Nepberichten en oplichterij via de telefoon

Phishing is nog altijd populair onder criminelen. Via valse berichten hengelen ze naar geld of persoonlijke gegevens. We bespreken de varianten. En we laten zien hoe je oplichterij via de telefoon herkent.

Bij online oplichterij spelen nepberichten een belangrijke rol. Criminelen sturen ze om privégegevens te achterhalen of je met malware op te zadelen. Tot voor enkele jaren gebeurde dit vooral per e-mail. Tegenwoordig versturen criminelen fraudeleuze berichten ook per sms, WhatsApp, Facebook Messenger en andere online platforms. Nieuw zijn nepberichten niet. Het gebeurde vroeger al per brief en fax. De fax is zo'n beetje uitgestorven, maar per brief komt oplichterij ook nu nog voor.

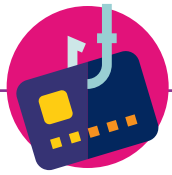
Hier bespreken we hoe je nepberichten en oplichterij via telefoon herkent. In de volgende hoofdstukken laten we zien hoe andere vormen van online fraude werken. Goed om te weten: cybercriminelen combineren vaak diverse vormen. Het begint bijvoorbeeld met phishing, waarna een malafide cryptotransactie volgt.

Phishing

Criminelen versturen dagelijks onvoorstelbare aantallen phishingberichten. Om een indicatie te geven: alleen Google verwijdert er dagelijks al 100 miljoen. Spamfilters houden veel phishingberichten tegen, maar soms glipt er een doorheen.

Phishing komt voor via alle online communicatiekanalen. Niet alleen per e-mail dus, maar ook via WhatsApp, Facebook Messenger, Instagram, enzovoort. Phishingberichten komen ook per sms binnen. Hiervoor is de term smishing bedacht (een samentrekking van sms en phishing).

In phishingberichten hengelen criminelen naar geld of gegevens. Vaak is het een dringend bericht met het verzoek in te loggen op een website, bijvoorbeeld van een bank, webshop of overheidsinstantie. Die website ziet er meestal bedrieglijk echt uit. Als je inlogt op zo'n site overhandig je je inloggegevens aan criminelen.
Via nepberichten verspreiden criminelen ook virussen. Ze vragen je bijvoorbeeld



Kijk uit voor bankkaart-phishing

Al gehoord van bankkaart-phishing? Fraudeurs sturen uit naam van de bank per e-mail of sms een verzoek om je bankkaart op te sturen. De kaart zou om uiteenlopende redenen binnenkort niet meer geldig zijn. Om aan je pincode te komen, sturen ze je een link toe. Die leidt naar een nagebouwde website van de bank met een formulier. Daar kun je je bankgegevens (persoonlijke gegevens, kaartnummer, pincode) invullen. Om geloofwaardig over te komen, vraagt de fraudeur soms de bankkaart verticaal doormidden te knippen. Helaas maakt dat de kaart niet ongeldig. Daarvoor moet je ook de koperkleurige betaalchip doorknippen. Overigens vragen banken nooit om je bankkaart terug te sturen. Ga hier dus nooit op in.

software te installeren om een postpakketje te volgen. Vaak betreft het hier ransomware. Deze software versleutelt bestanden op de computer. Pas na betaling geven de criminelen de bestanden weer vrij.

Let vooral op met berichten uit naam van banken, pakjesdiensten, incassobureaus, overheidsinstellingen, energiebedrijven en internetproviders. De berichten gaan vaak over incasso's, vorderingen, bankkaarten, beveiligingsproblemen, boetes, facturen, verlopen accounts, mislukte betalingen, gemiste pakketleveringen en autoschademeldingen. Ook winacties zijn vaak nep, bijvoorbeeld uit naam van grote supermarktketens of webshops.

Om problemen te voorkomen is het belangrijk niet te klikken op links in phishingberichten. In de volgende paragrafen enkele aanwijzingen waarmee je phishingberichten kunt herkennen.

Link klopt niet

In veel phishingberichten staat een link. Vaak leidt zo'n link naar een website waar je gegevens in kunt vullen, bijvoorbeeld de inloggegevens van je bank. De link kan ook leiden naar een website met malware.

