Pregled psiholoških, sociooloških i tehničkih aspekata socijalnog inženjeringa

Hanich, Jelena

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Jelena Hanich

PREGLED PSIHOLOŠKIH, SOCIOLOŠKIH I TEHNIČKIH ASPEKATA SOCIJALNOG INŽENJERINGA

ZAVRŠNI RAD

Varaždin, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Jelena Hanich

Matični broj: 0016144287

Studij: ***Primjena informacijske tehnologije u poslovanju***

PREGLED PSIHOLOŠKIH, SOCIOLOŠKIH I TEHNIČKIH ASPEKATA SOCIJALNOG INŽENJERINGA

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Igor Tomičić

Varaždin, svibanj 2022.

Jelena Hanich

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristila drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autorica potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Napadi socijalnog inženjeringa predstavljaju sigurnosnu prijetnju u kibernetičkom prostoru. U ovom završnom radu predstavljen je konceptualni model poveznice napada socijalnog inženjeringa unutar djelovanja psiholoških, sociooloških i tehničkih aspekta. Navedeno istraživanje je provedeno kombiniranjem utjecaja mehanizama učinaka, psihološkog elementa ranjivosti te primarnih vrsta socijalnog inženjeringa. Odnosno, sve vrste napada socijalnog inženjeringa uspijevaju pod utjecajem psiholoških i sociooloških aspekata budući da je ljudski faktor centar svakog računalnog sustava, što ujedno znači da tehnički aspekt nije uvijek nužan u provođenju socijalnog inženjeringa. Kako ulaganja u kibernetičku sigurnost predstavlja sve veću važnost, tehnički aspekti obmanjivanja postaju sve teži i izazovniji, a napadi u kojima se manipulira psihološkim i sociološkim aspektima postaju sve češći. Obrazovanje organizacije i pojedinaca treba biti prioritet u obrani od socijalnog inženjeringa kako bi se podigla svijet o psihološkim i sociološkim elementima ranjivosti koje napadači često iskorištavaju u svoju korist.

Ključne riječi: socijalni inženjering; psihološki aspekt; sociološki aspekt; tehnički aspekt; kibernetička sigurnost.

Sadržaj

1. UVOD

U kontekstu računalne i kibernetičke sigurnosti, socijalni inženjering opisuje vrstu napada u kojem napadač iskorištava ljudske ranjivosti sredstvima kao što su utjecaj, uvjeravanje, obmana, manipulacija i navođenje, kako bi došao do povjerljivih informacija, hakirao računalni sustav i mrežu, dobiti neovlašteni pristup zabranjenim područjima ili prekršio sigurnosne ciljeve (kao što su povjerljivost, integritet, dostupnost, mogućnost kontrole i revizija) unutar elemenata kibernetičkog prostora (kao što su infrastruktura, podaci, resursi, korisnik i rad). Drugim riječima, socijalni inženjering je vrsta napada u kojem napadač iskorištava ljudsku ranjivost kroz društvenu interakciju kako bi narušio sigurnost kibernetičkog prostora. Ne postoji računalni sustav koji se ne oslanja na ljude ili koji ne uključuje ljudske čimbenike, a ti ljudski čimbenici su ranjivi ili ih vješti napadači u velikoj mjeri mogu pretvoriti u sigurnosne ranjivosti. Ovi neizbježni i ranjivi ljudski čimbenici čine socijalni inženjering univerzalnom prijetnjom kibernetičke sigurnosti.

Tema ovog završnog rada je istražiti i sažeto opisati psihološke, sociološke i tehničke aspekte socijalnog inženjeringa kako bi se doprinijela veća pozornost vrlo popravljivim čimbenicima koji su dio ljudske prirode. Značajnost ove teme očituje se u velikom prostoru za napredak u osiguravanju kibernetičke sigurnosti kroz obrazovanje organizacija i pojedinaca o psihološkim i sociološkim aspektima koji su ukorijenjeni u neznanju, nepažljivosti, brzopletosti, pohlepi, nepoznavanju osnova sigurnosnih procedura, itd. Ujedno je izvršena klasifikacija psiholoških i sociološkim aspekata s obzirom na osnovne vrste socijalnog inženjeringa radi olakšanog i sažetog prikaza tematike.

2. METODE I TEHNIKE RADA

Ovo poglavlje predstavlja metodologiju diplomskog rada, odnosno predmet rada i cilj istraživanja, metode istraživanja te izvore podataka korišteni pri izradi. Predmet ovog završnog rada je sažeto opisati i prikazati tehničke, psihološke i sociološke aspekte socijalnog inženjeringa. Cilj ovog istraživanja je olakšati razumijevanje o tome na koji način se vrste socijalnog inženjeringa provode s obzirom na psihološke, sociološke i tehničke aspekte provođenja. Kod pisanja ovog završnog rada korištena je deskriptivna metoda koja se očituje kroz opisani i olakšani prikaz u obliku slika, deduktivna metoda u svrhu donošenja zaključaka na temelju raspoloživih podataka, metoda kompilacije na temelju koje su preuzeti određeni dijelovi teksta iz članaka, internetskih stranica i znanstvene literature. Koristeći se metodom klasifikacije prikazane su različite podjele. Prilikom pisanja ovog završnog rada korištene su različite vrste znanstvenih izvora. Korištene su knjige, stručni i znanstveni članci te pojedini internetski izvori.

3. POJMOVNO I KLASIFIKACIJSKO ODREĐENJE SOCIJALNOG INŽENJERINGA

U prvom poglavlju je opisan pojam, uloga i implikacija socijalnog inženjeringa. Drugo poglavlje opisuje klasifikaciju socijalnog inženjeringa te psihološke, tehničke i sociološke aspekte s obzirom na klasificiranu podjelu kako bi se otkrili korijenski uzroci nekih od najčešćih napada socijalnog inženjeringa.

3.1. Pojam i uloga socijalnog inženjeringa

Zaštita osjetljivih informacija od vitalne je važnosti za vlade, organizacije i pojedince. Iako se učinkovitost zaštite povjerljivih informacija povećava iz dana u dan, ljudi su i dalje podložni raznim metodama manipulacije. Čin utjecaja i manipuliranja ljudima radi otkrivanja osjetljivih informacija poznat je kao socijalni inženjering ili društveni napadi. Socijalni inženjering sastoji se od tehnika koje se koriste za manipuliranje ljudima u izvođenju željenih radnji ili otkrivanju povjerljivih informacija. Napadač unutar socijalnog inženjeringa na temelju prijevare navodi osobu da omogući pristup povjerljivim informacijama ili da prekrši uobičajene sigurnosne procedure. Socijalni inženjering se može koristiti u interakcijama “licem u lice”, putem telefona, e-pošte, web stranica, SMS poruka, itd. Socijalni inženjering je ukorijenjen u korištenju tehnologije i socijalne psihologije [1].

U kibernetičkoj sigurnosti, socijalni inženjering odnosi se na manipulaciju pojedincima kako bi ih se potaknulo na izvršenje određenih radnji ili da bi otkrili informacije koje ugrožavaju sigurnosne procedure te koje mogu biti od krajnje financijske koristi napadaču. Socijalni inženjering sam po sebi ne zahtijeva nužno veliku količinu tehničkog znanja da bi bio uspješno proveden. Odnosno, socijalni inženjering koristi uobičajene aspekte sociološkim principa i ljudske psihologije kao što su znatiželja, lakovjernost, pohlepa, nepromišljenost, strah, apatija, itd. Tehnike socijalnog inženjeringa najčešće se koriste za isporuku zlonamjernog softvera, ali u nekim slučajevima samo su dio napada, kao sredstvo za dobivanje dodatnih informacija, počinjenja prijevare ili dobivanja pristupa sigurnosnim sustavima. Tehnike socijalnog inženjeringa kreću se od neselektivnih napada širokih razmjera koji su direktni i obično se mogu lako identificirati do sofisticiranih višeslojnih prilagođenih napada koji se gotovo ne mogu razlikovati od stvarnih uobičajenih interakcija. Socijalni inženjeri su kreativni i može se očekivati da će se njihove taktike razvijati kako bi iskoristile prednosti novih tehnologija i društvenih situacija [2].

