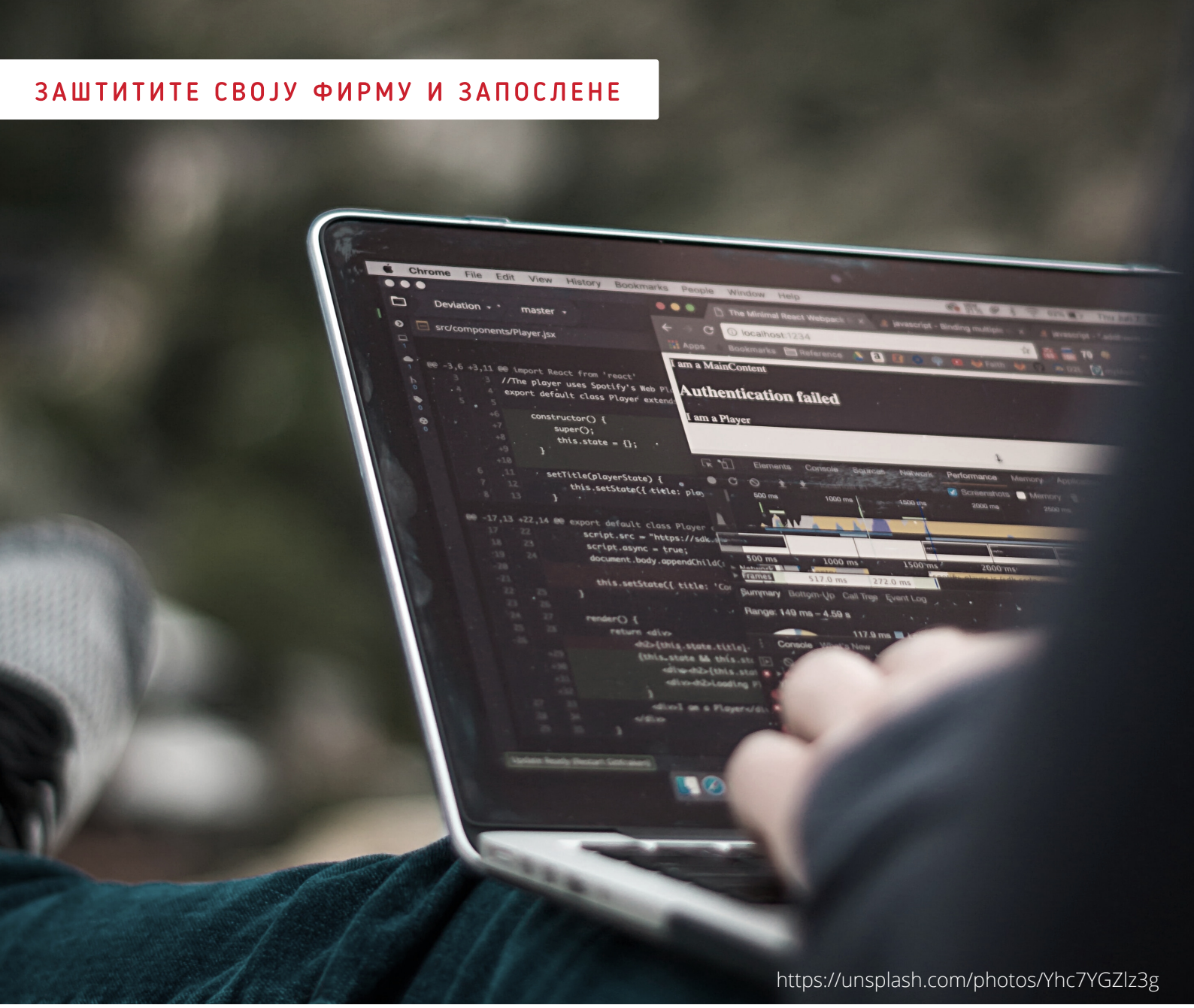
ЗАШТИТИТЕ СВОЈУ ФИРМУ И ЗАПОСЛЕНЕ



https://unsplash.com/photos/Yhc7YGZlz3g

СОЦИЈАЛНИ ИНЖЕЊЕРИНГ

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

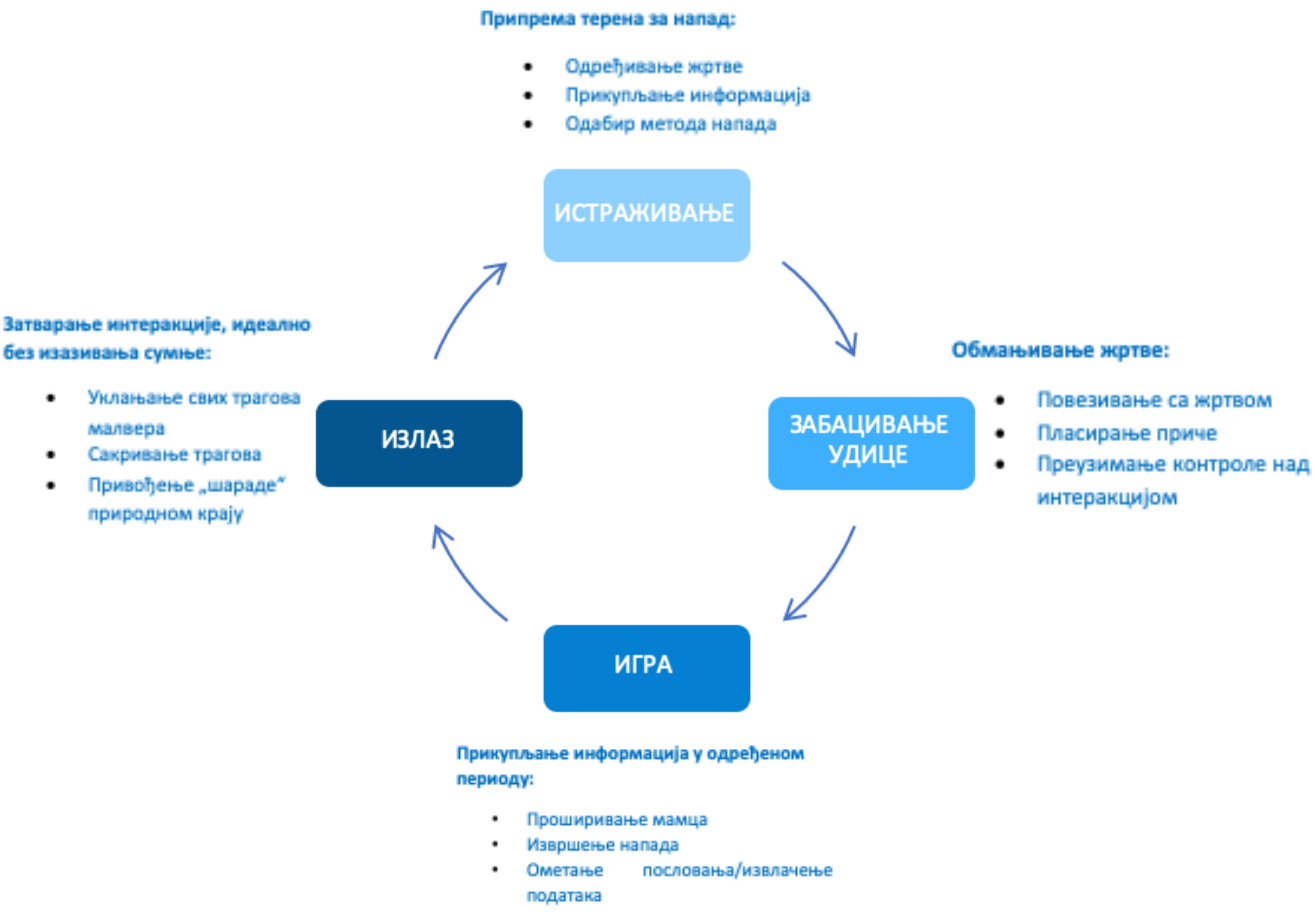
СРБ-ЦЕРТ

СОЦИЈАЛНИ ИНЖЕЊЕРИНГ

Социјални инжењеринг представља тип сајбер напада, који садржи широк спектар манипулација којима се људи наводе да одају поверљиве информације о себи или компанији у којој раде.