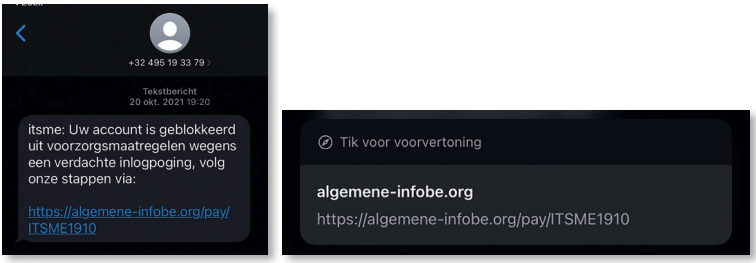
Hoe weet je of je een link kunt vertrouwen? Het webadres waar de link naar leidt moet logisch zijn. We nemen een phishingbericht uit naam van Fluvius als voorbeeld. De link in het bericht leidt naar een vreemd webadres. Dat is een duidelijke aanwijzing dat we hier met een nepbericht te maken hebben: het internetadres van Fluvius is fluvius.be.

De link in de mail leidt duidelijk niet naar de officiële website van Fluvius.

Check de link

Bedenk dat het getoonde webadres niet altijd overeenkomt met het webadres waar de link naartoe leidt. Hoe controleer je een link in een mail? Dit hangt af van het apparaat waarmee je het bericht ontvangt.

- **Link checken op de computer:** beweeg de cursor over de link. Onderin het venster staat het webadres. Soms verschijnt het echte webadres in een venstertje rechtsboven de cursor, zoals bij het voorbeeld van Fluvius op de vorige bladzijde.
- **Link checken op smartphone of tablet:** raak de link lang aan. Er verschijnt een soort pop-up met het volledige webadres, zie de afbeelding.



De link in een sms die beweert van itsme te komen, gaat allesbehalve naar de officiële website van itsme (https://www.itsme-id.com).

In hoofdstuk 3 leggen we uitgebreid uit hoe je neplinks herkent.

Onjuiste afzender

Een phishingmail is vaak te herkennen aan een onjuiste afzender. In het voorbeeld (zie afbeelding) heeft het e-mailadres helemaal niets te maken met itsme. Helaas maken criminelen het jou niet altijd makkelijk. Er zijn namelijk spammers die erin slagen om een verzendadres te vervalsen. Ze gebruiken een techniek (spoofing) om het afzendadres te wijzigen in een geloofwaardig alternatief.

Een mail van itsme? Het adres @japanartist.com doet anders vermoeden!

Valse QR-code

Relatief nieuw is phishing met QR-codes. Door zo'n code te scannen kun je snel naar een website gaan. Criminelen gebruiken ze om je naar nepsites te leiden, bijvoorbeeld de nagemaakte site van een bank of energieleverancier. Je kunt valse QR-codes tegenkomen in online berichten, bijvoorbeeld per e-mail of WhatsApp.

Bij het scannen van een QR-code met de camera-app van je telefoon (of met een speciale app om QR-codes te scannen) verschijnt het webadres in beeld. Controleer eerst of dit webadres klopt (zie hoofdstuk 3 "Neplinks herkennen"). Ga daarna pas naar de betreffende website.

Onpersoonlijke aanhef

Spammers beschikken vaak alleen over je e-mailadres. Daardoor kunnen ze je niet persoonlijk aanspreken met voor- en achternaam. Veel phishingmails zijn te herkennen aan een onpersoonlijke aanhef zoals "Beste klant" of "Geachte relatie".


Er staat een document voor u klaar

Geachte heer/mevrouw ,

Er staat een document in uw My eBox van Federale overheidsdienst financiën. Ga naar My eBox om het bericht te bekijken. Mogelijk moet u naar aanleiding van dit bericht actie ondernemen. Lees het daarom op tijd.

Met vriendelijke groet,

FOD Financiën

my e-box

Via datalekken komen cybercriminelen aan lijsten met e-mailadressen, voor- en achternamen en andere persoonlijke gegevens. Daardoor zien we steeds vaker nepberichten met een persoonlijke aanhef.

Urgentie en dreiging

Urgentie uitstralen is een bekend drukmiddel om slachtoffers te laten reageren. Zo dreigen nepmails uit naam van banken vaak met het blokkeren van een rekening. Phishingmails van incassobureaus waarschuwen voor hoge kosten als betaling uitblijft. Ook zijn er veel nepmails die dreigen met sluiting van een account "uit veiligheidsoverwegingen".

Van: F.O.D. Financiën Brussel <fodfinancien@mail.be>
Verzonden: zaterdag 16 juli 2022 4:30
Onderwerp: Dit is een automatisch gegenereerd bericht.

Beste Relatie,

U heeft een openstaand bericht ontvangen van onze servicedesk waarop u dient te reageren voor 18 juli 2022. Druk op de onder weergeven extensie om de online versie van uw bericht te bekijken.
> Bericht weergeven
Waarom krijg je deze e-mail?
Bij berichten die belangrijk voor je kunnen zijn, krijg je een seintje van ons.

