Meegewerkt met de oplichter

3 NIEUWE FRAUDEVORMEN ONTRAFELD

Criminelen verzinnen steeds nieuwe trucs om mensen digitaal op te lichten. We bespreken drie nieuwe trucs, met als gemene deler: slachtoffers werken ongemerkt mee. Hoe werken de trucs, hoe voorkom je ze en: vergoeden de banken de schade?

Tekst: **Vincent van Amerongen**

Jozef Tomesen werd slachtoffer van telefonische spoofing

foto beeldredaktie

1 Telefonische spoofing

'Het is ruim een maand geleden, maar mijn vrouw en ik slapen er nog steeds slecht van'. Aan het woord is Jozef Tomesen, die slachtoffer is geworden van telefonische spoofing. Daarbij word je opgelicht door iemand die zegt van de bank te zijn, met het noodnummer van die bank op je scherm. Helemaal bedrieglijk als je het noodnummer van de bank in je contactenlijst hebt opgeslagen.

Tomesen werd medio februari 's middags gebeld op zijn vaste lijn door iemand die zich voorstelde als een medewerker van de Rabobank. 'Hij sprak rustig en ontspannen en kwam deskundig over. Hij vroeg: "Bent u nu bezig met een transactie? Nee? Daar waren we al bang voor".'

Tomesen werd wijsgemaakt dat zijn geld snel veiliggesteld moest worden om te voorkomen dat hij slachtoffer zou worden van phishing. Hij rook geen onraad. Het noodnummer van de Rabobank stond immers in beeld. En vanwege de professionaliteit van de oplichter: 'Hij had overal een antwoord op, wist uit zichzelf de laatste cijfers van

mijn rekening en gaf tussendoor zelfs financiële tips'. Het uiteindelijke bedrag, dat in meerdere transacties naar verschillende rekeningen werd overgemaakt, is zo hoog dat Tomesen het niet genoemd wil hebben. Pas in de loop van de avond viel het kwartje. 'Ik zou nog worden teruggebeld maar dat gebeurde niet. Toen ben ik mijn rekening gaan checken. Alles was weg.'

Aanvankelijk wijst de lokale Rabobank-filiaal zijn verzoek om compensatie bot af ('daar kunnen we niet aan beginnen'), maar Tomesen blijft aandringen. Kort na ons interview belt een opgetogen Tomesen dat de bank het volledige bedrag tóch terugboekt.

Vlotte babbel

In korte tijd heeft de politie al tientallen meldingen gekregen over deze telefonische spoofing met een totaal schadebedrag van meer dan een miljoen euro. 'We zijn druk bezig met het onderzoek om de daders op te sporen', zegt Caroline Sander van het Electronic Crimes Task Force (ECTF), een samenwerkingsverband tussen de politie en de banken. 'Technisch gezien is het eenvoudig om iemand te spoofen. Verder heb je vooral een vlotte babbel nodig.'

Net als bij de andere nieuwe fraudevormen gaat het om groepen jonge mensen die opereren vanuit Nederland en de taal goed machtig zijn. 'Het zijn groepen waarin iedereen een vaste taak heeft: de een is technisch onderlegd, de ander ronselt bankpassen om het buitgemaakte geld mee te pinnen, weer een ander doet de babbeltruc. En ze geven het geld ook gewoon in Nederland uit, aan mooie spulletjes.'

Sander benadrukt daarnaast het belang van aangifte doen, ook al kan niet elke zaak worden opgepakt. 'Deze daders werken vaak in een groep en maken meerdere slachtoffers. Elke aangifte helpt geeft ons informatie over de omvang en hun werkwijze. En dus een grotere kans om de zaak op te lossen.'

foto beeldredaktie

Jurgen Hoogenboezem was getuige van een WhatsApp-kaping

2 WhatsApp kapen

Een tweede truc die in opkomst is, is een nieuwe vorm van fraude via WhatsApp. Daarbij neemt de oplichter iemands WhatsApp-account over om zijn of haar kennissenkring te bestoken met een appje als deze: 'Hoi, ik kan even niet bij mijn spaargeld, kun jij deze factuur even betalen? Morgen krijg je het terug'. Langs deze slinkse route is een contactpersoon van Jurgen Hoogenboezem begin maart voor bijna €2800 opgelicht.

Deze WhatsApp-kaping zit geraffineerd in elkaar en begon in het geval van Hoogenboezem op Marktplaats. 'Mijn vrouw had een advertentie voor laarzen op Marktplaats gezet. Ze kreeg een WhatsApp-berichtje van iemand die geïnteresseerd was, en kwam een prijs overeen. Kort daarop kreeg ze een sms'je met een verificatiecode voor WhatsApp, met daarachteraan een appje: 'sorry, dat was voor mijn vrouw, kun je me die code sturen?'. Wat er echt aan de hand was: de oplichter probeerde haar WhatsApp-account over te nemen. Hoogenboezems vrouw, druk met haar eigen zaak, doet dat en denkt er verder niet over na. Die verificatiecode is precies wat de oplichters nodig hebben om haar WhatsApp-account over te nemen en daarmee binnen haar vriendenkring om geld te vragen.

