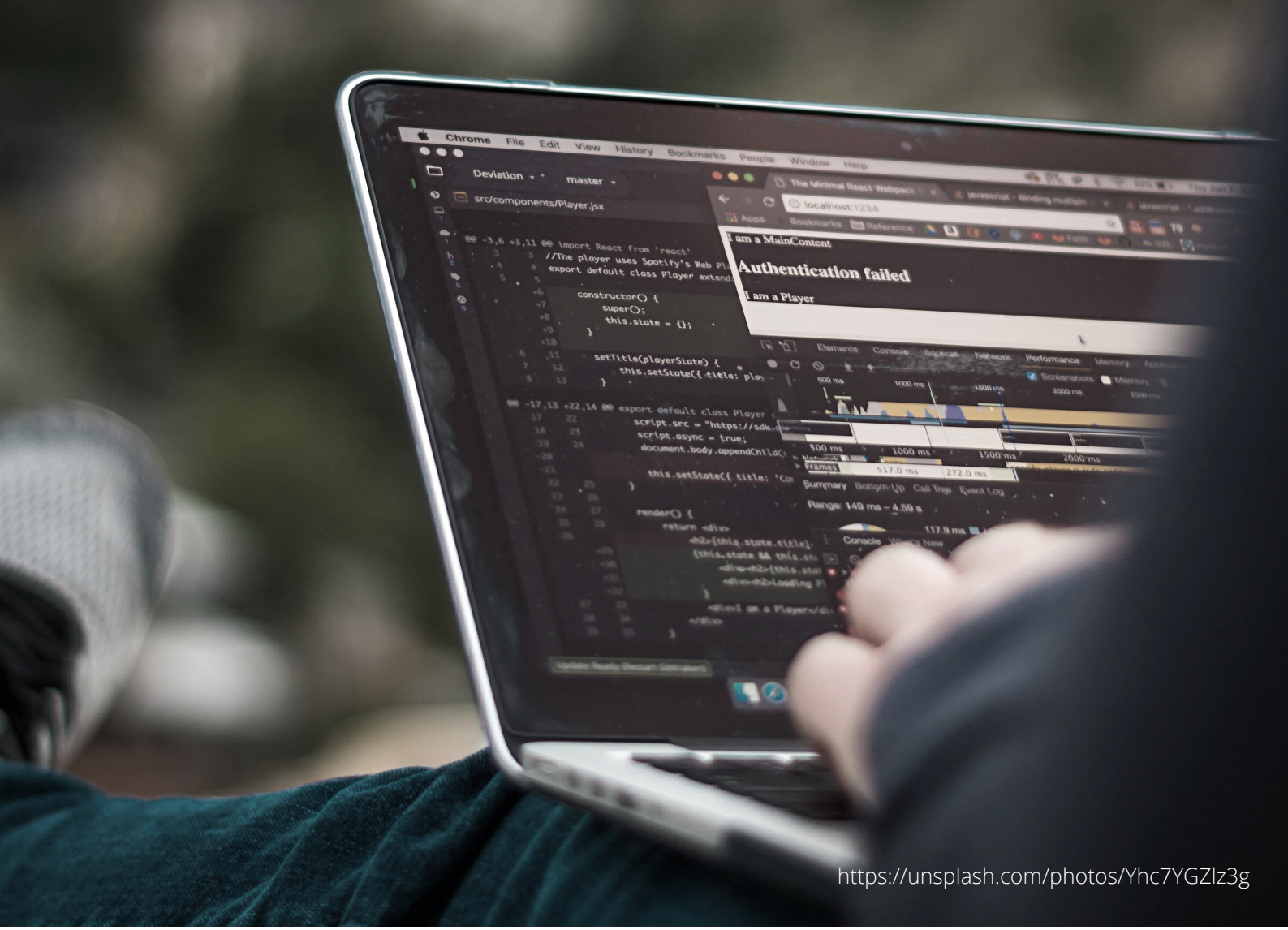


https://unsplash.com/photos/Yhc7YGZlz3g

SOCIJALNI INŽENJERING

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

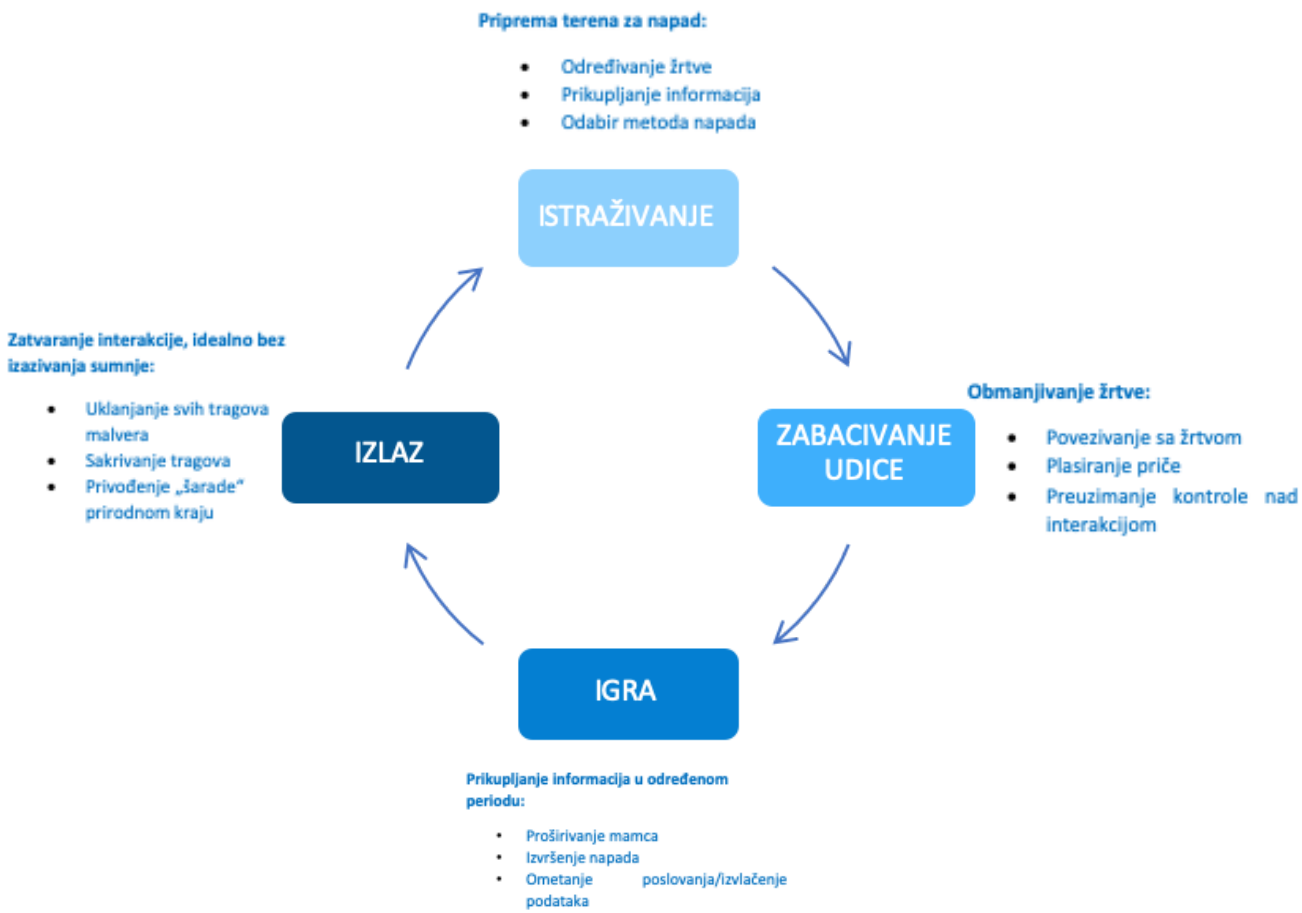
SRB-CERT

SOCIJALNI INŽENJERING

Socijalni inženjering predstavlja tip sajber napada, koji sadrži širok spektar manipulacija kojima se ljudi navode da odaju poverljive informacije o sebi ili kompaniji u kojoj rade.

Psihološkom manipulacijom korisnici se navode na odavanje informacija o kompaniji u kojoj rade, ali i na kršenje bezbednosnih mera kompanije. Drugim rečima, socijalni inženjering je svaka aktivnost koja podrazumeva navođenje korisnika/osobe da preduzme radnju koju inače ne bi preduzeo, a sve u cilju prikupljanja što većeg broja podataka koji se kasnije mogu zloupotrebiti. „Socijalni inženjeri" zloupotrebljavaju ranjivost koju poseduje svaka organizacija – ljudsku psihologiju, sa ciljem da nešto dobiju od vas (lozinka, drugi podaci o zaposlenima ili informacionom sistemu) ili da vi učinite nešto za njih (određena uplata, omogućite ulaz u prostorije kompanije i sl.).

