni samo zloraba določenega osebnega podatka, ampak je povezana z namenom, da storilec pridobi določeno korist. Prizadete so lahko tudi osebnostne pravice, predvsem pravica do osebnega dostojanstva. Žrtve kraje identitete večkrat trpijo zaradi izgube dobrega imena, ugleda, časti, doživljajo stalne čustvene pretrese, ker je kraja določenih osebnih podatkov nepopravljiva.

Goljufija na podlagi spletne kraje identitete je problem in zaradi tega veliko ljudi okleva pri prijavi na spletne strani, ki za druge predstavljajo vsakodnevne aktivnosti (npr. nakupovanje preko e-trgovin, uporaba spletnih strani za dražbe ali uporaba spletnega bančništva). Spletna kraja identitete je danes vsekakor aktualna tema, vendar pa predstavlja le majhen odstotek vseh goljufij s pomočjo kraje identitete. (Havliček, Kraja identitete na spletu, 2012)

3.1 KAKO SE ZAŠČITITI PRED KRAJO IDENTITETE

Prvi korak v boju proti kraji identitete je, da se zmanjša tveganje tako, da posameznik zaščiti svoje osebne podatke. Posameznik naj se pozanima, za kakšen namen spletna podjetja uporabljajo osebne podatke in kako jih hranijo. Pri spletnih transakcijah naj si posameznik vzame čas za pregled politike zasebnosti, ki jo ima neka spletna stran. Posameznik naj se prepriča, da spletna stran ponuja varno podatkovno šifriranje in druge storitve za zaščito osebnih podatkov.

Priporočljive vsakdanje prakse so spremljanje pravočasnosti računov in bančnih izpiskov, ki prihajajo preko navadne pošte, ustrezno uničenje papirnih dokumentov, ki lahko vsebujejo številke kreditnih kartic in druge identifikacijske osebne podatke. Posameznik naj ne posreduje informacij preko telefona ali elektronske pošte, še posebej, če ga je sogovornik kontaktiral sam. Davčno številko in EMŠO naj zaupa le takrat, ko je res nujno potrebno. Posameznik naj bo pozoren pri podpisovanju dokumentov. Na praznih predelih dokumentov, ki jih podpisuje, naj potegne črto in nikoli ne podpisuje praznih strani. Če

posameznika dlje časa ni doma, naj se dogovori s sosedom ali prijateljem, da mu prazni poštni nabiralnik.

Posameznik naj bo zelo pozoren pri kopijah osebnih dokumentov. Z namenom zaščite osebnih podatkov in s tem preventivnega delovanja proti kraji identitete sta sprejeta dva zakona, ki med drugim urejata tudi kopiranje osebnih dokumentov: Zakon o osebni izkaznici in Zakon o potnih listinah. Kopiranje osebnih dokumentov je možno samo v primerih, ki jih določa zakon. Ni torej dovolj, da je kopiranje predpisano v notranjih pravilih upravljavca. Zakon določa, da lahko osebne dokumente poleg imetnika kopirajo notarji in finančne družbe, ki opravljajo finančne storitve, če jo potrebujejo za dokazovanje identitete državljana v konkretnem postopku. Kopiranje osebnih dokumentov je dovoljeno še na podlagi pisne privolitve posameznika. Upravljavec osebnih podatkov je na podlagi vloge imetnika osebnega dokumenta dolžan izdati potrdilo o kopiji.

Za prijavo kraje identitete sta pristojna tožilstvo in policija. Storilcu grozi kazen do treh let zapora. V primeru finančnega oškodovanja, če se to dokaže v kazenskem postopku, lahko žrtev zahteva odškodnino. Sicer je povračilo škode izpraznjenega računa odvisno od pogodbe, ki jo je posameznik podpisal pri svoji banki. (Havliček, Kraja identitete na spletu, 2012)

3.2 NAJRANLJIVEJŠE TOČKE ZA KRAJO IDENTITETE

Kraja identitete se lahko zgodi kadarkoli in kjerkoli, zato se je dobro zavedati, kako ranljivi smo ljudje. Med najpogosteje ukradenimi stvarmi je najti denarnico, v kateri se lahko najde ogromno osebnih podatkov, ki se jih da zlorabiti. Za tatove so najbolj privlačni osebni dokumenti, kot sta npr. potni list in vozniško dovoljenje. Tat identitete lahko posameznikove osebne dokumente uporabi za svojo identifikacijo ali pa jih uporabi kot vir za pridobivanje še več informacij in podatkov o žrtvi. Da bi se takšnim nevšečnostim izognilo, je priporočljivo dokumente in kartice, ki se jih ne potrebuje, odstraniti iz denarnice in jih shraniti na varno. V primeru kraje je treba v čim krajšem času poklicati policijo, poleg tega pa je treba s krajo seznaniti tudi banko, če je med odtujenimi dokumenti tudi bančna kartica.

Poleg denarnice je tatovom zelo lahko dosegljiv poštni nabiralnik. Po pošti se pošilja veliko osebnih podatkov, vključno z bančnimi in kreditnimi karticami, osebnimi dokumenti, obrazci ter drugimi dokumenti. Temu se včasih ni mogoče izogniti, vendar pa je možno veliko storiti za zmanjšanje možnosti, da bodo tako poslani podatki zlorabljeni. Posameznik naj spremlja, katere dokumente pričakuje po pošti. Če ugotovi, da pričakovanih dokumentov ni prejel ali da so bili poslani na napačen naslov, naj o tem takoj obvesti pošto. Precej pomembna zadeva je tudi redno praznjenje in zaklepanje poštnega nabiralnika.

Pravi zaklad za tatove identitet so tudi koši za smeti. Največja napaka je, da se dokumente, ki niso več uporabni, odvrže v smeti. S tem se omogoči tatovom, da z navidez nepomembnimi dokumenti ukradejo posameznikovo identiteto. Dokumenti namreč lahko vsebujejo veliko podatkov, s pomočjo katerih se lahko nepridipravi začnejo izdajati za

žrtev. Tat identitete lahko na primer pridobi kontakte posameznikovih prijateljev, s katerimi stopi v stik in se pred njimi izdaja za svojo žrtev. Poleg tega lahko odvrženi dokumenti vsebujejo tudi takšne podatke, s katerimi lahko tat identitete ustvari osebni profil žrtve. Preden se v smeti odvrže dokumente z osebnimi podatki (kreditne in bančne kartice, plačilne liste in bančni izpiski, pretečeno vozniško in prometno dovoljenje, ipd.), jih je treba uničiti.

Na svojem računalniku ima vsak posameznik shranjenih mnogo osebnih dokumentov, fotografij in glasbo, s pomočjo katerih lahko nekdo hitro ugotovi, za koga gre in kakšni so njegovi interesi. Poleg tega se računalnik uporablja tudi za brskanje po internetu, kjer je posameznik še posebej izpostavljen kraji identitete. Zato je zelo pomembno, da svoj računalnik zaščiti pred vdori vsiljivcev in jim tako onemogoči dostop do osebnih podatkov. Na računalnik je treba za boljšo obrambo pred vdori namestiti požarni zid ter zaščitno programsko opremo, ki se bo avtomatsko posodabljala, poleg tega pa je priporočljivo namestiti tudi licenčno protivirusno programsko opremo. Preden posameznik sprejme posodobitve programov, ki jih že ima nameščene na računalniku (npr. Word, Flash itd.), naj se prepriča, da obvestila o posodobitvi prihajajo s strani pooblaščenega podjetja. V primeru prodaje, oddaje ali zavrženja računalnika naj z njega izbriše vse svoje osebne podatke in osebne dokumente. Zgolj pritisk na gumb »izbriši/delete« ni dovolj. Po potrebi naj trdi disk fizično uniči in se prepriča, da z uničenega računalnika ni mogoče dobiti nobenih osebnih podatkov.

Poleg računalnikov lahko omenim tudi mobilne telefone. Najnovejši mobilni telefoni so pravzaprav majhni računalniki, ki opravljajo vedno več funkcij. Vsebovali bodo vedno več informacij o posameznikovih zasebnih in službenih aktivnostih. Tako je mobilni telefon postal zelo koristen pripomoček za tatove identitete. Če mobilni telefon ni ustrezno zavarovan, lahko do osebnih podatkov in drugih informacij dostopa kdorkoli, ki z njim razpolaga, zato je priporočljivo uporabiti dodatna gesla in po možnosti še kodiranje telefona, ki bo precej otežilo nepooblaščen dostop do podatkov. Najbolj varno pa je, da se na mobilni telefon ne shranjuje občutljivih informacij. Predvsem se je pametno izogniti shranjevanju informacij o spletnem bančnem poslovanju, stanju na svojem bančnem računu, o številki kreditne kartice, službenih in zasebnih spletnih sporočilih, geslih in PIN številkah. Poleg tega je treba redno preverjati račune. Prepričati se je treba, da ni nikakršnih še tako majhnih nepravilnosti. Tatovi identitete pogosto začnejo z majhnimi zneski in tako preverijo, ali bo žrtev razliko opazila. Če posameznik meni, da je na računu odkril nepravilnosti, naj zadevo takoj razišče. V primeru kraje ali izgube mobilnega telefona pa naj takoj kontaktira svojega mobilnega operaterja in blokira svoj račun.

Spletno nakupovanje je lahko zelo uporabno in učinkovito, vendar so z njim povezana tudi večja tveganja. Posameznik naj ne uporablja spletnih strani, če ni prepričan, da so vredne zaupanja. Na svetovnem spletu naj preveri, ali gre za izvajanje zakonitega poslovanja. Da vsiljivci ne bi spremljali spletnih transakcij, je treba biti pazljiv, saj niso vse spletne strani tisto, za kar se predstavljajo. Kadar posameznik plačuje preko spleta, naj se prepriča, da je ta del spletne strani zavarovan (spletni naslov se začne z »https«) in da je v vrstici s spletnim naslovom prikazana zaklenjena ključavnica. Ko nakupuje preko spleta, naj vedno

zahteva potrdilo ali račun o opravljeni transakciji. Vsaka zakonita spletna trgovina bo takšno potrdilo priskrbela. Preden prvič nakupuje preko nepoznane spletne trgovine, naj uporabnik testira povezavo, pokliče telefonsko številko za pomoč strankam in se tako prepriča, da trgovina dejansko obstaja (preko storitve za uporabnike naj se postavijo preprosta vprašanja glede njihovega poslovanja). Po končani operaciji naj se uporabnik ne pozabi odjaviti iz spletnih bančnih poslovalnic in drugih javnih portalov. Tako se prepreči hekerjem, da pridobijo informacije o posamezniku. Nikoli naj se ne posreduje gesel in uporabniških imen preko telefona ali spletne pošte ter nikoli ne odgovarja in ne klika na povezave v spletni pošti, ki zahtevajo navedbo osebnih podatkov. Verjetno gre za nepridiprave, ki skušajo pridobiti osebne podatke.