3.2. Klasifikacija socijalnog inženjeringa

Postoje dvije osnovne vrste socijalnog inženjeringa: komunikacija “licem u lice” i napadi putem tehnologije. Socijalni inženjering utemeljen na ljudskoj komunikaciji zahtijeva fizičku interakciju kako bi se postigao cilj prijevare. To može značiti lažno predstavljanje, autorizacija treće strane, manipulacija teme razgovora itd. Socijalni inženjering utemeljen na tehnologiji zahtijeva elektroničko sučelje za postizanje željenog cilja. To može uključivati korištenje e-pošte, web stranica, software-a, društvenih mreža, digitalnih proizvoda, itd. Na primjer, napadač može slati lažne e-poruke pretvarajući se da su od legitimnog subjekta, te tako prevariti žrtvu da povjeruje da e-pošta potječe iz legitimnog izvora što se kasnije zloupotrebljava radi stjecanja osjetljivih i povjerljivih informacija. Prijetnje socijalnog inženjeringa koje se temelje na ljudskom elementu su u porastu zbog kontinuiranog poboljšanja zaštite od prijetnji temeljenih na tehnologiji [3]. Postoji mnogo vrsta socijalnog inženjeringa koje se podalje mogu klasificirati, u nastavku je sažeto klasificirana primarna grupacija tehnika napada unutar socijalnog inženjeringa.

1) Napadi krađe identiteta

Napadi krađe identiteta najčešći su napadi unutar socijalnog inženjeringa [4]. Cilj im je prijevarno stjecanje privatnih i povjerljivih informacija, najčešće putem telefonskih poziva ili e-pošte. Napadači obmanjuju žrtve kako bi pridobili osjetljive i povjerljive informacije. Uključuju lažne web stranice, e-poštu, plaćene oglase, antivirusne programe, lažne nagrade, besplatne ponude, itd. Na primjer, to može biti poziv ili e-mail lažnog odjela lutrije o osvajanju novčane nagrade i traženju privatnih podataka ili klikanju na poveznicu priloženu u e-pošti. Napadači često kreiraju web stranice koje su dizajnirane isto kao i originalne web stranice, no razlika je u drugačijoj URL poveznici. Brojni su načini manipuliranja preusmjeravanja i manipuliranja URL poveznicama. Povjerljivi podaci mogu biti podaci o kreditnoj kartici, podaci o osiguranju ili bilo koje druge informacije koje bi osoba mogla koristiti za zloupotrebljavanje računa žrtava kao što su internetsko bankarstvo ili bilo koji drugi računi koji sadržavaju financijska sredstva [5].

2) Kreiranje scenarija (eng. *pretexting*)

Kreiranje scenarija se provodi koristeći lažne i uvjerljive scenarije kako bi se ukrali osobni podaci žrtve, temelje se na izgovorima koji navode žrtvu da vjeruje napadaču [6]. Napad se izvodi putem telefonskih poziva, e-pošte ili fizičkih medija. Napadači koriste objavljivanje informacija u telefonskim imenicima ili javnim web stranicama na kojima se napadači sastaju kako bi izvršili svoj napad. Izlika može biti ponuda za obavljanje usluge ili dobivanje posla, pitanja o osobnim podacima, pomoć prijatelju da pristupi računu uz obećanja davanja velike

provizije ili dobitak na lutriji. Odnosno, kreiranje scenarija obuhvaća stvaranje scenarija u kojem je napadač predstavljen kao primarni izvor informacija, potencijalne žrtve su stavljene u kušnju otkriti određene privatne informacije. Na primjer, napadač može kreirati scenarij u kojem se predstavlja kao prava osoba koju zaposlenici kao potencijalne žrtve mogu pitati određene informacije. Pod uvjetom da je napadač dobro pripremljen te je istražio sve esencijalne informacije, ima povećanu šansu pridobiti privatne informacije od zaposlenika ili druge vrste žrtava [7].

3) Surfanje preko ramena (eng. *shoulder surfing*)

Surfanje preko ramena obuhvaća vrstu socijalnog inženjeringa u kojoj napadač pokušava špijunirati žrtvu dok unosi vlastite podatke poput korisničkog imena i lozinke. Razvijanjem prijenosnih računala i bežičnih mreža rezultiralo je korištenjem kafića, restorana i zračnih luka kao lokacija na kojima napadači nastoje iskoristiti nepažnju žrtava. Drugi način obavljanja surfanja preko ramena jest slušanje javnih razgovora koji se odvijaju među zaposlenicima budući da je česti događaj raspravljanje i otkrivanje osjetljivih i povjerljivih informacija na javnom mjestu od strane nepažljivih zaposlenika. Ujedno, rizik surfanja preko ramena nije ograničen na javna okruženja. Mnogo puta napadači planiraju dobiti vizualni pristup ekranu računala dok je zaposlenik zaokupiran te na svom uobičajenom radnom mjestu. Posjetitelji nekog poduzeća, na primjer, mogu lako baciti pogled na ekrane dok hodaju uokolo i obilaze poduzeće. Rizik je u tome što mnogi ljudi vjeruju da su sigurni od zlonamjernih aktivnosti na poslu, no dobavljače, klijente, druge posjetitelje, čak i suradnike treba smatrati kao mogućim rizicima zloupotrebe privatnosti [8].

4) Mamac

Mamac je vrsta krađe identiteta u kojoj napadači pozivaju korisnike da kliknu na URL poveznicu kako bi dobili besplatne pogodnosti (filmovi, besplatni medijski zapisi i drugi digitalni proizvodi). Slično je implikaciji trojanskog konja gdje se napad izvodi iskorištavanjem nezaštićenih računalnih materijala kao što su mediji za pohranu ili USB stick koji sadrži zaraženi softver. Dakle, ova vrsta napada obuhvaća i fizičke medije oslanjajući se na znatiželju i neopreznost zaposlenika, na primjer, napadač namjerno ostavi USB stick pored računala zaposlenika, kada zaposlenik priključi USB disk u svoje računalo, zaraženi software izvršava napad nezaštićenih računalnih materijala. Ova vrsta napada često izvodi zlonamjerne radnje “u pozadini”, a da to žrtve ne primjećuju [9].

5) Napad izmamljivanja

Napad izmamljivanja se koristi radi izvlačenja potrebnih informacija tokom naizgled normalnog razgovora. Napadač treba osmisliti scenarij ili izmišljenu priču kako bi opravdao postavljanje

određenih pitanja kako bi se korak po korak otkrile potrebne informacije. Način provođenja napada izmamljivanja je često vrlo suptilan, kreativan i kvalitetno osmišljen kako bi se unaprijed odredili odgovori na sva moguća pitanja ili komentare potencijalnih žrtava. Na primjer, u grupnom razgovoru određene organizacije, dvoje napadača mogu pokrenuti temu otkrivajući vlastitu lozinku za koju je jedan napadač saznao da nije dovoljno snažna te kako ju je potrebno korigirati. Zatim, drugi napadač također otkriva svoju lozinku (ili se može raditi o nekoj drugoj suptilnijoj povjerljivoj informaciji) te se polako pokušava kroz razgovor navoditi zaposlenike da odaju vlastite povjerljive informacije [8]. Napad izmamljivanja se primarno temelji na sociološkim elementima te psihološkom elementu IDT-a (eng. interpersonal deception theory – IDT), što je podalje analizirano u sljedećem poglavlju.