Napadi socijalnog inženjeringa se odvijaju u nekoliko faza. Napadač prvo istražuje žrtvu od koje namerava da prikupi osnovne informacije poput potencijalnih načina ulaska i ranjivosti bezbednosnih protokola. Zatim, napadač radi na zadobijanju poverenja žrtve i navodi je na aktivnosti kojima se krše mere zaštite i bezbednosne procedure, poput otkrivanja osetljivih informacija ili odobravanja pristupa kritičnim resursima. U idealno osmišljenim napadima poslednja faza podrazumeva uklanjanje svih tragova manipulativnog ponašanja, odnosno malvera (Slika 1).



Slika 1. Životni ciklus napada socijalnog inženjeringa

Ono što socijalni inženjering čini problemom visokog rizika je to što se oslanja na ljudsku grešku, a ne na ranjivosti hardvera, softvera i operativnih sistema. Greške koje su napravili legitimni korisnici su teže predvidive i teže ih je identifikovati i umanjiti, nego malver napad.

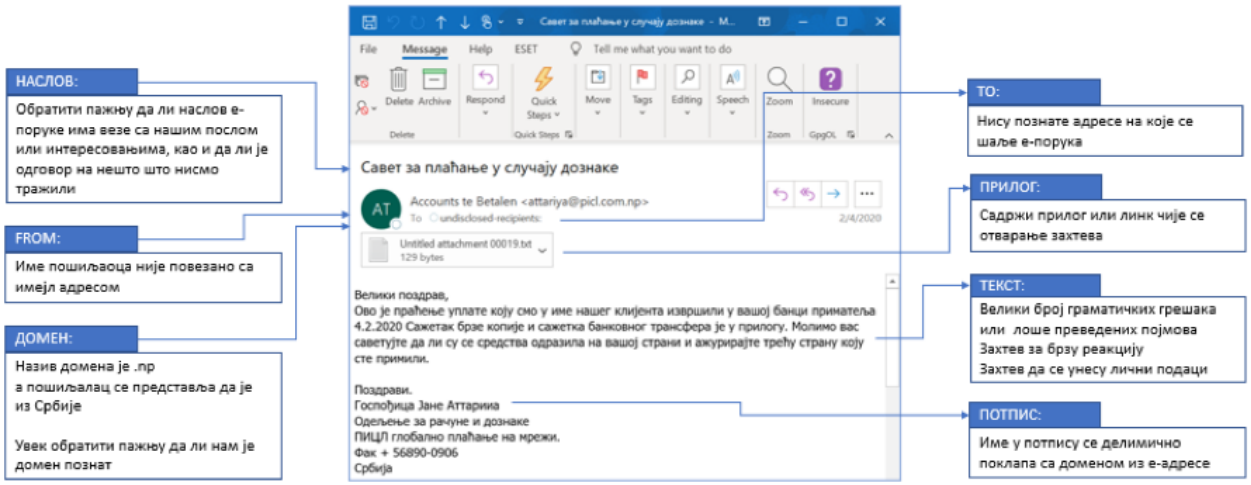
Napadi socijalnog inženjeringa imaju mnogo različitih formi i mogu se sprovesti svuda gde postoji interakcija - socijalni odnos među ljudima.

Najčešći oblici napada socijalnog inženjeringa su:

- *Phishing*
- *Spear phishing*
- *Baiting*
- *Pretexting*
- *Scareware*
- *Tailgating*

1. *PHISHING*

Fišing je jedan od najčešćih vidova napada socijalnog inženjeringa. Šta je fišing?



Slika 2. *Phishing*

Poruka e-pošte ili SMS poruka koja primaoca navodi na brzu reakciju, a ima za cilj krađu kredencijala ili distribuciju zlonamernog softvera. Tekst poruke stvara osećaj straha, hitnosti ili radoznalosti, pa se od primaoca poruke traži klik na link ili preuzimanje dokumenta iz priloga. Klik na link vodi na lažnu stranicu, koja liči na legitimnu, i kreirana je u cilju prikupljanja podataka kao što su e-adresa i lozinka. Klik na „*Enable Content*" ili „*Enable Editing*" u dokumentu iz priloga, automatski pokreće zlonamerni softver koji ubrizgava određene procese u operativni sistem primaoca, kako bi onemogućio detekciju od strane antivirusa i drugih bezbednosnih softverskih rešenja.

S obzirom da se identične ili skoro identične poruke šalju svim korisnicima u fišing kampanjama, njihovo otkrivanje i blokiranje je mnogo lakše za mejl servere koji imaju pristup platformi za deljenje pretnji (*Threat Intelligence*).

