ZAŠTITITE SVOJU FIRMU I ZAPOSLENE

https://www.pexels.com/photo/blur-cellphone-close-up-device-369376/

# GLASOVNI I SMS FIŠING – *VISHING* I *SMISHING*

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

# *VISHING*, *SMISHING* I KAKO SE ZAŠTITITI

Sa razvojem novih tehnologija, sve je lakše kontaktirati više ljudi. Napadači mogu istovremeno da upućuju stotine poziva koristeći tehnologiju *Voice Over Internet Protocol* (*VoIP*) i lako mogu da podmetnu *ID* pozivaoca da bi poziv izgledao kao da dolazi iz pouzdanog izvora, kao što je banka.

Ovaj tip napada ima veći procenat uspešnosti za napadača nego *fišing* poruke, zbog:

- Većeg broja ljudi do kojih se može doći, nego putem e-poruka,
- Veći stepen poverenja ljudi ka pozivima nego e-porukama,
- Automatske validacije sistema,
- Telefonskim pozivima je moguće lakše doći do određenih ciljnih grupa, kao što su pripadnici starije populacije,
- Otvaranje sve većeg broja pozivnih centara je doprineo povećanju poverenja i prihvatanja poziva od osoba koje ne poznajemo, a pitaju za poverljive informacije.

*Vishing* i *smishing* predstavljaju uobičajene vrste *fišing* napada, koji napadaju žrtvu putem glasovnih poziva i slanjem poruka. Obe vrste koriste tradicionalnu metodu *fišing* prevara koja od žrtve zahteva hitnu reakciju. Cilj je sličan, dok su načini isporuke različiti.

## ŠTA JE *VISHING*?

Vishing je glasovni fišing i predstavlja vrstu fišing napada koja se prenosi putem telefonskih poziva i *Skype*-a, a kao ciljnu grupu ima korisnike *Voice Over Internet Protocol- VoIP* usluge.

Napadači koriste različite *ID*-jeve koji odaju utisak da su od pouzdane osobe. Čini se da je poziv upućen iz lokalnog područja ili organizacije koju poznajete. Kada se poziv propusti, napadači obično ostave poruku u kojoj traže da ih pozovete.

Napadači imaju za cilj prikupljanje podataka o kreditnim karticama, datumima rođenja, kredencijalima za različite naloge ili brojeva telefona kontakata žrtve kako bi saznali njene lične podatke.

Za vreme telefonskog poziva, napadač koristi socijalni inženjering da bi žrtvu naterao da deli lične i finansijske podatke, kao što su brojevi računa i lozinke. Napadač se obično predstavlja kao predstavnik policije, osoba koja nudi pomoć u instaliranju softvera (upozorenje: To je verovatno zlonamerni softver), ili najčešće kao predstavnik banke govoreći žrtvi da joj je račun ugrožen. Više o socijalnom inženjeringu pogledati na linku.

# UOBIČAJENE *VISHING* PREVARE

Nekoliko najčešćih tema *vishing* prevara su:

**„Kompromitovani“ račun banke ili kreditne kartice**

Bilo da se radi o osobi ili o unapred snimljenoj poruci, žrtva dobija informaciju da postoji problem sa nalogom ili uplatom koju je žrtva izvršila. Od žrtve će se možda zahtevati kredencijali za prijavljivanje da bi se rešio problem ili će se zatražiti nova uplata. Preporuka je da umesto davanja ličnih podatka, žrtva spusti slušalicu i nazove svoju finansijsku instituciju na njihov javno dostupan broj, kako bi se proverila informacija.

**Neželjene ponude za kredite ili investicije**

Napadači pozivaju sa ponudama kojesu previše dobre da bi bile istinite. Jedan od primera je i poziv u kojem se korisnicima predstavlja ponuda da sa malo uloženog novca mogu zaraditi milione dolara, zatim da se brzim rešenjem otplate dugovanja ili da se u jednom mahu oproste svi studentski zajmovi. Tipičan je zahtev da se „deluje odmah“ i plati mala naknada za to. Dakle, ako je ponuda previše dobra da bi bila istinita, to je uglavnom upravo tako kako se i čini. Savet je da žrtva ne preduzima radnje na ovakve vrste ponuda. Legitimni zajmodavci i investitori neće davati ovakve vrste ponuda i neće započeti kontakt iznenada.

