SPOOFING

Dit artikel is bedoeld om u scherper maken zodat u geen slachtoffer wordt van oplichters. Dat u met plezier internet, sociale media, e-mail en whatsapp blijft gebruiken, maar wel bewust bent van de gevaren. Als u de gevaren kent wordt het juist veiliger.

Spoofing: dat is als een oplichter tijdelijk een valse identiteit aanneemt, dat kan zowel als persoon of als bedrijf zijn. Dit kan bijvoorbeeld per e-mail, een website, een telefoonnummer, sociale media of zelfs aan uw voordeur.

Hoe voorkomt u om slachtoffer te worden van oplichting? Wat algemene adviezen:

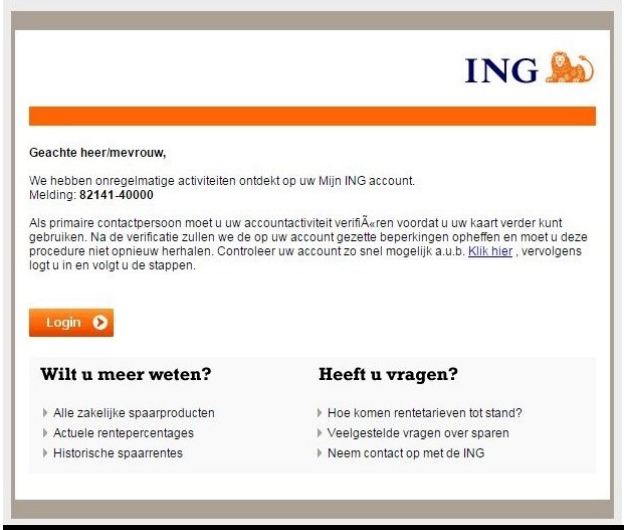
- Wees altijd wantrouwig als u onverwacht wordt benaderd per e-mail, een website, telefoon (whatsapp of sms) of sociale media (Facebook). Ook al doet men zich voor als een bekende van u of iemand van een bekend bedrijf (vaak bank).
- Een bank zal u nooit om uw gegevens vragen. Zal nooit vragen uw betaalpas in te leveren of vragen om uw geld naar een veilige rekening over te maken omdat er een veiligheidsprobleem is.
- Een helpdesk (vaak Microsoft) zal u nooit bellen omdat zij een probleem met uw computer hebben opgemerkt. Die service bestaat niet. Laat u nooit verleiden om achter uw computer plaats te nemen en te doen wat zij van u vragen.
- Als u via een link naar een website gaat, controleer dan altijd eerst of het een betrouwbare website is voordat u ook maar ergens in die website op klikt of een transactie aangaat.
- Als een bekende u om geld vraagt zal deze altijd begrijpen als u wantrouwig bent en dat u zelf wilt terugbellen om dan pas zijn/haar verzoek te bespreken. Laat u nooit onder druk zetten. Een bekende kan beter teleurgesteld zijn dat u niet direct helpt dan dat u al uw spaargeld kwijtraakt.
- Overleg met iemand die u vertrouwt, of met het bedrijf voordat u ook maar ergens op ingaat. Gebruik altijd de bij u bekende telefoonnummers. Laat u informeren of het verzoek of aanbod dat u krijgt wel klopt.

De meerdere soorten spoofing zijn in vijf groepen ingedeeld en per groep zijn de handelingen beschreven die u kunt doen om te voorkomen dat u slachtoffer wordt.

Spoofing per e-mail en website

In een e-mail wordt u gevraagd om ergens op te klikken. Doe dit nooit direct. Doe eerst één of meerdere van de volgende checks.