De Fraudehelpdesk ontving tot en met begin april dit jaar al 63 meldingen van WhatsApp-kaping, tegen 148 in heel 2019. Dat is nog altijd maar een fractie van de 'klassieke' WhatsApp-oplichting. Bij deze vorm appt de oplichter vanaf een onbekend telefoonnummer maar met naam en foto van een bekende ('hoi pap, ik heb een nieuw nummer').

De financiële schade bij de WhatsApp-kaping is volgens woordvoerder Tanya Wijngaarde lastig te schatten. 'Dat komt omdat de mensen die benaderd worden om geld over te maken, niet degenen zijn die melden dat hun account is gehackt.'

Er is gelukkig een eenvoudige manier om te voorkomen dat je WhatsApp-account wordt gekaapt: door er een extra pincode-slot op te zetten. Hoe je dat doet, lees je op pagina 13.

→

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 nog in beroep gaan bij het **Kifid**, de geschillencommissie van de banken.

3 Fraude met QR-codes

De derde truc valt vooral op doordat alleen ING-klanten de dupe lijken te worden: het gaat om een fraude waarbij kwaadwillenden je met een smoes een QR-code laten scannen om toegang tot je bankrekening te krijgen. Bij Robert ('liever geen achternaam') begon de ellende toen hij iets te koop aanbood op Marktplaats.

'Iemand uit Vlissingen reageerde en we kwamen een prijs overeen. Toen zei hij: "Zit je bij de ING? Ik ook. Ik stuur je een QR-code om het overgeboekt te krijgen vanaf mijn zakelijke rekening." Ik had geen argwaan. Ik heb wel vaker betalingen gedaan met een QR-code.' De eerste keer mislukte de betaling. 'Toen begon hij agressief te worden. Ik voelde me onder druk gezet en klikte door een paar schermen heen. Nog geen 5 minuten later had ik ING aan de lijn. Er was €5000 van mijn rekening gepind.'

Rick, een ander slachtoffer, werd op straat aangesproken door een groepje jongens. 'Ze hadden geld nodig voor de parkeermeter en die accepteerde alleen pinpassen. Of ik €5 kon overmaken via een QR-code, dan gaven ze mij €5 contant. Ze vroegen om mijn telefoon om een QR-code te scannen. Ik kon half meekijken maar zag niets vreemds.' Pas 's avonds kwam hij erachter dat al zijn spaargeld, €4600, was verdwenen.

Beide slachtoffers voelen grote schaamte, maar zijn ook verbaasd dat het misbruik met een QR-code bij ING zó eenvoudig is. Robert: 'Er zijn in totaal acht transacties uitgevoerd zonder dat er maar één keer een code hoefde te worden ingetoetst. Hoe is dat mogelijk? Terwijl ING me direct erna belde. Ik krijg mijn geld niet terug, omdat ik zelf toegang heb gegeven. Ook Rick vindt dat ING aan 'victim blaming' doet. 'Maar ik heb me gewoon aan hun veiligheidsregels gehouden. En het komt kennelijk vaak voor, want toen ik ze belde, vroegen ze zelf al: 'Was het een QR-code?' Hij kreeg zijn geld gelukkig wel terug, omdat het kon worden teruggehaald.

ING overstag

Het is op zijn minst opmerkelijk dat QR-fraude vrijwel alleen ING-klanten treft. Dat wijst erop dat misbruik bij ING eenvoudiger is dan bij andere banken. Van de grootbanken kun je alleen bij de Rabobank ook met een QR-code een tweede toestel koppelen. Maar bij de Rabobank moet je je geheime code op het nieuwe toestel invoeren, bij ING op het oude.

Dick Snel, cybersecurity-expert bij Onvio: 'Bij de Rabobank is dat veiliger. Als je bij de Rabobank je huidige pincode op het nieuwe apparaat moet invoeren, voorkom je daarmee de aanval. De oplichter weet jouw pin namelijk niet'.

ING is al in september 2019 door het tv-programma Kassa op het matje geroepen. Zij beloofden toen alle slachtoffers te compenseren én de app beter te beveiligen met extra waarschuwingsschermen.

Aanvankelijk laat ING ons weten de schade niet te vergoeden. Deze klanten hebben immers zelf de QR-code gescand. Twee weken later gaat de bank toch overstag: alle gedupeerden krijgen alsnog hun geld terug.