6) Obrnuti napadi socijalnog inženjeringa (eng. reverse social engineering)

Metode obrnutog socijalnog inženjeringa baziraju se na tome da su žrtve nasamarene tako da sami stupe u kontakt s napadačima. Obrnuti društveni inženjering vrlo je jedinstven oblik društvenog inženjeringa, trik je u tome da napadač najprije upotrijebi tradicionalni napad socijalnog inženjeringa kako bi natjerao žrtve da povjeruju da je napadač dio legitimne organizacije, kao što je služba tehničke podrške. Problem je što žrtve ne znaju da je osoba koju zovu u pomoć sam napadač. Zbog prirode obrnutih napada socijalnog inženjeringa, haker može dobiti mnogo više informacija u tim slučajevima nego što bi to bio slučaj od uobičajenih napada društvenog inženjeringa. Napadač ima trenutni legitimitet jer žrtva vjeruje napadaču. To se razlikuje od tradicionalnog napada socijalnog inženjeringa gdje je najteži aspekt za napadača postizanje legitimiteta u očima žrtve [10]. Napad obrnutog socijalnog inženjeringa uključuje tri glavna koraka: izazivanje problema kao što je rušenje mreže, pokretanje komunikacije radi uvjeravanja da je sam napadač jedina osoba koja može eliminirati nastali problem, rješavanje kreiranog problema uz dobivanje ciljne povjerljive informacije [11].

4. ISTRAŽIVANJE MEĐUSOBNE POVEZANOSTI PSIHOLOŠKIH, SOCIOLOŠKIH I TEHNIČKIH ASPEKATA SOCIJALNOG INŽENJERINGA

Ljudski element je nezaustavni dio socijalnog inženjeringa. Svaki računalni sustav se bazira na ljudima te uvijek uključuje ljudske čimbenike koji su ranjivi te koje napadači socijalnog inženjeringa nastoje iskoristiti radi ugrožavanja sigurnosnih procedura. Ovo poglavlje završnog rada analizira mehanizme učinka socijalnog inženjeringa kroz psihološke i sociološke aspekte.

4.1. Psihološki i sociološki aspekti socijalnog inženjeringa

U nastavku su detaljno opisani psihološki i sociološki principi ljudske prirode koji predstavljaju primarne mehanizme učinaka socijalnog inženjeringa. Psihološki i sociološki principi su preuzeti iz članka recenziranog znanstvenog rada - IEEE Access. Ujedno su podaci iz tablice (vrste socijalnog inženjeringa, efektni mehanizmi i psihološki elementi ranjivosti) prikazane na kraju ovog poglavlja opisani na temelju primjera iz navedenog rada. Unutar samog rada se analiziraju i razmatraju mehanizmi učinka socijalnog inženjeringa u 6 aspekata: 1) uvjeravanje, 2) društveni utjecaj, 3) spoznaja, stav i ponašanje, 4) povjerenje i obmana, 5) jezik, misao i odluka, 6) emocije i odluke. Psihološki principi korišteni u radu obuhvaćaju navedene aspekte, izuzet društvenog utjecaja koji je korišten radi prikazivanja sociološkihprincipa.

A. Psihološki aspekt socijalnog inženjeringa

1) Sličnost kao proces uvjeravanja

Sličnost poziva na dopadanje, različitost dovodi do nesviđanja. Što su nečiji stavovi sličniji pojedincu, taj pojedinac će biti naklonjeniji unutar takvog odnosa [12]. Naprotiv, manje se tom pojedincu sviđaju osobe s kojima nema zajedničkih karakteristika i stavova [13]. Osim toga, fizička privlačnost također utječe na spremnost pružanja pomoći. Privlačni ljudi dobivaju više pomoći od onih za koje se smatraju neatraktivnima [14], [15]. Samim time, bilo bi mnogo manje učinkovito da napadač pokušava uvjeravati svoje žrtve na način koji je očito protivan njihovoj sklonosti, mislima ili osobnosti. Sukobi mišljenja i stavova ne samo da dovode do nesklonosti potencijalne žrtve, već mogu implicirati emocionalnu nesigurnost što izaziva osjećaj nezadovoljstva. Primarni dio procesa uvjeravanja u socijalnom inženjeringu je pretvaranje napadača da dijeli iste ideje, ciljeve i preferencije kao potencijalna žrtva [16].

2) Umjetnost u nagovoru i manipulaciji

“Ljudi sve više imaju ograničen raspon pažnje vidom, sluhom i mislima” [41]. Ometanje olakšava uvjeravanje uglavnom otežavajući proces protuargumenata i povećavajući napor u komunikaciji. Ometanje može natjerati žrtvu da uloži veliki napor kako bi čuo i razumio određenu vrstu poruke. Eksperimenti pokazuju da umjereno ometanje olakšava uvjeravanje, odnosno umjereno ometanje proizvodi veće šanse uvjeravanja nego snažno ometanje jer su žrtve manje skloni sumnjati da je umjereno uvjeravanje namijenjeno [17]. Rastresene osobe koje imaju nisku sklonost suprotstavljanju argumentima bit će najmanje otporne na uvjeravanje [18]. Ometanje se često koristi u napadima zlonamjerne manipulacije, proces razmišljanja o sigurnosti bit će inhibiran i poremećen ako se fokus žrtve kontinuirano distraktira.

3) Vjerodostojnost izvora i poslušnost autoritetu kod uvjeravanja

“Ljudi imaju tendenciju da automatski validiraju autoritativne poruke i brojeve” [41]. U većini kultura, posebno u kolektivističkoj kulturi, ljudi su naučeni da vjeruju onima koji su autoritativni, stručni i samopouzdani, budući da te karakteristike označavaju vjerodostojnost, znanje, pouzdanost i niski rizik. Eksperimenti o poslušnosti autoritetu pokazuju da je autoritet toliko moćan i utjecajan na neovisno razmišljanje i racionalno ponašanje određenih pojedinaca da potiskuju te karakteristike prilikom komuniciranja čime su izloženi većem riziku socijalnog inženjeringa [19], [20]. Čak i simboli autoriteta mogu potaknuti individualnu usklađenost. Na primjer, u eksperimentu koji je provela studija [19], bolničkim sestrama je nepoznati liječnik (koji predstavlja stručnost i autoritet) naredio da pacijentima daju lijek koji je neadekvatan, no koji je zapakiran u originalnoj ambalaži. Iako su gotovo sve medicinske sestre u kontrolnoj skupini tvrdile da ne žele poslušati naredbu, u eksperimentalnom procesu su sve 22 medicinske sestre, osim jedne, poslušale naredbu, sve dok ih nisu presreli na putu prema pacijentima. To objašnjava zašto se simboli koji odražavaju autoritet, stručnost i vjerodostojnost, kao što su uniforma, značka, poznati logo i “insajderska terminologija” često korištene u napadima socijalnog inženjeringa [20]. Studija [21] također pokazuje da je autoritativni pristup učinkovit u uvjeravanju žrtava da su URL poveznice za krađu identiteta unutar e-pošte sigurne.

