

NIEUWE FRAUDE: BANKSPOOFING

Oplichters hebben weer iets nieuws bedacht: ze doen zich voor als bankmedewerkers en laten hun slachtoffers duizenden euro's overmaken. Banken vergoeden de schade in principe niet. Lees en huiver...

DE 'BANK' AAN DE LIJN

Anneke van der Meer krijgt eind september een telefoontje van een ABN Amro-medewerker. Ze is van de afdeling Fraudebestrijding en wil weten of Van der Meer net €2500 aan het overboeken is. En is er misschien afgelopen week een onbekend bedrag van haar rekening afgeschreven? Verontrust logt Van der Meer in via internetbankieren. Ondertussen vraagt ze hoe ze kan verifiëren of de medewerker echt van ABN Amro is. Dit kan Van der Meer volgens de medewerker simpel controleren: als je het noodnummer van de bank via Google opzoekt, zie je hetzelfde nummer als waarmee zij belt. Dat klopt inderdaad. Van der Meer moet echt haar geld veiligstellen. De bank heeft 72 uur nodig

Banken vergoeden bankspoofing meestal niet, omdat slachtoffers het geld zelf hebben overgeboekt

om haar rekening te herstellen, vertelt de behulpzame medewerker. In de tussentijd kan Van der Meer het naar een kluisrekening overmaken, daar is het veilig. In totaal geeft ze drie betaalopdrachten van elk bijna €5000. Drie kwartier later wordt ze weer gebeld, dit keer écht door ABN Amro. Waarom ze zulke grote bedragen probeert over te maken? Dan wordt duidelijk dat ze opgelicht is. Volgens de medewerker kan mevrouw aangifte doen bij de politie, verder is er niets meer aan te doen. De bank hield nog wel twee van de drie overboekingen tegen. Maar de schade voor Van der Meer is toch bijna €5000.

Honderden slachtoffers

Er zijn dit jaar honderden klanten slachtoffer geworden van deze nieuwe vorm van

20

MILJOEN EURO IS IN 2020 DE GESCHATTE SCHADE VOOR NIEUWE FRADEVORMEN ZOALS BANKSPOOFING

online oplichting. Bij bankspoofing, zoals deze fraude wordt genoemd, misbruiken criminelen het telefoonnummer van een bank. Doordat het lijkt alsof je echt wordt gebeld vanaf het telefoonnummer van de bank, trap je er gemakkelijk in. Voorafgaand aan het telefoontje is het slachtoffer soms al op een phishingbericht ingegaan. Hierdoor weet de oplichter bijvoorbeeld het banksaldo en wat de laatste afschrijvingen zijn. Dit wekt nog meer vertrouwen. En maakt het slachtoffer extra ontvankelijk voor het verhaal, want hij heeft inderdaad op een fout linkje geklikt. De oplichter laat hem geloven dat zijn rekening misbruikt wordt. Om het (spaar)geld veilig te stellen, moet hij het tijdelijk overmaken naar een zogenaamde kluisrekening. In werkelijkheid is dit de rekening van een katvanger: iemand die zijn rekening beschikbaar stelt om zo het geld door te sluisen of op te nemen.

Niet coulant

Slachtoffers die bij hun bank aankloppen voor een schadevergoeding, komen vaak van een koude kermis thuis. Banken vergoeden deze vorm van oplichting niet, omdat slachtoffers het geld zelf hebben overgeboekt. Banken noemen dit niet-bancaire fraude. Volgens de banken zijn ze volgens de wet alleen aansprakelijk als de crimineel de betaalopdracht heeft uitgevoerd, bijvoorbeeld doordat hij inloggegevens heeft ontfoetseld. Spoofing valt volgens de banken dus buiten de voorwaarden voor vergoeding van fraude. Wij vroegen de banken naar hun beleid bij

bankspoofing. De meeste beroepen zich inderdaad op de wet en vergoeden niets. ABN Amro en ING zijn het striktst, ze vergoeden in beginsel niet. Triodos Bank en Volksbank (ASN Bank, RegioBank en SNS) geven een kleine opening; uit coulance gaan ze soms over tot een (gedeeltelijke) vergoeding. Knab bekijkt per fraudemelding hoe ermee omgegaan wordt. Rabobank is de enige die aangeeft een groot deel van de spoofing-schade te vergoeden. De bank kijkt in hoeverre er misbruik is gemaakt van de positie van de bank, bijvoorbeeld doordat de site of klantenservice is nagebootst. Bij spoofing is dit volgens de Rabobank het geval. Daarmee is de bank ruimhartiger dan de andere banken. Wij vinden dat vergoeden de standaard moet zijn, en dat slachtoffers niet afhankelijk moeten zijn van coulance van hun bank.

Afschuiven

Banken schuiven te gemakkelijk hun verantwoordelijkheid af bij bankspoofing. Ook al heeft de klant het geld zelf overgemaakt, het is toch een zeer doortrapte vorm van fraude. De schade is vaak groot. Niet alleen financieel, maar meestal ook psychisch. Veel slachtoffers schamen zich. Banken hebben een morele plicht bij deze ▶

VOORKOM BANKSPOOFING

- Weet dat een bank nooit belt om te zeggen dat je geld moet veiligstellen, overboeken naar een 'kluisrekening' of iets vergelijkbaars.
- Vraag bij twijfel de medewerker naar zijn naam, hang op en bel zelf naar de bank.
- Trap er niet in als de 'bank' informatie verstrekt om te bewijzen dat de bank je belt. De oplichter weet soms persoonlijke gegevens van je via phishing of internet.