Met vriendelijke groet,
FOD Financien Brussel

Deze phishingmail wil je doen klikken door tijdsdruk op te leggen.

Onrealistische belofte

Veel spamberichten beloven mooie prijzen of een waardebon. Na het klikken op de link vragen de spammers om privégegevens. Het komt ook voor dat ze je een duur betaalnummer laten bellen of je opzadelen met een duur sms-abonnement. De beloofde waardebon is een lokmiddel, die zul je nooit ontvangen.

Ga niet in op winacties, tenzij ze op de officiële website of sociale media van de verkoper staan. Afmelden van nepmails over winacties kan averechts werken. Als je op de afmeldlink klikt, weten de spammers dat de e-mail gelezen wordt.

Een phishingmail uit naam van Hema die je een waardebon van € 500 belooft.

Taalfouten

Het taalgebruik van spammers is er op vooruitgegaan. Een bericht geschreven in foutloos Nederlands kan best phishing zijn. Toch zijn er nog altijd volop spamberichten geschreven in tenenkrommend Nederlands, getuige de volgende e-mail.

Van: Azim Premji <hajaraibrahim6452@gmail.com>
Verzonden: vrijdag 7 oktober 2022 15:33
Onderwerp:

--
We zijn trots om aan te kondigen dat de Azim Premjl Philanthropies Foundation, u $ 500.000,00 heeft ontvangen van de Azim Premjl Philanthropies Foundation, uw e-mailadres is willekeurig online geselecteerd tijdens uw zoekopdracht. Neem dan zo snel mogelijk contact met ons op, zodat ik weet dat uw e-mailadres correct is. Neem contact met ons op voor meer informatie!

E-mail: azimprmj@gmail.com

HCL Corporation en de Azim Premjl Foundation
Bedrijfscommunicatiemanager
Met vriendelijke groeten,
Azim Premji.

Goed geschreven kun je deze phishingmail niet noemen.

E-mail met bijlage

Sommige spammails bevatten een bestand als bijlage die kwaadaardige software kan bevatten. Wanneer je die opent, wordt er malware op je toestel geïnstalleerd. Open dus nooit een bijlage van een afzender die je niet vertrouwt. Kijk zeker naar het bestandsformaat. Onder meer zip-, exe- en javascript (js)-bestanden zijn verdacht.

Scan deze QR-code voor meer tips om phishingberichten te ontmaskeren
www.testaankoop.be/phishing

Spear phishing

Over het algemeen richten fraudeurs zich bij phishing op grote groepen mensen. Ze versturen duizenden mails. De meeste ontvangers zullen niet ingaan op de poging tot oplichterij, maar een enkeling trapt erin.

Effectiever is gerichte phishing of spear phishing. Deze methode is in opkomst. Bij spear phishing doet de crimineel eerst onderzoek. Hij bekijkt bijvoorbeeld je socialemedia-accounts. Kennis die hij zo opdoet, gebruikt hij om je vertrouwen te winnen als hij je contacteert. Er zijn vele varianten. Een bekend voorbeeld is iemand die belt uit naam van de bank en zegt dat er iets mis is met je bankrekening. Spear phishing kwam aanvankelijk vooral voor bij bedrijven en instellingen. Crimi-

nelen stuurden berichten naar een directeur of iemand op de financiële afdeling. In de bijlage stopten ze bijvoorbeeld een kwaadaardig programma of geloofwaardig uitziende factuur. Tegenwoordig krijgen consumenten ook te maken met spear phishing. Iemand doet zich voor als goede vriend of bankmedewerker en vraagt met een smoes om geld of inloggegevens. Voorbeelden zijn hulpvraagfraude en telefoontjes uit naam van de bank.

Phishing via een foto

Hoera, je hebt je rijbewijs gehaald! Veel mensen willen het goede nieuws graag delen via Facebook, Twitter of Instagram. Vaak met een foto van het begeerde document erbij. Pas daarmee op. Je maakt het criminelen zo heel makkelijk om persoonsgegevens te stelen. Wil je met je rijbewijs of paspoort op de foto, dek dan op zijn minst de persoonlijke gegevens af.

Hulpvraagfraude

Bij hulpvraagfraude doen criminelen zich voor als iemand die je kent. Met een smoes vragen ze om geld. Dat gaat zeer geraffineerd. In veel gevallen doen ze zich voor als zoon of dochter. In die rol laten ze weten een “nieuw nummer” te hebben, bijvoorbeeld omdat hun oude telefoon kapot is. Niet veel later vertellen ze een dringende rekening niet te kunnen betalen. Of papa/mama even wil voorschieten?

