Varstvo osebnih podatkov

Predmet = Soc. Spretnosti

Contents

1. Uvod....4

....5

2. Varstvo osebnih podatkov....5

2.1 Kaj je osebni podatek....5

2.2 Kdaj se lahko osebni podatki obdelujejo ?....6

2.3 Pod kakšnimi pogoji se osebni podatki lahko posredujejo pogodbenemu obdelovalcu osebnih podatkov?....6

2.4 Pod kakšnimi pogoji se lahko osebni podatki obdelujejo za zgodovinske, statistične in znanstveno-raziskovalne namene?....6

2.5 Kdaj se osebni podatki lahko posredujejo drugim pravnim ali fizičnim osebam?....7

2.6 Na kakšen način je treba posameznika informirati o obdelavi njegovih osebnih podatkov?....7

2.7 Kakšne so dolžnosti upravljavcev osebnih podatkov v zvezi z zavarovanjem osebnih podatkov?....8

2.8 Kakšne so pravice posameznika glede njegovih osebnih podatkov?....9

2.9 Kako lahko ukrepam, če so kršene moje pravice do varstva osebnih podatkov oziroma so bili moji osebni podatki obdelovani v nasprotju z zakonom?....10

2.10 Kdaj se osebni podatki lahko iznesejo iz države?....10

2.11 Kdaj se osebni podatki lahko uporabljajo za namene ponujanja blaga, storitev ali zaposlitev?....11

3. Varstvo osebnih podatkov – delovno okolje....12

3.1 Fotografiranje, nadzor telefonskih klicev....14

3.2 Preverjanje alkoholiziranosti....14

3.3 Zbirke osebnih podatkov....15

3.4 10 najpogostejših kršitvev ZVOP-1 v delovnih razmerjih....15

4. Kako uporabljati FACEBOOK....15

....16

4.1 10 nastavitev zasebnosti, ki bi jih moral poznati vsak uporabnik Facebooka....17

4.2 Prijava zlorabe osebnih podatkov na samem spletnem omrežju....20

5. Kraja identitete....20

5.1 Kaj je kraja identitete?....21

5.2 Pridobivanje osebnih podatkov s pomočjo kopij osebnih dokumentov....24

5.3 Se kraja osebne identitete dogaja tudi v Sloveniji....26

5.4 Zavarovanje osebnih podatkov, kot ga določa Zakon o varstvu osebnih podatkov (ZVOP-1)....27

5.5 Prijava kršitev....28
6. Spletno nadlegovanje....29
Slovar besed....29
6.1 Kaj je spletno nadlegovanje ?....30
6.2 Zakaj je nevarno ?....31
6.3 Vzroki....32
6.4 Kako poteka ?....32
6.5 Neposredni napadi....32
7. Viri....34
https://www.ip-rs.si/publikacije/prirocniki-in-smernice/....35
http://en.wikipedia.org/wiki/Identity_theft....35
http://e-uprava.gov.si/e-uprava/dogodkiPrebivalci.euprava?zdid=632....35
http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html....35
https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu-samo-za-mlade/....35
8. Zaključek....35

1. Uvod

Torej v tej temi vam bom povedal nekaj o varovanju osebnih podatkov. Veliko bom povedal o zlorabi le the podatkov na medmrežju po domače internetu. Prikazal bom tudi praktičen primer zlorabe v spletnih klepetalnicah , elektronski pošti , ...

2. Varstvo osebnih podatkov

2.1Kaj je osebni podatek

Osebni podatek je kateri koli podatek , ki se nanaša na osebo , če vemo , kdo je ta oseba . Primer – Janez Novak je najpogostejše slovensko ime. In če rečemo samo Janez Novak , ne vemo , za katerega Janeza

Novaka gre . Če pa rečemo Janez Novak iz male vasice kjer živi samo en Janez Novak potem vemo , kdo je ta oseba. Tako ime in priimek postaneta osebni podatek , ki ga varuje zakon o varstvu osebnih podatkov varuje . Določljiva fizična oseba pa je tista, ki se jo lahko neposredno ali posredno identificira s pomočjo njenih identifikacijskih številk (npr. EMŠO, davčna številka, številka zdravstvenega zavarovanja, telefonska številka, registrska številka vozila), ali s sklicevanjem na dejavnike, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto (npr. zaposlitev, naslov, funkcijo, položaj ali status v določenem subjektu, ipd.).

2.2 Kdaj se lahko osebni podatki obdelujejo ?

Obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana.

Osebni podatki se lahko obdelujejo le, če tako določa zakon, ali če je podana osebna privolitev posameznika, čigar podatek se obdeluje. Tudi namen obdelave mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora ta biti predhodno seznanjen z njenim namenom.

2.3 Pod kakšnimi pogoji se osebni podatki lahko posredujejo pogodbenemu obdelovalcu osebnih podatkov?

Zakon o varstvu osebnih podatkov upravljavcu omogoča, da posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo poveri drugi pravni ali fizični osebi -pogodbenemu obdelovalcu, ki podatke obdeluje v imenu in na račun upravljavca osebnih podatkov. Pri tem pa morata biti izpolnjena dva pogoja:

1. pogodbeni obdelovalec mora biti registriran za opravljanje takšne dejavnosti;
2. medsebojne pravice in obveznosti morajo biti urejene v pogodbi; Ta mora obvezno vsebovati tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov, upravljavec pa mora izvajanje dogovorjenih postopkov in ukrepov tudi nadzorovati.

2.4 Pod kakšnimi pogoji se lahko osebni podatki obdelujejo za zgodovinske, statistične in znanstveno-raziskovalne namene?

Osebni podatki se v omenjene namene lahko obdelujejo ne glede na prvotni namen zbiranja. Tako zbrani podatki se objavijo ali posredujejo uporabniku v anonimni obliki. V neanonimni pa le, če drug zakon določa drugače, če je posameznik, na katerega se podatki nanašajo, objavo dovolil s pisno

privolitvijo, ali če je za takšno objavo podano pisno soglasje dedičev umrle osebe iz prvega in drugega dednega razreda.

2.5 Kdaj se osebni podatki lahko posredujejo drugim pravnim ali fizičnim osebam?

Osebne podatke se lahko posredujejo drugim osebam le v primeru:

- če obstaja za to izrecna podlaga v katerem od zakonov,

- če je posameznik privolil v posredovanje osebnih podatkov,

- če je posredovanje osebnih podatkov potrebno zaradi izpolnjevanja pogodbe ali uveljavljanje pravic iz pogodbenega razmerja,

- izjemoma tudi v primeru, če je posredovanje osebnih podatkov nujno zaradi izvrševanja zakonitih pristojnosti, nalog ali obveznosti javnega sektorja in se s tem ne poseže v opravičen interes posameznika,

- če je posredovanje osebnih podatkov nujno zaradi uresničevanja zakonitih interesov zasebnega sektorja in ti interesi očitno prevladujejo nad interesi posameznika, na katerega se osebni podatki nanašajo.

Upravljavec centralnega registra prebivalstva ali evidenc stalno in začasno prijavljenih prebivalcev mora na način, ki je določen za izdajo potrdila, upravičencu, ki izkaže pravni interes za uveljavljanje pravic pred osebami javnega sektorja, posredovati osebno ime in naslov stalnega ali začasnega prebivališča posameznika, zoper katerega uveljavlja svoje pravice. Ob tem mora upravičenec jasno izkazati svoj pravni interes, za uveljavljanje katerih pravic rabi zahtevane podatke ter pred katerimi osebami javnega sektorja bo te svoje pravice uveljavljal. Upravljavec osebnih podatkov mora pri posredovanju zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je možno zakonsko varstvo pravice posameznika pred nedopustnim posredovanjem osebnih podatkov. Upravljavec zbirke osebnih podatkov je po ZVOP-1 dolžan v 30-tih dneh posamezniku posredovati seznam uporabnikov, ki so jim njegovi osebni podatki bili posredovani in mu sporočiti kdaj, na kakšni podlagi in za kakšen namen so bili posredovani.

2.6 Na kakšen način je treba posameznika informirati o obdelavi njegovih osebnih podatkov?

Kadar se osebni podatki zbirajo neposredno od posameznika, mu mora upravljavec osebnih podatkov ali njegov zastopnik sporočiti svoje podatke (osebno ime, naziv oziroma firma in naslov oziroma sedež) ter namen obdelave osebnih podatkov. V posebnih okoliščinah navede tudi:

- uporabnika ali vrste uporabnikov njegovih osebnih podatkov,

- ali je zbiranje osebnih podatkov obvezno oziroma prostovoljno, ter možne posledice, če podatkov ne bo podal prostovoljno,

- informacijo o pravici do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja in izbrisa osebnih podatkov, ki se nanašajo nanj.

Posebne okoliščine

ZVOP-1 ne opredeljuje, katere so posebne okoliščine zbiranja osebnih podatkov. Ker pa je temeljito informiranje predpogoj za pošteno in zakonito obdelavo osebnih podatkov vsakega posameznika, mu je potrebno vedno dati vse potrebne informacije, ki jih zahteva. Še zlasti je to potrebno, če se osebni podatki obdelujejo na podlagi osebne privolitve posameznika ali na podlagi pogodbenega razmerja in bodo ti podatki posredovani tudi drugim uporabnikom. Prav tako je potrebno dosledno informiranje, ko posameznik ne želi prostovoljno posredovati določenih osebnih podatkov in zaradi tega lahko trpi tudi posledice. Informacije morajo biti jasne in razumljive, saj se posameznik lahko le na podlagi teh odloči, ali bo za obdelavo svojih osebnih podatkov podal osebno privolitev oziroma, ali bo svoje osebne podatke upravljavcu sploh posredoval.