Психолошком манипулацијом корисници се наводе на одавање информација о компанији у којој раде, али и на кршење безбедносних мера компаније. Другим речима, социјални инжењеринг је свака активност која подразумева навођење корисника/особе да предузме радњу коју иначе не би предузео, а све у циљу прикупљања што већег броја података који се касније могу злоупотребити. „Социјални инжењери“ злоупотребљавају рањивост коју поседује свака организација – људску психологију, са циљем да нешто добију од вас (лозинка, други подаци о запосленима или информационом систему) или да ви учините нешто за њих (одређена уплата, омогућите улаз у просторије компаније и сл.).

Напади социјалног инжењеринга се одвијају у неколико фаза. Нападач прво истражује жртву од које намерава да прикупи основне информације попут потенцијалних начина уласка и рањивости безбедносних протокола. Затим, нападач ради на задобијању поверења жртве и наводи је на активности којима се крше мере заштите и безбедносне процедуре, попут откривања осетљивих информација или одобравања приступа критичним ресурсима. У идеално осмишљеним нападима последња фаза подразумева уклањање свих трагова манипулативног понашања, односно малвера (Слика 1).



Слика 1. Животни циклус напада социјалног инжењеринга

Оно што социјални инжењеринг чини проблемом високог ризика је то што се ослања на људску грешку, а не на рањивости хардвера, софтвера и оперативних система. Грешке које су направили легитимни корисници су теже предвидиве и теже их је идентификовати и умањити, него малвер напад.

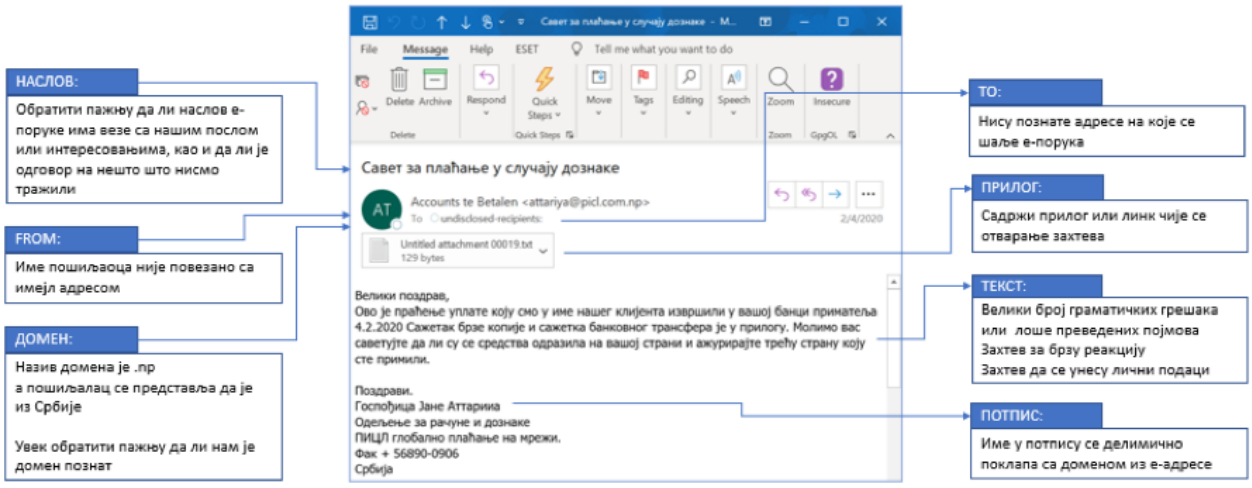
Напади социјалног инжењеринга имају много различитих форми и могу се спровести свуда где постоји интеракција - социјални однос међу људима.

Најчешћи облици напада социјалног инжењеринга су:

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

1. *PHISHING*

Фишинг је један од најчешћих видова напада социјалног инжењеринга. Шта је фишинг?



Слика 2. *Phishing*

Порука е-поште или SMS порука која примаоца наводи на брзу реакцију, а има за циљ крађу креденцијала или дистрибуцију злонамерног софтвера. Текст поруке ствара осећај страха, хитности или радозналости, па се од примаоца поруке тражи клик на линк или преузимање документа из прилога. Клик на линк води на лажну страницу, која личи на легитимну, и креирана је у циљу прикупљања података као што су е-адреса и лозинка. Клик на „*Enable Content*" или „*Enable Editing*" у документу из прилога, аутоматски покреће злонамерни софтвер који убризгава одређене процесе у оперативни систем примаоца, како би онемогућио детекцију од стране антивируса и других безбедносних софтверских решења.