Varnostne kode, PIN številke in gesla naj se obravnava na enak način kot fizične ključe, naj se jih varuje. Enako velja tudi za podatke, ki se jih uporablja za prijavo na razne spletne strani. Če nekdo pridobi gesla, se lahko zlahka izdaja za svojo žrtev. Prav tako lahko spremeni ali ustvari uporabniške račune in se vključuje v družabna omrežja v žrtvinem imenu. Če tat identitete pridobi geslo za vstop v spletno družabno socialno omrežje, s tem dobi tudi dostop do kontaktov. Zato je treba uporabljati gesla, ki se jih je mogoče zlahka zapomniti, vendar pa jih je hkrati težko uganiti. Če je le možno, se je pri izbiri gesel pametno izogibati imenom družinskih članov, hišnih ljubljenčkov ipd., poleg tega pa je priporočljivo, da se ne uporablja istih gesel za različne storitve in račune.

Zavedati se je treba, da so gesla in kode le eden izmed mnogih načinov za pridobitev osebnih podatkov. Za tatove identitet so zelo uporabni podatki tudi EMŠO, davčna številka in številka zdravstvene kartice, ki pa so s strani države definirani kot odobreni, trajni in enoznačni identifikatorji. Te številke posameznika spremljajo od rojstva do smrti; veliko informacij o njem je povezanih s temi identifikatorji. Za potrebe avtentikacije se uporabljajo v mnogih situacijah in prav zato so koristen pripomoček za tatove identitete. Ti lahko npr. z uporabo posameznikovega identifikatorja zbirajo informacije o njem iz različnih virov. Tat identitete lahko v njegovem imenu vzame na banki kredit ali pridobi druge koristi.

Zato je treba biti pri posredovanju enoznačnih identifikatorjev še posebej previden. Vedno se velja vprašati, ali je posredovanje res potrebno oziroma nujno. Če posameznik v to ni prepričan, naj se vedno pozanima, zakaj mora te podatke posredovati. Javni organi, delodajalec in finančne institucije velikokrat te osebne podatke v resnici potrebujejo, vendar bodo v vseh primerih tudi vedno pojasnili zakaj. Posebej pomembno je, da se EMŠA, davčne številke ali številke zdravstvene kartice nikoli ne pošilja po nezavarovani liniji ali po faksu. Če jo je že treba poslati, naj se uporabi kodiran zapis. V primeru da posameznik najde svoje enoznačne identifikatorje na listinah, za katere se mu zdi, da zanje niso potrebni, naj nemudoma ukrepa. Pri poslovanju velja izbirati tiste partnerje, ki ne uporabljajo enoznačnih identifikatorjev kot sredstva za identifikacijo ali kot pogoja za uporabo njihovih storitev.

Debetne in kreditne kartice se uporabljajo vsakodnevno, vendar je treba paziti, kdo vse lahko dostopa do podatkov s kartice. Nikoli naj se ne posreduje podatkov s kreditne

kartice po telefonu ali preko spleta, če posameznik ni popolnoma prepričani s kom komunicira. Tatovi identitete so še posebej zainteresirani za številko kreditne kartice, za datum poteka veljavnosti ter za dodatno varnostno kodo (CVC koda) na hrbtni strani kartice. Posameznik naj bo pozoren, kje in komu posreduje podatke s svoje kreditne kartice in naj je nikoli ne spusti s pogleda. Ker gre pri kreditnih karticah za večje vsote denarja, ki so naložene na račun, je treba poskrbeti, da informacije o karticah ne zaidejo v napačne roke. Podatke naj posameznik razkrije le, če je bil on tisti, ki je sprožil kontakt. Tatovi ga lahko kontaktirajo pod pretvezo, da so uslužbenci njemu znanega podjetja ali njegove banke. Mora pa biti pozorni tudi na datum poteka veljavnosti svoje kartice. V primeru da v nekem razumnem času pred potekom veljavnosti od banke ne dobi nove kartice, naj le-to takoj pokliče, saj obstaja možnost, da je tat iz nabiralnika ukradel novo kartico. (Informacijski pooblaščenec, 2015)

3.2.1 RAZKRIVANJE OSEBNIH PODATKOV

Za tatove identitete predstavlja telefon zelo uporabno orodje. Če posameznik ni pazljiv, lahko od njega in iz njegovih kontaktov zberejo veliko informacij, ki jih nato lahko uporabijo proti njemu. Zaupanja vredna podjetja ne kličejo in od ljudi ne zahtevajo tajnih podatkov po telefonu.

Veliko informacij o sebi dajejo na splet tudi uporabniki sami, še posebej na svoje profile na raznih spletnih družabnih omrežjih (npr. Facebook). Hekerji in tatovi identitete lahko vdrejo v uporabniški račun. Z ribarjenjem podatkov (phishing) lahko nepridiprav ukane in uporabnika prepriča, da mu razkrije svoja gesla, s katerimi dostopa do svojih računov, informacij ali aplikacij. Podatke lahko z računalnika zbirajo in posredujejo naprej tudi virusi in druge škodljive kode. Da ne bi prišlo do nepričakovanega razkritja osebnih podatkov, velja upoštevati naslednje nasvete:

- Posameznik naj nikoli ne razkriva svojih gesel za vstop v uporabniške račune po telefonu, e-mailu ali prek drugih osebnih kontaktov.
- Če posameznik prejme ponudbo, ki izgleda predobro, da bi bila resnična, potem verjetno tudi res je zavajajoča. Posameznik naj nikoli ne dovoli, da mu razne nagrade zameglijo razum – ne pusti naj se premamiti in tako razkriti svojih osebnih podatkov nekemu popolnoma neznanemu podjetju ali posamezniku.
- Na spletnih družabnih omrežjih (npr. Facebook) naj posameznik nikoli ne objavlja tistih podatkov, za katere ne želi, da bi jih videli tudi njegovi bodoči delodajalci, družina, partner ali izobraževalna ustanova. Če želi na spletu objaviti fotografijo nekoga drugega, ga mora prej vprašati za dovoljenje.
- Posameznik naj prebere varnostne nastavitve (nastavitve zasebnosti) na spletnih družabnih omrežjih in z njihovo uporabo nadzoruje, kdo lahko vidi njegove podatke.
- Pogosto naj menjuje svoja gesla in uporablja različna gesla za dostop do različnih storitev.
- Posameznik naj se nikoli ne odziva na elektronska sporočila, ki od njega zahtevajo določene osebne podatke, in nikoli ne odpira spletnih povezav, ki ga sprašujejo po

osebnih podatkih. Možno je, da je na drugi strani nepridiprav, ki želi od njega dobiti določene podatke. (Informacijski pooblaščenec, 2015)

3.2.2 PREVERJANJE KREDITNE SPOSOBNOSTI

V sodobni družbi podjetja in organizacije vedno pogosteje preverjajo kreditne sposobnosti. Če je posameznik na primer zaprosil za posojilo, bo podjetje najverjetneje predhodno preverilo, ali je kreditno sposoben. Preverjanje kreditne sposobnosti je pomembna metoda za odkrivanje kraje identitete. Če posameznik ugotovi, da je nekdo brez njegove vednosti preverjal njegovo kreditno sposobnost, naj se takoj pozanima, kdo je to bil in s kakšnim namenom je to naredil.

Če ugotovi, da je nekdo nepredvideno preverjal njegovo kreditno sposobnost, naj posameznik prosi kreditodajalca oz. svojo banko, da mu posreduje potrebne izpiske (Kdo je zaprosil za preverjanje in zakaj? Katere podatke je pridobil?). Kontaktira naj podjetje, ki naj bi zaprosilo za preverjanje. Če sumi, da bi utegnil biti žrtev kraje identitete, naj o tem takoj obvesti kreditodajalca. Posameznik naj zaprosi za potrebno ukrepanje in za blokiranje vseh drugih, ki bi želeli preveriti njegovo kreditno sposobnost. Če je treba, naj se obrne tudi na Informacijskega pooblaščenca ali na policijo.

V primeru, da ugotovi, da je nekdo preverjal njegovo kreditno sposobnost in potem odprl nov račun, ki ga ne prepozna, naj posameznik takoj kontaktira (ustno in pisno) podjetje, pri katerem je bil račun odprt, razloži, da račun ni njegov, in prosi za takojšnje zaprtje računa. (Informacijski pooblaščenec, 2015)

4 PRIMER KRAJE IDENTITETE

V svetu so vse pogostejše kraje identitete, in kljub temu da varnostni organi redno opozarjajo na nevarnosti, se zelo pogosto zgodi, da ljudje nasedejo prevarantom. Lahko se zgodi, da človek nasede pri določeni stvari, ki se na prvi pogled sploh ne zdi sumljiva.

Ravno to se je zgodilo mlademu dekletu, ki je želelo ostat anonimno, vendar je svojo zgodbo vseeno želelo deliti z ostalimi z namenom, da ne bi tudi oni nasedli takšnim prevaram. Začelo se je. ko je poskušalo najeti stanovanje v Luksemburgu prek spleta. Na eni od mnogih spletnih strani z oglasi je dekle našlo primerno garsonjero za začetek življenja v Luksemburgu, zato je takoj pisalo lastnici.

Lastnica je bila sprva zelo prijazna in tudi na elektronsko pošto je redno in hitro odgovarjala. Sporočila je, da za najem in pogodbo potrebuje kopijo potnega lista najemnika. Dekle je že prej pozanimalo in izvedelo, da to ni neobičajna praksa in je zato tudi ugodilo njeni prošnji ter skeniralo potni list ter ga poslalo lastnici. Ko je dobilo pogodbo, je lastnica garsonjere še prosila, ali dekle lahko nakaže varščino za stanovanje, kar je seveda tudi storilo.

Nekaj tednov kasneje, pa je lastnica garsonjere potencialni najemnici sporočila, da mora nujno oditi v London obiskat mamo. Sporočila ji je tudi, da se bo v Luksemburg vrnila pravočasno, vendar ji je najemodajalka nekaj dni kasneje poslala še eno sporočilo, v katerem je prosila, ali ji lahko posodi nekaj denarja za letalsko karto, saj je ves denar porabila za zdravila za bolno mamo in se sedaj ne more pravočasno vrniti nazaj v Luksemburg, da bi ji predala ključe garsonjere, kar pa je dekle seveda zavrnilo.

