

Projektno delo z negospodarskim in neprofitnim sektorjem –
Študentski inovativni projekti za družbeno korist 2016 – 2018

Projekt

SOCIALNI INŽENIRING - NEVARNOST SODOBNE DRUŽBE

Elaborat

Študenti:

Urban Ažman, Turizem I, FKPV

Ana Bastelj, Turizem I, FKPV

Michele Kovač, Management inf. in
elektronskega poslovanja II, EPF

Ana Ocvirk, Predšolska vzgoja, PF

Ana Peterka, Interdisciplinarni študijski
program rač. in matematika,

Patricija Potisk, Turizem I, FKPV

Taja Savić, Bibliotekarstvo, inf. znanost
in knjigarstvo, FF

Mentorji in drugi sodelavci:

doc. dr. Tatjana Kovač, pedagoški
mentor I, Poslovna informatika, FKPV

doc. dr. Tatjana Dolinšek, pedagoški
mentor II, Komerciala, FKPV

mag. Petra Vovk Škerl, pedagoški
mentor III, Turizem, FKPV

dr. Franci Čeč, strokovni sodelavec,
Inštitut za coaching

Katja Špegelj dipl. ekon. (VS),
podporno strokovno osebje FKPV

KAZALO VSEBINE

1 PREDSTAVITEV PROJEKTA	5
1.1 Utemeljitev in povzetek vsebinske zasnove	5
1.1.1 <i>Utemeljitev iz prijave projekta</i>	5
1.1.2 <i>Utemeljitev z vidika študentov</i>	6
1.2 Problem	6
1.2.1 <i>Problem iz prijave projekta</i>	6
1.2.2 <i>Problem z vidika študentov</i>	7
1.3 Aktivnosti.....	8
1.4 Vključeni mentorji in študenti	8
2 PREDSTAVITEV PODROČIJ	9
2.1 Coaching	9
2.1.1 <i>Teoretična izhodišča</i>	9
2.1.2 <i>Modeli coachinga.....</i>	9
2.1.3 <i>Lastnosti coacha.....</i>	10
2.2 Socialni inženiring	10
2.2.1 <i>Teoretična izhodišča</i>	10
2.2.2 <i>Stopnje socialnega inženiringa</i>	11
2.2.3 <i>Vrste socialnega inženiringa</i>	11
2.2.3.1 <i>Človeško osnovani napadi.....</i>	11
2.2.3.2 <i>Računalniško osnovani napadi</i>	12
2.2.3.3 <i>Varnost</i>	14
3 RAZISKAVA	15
3.1 Predstavitev raziskave in metodologija	15
3.2 Kvalitativna raziskava – globinski intervjuji	15
3.3 Kvantitativna raziskava – anketa.....	16
3.3.1 <i>Vzorec</i>	16
3.3.2 <i>Rezultati.....</i>	17
3.3.3 <i>Prvi sklop vprašanj.....</i>	17
3.3.4 <i>Tretji sklop vprašanj.....</i>	21

3.3.5	<i>Drugi sklop vprašanj</i>	25
4	PROGRAM ZA KREPITEV RAZUMEVANJA SOCIALNEGA INŽENIRINGA	32
5	JAVNA PREDSTAVITEV IZSLEDKOV	34
6	ZAKLJUČEK	34
7	VIRI IN LITERATURA	35
8	PRILOGE	36

KAZALO TABEL

Tabela 1: Varovanje osebnih podatkov preko E-pošte.....	25
Tabela 2: Varovanje osebnih podatkov preko telefona	26
Tabela 3: Kaj storim po uporabi dokumentov, stare računalniške opreme, koledarjev ipd., ko jih več ne potrebujem?	29
Tabela 4: Zaupljivost osebi, ki se izdaja za uradno osebo	30

1 PREDSTAVITEV PROJEKTA

Javni štipendijski, razvojni, invalidski in preživninski sklad Republike Slovenije je objavil javni razpis Projektno delo z negospodarskim in neprofitnim sektorjem - Študentski inovativni projekti za družbeno korist 2016 – 2018, ki ga delno financira Evropska unija iz Evropskega socialnega sklada. Predmet javnega razpisa je bilo sofinanciranje projektov, ki se izvajajo v skupinah od 6 do 10 študentov pod mentorstvom pedagoškega mentorja in strokovnega sodelavca iz lokalnega/regionalnega okolja. V okviru projektov študenti proučujejo različne kreativne in inovativne rešitve za izzive negospodarskega in neprofitnega sektorja.

Fakulteta za komercialne in poslovne vede je v partnerstvu z Inštitutom za coaching prijavila projekt Socialni inženiring - nevarnost sodobne družbe, v katerega je bilo pri izvedbi poleg mentorjev in strokovnih sodelavcev iz omenjenih partnerskih organizacij vključenih sedem študentov iz različnih slovenskih fakultete in različnih stopenj študija. Projekt v skupni vrednosti 14.264 € je trajal od 1.6.2017 do 30.9.2017, ugotovitve pa bodo implementirane tako v učne načrte kot tudi v poslovno prakso partnerskih organizacij.

1.1 Utemeljitev in povzetek vsebinske zasnove

1.1.1 Utemeljitev iz prijave projekta

Inštitut za coaching je zavod, ki usposablja posameznike, da z uporabo posebnih metod sprožijo lastni miselni proces ter tako hitro dosežejo odlične rezultate. Inštitut svojim slušateljem iz Posavja zagotavlja tudi znanja s področja poslovnih tveganj, vendar področja socialnega inženiringa še ne vključuje v dovolj velikem (želenem) obsegu. Socialni inženiring namreč kot tehnika prevare tako posameznike kot tudi organizacije spravlja v slabši položaj, zato je razumevanje tega področja izjemno pomembno.

V Inštitutu do sedaj še niso naredili poglobljene raziskave glede razumevanja socialnega inženiringa v lokalnem okolju ter posledic in tveganj, ki jih lahko nerazumevanje področja prinese v življenje posameznikov ali v prakso delovanja podjetij. Izsledki takšne raziskave bi pripomogli k boljšemu prepoznavanju segmentov, na katere se mora s svojim delovanjem osredotočiti Inštitut. Zato bodo to primarno raziskavo z verodostojno analiziranimi rezultati kot vmesni cilj projekta izvedli študentje pod mentorstvom pedagoških mentorjev ter na osnovi izsledkov pripravili program za krepitev razumevanja socialnega inženiringa in z njim povezanih tveganj, kar je končni cilj projekta. Na osnovi slednjega bo partnerska

organizacija lahko svojim slušateljem iz Posavja zagotavlja več vsebin s področja socialnega inženiringa. Rezultat bo pripravljen v obliki elaborata in javno predstavljen.

Z izvedbo projekta pridobijo vsi deležniki. Študenti praktično spoznajo področji coaching in socialni inženiring. Organizacija, dobi informacijo o stopnji razumevanja področja in program za krepitev razumevanja področja, kar lahko kasneje uporabi pri svoji politiki delovanja. FKPV okrepi sodelovanje z gospodarstvom ter pridobljene vsebine vključi v svoj kurikulum. Okolje na osnovi aktivnosti tekom trajanja projekta in po njem bolje razume področje in z njim povezana tveganja.

1.1.2 Utemeljitev z vidika študentov

Smo študentje različnih fakultet z vse Slovenije. S Fakulteto za komercialne in poslovne vede sodelujemo v projektu, v okviru katerega raziskujemo seznanjenost ljudi s socialnim inženiringom. V projektu je zajet pojem socialnega inženiringa in rešitve, kako se pred njim ubraniti. Socialni inženiring pomeni uporabljanje vpliva in prepričevanja z namenom zavajanja ljudi, da verjamejo, da je socialni inženir nekdo, ki to ni, ali z manipulacijo. Posledica tega je, da lahko socialni inženir izkoristi ljudi tako, da od njih pridobi informacije z ali brez uporabe tehnologije. Z zlorabo zaupanja, z uporabo socialnih veščin oziroma psiholoških tehnik, kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva ipd., pridobi od žrtve osebne podatke (najpogosteje ime, priimek, št. transakcijskega računa, razna gesla, EMŠO, št. potnega lista ...) in jih uporabi za pridobivanje večinoma premoženjske koristi-izsiljuje, grozi).

Poleg opisa problema in rešitev, kako se ubraniti pred socialnim inženiringom, smo ustvarili anketo za pridobitev podatkov. Na podlagi odgovorov smo naredili analize, ki nam povedo, kako pomembno je, da se ljudje ozaveščamo o tovrstnih napadih.

1.2 Problem

1.2.1 Problem iz prijave projekta

Socialni inženiring predstavlja nevarnost sodobne družbe, predvsem manjša lokalna okolja, saj četudi ni povezan izključno z napadi na informacijske sisteme, je njegov razmah v zadnjem obdobju prav zaradi razvoja in pomena informacijskih sistemov izjemno povečan.

Tako za posameznike kot tudi za delovanje podjetij je pomembno, da je zavedanje omenjenega tveganja oziroma razumevanje socialnega inženiringa na dovolj visoki ravni.

Inštitut bi za boljše prepoznavanje ciljnih segmentov, ki potrebujejo svetovanje na področju nevarnosti socialnega inženiringa na področju Posavja, potreboval poglobljeno raziskavo glede razumevanja socialnega inženiringa ter posledic in tveganj, ki jih lahko nerazumevanje področja prinese v življenje posameznikov ali v prakso delovanja podjetij, vendar v Inštitutu nimajo niti ustrezne programske opreme niti metodološkega znanja, da bi takšno raziskavo lahko izvedli in rezultate verodostojno obdelali. Zato bodo to primarno raziskavo izvedli študentje pod mentorstvom pedagoških mentorjev ter na osnovi izsledkov pripravili program za krepitev razumevanja socialnega inženiringa.

Ob podpori pedagoških mentorjev, ki so strokovnjaki za ekonomijo in metodološko področje (PM2) oziroma vodenje (PM3) ter področje poslovne informatike oziroma novih tehnologij (PM1), bodo študenti zasnovali in izvedli primarno raziskavo razumevanja socialnega inženiringa, analizirali rezultate ter predstavili izsledke v obliki elaborata. Ob podpori strokovnega sodelavca bodo spoznali področje coaching oziroma delovanje partnerske organizacije. Na osnovi izsledkov bodo pripravili program za krepitev razumevanja socialnega inženiringa za posamezne segmente. Rezultat bo pripravljen v obliki elaborata in javno predstavljen. Tako s samo raziskavo kot tudi z javno predstavitvijo izsledkov se bo prispevalo k boljšemu razumevanju obravnavanega področja v širši javnosti.