Više o načinima umanjenja rizika od fišing napada možete pronaći ovde

2. SPEAR PHISHING

Ovo je ciljana verzija prevare fišingom kojom napadač bira određene pojedince ili kompanije.

Tekst poruke se kreira na osnovu karakteristika pojedinca ili kompanije, radnih mesta i kontakata žrtava, kako bi napad bio manje upadljiv. Ovaj tip fišinga zahteva od napadača mnogo više napora, a za realizaciju napada može biti potrebno i nekoliko nedelja i meseci. Ukoliko se vešto izvedu veoma ih je teško detektovati i imaju visok stepen uspešnosti.

Jedan od scenarija *spear phishing*-a je onaj u kojem se napadač predstavlja kao kolega iz IT službe i šalje poruku e-pošte jednom ili više zaposlenih. Tekst poruke, potpis i način komunikacije je vrlo sličan uobičajenom načinu komunikacije sa IT službom što primaoce navodi da misle da je poruka autentična. Porukom se traži od primalaca da promene lozinku klikom na link, koji ih preusmerava na zlonamernu internet stranicu na kojoj napadač snima sve kredencijale koje unesu.

3. BAITING

Baiting je napad veoma sličan fišingu, ali ono što ih razlikuje od drugih vrsta socijalnog inženjeringa je obećanje neke stvari ili dobra koje napadači koriste kako bi privukli žrtve.

Korišćenjem lažnog obećanja napadač „igra na kartu“ pohlepe ili radoznalosti žrtve i tako je namamljuje u klopku koja krade lične podatke ili distribuira malver u operativni sistem organizacije u kojoj žrtva radi. Najčešći oblik „mamca“ je fizički medijum za širenje zlonamernog softvera.

Na primer, napadači ostavljaju mamac, najčešće USB sa zaraženim malverom na vidljivim mestima gde potencijalne žrtve mogu sigurno da ga vide (npr. toalet, lift, parking, hodnik). USB ima autentičan izgled, kao što je nalepnica na kojoj piše ''Plate'' kako bi žrtve iz radoznalosti pokupile „mamac“, ubacile u poslovni ili kućni računar i automatski instalirale zlonamerni softver.

Onlajn *baiting* napad za mamac koristi primamljive oglase za besplatno preuzimanje muzike, filmova ili aplikacija sa internet stranica koje su zaražene zlonamernim softverom.

4. PRETEXTING

Ovo je vrsta socijalnog inženjeringa kod koje se napadači fokusiraju na stvaranje dobrog izgovora ili izmišljenog scenarija, koji koriste za pokušaj krađe ličnih podataka žrtava.

Napadač vešto kreira lažnu informaciju i obično telefonom ili u direktnom kontaktu traži određenu dopunu informacija od žrtve, koja je neophodna da bi se potvrdio njen identitet. Podatke koje pribavi na ovaj način napadač zapravo koristi za krađu identiteta ili u izvršenju nekog drugog krivičnog dela.

Napad obično započinje uspostavljanjem poverenja sa žrtvom lažnim predstavljanjem, kao saradnika, policije, bankarskih i poreskih službenika, ili drugih službenih lica. Na ovaj način prikupljaju se sve vrste relevantnih informacija i zapisa, poput jedinstvenih matičnih brojeva, adrese stanovanja, telefonskih brojeva, datuma odmora, bankovnih evidencija, pa čak i podataka o merama zaštite i bezbednosti kompanije u kojoj je žrtva zaposlena.

Napredniji napadi navode žrtve da zloupotrebe ranjivosti kompanije u kojoj rade, bilo fizičke ili digitalne. Na primer, napadač može da se predstavi kao spoljni revizor IT usluga fizičkom obezbeđenju kompanije i zatraži dozvolu za ulazak u zgradu. Dok fišing napadi uglavnom zloupotrebljavaju strah i hitnost, ovi napadi koji se oslanjaju na izgradnju lažnog osećaja poverenja sa žrtvom, kroz verodostojnu priču koja žrtvi ostavlja malo prostora za sumnju.

5. SCAREWARE

Scareware predstavlja napad lažnim alarmima i izmišljenim pretnjama, kojim se žrtva obaveštava da je njen operativni sistem zaražen zlonamernim softverom i navodi da instaliraju softver koji će im pomoći da se reše zlonamernog sadržaja, a zapravo od softvera koji instaliraju nema stvarne koristi za korisnika, već za napadača.

Uobičajeni primer ovog napada su baneri koji se pojavljuju u vašem veb pretraživaču dok pretražujete na internetu, na kojima se obično prikazuje tekst poput „Računar može biti zaražen štetnim špijunskim softverom“. Ili vam se nudi da instalirate alat koji je zaražen malverom ili vas usmerava na zlonamernu lokaciju na kojoj se računar zarazi.

