De fraudeur bijt en laat niet los

Onlinefraudeurs slaan vaker achter elkaar toe als ze eenmaal beet hebben. Dat is het beeld dat oprijst uit de fraudevormen die we de laatste tijd signaleren. Vooral 'hulp' bieden aan kwetsbare slachtoffers die ze zelf net hebben opgelicht, is nu populair bij fraudeurs.

Tekst **Vincent van Amerongen**
Beeld **Pixels&inkt**

De afgelopen tijd was het vaak in het nieuws: bankspoofing. In de Digitaalgids van mei signaleerden we deze zeer geraffineerde vorm van fraude al: nepbankmedewerkers die je bellen en je wijsmaken dat je geld moet worden 'veiliggesteld'. Dat ze daarbij lijken te bellen met het nummer van de bank ('spoofen'), wekt extra vertrouwen.

Inmiddels weten we meer over hun werkwijze en zien we alweer nieuwe varianten opduiken. Wat daarbij opvalt is dat bankspoofing wordt gecombineerd met andere fraude. 'Wat voor ons dit jaar nieuw was, was de combinatie van meerdere handelingen en fraudevormen om overtuigender over te komen', zegt Tanya Wijngaarde van de Fraudehelpdesk. Soms gaat het nog een stap verder. Eerst lichten de fraudeurs mensen op, om ze daarna zogenaamd als redder in nood te hulp te schieten. In werkelijkheid lichten ze je een tweede keer op.

We doen vier nieuwe vormen van deze 'combinatiefraude' uit de doeken. ➜

Fraude met meeste schade

(in miljoenen euro's)

Beleggingsfraude
11,1
(vooral bitcoinfraude)

Identiteitsfraude rechtspersonen
8,6
(waarvan bankspoofing 3,7 miljoen)

Voorschotfraude
6,6
(met name datingfraude)

Identiteitsfraude natuurlijke personen
6,2
(waarvan WhatsAppfraude 3,6 miljoen)

Bron: Fraudehelpdesk, cijfers jan-okt 2020


Heey pap, mn tel was kapot, dit is mijn nieuwe nummer
Heb ook een probleem met de bank en kan mijn huur niet overmaken.. Wil jij het voorschieten, krijg je het eind van de week terug.
Tuurlijk, hoeveel heb je nodig? En op welke rekening moet ik het storten?
ING BANK

1 Eerst gephisht, dan gespooft

Hoe kan het toch dat die zogenaamde bankmedewerkers zo geloofwaardig overkomen? Eén: ze lijken te bellen met het telefoonnummer van de bank. Twee: ze komen zeer beleefd en professioneel over. Ze blijken in veel gevallen nog een derde ijzer in het vuur te hebben. Wat veel slachtoffers namelijk rapporteren, is dat de 'bankmedewerker' hun saldo kende en recente transacties wist te noemen. Hoe dat mogelijk is, weten we intussen. Wijngaarde: 'Ze sturen eerst een phishinglinkje waardoor ze toegang krijgen tot iemands bankrekening. Met al die specifieke informatie over die rekening komen ze tijdens het gesprek erg overtuigend over.'

Volgens ING gaat aan zeker 40% van de bankspoofinggevallen phishing vooraf. Zo ook bij de 49-jarige Marco ('ik blijf liever anoniem'). Bij hem begint de ellende op Marktplaats. Op een vrijdagavond in september zet hij de camera van zijn dochter op Marktplaats. Na een uur meldt zich een koper, die voorstelt om te communiceren via WhatsApp ('Ik heb geen Marktplaats-app'): een bekende truc van criminelen om geen sporen achter te laten. De koper geeft zijn adres en stuurt kort daarop een DHL-linkje 'om de verzendkosten te betalen'. Marco klikt erop en wordt naar een nepsite gestuurd. Kennelijk weet de oplichter via die route toegang tot Marco's ING-rekening te krijgen. Als hij een sms van zijn bank krijgt ('Heeft u geprobeerd een tweede telefoon te activeren?') weet hij: ik ben in die link getrapt.

Net op het moment dat hij hierover ING wil bellen, wordt hij zélf gebeld door de 'fraudehelpdesk' van de bank. Die wil hem helpen, want er zijn verdachte activiteiten op zijn rekening. Dat klopt: het zijn de criminelen zelf die voor zijn oog geld overboeken van zijn spaarnaar zijn betaalrekening. Ook het 020-nummer van de ING klopt.

Vervolgens wordt hij op de inmiddels kenmerkende bankspoofing-manier voor bijna €10.000 opgelicht. De crimineel vraagt Marco geld naar 'veilige rekeningen' over te maken. In dit geval was het gekozen tijdstip ook uitgekookt: de échte ING-klantenservice is na 21 uur 's avonds gesloten.