S to zavrnitvijo pa so seveda začele težave. Gospa je po zavrnitvi postala zelo nesramna in žaljiva, zato je dekle urednikom spletne strani z oglasi to gospo prijavilo. Potem ko se je dekle te gospe rešilo, je po prebiranju foruma ugotovilo, da je postalo žrtev prevare, vendar je mislilo, da se je vsega tega rešilo. Nekaj časa po preselitvi v Luksemburg pa so se ponovno začele težave; oseba je postala žrtev kraje identitete. Začela je dobivati številna sporočila, s katerimi so nadlegovali njo in tudi njenega očeta. V nekaterih sporočilih so ji posredovali tudi zneske, ki naj bi jih bila dolžna vrniti; vrteli so se tudi do 100.000 evrov in več. Čeprav je pošiljavcem sporočil sporočila, da z njihovo izgubo denarja nima nič in da nima denarja, so bile grožnje vsak dan hujše. Po preteku nekaj časa je sprevidela, da bo najboljša rešitev, da se obrne na policijo. S tem se je zadeva tudi umirila, saj je policija stopila v stik z ostalimi žrtvami, tako da so se grožnje končale. Če pa je slučajno še prišla kakšna grožnja do nje, je vse skupaj predala policiji, da so zadevo rešili.

Osebo, ki je ukradla identiteto temu dekletu, so izsledili v Švici, tiralico za njo pa je izdala tudi nemška policija. Potem ko so to osebo ujeli, so ugotovili, da je bila vpletena v ogromno prevar s prodajo in najemi nepremičnin. Zadeva se je za omenjeno dekle na koncu vendarle srečno končala. (Jurinčič, 2013)

5 VAROVANJE INFORMACIJ

Varnost informacij je pomembna tema, s katero se morajo ukvarjati upravni odbori podjetij. Dandanes se podjetja pri poslovanju zanašajo na notranje računalniške sisteme in internet. Ne morejo si privoščiti prekinitve poslovanja. Varnostni incident ima lahko širše negativne posledice na dohodke podjetja, zaupanje strank in stike z javnostjo. Zaradi teh posledic je varnost informacij pomemben sestavni del učinkovite poslovne strategije. Program za varovanje informacij naj bo zato ena glavnih prioritet poslovanja v podjetju. (Egan in Mather, 2005 str. 2.)

Organizacije morajo doseči raven zaščite, ki jim omogoča racionalno uporabo informacijskih in drugih sredstev ter onemogoča morebitne varnostne incidente, povezane z varovanjem informacij. Dogodki 11. septembra 2001, vdori v strogo varovane računalniške sisteme, računalniški virusi, kraje patentov in druge intelektualne lastnine so razlogi, ki opravičujejo povečane napore ter investicije v varnost in zagotavljanje nemotenega poslovanja. (Berčič, in drugi, 2003, str. 18)

Cvetko (1999, str. 148) pravi, da je občutljivost osebnih podatkov različna. Po občutljivosti ločimo zelo občutljive, občutljive in manj občutljive podatke. Glede na ankete, ki so bile narejene tako pri nas kot tudi v tujini, je ugotovil, da se delitev osebnih podatkov v posamezne kategorije bistveno ne razlikuje. Med zelo občutljive podatke se lahko šteje podatke o finančnem stanju (računi, posojila, premoženjsko stanje), med občutljive podatke spadajo podatki o posameznikovih interesnih dejavnostih pa tudi evidence, ki vsebujejo podatke o zdravstveni dokumentaciji, socialnih registrih in podobno. Med manj občutljive podatke pa se šteje podatke o članstvu v raznih organizacijah in društvih ter podatke, ki jih vsebujejo različni registri, kot so npr. davčni ali zemljiškoknjižni registri, pokojninsko in invalidsko zavarovanje. Glede na razvrstitev po občutljivosti je pomembno urediti tudi varstvo, kajti zloraba pri zelo občutljivih podatkih lahko povzroči povsem drugačen odziv kot zloraba manj občutljivih podatkov.

Pri varovanju informacij ima posebno vlogo tudi Informacijski pooblaščenec, in sicer ima pregled nad obdelavo osebnih podatkov, kot jo ureja Zakon o varstvu osebnih podatkov ter preprečuje in odpravlja kršitve tega zakona.

»Zakon o varstvu osebnih podatkov načelno določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Določa tudi, da je na ozemlju Republike Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotovljeno varstvo osebnih podatkov. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo.« (Informacijski pooblaščenec, 2016)

Obdelovanje osebnih podatkov je možno le, če je njihova obdelava določena z zakonom ali pa v primeru, ko ima upravljavec zbirke podatkov pisno privolitev posameznika. Za pravne in fizične osebe, ki opravljajo javno službo ali dejavnost po zakonu, ki ureja

gospodarske družbe, pa velja, da lahko neposredno na podlagi tega zakona, obdelujejo osebne podatke oseb, s katerimi so v pogodbenem razmerju, vendar le, če gre za osebne podatke oseb, s katerimi so v pogodbenem razmerju, vendar le v primeru, če gre za osebne podatke, ki se jih potrebuje za izpolnjevanje pogodbenih obveznosti ali uveljavljanje pravic pogodbenega razmerja. Za nosilce javnih pooblastil in državne organe ter organe lokalnih skupnosti je določilo malce drugačno, ker ti lahko obdelujejo le tiste osebne podatke, ki jih določa zakon.

Pri varovanju informacij ima pomembno vlogo tudi inšpekcijski nadzor, ki skrbi za odpravljanje nepravilnosti, zato je preventivno ukrepanje pomembno tudi z vidika nadzora. Če pri opravljanju inšpekcijskega nadzora nadzornik ugotovi kršitev Zakona o varstvu osebnih podatkov ali drugega zakona ali kakšnega drugega predpisa, ki ureja varstvo osebnih podatkov, ima pravico, da odredi odpravitev pomanjkljivosti ali nepravilnosti v načinu in roku, ki ga določi nadzornik sam. Poleg tega lahko izda osebam zasebnega ali javnega sektorja prepoved obdelave osebnih podatkov, če niso zagotavljale ali niso izvajale ukrepov in postopkov za zavarovanje osebnih podatkov. Če nadzornik ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami zakona, lahko odredi prepoved obdelave osebnih podatkov ter anonimiziranje, blokiranje ali uničenje osebnih podatkov. Poleg tega ima nadzornik možnost tudi odrediti prepoved iznosa osebnih podatkov v druge države ali njihovega posredovanja tujim uporabnikom osebnih podatkov v primeru, če jih posredujejo v nasprotju z določbami zakona ali obvezujoče mednarodne pogodbe. Nadzornik pa lahko poleg vseh teh ukrepov odredi tudi druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek. (Informacijski pooblaščenec, 2016) Za prepoved zlorab in varstvo pravic posameznikov so zelo pomembni nadzorni mehanizmi, ki jih lahko uporabi posameznik, če misli, da se njegovi osebni podatki obdelujejo nezakonito. Pomembna pomanjkljivost obstoječega mehanizma v času po osamosvojitvi je bila odsotnost učinkovitih in neodvisnih nadzornih mehanizmov, kar pa se je v zadnjem času lepo uredilo. (Rovšek, 2005, str. 76)

5.1 POMEMBNE NEVARNOSTI PRI VAROVANJU INFORMACIJ

Podjetja se morajo zavedati šestih pomembnih nevarnosti in jih upoštevati:

- zahteve pri e-poslovanju;
- napadi na varovane informacije;
- nezrel trg varovanja informacij;
- pomanjkanje strokovno usposobljenega osebja za varovanje informacij;
- vladna zakonodaja in industrijski pravilniki;
- mobilna delovna sila in brezžična omrežja. (Egan in Mather, 2005, str. 6)

5.1.1 ELEKTRONSKO POSLOVANJE

Elektronsko poslovanje je pomembna pridobitev na poslovni ravni. To je podjetjem omogočilo nove načine ponujanja izdelkov in storitev svojim strankam. Zaradi novih načinov ponujanja izdelkov in storitev lahko sedaj z večjimi družbami tekmujejo tudi

manjša podjetja. Storitve e-poslovanja so zelo všeč predvsem potrošnikom, ki ne želijo porabiti svojega prostega časa za obiskovanje trgovin in se ukvarjati z dolgimi vrstami na blagajnah, ampak si rajši nakupijo stvari, ki jih potrebujejo, kar prek spletnih trgovin. Med prvimi na področju e-poslovanja sta bili podjetji eBay in Amazon. Nakup izdelkov na internetu sta popolnoma poenostavili, stranke lahko brez težav kupijo želeni izdelek. (Egan in Mather, 2005, str. 7)

Prednosti za uporabnike e-poslovanja (Saba, 2010):

- različne možnosti dostopa do storitev in informacij;
- storitve so prilagojene v večji meri;
- uporabniki so vključeni v oblikovanje storitev in njihove izboljšave;
- uporabniki so vključeni v proces odločanja;
- stroški so nižji;
- prihrani se čas za opravljanje storitev in pridobivanje informacij;
- storitve so na voljo tudi izven delovnega časa.

Prednosti za podjetja (Saba, 2010):

- kljub začetnim višjim investicijskim stroškom se dolgoročno posluje z nižjimi stroški;
- poslovanje je preglednejše;
- viri so bolje razporejeni;
- storitve za uporabnike so hitrejše;
- kakovost storitev je višja;
- manj je napak in podvajanja dela;
- elektronsko komuniciranje prinaša boljšo in modernejšo podobo podjetja pri poslovnih partnerjih in strankah;
- višja kakovost storitev oz. izdelka.

Slabost elektronskega poslovanja je predvsem v tem, da ni dovolj velikega deleža uporabnikov, ki bi imeli možnost uporabe informacijske tehnologije. Omejitve predstavljajo različni dejavniki:

- socialne potrebe (npr. osebni stik);
- kulturna vprašanja (npr. jezikovne ovire);
- ekonomski dejavniki (dostopnost informacijske tehnologije);
- dejavniki povezani z učenjem (npr. spoznavanje nove tehnologije, računalniška pismenost, spreminjanje navad, ipd.);
- fizični dejavniki (npr. telesne nezmožnosti, slepota);
- razvitost omrežja za zagotavljanje storitev informacijske tehnologije (Saba, 2010).

Druge slabosti, ki prav tako vplivajo na e-poslovanje:

- možnost zlorabe informacijske tehnologije;
- nezaupanje v novosti;
- neosebnost takšne oblike komuniciranja;

- napake in zamude, ki se pojavijo ob uvajanju novih tehnologij (Saba, 2010).

5.1.2 RAST IN ZAPLETENOST NAPADOV NA VAROVANE INFORMACIJE

Napadi na varovane informacije po svetu vsako leto povzročijo škodo v višini več milijard evrov. Ranljive točke so luknje in pomanjkljivosti v sistemih, ki jih hekerji lahko izkoristijo za napad na sistem. Lahko se zgodi, da npr. skrbnik sistema pozabi omejiti določene pravice na pooblaščene uporabnike. Drugi primeri pa vključujejo ranljivost zaradi napak v programski opremi, ki pa bi jih moral izdelovalec programske opreme zaznati že med postopkom preskušanja. (Egan in Mather, 2005, str. 10)

5.2 CILJI IN NAMEN UVAJANJA SISTEMA VAROVANJA INFORMACIJ

Cilji uvajanja sistema varovanja informacij so zaščita informacij pred:

- nepooblaščenim razkritjem ali očitnim prestrezanjem – načelo zaupnosti;
- neavtoriziranim spreminjanjem, varovanjem točnosti in celovitosti – načelo neoporečnosti;
- uničenjem in zlorabo ter zagotavljanjem dostopnosti informacij in storitev, ko se le-te potrebujejo – načelo razpoložljivosti (Berčič, in drugi, 2003, str. 22).