Soms is het technologisch ook erg geavanceerd. Zo nemen ze het stemgeluid op van personen voor wie ze zich willen uitgeven. Later gebruiken ze die opnamen om slachtoffers te overtuigen. De fraude komt vooral voor via WhatsApp, maar ook andere communicatiemiddelen (zoals Facebook Messenger) zijn kwetsbaar.

Zo kun je hulpvraagfraude voorkomen:

- **Wantrouw een nieuw nummer:** wees achterdochtig als iemand zich voordoet als een “bekende” met een nieuw nummer. Het kan gaan om fraude. Dat de foto van de persoon klopt is geen bewijs. Die kan van sociale media zijn geplukt. Ook een spraakbericht van de bekende is geen bewijs. Dit kan een buitgemaakte opname zijn.
- **Schiet geen geld voor:** als het nieuwe contact vraagt geld voor te schieten, klopt er iets niet. Aangezien deze manier van oplichten alom bekend is, wachten criminelen soms een paar dagen voordat ze vragen om geld. De eerste dagen is er sprake van normaal contact over koetjes en kalfjes.
- **Bel bij twijfel:** twijfel je of je te maken hebt met een fraudeur? Bel de persoon dan op. Gebruik hiervoor het oude nummer. Als de bekende op dat nummer opneemt,

is meteen duidelijk dat het nieuwe nummer van een fraudeur is. Doe aangifte van fraude. Als je het nieuwe nummer belt, bestaat de kans dat je een buitgemaakte stemopname krijgt te horen van de bekende. Dit is dus geen bewijs dat de bekende daadwerkelijk een nieuw nummer heeft. Voer een daadwerkelijk gesprek en ga niet akkoord alleen omdat je het stemgeluid hebt herkend en de “bekende” aangeeft dat de verbinding slecht is.

- **Controleer het nummer:** kun je de bekende niet bereiken? Controleer het nieuwe nummer door het in te typen in een zoekmachine. Als iemand eerder fraude heeft gepleegd met dit nummer bestaat de kans dat je een melding vindt.
- **Geef geen verificatiecode door:** vraagt iemand om een zogenaamd per ongeluk gestuurde WhatsApp-verificatiecode door te sturen? Ga hier niet op in. De persoon probeert je account over te nemen. De code is bedoeld om een nieuwe telefoon te koppelen aan je WhatsApp-account.

Frauduleuze telefoontjes

Phishing komt ook voor per telefoon. Criminelen bellen je brutaalweg op. Dergelijke neptelefoontjes staan ook wel bekend onder de naam vishing, een samentrekking van voice en phishing. Uit het niets belt een “medewerker” van bijvoorbeeld Microsoft, de bank of politie je op met een nepverhaal.

Bekende neptelefoontjes

Bekend zijn de telefoontjes uit naam van een bank. Een “bankmedewerker” vertelt je dat er sprake is van een cyberaanval. Om te voorkomen dat je slachtoffer wordt, moet je je spaargeld “veilig stellen” door het naar een ander rekeningnummer over te maken. Helaas is dat net het bankrekeningnummer van de crimineel waarmee je aan de telefoon hangt.

Een andere bekende variant zijn telefoontjes uit naam van een helpdesk, bijvoorbeeld van Microsoft of een andere computerfirma. De beller beweert dat er problemen zijn gesignaleerd op je computer en is zo vriendelijk dit te willen oplossen. In werkelijkheid is er geen probleem. Je hebt te maken met een crimineel die geld wil buitmaken, bijvoorbeeld door malware te installeren op de computer.

Meekijksoftware

Bij veel neptelefoontjes, onder meer uit naam van Microsoft, speelt meekijksoftware een belangrijke rol. Om het zogenaamde probleem op te lossen vraagt de malafide helpdeskmedewerker software te installeren waarmee hij kan meekijken op je computerscherm. Dit gaat vaak om de programma’s Teamviewer of Anydesk. Na installatie kan de crimineel alles zien wat er op het scherm gebeurt, ook als je bankgegevens invult.

Robocalls

Criminelen zijn creatief in het verzinnen van nieuwe manieren om slachtoffers te maken. Een vrij recent verschijnsel zijn “robocalls”. Uit het niets krijg je een telefoontje waarin een computerstem (meestal Engelstalig) beweert te bellen namens een gezaghebbende instantie, bijvoorbeeld de politie of een overheidsdienst. Het bericht beweert dat je betrokken bent bij ernstige feiten, zoals witwaspraktijken of een arrestatiebevel. Na het indrukken van een toets krijg je de oplichters aan de lijn. Die proberen privégegevens te ontfutselen of geld buit te maken.