Zbiranje podatkov od drugih oseb ali iz drugih zbirk osebnih podatkov

Če osebni podatki niso bili zbrani neposredno od posameznika, mu mora upravljavec osebnih podatkov ali njegov zastopnik najpozneje ob vpisu ali posredovanju njegovih podatkov uporabniku osebnih podatkov sporočiti podatke o upravljavcu osebnih podatkov in njegovem morebitnem zastopniku (osebno ime, naziv oziroma firma in naslov oziroma sedež) in namen njihove obdelave. V posebnih okoliščinah pa dodatno še:

- informacijo o vrsti zbranih osebnih podatkov;

- navedbo uporabnika ali vrste uporabnikov njegovih osebnih podatkov;

- informacijo o pravici do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja in izbrisa osebnih podatkov, ki se nanašajo nanj.

2.7 Kakšne so dolžnosti upravljavcev osebnih podatkov v zvezi z zavarovanjem osebnih podatkov?

Organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov morajo biti opredeljeni v notranjih aktih organizacij in morajo v prvi vrsti preprečiti nepooblaščeno obdelavo in slučajno ali namerno nepooblaščeno uničevanje in izgubo podatkov ali njihovo spreminjanje. Zato je v

notranjih aktih potrebno predpisati, kako se varujejo prostori, oprema in sistemska programska oprema, kako se varuje aplikativna programska oprema, s katero se obdelujejo, kako se preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, kako se zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov ter kako se omogoča poznejše ugotavljanje, kdaj so bili posamezni podatki vneseni, uporabljeni ali obdelani, kdo je to izvajal in kdaj. Seveda se morajo predpisani postopki in ukrepi tudi dejansko izvajati, zato je treba s temi akti seznaniti vse zaposlene in določiti odgovorne osebe za posamezne zbirke osebnih podatkov in osebe, ki zaradi narave njihovega dela lahko obdelujejo določene osebne podatke.

2.8 Kakšne so pravice posameznika glede njegovih osebnih podatkov?

Upravljavec osebnih podatkov mora na zahtevo posameznika:

1. omogočiti vpogled v katalog zbirke osebnih podatkov;

2. potrditi, ali se podatki v zvezi z njim obdelujejo ali ne, in mu omogočiti vpogled, prepis ali kopiranje njegovih podatkov, ki so vsebovani v zbirki osebnih podatkov;

3. posredovati izpis teh osebnih podatkov,

4. posredovati seznam uporabnikov, katerim so bili ti osebni podatki posredovani, kdaj, na kakšni podlagi in za kakšen namen;

5. dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave;

6. dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;

7. pojasniti tehnične oziroma logično-tehnične postopke obdelave osebnih podatkov posameznika.

Stroške v zvezi z zahtevo in vpogledom krije upravljavec zbirke osebnih podatkov.

Na zahtevo posameznika mora upravljavec njegove osebne podatke tudi dopolniti, popraviti, blokirati ali izbrisati, če posameznik dokaže, da so nepopolni, netočni ali neažurni ali pa so bili zbrani oziroma obdelani v nasprotju z zakonom. To mora upravljavec opraviti v 15 dneh od dneva prejema zahteve. O tem mora obvestiti vlagatelja zahteve ali ga obvestiti o razlogih, zaradi katerih tega ne bo storil. V istem roku mora odločiti o ugovoru. Upravljavec mora na zahtevo posameznika o spremembah in dopolnitvah osebnih podatkov posameznika obvestiti vse druge uporabnike osebnih podatkov in pogodbene obdelovalce, ki jim je posredoval te podatke, razen, če bi to povzročilo velike stroške, nesorazmerno velik napor ali zahtevalo veliko časa. Posameznik ima kadarkoli pravico, da z ugovorom zahteva prenehanje obdelave njegovih osebnih podatkov. Ugovoru se ugodi, če posameznik dokaže, da niso izpolnjeni pogoji za obdelavo.

Posameznik, ki ugotovi, da so kršene njegove pravice iz ZVOP-1, lahko zahteva tudi sodno varstvo. Sodno varstvo lahko zahteva ves čas, dokler kršitev traja, če je kršitev že prenehala, pa lahko v primeru, da mu v zvezi s kršitvijo ni zagotovljeno drugo sodno varstvo, vloži tožbo za ugotovitev, da je kršitev obstajala.

2.9 Kako lahko ukrepam, če so kršene moje pravice do varstva osebnih podatkov oziroma so bili moji osebni podatki obdelovani v nasprotju z zakonom?

Posameznik, ki meni, da so kršene njegove pravice do varstva osebnih podatkov ali da so bili njegovi osebni podatki obdelovani v nasprotju z določbami zakona lahko pri upravljavcu osebnih podatkov na podlagi 30. člena ZVOP-1:

• uveljavlja pravico do vpogleda, prepisa, izpisa ali kopiranja osebnih podatkov, ki se nanašajo nanj,

• zahteva seznam uporabnikov, katerim so bili posredovani njegovi osebni podatki ter pojasnilo o tem, kdaj, na kakšni podlagi in za kakšen namen so bili njegovi osebni podatki posredovani posameznemu uporabniku,

• zahteva informacije o virih, na katerih temeljijo zapisi, ki jih o njem vsebuje zbirka osebnih podatkov in o metodi obdelave,

• zahteva informacije o namenu obdelave in o vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna obvestila v zvezi s tem,

• zahteva pojasnitev tehničnih oziroma logično-tehničnih postopkov odločanja, če se izvaja avtomatizirano odločanje z obdelavo njegovih osebnih podatkov.

Posameznik se lahko v primeru suma kršitev njegovih pravic oziroma v primeru suma kršitve določb zakona vedno obrne tudi na Informacijskega pooblaščenca, ki mu bo v zvezi s tem dal vsa potrebna pojasnila. Če meni, da so kršene njegove pravice iz Zakona o varstvu osebnih podatkov, lahko s tožbo pri Upravnem sodišču Republike Slovenije zahteva sodno varstvo, pri čemer pa je pomembno, da svoje pravice uveljavlja najprej neposredno pri upravljavcu osebnih podatkov. Če je bila posamezniku z nezakonito obdelavo osebnih podatkov povzročena škoda, lahko od povzročitelja po določbah zakona, ki ureja obligacijska razmerja, zahteva tudi odškodnino.

2.10 Kdaj se osebni podatki lahko iznesejo iz države?

Za obdelovalca ali uporabnika osebnih podatkov, s sedežem ali je registracijo v državi članici EU ali EGS veljajo enaki pogoji posredovanja osebnih podatkov kot za subjekte, ki so ustanovljeni in imajo sedež v Sloveniji.

Če pa je upravljavec osebnih podatkov iz tretje, osebne podatke lahko poseduje, če Informacijski pooblaščenec izda odločbo, da država, v katero se osebni podatki iznašajo, zagotavlja ustrezno raven njihovega varstva. Informacijski pooblaščenec vodi seznam tretjih držav, ki imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov, ali pa da varstva nimajo zagotovljenega. Brez predhodne odločitve Informacijskega pooblaščenca pa se osebni podatki lahko iznesejo in posredujejo v tretjo državo, če:

1. tako določa drug zakon ali obvezujoča mednarodna pogodba,

2. je posameznik, čigar osebni podatki se iznašajo, v to privolil,

3. je iznos potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov, ali za izvršitev predpogodbenih ukrepov na zahtevo posameznika, na katerega se nanašajo osebni podatki;

4. je iznos potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjeno med upravljavcem osebnih podatkov in tretjo stranko;

5. je iznos potreben zato, da se zavaruje življenje ali zdravje posameznika, na katerega se nanašajo osebni podatki, pred hujšim ogrožanjem;

6. se iznos opravi iz registrov, javnih knjig ali uradnih evidenc, ki so že po zakonu namenjene zagotavljanju informacij,

7. upravljavec osebnih podatkov zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva, predvsem v določbah pogodb ali v splošnih pogojih poslovanja.

2.11 Kdaj se osebni podatki lahko uporabljajo za namene ponujanja blaga, storitev ali zaposlitev?

Upravljavec lahko v te namene uporablja le tiste osebne podatke, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti. Za neposredno trženje lahko uporablja le osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko ter telefaks številko in elektronski naslov, druge osebne podatke pa le na podlagi izrecne pisne privolitve posameznika. Upravljavec mora posameznika vedno opozoriti, da lahko kadarkoli zahteva, da upravljavec preneha uporabljati njegove osebne podatke za neposredno trženje. Če posameznik to zahteva, je upravljavec dolžan v 15 dneh preprečiti uporabo osebnih podatkov za trženje ter o tem v petih dneh na dogovorjen način obvestiti posameznika, ki je to zahteval.

3. Varstvo osebnih podatkov – delovno okolje

5 zlatih pravil

1. Pravilo = Delodajalec lahko od zaposlenega zbira in nadalje obdeluje le toliko osebnih podatkov, kolikor je to nujno zaradi izvrševanja pravic in dolžnosti iz delovnega razmerja in kar določa zakonodaja

2. Pravilo = Delavec ima tudi na delovnem mestu pravico do zasebnosti, sorazmerno z zakonitim ciljem, ki mu delodajalec sledi.

3. Pravilo = Vsakršno obdelavo osebnih podatkov v okviru delovnega razmerja je potrebno izvrševati kar se da restriktivno, vendar je ni dopustno izsiliti.

4. Pravilo = Za osebne podatke, ki niso zajeti v 1. pravilu, je potrebno pridobiti osebno privolitev zaposlenega, vendar ne z izsilitvijo.

5. Pravilo = Poseg v zasebnost delavca na delovnem mestu je mogoče izvesti le, ko pride do kolizije z neko drugo ustavno pravico in ta v konkretnem primeru prevlada.