Cilji, ki jim mora slediti organizacija pri uvajanju sistema varovanja informacij, so:

- zagotavljanje dolgoročnega poslovanja organizacije;
- poslovanje skladno z zakonodajo, predpisi in standardi;
- uspešno in učinkovito poslovanje;
- obvladovanje in minimiziranje tveganj poslovanja (Berčič, in drugi, 2003, str 22).

Da bi to lahko uresničili, je treba:

- uvajati načela varovanja informacij v vse poslovne funkcije in poslovne procese;
- jasno razmejiti vloge, odgovornosti in dolžnosti;
- ovrednotiti poslovne procese in oceniti varnostna tveganja v poslovnih procesih;
- zagotoviti pravilno in zanesljivo delovanje naprav informacijske tehnologije;
- preprečevati nepooblaščen dostop, škode in motnje v storitvah informacijske tehnologije;
- zagotoviti nemoteno poslovanje;
- zmanjševati nevarnosti človeških napak, kraj, prevar in zlorab sredstev informacijskega sistema;
- obvladovati dostop do informacij in informacijskega sistema;
- zagotavljati spoštovanje zakonskih, kazenskih in civilnopravnih obveznosti ter zahtev. (Berčič, in drugi, 2003, str. 23)

6 OSEBNI DOKUMENTI

6.1 KAJ JE OSEBNI DOKUMENT?

Večina ljudi govori o osebnih dokumentih, vendar slovenska zakonodaja tega pojma sploh ne definira. Slovenska zakonodaja namesto osebnih dokumentov uporablja pojem javna listina. K javnim listinam se štejejo vsi dokumenti, ki so opremljeni s fotografijo in jih je izdal državni organ. Javne listine uporabljamo za identifikacijo osebe oz. dokazovanje istovetnosti in državljanstva. Med javne listine spadajo naslednji dokumenti (MNZ, 2016):

- osebna izkaznica (Javna listina, ki se uporablja za dokazovanje istovetnosti in državljanstva. Uporablja se tudi za nastopanje v pravnem prometu, kot so npr. banke, pošte, poleg tega pa se uporablja tudi kot potovalni dokument za potovanja in bivanje v evropskih državah za obdobje do 90 dni.) (ZOIzk-1, Uradni list RS, št. 35/2011, 1. člen);
- potni list (Javna listina, ki se uporablja za prehod državne meje ter dokazovanje istovetnosti in državljanstva tako v Sloveniji kot tudi v drugih državah.) (ZPLD-1, Uradni list RS, št. 29/11, 1. člen);
- obmejna prepustnica (Javna listina, ki se izda državljanom, ki imajo stalno prebivališče na obmejnih območjih. Ta listina dovoljuje imetniku prestopanje meje na mejnih prehodih za obmejni promet, meddržavnih in mednarodnih prehodih in neprekinjeno bivanje na obmejnem območju druge pogodbenice za obdobje do 7 dni.) (BHROPS, Uradni list RS – Mednarodne pogodbe, št. 20/01, 3. člen);
- vozniško dovoljenje (Dokument, ki se izda oz. katerega veljavnost se podaljša osebi, ki ima v Republiki Sloveniji stalno oz. začasno prebivališče več kot šest mesecev. Vozniško dovoljenje za vožnjo motornih vozil kategorij A2, A, B, BE, C1, C1E, C in CE se vozniku začetniku izda z veljavnostjo do dopolnjenega 21. leta starosti oziroma za dve leti po prvi pridobitvi vozniškega dovoljenja. Vozniško dovoljenje se vozniku začetniku podaljša, ko opravi program dodatnega usposabljanja voznikov začetnikov.) (ZVoz, Uradni list RS št, 109/10 in 25/14, 53. člen);
- orožni list (Dovoljuje posamezniku posest in nošenje vpisanega kosa orožja in se izda za lovsko in športno orožje z veljavnostjo dvajsetih let, za varnostno orožje pa z veljavnostjo desetih let, po preteku veljavnosti dovoljuje orožni list posamezniku posest orožja brez pravice nošenja in prenašanja.) (ZOro-UPB1, Uradni list RS št. 23/2005, 11. člen);
- potrdilo o usposobljenosti za voditelja čolna (To je listina, ki jo pridobi oseba, ki opravi izpit za voznika čolna. Preizkus znanja za upravljanje čolna lahko oseba opravi le pred izpitno komisijo Uprave Republike Slovenije za pomorstvo na sedežu Uprave Republike Slovenije za pomorstvo v Kopru, v prostorih Ministrstva za infrastrukturo v Ljubljani in v prostorih Javne agencije za železniški promet v Mariboru.) (e-Uprava RS, 2016).

6.2 OBDELAVA IN KOPIRANJE OSEBNIH DOKUMENTOV

ZVOP-1 (Uradni list RS, št. 94/2007) v 8. členu, ki je splošne narave, določa, da se osebni podatki lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. Namen obdelave osebnih podatkov mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov.

9. člen ZVOP-1 določa, da se lahko osebni podatki v javnem sektorju (kamor spadajo tudi sodišča in upravne enote) obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon. Z zakonom se lahko določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika.

Nosilci javnih pooblastil lahko obdelujejo osebne podatke tudi na podlagi osebne privolitve posameznika brez podlage v zakonu, kadar ne gre za izvrševanje njihovih nalog kot nosilcev javnih pooblastil. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od zbirk osebnih podatkov, ki nastanejo na podlagi izvrševanja nalog nosilca javnih pooblastil.

Ne glede na prvi odstavek tega člena se lahko v javnem sektorju obdelujejo osebni podatki posameznikov, ki so z javnim sektorjem sklenili pogodbo ali pa so na podlagi pobude posameznika z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe. Ne glede na prvi odstavek tega člena se lahko v javnemu sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo.

3.a člen Zakona o osebni izkaznici (Uradni list RS, št. 71/2008) določa, da upravljavci zbirk osebnih podatkov smejo osebne izkaznice kopirati samo v primerih, ki jih določa zakon. Osebno izkaznico lahko poleg njenega imetnika kopirajo notarji in finančne družbe, ki opravljajo finančne storitve, če jo potrebujejo za dokazovanje identitete državljana v konkretnem postopku. Pojma finančna družba in finančne storitve sta opredeljena v zakonu, ki ureja bančništvo. Kopiranje osebne izkaznice je dovoljeno tudi na podlagi pisne privolitve imetnika osebne izkaznice. Ob kopiranju osebne izkaznice je treba z ustrezno oznako na kopiji zagotoviti, da se kopija osebne izkaznice ne bo uporabljala za druge namene. Prepovedano je nadaljnje kopiranje kopije. Na vlogo imetnika osebne izkaznice je upravljavec zbirk osebnih podatkov dolžan izdati potrdilo o kopiji osebne izkaznice, na katerem je naveden namen rabe kopije in rok, za katerega upravljavec kopijo potrebuje. Imetnik osebne izkaznice lahko kopijo označi s svojim podpisom. Kopijo osebne izkaznice je prepovedano hraniti v elektronski obliki.

Enako 4.a člen Zakona o potnih listinah (Uradni list RS št. 3/06 in 44/08; ZPLD-1) določa, da smejo upravljavci zbirk osebnih podatkov potne listine kopirati samo v primerih, ki jih

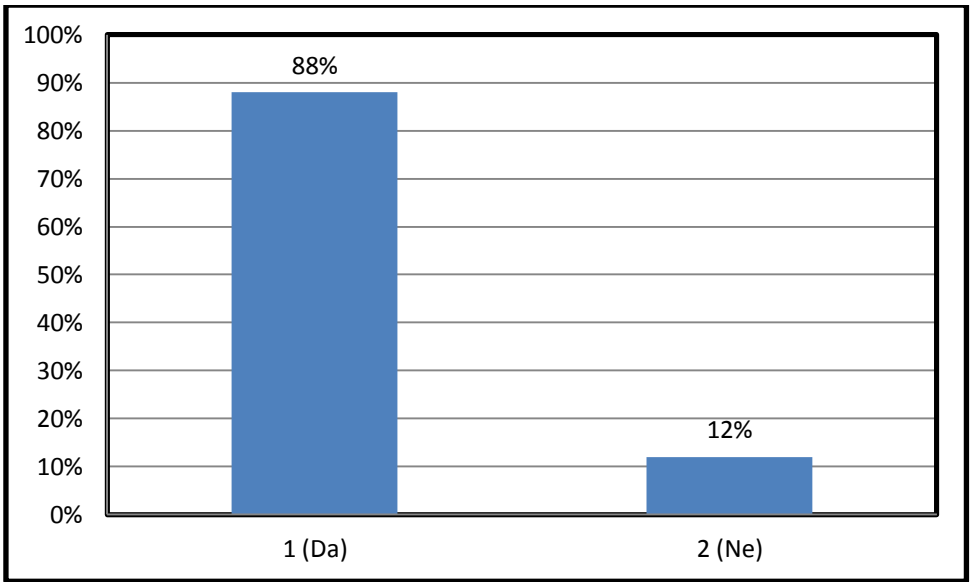
določa zakon. Potno listino lahko poleg njenega imetnika kopirajo notarji in finančne družbe, ki opravljajo finančne storitve, če jo potrebujejo za dokazovanje identitete državljana v konkretnem postopku. Pojma finančna družba in finančne storitve sta opredeljena v zakonu, ki ureja bančništvo. Kopiranje potne listine je dovoljeno tudi na podlagi pisne privolitve imetnika potne listine. Ob kopiranju potne listine je treba z ustrezno oznako na kopiji zagotoviti, da se kopija potne listine ne bo uporabljala za druge namene. Prepovedano je nadaljnje kopiranje kopije. Na vlogo imetnika potne listine je upravljavec zbirk osebnih podatkov dolžan izdati potrdilo o kopiji potne listine, na katerem je naveden namen rabe kopije in rok, za katerega upravljavec kopijo potrebuje. Imetnik potne listine lahko kopijo označi s svojim podpisom. Kopijo potne listine je prepovedano hraniti v elektronski obliki.

7 ANALIZA ANKETNEGA VPRAŠALNIKA

Vprašanje 1: Ali ste uporabnik spletnih socialnih omrežij (Facebook, Instagram, Twitter ...), elektronske pošte (Gmail, Hotmail, Yahoo ...) ali kakršnegakoli drugega spletnega računa?

S prvim vprašanjem sem želel ugotoviti, koliko ljudi sploh uporablja razna socialna omrežja, elektronsko pošto ali kakšen drug spletni račun. Prišel sem do rezultata, da je kar 88 % vprašanih uporabnikov raznih socialnih omrežij oz. drugih spletnih računov, medtem ko ostali (12 %) niso uporabniki spletnih socialnih omrežij.