4) Model kognitivnog odgovora (periferni put uvjeravanja)

Petty [22] je proveo analizu kognitivnog odgovora o postojanosti promjena stava izazvanih uvjerljivim komunikacijama, u kojem je predložen model kognitivnog odgovora koji pokazuje da su trajne promjene stavova rezultat kognitivnog reagiranja na sadržaj poruke, dok su privremene promjene stavova rezultat znakova uvjeravanja. Kognitivni odgovor dogodio se za promišljenu obradu komunikacije kada primatelji imaju motivaciju i sposobnost. Ako je primatelj motiviran (uključenost u problem, relevantnost, predanost, vjerodostojnost izvora,

itd.) i ima sposobnost (npr. poruka nije izrazito složena i nepoznata) da obradi sadržaj, promjena u kognitivnoj strukturi dovest će do trajne promjene stava [23]. Na temelju proučavanja dvaju puta do uvjeravanja, Petty i Cacioppo [24], [25] razvili su model vjerojatnosti razrade kako bi raspravljali o širokom rasponu varijabli koje su se pokazale ključnima u utjecaju na vjerojatnost razrade, a time i na putove do uvjeravanja. Put se događa kada su žrtve motivirane nekim čimbenicima i imaju sposobnost razmišljanja o problemu te argumenti se ispituju i pomno obrađuju. Motivacija može biti zanimljiva, važna ili osobno povezana. Vrlo je vjerojatno da će metu uvjeriti ako su argumenti jaki i uvjerljivi. Kada mete nisu u stanju pažljivo razmišljati ili kada nisu motivirane (npr. zauzete su ili rastresene, poruka je dosadna), mogli bi slijediti periferni put uvjeravanja. U ovoj situaciji, ciljevi koje treba uvjeriti su u niskoj razini uključenosti; možda neće postojati sposobnost ili motivacija za analizu kvalitete argumenata i promišljanje o suštini poruka, a argumenti neće biti zabrinuti za detaljnu obradu [26]. Za napade socijalnog inženjeringa često su uključeni ljudi koji računala smatraju osnovnim sredstvom rada kao što su administratori sustava, službenici računalne sigurnosti, tehničari, itd. Ove vrste žrtava vjerojatnije uvjeravaju jaki argumenti a slabi argumenti imaju tendenciju generiranja izazova. Ljudi kao što su zaštitari, čistači i recepcionari smatraju se slabije uključenima [12]. Oni općenito nisu u stanju razumjeti tehnički kontekst ili ih malo zanima sadržaj zahtjeva, nastoje izbjegavati i zamarati se dubljim analiziranjem zahtjeva i donijeti odluku na temelju slabijih argumenata. Samim time se smatra da uvjeravanje nije “ili/ili” izbor, već način “više i manje” [27].

5) Noga u vratima – utjecajnost ponašanja (eng. foot in the door)

“Ako želite da vam ljudi učine veliku uslugu, učinkovita strategija je da ih navedete da prvo učine malu uslugu za vas” [28]. Ovaj fenomen da će, nakon što netko pristane na mali zahtjev, vjerojatnije udovoljiti većem zahtjevu, poznat je kao efekt noga u vratima (eng. *foot in the door*). Taj je učinak još uvijek efikasan u online kontekstu, kao i u drugim komunikacijskim modalitetima, budući da funkcionira kroz motive unutarnje dosljednosti pojedinca. U usporedbi s činjenicom da stav predviđa ponašanje, efekt noga u vratima pokazuje da ponašanje utječe na stav. Čini se da ljudi grade vlastiti imidž nakon što su učinili malu uslugu, nesvjesno se osjećaju kao da su investirali u tu osobu te u potencijalni budući odnos. Kako bi održali dosljednost ove slike, ublažili pritisak ili kognitivnu disonancu uzrokovanu razlikama između unutarnjeg stava i vanjskog ponašanja, ljudi pokušavaju upravljati svojim kasnijim stavovima i ponašanjima kako bi bili u skladu s njihovim prethodnim ponašanjima [28]. “Teorija kognitivne disonance pokazuje da osjećamo napetost ili nedostatak sklada kada se istovremeno percipiraju dvije psihološki nekonzistentne spoznaje (misli, uvjerenja itd.). Kako bismo smanjili

tu nelagodu, često prilagođavamo svoje razmišljanje, posebno kada vanjski poticaji nisu dovoljni da opravdaju naše ponašanje" [41]. Kognitivna disonanca se javlja prilikom suočavanja s važnom odlukom između dvije jednako privlačne alternative, 1) subjektivno se vrši jedna selekcija iako objektivni razlozi podržavaju drugu, ili 2) prisjećanje prednosti onoga što se odbilo i nedostataka onoga što se odabralo. Kako bi se smanjila kognitivna disonanca, može se opravdati vlastiti odabir prilagođavanjem ideja, pa čak i revidiranjem sjećanja ili usklađivanjem rezultata s određenom subjektivnom spoznajom. Kognitivna disonanca objašnjava suprotnosti između ponašanja i stavova pojedinaca, također objašnjava temeljni mehanizam predanosti i dosljednosti. To također objašnjava zašto se uslužnost često iskorištava u napadima socijalnog inženjeringa. Na primjer, kognitivna disonanca se može iskoristiti tako da napadač iskorištava uslužnost zaposlenika ispitivanjem određenih pitanja, te tako da svako sljedeće pitanje sve više ruši sigurnosne procedure, do granice gdje zadnje pitanje otkriva ključne podatke koji su potrebni za provođenje napada socijalnog inženjeringa. Ljubaznost i zbunjenost prikrivenog napadača ostavlja dojam bezopasne osobe kojoj je potrebna pomoć, iako pitanja postaju neprikladnija, kognitivna disonanca utječe na održavanje vlastitih prvobitnih uvjerenja, iako novi dokazi ukazuju na suprotno.

6) Efekt promatrača, difuzija odgovornosti i deindividuacija

Učinak promatrača opisuje fenomen da je manja vjerojatnost da će osoba pružiti pomoć kada su prisutni promatrači. Drugim riječima, manje je vjerojatno da će osoba kojoj je potrebna pomoć dobiti pomoć kada je mnogo ljudi u blizini [29]. Vjerojatnije je da će osoba kojoj je potrebna pomoć dobiti pomoć kada su promatrači sami, a što je više slučajnih prolaznika u hitnoj situaciji, manja je vjerojatnost ili sporije da će prolaznik intervenirati kako bi pružio pomoć. Isto je i u online okruženju, oni koji su primili e-mail (zahtjev za pomoć) uz naznaku da nije kontaktiran niti jedan ili nekoliko drugih ljudi, češće pružaju pomoć od onih koji su primili zahtjev uz naznaku da su kontaktirani i mnogi drugi. Kada pojedinci u skupinama napuste uobičajena ograničenja, zaborave svoj individualni identitet i slijede norme grupe ili gomile, odnosno odvija se deindividuacija. Ljudima se u grupnim situacijama omogućava da izgube svoju samosvijest, da prenesu odgovornost na sve članove grupe i da odgovore na grupne norme bez obzira na to jesu li dobre ili loše. Individuirani ljudi svoje postupke doživljavaju kao grupne. Anonimnost, velika grupa, uzbudljive i ometajuće aktivnosti čimbenici su koji promiču deindividuaciju. U napadima socijalnog inženjeringa, žrtve se mogu dovesti u određene grupne situacije i iskorištavati pomoću ovih mehanizama za izvođenje radnji koje ugrožavaju

sigurnost kibernetičkog prostora [30]. Primjer se nalazi u tablici 1. pod stavkom obrnutog socijalnog inženjeringa.