Het whatsappje met de phishinglink dat Marco ontving

Fraude voorkomen

WhatsApp-fraude

- Vraagt een bekende je via WhatsApp dringend om een rekening te betalen? Bel die persoon om het te checken.
- Appt deze persoon vanaf een nieuw nummer? Dat is extra verdacht. Bel die persoon op het oude nummer.
- Hoor je een bekende stem ('Hallo?') als je het nieuwe nummer belt? Die kan nep zijn. Criminelen nemen soms de stem van een bekende van je op en spelen die af als je belt.

Bankspoofing

- Je bank belt je nooit om te zeggen dat je geld moet veiligstellen, moet overboeken naar een 'kluisrekening' of iets vergelijkbaars.
- Bij twijfel: vraag de 'medewerker' om zijn naam, hang op en bel zelf naar de bank.
- Vertrouw niet op het 'bekende' nummer dat je ziet in het display. Oplichters kunnen dat namaken.
- Zwicht niet voor persoonlijke informatie om zogenaamd te bewijzen dat de bank je belt. Die kunnen ze via phishing of social media hebben verkregen.
- Bankmedewerkers komen nooit aan huis om je te 'helpen' tegen oplichting of om een bankpas op te halen. Laat ze niet binnen, maar bel de politie en je bank.

2 Eerst WhatsApp-fraude, dan spoofing

Er zijn helaas meer varianten waarbij het 'belletje van de bank' niet uit de lucht komt vallen. Lisanne (ook liever geen achternaam) was 's middags in het museum met haar kleinkinderen toen ze een appje kreeg van haar 'dochter'. Haar telefoon was stuk, zei ze, vandaar dat ze appte vanaf een nieuw nummer. Inderdaad, een klassiek geval van WhatsApp-fraude. Lisanne had van alles aan haar hoofd en de oplichters profiteerden daar optimaal van. In de loop van de middag en avond maakte ze in totaal €7000 over om 'rekeningen te betalen' van haar 'dochter'. Maar hier eindigt het verhaal nog niet.

Om 10 uur 's avonds werd ze gebeld door 'een heel keurige meneer van de ING'. Vanaf het echte nummer van de bank. De bank had verdachte transacties gezien op haar rekening. In werkelijkheid had Lisanne wederom de oplichter aan de lijn. Dankzij de WhatsApp-truc kwam hij nu extra geloofwaardig over, omdat hij haar rekeningnummers en saldi kende. Lisanne had namelijk eerder die dag haar 'dochter' via WhatsApp schermfoto's gestuurd van de overboekingen. Aan het eind van de avond was ze volledig uitgeput en liefst €41.000 armer.

Totale schade door fraude

(in miljoenen euro's)

bron: Fraudehelpdesk

3 Eerst gebeld, daarna huisbezoek

In voorbeelden 1 en 2 ging het om bankspoofing. ING, de bank met de meeste gedupeerden, heeft gelukkig eindelijk een maatregel genomen die bankspoofing stukken lastiger maakt: een wachttijd van 4 uur op het verhogen van de overboeklimiet. Misschien is dat de reden dat oplichters de aloude babbeltruc van stal lijken te hebben gehaald: een bezoek aan huis.

Ook nu weer zien we een een-tweetje. Eerst belt een 'bankmedewerker' met een alarmerend bericht ('uw bankpas is niet meer goed' of 'iemand probeert uw rekening leeg te halen'), waarna hij aanbiedt om langs te komen om het op te lossen. De NOS berichtte onlangs over de 81-jarige Joop Rotteveel. 'Er kwam een jonge knaap binnen die een pasje van een bank liet zien', vertelt hij. Voor hij er erg in had, had de oplichter op zijn computer de daglimiet verhoogd. En zogenaamd om misbruik te voorkomen, nam hij de pinpas mee. De oplichter knipte de pas daarbij demonstratief door midden. Rotteveel wist niet dat de pas werkt zolang de chip nog werkt. De magneetstrip doet er niet meer toe. Daarna werd er met die pas voor duizenden euro's gepind.

De Fraudehelpdesk heeft op dit moment nog maar een handvol meldingen gekregen over 'bankbezoeken' aan huis, maar de politie ziet wel een opvallende stijging. Vooral ouderen zijn het doelwit.

Opgelicht, wat nu?