Grafikon 1: Uporaba socialnih spletnih omrežij

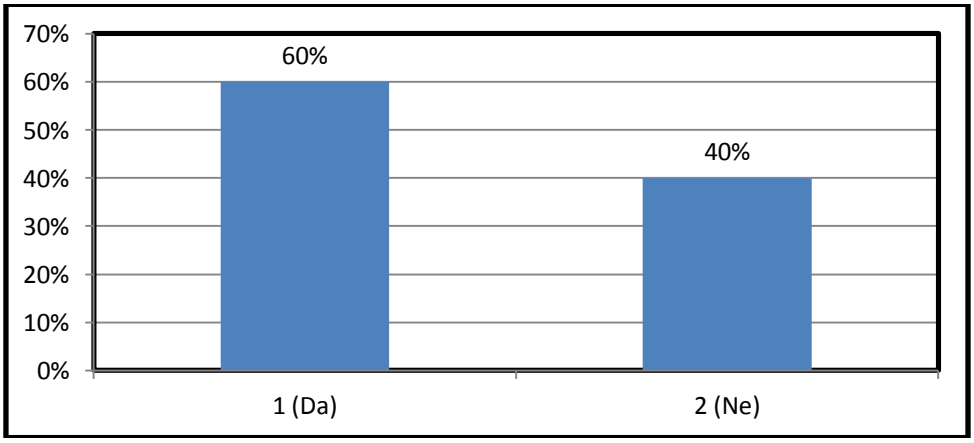


Vir: lasten

Vprašanje 2: Ali ste se pri prvi registraciji seznanili s pogoji vpisa in navodili uporabe?

Analiza odgovorov na drugo vprašanje je pokazala, da se kar 40 % uporabnikov spletnih omrežij ni seznanilo s pogoji vpisa in navodili uporabe, medtem ko pa si je ostalih 60 % uporabnikov vzelo čas ter navodila in pogoje vpisa natančno prebralo.

Grafikon 2: Seznanjenost s pogoji vpisa in navodili uporabe

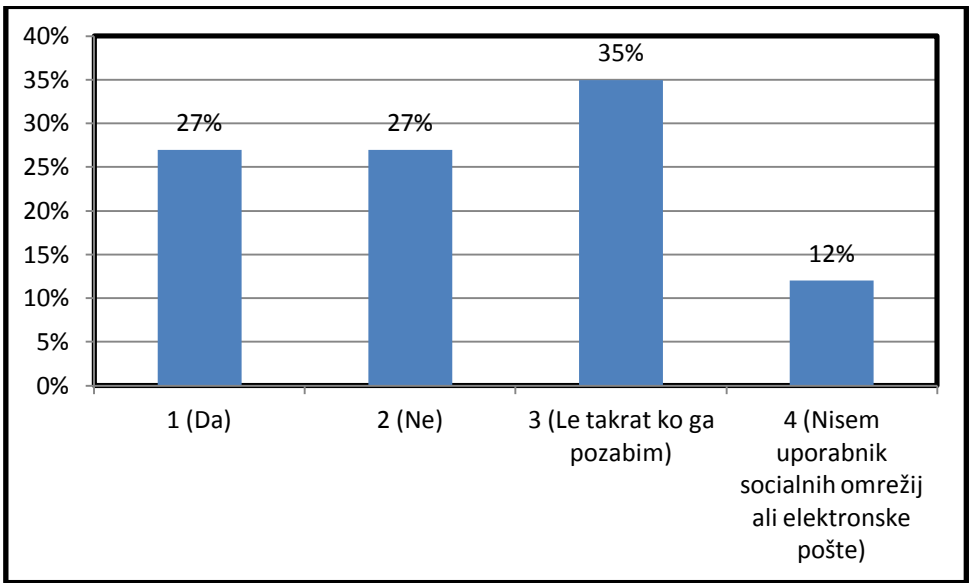


Vir: lasten

Vprašanje 3: Ali kdaj zamenjate svoje geslo na socialnih omrežjih ali pri elektronski pošti?

Zanimalo me je tudi, ali uporabniki kdaj zamenjajo geslo, in prišel sem do zelo raznolikih odgovorov. 27 % uporabnikov je odgovorilo, da vztraja pri geslih, ki so jih izbrali pri prvem vpisu, prav tako pa jih je tudi 27 % uporabnikov odgovorilo, da redno menjajo gesla, medtem ko jih 35 % menja le takrat, ko so stara pozabili. Ostalih 12 % anketirancev pa nima teh težav, saj niso uporabniki spletnih socialnih omrežij ali kakšnega drugega računa.

Grafikon 3: Gesla

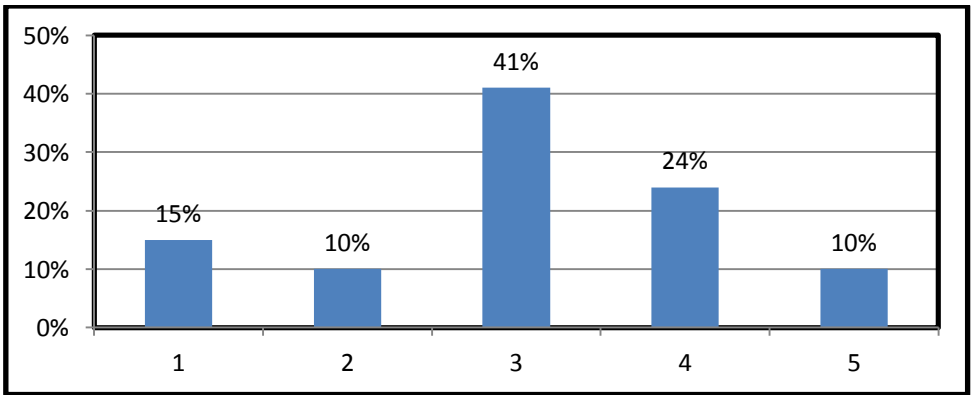


Vir: lasten

Vprašanje 4: Kakšna je zahtevnost vaših gesel od 1 do 5?

Zanimalo me je, kako bi uporabniki ocenili zahtevnost svojih gesel. Odločil sem se, da jim ponudim na izbiro številčno ocenjevanje od 1 do 5 (pri čemer je 1 pomenilo lahko, 5 pa zelo težko). Prišel sem do ugotovitve, da 41 % anketirancev meni, da so njihova gesla srednje zahtevna. 24 % anketirancev je težavnost gesel ocenila s štiri, 10 % pa s pet. 15 % anketirancev meni, da je njihovo geslo zelo lahko, zadnjih 10 % anketirancev pa je izbralo težavnost 2.

Grafikon 4: Zahtevnost gesel

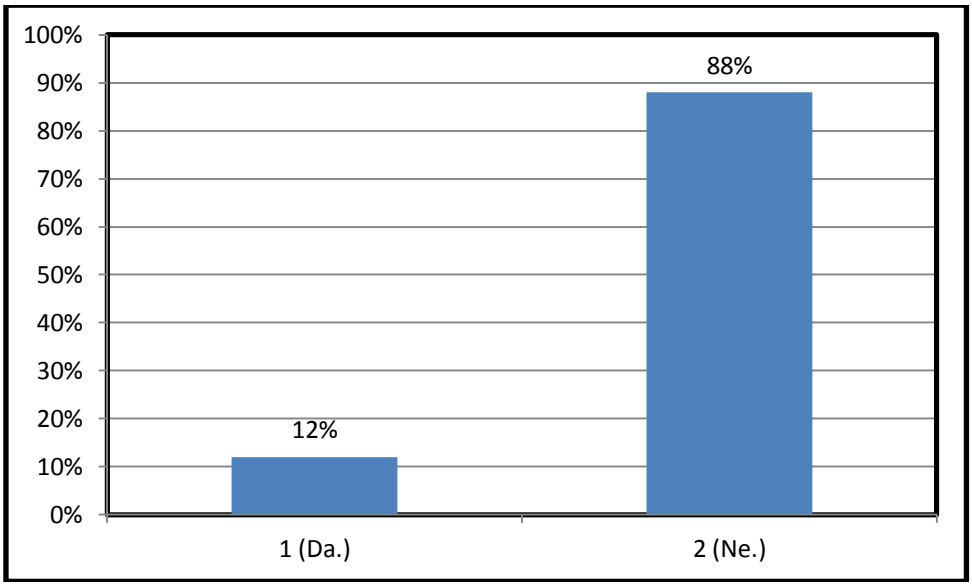


Vir: lasten

Vprašanje 5: Ali ste že bili kdaj žrtev vdora v svoj spletni račun?

Zaradi vedno pogostejših vdorov v spletne račune in socialna omrežja me je zanimalo, ali je kdo od anketirancev že kdaj postal žrtev vdora. K sreči 88 % anketirancev ni imelo neprijetnih izkušenj z vdori, medtem ko ostalih 12 % ni imelo te sreče.

Grafikon 5: Vdor v spletni račun

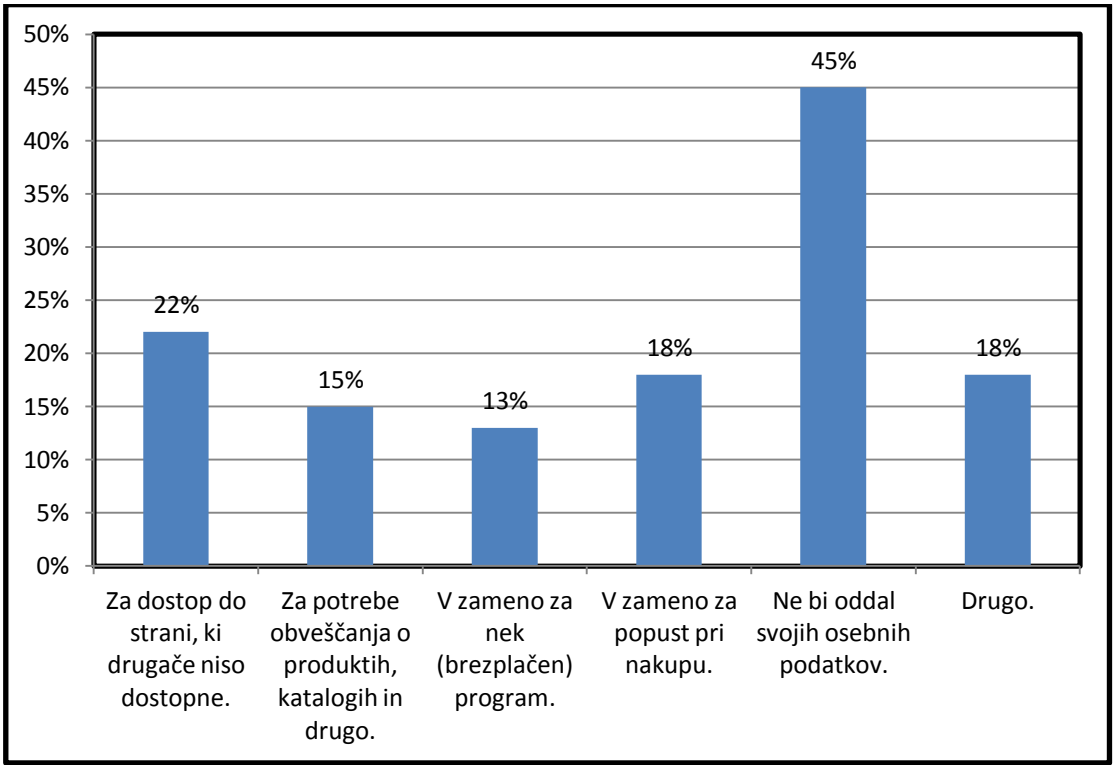


Vir: lasten

Vprašanje 6: V katerih primerih bi oddali svoje osebne podatke?