7) Oskudica kao percipirana vrijednost

Oskudica manipulira ljudima uglavnom utječući na spoznaju vrijednosti, pobuđujući emocije i pojačavajući motivaciju, prilike se čine vrjednijima kada su percipirane kao manje dostupne ili kao uskoro nedostupne. Štoviše, oskudica povećava motivaciju i potiče negativno ponašanje pobuđujući emocije kao što su strah, tjeskoba, neumjerena želja i pohlepa. U mnogim scenarijima socijalnog inženjeringa, napadači iskorištavaju žrtve s ponudom ili zahtjevom baziranim na oskudnosti kako bi otkrili informacije ili pokrenuli zlonamjernu URL poveznicu uvjeravajući ih da će uskoro “isteći vrijeme” [15].

8) Složenost međuodnosa povjerenja i socijalnog inženjeringa

Povjerenje je važna varijabla koja predviđa podložnost korisnika napadima socijalnog inženjeringa, Chitre i sur. [31] proveli su istraživanje koje pokazuje da 90% sudionika misli da ljudi u Indiji općenito imaju višu razinu društvenog povjerenja, što implicira da su ranjiviji na napade temeljene na društvenom inženjeringu. U mnogim scenarijima napada socijalnog inženjeringa potrebno je uvjeriti žrtve da je napadač osoba od povjerenja. Prema [32], pozitivna korelacija između povjerenja i niskog rizika od spremnosti pomoći, izgradnje odnosa i dijeljenja informacija može biti značajan razlog zašto napadači posvećuju veliku pozornost povjerenju. U nekim scenarijima napada, iako je uočen određeni rizik, napadi socijalnog inženjeringa su se ipak događali jer je izgrađeno jače povjerenje. Shodno tome, čimbenici koji utječu na izgradnju povjerenja i čimbenici koji utječu na obmanu postaju primarni parametri koje napadači žele kontrolirati kako bi izvršili napad socijalnog inženjeringa.

Sztompka [33] je raspravljao o drugim čimbenicima koji utječu na izgradnju povjerenja, kao što su ugled, učinak, izgled, odgovornost i situacija koja izaziva povjerenje. Osim navedenih čimbenika, na izgradnju povjerenja i uspjeh napada socijalnog inženjeringa mogu utjecati i drugi faktori situacije, kao što su cyber-okruženje (trenutna komunikacija, društvene mreže, web stranice itd.), društvena kultura, sigurnosna strategija i prirodno okruženje. Za napade socijalnog inženjeringa, karakteristike žrtve (uključujući sklonost povjerenju) su čimbenici koje napadač može identificirati, ali ih slabo može kontrolirati. Stoga napadači obično daju sve od sebe da pokažu svoje čimbenike vrijedne povjerenja i manipuliraju situacijskim čimbenicima kako bi iskoristili stečeno povjerenje.

9) Čimbenici koji utječu na obmanu (eng. interpersonal deception theory – IDT)

Iako je većina ljudi uvjerena da mogu otkriti ili prevenirati društvenu prijevaru, teorija interpersonalne obmane (IDT) [34] sugerira da to najčešće nisu u mogućnosti. IDT pokušava objasniti proces i ishode prijevare u međuljudskim odnosima na temelju analize obmana, prijedloga i evaluacije. Prema IDT-u, u komunikaciji prijevare napadači poduzimaju više strateških aktivnosti za upravljanje te manipuliranje informacijama, ponašanjem i slikom kako bi zavarali žrtve, reciprocitet je prevladavajući obrazac prilagodbe interakcije između pošiljatelja i primatelja. Tijekom međuljudske obmane često se koriste tri vrste obmane koje se identificiraju kao krivotvorenje (npr. laž, kreiranje fikcije), prikrivanje (npr. djelomične istine, skrivanje esencijalnih informacija) i nedoumice (npr. izbjegavanje problema) [34]. Primjer je obuhvaćen u tablici 1. pod stavkom napada izmamljivanja.

10) Utjecaj emocija i osjećaja na donošenje odluka

Poznato gledište o ljudskom donošenju odluka je da ljudi donose odluke kroz dualni sustav emocija i razuma: jedan dio je općenito emocionalan, brz, automatiziran, a drugi je kognitivni, spor, deliberativan. Odnosno, mehanizmi emocija i donošenja odluke su vrlo složeni. Istraživanja vezana uz emocije i donošenje odluka postigla su mnoge rezultate, kao što su teorija limbičkog sustava emocija, teorija emocionalnog mozga (amigdala) i dva kruga (subkortikalni i kortikalni krug) [35]. Phelps i sur. [36] pokazuje da postoji više neuronskih sklopova koji su u osnovi modulacije donošenja odluka emocijama ili afektom. Mnogo je izazova u istraživanju emocija i osjećaja, npr. teško je točno manipulirati i izmjeriti emocije i afekte. Međutim, ovo područje se razvija skupa s razvojem kognitivne znanosti, neuroznanosti, znanosti o mozgu, anatomije i tehnika instrumenata. Iako je došlo do određene nekompatibilnosti, jedna stvar s kojom se slažu brojne studije u različitim područjima (npr. socijalna psihologija, neuroznanost, znanost o mozgu i anatomija) jest da emocije i osjećaji utječu na donošenje odluka. Emocije i raspoloženje izazivaju tendencije djelovanja i prenose ih na proces odlučivanja. Pojedinci u tužnim emocijama skloni su tražiti opcije visokog rizika/visoke nagrade, ali pojedinci u tjeskobnim emocijama preferiraju opcije niskog rizika/niske nagrade. Ljudi u emocijama straha izražavaju pesimistične procjene rizika i izbore nesklone riziku, ali ljudi u emocijama ljutnje izražavaju optimistične procjene rizika i izbore u potrazi za rizikom. U sretnom stanju ljudi brže donose odluke. Za napade socijalnog inženjeringa to implicira da će manipuliranje emocijama i osjećajima utjecati, čak i promijeniti odluku te razmišljanje potencijalne žrtve. Promjena emocija može promijeniti izbore [36].

B. Sociološki aspekti socijalnog inženjeringa

1) Utjecaj i sukladnost grupe

Ljudi većinom žive u grupama te su samim time pod utjecajem tih grupa. Sukladnost je promjena ponašanja ili uvjerenja unutar socijalnog inženjeringa u skladu s drugima kao

rezultat stvarnog ili zamišljenog grupnog utjecaja. Mnogo je čimbenika koji utječu na konformizam, kao što su veličina grupe, grupna jednoglasnost, grupna kohezija i javni odaziv pojedinca. Mala skupina može dovesti do velikog učinka usklađenosti, ljudi se jasno prilagođavaju kada se grupa poveća na određenu veličinu. Kako se veličina grupe povećala s 3 na 5, postotak ljudi koji su oponašali grupu povećao se sa 60% na 80%. Grupna kohezija povećava konformizam te povećava rizik socijalnog inženjeringa [20].