**Poreska prevara**

Postoji mnogo varijacija ove vrste prevara, ali obično će žrtva dobiti unapred snimljenu poruku, koja je obaveštava da nešto nije u redu sa poreskom prijavom. Napadači ovo obično uparuju sa lažnim *ID*-jem pozivaoca napravljenim tako da izgleda kao da poziv dolazi iz poreske uprave. Pre nego što žrtva nastavi sa komunikacijom, potrebno je da se raspita i proveri sledeće informacije: na koji način poreska uprava može da zatraži informacije, kao i o načinu mogućeg kontaktiranja.

# KAKO UOČITI *VISHING* PREVARU?

Signali pomoću kojih je moguće otkriti prevaru:

- Pozivatelj tvrdi da predstavlja neku npr. agenciju, banku, poresku i sl. i traži lične ili finansijske podatke. Ako osoba nije zatražila kontakt, nijedna od ovih institucija neće uspostaviti kontakt putem e-pošte, tekstualnih poruka ili kanala na društvenim mrežama. Dakle, korisnik bi trebalo da bude skeptičan prema svima koji pozovu sa ovakvim ponudama.

- Postoji osećaj izuzetne hitnosti. Napadači će pokušati da iskoriste osećaj straha kod potencijalne žrtve, koristeći pretnje hapšenjem i probleme sa nalogom žrtve. Ako žrtva primi jedan od ovih telefonskih poziva, potrebno je da ne otkriva svoje podatke, spusti slušalicu i obavi svoju istragu, kojom će proveriti ovakve informacije i ponude.

- Pozivatelj traži podatke od žrtve. Od potencijalne žrtve se traži da potvrdi svoje ime, prezime, adresu, datum rođenja, JMBG, informacije o bankovnom računu i druge podatke za identifikaciju. Neretko se dešava da napadači već poseduju neke od ličnih podataka potencijalne žrtve, kako bi žrtva poverovala da je osoba koja je poziva zaista ona za koju se predstavlja i na taj način napadaču otkriju i druge informacije. Otkriveni podaci se mogu iskoristiti za druge zlonamerne aktivnosti ili ih napadači mogu prodati na *dark-web*-u.

# KAKO FUNKCIONIŠU *VISHING* PREVARE?

Primer *Vishing* prevare može biti sledeći:

- Napadač kreira lažni tekst e-pošte pretvarajući se da je npr. dobavljač i šalje ga ciljanoj kompaniji navodeći da je potrebno ponovo poslati podatke o kreditnoj kartici zbog „problema“. Ova e-pošta može sadržati link za veb sajt ili telefonski broj za „ažuriranje“ podataka kreditne kartice - i jedno i drugo će biti lažno.

- Ovakve poruke, sistem zaštite e-pošte organizacije,može blokirati ukoliko poruke dolaze sa poznatih zlonamernih adresa ili ukoliko ih poveže sa poznatim zlonamernim URL adresama. Alternativno, e-adresa je možda u potpunosti izmišljena i koristi se samo za kontinuiranu komunikaciju izgrađujući na taj način poverenje korisnika u konkretan poziv.

- Nakon toga, napadač zove organizaciju i traži da razgovara sa žrtvama u vezi sa e-poštom o podacima na kartici. Kada dođu do odgovarajuće mete, dalje govore da postoji problem sa naplatom, a sve dok se podaci o kartici ne pošalju ponovo porudžbine se obustavljaju i nije moguće izvršiti dodatna plaćanja.

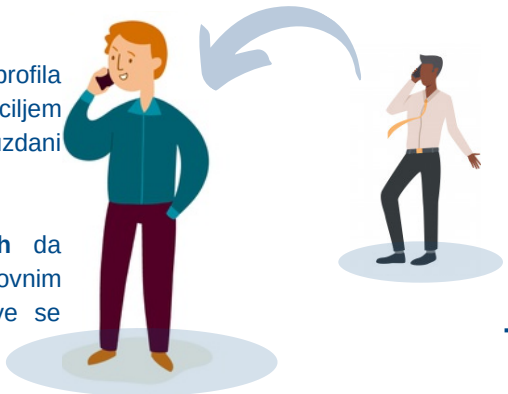
- Ako je meta zabrinuta zbog mogućeg obustavljanja daljih porudžbina i nije sumnjiva prema zahtevu za ponovnim slanjem podataka, verovatno će rado predati detalje o svojoj kartici kako bi rešili problem. Napadač zatim proverava da li su detalji stvarni i potvrđuje prijem i slanje pre nego što prekine vezu.

***Vishing*** predstavlja vrstu fišing napada koja se vrši putem telefonskih poziva, a sa ciljem prikupljanja finansijskih ili ličnih podataka

**Sajber kriminalci**

sakupljaju **lične podatke** sa profila na društvenim mrežama, sa ciljem da se žrtvi predstave kao pouzdani izvor.