Ker obstaja vedno več spletnih strani in trgovin, ki za dostop zahtevajo uporabnikove osebne podatke, me je zanimalo, kako se odločajo anketiranci v takšnih situacijah. Rezultati so pokazali, da kar 45 % anketirancev ne bi oddalo svojih osebnih podatkov. 22 % anketirancev bi svoje osebne podatke oddalo zato, da bi lahko dostopali do določenih strani, ki drugače niso dostopne, 18 % bi jih oddalo v zameno za popust pri nakupu, 15 % bi jih oddalo za potrebe obveščanja o produktih, katalogih, 13 % bi svoje osebne podatke oddalo v zameno za nek brezplačen program, medtem ko pa bi jih zadnjih 18 % oddalo v kakšnem drugem primeru, ki v vprašalniku niso bili navedeni.

Grafikon 6: Osebni podatki in splet

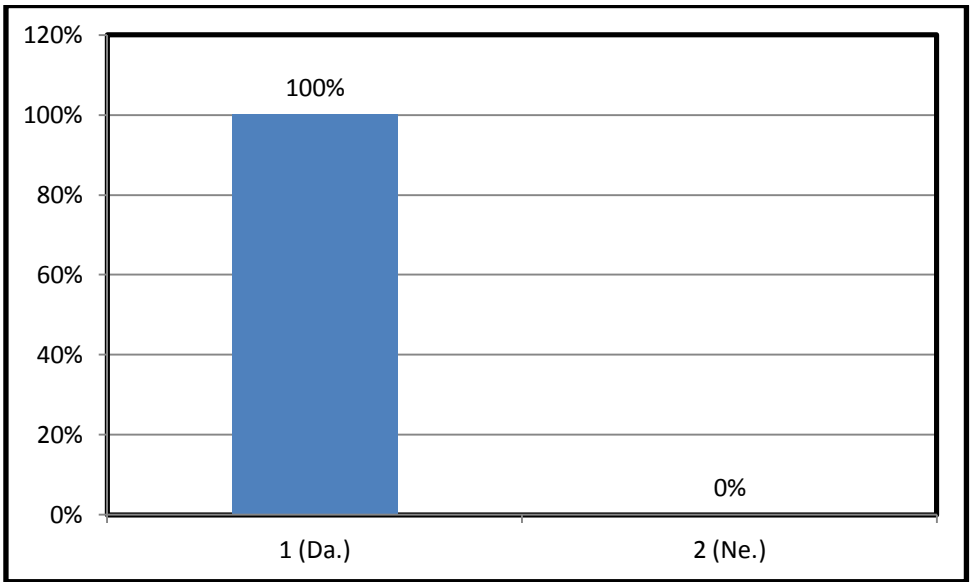


Vir: lasten

Vprašanje 7: Ali ste oz. ste bili v kakršnemkoli delovnem razmerju (lahko tudi študentsko delo)?

Pri slednjem vprašanju me je zanimalo, ali so bili anketiranci že kdaj v kakršnemkoli delovnem razmerju. Izkazalo se je, da so prav vsi že kdaj delali.

Grafikon 7: Delovno razmerje

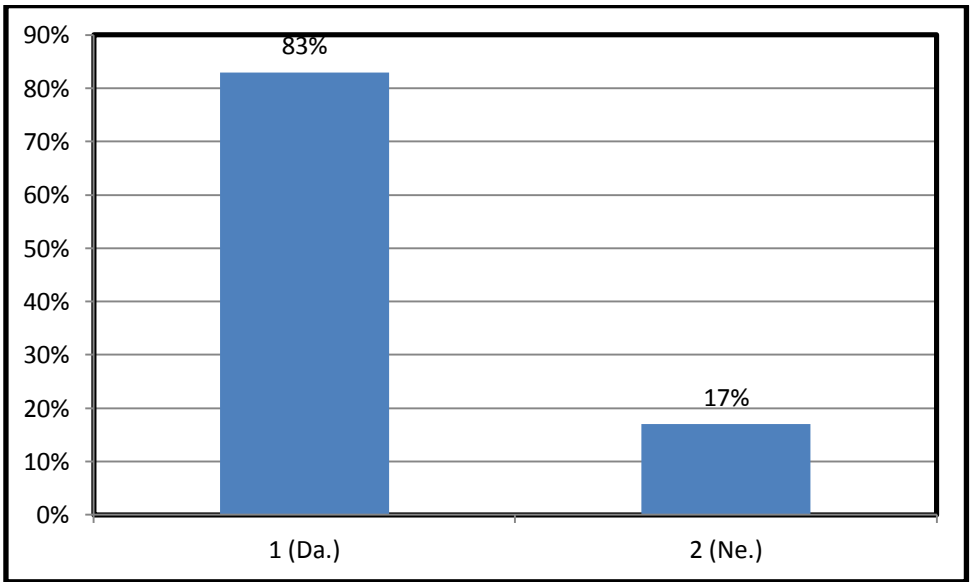


Vir: lasten

Vprašanje 8: Ali ste se pred sklenitvijo delovnega razmerja seznanili s pravicami in dolžnostmi?

Pri osmem vprašanju me je zanimalo, ali so se anketiranci pred sklenitvijo delovnega razmerja seznanili s pravicami in dolžnostmi. Izkazalo se je, da jih je 83 % na to vprašanje odgovorilo pritrdilno, ostalih 17 % pa se pri sklenitvi delovnega razmerja ni seznanilo s pravicami in dolžnostmi.

Grafikon 8: Pravice in dolžnosti

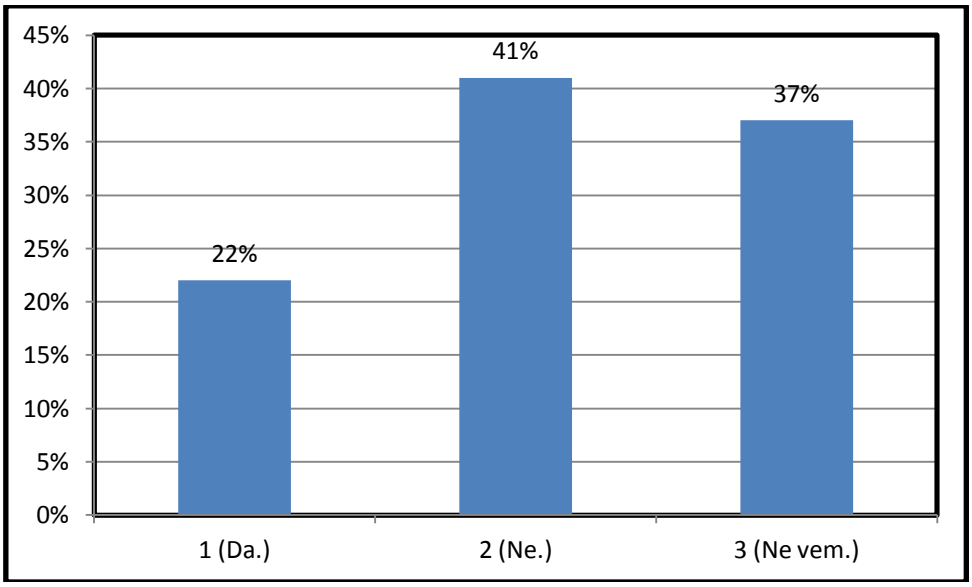


Vir: lasten

Vprašanje 9: Ali menite, da je zasebnost v delovnih razmerjih pri nas dovolj varovana s pozitivnimi predpisi?

Od anketirancev sem pri naslednjem vprašanju želel izvedeti, ali je po njihovem mnenju zasebnost v delovnih razmerjih pri nas dovolj varovana s pozitivnimi predpisi. 41 % anketirancev meni, da zasebnost v delovnih razmerjih pri nas ni dovolj varovana s pozitivnimi predpisi, medtem ko pa 22 % anketirancev meni ravno nasprotno. 37 % anketirancev pa je pri tem vprašanju ostalo nevtralnih in odgovorilo z »ne vem«.

Grafikon 9: Varovanje zasebnosti

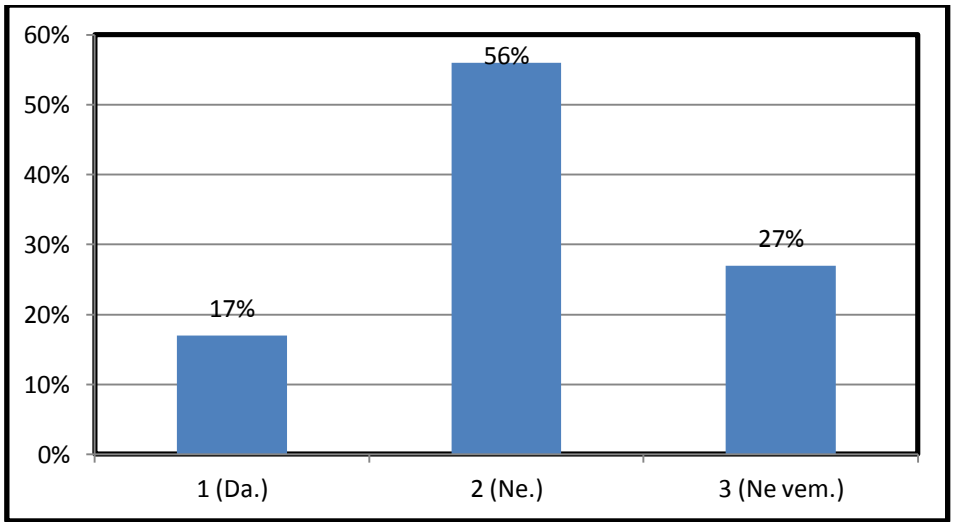


Vir: lasten

Vprašanje 10: Ali menite, da predpisi sami zadoščajo za ustrezno varovanje zasebnosti?

56 % anketirancev meni, da predpisi sami ne zadoščajo za ustrezno varovanje zasebnosti, medtem ko jih 17 % trdi ravno nasprotno. Na koncu je ostal še odgovor »ne vem«, ki ga je izbralo 27 % anketirancev.