2) Normativni i informacijski utjecaj

Obično se pojedinac može prikloniti grupi kako bi bio prihvaćen ili kako bi dobio važne informacije, prvo se naziva normativni utjecaj, a drugo informacijski utjecaj. Sukladnost uzrokovana normativnim utjecajem motivirana je željom da se bude prihvaćen, voljen ili da se izbjegne grupni pritisak. Kada odstupaju od normi društvenih grupa, ljudi često snose društveni pritisak i plaćaju emocionalnu cijenu. Uostalom, za većinu ljudi društveno odbacivanje je vrlo bolno i nelagodno. Dakle, pojedinci se namjerno ili nenamjerno usklađuju sa skupinama kako bi tražili prihvaćanje i uvažavanje grupa. Ovo je također poznato kao društvena validacija. Ljudi obično pretpostavljaju da su grupne akcije ispravnije i manje rizične, što utječe na njihovo ponašanje, uvjerenje i odluku. Ovo je također poznato kao društveni dokaz. Ljudi određuju što je točno tako što validiraju što drugi ljudi misle da je ispravno. Usklađivanje s grupama može biti korisno u nekim situacijama, međutim, prihvaćanje informacijskog utjecaja bez razmišljanja će dovesti do slijepog praćenja. U napadima socijalnog inženjeringa, napadač često stvara specifične informacije i scenarij u kojem se normativni utjecaj i informacijski utjecaj koriste za manipuliranje ciljevima kako bi izvršili određene radnje koje pogoduju napadaču [37].

3) Teorija socijalne razmjene i norma reciprociteta

Teorija socijalne razmjene pokazuje da ljudi razmjenjuju ne samo materijalna dobra i novac već i društvena dobra kao što su ljubav, usluge, informacije i status. Razmatranje ili suptilna kalkulacija o troškovima i nagradi predviđaju odluku i ponašanje ljudi. Norma reciprociteta odnosi se na tendenciju ljudi da uzvraćaju usluge kao znak zahvalnosti [38]. “Slično ćemo se pokušati odužiti onim što nam je pružila druga osoba. Ako nam drugi učine uslugu, mi ćemo njima zauzvrat učiniti uslugu” [15]. Kao univerzalna društvena norma, reciprocitet uvijek utječe na ljude skupa s procesom socijalizacije. Ljudi univerzalno internaliziraju ideju da uzvraćaju drugima za njihovu dobrotu i pomoć. Osim toga, za sve društvene interakcije, razmjena bi trebala biti dugoročno uravnotežena. Primanje bez davanja zauzvrat krši normu reciprociteta. U napadu inverznog socijalnog inženjeringa, npr. napadač se predstavlja kao osoba koja pripada administratoru sustava, IT odjelu, službi za pomoć ili tehničkoj podršci, a zatim čeka (npr. novog zaposlenika) da zatraži pomoć za rješavanje greške računala ili mreže. Nakon što

se to dogodi, napadač pokušava iskoristiti novog zaposlenika tražeći uslugu ili traženjem lozinke. To uspijeva jer se od novog zaposlenika očekuje da uzvrati napadaču u sigurnosnom kontekstu i ispuni društvenu razmjenu [15].

4) Norma društvene odgovornosti i moralna dužnost

Za razliku od norme reciprociteta gdje se razmatra ravnoteža davanja i primanja, norma društvene odgovornosti zagovara da ljudi trebaju pomagati onima kojima je pomoć potrebna, a da se ne tiče budućeg uzvrata i razmjene. To je svojevrsno očekivanje prema moralnoj dužnosti za pomaganjem. U zemljama kolektivističke kulture ljudi snažnije podržavaju normu društvene odgovornosti nego zemlje individualističke kulture. Zagovaraju obvezu pomaganja drugima čak i ako se ne suočavaju sa životno opasnom nevoljom. Norma društvene odgovornosti i moralna dužnost imaju učinak napada socijalnog inženjeringa na najmanje dva načina. Jedan od načina je da napadač iskorištava sklonost žrtve da bude od pomoći (koja se internalizirala u formiranju društvene norme) kako bi izmamila informacije ili zadobila uslugu koja olakšava napad. Drugi način je da se tijekom napada socijalnog inženjeringa grupni pritisak uzrokovan normom društvene odgovornosti i moralnom dužnošću koristi kako bi se utjecalo na ponašanje žrtve, posebno za one koji nisu voljni pružiti pomoć [33].

5) Samootkrivanje i izgradnja odnosa

Derlega i Berg [40] istraživali su samootkrivanje i opisali učinak reciprociteta otkrivanja koji pokazuje da tijekom izgradnje društvenog odnosa samootkrivanje rezultira recipročnom samootkrivanju. Ljudi su najčešće spremni otkriti više onima koji su otvoreni te koji otkrivaju svoje probleme, tajne, tužne priče, itd. Za mnoge je zadovoljstvo biti odabran kao osoba za tuđe samootkrivanje, ne samo da ljudi više vole one koji su otvorenog karaktera već su veće šanse da će se i sami otvoriti, odnosno otkriti povjerljive informacije. Neki ljudi (većina njih su žene) posebno su vješti u navođenju ljudi da se otvore, lako mogu izmamiti intimna otkrića od drugih, čak i od onih koji inače ne otkrivaju previše. Razotkrivanje u kojem se ljudi otvaraju drugoj osobi, kao i skidanje “lažne maske” i validiranju pravog vlastitog identiteta, njeguje se stvoreni odnos što implicira povjerenje i olakšava društvenu interakciju. Navedeno služi kao česta tehnika u socijalnom inženjeringu što pokazuje značajnost načina komunikacije u cilju otkrivanja povjerljivih informacija žrtve.

4.2. Konceptualni model povezanosti psiholoških, sociooloških i tehničkih aspekta socijalnog inženjeringa

Iz perspektive žrtve u socijalnom inženjeringu, psihološki elementi ranjivosti predstavljaju određene emocionalne (psihološke) karakteristike, te su osnovni razlog zašto žrtva biva

nasamarena napadom socijalnog inženjeringa. Kao jedan od fokusa konfrontacije između napada socijalnog inženjeringa i obrane, psihološka ranjivost je ono što napadači žele iskoristiti i ono što žrtve trebaju (ili moraju) eliminirati ili ublažiti. Svaka vrsta socijalnog inženjeringa iziskuje iskorištavanje određenih psiholoških elemenata ranjivosti potencijalnih žrtava [41], što je prikazano u sljedećoj tablici. Sve navedene podatke je moguće povezati te tablično prikazati radi sažetog i olakšanog prikaza. U nastavku je prikazano primarnih 6 vrsta socijalnog inženjeringa kako bi se ilustrirala međupovezanost psiholoških, sociooloških i tehničkih aspekta socijalnog inženjeringa (tj. mehanizmi učinaka, psihološki element ranjivosti i metode napada).

Tablica 1. Konceptualni model povezanosti vrsta socijalnog inženjeringa sa psihološkim, sociološkim i tehničkim aspektima

Vrste socijalnog inženjeringa	Efektni mehanizmi	Psihološki element ranjivosti
1) Napadi krađe identiteta - napadač šalje e-mail s lažnom adresom (ili putem skačućih prozora, eng. pop-up window) kako bi obavijestio potencijalne žrtve da postoji vrlo povoljan kupon na hranu (ili povoljne ulaznice za sportske događaje) u ograničenom vremenu. E-poruke sadrže primamljive slike hrane ili strastvene sportske postere. To mami mete da kliknu na zlonamjerne URL poveznice, da otkriju privatne informacije, itd.	• IDT • Periferni put uvjeravanja • Umjetnost u nagovoru i manipulaciji • Utjecaj emocija i osjećaja na donošenje odluka • Oskudica kao percipirana vrijednost • Efekt promatrača, difuzija odgovornosti i deindividuacija	• Tuga • Suosjećanje • Želja za pomoći • Ljubaznost • Dobročinstvo • Krivnja • Lakovjernost • Strah
2) Kreiranje scenarija (eng. *pretexting*) - napadač traži povjerljive podatke pretvarajući se da je spajač optičkih kabela i pretvarajući se da, na primjer, ožičava dvjesto parnih terminala za policiju. Tko bi želio odbiti pružiti pomoć zaposleniku drugog poduzeća koji se nosi s tim teškim zadatkom? Meta (zaposlenik) je sam imao loše dane na poslu i "malo" će prekršiti pravila kako bi pomogao zaposleniku s problemom.	• Norma društvene odgovornosti i moralna dužnost • Sličnost kao proces uvjeravanja • Utjecaj emocija i osjećaja na donošenje odluka • IDT • Složenost međuodnosa povjerenja i socijalnog inženjeringa • Periferni put uvjeravanja	• Uzbuđenje • Sreća • Pohlepa • Ekstraverzija • Strah • Impulzivna i intuitivna prosudba • Predrasude • Zavist