1 Neem direct contact op met je bank. Laat rekeningen en passen blokkeren en vraag wat je moet doen om je geld terug te krijgen.
2 Verzamel bewijsmateriaal. Maak schermafbeeldingen van appjes, sms'jes en QR-codes.
3 Doe aangifte bij de politie. De meeste banken vergoeden je schade anders sowieso niet.
4 Controleer je computer of smartphone op schadelijke software.
5 Wijzig wachtwoorden en wacht met internetbankieren tot je er zeker van bent dat je apparaten vrij zijn van schadelijke software.
6 Vergoedt de bank niet, ook niet na een officiële klacht? Dan kun je in beroep gaan bij de geschillencommissie Kifid.

→

4 Beleggingsfraude, daarna 'geholpen'

Door alle media-aandacht voor WhatsApp-fraude en bankspoofing zou je het misschien niet denken, maar volgens de Fraudehelpdesk richt beleggingsfraude de meeste schade aan: in 2020 tot 1 oktober al €10 miljoen – zie de cijfers op pagina 10. Het gaat om relatief weinig mensen, maar die lijden wel vaak tonnen schade. Bij deze oplichting worden mensen verleid om te investeren in bitcoins, vaak zogenaamd aangeprezen door bekende Nederlanders als Jort Kelder en Matthijs van Nieuwkerk.

Bitcoinfraude bestaat al langer. Maar net als bij bankspoofing hebben ook bij deze fraudevorm oplichters ontdekt dat je slachtoffers daarna 'hulp' kunt aanbieden.

De 62-jarige Frits (die ook anoniem wil blijven) ondervond het aan den lijve. Het begint in juni 2019 bij een juichende Facebook-advertentie met BN'ers over beleggen in bitcoins. Hij besluit een klein bedrag in te leggen, en dat lijkt te renderen. Dus als hij gebeld wordt met de vraag of hij meer wil inleggen, hapt hij toe. Hij laat zijn pc overnemen ('ik werk in de IT dus ik vond dat heel normaal') en laat €6000 overboeken naar een neprekening. Hij onderhoudt wekelijks contact, tot in maart 2020, bij het begin van de coronacrisis, zijn (nep)saldo terugloopt tot onder nul. Het bedrijf is van de radar verdwenen.

Dan wordt Frits enkele maanden later, in augustus, gebeld door een 'lieve juffrouw' van 'Consumers Protection' die zijn verhaal van de politie had gekregen en hem wel wil helpen. Een vertrouwenwekkende mail en gesprekken met charmante deskundigen trekken hem over de streep. Hij moet wederom inleggen op bitcoinrekeningen, 'anders gaat de belasting moeilijk doen'. De rekeningen zijn ditmaal wel echt, alleen niet van hem, maar van de oplichters. Uiteindelijk gaat Frank voor ruim €20.000 het schip in en blijft hij zitten met een schuld.

Het nep-bitcoinaccount van Frits

Voorbeeld van een 'nieuwsbericht' van bitcoinfraudeurs

Conclusie

Het is duidelijk dat je niet zomaar van online-oplichters af bent. Als ze eenmaal beet hebben en weten dat je kwetsbaar bent, laten ze niet snel meer los. Het goede nieuws is dat de banken slachtoffers van bankspoofing gaan compenseren, al ging dat niet zonder slag of stoot. De Consumentenbond wil nu dat de wet wordt aangepast om consumenten beter te beschermen bij toekomstige fraudevormen – zie ook het kader op deze pagina.

Voorkom online oplichting

Internetcriminelen verzinnen steeds weer nieuwe trucs en zijn actiever dan ooit. Ons boek 'Voorkom online oplichting' gaat uitgebreid in op alle vormen van oplichting via internet. We geven veel praktische tips en adviezen waarmee je kunt voorkomen dat je zelf online wordt opgelicht.

€22 (niet-leden €27,50), als e-book €14 (niet-leden €17,50)
consumentenbond.nl/voorkomonlineoplichting

Banken gaan bankspoofing vergoeden

Onder grote druk vanuit de politiek, Kassa en de Consumentenbond gaan de vier grootbanken spoofing nu toch compenseren. Tot nog toe vergoedde alleen de Rabobank de schade, en alleen uit coulance. Vincent van Amerongen is campagneleider bankoplichting: 'ING en ABN Amro zeiden steeds: je hebt het geld zelf overgemaakt. Dan hoeven we de schade niet te vergoeden.'
Na een gesprek met het ministerie van Financiën krijgen slachtoffers nu dus toch hun geld terug, maar wel onder voorwaarden. Van Amerongen ziet nog wel losse eindjes. Zo doen nog niet alle banken mee. 'En het blijft coulance. Dit soort bescherming moet bij wet worden vastgelegd'.
Lees ook het artikel op pagina 8, en het laatste nieuws op **consumentenbond.nl/vergoed-bankoplichting**.

Consumenten bond

Digitaal bijblijven?

In de Digitaalgids vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding