ГЛАСОВНИ И СМС ФИШИНГ – VISHING И SMISHING

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

VISHING, *SMISHING* И КАКО СЕ ЗАШТИТИТИ

Са развојем нових технологија, све је лакше контактирати више људи. Нападачи могу истовремено да упућују стотине позива користећи технологију *Voice Over Internet Protocol* (*VoIP*) и лако могу да подметну *ID* позиваоца да би позив изгледао као да долази из поузданог извора, као што је банка.

Овај тип напада има већи проценат успешности за нападача него фишинг поруке, због:

- Већег броја људи до којих се може доћи него путем е-порука,
- Већи степен поверења људи ка позивима него е-порукама,
- Аутоматске валидације система,
- Телефонским позивима је могуће лакше доћи до одређених циљних група, као што су припадници старије популације,
- Отварање све већег броја позивних центара је допринео повећању поверења и прихватања позива од особа које не познајемо, а питају за поверљиве информације.

Vishing и *smishing* представљају уобичајене врсте фишинг напада, који нападају жртву путем гласовних позива и слањем порука. Обе врсте користе традиционалну методу фишинг превара која од жртве захтева хитну реакцију. Циљ је сличан, док су начини испоруке различити.

ШТА ЈЕ *VISHING*?

Vishing је гласовни фишинг и представља врсту фишинг напада која се преноси путем телефонских позива и *Skype*-а, а као циљну групу има кориснике *Voice Over Internet Protocol- VoIP* услуге.

Нападачи користе различите *ID*-јеве који одају утисак да су од поуздане особе. Чини се да је позив упућен из локалног подручја или организације коју познајете. Када се позив пропусти, нападачи обично оставе поруку у којој траже да их позовете.

Нападачи имају за циљ прикупљање података о кредитним картицама, датумима рођења, креденцијалима за различите налоге или бројева телефона контаката жртве како би сазнали њене личне податке.

За време телефонског позива, нападач користи социјални инжењеринг да би жртву натерао да дели личне и финансијске податке, као што су бројеви рачуна и лозинке. Нападач се обично представља као представник полиције, особа која нуди помоћ у инсталирању софтвера (упозорење: То је вероватно злонамерни софтвер), или најчешће као представник банке говорећи жртви да јој је рачун угрожен.Више о социјалном инжењерингу погледати на линку.

УОБИЧАЈЕНЕ *VISHING* ПРЕВАРЕ

Неколико најчешћих тема *vishing* превара су:

„Компромитовани“ рачун банке или кредитне картице

Било да се ради о особи или о унапред снимљеној поруци, жртва добија информацију да постоји проблем са налогом или уплатом коју је жртва извршила. Од жртве ће се можда захтевати креденцијали за пријављивање да би се решио проблем или ће се затражити нова уплата. Препорука је да уместо давања личних података, жртва спусти слушалицу и назове своју финансијску институцију на њихов јавно доступан број, како би се проверила информација.

Нежељене понуде за кредите или инвестиције

Нападачи позивају са понудама које су превише добре да би биле истините. Један од примера је и позив у којем се корисницима представља понуда да са мало уложеног новца могу зарадити милионе долара, затим да се брзим решењем отплате дуговања или да се у једном маху опросте сви студентски зајмови. Типичан је захтев да се „делује одмах“ и плати мала накнада за то. Дакле, ако је понуда превише добра да би била истинита, то је углавном управо тако како се и чини. Савет је да жртва не предузима радње на овакве врсте понуда. Легитимни зајмодавци и инвеститори неће давати овакве врсте понуда и неће започети контакт изненада.

Пореска превара

Постоји много варијација ове врсте превара, али обично ће жртва добити унапред снимљену поруку, која је обавештава да нешто није у реду са пореском пријавом. Нападачи ово обично упарују са лажним *ID*-јем позиваоца направљеним тако да изгледа као да позив долази из пореске управе. Пре него што жртва настави са комуникацијом, потребно је да се распита и провери следеће информације: на који начин пореска управа може да затражи информације, као и о начину могућег контактирања.

КАКО УОЧИТИ *VISHING* ПРЕВАРУ?

Сигнали помоћу којих је могуће открити превару:

- Позиватељ тврди да представља неку нпр. агенцију, банку, пореску и сл. и тражи личне или финансијске податке. Ако особа није затражила контакт, ниједна од ових институција неће успоставити контакт путем е-поште, текстуалних порука или канала на друштвеним мрежама. Дакле, корисник би требало да буде скептичан према свима који позову са оваквим понудама.
- Постоји осећај изузетне хитности. Нападачи ће покушати да искористе осећај страха код потенцијалне жртве, користећи претње хапшењем и проблеме са налогом жртве. Ако жртва прими један од ових телефонских позива, потребно је да не открива своје податке, спусти слушалицу и обави своју истрагу, којом ће проверити овакве информације и понуде.

- Позиватељ тражи податке од жртве. Од потенцијалне жртве се тражи да потврди своје име, презиме, адресу, датум рођења, ЈМБГ, информације о банковном рачуну и друге податке за идентификацију. Неретко се дешава да нападачи већ поседују неке од личних података потенцијалне жртве, како би жртва поверовала да је особа која је позива заиста она за коју се представља и на тај начин нападачу открију и друге информације. Откривени подаци се могу искористити за друге злонамерне активности или их нападачи могу продати на *dark-web*-у.

КАКО ФУНКЦИОНИШУ *VISHING* ПРЕВАРЕ?