С обзиром да се идентичне или скоро идентичне поруке шаљу свим корисницима у фишинг кампањама, њихово откривање и блокирање је много лакше за мејл сервере који имају приступ платформи за дељење претњи (*Threat Intelligence*).

Више о начинима умањења ризика од фишинг напада можете пронаћи овде

2. SPEAR PHISHING

Ово је циљана верзија преваре фишингом којом нападач бира одређене појединце или компаније.

Текст поруке се креира на основу карактеристика појединца или компаније, радних места и контаката жртава, како би напад био мање упадљив. Овај тип фишинга захтева од нападача много више напора, а за реализацију напада може бити потребно и неколико недеља и месеци. Уколико се вешто изведу веома их је тешко детектовати и имају висок степен успешности.

Један од сценарија *spear phishing*-а је онај у којем се нападач представља као колега из ИТ службе и шаље поруку е-поште једном или више запослених. Текст поруке, потпис и начин комуникације је врло сличан уобичајеном начину комуникације са ИТ службом што примаоце наводи да мисле да је порука аутентична. Поруком се тражи од прималаца да промене лозинку кликом на линк, који их преусмерава на злонамерну интернет страницу на којој нападач снима све креденцијале које унесу.

3. BAITING

Baiting је напад веома сличан фишингу, али оно што их разликује од других врста социјалног инжењеринга је обећање неке ствари или добра које нападачи користе како би привукли жртве.

Коришћењем лажног обећања нападач „игра на карту“ похлепе или радозналости жртве и тако је намамљује у клопку која краде личне податке или дистрибуира малвер у оперативни систем организације у којој жртва ради. Најчешћи облик „мамца“ је физички медијум за ширење злонамерног софтвера.

На пример, нападачи остављају мамац, најчешће USB са зараженим малвером на видљивим местима где потенцијалне жртве могу сигурно да га виде (нпр. тоалет, лифт, паркинг, ходник). USB има аутентичан изглед, као што је налепница на којој пише ''Плате'' како би жртве из радозналости покупиле „мамац“, убациле у пословни или кућни рачунар и аутоматски инсталирале злонамерни софтвер.

Онлајн *baiting* напад за мамац користи примамљиве огласе за бесплатно преузимање музике, филмова или апликација са интернет страница које су заражене злонамерним софтвером.

4. PRETEXTING

Ово је врста социјалног инжењеринга код које се нападачи фокусирају на стварање доброг изговора или измишљеног сценарија, који користе за покушај крађе личних података жртава.

Нападач вешто креира лажну информацију и обично телефоном или у директном контакту тражи одређену допуну информација од жртве, која је неопходна да би се потврдио њен идентитет. Податке које прибави на овај начин нападач заправо користи за крађу идентитета или у извршењу неког другог кривичног дела.

Напад обично започиње успостављањем поверења са жртвом лажним представљањем, као сарадника, полиције, банкарских и пореских службеника, или других службених лица. На овај начин прикупљају се све врсте релевантних информација и записа, попут јединствених матичних бројева, адресе становања, телефонских бројева, датума одмора, банковних евиденција, па чак и података о мерама заштите и безбедности компаније у којој је жртва запослена.

Напреднији напади наводе жртве да злоупотребе рањивости компаније у којој раде, било физичке или дигиталне. На пример, нападач може да се представи као спољни ревизор ИТ услуга физичком обезбеђењу компаније и затражи дозволу за улазак у зграду. Док фишинг напади углавном злоупотребљавају страх и хитност, ови напади који се ослањају на изградњу лажног осећаја поверења са жртвом, кроз веродостојну причу која жртви оставља мало простора за сумњу.

5. SCAREWARE

Scareware представља напад лажним алармима и измишљеним претњама, којим се жртва обавештава да је њен оперативни систем заражен злонамерним софтвером и наводи да инсталирају софтвер који ће им помоћи да се реше злонамерног садржаја, а заправо од софтвера који инсталирају нема стварне користи за корисника, већ за нападача.