- Controleer of het afzenderadres van de e-mail correct is. Let op, soms wijkt het adres slechts een enkele letter af. Weet u niet wat wel het juiste e-mailadres moet zijn? Doe de volgende stap.
- Zet de cursor op de link (NIET KLIKKEN!), het websiteadres waar de link u naartoe wilt sturen wordt zichtbaar, dat kan een pop-up zijn of een regel helemaal aan de onderzijde van uw scherm. Klik er niet op! Kijk of het websiteadres (URL) de echte website is. Let op: een vals adres kan soms slechts een enkele letter verschillen van het echte. Weet u niet hoe het websiteadres precies moet zijn? Ga dan naar Google en zoek op de bedrijfsnaam waar de link in de e-mail naar verwijst. In de zoekresultaten



Men doet zich voor als uw bank. Geloof het niet!

vindt u de officiële website, klik daarop. In de adresregel van deze website leest u de correcte schrijfwijze van het websiteadres. Bent u nog niet overtuigd? Doe dan de volgende stap.

- Schrijf het websiteadres van de link op. Schrijf niet de hele regel op. Ga tot de eerste slash ("/") die staat na ".nl", ".com", ".org" o.i.d. Typ in de zoekregel van Google de bedrijfsnaam in van het bedrijf waar de mail u naar verwijst en typ daarbij waar de e-mail over gaat. Typ eventueel "oplichting" of "hoax" bij de zoekopdracht. Stel dat de e-mail u wilt sturen naar de website www.museum.nl en dat de boodschap is dat uw museumjaarkaart is gehackt en u een nieuw moet aanvragen. Dan zou de zoekopdracht er als volgt kunnen uitzien: "www.museumkaart.nl museumpas gehackt oplichting". Als het inderdaad oplichting is dan leest u dat ongetwijfeld bij één van de zoekresultaten.
- Een extra check is mogelijk. Ga naar www.vraaghetdepolitie.nl en typ daar het websiteadres in waarover u twijfelt. U ziet dan of er negatieve meldingen over die website zijn.
- Nog steeds twijfels? Bel, e-mail of chat met het bedrijf dat u via deze e-mail lijkt te benaderen en vraag of het klopt dat je museumjaarkaart is gehackt.
- Is de e-mail onbetrouwbaar? Verwijder hem naar de prullenbak en maak dan ook de prullenbak leeg. Die e-mail kunt u maar beter kwijt zijn.

In deze video ziet u hoe u e-mails kunt controleren of het spam is.

Klik hier om te zien welke valse e-mails er zijn en hoe u ze herkent.

Spoofing per telefoon

U wordt gebeld met het verzoek om een probleem op te lossen dat bij u is geconstateerd (bijv. op uw computer of bank). Geloof dit nooit.

- Zeg altijd dat het gesprek u nu niet uitkomt en dat u terugbelt.
- Beantwoord geen enkele vraag, maar houdt vast dat u terugbelt.
- Vraag naar het telefoonnummer, firmanaam en de naam van de bellende persoon. Nu krijgt u allerlei redenen te horen dat u niet kunt bellen en dat zij u zullen bellen. Zeer waarschijnlijk krijgt u geen naam of nummer.
- Niet accepteren! U belt terug! Sta erop! Ga niet in discussie! Een betrouwbaar persoon/bedrijf doet daar niet moeilijk over. Krijgt u geen medewerking, leg dan neer!
- Stel, u krijgt toch een telefoonnummer, ga dan eerst checken of dit nummer als gevaarlijk bekend staat. Google dit telefoonnummer, staat het als onbetrouwbaar bekend, dan kunt u blij zijn dat u correct hebt gehandeld. Gebruik in ieder geval het gekregen nummer nooit om terug te bellen.
- Zoek altijd zelf het telefoonnummer van dat bedrijf op en bel daarmee terug. Vraag dan of het klopt dat u gebeld bent omdat er een probleem bij u is geconstateerd.

Spoofing met whatsapp en sms

Een "bekende" stuurt u een bericht met een onbekend telefoonnummer. Diegene heeft een mooi verhaal klaar om geld te vragen, dat er haast bij is en dat die persoon nu niet gebeld kan worden. Er wordt op uw gevoel gespeeld. Help me, ik zit in nood. Geloof dit nooit! Hoe aannemelijk het ook klinkt.