Grafikon 10: Predpisi o varovanju zasebnosti

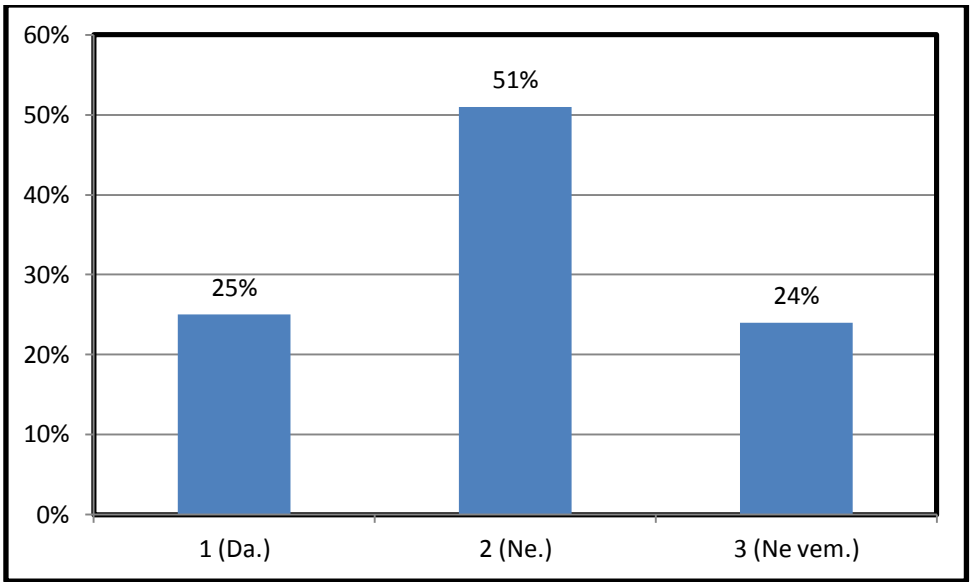


Vir: lasten

Vprašanje 11: Ali menite, da se varovanje zasebnosti v delovnih razmerjih v praksi uspešno uveljavlja?

Tudi pri tem vprašanju je večina anketirancev izbrala odgovor »ne«, kar znaša 51 %. 25 % jih meni, da se varovanje zasebnosti v delovnih razmerjih v praksi uspešno uveljavlja, medtem ko jih je 24 % ostalo nevtralnih in odgovorilo z »ne vem«.

Grafikon 11: Varovanje zasebnosti v praksi

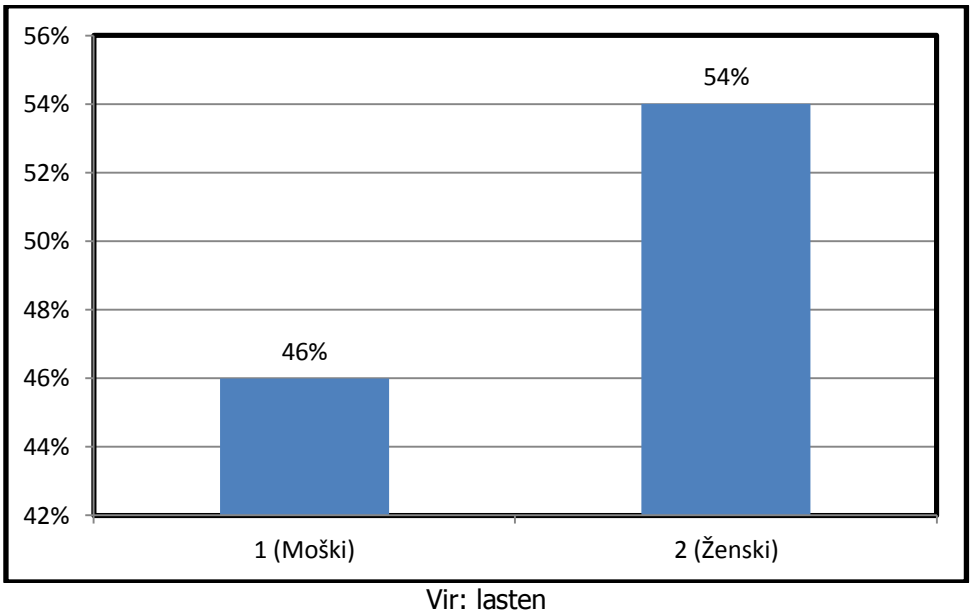


Vir: lasten

Vprašanje 12: Spol?

V anketi je sodelovalo 59 anketirancev. S 54 % je rahlo prevladal ženski spol, moških pa je bilo 46 %.

Grafikon 12: Spol

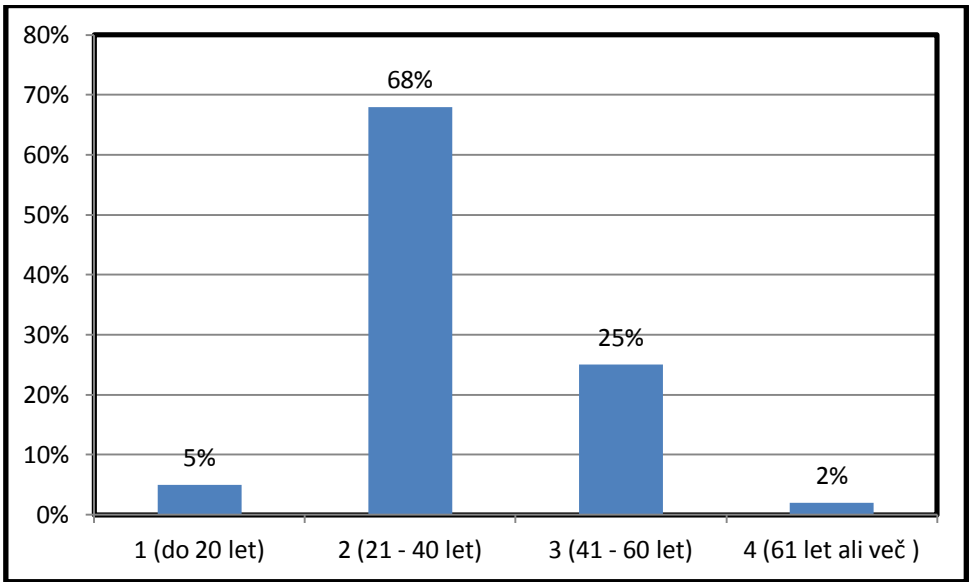


Vir: lasten

Vprašanje 13: V katero starostno skupino spadate?

Največ anketirancev je bilo starih med 21 in 40 leti. Teh je bilo kar 68 %, na drugem mestu so bili stari od 41 do 60 let, ki jih je bilo 25 %. Starejši od 60 let je bil le 1 anketiranec (2 %), medtem ko so bili mlajši od 20 let le trije anketiranci (5 %).

Grafikon 13: Starostne skupine



Vir: lasten

7.1 UGOTOVITVE

V prvem delu raziskovalnega dela sem ugotovil, da je uporabnikov raznih spletnih socialnih omrežij ter elektronskih pošt vedno več, žal pa so raziskave pokazale, da je kar precej visok odstotek uporabnikov, ki se pri prvi registraciji niso seznanili z navodili ter pogoji vpisa, poleg tega pa tudi niso ravno skrbni pri redni menjavi gesel. K sreči velika večina anketirancev še ni bila žrtev vdora v spletne račune, se jim pa to lahko zgodi, če ne bodo pazljivi. Za mnogo prevar, vdorov in kraj osebnih podatkov smo krivi ljudje sami, ker ne poskrbimo dovolj za lastno varnost na spletu.

V drugem delu raziskovalnega dela pa me je zanimalo mnenje anketirancev o varovanju zasebnosti v podjetjih. Raziskava je pokazala, da se je večina anketirancev pri sklenitvi delovnega razmerja seznanila s pravicami in dolžnostmi. Ko pa je beseda nanesla na varovanje zasebnosti v delovnih razmerjih in njihove predpise, pa sem ugotovil, da se slaba tretjina anketiranih ni nikoli poglabljala v to področje, kar dokazuje izbira odgovora »ne vem«. Glede na rezultate sem ugotovil, da okrog 50 % anketirancev meni, da predpisi sami ne zadoščajo za ustrezno varovanje zasebnosti, poleg tega pa menijo, da se tudi v praksi ne uveljavljajo uspešno. Menim, da bi morali biti ljudje bolj ozaveščeni glede zlorabe in kraje osebnih podatkov. Morda bi bilo smiselno, da bi na tem področju z raznimi reklamnimi sporočili, propagandnim materialom tudi država poskusila čim bolj ozavestiti in seznaniti ljudi z nevarnostmi uporabe spletnih vsebin.

8 ZAKLJUČEK

Varstvo osebnih podatkov je ena izmed temeljnih človekovih pravic, ki je v demokratičnih sistemih urejena z ustreznimi predpisi. Iz 38. člena Ustave RS izhaja, da je varstvo osebnih podatkov pravica, ki je in mora biti urejena s posebnim zakonom. Po tem zakonu cilj varstva osebnih podatkov ni le varstvo osebnih podatkov samih, ampak gre tudi za varstvo posameznika, na katerega se podatki nanašajo, in s tem varstvo njegove informacijske zasebnosti.

Veljavni Zakon o varstvu osebnih podatkov določa pravice, postopke in ukrepe, s katerimi se preprečujejo nezakoniti in prekomerni posegi v integriteto človekove osebnosti, ki so lahko posledica obdelave osebnih podatkov, ki se nanašajo nanj. V Republiki Sloveniji je v skladu z veljavno zakonodajo vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotovljeno varstvo osebnih podatkov.

Vsak posameznik se mora zavedati, kako pomembno je skrbeti za varstvo osebnih podatkov. Ker živimo v časih, ko lahko kadarkoli in kjerkoli pride do zlorabe osebnih podatkov, je treba biti še posebej previden. Najmanj previdni med vsemi so običajno najstniki in otroci, ki se ne zavedajo posledic, ki jih lahko doletijo, če na družabnem omrežju pustijo kakšne podatke, ki niso namenjeni širši javnosti. Velik problem vseh je tudi slaba zaščita računalnika z varnostnimi programi. Varnostni programi, kot so npr. antivirusni programi in požarni zidovi, pa ne bodo preprečili zlorab, če jih uporabniki ne bodo redno obnavljali in posodabljali.

Posledica nepooblaščenega odvzema osebnih podatkov je lahko kraja identitete, kjer se tat z ukradenimi osebnimi podatki izdaja za žrtev. V izogib takšnim nevšečnostim je treba vse osebne dokumente in listine, ki vsebujejo osebne podatke, uničiti na ustrezen način. Na takšnih izpiskih in dokumentih je dovolj podatkov, da tat v imenu žrtve izvede finančne transakcije, najame posojilo, nakupi blago za večjo količino denarja, vzame hipoteko na žrtvino hišo itd.