1 PRAVILO (obrazložitev)

Zakon o delovnih razmerjih (ZDR) varuje delavca kot šibkejšo stranko v delovnem razmerju z delodajalcem, zato tudi omejuje delodajalca, da zbira zgolj tiste podatke, ki jih nujno potrebuje. Hud poseg v zasebnost delavca bi na primer pomenil, če bi ga delodajalec spraševal o njegovem zdravju, številu otrok (če jih delavec nima zavarovane po sebi), morebitni nosečnosti ipd.Prav tako delodajalec ne sme od osebnega zdravnika delavca ali zdravnika, h kateremu je delavec napoten na službeni pregled, zahtevati, da mu v spričevalu razkriva diagnozo, še manj lahko to zahteva od zaposlenega. Zdravnik lahko izda samo spričevalo, ali je delavec sposoben za opravljanje dela ali ne.Po drugi strani pa ima lahko v določenih primerih tudi delodajalec pravico, da preverja delavca – klasičen primer je detektiv (s katerim mora delodajalec obvezno skleniti pogodbo o pogodbeni obdelavi), ki ugotavlja, ali se delavec na bolniškem dopustu res drži zdravnikovih navodil ali ne. Seveda pri tem brez dovoljenja delavca ne sme vstopiti v stanovanje. Zato imata tako delodajalec kot detektiv pravico od zdravnika izvedeti režim gibanja.

2. PRAVILO (obrazložitev)

Neka ameriška raziskava je ugotovila, da se pri delodajalcih, ki so omogočili svojim zaposlenim nekaj časa za zasebnost na delovnem mestu, bistveno zmanjša število dni izkoriščenega dopusta in bolniškega dopusta.Ljudje večino svojega časa preživimo v službi, ki dejansko postaja naš drugi dom. Nemogoče je torej, da delavec ne bi smel uresničevati svoje pravice do zasebnosti tudi na delovnem mestu. Takšnemu

stališču pritrjuje tudi Evropsko sodišče za človekove pravice, ki je v svojih sodbah v primerih Hallford in Copland proti Združenemu kraljestvu obakrat poudarilo pravico delavca do zasebnosti na delovnem mestu, na vsak nadzor (npr. nadzor nad telefonskimi klici, e-pošto, sledenje z GPS napravami) pa je potrebno delavca vnaprej opozoriti in mu povedati, za kateri namen in v katerih primerih se nek ukrep lahko uporablja. Če se npr. službeni avto uporablja tudi za zasebno uporabo, je potrebno delavcu omogočiti, da napravo po koncu delovnega časa izključi.

3. PRAVILO (obrazložitev)

Delodajalcu ZDR in Zakon o varstvu osebnih podatkov (ZVOP-1) preprečujeta, da bi določila teh dveh zakonov razlagal široko. Načela obeh (predvsem načelo sorazmernosti) mu takšno ravnanje močno omejujeta. Klasičen primer je npr. videonadzor delovnih prostorov, ki se lahko uvede v res izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi. Le redko kateri delodajalec lahko po naših izkušnjah upraviči takšen videonadzor, saj se ti vse prehitro odločajo za uvedbo videonadzora, ki ne ustreza zakonskim zahtevam, pred tem pa ne pomislijo, kakšne posledice jih lahko doletijo (ne le globa pri Pooblaščencu, pač pa tvegajo tudi odškodninsko tožbo in v skrajnem primeru tudi kazensko ovadbo).Podobno velja za uvedbo biometrije pri delodajalcu, ki jo ta lahko uvede, kadar druge možnosti varovanja odpovedo in je dobrina, ki jo delodajalec želi varovati, nekega večjega pomena(npr. trezorji bank, pogosti fizični napadi na zaposlene …). Pri tem je potrebno poudariti, da lahko delodajalec biometrijo uvede le nad svojimi zaposlenimi.

4. PRAVILO (obrazložitev)

Ker je delavec v delovnem razmerju šibkejša stranka, se v praksi pogosto zgodi, da delodajalci delavca izsilijo, da v nekaj privoli. Pooblaščenec takšne primere preiskuje zelo natančno, z zaslišanji prič in izvedbo vseh možnih dokazov. V kar nekaj primerih je že naletel na izsilitev in uvedel prekrškovni postopek.Delodajalec torej veliko tvega, če od delavca izsili privolitev za obdelavo osebnih podatkov. Takšnih primerov v prihodnosti pričakujemo vse več, posebej ob upoštevanju dejstva, da je že sedaj večino prijav, ki jih Pooblaščenec prejme, prav s področja delovnih razmerij.

5. PRAVILO(obrazložitev)

Pravica do zasebnosti, katere del je tudi varstvo osebnih podatkov,je ustavna pravica in je kot takšna lahko omejena le z drugo ustavno pravico, pri čemer je tehtanje med obema pogosto zelo težavno. Npr.: delodajalec ima seveda pravico izvrševati pravice, ki izhajajo iz lastninske pravice, po drugi strani pa mora varovati zasebnost delavca. Izjemno pogost primer, s katerim se srečuje Pooblaščenec, je branje elektronske pošte delavca s strani delodajalca. Nedvomno je potrebno poudariti, da če delavec o možnostih takšnega posega ni bil vnaprej obveščen, bo imel delodajalec več težav z obrazložitvijo posega v službeno elektronsko pošto zaposlenega (zasebni poštni predal – npr. gmail, hotmail, yahoo … je v izključni pravici delavca in delodajalec ne sme pod nobenim pogojem vpogledovati vanj).

Pri tem je nujen dogovor med delodajalcem in zaposlenim, da se vnaprej dogovorita za način uporabe službene elektronske pošte in za pogoje, pod katerimi lahko delodajalec vpogleda v službeno elektronsko pošto zaposlenega. Priporočamo, da se o tem sestavi pisni dogovor, tako, da so pravila vnaprej jasna. Kljub takšnemu vnaprejšnjemu dogovoru pa mora biti poseg v komunikacijsko zasebnost utemeljen za konkreten primer preiskovanja domnevnih kršitev delavca in v skladu z načelom sorazmernosti. To načelo nam pomaga pretehtati, katera pravica je v konkretni situaciji močnejša od druge.

Ko delavec odide iz službe, Pooblaščenec svetuje, da delodajalec in delavec skupaj pregledata računalnik. Tako ima delavec možnost izbrisati ali kopirati svojo elektronsko pošto in druge osebne podatke, delodajalec pa se zavaruje, da delavec ne izbriše službene elektronske pošte.Priporočamo tudi, da ob sumu storitve kaznivega dejanja takoj pokličete policijo, ki bo dokaze, ki se morda nahajajo v e-pošti, zakonito prečrpala z diska (z odredbo sodišča).

3.1 Fotografiranje, nadzor telefonskih klicev

Delodajalci se morajo načela, da lahko zbirajo zgolj tiste osebne podatke, ki jih nujno potrebujejo, držati tudi pri nadzoru zapo-slenih.

Fotografiranje in objavljanje fotografij zaposlenih na (denimo) spletnih straneh je možno zgolj, če zaposleni v to izrecno privoli

– izsiljene privolitve ni mogoče šteti za privolitev.

Glede nadzora uporabe telefona Pooblaščenec opozarja, da delodajalec ne sme kar prosto, preko t. i. razčlenjenega računa, preverjati, koga je zaposleni klical, pač pa mora dati zaposlenemu možnost pojasniti, koliko je bilo službenih in koliko zasebnih klicev, predvsem pa pred tem povedati, kakšen limit porabe ima delavec na konkretni telefonski številki. Najčistejša rešitev v takšnih primerih je, da delodajalec določi vsoto, do katere lahko zaposleni telefonira (enako velja pri zaposlenih, ki uporabljajo službeni mobilni telefon tudi za zasebno uporabo), presežek pa plača zaposleni, razen, če se delodajalec ne strinja z delavčevo obrazložitvijo povečanega obsega klicev za službene namene.

3.2 Preverjanje alkoholiziranosti

Delodajalec ima pravico preveriti, ali je zaposleni pod vplivom alkohola, vendar zgolj z osebno privolitvijo zaposlenega. Če delavec alkotest odkloni, mora delodajalec dejstvo, da je bil zaposleni pod vplivom alkohola, dokazovati na druge načine, npr. s pričami.

3.3 Zbirke osebnih podatkov

Delodajalci morajo voditi evidenco zbirk osebnih podatkov v skladu z Zakonom o evidencah na področju dela in socialne varnosti in ZDR, ter te zbirke ustrezno zaščiti pred nepooblaščenimi dostopi in zaposlenim, ki rokujejo s temi zbirkami, določiti jasne dostopne pravice.

3.4 10 najpogostejših kršitvev ZVOP-1 v delovnih razmerjih

1. Vpogledi v elektronsko pošto zaposlenih in nadzor nad uporabo interneta;
2. pridobivanje zdravstvenih podatkov zaposlenih;
3. nepravilno izvajanje nadzora bolniškega staleža;
4. neutemeljen videonadzor delovnih prostorov;
5. delodajalci zaposlenih pisno ne obvestijo o uvedbi videonadzora;
6. delodajalci ustrezno ne zavarujejo zbirk osebnih podatkov zaposlenih;
7. neutemeljeno sledenje zaposlenim z GPS napravami, mobilnimi telefoni ipd.;
8. neutemeljen nadzor nad telefonskimi klici zaposlenih;
9. delodajalci ne omogočijo delavcu, da se seznani z lastnimi osebnimi podatki;
10. prekomerno zbiranje osebnih podatkov zaposlenih

4. Kako uporabljati FACEBOOK

Vsi se držimo nekaterih pravil glede varnosti in zasebnosti, ki so nam jih že v zgodnjem otroštvu priučili starši: preden prečkaš cesto, poglej v obe smeri; v avtu si vedno pripni varnostni pas; ne govori z neznanci ipd. V obdobju informacijske tehnologije pa je čas, da k seznamu prej navedenih pravil dodamo še eno: Na spletu ne objavljaj nobenih podatkov o sebi, za katere ne želiš, da jih vidi cel svet! Medtem, ko si lahko s pomočjo spletnih družabnih omrežij povečaš krog svojih prijateljev ter se zabavaš s pomočjo različnih zabavnih vsebin, pa z njihovo uporabo hkrati povečaš tudi svojo izpostavljenost osebam z manj prijateljskimi nameni. Več kot imajo taki ljudje na voljo podatkov, več je možnosti, da jih bodo izkoristili na najrazličnejše načine.