Пример *Vishing* преваре може бити следећи:

- Нападач креира лажни текст е-поште претварајући се да је нпр. добављач и шаље га циљаној компанији наводећи да је потребно поново послати податке о кредитној картици због „проблема“. Ова е-пошта може садржати линк за веб сајт или телефонски број за „ажурирање“ података кредитне картице - и једно и друго ће бити лажно.

- Овакве поруке, систем заштите е-поште организације, може блокирати уколико поруке долазе са познатих злонамерних адреса или уколико их повеже са познатим злонамерним *URL* адресама. Алтернативно, е-адреса је можда у потпуности измишљена и користи се само за континуирану комуникацију изграђујући на тај начин поверење корисника у конкретан позив.

- Након тога, нападач зове организацију и тражи да разговара са жртвама у вези са е-поштом о подацима на картици. Када дођу до одговарајуће мете, даље говоре да постоји проблем са наплатом, а све док се подаци о картици не пошаљу поново поруџбине се обустављају и није могуће извршити додатна плаћања.

- Ако је мета забринута због могућег обустављања даљих поруџбина и није сумњива према захтеву за поновним слањем података, вероватно ће радо предати детаље о својој картици како би решили проблем. Нападач затим проверава да ли су детаљи стварни и потврђује пријем и слање пре него што прекине везу.

Vishing представља врсту фишинг напада која се врши путем телефонских позива са циљем прикупљања финансијских или личних података

Сајбер криминалци сакупљају **личне податке** са профила на друштвеним мрежама са циљем да се жртви представе као поуздани извор.

Након што се **створи страх** да постоји проблем са банковним рачуном или уплатом, од жртве се захтева **хитна реакција**

Тактике манипулације

Позиви са понудама које су **сувише примамљиве да би биле истините.**

Лажни ID као мамац да би позив деловао као да је из поузданог извора

freepik.com

ШТА ЈЕ *SMISHING*?

Smishing је познат и као *SMS* фишинг и представља уобичајену врсту фишинг напада који се преноси путем *SMS* (*Short Message Service*) на мобилним телефонима.

Smishing порука садржи претњу или примамљиву понуду како би жртва кликнула на линк или позвала број и поделила осетљиве информације у одређеном року. Понекад нападачи могу захтевати инсталацију и неког сигурносног софтвера за који се испостави да је злонамеран.

Типична smishing порука може стићи са информацијом да је банковни рачун суспендован и да је за откључавање потребно отворити линк или прилог, након чега се инсталира злонамерни софтвер на систем жртве.

КАКО СЕ ЗАШТИТИТИ ОД *VISHING* И *SMISHING* ПРЕВАРА?

Корисници су све више свесни превара и пријема нежељене е-поште и предузимају све могуће кораке како би их избегли. Међутим, још увек нису свесни позива и *SMS*-ова, јер њих сматрају легитимнијим. Са порастом е-трговине, људи користе своје мобилне телефоне за куповину, банкарство и друге паметне активности, а могућности за нападаче су многобројне.

Најбољи начин за одбрану од *vishing*-а и *smishing*-а је да, пре свега, корисници буду свесни постојања могућности превара на мрежи и путем телефона. Не треба веровати непознатом позиваоцу, или кликтати на линкове које шаље непозната особа. Неопходно је потражити бројеве и адресе е-поште пре него што корисник ступи у контакт. Не треба делити било какве осетљиве информације позиваоцу, као што су подаци о банковном рачуну, детаље о кредитним картицама итд., уместо тога би корисници требало да контактирати своју банку како би били сигурни да је извор легитиман.

Препорука је да се не јављате на непознате бројеве телефона, с обзиром да се идентификације позиваоца лако могу лажирати. Уколико се јавите и посумњате да је то телефонски позив од непровереног позиваоца, прекините позив и блокирајте број.

Уколико добијете аутоматску поруку у којој се тражи да притиснете тастере или одговорите на питања, немојте то чинити. На пример, порука може да каже „Притисните 2 да бисте били уклоњени са наше листе“ или „Реците ''Да'' да бисте разговарали са оператором“. Нападачи се често користе овим триковима да би идентификовали потенцијалне циљеве за више робо-позива. Такође могу да сниме глас одређеног корисника и касније га користе приликом навигације гласовно аутоматизованим телефонским менијима везаним за корисничке налоге.

Препорука је да се претходно потврди идентитет позиваоца. Ако особа наведе број за повратни позив, то је можда део преваре - зато не би требало користити ову опцију. Уместо тога, пожељно је да корисник провери званични јавни телефонски број компаније и позове организацију.

КАКО СЕ ОПОРАВИТИ НАКОН *VISHING* НАПАДА?

Ако сте своје финансијске податке дали некоме за кога се касније испостави да је преварант, контактирајте своју финансијску институцију. Било да се ради о издавачу кредитне картице, банци или другој институцији, назовите и питајте о свим могућностима сторнирања лажних трансакција и блокирању будућих трошкова.

Можда ће бити неопходно да промените и бројеве рачуна како бисте били сигурни да нико не користи ваше постојеће. Замрзавање рачуна платних картица може спречити даљу злоупотребу вашег рачуна.

Иако *vishing* напади имају за циљ превару, ту превару је могуће спречити. Применом наведених препорука можете спречити злонамерне нападаче који покушавају да дођу до ваших личних података путем телефона.

Пример једне *vishing* кампање у Републици Србији можете видети на следећем линку.

Извори:

- Norton: Online scams vishing
- Infoguardsecurity: Smishing and vishing
- Quostar: Whatisvishing
- IBM: The vishing guide
- IT klinika: Vishing kampanja u Srbiji

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

#odbraniseznanjem

СРБ-ЦЕРТ