Scareware napad se može sprovesti i putem neželjenih poruka e-pošte kojima se dostavljaju lažna upozorenja ili korisnicima nudi kupovina rizičnih (bezvrednih ili štetnih) usluga.

6. *TAILGATING*

Ovo je vrsta napada kod koje napadač, iako bez odgovarajuće dozvole, dospe u prostorije kojima je pristup zabranjen tako što prati zaposlenog koji ima odgovarajuću dozvolu/autentifikaciju.

Napadač se može predstavljati kao vozač isporuke i čekati ispred zgrade pravi trenutak da započne napad i kada zaposleni otvori vrata, napadač traži od zaposlenog da zadrži vrata i na taj način dobija pristup zgradi.

Ovaj vid napada je znatno teže izvesti u kompanijama kod kojih je za ulazak u zgradu potrebna tzv. ključ kartica. Međutim, u nekim kompanijama napadači mogu da započnu razgovor sa zaposlenima i iskoriste ovo kratko poznanstvo da bi prošli pored obezbeđenja koje je na ulazu. Zato se posebna pažnja zahteva na tačkama pristupa službenim prostorijama, kao što su područja za isporuku i utovar, preko kojih napadači mogu neovlašćeno ući u službene prostorije i otpočeti realizaciju plana napada.

PREPORUKE ZA PREVENCIJU OD NAPADA SOCIJALNOG INŽENJERINGA

Socijalni inženjeri manipulišu ljudskom psihologijom, odnosno osećanjima kao što su radoznalost ili strah, kako bi sproveli svoje planove i uvukli žrtve u svoje zamke. Zato budite obazrivi kada primite e-poštu kojom se od vas zahteva hitna reakcija, kada vas privuče ponuda prikazana na internet stranici ili kada naiđete na „izgubljeni“ USB.

Obazrivost vam može pomoći da se zaštitite od većine napada socijalnog inženjeringa u sajber prostoru, kao i rad na sebi i svom znanju. Odbranite se znanjem :

- Ne otvarajte poruke e-pošte i priloge iz sumnjivih izvora

Ako ne poznajete pošiljaoca ne morate da odgovarate na poruku, čak i ako ga poznajete, a sumnjate u verodostojnost poruke poželjno je da dodatno proverite i potvrdite informacije iz drugih izvora, putem telefona ili preko zvanične internet stranice. Treba imati na umu da se adrese e-pošte mogu lažirati, a čak i e-pošta poslata iz pouzdanog izvora može biti kreirana od strane napadača. Ukoliko ste primili poruku e-pošte od vaše banke, ne mora da znači da je zaista od vaše banke jer je lažiranje ovog tipa moguće izvesti. Ukoliko ste pronašli USB proverite sa nadležnim kolegama da li je sadržaj legitiman, jer može sadržati zlonamerni softver koji samo čeka da bude instaliran.

- Korišćenje multifaktorske autentifikacije

Jedna od najvažnijih i najvrednijih informacija koje napadači pokušavaju da pribave su kredencijali korisnika. Korišćenje multifaktorske autentifikacije obezbeđuje zaštitu vašeg naloga u slučaju kompromitovanja operativnog sistema.

- Pazite na primamljive ponude

Ako ponuda zvuči previše primamljivo, neophodan je dodatni oprez i provera svakog zahteva kojim se od vas traži dostavljanje podataka, klik na link ili preuzimanje besplatnog sadržaja. Često vam i pretraživanje teme na internetu može brzo pomoći da utvrdite da li ste primili legitimnu ponudu ili je u pitanju „mamac".

- Redovno ažuriranje antivirusnih/antimalver softvera

Preporuka je aktiviranje automatskog ažuriranja antivirusnog/antimalver softvera. Poželjno je periodično skeniranje operativnih sistema kako bi proverili postojanje eventualnih pretnji. Nema antivirusa/antimalver softvera koji u potpunosti mogu zaštiti korisnike od mogućih pretnji i rizika od kompromitovanja podataka, ali svakako pružaju zaštitu od većine aktuelnih pretnji.

Nacionalni CERT Republike Srbije ne promoviše ili favorizuje bilo koji od korišćenih javnih izvora, među kojima su i komercijalni proizvodi i usluge. Sve preporuke, analize i predlozi dati su u cilju prevencije i zaštite od bezbednosnih rizika.

Izvori:

https://www.imperva.com/learn/application-security/social-engineering-attack/

https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/