Nekateri celo prepričajo nič hudega sluteče naivneže, da se z njimi srečajo osebno, kar lahko povzroči resnično nevarne situacije, še posebej za otroke. »Dodam samo osebe, ki bi jih pozdravila na ulici in morda z njimi rekla kakšno besedo. Ljudi, ki jih sicer poznam, vendar jih ne pozdravljam in ne ogovarjam, pa ne dodajam. Zakaj bi se v virtualnem svetu pretvarjali, da smo prijatelji, če pa v resničnem življenju nismo? V resnivi dodajamo osebe, ki jih v resnici ne poznamo, in tako povečujemo možnost zlorabe svojih osebnih podatkov in vdora v svojo zasebnost.»Pa kaj, če razkrijem svoje osebne podatke?« meni večina. Naj odgovor podamo kar v obliki še enega vprašanja: Kako bi se počutil, če bi učiteljica ali v prihodnosti delodajalec tvoje ime vtipkal v Google, iskalnik pa bi našel tvojo sliko z nore zabave, ki si jo sam (ali pa tvoj prijatelj) objavil na Facebook profilu? Meniš, da bi bil še vedno primeren kandidat za službo, ali si bo delodajalec raje izbral nekoga, z bolj “umirjenim profilom?

4.1 10 nastavitev zasebnosti, ki bi jih moral poznati vsak uporabnik Facebooka

Odstrani se iz Googla

Če ne želiš, da se informacija o tvojem FB profilu prikaže v rezultatih spletnih iskalnikov, sledi naslednjim korakom. Pojdi na »Uporabniški račun« in potem klikni »Nastavitve zasebnosti«.

Levo spodaj pod naslovom Aplikacije in spletne strani klikni na »Uredi nastavitve« ter pri »Javno iskanje« odstrani kljukico pred »Omogočeno javno iskanje«. S tem javni iskalniki ne bodo več prikazali tvojega profila.

Odstrani se iz FB rezultatov iskanj

Če ne želiš, da te lahko na FB najde vsakdo, na strani »Nastavitve zasebnosti«, pod naslovom Povezovanje na Facebook pri »Išči se na Facebooku« nastavitev iz »vsi« spremeni na »samo prijatelji« (to te bo popolnoma umaknilo iz rezultatov iskanja na FB), lahko pa določiš tudi druge skupine, v okviru katerih te uporabniki lahko najdejo pri iskanju – npr. »Prijatelji mojih prijateljev«.

Izogni se zate neprijetnim označenim fotografijam in videom (Tags), da se pojavijo v Novicah (Newsfeed) tvojih prijateljev.

Na strani »Nastavitve zasebnosti« v osrednjem pravokotniku klikni »Uredi nastavitve«. V drugem razdelku (Stvari, ki jih delijo ostali), pod naslovom »Fotografije in videi, v katerih sem označen/a« ustrezno spremeni nastavitev (vsi, prijatelji mojih prijateljev ali samo prijatelji). Če bi rad, da je ves slikovni material, na katerem si označen, popolnoma zaseben in ga lahko vidiš samo ti, izberi možnost »Urejanje« in v prvem razdelku označi »Samo jaz«. Če pa bi rad, da fotografije vidijo le določeni prijatelji, jih lahko izbereš in dodaš pod možnostjo »Določeni ljudje«.

Zaščiti svoje albume

Pogosto uporabniki določijo, da fotografij, na katerih so označeni, določeni prijatelji ne morejo videti, hkrati pa pustijo, da so njihovi albumi še vedno vidni vsem. Če bi rad, da so tvoje fotografije nevidne drugim, moraš to določiti za vsak album posebej. Zasebnost albumov urediš tako, da na strani »Nastavitve zasebnosti« v osrednjem pravokotniku klikneš »Uredi nastavitve«. Na koncu prvega razdelka (Stvari, ki jih delim jaz) klikni na »Uredi zasebnost albumov« in prikažejo se vsi tvoji albumi. Za vsakega posebej lahko določiš, da ga vidijo vsi, prijatelji tvojih prijateljev, zgolj tvoji prijatelji, ali pa pod »Urejanje« nastaviš, da določen album vidiš samo ti oz. zgolj določeni ljudje.

Obdrži svoje kontaktne podatke v zasebnosti

Če želiš omejiti javnost svojih kontaktnih podatkov, na strani »Nastavitve zasebnosti« v osrednjem pravokotniku klikni »Uredi nastavitve«. V tretjem razdelku (Kontaktni podatki) po želji uredi nastavitve..Za vsak podatek lahko narediš posebno nastavitev, tako da prijatelji, s katerimi določenih kontaktov ne želiš deliti, ne morejo npr. videti tvoje telefonske številke. Vsekakor pa priporočamo, da teh podatkov v svoj profil sploh ne vpisuješ.

Prepreči, da se zgodbe o tebi pojavljajo v Novicah (Newsfeed) tvojih prijateljev

Nekateri imajo svoje dejavnosti na FB radi javno vidne, drugi ne, in za slednje velja tale nasvet: če za določeno svojo aktivnost, ki se prikaže tudi na tvojem zidu, ne želiš, da se pojavi v Novicah vseh tvojih prijateljev, tako novico preprosto izbriši s svojega zidu (klikneš križec, ki se prikaže na desni strani objave, ko čez njega zapelješ miško), s čimer bo izginila tudi iz Novic, ki se prikažejo tvojim prijateljem.

Zaščita pred objavljenimi zgodbami iz aplikacij

Ko dodaš kako aplikacijo, se na tvojem profilu običajno takoj znajde novica o tem. Obstaja recimo aplikacija »Have lunch«, ki brez opozorila na tvojem profilu objavi sporočilo »Nick just published to the world that he is having lunch«. Temu se lahko izogneš tako, da ne dodajaš aplikacij ali pa da vsakič, ko kako dodaš, iz svojega profila izbrišeš sporočilo.Nadzoruj, kdo lahko vidi in kdo lahko komentira tvoje objavePoleg tega, da lahko nadzoruješ, kdo vidi tvoj zid in kdo lahko na njem objavlja, lahko nadzoruješ tudi, kdo lahko vidi tvojo posamično objavo. Ko na svojem zidu objavljaš nov status ali novico, se desno pod objavo prikaže ikona ključavnice. S klikom na ikono lahko določenim skupinam prijateljev ali zgolj določeni osebi preprečiš, da vidi to objavo. Lahko pa nadzoruješ tudi, kdo lahko komentira tvoje objave. Če bi rad preprečil določenim osebam, da komentirajo tvoje objave, na strani »Nastavitve zasebnosti« v osrednjem pravokotniku klikni »Uredi nastavitve«. V drugem razdelku (Stvari, ki jih delijo ostali), pod naslovom »Lahko komentira objave« izberi primerno nastavitev.

Obdrži svoj seznam prijateljev zase:

Čeprav je zabavno imeti na stotine prijateljev, je včasih dobro, da seznam tvojih prijateljev ni viden prav vsem. Tako tudi ne more priti do zlorabe tvojega seznama. Nastavitve glede vidnosti liste prijateljev lahko spremeniš na strani »Nastavitve zasebnosti«. Pod naslovom Povezovanje na Facebook pri »See your friend list« lahko nastaviš, da seznam tvojih prijateljev vidijo samo prijatelji tvojih prijateljev, samo tvoji prijatelji ali pa celo samo določene osebe oz. samo ti.

Nadzoruj, katere aplikacije, igre in spletne strani uporabljaš ter katere informacije z njimi deliš

Na strani »Nastavitve zasebnosti« spodaj levo pod naslovom Aplikacije in spletne strani klikni »Uredi nastavitve«. Na tej strani lahko izbrišeš aplikacije, ki jih ne želiš več uporabljati, oziroma omejiš nabor podatkov, ki jih aplikacije zbirajo o tebi.

To je 10 majhnih korakov, kako lahko zaščitiš svojo zasebnost na FB. Vendar pa najboljši nasvet ostaja previdnost in premišljenost. Vsak uporabnik spletnih družabnih omrežij se mora zavedati, da postanejo vsebine, koi jih enkrat objavi na spletu, do določene mere javne in kot take jih lahko uporablja praktično

vsak, ki ima do njih dostop. Če posameznik dostopa do svojega profila ne zaščiti, je odgovornost za zlorabo njegovih podatkov izključno na njegovi strain.

4.2 Prijava zlorabe osebnih podatkov na samem spletnem omrežju

Vedno sam odločaš o tem, katere informacije in slike boš objavil na svojem profilu ter s kom jih boš delil, in sicer preko »Nastavitve zasebnosti«. V primeru, da na svojem profilu ne želiš imeti določenih komentarjev drugih uporabnikov, lahko le-te izbrišeš. V primeru, da meniš, da je neka vsebina na družabnem omrežju v nasprotju s pogoji uporabe takega portala, portali ponujajo možnost prijave zlorabe vsebine.

5. Kraja identitete

Veliko stvari imamo lahko v lasti. Te stvari so lahko kupljene, podedovane ali podarjene, lahko imajo svojo denarno ali pa sentimentalno vrednost. Lahko jih izgubimo, jih podarimo, nam jih zarubijo ali pa celo ukradejo. Ena izmed najbolj osebnih stvari, ki nam jo lahko ukradejo, pa je naša osebna identiteta. Kraja identitete postaja predvsem na podlagi vedno bolj razširjenega virtualnega udejstvovanja posameznikov vse večji problem.

Zadnje desetletje je najhitreje razvijajoča se vrsta kriminala prav kraja identitete. Kriminalec s tujim imenom, naslovom, EMŠO, davčno številko, še bolje pa številko bančnega računa ali kartice, v banki ali pri trgovcu v imenu žrtve bliskovito izvede nekaj finančnih transakcij, si najame posojilo, nakupi blaga za večjo količino denarja, morda vzame kar hipoteko na žrtvino hišo in si na njen račun kupi ali pa si s tem pridobi pravice za npr. vstop v določene prostore. Do številke npr. bančnega računa lahko pride na več načinov, raziskave kažejo, da se kar 46 % tovrstnih kraj zgodi zaradi pozabljene kreditne kartice oziroma kako drugače pridobljenih podatkov o bančnem računu. Tatovi na primer prebrskajo smetišče in na osnovi zavrženih računov pridejo do želenih podatkov. Morda vdrejo v poštni nabiralnik ali pošto preusmerijo na svoj naslov z zahtevo po “začasni spremembi” naslova svoje žrtve, tako pa pridejo podatkov, ki jih potrebujejo za svoje nakane.