1.2.2 Problem z vidika študentov

V današnjem času podjetja oziroma organizacije razpolagajo s številnimi informacijami in različnimi podatki o podjetju in zaposlenimi, zato morajo z njimi ravnati učinkovito, spoštljivo in skrbno. Ustrezno varovanje podatkov zmanjšuje poslovna tveganja na skoraj vseh področjih in prispeva k uspešnosti in vrednosti zaupanja podjetja. V projektu je predstavljen socialni inženiring in napotki o tem, kako se mu ubraniti.

Največji problem je pomanjkanje ozaveščenosti zaposlenih in organizatorjev, saj ti lahko hitro postanejo žrtve teh napadov.

1.3 Aktivnosti

V sklopu projekta smo začeli sodelovati in ustvarjati junija 2017. Dobili smo vsa gradiva in še v istem mesecu opravili globinske intervjuje z gospodom Čečem, ki nam je še enkrat na kratko opisal in predstavil pojem socialnega inženiringa ter povsem odvisno temo socialnega inženiringa, tj. coaching. Izvedli smo tako kvantitativno kot tudi kvalitativno raziskavo, ki smo jo obdelovali večinoma od doma in v knjižnici Fakultete za komercialne in poslovne vede, v Sevnici, Radečah ter na terenu. Potrebna je bilo dosti medsebojnega usklajevanja. Julija smo pripravljali vprašanja za ankete, zbirali nove informacije in se na podlagi odgovorov intervjuja odločali za ustrezna vprašanja pri sestavi anket. Ankete smo začeli pošiljati v mesecu avgustu preko skupne elektronske pošte na naslove, ki smo jih iskali na spletni strani Bizi.si za Spodnje-posavsko regijo. Septembra 2017 smo vse podatke, pridobljene iz anket, uredili v Excellovo tabelo in dokončali raziskovalno delo ter pripravili program za krepitev razumevanja socialnega inženiringa.

Mentorice s FKPV so študentom nudile podporo na svojih strokovnih področjih, strokovni sodelavec iz organizacije, Inštituta za coaching, je zagotovil dostop do potrebnih podatkov v organizaciji in lokalnem okolju ter zagotovil podporo pri izvajanju globinskih intervjujev v lokalnem okolju.

1.4 Vključeni mentorji in študenti

V projekt je bilo vključenih 8 študentov iz različnih fakultet po Sloveniji:

- Urban Ažman, Turizem I, FKPV
- Ana Bastelj, Turizem I, FKPV
- Michele Kovač, Management informatike in elektronskega poslovanja, EPF
- Ana Ocvirk, Predšolska vzgoja, PF
- Ana Peterka, Interdisciplinarni študijski program računalništvo in matematika,
- Patricija Potisk, Turizem I, FKPV
- Taja Savič, Oddelek za bibliotekarstvo, informacijsko znanost in knjigarstvo, FF

Podporo so nudili mentorji in ostali sodelavci:

- doc. dr. Tatjana Kovač, pedagoški mentor I, Poslovna informatika, FKPV
- doc. dr. Tatjana Dolinšek, pedagoški mentor II, Komerciala, FKPV
- mag. Petra Vovk Škerl, pedagoški mentor III, Turizem, FKPV
- dr. Franci Čeč, strokovni sodelavec, Inštitut za coaching
- Katja Špegelj dipl. ekon. (VS), podporno strokovno osebje FKPV

2 PREDSTAVITEV PODROČIJ

2.1 Coaching

2.1.1 Teoretična izhodišča

Coaching predstavlja pomoč posamezniku, da doseže poslovne cilje. Pri coachingu sodelujeta coach in klient, predvsem pa je pomembno, da posameznik (klient) za doseg ciljev uporablja lastne zunanje in notranje vire. Notranji viri so npr. samozavest, strokovno znanje in sposobnosti, zunanji pa oprema, denar in čas. Pri tem ga coach le usmerja (<http://www.rcr-zasavje.si/uploads/files/Coaching.pdf>).

Coaching je pravzaprav sredstvo za doseganje rezultatov, izboljšanje načina in učinkov dela (<https://books.google.si/books?h>). Pogosto ga zamenjujemo z mentorstvom, vendar med pojmom obstajajo razlike. Mentor je navadno starejši sodelavec z dolgoletnimi izkušnjami, ki svetuje in usmerja sodelavce (<http://www.rcr-zasavje.si/uploads/files/Coaching.pdf>), vendar je mentorstvo včasih tudi spontana vloga, coaching pa je profesionalna dejavnost, ki jo izvaja ustrezno usposobljena oseba: coach (<https://www.amazon.co.uk/Critical-Introduction-Coaching-Mentoring/dp/1446272281>).

Značilnosti coachinga so torej ustvarjalen in akcijski pristop k težavi, učinek na podjetje je neposreden, je aktualen in se ne ukvarja s preteklostjo, coach ni nujno izkušen, navadno je individualen in ne usmerja klientov. Coaching je učinkovit in v podjetjih izboljša in zviša raven dela ter prinaša trdne spremembe. Prinaša tudi mnogo koristi za podjetja, saj coaching med drugim prispeva tudi k boljši komunikaciji med zaposlenimi, poveča konkurenčnost in dobiček podjetja ter poskrbi za profesionalni razvoj zaposlenih (<http://www.rcr-zasavje.si/uploads/files/Coaching.pdf>).

2.1.2 Modeli coachinga

Čeč (<http://www.rcr-zasavje.si/uploads/files/Coaching.pdf>) navaja dva modela coachinga: »Grow« in »ADAPT«.

Model grow uporabljamo takrat, kadar želimo identificirati težavo, način reševanja in razlago ciljev. Coach svojemu klientu pomaga, da najde rešitve in se samostojno odloča. Skupaj si zastavita cilj, ki ga želi klient doseči, razpravljata o trenutnih razmerah in realnih možnostih za razrešitev težav ter se pogovorita o možnih dejanjih.

Za model ADAPT je značilno delovanje v petih korakih: ocena trenutnega stanja, razvoj plana, delo na konkretnem planu, kontrola plana, povej in vprašaj (pogovor o napredku).

2.1.3 Lastnosti coacha

Veščine uspešnega coacha so prepoznavanje pomena govornice telesa in uporaba le-te, saj lahko preko telesne govornice sporočamo tudi to, česar nismo nameravali, prav tako pa coach ustvarja spodbudno okolje z obvladanjem svoje govornice telesa. Tako tudi gradi zaupanje s klientom, kar pozitivno vpliva na odnos in uspešno doseganje ciljev.

Aktivno poslušanje je prav tako ena izmed veščin, pri kateri je pomembno, da coach sliši tudi neizrečeno in je pozoren tudi na ton in barvo glasu, saj tudi to predaja nebesedna sporočila. Glede na slišano coach postavlja vprašanja, zato je dobro, da zna zastaviti ustrezna vprašanja, ki so problemsko naravnana in usmerjena v prihodnost, v razreševanje težav (<http://www.rcr-zasavje.si/uploads/files/Coaching.pdf>).

Zelo pomembna kompetenca coacha je tudi strokovno znanje, ki mu omogoča dobro profesionalno delovanje. Selan Kure (http://www.revija.zzsp.org/pdf/SocPed_2014-3-4.pdf) navaja še druge značilnosti, ki bi morale označevati coacha: »dostopnost, toplina, sprejemanje, strpnost, veščine dobrega sporočanja in poslušanja, sposobnost izražanja empatije, kreativnost, prilagodljivost pri kreiranju idej, zavzetost k napredovanju in doseganju rezultatov, odprtost do klientovih reakcij, bistroumnost, poznavanje sebe, razumevanje lastnih močnih in šibkih točk, omejitev in priložnosti« (http://www.revija.zzsp.org/pdf/SocPed_2014-3-4.pdf).

2.2 Socialni inženiring

2.2.1 Teoretična izhodišča

Socialni inženiring je usmerjanje nekoga ali nečesa, da lahko dosežemo rezultate, ki so nam v korist (Hadrnag, 2011). Prav tako zajema komunikacijo in načine manipuliranja z ljudmi v vsakdanjih situacijah. Socialni inženiring lahko uporabljajo že otroci, učenci ter odrasli v svojih poklicih, z namenom pridobiti določene ugodnosti. Zanj je značilna zloraba zaupanja, manipulacija in uporaba psiholoških tehnik (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

Socialni inženiring je pravzaprav tehnika pridobivanja informacij, do katerih socialni inženir nima dovoljenja dostopati. Informacije so lahko digitalne, saj so tovrstni napadi navadno usmerjeni na informacijske sisteme, lahko pa so tudi v ustni ali pisni obliki (<https://dk.um.si/lzpisGradiva.php?lang=slv&id=30242>).

2.2.2 Stopnje socialnega inženiringa

Socialni inženiring vsebuje 4 stopnje, ki pa so med seboj povezane. Po zaključenih štirih stopnjah se lahko krog še enkrat ponovi, z razširitvijo kakšne stopnje ali pa izpustitvijo. Te so:

– *Zbiranje informacij*

Ta korak mora biti izveden najbolj kakovostno, saj je od kakovosti podatkov odvisen uspeh socialnega inženirja. Inženir poskuša pridobiti čim več informacij o osebi ali podjetju (načini varovanja, infrastrukturni načrt ...);

– *Vzpostavitev odnosa*

Naslednji korak je uporaba zbranih informacij z namenom, da z žrtvijo razvije odnos in da mu žrtev začne zaupati. Inženir uporabi različne psihološke tehnike, manipulacijo in uporablja svoje igralske sposobnosti, da v žrtvi vzbudi zaupanje;

– *Izkoriščanje odnosa*

V tem koraku žrtev izda podatke, ki jih inženir želi pridobiti;

– *Izvršitev zastavljenega cilja*

Socialni inženir v zadnjem koraku doseže svoj cilj, saj uporabi podatke, ki jih je pridobil od žrtve. Lahko so njegov cilj že sami podatki (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

2.2.3 Vrste socialnega inženiringa

2.2.3.1 Človeško osnovani napadi

Socialni inženir je v neposredni interakciji s svojo žrtvijo, da pridobi želene informacije.

- *Neposredni pristop*

Napadalec navadno le vpraša po podatkih, ki jih želi izvedeti. Vendar je za takšno tehniko potrebna dobra priprava. Socialni inženir se lahko pretvarja, da je študent, ki izvaja ankete, da je novi zaposleni, ki potrebuje pomoč in tako dobi gesla, ali pa se pretvarja, da je tehnična pomoč in na takšen način dobi gesla in druge osebne podatke (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

- *Prisluškovanje*

Socialni inženir brez pooblastila posluša, ali bere zaupna sporočila, kjer dobi želene podatke (Singh Patel, 2013).

- *Gledanje čez ramo*

Socialni inženir preprosto opazuje žrtev, ko vpisuje svoje podatke, na primer pri plačevanju s karticami ali pri dvigovanju denarja na bankomatih (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

- *Obratni socialni inženiring*

Socialni inženir se pretvarja, da je oseba na višjem položaju. S svojo zaigrano avtoriteto preprosto vpraša po podatkih in podrejeni mu navadno brez vprašanj podatke tudi posredujejo (Singh Patel, 2013).