Na varovanje osebnih podatkov ter informacij morajo poleg posameznikov oz. fizičnih oseb skrbeti tudi vsa podjetja, ustanove oz. vsi tisti organi, ki operirajo z osebnimi podatki. V primeru varnostnega incidenta v podjetju lahko pride do posledic na finančnem področju, še huje pa je, če pride do nezaupanja strank v podjetje, kar lahko usodno vpliva na stabilnost podjetja. Napadi na varovane informacije niso nobena redkost, poleg tega pa je takih dogodkov po svetu vsako leto več. Tovrstni napadi po vsem svetu letno povzročijo za več milijard evrov škode.

Na povečane napade na varovane osebne podatke predstavlja med drugim tudi hiter razvoj postopkov in metod do hitrejših dostopov do podatkov, predvsem v računalniških komunikacijah. S tem se je povečala tudi nevarnost razkritja podatkov oz. nevarnost dostopa do njih nepooblaščenim osebam. Ravno zaradi takšnih nevšečnosti mora država z zakonodajo zelo podrobno in nazorno opredeliti določila za zavarovanje podatkov in varstvo posameznikov, na katere se podatki nanašajo. Na varovanje osebnih podatkov ter

informacij morajo poleg posameznikov oz. fizičnih oseb skrbeti tudi vsa podjetja, ustanove oz. vse tiste organizacije, ki operirajo z osebnimi podatki z namenom, da poskrbijo za zaščito informacijskih sistemov, zavarujejo prostore, kjer se zaupni podatki hranijo, varujejo sistemsko in računalniško opremo ter podatke, ki se obdelujejo z računalniško opremo, poskrbeti morajo za pravilen zajem in posredovanje zaupnih podatkov in poskrbeti, da se podatki, ki so neuporabni in se ne potrebujejo več, pravočasno izbrišejo itd.

Rezultati ankete so pokazali, da anketirani ljudje niso najbolj vešči varovanja osebnih podatkov. Poleg tega me je v anketi še zanimalo, kakšno mnenje imajo anketiranci glede varovanja zasebnosti v podjetjih. Rezultati so pokazali, da je večina anketiranih mnenja, da bi bilo treba urediti predpise o varovanju zasebnosti v podjetjih, poleg tega pa anketa kaže na to, da se ti predpisi v praksi ne uveljavljajo najbolje.

LITERATURA IN VIRI

Literatura

1. Berčič, B., Bojanec, A., Krkoč, P., Mrhar, P., Patru, P., Šinigoj, A., Valenčič, I. (2003). *Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici*: Inštitut za Informacijsko Varnost.
2. Egan, M., Mather, T. (2005). *Varovanje informacij – grožnje izzivi in rešitve*. Ljubljana: Pasadena.
3. Suša, M. (2009). *Socialni inženiring na internetu,* diplomsko delo. Ljubljana: Fakulteta za družbene vede.
4. Perič, G. (2014). *Kraja identitete v informacijski družbi*, diplomsko delo. Ljubljana: Fakulteta za družbene vede.
5. Kovačič, M. (2003). *Zasebnost na internetu*. Ljubljana. Mirovni inštitut, Inštitut za sodobne družbene in politične študije.
6. Cvetko, A. (1999). *Varovanje zasebnosti v delovnih razmerjih*. Ljubljana. Gospodarski vestnik.
7. Rovšek, J. (2005). *Zasebno in javno v medijih. Ljubljana*. Mirovni inštitut, Inštitut za sodobne družbene in politične študije.

Viri

8. (2007) Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1), Ur. list RS, št. 94/2007.
9. (2011) Zakon o osebni izkaznici (ZOIzk-1), Ur. list RS, št. 35/2011.
10. (2011) Zakon potnih listinah (ZPLD-1-UPB4), Ur. list RS, št. 29/11.
11. (2001) Zakon o ratifikaciji Sporazuma med Republiko Slovenijo in Republiko Hrvaško o obmejnem prometu in sodelovanju (BHROPS), Ur. list RS – Mednarodne pogodbe, št. 20/01.
12. (2010) Zakon o voznikih (ZVoz), Ur. list RS, št. 109/2010.
13. (2005) Zakon o orožju (ZOro-1-UPB1), Ur. list RS, št. 23/2005.
14. Resnik, S. (2010). *Prednosti in slabosti e-poslovanja*. Pridobljeno 3.3.2016 iz: http://mladipodjetnik.si/novice-in-dogodki/novice/prednosti-in-slabosti-e-poslovanja.
15. Skrt, R. (2005). *Pharming napadi*. Pridobljeno 16.3.2016 iz: http://www.nasvet.com/pharming-napadi/.
16. Jurinčič, N. (2013). *Ponoči razmišljam, ali kje na svetu kdo izkorišča mojo identiteto za zločine*. Pridobljeno 22.3..2016 iz: http://www.24ur.com/novice/crna-kronika/ponoci-razmisljam-ce-kje-na-svetu-kaksen-zlocinec-izkorisca-mojo-identiteto.html.
17. Havliček, M. (2012). *Kraja identitete na spletu*. Pridobljeno 3.4.2016 iz: http://eudace.eu/knjiznica/clanki/2013021409361182/.
18. Havliček, M. (2012). *Protipravno objavljeni osebni podatki na spletnih portalih*. Pridobljeno 3.4.2016 iz: http://eudace.eu/knjiznica/clanki/2013021409523434/.

19. Murn. A. (2015). *Uporabnost Facebook profila*. Pridobljeno (18.4.2016) iz: http://www.preberite.si/author/alesmurn/.
20. Informacijski pooblaščenec. (21. 4. 2016). *Kraja identitete – test*. Pridobljeno iz: http://www.ip-rs.si/kraja-identitete/test/index.html.
21. Informacijski pooblaščenec (24. 4. 2016). *Mladi in varstvo osebnih podatkov na spletu*. Pridobljeno iz: https://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Mladi_in_varstvo_osebnih_podatkov_na_spletu_-_nasveti_IP_maj2009.pdf.
22. Informacijski pooblaščenec. (27. 4. 2016). *Varstvo osebnih podatkov na internetu*. Pridobljeno iz: https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/.
23. Informacijski pooblaščenec. (28. 4. 2016). *Socialni inženiring in kako se pred njim ubraniti*. Pridobljeno iz: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.
24. Banisar, D. (23. 5. 2000). *Privacy & Human Rights 1999*. Pridobljeno iz: http//www.privacyinternational.org/survey/index99.html.
25. Presentia. (11. 9. 2008). *Kaj je spoofing?*. Pridobljeno (29.4.2016) iz: http://www.presentia.si/baza-znanja-helpdesk/2008/kaj-je-spoofing/.
26. Flibo d.o.o.. (29. 4. 2016). *Cilj in namen zlonamerne programske opreme ˝virusi˝*. Pridobljeno iz: http://flibo.si/?stran=virusi.
27. Šolski center Celje (2. 5. 2016). *Vohunski virusi*. Pridobljeno iz: http://web.sc-celje.si/tomi/seminarske2015/Virusi/Jernej/3Vohunskivirusi.html.
28. SI-CERT. (5. 5. 2016). *Vrste zlonamernih programov*. Pridobljeno iz: https://www.varninainternetu.si/article/vrste-zlonamernih-programov/.
29. Fakulteta za računalništvo in informatiko. (7. 5. 2016). *Računalniški virusi in črvi*. Pridobljeno iz: http://colos.fri.uni-lj.si/eri/INFORMATIKA/RACUNALNISKA_OMREZJA/virusi_crvi.html.
30. Telekom Slovenije. (7. 5. 2016). *Teme pomoči – Kaj je nezaželena elektronska pošta (spam)?*. Pridobljeno iz: http://www.telekom.si/pomoc-in-podpora/teme-pomoci/internet/e-posta/pogosta-vprasanja#faq=19.
31. MNZ. (8. 5. 2016). *Osebni dokumenti in prebivališče*. Pridobljeno iz: http://www.mnz.gov.si/si/mnz_za_vas/osebni_dokumenti_in_prebivalisce/.
32. E-uprava RS (16. 6. 2016). *Preizkus znanja za upravljanje čolna*. Pridobljeno iz: https://e-uprava.gov.si/podrocja/promet-prometna-infrastruktura/pomorski-promet/preizkus-znanja-za-upravljanje-colna.html.

PRILOGA

ANKETNI VPRAŠALNIK

1. **Ali ste uporabnik spletnih socialnih omrežij (Facebook, Instagram, Twitter ...), elektronske pošte (Gmail, Hotmail, Yahoo ...) ali kakršnegakoli drugega spletnega računa?**

   ○ Da
   ○ Ne

2. **Ali ste se pri prvi registraciji seznanili s pogoji vpisa in navodili uporabe?**

   ○ Da
   ○ Ne

3. **Ali kdaj zamenjate svoje geslo na socialnih omrežjih ali pri elektronski pošti**

   ○ Da
   ○ Ne
   ○ Le takrat ko ga pozabim
   ○ Nisem uporabnik socialnih omrežij ali elektronske pošte

4. **Kakšna je zahtevnost vaših gesel od 1 do 5?**

	1	2	3	4	5
Lahko (1), zelo težko (5)	○	○	○	○	○

5. **Ali ste že bili kdaj žrtev vdora v svoj spletni račun?**

   ○ Da.
   ○ Ne.

6. **V katerih primerih bi oddali svoje osebne podatke?**
   Možnih je več odgovorov

   ☐ Za dostop do strani, ki drugače niso dostopne.
   ☐ Za potrebe obveščanja o produktih, katalogih in drugo.
   ☐ V zameno za nek (brezplačen) program.
   ☐ V zameno za popust pri nakupu.
   ☐ Ne bi oddal svojih osebnih podatkov.
   ☐ Drugo.

7. **Ali ste kdaj v kakršnemkoli delovnem razmerju (lahko tudi študentsko delo)?**

   ○ Da.
   ○ Ne.

8. **Ali ste se pred sklenitvijo delovnega razmerja seznanili s pravicami in dolžnostmi?**

   ○ Da.
   ○ Ne.

9. **Ali menite, da je zasebnost v delovnih razmerjih pri nas dovolj varovana s pozitivnimi predpisi?**

   ○ Da.
   ○ Ne.
   ○ Ne vem.

10. **Ali menite, da predpisi sami zadoščajo za ustrezno varovanje zasebnosti?**

    ○ Da.
    ○ Ne.
    ○ Ne vem.

11. **Ali menite, da se varovanje zasebnosti v delovnih razmerjih v praksi uspešno uveljavlja?**

    ○ Da.
    ○ Ne.
    ○ Ne vem.

12. **Spol:**

    ○ Moški
    ○ Ženski

13. **V katero starostno skupino spadate?**

    ○ do 20 let
    ○ 21–40 let
    ○ 41–60 let
    ○ 61 let ali več