PRIMER = Informacijski pooblaščenec je obravnaval primer, ko je nekdo očitno ponaredil podpis posameznika in v njegovem imenu od operaterja zahteval razčlenjeni telefonski račun. Ko je razčlenjeni račun prispel v poštni nabiralnik žrtve, je vanj vlomil in tako pridobil seznam telefonskih številk, ki jih je žrtev pogosto klicala. Nadaljevalo se je z nadlegovanjem družinskih članov, prijateljev in znancev po telefonu, storilca pa policija ni uspela najti. Informacijski pooblaščenec je operaterja kaznoval zaradi malomarnega preverjanja identitete prosilca za razčlenjeni račun, saj se je podpis na faksu očitno razlikoval od ostalih podpisov posameznika, katerega identiteto je prevzel nadlegovalec.

Od leta 1990 je bilo v ZDA, kjer se je tovrstni kriminal “rodil”, že 33,4 milijona žrtev, številka pa se letno povečuje za približno 50 %. Kar 88 % žrtev s tatom svoje identitete ni nikoli imelo nobenega stika, uspeh policije pri lovljenju tovrstnih nepridipravov pa je pičel. Kriminalec moderne dobe svoj podvig izvede v tednu ali dveh in izgine, žrtev pa za prevaro v njegovem imenu izve šele čez čas, ko začno na njegov naslov npr. prihajati praviloma ogromni računi. Preden dokaže nedolžnost in se znebi posledic prevare, minejo meseci, če ne leta, po izračunu strokovnjakov pa vsak oškodovani za “čiščenje” svojega dobrega imena za upravne, varnostne ali detektivske oziroma sodne stroške v povprečju porabi 740 dolarjev. Namen pričujočih smernic je pojasniti, kaj kraja identitete sploh pomeni, katere vrste kraje identitete poznamo, kako je urejena v slovenski zakonodaji, kako tatovi identitet pridobivajo osebne podatke ter kako zavarovati svoje osebne podatke in s tem preprečiti njihovo zlorabo.

5.1 Kaj je kraja identitete?

Kraja identitete je definirana kot uporaba osebnih podatkov oz. identitete nekoga drugega za pridobitev neke koristi ali inkriminacijo druge osebe.Kraja identitete je v Sloveniji z novim Kazenskim zakonikom definirana kot kaznivo dejanje, pri katerem storilec pridobi določene ključne osebne podatke, kot so na primer številke osebnih dokumentov, skupaj z enoznačnimi identifikatorji, kot so v našem pravnem redu EMŠO in davčna številka, za pridobivanje osebne, ne zgolj premoženjske koristi. Škodljive posledice tega kaznivega dejanja namreč ne obsegajo zgolj pridobitve premoženjske koristi, ampak tudi druge koristi (na primer vstop v določene prostore). Kraja identitete pa ima lahko za osebo, katere identiteta je bila ukradena, naslutene posledice, saj se jo lahko okrivi za dejanja, ki jih sama ni storila. Mnoge države, med njimi tudi Slovenija, so zato že sprejele zakonodajo, ki krajo identitete uvršča med kazniva dejanja.

Kraja identitete pomeni posebno vrsto hudega in nepovratnega posega v informacijsko zasebnost oziroma v varstvo osebnih podatkov. Žrtve kraj identitete so lahko prizadete v takšni intenziteti, ki je primerljiva s posledicami drugih nasilnih kaznivih dejanj, ki se nanašajo na življenje in telo ali premoženje. Kraja identitete se namreč ne nanaša le na premoženjski vidik (npr. izpraznjenje bančnega računa, prodaja vrednostnih papirjev …), ampak posega v osebnost žrtve, saj so zabeleženi celo primeri, ko je bila posameznikom odvzeta prostost zaradi suma storitve kaznivega dejanja (predvsem pri kraji biometričnih osebnih podatkov, npr. prstnega odtisa).

S pomočjo različnih načinov pridobitve osebnih podatkov se lahko storilec začne izdajati za nekoga drugega in v njegovem imenu vstopa v različna pravna razmerja (npr. zaposlitev, pridobitev določene izobrazbe, pridobitev osebnih dokumentov …). Kraja identitete torej ni samo zloraba določenega osebnega podatka, saj je vedno povezana vsaj z namenom, da storilec pridobi določeno korist. Pri tem pa ne gre le za pravico do varstva osebnih podatkov, ampak tudi za druge pravice, ki izvirajo iz širše pravice do zasebnosti, denimo varstvo tajnosti pisem in drugih občil – 37. člen Ustave RS. Prizadete so lahko tudi osebnostne pravice, zlasti pravica do osebnega dostojanstva, saj žrtve tega dejanja trpijo zaradi izgube dobrega imena, ugleda, časti oziroma doživljajo stalne čustvene pretrese predvsem zato, ker je kraja določenih osebnih podatkov nepopravljiva (npr. kraja biometričnih osebnih podatkov, kraja enoličnega identifikatorja).

Pri kraji identitete poznamo več vrst napadov:

• glede na osebo, ki izvaja napad (napad lahko izvaja pooblaščena ali nepooblaščena oseba),

• glede na to, ali so podatki ukradeni iz podatkovne zbirke ali med pretokom po omrežju (neposredni napad na shrambo podatkov ali medij za prenos podatkov; obstaja pa tudi možnost kraje podatkov pri skeniranju dokumentov iz analogne v digitalno obliko),

• glede na motiv (finančna kraja identitete, kriminalna kraja identitete in prevzem identitete v vsakdanjem življenju),

• glede na izbrano metodo (poznamo tehnične in ne-tehnične metode)

Identiteto drugega se lahko nezakonito pridobi na različne načine in je odvisna predvsem od splošnega nivoja varstva osebnih podatkov v določeni družbi oziroma pravnem redu. Pripravljalna dejanja za to kaznivo dejanje obsegajo različne vrste kaznivih in nekaznivih dejanj: kraja denarnice z osebnimi dokumenti, prestrežena elektronska sporočila, računalniški virus, t.i. phishing, pharming, pridobitev določenih podatkov s prevaro, celo z iskanjem osebnih podatkov, odvrženih v smeti (dumpster diving) ipd.

Ker sta zloraba osebnih podatkov in kraja identitete v veliki meri povezani z razvojem informacijsko-komunikacijskih tehnologij, v nadaljevanju podajamo razlago najpogostejših načinov za pridobitev osebnih podatkov iz internetnega omrežja.

Ribarjenje (phishing)

Izraz ribarjenje podatkov (phishing) izvira iz angleških besed za geslo (password) in ribarjenje (fishing). Gre za nezakonit način zavajanja uporabnikov, pri katerem poskuša prevarant s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnikov na takšen ali drugačen način izvabiti njihove osebne podatke, kot so: številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila in ostale osebne podatke. Pri tem uporabljajo različne tehnike, ki spadajo v domeno t. i. socialnega inženiringa. Praviloma najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa od vas z lažnim elektronskim sporočilom poskušajo izvabiti bodisi obisk te strani ali kar takoj pridobiti vaše podatke z vašim odgovorom na to sporočilo.

Gre za primer, ko storilec pošlje elektronsko sporočilo, ki je videti na primer kot pravo sporočilo banke. V sporočilu bo pošiljatelj navedel, da je prišlo do problemov z uporabnikovim bančnim računom, zaradi česar ga prosijo, da mu pošlje številko računa oz. uporabniško ime in geslo. V kolikor bi uporabnik na takšno sporočilo odgovoril, bi postal žrtev spletne prevare.

Pharming napadi

Napadi pharming (gre za skovanko med angleškima besedama farming in pharmacy, navezuje pa se na tehniko genetskega inženiringa,v svetu interneta bi lahko govorili o inženiringu naslovov spletnih mest), so za uporabnika zelo nevarni, saj jih je težkoprepoznati. Glavna razlika med phishing-om in pharming-om je v tem, da gre pri pharmingu bolj za tehnični napad kot za tehniko socialnega inženiringa, na katerem temelji ribarjenje podatkov. Praviloma gre bodisi za neposreden napad na DNS strežnike bodisi za napad na določeno datoteko, ki se nahaja na računalniku uporabnika (gre za t.i. datoteko o gostiteljih oz. host file, kjer se nahajajo podatki o URL-jih in domenah). Uporabnik je v teh primerih prepričan, da se nahaja na pravi strani, saj je vtipkal pravi URL naslov strani, v resnici pa ga je eden od omenjenih načinov napada preusmeril na lažne strani, ne da bi se pri tem spremenil URL naslov v oknu brskalnika. Uporabnik je seveda v tem lažnem zaupanju dovolj samozavesten, da vnaša svoje osebne podatke v obrazce, ki se nahajajo na takšnih straneh.

Socialni inženiring

Socialni inženiring je nabor tehnik napadalca za prepričevanje uporabnika ali administratorja sistema, da mu izda avtentikacijske podatke, s katerimi se nato nezakonito prijavi v sistem. Socialni inženiring temelji na t.i. imenovanih kognitivnih odklonih in izkorišča reagiranje ljudi v določenih situacijah (npr. pod pritiskom). Izvajalci socialnega inženiringa s pomočjo obvladovanja veščin prevzemanja identitete drugih ljudi lahko izjemno uspešno pridobijo pomembne podatke. Verjetno najbolj znani hacker, Kevin Mittnick, je slovel ravno po zmožnostih izvabljanja podatkov od ljudi.

Pri socialnem inženiringu so lahko zelo koristna omrežja za spletno druženje (npr. Facebook), kjer ljudje sami od sebe objavljajo številne osebne podatke. ki napadalcu omogočijo boljše poznavanje žrtve in s tem predvidevanje njenega reagiranja.