- *Brskanje po smetnjakih*

V koših za smeti lahko socialni inženir najde koristne podatke, ki jih zavržemo, ne da bi jih pred tem ustrezno zaščitili in uničili. To je lahko tudi računalniška oprema, zunanji nosilci podatkov, zavrženi dokumenti (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

2.2.3.2 Računalniško osnovani napadi

Socialni inženir uporablja računalniške programe, da pridobi želene informacije.

- *Ribarjenje (phishing)*

Ime te tehnike je skovanka iz angleških besed password (geslo) in fishing (ribarjenje). Socialni inženir s pomočjo lažnih sporočil ali spletnih strani poskuša dobiti osebne podatke žrtve, s katerimi lahko dosega do npr. bančnega računa. Socialni inženir lahko pošlje elektronsko sporočilo, ki je videti verodostojno in nas vabi, da vpišemo določene osebne podatke. Če to storimo, te podatke dobi socialni inženir in jih zlorabi (Singh Patel, 2013).

- *Pojavna okna*

Pojavna okna, ki se odprejo, kadar smo povezani z medomrežjem, nas vabijo, da kliknemo na povezavo, ki nas preusmeri na spletno stran socialnega inženirja. Tam želijo, da vpišemo osebne podatke ali pa na računalnik naložimo program, ki pa lahko vsebuje viruse (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

- *Spletni iskalniki*

S pomočjo spletnih iskalnikov lahko socialni inženir sam poišče naše podatke, ki so dosegljivi na spletu. Skoraj vsak podatek, ki ga inženir dobi, mu lahko koristi. Včasih so ti podatki lahko zgolj podatki o naših interesih in hobijih, vendar lahko spretni socialni inženirji tudi tovrstne podatke uporabijo v svojo korist (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

- *Socialna družabna omrežja*

Ko si na družabnem omrežju ustvarimo profil, prostovoljno objavimo veliko podatkov o sebi. Zato so družabna omrežja lahka tarča za inženirje, saj lahko zgolj z brskanjem pridobijo veliko število podatkov, ki jih potem izkoristijo (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

- *Pharming napadi*

Ime izvira iz angleških besed farming in pharmacy, označuje pa tehnični napad, kjer napadalec z računalniškimi programi preusmeri uporabnike na lažne strani. Na lažnih straneh nato uporabniki z zaupanjem vpisujejo svoje podatke, saj ne vedo, da v tistem trenutku ne uporabljajo varne in zaupljive spletne strani (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

- *Virusi*

Virusi, črvi in trojanski konji so vrsta napadov, kjer lahko prevzamejo datoteke na naših računalnikih, nam onemogočajo dostop in brišejo datoteke. Najdemo jih lahko v datotekah med vsiljeno pošto, zato moramo biti previdni pri odpiranju sporočil, ki so videti sumljiva (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf).

Socialni inženiring se lahko izvaja tudi preko telefona, kjer inženir pokliče v podjetje in z različnimi psihološkimi tehnikami pridobi podatke.

2.2.3.3 Varnost

Pri zavarovanju pred socialnim inženiringom je pomembna tehnična oprema, kot so antivirusni programi in ostale zaščite, ki nam zagotavljajo tehnološko varnost, vendar je predvsem pomembna varnost pred osebnimi napadi. Pri tovrstnih napadih so lahko inženirji uspešnejši, saj s psihološkimi zvijačami preprosto prevarajo človeka. Zato je pomembno, da poznamo tehniko, ki nam lahko pomaga pri prepoznavanju napada in nato prilagodimo odziv. Priporočeno je, da pomislimo na:

- Legitimnost: ali se nam zdi, da so zahteve oz. vprašanja, ki nam jih postavljajo primerne in običajne?
- Pomembnost: ali so informacije, ki jih želijo pridobiti od nas, pomembne in imajo veliko težo?
- Vir: ali je mogoče vir zahteve preveriti?
- Odzivnost: ali si lahko vzamete čas za premislek, preden odgovorite oz. ukrepate (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf)?

3 RAZISKAVA

3.1 Predstavitev raziskave in metodologija

3.2 Kvalitativna raziskava – globinski intervjuji

Globinski intervjuji so bili izvedeni v Sevnici in Radečah, 12. 9. 2017. V globinskih intervjujih so sodelovali trije direktorji različnih ustanov in podjetij. Študenti, ki sodelujemo v projektu Socialni inženiring, smo poskušali ugotoviti, ali izpraševanci vedo, kaj pomeni »socialni inženiring« in v kolikšni meri so seznanjeni z obravnavano tematiko. Pri globinskih intervjujih je bil prisoten tudi naš mentor g. Franci Čeč.

Vsakemu izmed njih so bila postavljena štiri glavna vprašanja:

- Kaj je socialni inženiring?
- Ste se že kdaj srečali z njim?
- Kakšne tehnike socialnega inženiringa poznate?
- Kako bi se ubranili pred socialnim inženiringom?

1. Direktorica knjižnice v Sevnici

Zataknilo se je pri razumevanju pomena besede »socialni inženiring«, saj je direktorica mislila, da naj bi to predstavljalo delo z računalniki in da se deli med uporabniki in zaposlenimi na dve mreži. Ob razlagi definicije socialnega inženiringa je direktorici tematika bila poznana. Pojasnila nam je, da gesla piše knjižničar in da jih menjajo vsako leto, da vodijo evidenco uporabnikov in da gesla zapisujejo ali označijo pod »zapomni si« na računalniku. Direktorica se še ni srečala s socialnim inženiringom, se je pa srečala s krajo identitete na Facebooku. Dokumente dajo v razrez, pisarne zaklepajo samo zvečer, nimajo kamer, ne varnostnika. Meni, da sta rešitvi antivirusni program, saj jo računalnik opozarja na škodljivo e-pošto, in izvedba izobraževanj za zaposlene. Imajo zunanjega serviserja, ki je s pogodbo zavezan k varovanju podatkov, prav tako kot ostali zaposleni. Direktorica je mnenja, da je tematika vedno bolj aktualna in pomembna.

2. Direktor nevladnega socialnega podjetja

Direktor se je seznanil z izrazom »socialni inženiring« pred dvema letoma na konferenci. Vedel je, da gre za osebe, ki se »predstavljajo« in da podatke kradejo iz nenavadnih podjetij. Je mnenja, da lahko socialni inženiring postane velik problem, še posebej v zdravstvu. Pravi, Socialni inženiring - nevarnost sodobne družbe

da moramo paziti na to, kaj objavljamo na spletu. Skrbi ga predvsem sinhronizacija med napravami. Negativnih izkušenj ni imel, vendar je pazljiv pri odpiranju datotek in e-pošte. Neke posebne zaščite na računalniku nima. Njihovi prostori niso posebej zavarovani s kamerami ali varnostniki, ker nimajo svojih poslovnih prostorov. Ima pa zaščiteno mrežo, ki jo uporablja pri delu. Tema se mu zdi pomembna in dodal je, da se morajo tega problema zavedati predvsem močnejša podjetja, da se premalo zavedamo groženj in da se je potrebno ustrezno zaščititi.

3. Direktor zasebnega podjetja

Direktor zasebnega podjetja sprva ni razumel izraza »socialni inženiring« oz. je podal napačno razlago, saj je govoril o ljudeh in si razlagal vsako besedo posamično. Ko smo mu pojasnili pojem socialnega inženiringa je zadevo razumel in povedal, da je imel veliko osebnih izkušenj na to temo, npr. ukraden dostop do spletne trgovine. Prepričan je, da je potrebno veliko vložiti in delati na zaupanju med zaposlenimi in lojalnosti v podjetju, saj s tem pridobiš reference. Direktorji se morajo zavedati, da so študentje bolj mobilni od redno zaposlenih. Poudaril je, da se moramo paziti socialnih omrežij, saj tudi če se zdi, nič ni zastonj. Njegova rešitev je postaviti in organizirati računovodski servis, ki bi skrbel za varnost, kot tudi za informiranje ljudi o morebitnih nevarnostih.

3.3 Kvantitativna raziskava – anketa

3.3.1 Vzorec

Na podlagi podatkov iz globinskega intervjuja smo oblikovali anketni vprašalnik, ki smo ga poslali različnim podjetjem v Spodnjem Posavju, saj smo želeli podatke iz področja dela g. Čeča. Populacijo so predstavljala podjetja, ki imajo objavljen e-naslov v bazi Bizi.si, pri čemer smo uporabili selektivno iskanje (samo podjetja iz regije Spodnje Posavje). Anketni vprašalnik smo oblikovali v spletni obliki (s pomočjo orodja Google dokumenti) in ga poslali na spletne naslove podjetij. Odgovorilo je 58 podjetij, kar predstavlja 6,4 % celotnega vzorca. V anketnem vprašalniku smo postavili tri vsebinske sklope vprašanj (skupaj 34 različnih vprašanj) na temo socialnega inženiringa ter coachinga.

V nadaljevanju prikazujemo zbirne podatke in rezultate, podrobnejši podatki pa so razvidni iz priloge. Za obdelavo podatkov smo uporabili MS Excel. Iz razvidnih rezultatov razberemo, koliko ljudi ukrepa ob tem problemu in nevednost problema.

3.3.2 Rezultati

Anketni vprašalnik je bil sestavljen iz 21 vprašanj, ki so bila razdeljena na tri sklope. Prvi sklop se nanaša na varovanje podatkov s strani anketirancev, drugi sklop so bila demografska vprašanja, tretji sklop pa se nanaša na podatke o tem, kako podjetja skrbijo za varnost.

V anketi je sodelovalo 58 anketirancev, 12 (20,7%) je bilo moških, 46 (79,3%) pa žensk. Glede na stopnjo izobrazbe jih ima največ, kar 16% srednješolsko oz. gimnazijsko izobrazbo, nato jim sledijo tisti, ki imajo univerzitetno oz. visokošolsko izobrazbo.

Povprečna starost anketiranih je 34 let (SD = 12 let). Najmlajši je bil star 20 let, najstarejši pa 65 let. Najpogostejša starost je bila 23 let, polovica anketirancev pa je starih do 31,5 let.

Področja dela anketirancev so bila vodstveni kader, tehnično osebje in ostala področja dela.

Vprašanja so bila razdeljena v 1., 2. in 3. sklop. Nekaj je bilo tudi demografskih vprašanj.