Nakon što se **stvori strah** da postoji problem sa bankovnim računom ili uplatom, od žrtve se zahteva **hitna reakcija**



**Taktike manipulacije**

Pozivi sa ponudama koje su **suviše primamljive da bi bile istinite.**

**Lažni ID** kao mamac da bi poziv delovao kao da je iz pouzdanog izvora

freepik.com

# ŠTA JE *SMISHING*?

*Smishing* je poznat i kao *SMS fišing* i predstavlja uobičajenu vrstu *fišing* napada koji se prenosi putem *SMS* (*Short Message Service*) na mobilnim telefonima.

*Smishing* poruka sadrži pretnju ili primamljivu ponudu kako bi žrtva kliknula na link ili pozvala broj i podelila osetljive informacije u određenom roku. Ponekad napadači mogu zahtevati instalaciju i nekog sigurnosnog softvera za koji se ispostavi da je zlonameran.

Tipična *smishing* poruka može stići sa informacijom da je bankovni račun suspendovan i da je za otključavanje potrebno otvoriti link ili prilog, nakon čega se instalira zlonamerni softver na sistem žrtve.

# KAKO SE ZAŠTITITI OD *VISHING* I *SMISHING* PREVARA?

Korisnici su sve više svesni prevara i prijema neželjene e-pošte i preduzimaju sve moguće korake kako bi ih izbegli. Međutim, još uvek nisu svesni poziva i *SMS*-ova, jer njih smatraju legitimnijim. Sa porastom e-trgovine, ljudi koriste svoje mobilne telefone za kupovinu, bankarstvo i druge pametne aktivnosti, a mogućnosti za napadače su mnogobrojne.

Najbolji način za odbranu od *vishing*-a i *smishing*-a je da, pre svega, korisnici budu svesni postojanja mogućnosti prevara na mreži i putem telefona. Ne treba verovati nepoznatom pozivaocu, ili kliktati na linkove koje šalje nepoznata osoba. Neophodno je potražiti brojeve i adrese e-pošte pre nego što korisnik stupi u kontakt. Ne treba deliti bilo kakve osetljive informacije pozivaocu, kao što su podaci o bankovnom računu, detalje o kreditnim karticama itd., umesto toga bi korisnici trebalo da kontaktirati svoju banku kako bi bili sigurni da je izvor legitiman.

Preporuka je da se ne javljate na nepoznate brojeve telefona, s obzirom da se identifikacije pozivaoca lako mogu lažirati. Ukoliko se javite i posumnjate da je to telefonski poziv od neproverenog pozivaoca, prekinite poziv i blokirajte broj.

Ukoliko dobijete automatsku poruku u kojoj se traži da pritisnete tastere ili odgovorite na pitanja, nemojte to činiti. Na primer, poruka može da kaže „Pritisnite 2 da biste bili uklonjeni sa naše liste“ ili „Recite ''Da'' da biste razgovarali sa operatorom“. Napadači se često koriste ovim trikovima da bi identifikovali potencijalne ciljeve za više robo-poziva. Takođe mogu da snime glas određenog korisnika i kasnije ga koriste prilikom navigacije glasovno automatizovanim telefonskim menijima vezanim za korisničke naloge.

Preporuka je da se prethodno potvrdi identitet pozivaoca. Ako osoba navede broj za povratni poziv, to je možda deo prevare - zato ne bi trebalo koristiti ovu opciju. Umesto toga, poželjno je da korisnik proveri zvanični javni telefonski broj kompanije i pozove organizaciju.

# KAKO SE OPORAVITI NAKON *VISHING* NAPADA?

Ako ste svoje finansijske podatke dali nekome za koga se kasnije ispostavi da je prevarant, kontaktirajte svoju finansijsku instituciju. Bilo da se radi o izdavaču kreditne kartice, banci ili drugoj instituciji, nazovite i pitajte o svim mogućnostima storniranja lažnih transakcija i blokiranju budućih troškova.

Možda će biti neophodno da promenite i brojeve računa kako biste bili sigurni da niko ne koristi vaše postojeće. Zamrzavanje računa platnih kartica može sprečiti dalju zloupotrebu vašeg računa.

Iako *vishing* napadi imaju za cilj prevaru, tu prevaru je moguće sprečiti. Primenom navedenih preporuka možete sprečiti zlonamerne napadače koji pokušavaju da dođu do vaših ličnih podatka putem telefona.

Primer jedne *vishing* kampanje u Republici Srbiji možete videti na sledećem linku.

*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:


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