Voorkom bankfraude

Hou deze basisregels in gedachte om te voorkomen dat je slachtoffer wordt van bankfraude.

- De bank (of een andere instantie) belt je nooit om te zeggen dat je geld moet veiligstellen, moet overboeken naar een “kluisrekening” of iets vergelijkbaars.
- Als het nummer of de naam van je bank in je telefoondisplay verschijnt, kan het toch een fraudeur zijn. Dankzij spoofing kan de fraudeur het nummer waarmee hij belt hebben aangepast.
- Stuur je bankkaart niet op (zelfs niet doorgeknipt). Laat ze ook niet ophalen.
- Vraag bij twijfel de “medewerker” om zijn naam, hang op en bel zelf naar de bank.
- Zwicht niet voor verstrekte informatie die wordt gegeven om zogenaamd te bewijzen dat de bank je belt. De oplichter weet soms persoonlijke gegevens van je via phishing of van internet.
- Houd nooit een te hoog saldo aan op je betaalrekening. Ook bij andere vormen van oplichterij (zoals een gestolen bankkaart) kan de schade zo minder makkelijk oplopen.
- Stel een lagere daglimiet in. En verhoog deze niet onder druk van een (nep-)medewerker.
- Heb je onverhoopt toch geld overgemaakt? Neem zo snel mogelijk contact op met de bank, doe aangifte bij de politie en meld het op **meldpunt.belgie.be**.

Spoofing

De term spoofing kwam al voorbij toen het over nepberichten per e-mail ging. Spoofing komt ook voor bij neptelefoontjes. Via een technische truc kunnen criminelen het nummer waarmee ze bellen vervalsen. Daardoor zie je in het telefoonscherm het echte nummer van de bank, politie of een andere instantie, terwijl je in werkelijkheid een crimineel aan de lijn hebt. Hierdoor komt de oplichtingspoging zeer geloofwaardig over.

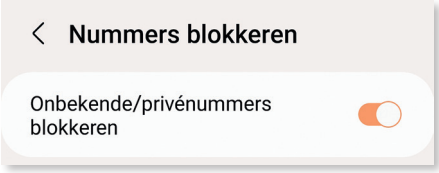
Terugbelfraude

Bij terugbelfraude bellen criminelen met een onbekend, vaak buitenlands telefoonnummer. Ze laten de telefoon twee keer overgaan en hangen dan op. Ze hopen dat je terugbelt naar dit nummer, want dan gaat de meter tikken. Het telefoonnummer is gekoppeld aan een dure betaaldienst. Hoe langer je aan de lijn blijft, des te meer de crimineel verdient. Het lijkt of er niet wordt opgenomen, maar in werkelijkheid komt de verbinding wel tot stand. De criminelen laten een bandje horen met de kiestoon, waardoor ze geld verdienen.

Om deze vorm van fraude te voorkomen, kun je instellen dat de telefoon bij onbekende telefoonnummers niet overgaat. De beller wordt automatisch naar je voicemail gestuurd. Deze oplossing helpt ook bij hinderlijke marketingtelefoontjes.

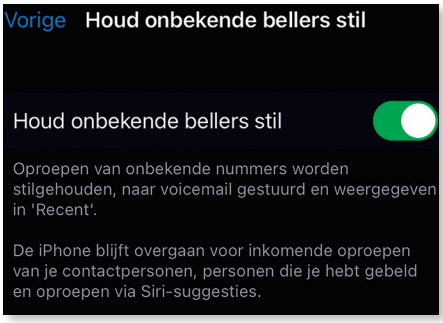
Android

1. Start de **Telefoon-app** en tik op ⋮.
2. Ga naar **Instellingen**.
3. Tik op **Nummers blokkeren**.
4. Zet het schuifje aan bij **Onbekende/privénummers blokkeren**.



iOS

1. Ga naar **Instellingen**.
2. Scrol naar beneden en kies **Telefoon**.
3. Scrol naar beneden en kies **Houd onbekende bellers stil**.
4. Zet het schuifje aan.



Winacties

Fraudeurs gebruiken pagina's en berichten op sociale media en apps om valse berichten de wereld in te sturen. Ze plaatsen er bijvoorbeeld winacties. Als je hierop ingaat, ontvang je een verzoek om betaalgegevens. De fraudeurs misbruiken vaak namen van bekende winkelketens. Rapporteer dit soort berichten. Veel socialemediasites hebben hier een speciale knop voor.