Virusi in črvi

Virusi so predstavniki škodljive kode, ki živijo znotraj datotek kot so npr. datoteke urejevalnika besedil Word, urejevalnika preglednic Excel in ostalih. Ob odprtju okužene datoteke se virus razširi in okuži ostale datoteke na računalniku.

Črvi so ravno tako samorepliciraj̆oči se programi, ki pa so za razliko od virusov nekoliko bolj inteligentni, saj znajo samodejno iskati primerne tarče za okužbo. Tako črvi kakor tudi virusi prinašajo s seboj breme (payload), ki jim omogoča prevzem nadzora nad okuženim računalnikom, brisanje datotek ali tatvino osebnih podatkov.

Bežen pregled tovrstnega področja nam pove, da se vsak teden pojavi okrog 50novih virusov in črvov. Število virusov in črvov se vsako leto poveča za 400 %, pri čemer postajajo njihovi avtorji/kriminalci vse

bolj inovativni. Tovrstni predstavniki zlonamerne kode so pogosto doma ravno v nezaželenih elektronskih sporočilih (spam), zato je potrebno biti pri odpiranju tovrstne pošte še posebno pazljiv.

Vohunska programska oprema, adware in trojanski konji

Vohunska programska oprema (spyware) je še ena od kategorij škodljive kode. Tovrstni programi se v računalnik naselijo med običajnim brskanjem po internetu, pri čemer za okužbo računalnika izrabijo varnostne pomanjkljivosti internetnega brskalnika (Mozilla, Internet Explorer, Opera ...). Nekateri od teh predstavnikov se v računalnik priplazijo tudi v obliki brezplačnih programov, ohranjevalnikov zaslona, raznih orodnih vrstic in P2P programov za deljenje datotek. Vohunska programska oprema lahko brez vednosti uporabnika spremeni telefonsko številko, na katero kliče modem, preko katerega se uporabnik povezuje v internet. Poleg tega lahko vohunska programska oprema beleži gesla in ostale zaupne podatke ter jih nato pošilja kriminalcem. Eden izmed bolj priljubljenih trikov vohunske opreme je tudi preusmerjanje brskalnika na neželene spletne lokacije, kar napadalcem omogoča vrsto kaznivih dejanj.

Adware je na drugi strani kategorija škodljive kode, ki zbira podatke o uporabnikih in njihovih internetnih navadah. Tovrstni predstavniki škodljive kode sporočajo svoje ugotovitve različnim agencijam, ki uporabnike nato zasipajo z različnimi reklamnimi oglasi in nezaželeno elektronsko pošto.

Vohunska programska oprema in adware se od svojih bratrancev virusov in črvov razlikuje po tem, da se ni sposobna širiti z enega računalnika naprej na ostale računalniške sisteme.

Še ena kategorija škodljivcev pa so trojanski konji, ki se v računalnik pritihotapijo v preobleki legitimnega programa. Ko uporabnik namesti legitimni program, se hkrati namesti tudi trojanski konj, ki napadalcu omogoči prevzem nadzora nad računalnikom.

5.2 Pridobivanje osebnih podatkov s pomočjo kopij osebnih dokumentov

Identiteto drugega se lahko nezakonito pridobi na podlagi dostopa do osebnega dokumenta. Z namenom zaščite osebnih podatkov in s tem preventivnega delovanja proti kraji identitete sta bila v letu 2008 novelirana dva zakona, ki med drugim sedaj urejata tudi kopiranje osebnih dokumentov: Zakon o osebni izkaznici (ZOIzk) in Zakon o potnih listinah (ZPLD). V predhodni ureditvi ni bilo kopiranje niti izrecno dovoljeno niti izrecno prepovedano. Številna podjetja, pa tudi organi iz javnega sektorja, so tako kopirali osebne dokumente po lastnem tolmačenju zakonodaje in svojih obveznosti.

Po izkušnjah Informacijskega pooblaščenca iz opravljenih inšpekcijskih nadzorov se je takšna nejasna pravna ureditev odrazila v številnih zbirkah fotokopij osebnih dokumentov, ki so bile vse prepogosto neustrezno zavarovane in morda zlorabljene v druge namene. Fotokopija osebne izkaznice ali potnega lista namreč uživa relativno visoko zaupanje med ljudmi in kdor se je lahko polastil takšne fotokopije, je vsaj pri poslovanju na daljavo (npr. prek faksa) relativno enostavno prevzel identiteto nekoga drugega.

Kopiranje osebne izkaznice ali potnih listih

Kopiranje osebnih dokumentov je v skladu s tema dvema zakonoma možno samo v primerih, ki jih določa zakon. Ni torej dovolj, da je kopiranje predpisano v podzakonskem aktu ali celo v notranjih pravilih (npr. pravilniku) upravljavca, ne glede na to, ali gre za zasebni ali javni sektor.

Zakon določa, da lahko osebne dokumente poleg njenega imetnika kopirajo notarji in finančne družbe, ki opravljajo finančne storitve, če jo potrebujejo za dokazovanje identitete državljana v konkretnem postopku. Poleg tega pa je kopiranje osebnih dokumentov dovoljeno še na podlagi pisne privolitve posameznika. Upravljavci osebnih podatkov lahko namreč osebne dokumente kopirajo tudi na podlagi pisne privolitve njihovih imetnikov.

Pooblaščenec poziva, da naj upravljavci osebnih podatkov zakonsko določilo, da se osebna dokumenta lahko kopirata za dokazovanje identitete državljana v konkretnem postopku, razlagajo čim ožje. Pri tem naj ne spregledajo niti splošnega načela, da je kopiranje dovoljeno zgolj takrat, ko tako določa zakon, ki mora izrecno dovoljevati tudi kopiranje na podlagi osebne privolitve. Poleg tega je nujno upoštevati tudi načelo sorazmernosti, ki ga opredeljuje ZVOP-1.

Ta v 3. členu določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.

Oznaka na kopijah in prepoved hranjenja kopij v elektronski obliki

Omenjena zakona od upravljavcev osebnih podatkov, ki bodo kopirali osebne dokumente, izrecno zahtevata, da kopijo ustrezno označijo z opozorilom o prepovedi uporabe v druge namene. Zakon ne predpisuje obličnosti vsebine oznake, zato je ta prepuščena upravljavcem osebnih podatkov. Kljub temu Pooblaščenec priporoča, da upravljavci na kopijo napišejo vsaj naslednje podatke:

– da gre za kopijo,

– naziv upravljavca osebnih podatkov,

– namen fotokopiranja in

– pravna podlaga za fotokopiranje (npr. pisna privolitev).

Žig ali vodni žig bosta morala biti postavljena na fotokopijo izkaznice ali potnega lista, kjer je vidna kopija oz. slika izkaznice in ne na bel rob, ki je okoli nje oz. na praznino lista, saj bo drugače mogoče vse ostalo odrezati in fotokopirati izkaznico brez oznak upravljavca.

Pooblaščenec priporoča primer oznake (žiga) na fotokopiji, kot je prikazan na zgornji fotografiji.

5.3 Se kraja osebne identitete dogaja tudi v Sloveniji

Nobenega razloga ni, ki bi nakazoval na to, da je Slovenija kakorkoli imuna na kraje identitete. Nenazadnje, vsake toliko časa slišimo kakšno novico v medijih, v kateri ne gre za nič drugega kot za klasično krajo identitete, le naslovi so pogosto drugačni (npr. »Kradel je telefonske impulze«). Informacijski pooblaščenec se je v praksi že srečal z nekaterimi primeri klasične kraje identitete.

V eni od trgovin, kjer je možno blago kupiti tudi tako, da se vam strošek nakupa obračuna pri mesečnem računu za telefonijo, je neznanka s ponarejenim potnim listom prevzela identiteto druge gospe in v njenem imenu naročila in prevzela več plazma televizorjev. Gospa, katere identiteta je bila ukradena, je bila osupla, ko je prejela mesečni račun, na katerem je bilo za več tisoč evrov dolgov za blago, ki ga ni nikoli kupila. Gospa je morala v trgovini dokazovati, da ni bila ona tista, ki je blago kupila in ga odnesla.

Posebna vrsta kraje identitete, ki je na pomen preverjanja identitete opozorila predvsem operaterja mobilne telefonije, je bil primer, ko so neznanci za nekaj malega denarja prepričali brezdomca, da je sklenil naročniško razmerje pri enem od pooblaščenih agencij za sklepanje naročniških razmerij. Zaradi pehanja po večjem številu naročnikov so novo naročniško razmerje sklenili brez večjih težav, neznanci pa so s pomočjo tako pridobljenega telefona opravili za več tisoč evrov neplačanih klicev v tujino.

Pooblaščenec opozarja na primer kraje identitete, zaradi katerega se je pred kratkim v težavah znašel BBC-jev novinar, ki je obiskal Slovenijo. Pred leti mu je bil ukraden potni list in nato izdan novi. Zaradi ukradenega potnega lista, s katerim je bilo v tujini storjeno kaznivo dejanje, in neažurnega podatka v mednarodno povezanih policijskih zbirkah, je dva dni preživel v priporu v Ljubljani, preden mu je uspelo razjasniti, da ni nič kriv. Gre za zelo nazoren prikaz, kako resne in včasih tudi dolgoročne posledice ima

lahko nespoštovanje načela točnosti in ažurnosti zbirk osebnih podatkov kot temeljnih načel varstva osebnih podatkov, ki bi se jih predvsem morali zavedati organi javnega sektorja. Velikokrat v današnjih časih slišimo argument “Saj nimam kaj skrivati, tu so moji osebni podatki, kar imejte jih!” in tudi evropske raziskave kažejo, da se posamezniki premalo zavedamo pomena posegov v zasebnost z izgovorom, da takšni posegi povečujejo varnost. A če ne zadostimo vsem kriterijem oziroma načelom varstva osebnih podatkov, potem lahko “trpijo” tudi tisti, ki nimajo kaj skrivati. Kraje identitete so možne namreč z mnogimi vrstami osebnih dokumentov in osebnih podatkov, zato bodimo res previdni, kako z njimi ravnamo in kako nanje pazimo.