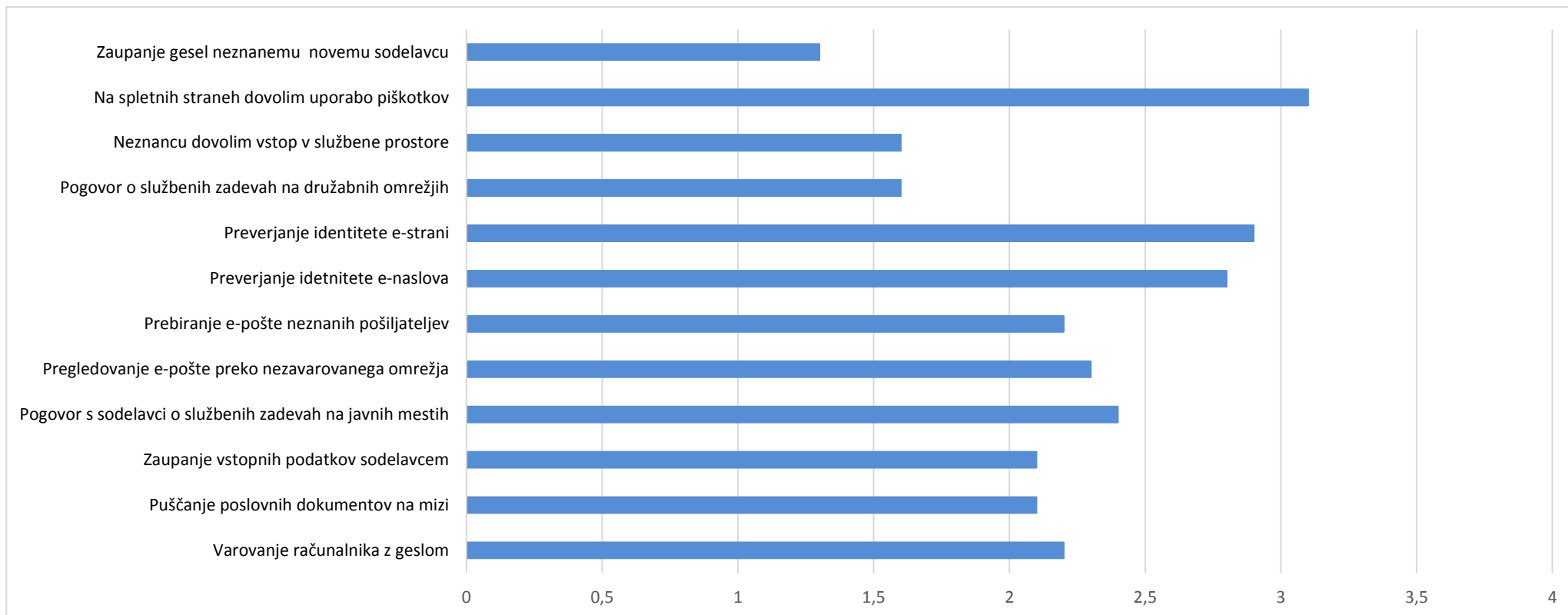
Anketiranci so v 1. in 3. sklopu vprašanj odgovarjali z odgovori Likartove lestvice, kar smo spremenili v številčne spremenljivke. Poleg glavnih podatkov smo izračunali tudi aritmetično sredino in standardni odklon.

V 2. sklopu vprašanj so odgovori opisnih spremenljivk, kjer smo vsako vprašanje posebej označili s komentarjem in grafom. Podrobnejši tabelarni in grafični prikaz je v prilogi, v nadaljevanju pa opisujemo zgolj povzetek ugotovitev.

3.3.3 Prvi sklop vprašanj

Vprašanja se nanašajo na varovanje podatkov na delovnem mestu, in sicer nas je zanimalo, kako anketiranci pripomorejo k diskretnosti podatkov v podjetju. V prvem sklopu vprašanj so bili ponujeni odgovori z: VEDNO (DA), POGOSTO PREJ DA KOT NE, REDKO PREJ NE KOT DA in NIKOLI. Vprašanja smo spremenili v številčne spremenljivke, pri čemer smo odgovor VEDNO (DA) spremenili v vrednost 1, vprašanje NIKOLI pa v vrednost 4.

	Vedno (da)		Pogosto prej da kot ne		Redko prej ne kot da		Nikoli		M	SD
	Število	Odstotek	Števil o	Odstotek	Število	Odstotek	Števil o	Odstote k		
Vprašanja 1. sklop										
Varovanje računalnika z geslom	9	15,50%	13	22,40%	18	31%	18	31%	2,2	1,1
Puščanje poslovnih dokumentov na mizi	4	6,90%	13	22,40%	25	43,10%	16	27,60%	2,1	0,9
Zaklepanje pisarne v krajši odsotnosti	0		0		0		0			
Zaupanje vstopnih podatkov sodelavcem	5	8,60%	12	20,70%	27	46,60%	14	24,10%	2,1	0,9
Pogovor s sodelavci o službenih zadevah na javnih mestih	3	5,20%	22	37,90%	29	50%	4	6,90%	2,4	0,7
Pregledovanje e-pošte preko nezavarovanega omrežja	5	8,60%	17	29,30%	26	44,80%	10	17,20%	2,3	0,9
Prebiranje e-pošte neznanih pošiljateljcev	4	6,90%	14	24,10%	27	46,60%	13	22,40%	2,2	0,8
Pred vnašanjem zaupnih podatkov preverim identiteto e-naslova	17	29,30%	18	31%	19	32,80%	4	6,90%	2,8	0,9
Pred vnašanje zaupnih podatkov preverim identiteto spletne strani	19	32,80%	16	27,60%	19	32,80%	4	6,90%	2,9	1,0
Pogovor o službenih zadevah na družabnih omrežjih	1	1,70%	9	15,50%	13	22,40%	35	60,30%	1,6	0,8
Neznancu dovolim vstop v službene prostore	2	3,40%	4	6,90%	21	36,20%	31	53,40%	1,6	0,8
Na spletnih straneh dovolim uporabo piškotkov	20	34,50%	26	44,80%	10	17,20%	2	3,40%	3,1	0,8
Neznanemu novemu sodelavcu po potrebi zaupam dostopna gesla	1	1,70%	2	3,40%	8	13,80%	47	81%	1,3	0,6



V raziskavi smo ugotovili:

- največ anketirancev, to je 18 (31,3 %), nikoli ne zavaruje svojega računalnika z geslom, 9 anketirancev (15,5 %) pa ga zavaruje. Povprečna ocena trditve je 2,2 (SD = 1,1);
- da 43 % anketirancev praviloma ne pušča dokumente na delovni mizi, ko zapustijo delovni prostor, 7 % pa jih pušča dokumente na mizi. Povprečna ocena trditve je 2,1 (SD = 0,9);
- da na vprašanje, ali anketiranci vedno zaklenejo svoje delovne prostore v krajši odsotnosti, ni odgovoril nihče (SD = 0,9);
- večina anketirancev 27 (46,6 %) po navadi ne zaupa vstopnih podatkov sodelavcem, le 8,6 % pa vedno zaupa. Povprečna ocena trditve je 2,1 (SD = 0,7);
- da se anketiranci večinoma pogovarjajo s sodelavci o službenih zadevah na javnih mestih. 37,9 % jih je odgovorilo, da se po navadi pogovarjajo in le 5,2 %, da se nikoli ne pogovarja s sodelavci na javnih mestih o službenih zadevah. Povprečna ocena trditve je 2,4 (SD = 0,9);
- da 26 (44,8 %) anketirancev po navadi ne pregleduje svoje e-pošte preko nezavarovanega omrežja, 8,6 % pa naj bi to počelo vedno. Povprečna ocena trditve je 2,3 (SD = 0,8);
- da je večina anketirancev izbrala pri vprašanju o varni uporabi e-pošte odgovor REDKO PREJ NE KOT DA (46,6 %), najmanj pa odgovor VEDNO (DA), 6,9 %. Povprečna ocena trditve je 2,2 (SD = 0,9);
- da se je ekvivalentno število anketirancev, 19 (32,8 %) odločilo za odgovora VEDNO (DA) in REDKO PREJ NE KOT DA na vprašanje, ali anketiranci pred vnosom zaupnih podatkov preverijo identiteto spletne strani. Samo 4 so izbrali odgovor NIKOLI. Povprečna ocena trditve je 2,9 (SD = 1,0);
- da je večina (60,3 %) na vprašanje, ki se je navezovalo na pogovor o službenih zadevah na družabnih omrežjih, odgovorila, da se o tem nikoli ne pogovarja, samo en udeleženec je izbral odgovor VEDNO (DA). Povprečna ocena trditve je 1,6 (SD = 0,8);
- da 31 (53,4 %) anketirancev nikoli ne dovoljuje vstop neznancem v službene prostore, le dva jih vedno spuščata. Povprečna ocena trditve je 1,6 (SD = 0,8);
- da 44,8 % pogosto ne dovoljuje uporabe piškotov na spletnih straneh, le 3,4 % pa jih nikoli ne dovoljuje. Povprečna ocena trditve je 3,1 (SD = 0,8);

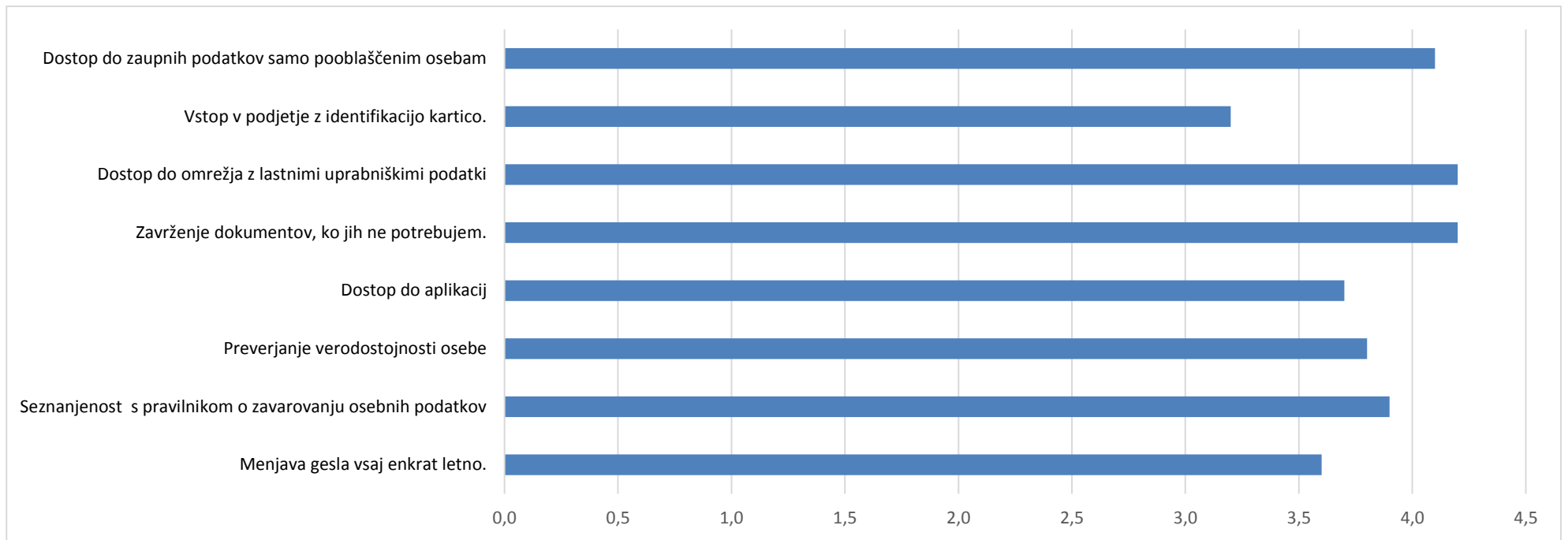
- da je kar 81 % (47 oseb) odgovorilo, da nikoli ne zaupa dostopnih gesel neznanemu novemu sodelavcu, samo eden je izbral odgovor VEDNO (DA). Povprečna ocena trditve je 1,3 (SD = 0,6).