ÉÉN

TELEFOONTJE EN AL
JE SPAARGELD IS WEG

vorm van fraude, vinden wij. Ze hebben hun klanten jarenlang gestimuleerd om hun bankzaken digitaal te regelen, ook als ze dat eigenlijk liever niet wilden. Juist voor deze laatste groep, die alsnog is overgestapt op digitaal bankieren, is het vaak nog lastiger om nieuwe trucs te doorzien.

Zo kregen wij laatst een melding van een lid, wiens 81-jarige vriendin bijna €50.000 kwijtraakte van haar ING-rekening. 'Zij bankierde na veel dwang van haar bank digitaal, op haar tablet. Maar ze is er niet mee grootgebracht. Nu het mis is gegaan, durft ze niet meer te bankieren en pinnen. Een bank heeft toch ook een zorgplicht voor deze groep ouderen. Ze heeft het gevoel dat de bank haar compleet heeft laten barsten.'

Een begrijpelijke reactie, vinden wij. We willen dat banken de schade voor slachtoffers van spoofing vergoeden. En dat ook toekomstige fraudevormen binnen de

verantwoordelijkheid van de bank gaan vallen. Want helaas weten we dat als bankspoofing niet meer werkt, criminelen weer iets nieuws verzinnen.

Voorkomen

Voorkomen is beter dan genezen. Wij vroegen banken daarom ook sinds wanneer en op welke manier ze hun klanten waarschuwen voor spoofing. De banken verwijzen onder meer naar de gezamenlijke landelijke campagne van de Betaalvereniging: 'Hang op, klik weg, bel uw bank'. Met deze campagne wordt volgens de banken al sinds begin dit jaar gewaarschuwd voor spoofing. Maar een directe waarschuwing tijdens het inloggen of overboeken lijkt ons in dit geval effectiever.

Het verschilt in hoeverre banken waarschuwen voor bankspoofing. ING bijvoorbeeld, waarover de meeste meldingen gingen, nam pas maatregelen na uitgebreide aandacht in de media. Klanten krijgen sinds begin november een waarschuwing na het inloggen. ING verhoogde ook de wachttijd voor het verhogen van je limiet voor overboekingen naar vier uur. En geeft dan nogmaals een waarschuwing. Goede maatregelen, maar voor eerdere slachtoffers komen ze te laat.

TOCH SLACHTOFFER?

- **Neem direct contact op met de bank. Ook al vergoedt die de schade vaak niet, soms kan er nog iets gedaan worden.**
- **Vraag de bank te bevestigen dat er direct een bericht is gestuurd naar de bank waarnaar geld is geboekt.**
- **Doe altijd aangifte bij de politie.**
- **Meld je bij de stichting Gibo (stichtinggibo.nl).**

Ook zijn de banken in gesprek met de telecomsector. Als spoofing technisch onmogelijk wordt gemaakt, kunnen criminelen zich in ieder geval niet zo makkelijk voordoen als bankmedewerkers. Wij houden het in de gaten.

Rekening blokkeren

Kunnen banken het geld dan niet gewoon terugboeken? Praktisch is dat vaak onmogelijk, omdat de oplichter ervoor zorgt dat het geld al is opgenomen. Zeker na de invoering van Instant Payments, waardoor het geld binnen vijf seconden op een andere rekening staat. Knab is de enige bank die aankondigde Instant Payments uit te zetten als de bank denkt dat dit nodig is. Om zo verdachte transacties nog op tijd stop te zetten.

Eenmaal bij de ontvanger mag een bank een 'geldige betaalopdracht' niet terugdraaien. Omdat slachtoffers deze opdrachten zelf uitvoeren, zijn ze geldig. Banken kunnen wel de betaalrekening(en) van de criminelen of katvangers blokkeren, maar dan is het vaak al te laat. Als slachtoffer kun je je het beste direct melden bij je eigen bank. Die stuurt dan een bericht naar andere banken. Is het geld nog niet opgenomen of naar een volgende rekening gestuurd, dan kun je het nog terugkrijgen (zie het kader 'Toch slachtoffer?'). De 81-jarige ING-klant nam zelf contact op met de banken waarnaar het geld was overgemaakt en wist via één bank de helft van de €50.000 terug te krijgen.



Vincent van Amerongen is hoofdredacteur van de Digitaal-gids en expert online oplichting

'Banken moeten gedupeerden compenseren'

'Het is voor consumenten bijna onmogelijk om deze doortrapte fraude te doorzien. Wij vinden daarom dat banken de gedupeerden moeten compenseren. En dan niet alleen uit coulance. Vergoeden moet het uitgangspunt zijn, en dat moet ook worden vastgelegd. Of de klant wel of niet het geld zelf heeft overgemaakt, mag daarbij geen rol spelen. Onze gesprekken met de banken hebben helaas niets opgeleverd. Minister Hoekstra gaat nu met de banken praten. Hopelijk trekt hij ze over de streep. En anders moet de wet maar worden aangepast.' Lees meer over onze actie op consumentenbond.nl/vergoed-bankoplichting. Geïnteresseerd in digitale onderwerpen? Op digitaal-gids.nl delen we regelmatig (gratis) artikelen en nieuwsberichten.

Smaakt dit naar meer?

Word lid en krijg direct toegang tot alle
onafhankelijke tests en informatie.