	• Vjerodostojnost izvora i poslušnost autoritetu kod uvjeravanja • Efekt promatrača, difuzija odgovornosti i deindividuacija • Utjecaj emocija i osjećaja na donošenje odluka	
3) Surfanje preko ramena (eng. *shoulder surfing*) – napadač se pretvara da je dostavljač ili konzultant kako bi dobio pristup ciljnom radnom mjestu i kako bi stupio u kontakt s potencijalnom žrtvom. Kada žrtva ne obraća pažnju, napadač prikuplja informacije poput korisničkog imena i lozinke "surfajući preko ramena" žrtve, provjeravajući istaknuta mjesta poput bilješki i dokumenata.	• Umjetnost u nagovoru i manipulaciji • IDT • Utjecaj emocija i osjećaja na donošenje odluka • Oskudica kao percipirana vrijednost	• Nemarnost • Nepromišljenost • Lakovjernost • Ljubaznost • Neznanje
4) Mamac – napadač namjerno ostavlja USB stick pored računala zaposlenika, USB može sadržavati logo samog poduzeća radi stjecanja povjerenja. Kada zaposlenik priključi USB disk u svoje računalo, zaraženi software izvršava napad nezaštićenih računalnih materijala.	• Sličnost kao proces uvjeravanja • IDT • Periferni put uvjeravanja • Utjecaj emocija i osjećaja na donošenje odluka	• Znatiželja • Uzbuđenje • Pohlepa • Želja za pomoći • Neiskusnost
5) Napad izmamljivanja – u grupnom razgovoru određene organizacije, dvoje napadača mogu pokrenuti temu otkrivajući vlastitu lozinku za koju je jedan napadač saznao da nije dovoljno snažna te kako ju je potrebno korigirati. Zatim, drugi napadač također otkriva svoju lozinku (ili se može raditi o nekoj drugoj suptilnijoj povjerljivoj informaciji) te se polako pokušava kroz razgovor navoditi zaposlenike da odaju vlastite povjerljive informacije	• Utjecaj i sukladnost grupe • Normativni i informacijski utjecaj • Teorija socijalne razmjene i norma reciprociteta • Samootkrivanje i izgradnja odnosa • IDT	• Konformizam • Prijaznost • Ekstraverzija • Lakovjernost • Učtivost • Poniznost • Nepovjerenje

6) Obrnuti napadi socijalnog inženjeringa – napadač šalje novom zaposleniku e-mail putem lažne mail adrese u kojem obavještava da će se uskoro provesti mrežni test, a ako dođe do kvara mreže, da kontaktira određeni telefonski broj. Napadač kreira grešku na mreži i čeka zahtjev novog zaposlenika. Nakon što je pomogao u rješavanju problema, napadač traži da ispuni anketu koja se koristi za razvoj programa obuke o sigurnosti za nove zaposlenike. U određenom pitanju se može tražiti otkrivanje lozinke za procjenu svijesti o sigurnosti novih zaposlenika.	• Teorija socijalne razmjene i norma reciprociteta • Utjecaj emocija i osjećaja na donošenje odluka, • Utjecaj i sukladnost grupe • IDT	• Neiskustvo • Intuitivna prosudba • Prijaznost • Lakovjernost • Konformizam • Želja za pomaganjem

Izvor: Wang i sur. (2021:11905)

Konceptualni model predstavljen u tablici pruža integrativnu i strukturnu perspektivu za razumijevanje kako napadi socijalnog inženjeringa djeluju iz različitih gledišta. Iako ovaj konceptualni model nije dovoljan za predstavljanje ontologije domene socijalnog inženjeringa, identificirao je tri značajna povezana aspekta kako bi se prikazalo putem kojih efektnih mehanizama socijalni inženjering djeluje. Ovaj model prenosi sažetu ideju da napadač unutar socijalnog inženjeringa formulira određene scenarije napada kako bi potaknuo kombinaciju metoda napada, mehanizama učinka i ljudskih ranjivosti kroz koje proces napada stupa na snagu kako bi se postigao cilj napada.

ZAKLJUČAK

Provodeći istraživanje o raznim načinima socijalnog inženjeringa i umjetnosti obmanjivanja te manipuliranja, može se zaključiti da i nakon korištenja najboljih, pa čak i najskupljih sigurnosnih tehnologija, organizacije i pojedinci su još uvijek potpuno ranjivi kao potencijalne žrtve socijalnog inženjeringa. To znači da je dobrom napadaču vrlo lako prikupiti informacije o toj organizaciji stjecanjem povjerenja i prijateljskim odnosom s pojedincima ili zaposlenicima. Tehnike socijalnog inženjeringa prikupljanja informacija koriste se već dugo no svakodnevno se pojavljuju novi te napredniji načini manipuliranja i obmanjivanja. Pojedinci i organizacije prije nisu bili previše svjesni ovih praksi i tehnika za osiguranje informacija, no danas je informacijska sigurnost glavna briga korporativnog svijeta. Ključni mehanizam za borbu protiv socijalnog inženjeringa mora biti edukacija potencijalnih žrtava kako bi se podigla njihova svijest o tehnikama socijalnog inženjeringa i kako ih uočiti. Odnosno, za zaštitu od socijalnog inženjeringa ključno je obrazovanje zaposlenika ili pojedinca, obuka i održavanje svijesti. Politike, procedure i standardi važan su dio cjelokupne kampanje protiv socijalnog inženjeringa.

Ovaj završni rad opisuje konceptualni model koji osigurava integrativni i strukturni pregled funkcioniranja temeljnih vrsta napada socijalnog inženjeringa kroz psihološke, sociološke i tehničke aspekte. Konceptualni model obuhvaća tri temeljna entiteta (mehanizmi učinaka, psihološki element ranjivosti i metode napada socijalnog inženjeringa) kako bi se dobio uvid u to kako napadi socijalnog inženjeringa djeluju na pojedince i organizacije. Konačno, predstavljena su šest temeljna scenarija napada socijalnog inženjeringa kako bi se ilustrirala primjena povezanosti razumijevanja djelovanja i raznih učinaka socijalnog inženjeringa.