5.4 Zavarovanje osebnih podatkov, kot ga določa Zakon o varstvu osebnih podatkov (ZVOP-1)

V skladu z 38. členom Ustave RS je zagotovljeno varstvo osebnih podatkov ter prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon, vsakdo pa se ima pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj ter pravico do sodnega varstva ob njihovi zlorabi. To pomeni, da je v skladu z Ustavo RS dovoljena tista obdelava osebnih podatkov, ki je vnaprej predvidena in določno opredeljena v posameznem zakonu.

ZVOP-1 kot temeljni in sistemski predpis s področja varstva osebnih podatkov v 1. točki 6. člena določa, da je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, pri čemer je posameznik določena ali določljiva fizična oseba, na katero se nanaša osebni podatek. Obdelava osebnih podatkov pomeni v skladu s 3. točko 6. člena ZVOP-1 kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje.

24. člen ZVOP-1 določa, da zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se:

1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodnoizhodnimi enotami;

2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;

3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;

4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;

5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatko.

5.5 Prijava kršitev

V teh primerih nemudoma prijavite kršitev:

• vsako tatvino nemudoma prijavite policiji, banki in zavarovalnici. Če ugotovite, da je nekdo odprl bančni račun v vašem imenu, takoj zahtevajte zaprtje računa in ukrepanje organov pregona.

• če nekdo uporablja bančno kartico v vašem imenu, to takoj sporočite izdajateljem, kot so: Visa, Maestro, MasterCard, Diners, American Express itd. Ko boste sporočilo posredovali enemu od naštetih, bo ta takoj opozoril druge izdajatelje. Tovrstna opozorila bodo preprečila odpiranje lažnih računov na vaše ime v prihodnje.

• obrnite se na Informacijskega pooblaščenca, ki bo zoper podjetje, v katerem so bili podatki zlorabljeni ustrezno ukrepal. Varovanje podatkovnih zbirk je namreč zapovedano z ZVOP-1

Zakon o varstvu osebnih podatkov vsebuje številne kazenske določbe, ki določajo globe (denarne kazni) za primere kršitev posameznih določb zakona in s tem vsaj posredno varujejo posameznike pred kršitvami in zlorabami njihovih osebnih podatkov. Pravice posameznika so neposredno ali posredno varovane tudi z zakonskimi določbami o inšpekcijskem nadzorstvu nad izvajanjem določb zakona o varstvu osebnih podatkov. Številne določbe, ki prepovedujejo takšne posege v posameznikovo zasebnost pa, kot že opisano, vsebuje tudi Kazenski zakonik.

Informacijski pooblaščenec kazensko ovadbo zaradi suma storitve kaznivega dejanja zlorabe osebnih podatkov poda v tistih primerih, ko ugotovi, da so izpolnjeni vsi elementi kaznivega dejanja, v ostalih primerih pa na podlagi ugotovljenih kršitev vodi postopek o prekršku.

Kazenski postopek

Zloraba osebnih podatkov iz 4. odstavka 143. člena Kazenskega zakonika (kraja identitete) je kaznivo dejanje, ki se preganja po uradni dolžnosti. V skladu s 146. in 147. členom Zakona o kazenskem postopku lahko vsakdo naznani kaznivo dejanje zlorabe osebnih podatkov iz 4. odstavka 143. člena Kazenskega zakonika tako, da vloži pisno ali ustno ovadbo na pristojno državno tožilstvo ali policij.

6. Spletno nadlegovanje

Slovar besed

Blog - spletni dnevnik oziroma spletna stran, ki jo vzpostavi posameznik zato, da na njej objavlja besedila (svoje misli, novice, zgodbe), fotografije, zvočne ali video posnetke, povezave na strani ...

Takojšnje/neposredno sporočanje ali (ang.) Instant Messaging (npr. MSN Messenger, Skype, Google Talk) - sistem oziroma program za hitro elektronsko komuniciranje med dvema ali več uporabniki. Uporabnik se prijavi in si uredi listo stikov, s katerimi lahko komunicira. Ko se oseba s seznama stikov prijavi v sistem, program uporabnika na to obvesti.

Klepetalnica – javen virtualni prostor za komunikacijo v realnem času. Uporabnik se registrira in lahko komunicira z drugimi uporabniki.

Spletne strani za ocenjevanje ali (ang.) Rating sites (npr. glasujzame.com) - spletne strani, na katerih uporabniki objavljajo npr. svoje fotografije, drugi uporabniki pa glasujejo, katere fotografije se jim zdijo najboljše. Na enak način lahko glasujejo za najljubše profesorje, najlepša dekleta, najbolj butast film ipd.

Sovražni govor - sovražni govor je izražanje mnenj in idej, ki so po svoji naravi diskriminatorna (ksenofobične, rasistične, homofobične in podobno) in uperjene proti različnim manjšinam (etničnim, narodnim, verskim, kulturnim, spolnim in podobno).

Forum – spletna stran, kjer člani s sorodnimi interesi odprto izmenjavajo mnenja o različnih temah.

Registracija za uporabo storitve – če želi oseba postati uporabnik neke storitve na spletu, se mora običajno za to registrirati in ponudniku storitve zaupati svoje (osebne) podatke.

Administrator – skrbnik spletnega mesta oziroma strani. Ob zlorabah ali objavi neprimernih vsebin na spletnem mestu je administrator tisti, ki prejme uporabnikovo pritožbo in poskrbi za odstranitev vsebine.

Nastavitve zasebnosti – nastavitve spletne storitve, omrežja ali spletne strani, ki uporabniku omogočajo, da določi, kdo lahko dostopa do podatkov o njem.

Obvestilo o varovanju zasebnosti – (angl. privacy policy) obvestilo ponudnika spletne storitve o tem, katere podatke o uporabnikih zbira, za kakšen namen, koliko časa jih hrani ... Več v smernicah Informacijskega pooblaščenca na to temo: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/.

Iskalnik (npr. Google, Najdi.si, Yahoo!...) – orodje za iskanje informacij na spletu.

Kraja identitete – kraja osebnih podatkov (npr. imena, naslova, rojstnega datuma, številk kreditnih kartic) in njihova nezakonita uporaba – lažno predstavljanje. Več v smernicah Informacijskega pooblaščenca na to temo: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Uporabniški profil – informacije, ki opisujejo uporabnika storitve ali programa. Običajno vsebujejo uporabniško ime, geslo, lahko tudi druge informacije (npr. datum rojstva).

Nazaželena pošta / spam – elektronska sporočila, običajno komercialne narave, ki jih pošiljatelj masovno pošilja. Običajno jih ponudnik elektronske pošte sam od sebe uvrsti v mapo »Spam« ali »Junk«.

Spletne igre - digitalne igre, ki jih je potrebno igrati z vzpostavljeno internetno povezavo. Lahko jih igra več igralcev hkrati, in ker so na spletu, jih lahko igrajo igralci z različnih lokacij. Igralci si ustvarijo svoje profile, s katerimi nastopajo v virtualnem svetu.

Spletno socialno omrežje (npr. Facebook, Netlog ...) – spletno mesto, virtualno okolje, kjer se zbirajo člani s podobnimi interesi. Člani si najprej ustvarijo svoje profile, nato pa lahko nalagajo besedila, objavljajo slike, komunicirajo z drugimi uporabniki, igrajo igre. Mnogo spletnih socialnih omrežij prepoveduje sodelovanje otrokom, mlajšim od 13 let.

Profil na spletnem omrežju ali spletni strani – osebni podatki uporabnika spletne strani, spletnega omrežja, sistema za takoj-šnje sporočanje, klepetalnice, spletne igre ipd., če želi nekdo uporabljati katero od naštetih storitev, si najprej ustvari svoj profil, v katerem navede podatke o sebi. Ta profil ga nato predstavlja v virtualnem svetu. Profili so lahko javni ali pa uporabnik omeji dostop in lahko profil vidijo le izbrani.

6.1 Kaj je spletno nadlegovanje ?

Spletno nadlegovanje (angl. cyberbullying)[1]označuje nadlegovanje preko interneta, mobilnih telefonov in drugih komunikacijskih sredstev, kjer otrok (ali skupina otrok) nadleguje drugega otroka, tako da mu pošilja grozilna sporočila, ga ponižuje ali drugače sramoti. Primeri metod spletnega nadlegovanja vključujejo:

- ustvarjanje lažnih profilov,
- ustvarjanje sovražnih spletnih strani,
- sovražni govor ter žaljivke,
- zasledovanje uporabnikov na spletu,
- krajo identitete,

[1] Izraz izhaja iz angleškega izraza »cyberbullying«. In čeprav se je v Sloveniji za tako vrsto nadlegovanja uveljavil izraz spletno nadlegovanje, to ne pomeni, da poteka samo prek spleta, ampak preko vseh sodobnih komunikacijskih sredstev.

• objavljanje posnetkov,

• zlorabe osebnih podatkov,

• objavljanje posnetkov, posnetih z mobilnimi telefoni na spletu.

Spletni nadlegovalci žal ne izbirajo sredstev. Uporabljene metode nadlegovanja so omejene zgolj z otroško in mladostniško domišljijo ter njihovo možnostjo dostopa do najrazličnejših sodobnih tehnologij.

Internet in ostale sodobne komunikacijske tehnologije mlade generacije potrebujejo, saj jim ponujajo ogromno možnosti za izobraževanje, raziskovanje in izpopolnjevanje. In tako kot jih v resničnem življenju ne moremo obvarovati v vseh življenjskih situacijah, jim tudi na spletu ne moremo omogočiti popolne varnosti. Lahko pa se naučimo prepoznavati znake spletnega nadlegovanja in mlajše generacije učimo o etiki na spletu ter jim ponudimo koristne napotke, ki naj bodo njihovo vodilo pri aktivnostih na spletu in uporabi sodobnih komunikacijskih sredstev.

6.2 Zakaj je nevarno ?

Zakaj je spletno nadlegovanje lahko še bolj nevarno od nadlegovanja »na igrišču«?