Iz prvega dela analize ugotavljamo, da so anketiranci večino trditev ocenili z oceno več ko 2, kar pomeni, da so na 4–stopenjski lestvici izbrali nikalne trditve. To nakazuje na nižjo raven varnosti osebnih podatkov, kar je razvidno tudi iz zgornjega grafa.

3.3.4 Tretji sklop vprašanj

Tretji sklop vsebuje osem vprašanj, ki ponujajo naslednje odgovore: POPOLNOMA VELJA, VELJA, NITI NE VELJA NITI VELJA, NE VELJA, SPLOH NE VELJA in NE MOREM ODGOVORITI, KER TRENUTNO NISEM ZAPOSLEN. Vprašanja smo prekodirali v številčne spremenljivke, pri čemer smo odgovor POPOLNOMA VELJA prekodirali v vrednost 1, vprašanje NE MORE ODGOVORITI, KER TRENUTNO NISEM ZAPOSLEN pa v vrednost 6.

Vprašanja 3. Sklop	Popolnoma velja		Velja		Niti ne velja niti velja		Ne velja		Sploh ne velja		Ne morem odgovoriti, ker trenutno nisem zaposlen		M	SD
	Št.	Odstotek	Št.	Odstotek	Število	Odstotek	Število	Odstotek	Število	Odstotek	Število	Odstotek		
Menjava gesla vsaj enkrat letno.	18	31,0%	10	17,2%	9	15,5%	5	8,6%	6	10,3%	10	17,2%	3,6	1,4
Sem seznanjen s pravilnikom o postopkih in ukrepih za zavarovanje osebnih podatkov.	16	27,6%	16	27,6%	12	20,7%	4	6,9%	1	1,7%	9	15,5%	3,9	1,0
Vem, kako preveriti verodostojnost osebe, preden ji posredujem zaupne podatke.	11	19,0%	20	34,5%	14	24,1%	4	6,9%	0	0,0%	9	15,5%	3,8	0,9
Dostopam lahko samo do aplikacij/programov/podatkov, s katerimi upravlja moj oddelek.	14	24,1%	21	36,2%	2	3,4%	6	10,3%	5	8,6%	10	17,2%	3,7	1,3
Ko določenih dokumentov, stare računalniške opreme, koledarjev ipd. ne potrebujem več, jih ustrezno zavržem (fizično uničenje, izbris podatkov, razrez).	20	34,5%	21	36,2%	4	6,9%	3	5,2%	1	1,7%	9	15,5%	4,2	0,9
Do službenega internetnega omrežja lahko dostopam le z lastnimi uporabniškimi podatki.	24	41,4%	16	27,6%	2	3,4%	4	6,9%	2	3,4%	10	17,2%	4,2	1,1
V podjetje lahko vstopam le z identifikacijsko kartico oziroma z jasno identifikacijo.	13	22,4%	11	19,0%	6	10,3%	9	15,5%	9	15,5%	10	17,2%	3,2	1,5
Do prostorov, kjer so hranjeni zaupni podatki (arhiv) ali pomembna oprema (strežnik), imajo dostop samo pooblaščenice osebe.	20	34,5%	17	29,3%	7	12,1%	4	6,9%	0	0,0%	10	17,2%	4,1	0,9



V raziskavi ugotavljamo:

- da je 10 anketirancev skoraj pri vseh vprašanih odgovorilo z NE MOREM ODGOVORITI, KER TRENUTNO NISEM ZAPOSLEN;
- da 18 anketirancev (31 %) menja geslo v podjetju vsaj enkrat letno, 5 oseb (8,6 %) pa gesla ne menjava tako pogosto. Povprečna ocena trditve je 3,6 (SD = 1,4);
- da je 16 udeležencev anketiranja seznanjenih s pravilnikom o postopkih in ukrepih za zavarovanje osebnih podatkov, samo en ni seznanjen. Povprečna ocena trditve je 3,9 (SD = 1,0);
- da največ oseb (34,5 %) preveri verodostojnost osebe, preden ji posredujejo zaupne podatke, najmanj (6,9 %) pa se je odločilo za odgovor odgovora NE VELJA. Odgovora SPLOH NE VELJA ni izbral nihče. Povprečna ocena trditve je 3,8 (SD = 0,9);
- da 21 (36,2 %) anketirancev lahko dostopa samo do aplikacij/programov/podatkov, s katerimi upravlja njihov oddelek, samo dva pa sta izbrala odgovor NITI NE VELJA NITI VELJA. Povprečna ocena trditve je 3,7 (SD = 1,3);
- da 21 (36,2 %) oseb zavrže (fizično uničenje, izbris podatkov, razrez) določene dokumente/staro računalniško opremo/koledarje ..., ko jih več ne potrebuje, le en pa tega ne stori. Povprečna ocena trditve je 4,2 (SD = 0,9);
- da lahko do službenega internetnega omrežja dostopa le z lastnimi uporabniškimi podatki 24 (41,4 %) anketirancev, najmanj jih je pa ekvivalentno izbralo odgovora NITI NE VELJA NITI VELJA in SPLOH NE VELJA. Povprečna ocena trditve je 4,2 (SD = 1,1);
- da samo 13 (22,4 %) anketiranih lahko v podjetje vstopa le z identifikacijsko kartico oziroma z jasno identifikacijo, 15,5 % pa lahko vstopa brez identifikacije. Povprečna ocena trditve je 3,2 (SD = 1,5);
- da je na vprašanje: "Do prostorov, kjer so hranjeni zaupni podatki (arhiv) ali pomembna oprema (strežnik), imajo dostop samo pooblaščen osebe", 20 anketirancev (34,5 %) odgovorilo s POPOLNOMA VELJA, samo štirje (6,9 %) pa so izbrali odgovor NE VELJA. Nihče ni izbral odgovora SPLOH NE VELJA. Povprečna ocena trditve je 4,1 (SD = 0,9).

V tretjem delu analize je bila aritmetična sredina več kot 3, kar na 5–stopenjski lestvici

pomeni, da navedene trditve BOLJ NE DRŽIJO, KOT PA DRŽIJO. Moramo pa seveda upoštevati, da je 10 ljudi odgovorilo z NE MOREM ODGOVORITI, KER TRENUTNO NISEM ZAPOSLEN, kar pa je zvišalo aritmetično sredino. Rezultati so razvidni iz zgornjega grafa.

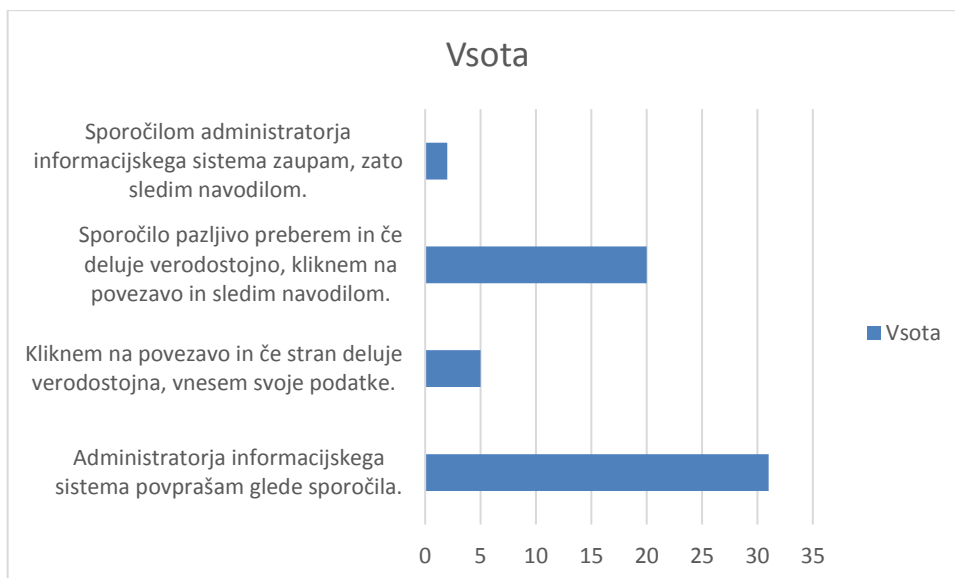
3.3.5 Drugi sklop vprašanj

Vmesni sklop vprašanj je sestavljen iz 6 vprašanj, kjer se sprašujemo po varnosti odpiranja e-pošte, identifikaciji, menjavi gesel in odvečnih zaupnih stvari. Vsako vprašanje ima različne odgovore, zato smo vsakega posebej opisali s komentarji in grafi.

Prvo vprašanje: Prejeli ste e-pošto od administratorja informacijskega sistema bančne ustanove. Od vas zahteva, da zaradi sprememb v sistemu sledite poslani povezavi in vnesete svoje uporabniško ime in geslo. Kaj storite?