LITERATURA

[1]. F. Mouton et al., “Social engineering attack framework,” Proc. of Information Security for South Africa (ISSA), 2014, pp. 1-9.
(poglavlje 3.1.)
[2]. Woodward, A. How hackers exploit 'the seven deadly sins', BBC News http://www.uk/news/technology-20717773
[3]. T. R. Peltier, “Social engineering: concepts and solutions,” Information Security and Risk Management, Nov. 2006, pp. 13-21.
(poglavlje 3.2.)
[4]. Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the International Conference on Computing, Communication, and Automation, Noida, India, 29–30 April 2016; pp. 537–540.
[5]. Perotta, L.; Holtz, M.D.; David, B.M.; Deus, F.G.; De Sousa, R.T. A formal classification of internet banking attacks and vulnerabilities. Int. J. Compute. Sci. Inf. Technol. 2011, 3, 186–197.
[6]. Gafir, I. Social engineering attack strategies and defence approaches. In Proceedings of the IEEE
International Conference on Future Internet of Things and Cloud, Vienna, Austria, 22–24 August 2016;
pp. 1–5.
[7]. Granger S. Social engineering fundamentals, part I: hacker tactics. Security Focus. 2001;18.
[8]. Elicitation, 2018. Dostupno na: https://www.social engineer.org/wiki/archives/Elicitation/Definition_of_Elicitation.htm.
[9]. Nadeem MS. MailDefence Blog, 2015. Dostupno na: https://blog.MailDefence.com/what-is-baiting-in-social-engineering/.
[10]. Winkler, I. Social Engineering and Reverse Social Engineering. National Computer Security Association. 2015;82-10-43. Dostupno na: http://www.today.info/AIMS/DSM/82-10-43.pdf
[11]. Beckers, K.; Pape, S. A serious game for eliciting social engineering security requirements. In Proceedings of
the International Requirements Engineering Conference, Beijing, China, 12–16 September 2016; pp. 16–25.
[12] D. Byrne, ‘‘An overview of research and theory within the attraction paradigm,’’ J. Social Pers. Relationships, vol. 14, no. 3, pp. 417–431, Jun. 1997.

[13] M. I. Norton, J. H. Frost, and D. Ariely, ‘‘Less is more: The lure of ambiguity, or why familiarity breeds contempt,’’ J. Personality Social Psycho., vol. 92, no. 1, p. 97, 2007.
[14] P. Miller, J. Kozu, and A. Davis, ‘‘Social influence, empathy, and prosocial behavior in cross-cultural perspective,’’ in Proc. Pract. Social Influence Multiple Cultures, 2001, pp. 63–77.
[15] R. B. Cialdini, Influence: Science and Practice. Boston, MA, USA: Allyn and Bacon, 2001.
[16] P. R. Mims, J. J. Hartnett, and W. R. Nay, ‘‘Interpersonal attraction and help volunteering as a function of physical attractiveness,’’ J. Psycho., vol. 89, no. 1, pp. 125–131, Jan. 1975.
[17] P. C. Rosenblatt, ‘‘Persuasion as a function of varying amounts of distraction,’’ Psychonomic Sci., vol. 5, no. 2, pp. 85–86, Feb. 1966.
[18] D. R. Brandt, ‘‘Listener propensity to counter argue, distraction, and resistance to persuasion,’’ Central States Speech J., vol. 30, no. 4, pp. 321–331, Dec. 1979.
[19] C. K., Höfling, E. Protzman, S. Dalrymple, N. Graves, and C. M. Pierce, ‘‘An experimental study in nurse-physician relationships,’’ The J. Nervous Mental Disease, vol. 143, no. 2, pp. 171–180, 1966. [20] S. Milgram and C. Gudehus, Obedience to Authority. New York, NY, USA: Ziff-Davis, 1978. [17] K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Hoboken, NJ, USA: Wiley, Aug. 2011.
[21] M. Butavicius, K. Parsons, M. Pattinson, and A. McCormack, ‘‘Breaching the human firewall: Social engineering in phishing and spear-phishing emails,’’ 2016, arXiv:1606.00887. [Online]. Available: http://arXiv.org/abs/1606.00887
[22] R. E. Petty, ‘‘A cognitive response analysis of the temporal persistence of attitude changes induced by persuasive communications,’’ Ph.D. dissertation, Graduate School, Ohio State Univ., Columbus, OH, USA, 1977. [Online]. Available: http://rave.ohiolink.edu/etic/view?acc
[23] R. E. Petty and J. T. Cacioppo, Attitudes Persuasion: Classic Contemporary Approaches. Dubuque, IA, USA: Wm. C. Brown, 1981.
[24] R. E. Petty and J. T. Cacioppo, Communication and Persuasion: Central and Peripheral Routes to Attitude Change. Berlin, Germany: Springer-Verlag, 1986.
[25] R. E. Petty and J. T. Cacioppo, ‘‘The Elaboration Likelihood Model of Persuasion,’’ in Advances in Experimental Social Psychology, vol. 19, L. Berkowitz, Ed. New York, NY, USA: Academic, Jan. 1986, pp. 123–205. [Online]. Available: http://www.sciencedirect.com/science/ article/pii/
[26] K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Hoboken, NJ, USA: Wiley, Aug. 2011.

[27] M. Butavicius, K. Parsons, M. Pattinson, and A. McCormack, ‘‘Breaching the human firewall: Social engineering in phishing and spear-phishing emails,’’ 2016, arXiv:1606.00887. [Online]. Available: http://arXiv.org/abs/1606.00887
[28] J. L. Freedman and S. C. Fraser, ‘‘Compliance without pressure: The flotin-the-door technique,’’ J. Personality Social Psycho., vol. 4, no. 2, p. 195, 1966.
[29] B. Latané and J. M. Dabbs, Jr., ‘‘Sex, group size and helping in three cities,’’ Sociometry, vol. 1, pp. 180–194, Jun. 1975
[30] S. G. Harkins and J. M. Jackson, ‘‘The role of evaluation in eliminating social loafing,’’ Personality Social Psycho. Bull., vol. 11, no. 4, pp. 457–465, Dec. 1985.
[31] A. Chitre, D. Singh, and V. Singh, ‘‘A comprehensive study of social engineering based attacks in India to develop a conceptual model,’’ Int. J. Inf. Net. Secure. (IVINS), vol. 1, no. 2, p. 45, Jun. 2012.
[32] R. C. Mayer, J. H. Davis, and F. D. Schoolman, ‘‘An integrative model of organizational trust,’’ Acad. Manage. Rev., vol. 20, no. 3, pp. 709–734, Jul. 1995.
[33] P. Sztompka, Trust: A Sociological Theory. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[34] J. K. Burgeon and D. B. Buller, Interpersonal Deception Theory. Atlanta, GA, USA: American Cancer Society, Dec. 2015, pp. 1–6.
[35] J. E. LeDoux and R. Brown, ‘‘A higher-order theory of emotional consciousness,’’ Proc. Nat. Acad. Sci. USA, vol. 114, no. 10, pp. iR2016– iR2025, Mar. 2017.
[36] E. A. Phelps, K. M. Lempert, and P. Sokol-Hessler, ‘‘Emotion and decision making: Multiple modulator neural circuits,’’ Annu. Rev. Neurosci., vol. 37, no. 1, pp. 263–287, Jul. 2014.
[37] M. Deutsch and H. B. Gerard, ‘‘A study of normative and informational social influences upon individual judgment,’’ The J. Abnormal Social Psycho., vol. 51, no. 3, p. 629, 1955.
[38] A. W. Goldner, ‘‘The norm of reciprocity: A preliminary statement,’’ Amer. Sociol. Rev., vol. 4, pp. 161–178, Dec. 1960.
[39] L. Berkowitz, ‘‘Social norms, feelings, and other factors affecting helping and altruism,’’ in Advances in experimental social psychology, vol. 6. Amsterdam, The Netherlands: Elsevier, 1972, pp. 63–108.
[40] V. J. Derlega and J. H. Berg, Self-Disclosure: Theory, Research, and Therapy. Cham, Switzerland: Springer, 1987.
[41] Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895-11910. Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.number=9323026 (04.04.2022.)

POPIS TABLICA