Pojav nadlegovanja med otroki in mladostniki je prisoten že od nekdaj, z razmahom sodobnih tehnologij pa se je nadlegovanje iz šole, igrišč pred blokom in drugih javnih prostorov preselilo na svetovni splet in druga komunikacijska sredstva.

Spletno nadlegovanje se od nadlegovanja »na šolskem igrišču« razlikuje po tem, da ni omejeno na določen čas in prostor.

Spletno nadlegovanje se lahko dogaja 24 ur na dan, 7 dni v tednu in 365 dni v letu, predvsem pa v prostorih, v katere prej nadlegovalci prej niso imeli vstopa. V času, ko svoje mobilne telefone in prenosne računalnike uporabljamo tako rekoč na vsakem koraku, imajo spletni nadlegovalci možnost, da otroka zasledujejo doma, v »varnem« zavetju njegove sobe, mu pošiljajo grozilna sporočila, medtem ko je na družinskem kosilu, ga nadlegujejo med poukom.

Od nadlegovanja v realnem svetu se spletno nadlegovanje razlikuje tudi po obsegu udeležencev. Množica ljudi, ki je povezana s spletnim nadlegovanjem, je lahko zelo velika, oziroma lahko zelo velika postane v zelo kratkem času. Elektronsko sporočilo s fotografijo žrtve nadlegovanja se lahko razširi z neverjetno hitrostjo, predvsem lahko spletni nadlegovalci brez problema ostanejo anonimni, če tako želijo, kar pa predstavljala še večje frustracije za žrtev spletnega nadlegovanja.

V nasprotju z nadlegovanjem »na igrišču«, kjer v večini primerov starejši, večji in močnejši nadlegujejo mlajše, manjše in šibkejše, se v svetu spletnega nadlegovanja vloge lahko zelo hitro menjajo. Žrtev lahko (npr. iz maščevanja) že v naslednjem trenutku postane nadlegovalec. Dosedanji nadlegovalec pa lahko kaj hitro sam postane žrtev spletnega nadlegovanja.

6.3 Vzroki

Ali poznamo vzroke spletnega nadlegovanja?

Do spletnega nadlegovanja lahko pride iz podobnih razlogov kot do vsakega drugega nadlegovanja: zaradi jeze, potrebe po maščevanju, zaradi zavisti, z namenom opozoriti nase, želje po moči in oblasti, opozarjanja na svoj socialni status, ipd. Do spletnega nadlegovanja lahko pride tudi zaradi dolgčasa ali preprosto iz zabave, pa tudi zaradi tega, ker imajo otroci in mladostniki pogosto nenadzorovan in neomejen dostop do takšnih in drugačnih tehnoloških igračk. Nekateri primeri nadlegovanja so sprva lahko mišljeni kot nedolžna šala, vendar pa se v naslednjem trenutku lahko sprevržejo v hudo nočno moro za žrtev. Lahko so zgolj posledica nepremišljenosti - otrok zapiše o sošolcu na spletu nekaj informacij, to sporočilo pa kar naenkrat postane predmet posredovanja in je poslano na ogromno število spletnih naslovov. Ker se od primera do primera razlikujejo motivi spletnega nadlegovanja, se razlikujejo tudi odgovori in rešitve za vsak posamezen primer.

6.4 Kako poteka ?

Nadlegovanje lahko poteka v obliki neposrednih ali posrednih napadov. Neposredno napadanje pomeni, da napadalci sporočila pošiljajo neposredno otroku - žrtvi, posredni napadi pa potekajo preko drugih oseb, ki se svoje vloge posrednika lahko zavedajo ali pa tudi ne.

6.5 Neposredni napadi

Nadlegovanje prek takojšnjega sporočanja in SMS sporočil

Otroci lahko drugim otrokom pošiljajo grozilna sporočila, neprimerne fotografije in drug material preko programov za takojšnje sporočanje, SMS sporočil ipd. Lahko ustvarijo tudi lažen profil na kateri od spletnih mest ali socialnih omrežij, ki omogoča takojšnje sporočanje. Uporabijo malce spremenjeno ime otroka (namesto ime.priimek@mail.com uporabijo priimek.ime12@mail.com), ki ga nadlegujejo, se pretvarjajo, da so ta otrok in v njegovem imenu nadlegujejo druge.Na enega otroka se lahko spravi cela skupina otrok, ki mu pošilja veliko število SMS sporočil z grozilno ali žaljivo vsebino. Napadeni tako lahko hitro prejme 1000 SMS sporočil z grdo vsebino. Če operater zaračunava dohodna SMS sporočila, pa je tak napad za prejemnika lahko tudi zelo drag. Take vrste nadlegovanje je izjemno lahko izvedljivo, otroci pa se običajno ne zavedajo, da čeprav grožnje niso izrečene iz oči v oči, taka sporočila žrtev kljub temu prizadenejo in so zelo resna stvar.

Kraja gesel

Otrok lahko zlorabi geslo drugega zato, da se npr. na socialnem omrežju pretvarja, da je ta otrok in pod pretvezo komunicira z drugimi, njegovimi prijatelji, jih žali in jezi. Ti pa sploh ne vedo, da ne komunicirajo s pravo osebo, ampak z nekom tretjim. Z zlorabljenim geslom lahko otroci na spletni strani ali profilu drugega objavljajo neprimerne fotografije s seksualno, rasistično ali drugo vsebino, ki lahko žali druge. Pogosto z ukradenim geslom otroku preprečijo dostop do njegovega lastnega računa elektronske pošte ali profila na spletnem omrežju. Ukradeno geslo pa je v končni fazi lahko v pomoč tudi hekerjem, ki ga uporabijo za to, da vdrejo v žrtvin računalnik.

Blogi

Blogi so spletni dnevniki in otroci jih lahko uporabljajo zato, da z drugimi delijo svoje zgodbe, si pošiljajo sporočila in objavljajo fotografije. Prav tako pa jih lahko uporabljajo tudi zato, da v njih obrekujejo druge otroke in objavljajo stvari iz njihovega zasebnega življenja, jih žalijo in ponižujejo. Otroci lahko ustvarijo blog ali spletno stran prav z namenom nadlegovanja drugega.

Spletne strani

Včasih so si otroci nagajali na igrišču, zdaj za to lahko uporabljajo svetovni splet. Na spletu lahko ustvarjajo strani, na katerih ponižujejo druge otroke, jih zasmehujejo in drugače nadlegujejo. Objavljajo lahko osebne podatke otrok, slike in druge podrobnosti iz njihovega zasebnega življenja. Taka množica objavljenih informacij pa lahko žrtev nadlegovanja spravi tudi v resno nevarnost, saj vsak, ki obišče stran, ve kdo je, kako izgleda, kje živi, kaj dela.

Pošiljanje fotografij preko elektronske pošte in mobilnih telefonov

Pošiljanje in objavljanje fotografij drugih oseb v nerodnih situacijah, pomanjkljivo oblečenih ipd. je še en način nadlegovanja. Težava s tako e-pošto je, da zelo hitro zaokroži med velikim številom najstnikov in jo je nemogoče kontrolirati. Kaj lahko se znajde tudi na različnih spletnih straneh, kjer fotografije lahko vidi praktično vsak. Prav tako že skoraj vsak mobilni telefon omogoča fotografiranje, kar olajša pošiljanje fotografij, predvsem pa omogoča skrivno slikanje drugih – v popolnoma zasebnih ali kočljivih situacijah, npr. v slačilnicah, kopalnicah ipd. Škoda, ki jo s tem utrpi najstnik ali otrok, je lahko nepopravljiva.

Ankete na spletu

Kdo je kul in kdo ni? Kdo je največja kmetica v šestem razredu? Taka in podobna vprašanja se lahko znajdejo na spletnih anketah, ki jih zelo preprosto z brezplačnimi aplikacijami na spletu sestavijo najstniki in otroci. Vprašanja so hitro lahko žaljiva in tudi na ta način otroci lahko nadlegujejo druge na spletu.

Interaktivne igre

Veliko otrok in mladostnikov igra video igre preko igralnih konzol, obstajajo pa tudi interaktivne igre na spletu. Hkrati z igranjem lahko mladi komunicirajo med sabo, tekmujejo ipd. V tekmovalnem vzdušju hitro pride do verbalnih napadov na druge tekmovalce, uporabe žaljivega jezika, groženj, preklinjanja. Stvar lahko pripelje celo do tega, da določenega tekmovalca izločijo iz igre, vdrejo v njegov igralni račun, razširjajo o njem govorice …

Pošiljanje zlobnih kod in virusov

Žrtvam spletnega nadlegovanja otroci lahko pošiljajo viruse in druge zlobne programe, z namenom, da poškodujejo žrtvin računalnik ali pa, da za njo s pomočjo virusov vohunijo.

Pošiljanje neprimernih vsebin (pornografija) in spama

Nadlegovalci lahko žrtvin elektronski naslov zlorabijo tako, da ga vpišejo na listo prejemnikov novic z določene strani, npr. s pornografsko ali drugo neprimerno vsebino. Žrtev bo tako prejela ogromno število elektronskih sporočil, poslanih s te strani, in rešitev je običajno lahko le sprememba elektronskega naslova.

Zloraba identitete

Veliko škode lahko žrtvi povzročijo nadlegovalci, ki se pretvarjajo, da so ona. V žrtvinem imenu objavljajo komentarje na spletnih forumih in omrežjih, žalijo druge in tako povzročijo, da se lahko cela skupina mladih obrne proti žrtvi, čeprav ni ničesar kriva.

7. Viri

https://www.ip-rs.si/publikacije/prirocniki-in-smernice/

http://en.wikipedia.org/wiki/Identity_theft

http://e-uprava.gov.si/e-uprava/dogodkiPrebivalci.euprava?zdid=632

http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html

https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu-samo-za-mlade/

8. Zaključek

Torej ta tema varstvo oosebnih podatkov je bila dosedaj v času mojega šolanja daleč najbolj obširna in lahko bi napisal še 100 strani če bi hotel ampak sem jih izpustil ker se mi niso zdele pomembne. Prav tako nisem dodal veliko slike ker ni bilo časa. Torej upam da je naloga narejena dobolj dobro.