Tabela 1: Varovanje osebnih podatkov preko E-pošte

Odgovori	%	Števil o
Administratorja informacijskega sistema povprašam glede sporočila.	53,4%	31
Kliknem na povezavo in če stran deluje verodostojna, vnesem svoje podatke.	8,6%	5
Sporočilo pazljivo preberem in če deluje verodostojno, kliknem na povezavo in sledim navodilom.	34,5%	20
Sporočilom administratorja informacijskega sistema zaupam, zato sledim navodilom.	3,4%	2
Skupna vsota	100,0%	58



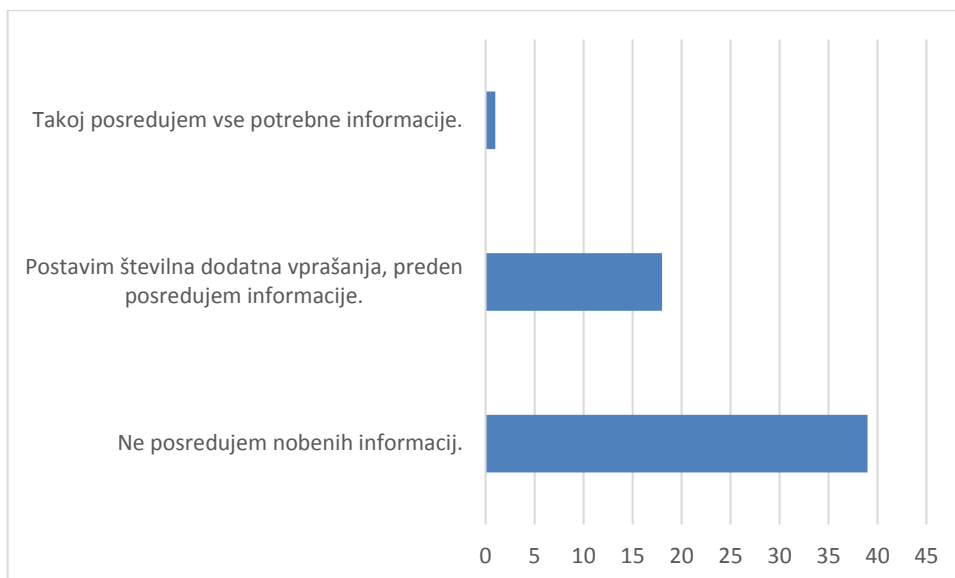
Graf 1: Varovanje osebnih podatkov preko E-pošte

Največ anketirancev je odgovorilo na vprašanje »Administratorja informacijskega sistema povprašam glede sporočila«, in to kar 31 (53,4%). Najmanj anketirancev (2) pa takoj zaupa in sledi navodilom (3,4%).

Drugo vprašanje: Prejeli ste klic osebe, ki trdi, da je iz neke organizacije, kjer ste zmagali na natečaju. Tega natečaja se ne spominjate, a ker se redno prijavljate na nagradne igre, mislite, da ste prav danes imeli srečo. Klicatelj vam sporoči, da ste osvojili velik znesek in potrebuje vaše podatke.

Tabela 2: Varovanje osebnih podatkov preko telefona

Odgovori	%	Število
Ne posredujem nobenih informacij.	67,2%	39
Postavim številna dodatna vprašanja, preden posredujem informacije.	31,0%	18
Takoj posredujem vse potrebne informacije.	1,7%	1
Skupna vsota	100,0%	58



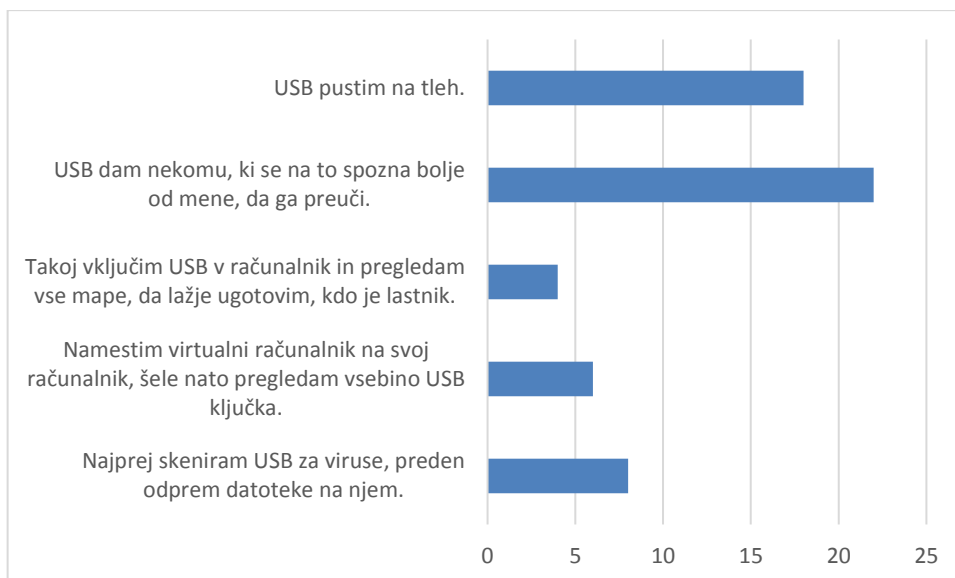
Graf 2: Varovanje osebnih podatkov preko telefona

Na vprašanje o zasebnosti podatkov preko telefona je največ anketirancev odgovorilo, da podatkov ne posredujejo 39 (67,2 %), le eden je odgovoril, da informacije pošlje takoj. Ostalih 18 (31 %) pa se vedno prepriča o pristojnosti vprašanj in želenih odgovorov, preden posreduje informacije.

Tretje vprašanje: Medtem, ko hodite proti vhodu v službo/šolo, vidite na tleh USB ključek. Na njem ni ničesar, kar bi vam lahko pomagalo identificirati lastnika. Zavedate se, koliko dela bi lahko šlo v nič, če ga je nekdo izgubil. Kaj naredite?

Tabela: 20: Kaj storim, če najdem USB ključek?

Odgovori	%	Število
Najprej skeniram USB za viruse, preden odprem datoteke na njem.	13,8%	8
Namestim virtualni računalnik na svoj računalnik, šele nato pregledam vsebino USB ključka.	10,3%	6
Takoj vključim USB v računalnik in pregledam vse mape, da lažje ugotovim, kdo je lastnik.	6,9%	4
USB dam nekemu, ki se na to spozna bolje od mene, da ga preuči.	37,9%	22
USB pustim na tleh.	31,0%	18
Skupna vsota	100,0%	58



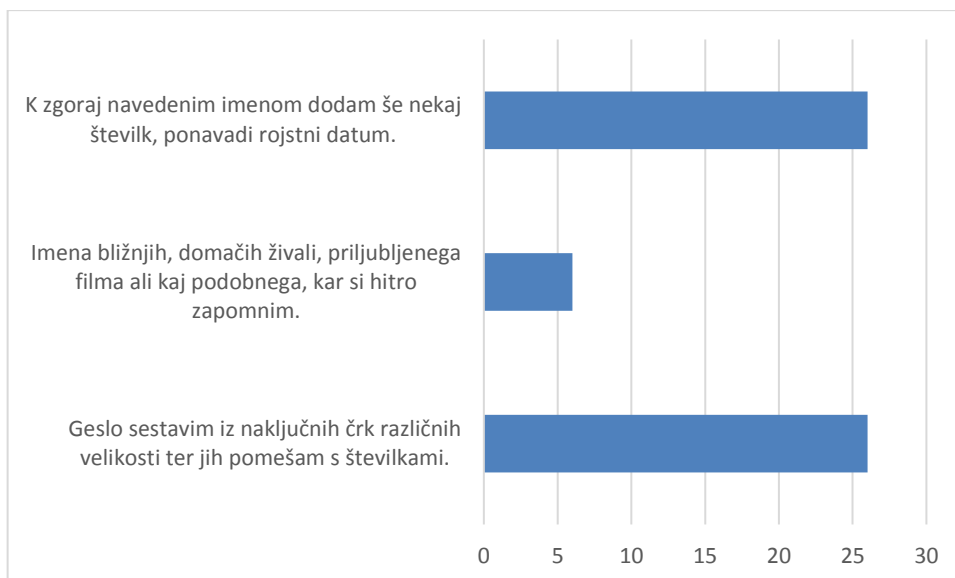
Graf 3: Kaj storim, če najdem USB ključek?

Na vprašanje, kaj anketiranci storijo z USB ključkom, ki ga najdejo, je največ anketirancev 22 (37,9 %) odgovorilo, da ga dajo drugi osebi, da ga preuči. Najmanj anketirancev (4 oz. 6,9 %) je odgovorilo, da USB ključ takoj pregledajo, da vidijo, kdo je lastnik ključka.

Četrto vprašanje: Kakšna gesla po navadi izberete, ko si ustvarjate uporabniški račun?

Tabela 21: Izvirnost pri sestavljanju gesel za uporabniški račun

Oznake vrstic	%	Število
Geslo sestavim iz naključnih črk različnih velikosti ter jih pomešam s številkami.	44,8%	26
Imena bližnjih, domačih živali, priljubljenega filma ali kaj podobnega, kar si hitro zapomnim.	10,3%	6
K zgoraj navedenim imenom dodam še nekaj števil, ponavadi rojstni datum.	44,8%	26
Skupna vsota	100,0%	58



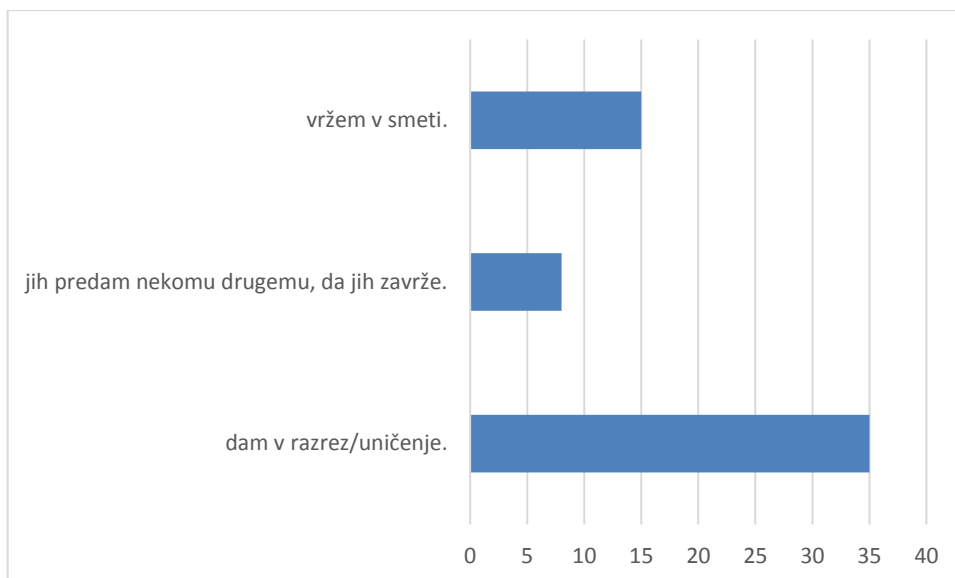
Graf 4: Izvirnost pri sestavljanju gesel za uporabniški račun

Za izbiro gesla sta se 2 odgovora pojavila v istem številu. Gesla večinoma sestavljajo iz naključnih črk različnih velikosti ter jih pomešajo s številkami ali pa k imenom dodajo še nekaj številk, po navadi rojstni datum. Za vsak odgovor je bilo 26 oseb (44,8 %). Najmanj anketirancev 6 (10,3 %) pa je odgovorilo, da imajo za gesla imena bližnjih, domačih živali, filma itd.