- App of sms dat u zult terugbellen, dat u niet zomaar geld leent. Dat u tijd nodig heeft om erover na te denken. Dat u alleen helpt als u diegene kan spreken (dan herkent u de stem wel).
- Is het een oplichter dan krijgt u allerlei aannemelijke redenen te horen waarom u niet kunt terugbellen. Laat u niet verleiden, niet onder druk zetten en schakel uw gevoel en uw behulpzaamheid even uit! Hoe zielig men ook doet, ga er niet in mee. Ga niet in discussie.
- Als een bekende echt in nood zit, zal die heus wel begrijpen dat u zekerheid wil.

Spoofing via Whatsapp.
Iemand doet zich voor als jouw kind. Ga er niet op in en blokkeer direct de afzender.

Spoofing met sociale media
Op sociale media zoals Facebook kan men een neppagina aanmaken. Met een valse identiteit. Er worden foto's en gegevens van de originele pagina afgehaald en op de neppagina geplaatst. Dit ziet er heel echt uit. Men neemt dan met messenger (privéchat van Facebook) contact met u op omdat u bevriend bent met die bekende persoon. Men vraagt meestal om financiële hulp.

- Zodra men om geld of iets dergelijks vraagt moeten alle alarmbellen gaan rinkelen. Hoe goed u diegene ook kent. Zelfs als u weet dat het niet vreemd klinkt als diegene geld zou kunnen nodig hebben.
- Vraag altijd waarom die persoon een nieuwe pagina heeft. U hoort dan een reden (smoes) die aannemelijk lijkt. En een uitleg waarom je de originele pagina van die bekende juist niet moet gebruiken. Klinkt allemaal logisch.
- Zeg dat u een controlevraag stelt om de identiteit vast te stellen.
- Bedenk een vraag die deze persoon kan weten, maar niet algemeen bekend is.
- De vraag wordt meestal ontweken en men speelt in op uw sociale gevoel. Je vertrouwt me toch wel?
- Zeg dat u terugbelt. U hoort dan meestal een 'verzonnen' reden waarom bellen niet kan. Die klinkt vaak aannemelijk.
- Ga er niet in mee, blijf erbij dat u zal bellen. Dat u alleen geldzaken doet als uzelf kunt bellen.
- Wordt u onder tijdsdruk gezet, ga er niet in mee. Dan had die ander er maar eerder aan moeten denken als ze geld nodig hebben. Geloof alle zielige verhalen nooit.
- Ga naar de officiële pagina van die bekende en stel daar de vraag met een privébericht of die persoon een nieuwe pagina heeft aangemaakt en om hulp vraagt. Het is nog beter als u die persoon even belt. Dan pas weet je of al het voorgaande echt is of ordinaire oplichting.

Klik hier hoe je een nepaccount op Facebook kunt herkennen.

Spoofing aan de deur
Ook mensen aan de deur kunnen oplichters zijn. Zij nemen een valse identiteit aan. Zij zeggen dat ze bijvoorbeeld van de energieleverancier zijn, de meteropnemer of thuiszorg. Men probeert met een smoes bij u binnen te komen en vaak komt men met twee personen. De een leidt af en de ander doorzoekt uw huis. Wat kunt u doen?

- Beveilig uw voordeur met een ketting of kierstandhouder.
- Bent u alleen thuis? Zorg dat uw achterdeur altijd op slot is.
- Overtuig u wie voor de deur staat voordat u opendoet.
- Meldt een bedrijf of organisatie zich zonder vooraankondiging, doe niet open en laat niemand binnen.
- Bel dat bedrijf of organisatie of het klopt dat er iemand voor de deur staat. Gebruik niet het telefoonnummer dat u van de aanbeller krijgt.

Op de website van ANBO staat een overzicht hoe u voorkomt om slachtoffer te worden. Klik hier.

De website van Zuster Jansen (thuiszorgorganisatie in Amsterdam) heeft een overzicht van de meest voorkomende babbeltrucs. Klik hier.

Wij hopen dat u nu beter bewapend bent tegen oplichting met spoofing en dat u kunt voorkomen om slachtoffer te worden. Geld kwijtraken is al een ramp, maar ook uw vertrouwen in de medemens krijgt een enorme knauw.