Уобичајени пример овог напада су банери који се појављују у вашем веб претраживачу док претражујете на интернету, на којима се обично приказује текст попут „Рачунар може бити заражен штетним шпијунским софтвером“. Или вам се нуди да инсталирате алат који је заражен малвером или вас усмерава на злонамерну локацију на којој се рачунар зарази.

Scareware напад се може спровести и путем нежељених порука е-поште којима се достављају лажна упозорења или корисницима нуди куповина ризичних (безвредних или штетних) услуга.

6. *TAILGATING*

Ово је врста напада код које нападач, иако без одговарајуће дозволе, доспе у просторије којима је приступ забрањен тако што прати запосленог који има одговарајућу дозволу/аутентификацију.

Нападач се може представљати као возач испоруке и чекати испред зграде прави тренутак да започне напад и када запослени отвори врата, нападач тражи од запосленог да задржи врата и на тај начин добија приступ згради.

Овај вид напада је знатно теже извести у компанијама код којих је за улазак у зграду потребна тзв. кључ картица. Међутим, у неким компанијама нападачи могу да започну разговор са запосленима и искористе ово кратко познанство да би прошли поред обезбеђења које је на улазу. Зато се посебна пажња захтева на тачкама приступа службеним просторијама, као што су подручја за испоруку и утовар, преко којих нападачи могу неовлашћено ући у службене просторије и отпочети реализацију плана напада.

ПРЕПОРУКЕ ЗА ПРЕВЕНЦИЈУ ОД НАПАДА СОЦИЈАЛНОГ ИНЖЕЊЕРИНГА

Социјални инжењери манипулишу људском психологијом, односно осећањима као што су радозналост или страх, како би спровели своје планове и увукли жртве у своје замке. Зато будите обазриви када примите е-пошту којом се од вас захтева хитна реакција, када вас привуче понуда приказана на интернет страници или када наиђете на „изгубљени“ USB.

Обазривост вам може помоћи да се заштитите од већине напада социјалног инжењеринга у сајбер простору, као и рад на себи и свом знању. Одбраните се знањем :

- Не отварајте поруке е-поште и прилоге из сумњивих извора

Ако не познајете пошиљаоца не морате да одговарате на поруку, чак и ако га познајете, а сумњате у веродостојност поруке пожељно је да додатно проверите и потврдите информације из других извора, путем телефона или преко званичне интернет странице. Треба имати на уму да се адресе е-поште могу лажирати, а чак и е-пошта послата из поузданог извора може бити креирана од стране нападача. Уколико сте примили поруку е-поште од ваше банке, не мора да значи да је заиста од ваше банке јер је лажирање овог типа могуће извести. Уколико сте пронашли USB проверите са надлежним колегама да ли је садржај легитиман, јер може садржати злонамерни софтвер који само чека да буде инсталиран.

- Коришћење мултифакторске аутентификације

Једна од најважнијих и највреднијих информација које нападачи покушавају да прибаве су креденцијали корисника. Коришћење мултифакторске аутентификације обезбеђује заштиту вашег налога у случају компромитовања оперативног система.

- Пазите на примамљиве понуде

Ако понуда звучи превише примамљиво, неопходан је додатни опрез и провера сваког захтева којим се од вас тражи достављање података, клик на линк или преузимање бесплатног садржаја. Често вам и претраживање теме на интернету може брзо помоћи да утврдите да ли сте примили легитимну понуду или је у питању „мамац“.

- Редовно ажурирање антивирусних/антималвер софтвера

Препорука је активирање аутоматског ажурирања антивирусног/антималвер софтвера. Пожељно је периодично скенирање оперативних система како би проверили постојање евентуалних претњи. Нема антивируса/антималвер софтвера који у потпуности могу заштити кориснике од могућих претњи и ризика од компромитовања података, али свакако пружају заштиту од већине актуелних претњи.

Национални ЦЕРТ Републике Србије не промовише или фаворизује било који од коришћених јавних извора, међу којима су и комерцијални производи и услуге. Све препоруке, анализе и предлози дати су у циљу превенције и заштите од безбедносних ризика.

Извори:

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/