Peto vprašanje: Kaj storim po uporabi dokumentov, stare računalniške opreme, koledarjev ipd., ko jih več ne potrebujem?

Tabela 3: Kaj storim po uporabi dokumentov, stare računalniške opreme, koledarjev ipd., ko jih več ne potrebujem?

Odgovori	%	Število
dam v razrez/uničenje.	60,3%	35
jih predam nekomu drugemu, da jih zavrže.	13,8%	8
vržem v smeti.	25,9%	15
Skupna vsota	100,0%	58



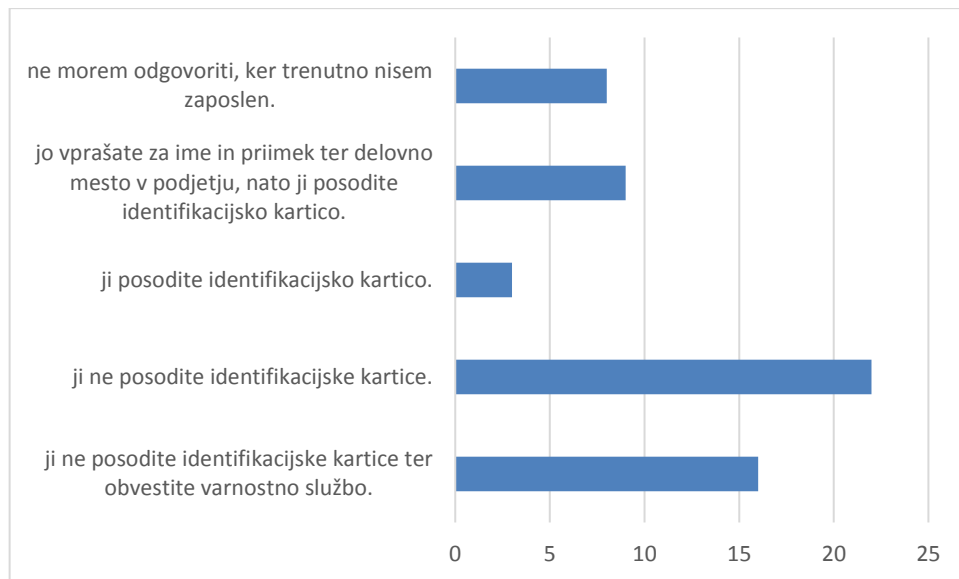
Graf 5: Kaj storim po uporabi dokumentov, stare računalniške opreme, koledarjev ipd., ko jih več ne potrebujem?

Na vprašanje o tem, kaj anketiranci storijo z odvečnimi pomembnimi stvarmi, kot so stara računalniška oprema, dokumenti ipd., je večina anketirancev 35 (60,3 %) odgovorila, da neuporabne stvari da v razrez ali uničenje. Najmanj anketirancev 8 (13,8 %) je odgovorilo, da jih preda nekemu drugemu, da jih zavrže.

Šesto vprašanje: Ste na odmoru. Do vas pristopi oseba, ki je sicer ne poznate, a je oblečena v uniformo vašega podjetja in prosi za identifikacijsko kartico, saj je svojo pozabila. Vi:

Tabela 4: Zaupljivost osebi, ki se izdaja za uradno osebo

Odgovori:	%	Število
ji ne posodite identifikacijske kartice ter obvestite varnostno službo.	27,6%	16
ji ne posodite identifikacijske kartice.	37,9%	22
ji posodite identifikacijsko kartico.	5,2%	3
jo vprašate za ime in priimek ter delovno mesto v podjetju, nato ji posodite identifikacijsko kartico.	15,5%	9
ne morem odgovoriti, ker trenutno nisem zaposlen.	13,8%	8
Skupna vsota	100,0%	58



Graf 6: Zaupljivost osebi, ki se izdaja za uradno osebo

Na vprašanje o zaupanju podatkov podjetju z identifikacijo je največ anketirancev 22 (37,9 %) odgovorilo, da osebi, ki vstopi v podjetje, ne izda svoje identifikacijske kartice. Le trije (5,2 %) pa so odgovorili, da bi osebi zaupali identifikacijsko kartico.

4 PROGRAM ZA KREPITEV RAZUMEVANJA SOCIALNEGA INŽENIRINGA

Živimo v obdobju, ko ljudje množično uporabljamo spletna socialna omrežja in se dnevno soočamo s prenasičenostjo s podatki. Prav tako je to tudi obdobje, ko je socialni inženiring na vzponu, zato bi bilo dobro definicijo socialnega inženiringa približati čim večjemu številu ljudi.

Izobraževanju o varnosti in nevarnostih na spletu bi morali posvečati mnogo več pozornosti. Ključni element obrambe pred socialnim inženiringom je izobrazba ljudi, ki pripomore k temu, da bi se zavedali tovrstnih prevar tako v organizacijah kot tudi v zasebnem življenju.

Da bi izboljšali raven razumevanja socialnega inženiringa v podjetjih in drugih organizacijah, je potrebno ljudi izobraževati in organizirati različne tečaje in druga izobraževanja, kjer bi jih naučili postopkov in standardov, ki narekujejo, kako ukrepati ob takšnih situacijah. Opozorjanje na potencialne nevarnosti, ki jih predstavlja socialni inženiring, mora biti sestavni del vseh izobraževanj in usposabljanj. Vsak posameznik se mora zavedati nevarnosti socialnega inženiringa, mora biti sposoben prepoznati namen zlorabe in braniti sebe ter podjetje pred napadi. Brez zadostnega izobraževanja in usposabljanja je možnost za uspešno obrambo pred napadi zelo majhna.

Poročanje o prepoznanih napadih je bistvenega pomena za evidentiranje možnih oblik napadov, kar nato omogoča vpeljavo novih preventivnih ukrepov.

V podjetjih je bistvena tudi varnostna politika, ki nudi pomoč pri usmerjanju zaposlenih k preventivnemu delovanju in preprečevanju napadov. Z jasnimi in razumljivimi pravilniki za uporabo spletnih socialnih omrežij dobijo zaposleni čisto predstavo, kakšno delovanje na spletnih socialnih omrežjih je od njih pričakovano. Politike in pravilniki pripomorejo pri odločitvah glede uporabe socialnih omrežjih in odpravljajo kakršnekoli dvoumnosti.

V zasebnem življenju bi razumevanje lahko krepili z različnimi organiziranimi predavanji na temo socialnega inženiringa, ki bi ga organizirali strokovnjaki s tega

področja. Posamezniki se lahko ozaveščajo tudi s prebiranjem različnih knjig ali člankov na to temo.

V srednjih šolah bi bilo priporočljivo dijake podučiti o definiciji socialnega inženiringa in kako se pred njim zaščititi, saj dijaki ogromne količine svojega prostega časa preživijo na socialnih omrežjih in bi bilo dobro, da bi se zavedali tveganj in bi znali odreagirati na napad. Tako dijake kot ostale posameznike v zasebnem življenju bi morali podučiti, kako se preventivno zavarovati pred napadi socialnega inženiringa. Na primer kako izbrati dobro varovano geslo za spletna socialna omrežja, kako varno spletno nakupovati ipd.

5 JAVNA PREDSTAVITEV IZSLEDKOV

Javna predstavitev celotnega projekta s poudarkom na ugotovitvah in predlogih je bila izvedena 28.9.2017 na FKPV. Predvidena je še javna predstavitev v lokalnem okolju.

6 ZAKLJUČEK

Študenti in mentorji smo v okviru projekta Socialni inženiring sodelovali štiri mesece. Želeli smo ugotoviti, kako so posamezniki in podjetja seznanjeni z vplivom socialnega inženiringa in s coachingom. Spoznali smo jih preko anket in preko globinskih intervjujev. Opazili smo, da se ljudje ne zavedajo, kakšen vpliv ima lahko socialni inženir na njihovo podjetje ter kako jih lahko zavede z različnimi triki. Opazili smo, da bo potrebno še veliko dela na tem področju.

Pri globinskih intervjujih smo direktorjem podjetij postavili štiri ključna vprašanja in izvedeli, da je za varnost najmanj poskrbljeno v javnem sektorju (knjižnica).

Anketa je vsebovala 34 vprašanj. Podjetjem je bila posredovana preko elektronskih sporočil. V anketi je sodelovalo 58 anketirancev, od teh je bilo največ žensk s srednješolsko izobrazbo. Poprečna starost anketirancev je bila 34 let.

Z anketo je bilo dokazano, da največji delež anketirancev nikoli ne zavaruje svojega računalnika z geslom, bolj pa so pazljivi pri puščanju dokumentov na delovni mizi. Samo 31 % anketirancev menja geslo v podjetju enkrat letno, ostali gesla ne menjavajo tako pogosto ali pa ga sploh ne menjajo.

Ker živimo v obdobju, ko ljudje množično uporabljamo spletna omrežja in se s tem izpostavljam različnim kibernetскими napadi, je posameznike nujno potrebno seznaniti, kako se lahko pred temi napadi ubranijo. Z namenom približati socialni inženiring čim večjemu številu ljudi bi jih bilo potrebno usmeriti na tečaje in izobraževanja na to temo, kjer bi se seznanili in naučili postopkov, kako ukrepati pri tovrstnih napadih.

S sodelovanjem v projektu smo spoznali veliko novega. Izvedeli smo, da ljudje še vedno v večini ne vedo, kaj pomeni izraz »socialni inženiring« in kako se pred njim ubraniti. Potrebujejo namreč dodatne informacije in izobraževanja glede internetne varnosti. Pomagamo si lahko skupaj, začne se pa z vsakim posameznikom posebej.

7 VIRI IN LITERATURA

1. Cox, E., Bachkirova, T., Clutterbuck, D. (2014). *The Complete Handbook of Coaching*. London: Sage Publications Ltd. Pridobljeno 29. 6. 2017 s spletne strani <https://books.google.si/books?h>.
2. Čeč, F. (2006). *S coachingom do večjih poslovnih in osebnih dosežkov: vodnik*. Zagorje ob Savi: Regionalni center za razvoj. Pridobljeno 28. 6. 2017 s spletne strani <http://www.rcr-zasavje.si/uploads/files/Coaching.pdf>.
3. Gray, D. E., Gravey, B. in Lane, A. D. (2016). *A Critical Introduction to Coaching and Mentoring: Debates, Dialogues and Discourses*. London: Sage Publications Ltd. Pridobljeno 29. 6. 2017 s spletne strani <https://www.amazon.co.uk/Critical-Introduction-Coaching-Mentoring/dp/1446272281>.
4. Gregorič, U. (2011). *Socialni inženiring v spletnih socialnih omrežjih*. Pridobljeno 25. 6. 2017 s spletne strani <https://dk.um.si/lzpisGradiva.php?lang=slv&id=30242>.
5. Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley Publishing, Inc.
6. Informacijski pooblaščenec. (2009). *Socialni inženiring in kako se pred njim ubraniti?* Pridobljeno 25. 6. 2017 s spletne strani https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.
7. Selan Kure, V. (2014). Model narativnega in NLP koučinga: oris in primerjava. *Socialna pedagogika*, 18(3-4), 153–192. Pridobljeno 28. 6. 2017 s spletne strani http://www.revija.zzsp.org/pdf/SocPed_2014-3-4.pdf.
8. Singh Patel, R. (2013). *Kali Linux Social Engineering*. Birmingham: Packt Publishing Ltd.

8 PRILOGE

Anketa o socialnem inženiringu

Smo študentje iz različnih fakultet po Sloveniji, ki s Fakulteto za komercialne in poslovne vede sodelujemo v projektu, v okviru katerega raziskujemo seznanjenost ljudi s socialnim inženiringom. Vljudno vas prosimo, če lahko izpolnite kratko anonimno anketo in s tem pripomorete k večji verodostojnosti rezultatov naše raziskave. Aktivna bo do konca avgusta 2017.

Za sodelovanje se vnaprej zahvaljujemo.

Ana Ocvirk, Patricija Potisk, Urban Ažman, Ana Bastelj, Ana Peterka, Taja Savič, Michel Kovač.

OCENITE, KAKO POGOSTO, OZIROMA V KOLIKŠNI MERI, VSEBINA SPODNJIH TRDITEV ODRAŽA VAŠA DEJANJA:

1. Računalnik pustim nezavarovan (brez gesla), tudi ko se za krajši čas oddaljim od njega.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)
2. Poslovne dokumente (npr. osnutek pogodbe, tehnično dokumentacijo) v svoji odsotnosti pustim na delovni mizi.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)
3. Svojo pisarno zaklepam tudi takrat, ko jo zapustim zgolj za nekaj minut.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)
4. Če bi me sodelavec prosil, bi mu zaupal svoje vstopne podatke.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

5. S sodelavci se o službenih zadevah pogovarjam tudi na javnih mestih (prireditve, kosila).
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

6. Elektronsko pošto pregledam tudi preko nezaščitenega in brezplačnega omrežja.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

7. Preberem vsako elektronsko sporočilo, tudi tisto, kjer ne poznam pošiljatelja.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

8. Preden vnašam podatke zaupne narave, preverjam identiteto elektronskega poštnega naslova.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

9. Preden vnašam podatke zaupne narave, preverjam identiteto spletne strani.
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

10. O službenih zadevah se pogovarjam tudi na družabnih omrežjih (Facebook, Twitter, Myspace ...).
 - Nikoli (ne)
 - Redko (prej ne kot da)
 - Pogosto (prej da kot ne)
 - Vedno (da)

11. Neznancu, ki se ukvarja z akvizitersko prodajo, dovolim vstop v službene prostore.

- Nikoli (ne)
- Redko (prej ne kot da)
- Pogosto (prej da kot ne)
- Vedno (da)

12. Na spletnih straneh dovolim uporabo piškotkov.

- Nikoli (ne)
- Redko (prej ne kot da)
- Pogosto (prej da kot ne)
- Vedno (da)

13. Novemu sodelavcu, za katerega nisem bil seznanjen, da je zaposlen v našem podjetju, po potrebi zaupam svoja gesla in dostope do informacij.

- Nikoli (ne)
- Redko (prej ne kot da)
- Pogosto (prej da kot ne)
- Vedno (da)

OZNAČITE ODGOVOR, KI VELJA ZA VAS.

14. Prejeli ste e-pošto od administratorja informacijskega sistema bančne ustanove. Od vas zahteva, da zaradi sprememb v sistemu sledite poslani povezavi in vnesete svoje uporabniško ime in geslo. Kaj storite?

- Sporočilom administratorja informacijskega sistema zaupam, zato sledim navodilom.
- Kliknem na povezavo in če stran deluje verodostojna, vnesem svoje podatke.
- Sporočilo pazljivo preberem in če deluje verodostojno, kliknem na povezavo in sledim navodilom.
- Administratorja informacijskega sistema povprašam glede sporočila.

15. Prejeli ste klic osebe, ki trdi, da je iz neke organizacije, kjer ste zmagali na natečaju. Tega natečaja se ne spominjate, a ker se redno prijavljate na nagradne igre, mislite, da ste prav danes imeli to srečo. Klicatelj vam sporoči, da ste osvojili veliko nagrado in želi preveriti informacije, ki ste jih navedli ob vstopu na natečaj. Zahtevani podatki vsebujejo vaš domači naslov in vaš EMŠO. Kaj naredite?

- Takoj posredujem vse potrebne informacije
- Postavim številna dodatna vprašanja, preden posredujem informacije.
- Ne posredujem nobenih informacij.

16. Medtem, ko hodite proti vhodu v službo/šolo, vidite na tleh USB ključek. Na njem ni ničesar, kar bi vam lahko pomagalo identificirati lastnika. Zavedate se, koliko dela bi lahko šlo v nič, če ga je nekdo izgubil. Kaj naredite?

- Takoj vključim USB v računalnik in pregledam vse mape, da lažje ugotovim, kdo je lastnik.
- Najprej skeniram USB za viruse, preden odprem datoteke na njem.
- Namestim virtualni računalnik na svoj računalnik, šele nato pregledam vsebino USB ključka.
- USB dam nekemu, ki se na to spozna bolje od mene, da ga preuči.
- USB pustim na tleh.

17. Kakšna gesla po navadi izberete, ko si ustvarjate uporabniški račun?

- Imena bližnjih, domačih živali, priljubljenega filma ali kaj podobnega, kar si hitro zapomnim.
- K zgoraj navedenim imenom dodam še nekaj števil, po navadi rojstni datum.
- Geslo sestavim iz naključnih črk različnih velikosti ter jih pomešam s številkami.

18. Ko določenih dokumentov, stare računalniške opreme, koledarjev ipd. ne potrebujem več, jih:

- vržem v smeti.
- dam v razrez/uničenje.
- jih predam nekemu drugemu, da jih zavrže.

19. Ste na odmoru. Do vas pristopi oseba, ki je sicer ne poznate, a je oblečena v uniformo vašega podjetja in prosi za identifikacijsko kartico, saj je svojo pozabila. Vi:

- ji posodite identifikacijsko kartico.
- jo vprašate za ime in priimek ter delovno mesto v podjetju, nato ji posodite identifikacijsko kartico.
- ji ne posodite identifikacijske kartice ter obvestite varnostno službo.
- ji ne posodite identifikacijske kartice.
- ne morem odgovoriti, ker trenutno nisem zaposlen.

OCENITE, V KOLIKŠNI MERI TRDITVE VELJAJO ZA DELO V VAŠEM PODJETJU:

20. V vašem podjetju menjate gesla vsaj enkrat letno.

- popolnoma velja
- velja
- niti ne velja niti velja
- ne velja
- sploh ne velja
- ne morem odgovoriti, ker trenutno nisem zaposlen

21. Sem seznanjen s pravilnikom o postopkih in ukrepih za zavarovanje osebnih podatkov.
- popolnoma velja
 - velja
 - niti ne velja niti velja
 - ne velja
 - sploh ne velja
 - ne morem odgovoriti, ker trenutno nisem zaposlen
22. Vem, kako preveriti verodostojnost osebe, preden ji posredujem zaupne podatke.
- popolnoma velja
 - velja
 - niti ne velja niti velja
 - ne velja
 - sploh ne velja
 - ne morem odgovoriti, ker trenutno nisem zaposlen
23. Dostopam lahko samo do aplikacij/programov/podatkov, s katerimi upravlja moj oddelek.
- popolnoma velja
 - velja
 - niti ne velja niti velja
 - ne velja
 - sploh ne velja
 - ne morem odgovoriti, ker trenutno nisem zaposlen
24. Ko določenih dokumentov, stare računalniške opreme, koledarjev ipd. ne potrebujem več, jih ustrezno zavržem (fizično uničenje, izbris podatkov, razrez).
- popolnoma velja
 - velja
 - niti ne velja niti velja
 - ne velja
 - sploh ne velja
 - ne morem odgovoriti, ker trenutno nisem zaposlen
25. Do službenega internetnega omrežja lahko dostopam le z lastnimi uporabniškimi podatki.
- popolnoma velja
 - velja
 - niti ne velja niti velja
 - ne velja
 - sploh ne velja
 - ne morem odgovoriti, ker trenutno nisem zaposlen

26.V podjetje lahko vstopam le z identifikacijsko kartico oziroma z jasno identifikacijo.

- popolnoma velja
- velja
- niti ne velja niti velja
- ne velja
- sploh ne velja
- ne morem odgovoriti, ker trenutno nisem zaposlen

27.Do prostorov, kjer so hranjeni zaupni podatki (arhiv) ali pomembna oprema (strežnik), imajo dostop samo pooblaščen osebe.

- popolnoma velja
- velja
- niti ne velja niti velja
- ne velja
- sploh ne velja
- ne morem odgovoriti, ker trenutno nisem zaposlen

SPLOŠNA VPRAŠANJA

28.Spol:

- moški
- ženska

29.Starost: _____

30.Poštna številka kraja bivanja: _____

31.Poštna številka kraja vašega podjetja: _____

32.Stopnja izobrazbe:

- OŠ ali manj
- nižje poklicno izobraževanje (2 leti)
- srednje poklicno izobraževanje (3 leta)
- gimnazijsko, srednje poklicno -tehniško izobraževanje, srednje tehniško oz. drugo strokovno izobraževanje
- višješolski program (do 1994), višješolski strokovni program
- specializacija po višješolskem programu, visokošolski strokovni programi
- specializacija po visokošolskem strokovnem programu, univerzitetni program
- specializacija po univerzitetnem programu, magisterij znanosti
- doktorat znanosti

33. Področja dela:

- vodstveni kader
- tehnično osebje
- ostala področja dela
- nisem zaposlen

34. Osnovna dejavnost podjetja (če niste zaposleni, vpišite "NE"): _____

Razlaga socialnega inženiringa

Socialni inženiring je tehnika pridobivanja informacij, do katerih socialni inženir nima dovoljenja dostopati. Informacije so lahko digitalne, saj so tovrstni napadi navadno usmerjeni na informacijske sisteme, lahko pa so tudi v ustni ali pisni obliki.

Socialni inženir zlorabi zaupanje žrtve, pri tem pa mu pomaga poznavanje socialnih veščin in psiholoških tehnik. Na ta način pride do zaupnih podatkov, ki mu navadno prinašajo premoženjsko korist.

NAJLEPŠA HVALA ZA REŠEVANJE ANKETE!

V kolikor vas področje podrobneje zanima, nas lahko do konca leta 2017 kontaktirate na elektronski naslov: projekt.socialni.inzeniring@gmail.com.