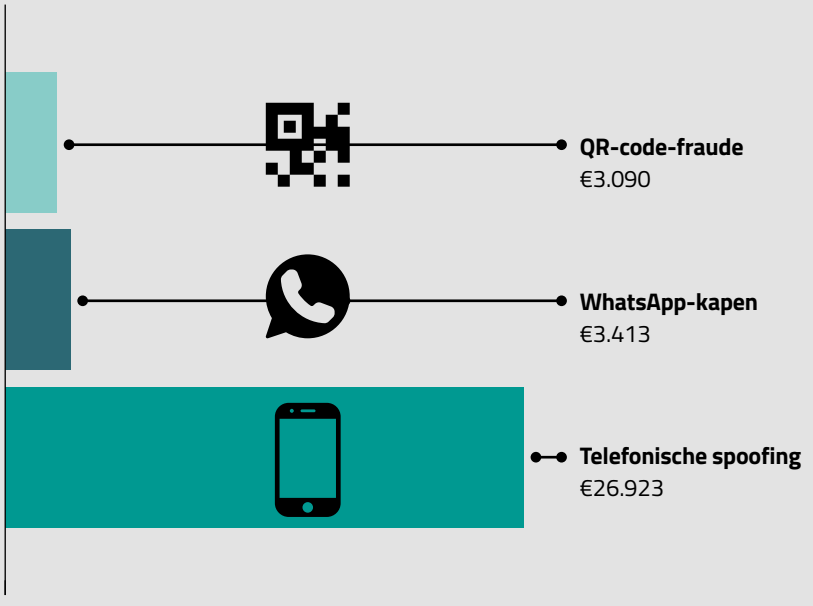
Woordvoerder Eva Hersbach: 'De reden hiervoor is dat we, ondanks extra waarschuwingen in het installatieproces, de afgelopen twee maanden helaas weer meer meldingen zien van klanten die worden opgelicht door het scannen van een QR-code'. Bovendien gaat de bank, om nieuwe slachtoffers te voorkomen, helemaal stoppen met de QR-code om een extra toestel te koppelen.

Bankregels achterhaald

ING erkent hiermee impliciet dat de oude criteria om schade te vergoeden,

Geleden schade per persoon

gemiddeld schadebedrag per persoon (stand 1 april)



2215 meldingen ontving de Fraudehelpdesk in 2020 al over WhatsApp-fraude (stand 6 april).

bron: Fraudehelpdesk

achterhaald zijn. De belangrijkste is dat klanten hun codes en pas niet moeten afstaan.

Maar met de nieuwe trucs laten oplichters slachtoffers zelf aan de juiste knoppen draaien om ze geld afhandig te maken. Dat gebeurt zo geraffineerd, dat ze het zelf niet doorhebben. Toch is het officiële standpunt van ABN Amro, Rabobank en ING nog steeds dat als je zelf hebt meegewerkt, je in beginsel niets terugkrijgt.

Ben Schellekens, campagneleider bij de Consumentenbond, heeft de Betaalvereniging Nederland in november vorig jaar al gevraagd om een herziening van die veiligheidsregels en een coulantere opstelling, maar die heeft nog geen actie ondernomen.

'We moeten helaas vaststellen dat de bestaande regels consumentonvriendelijk zijn, en dat de banken tot nu toe nauwelijks bereid zijn dit te veranderen. De Consumentenbond is hierover niet tevreden en zal de banken hierop aanspreken.'

Meer informatie:
www.consumentenbond.nl/veilig-internetten

Zo voorkom je fraude

WhatsApp-kaping

▪ Zet **tweefactorauthenticatie** aan in WhatsApp: Open WhatsApp en tik op Instellingen > Account > Verificatie in 2 stappen > Inschakelen. Kies een code die je niet kunt vergeten, maar die niet te makkelijk te raden is. WhatsApp zal je geregeld om de code vragen, zodat je die niet vergeet.

▪ Zet een **pincode** op je voicemail van je mobiele telefoon die je niet makkelijk kunt raden. Oplichters kunnen de verificatiecode namelijk ook laten doorbellen in de hoop dat dat bericht in je voicemail terechtkomt.

▪ Als een bekende je via WhatsApp dringend vraagt om een rekening te betalen, bel die persoon dan altijd om te checken of het klopt.

Fraude met QR-codes

▪ Wees altijd alert met QR-codes. Scan nooit een QR-code van een **onbekende**.

▪ Geef ook nooit je **toestel** uit handen aan een **onbekende**.

▪ Laat je niet **afleiden** nadat je een QR-code hebt gescand. Lees de teksten goed die in je scherm verschijnen en of die inderdaad zijn wat je verwachtte.

Telefonische spoofing

▪ Banken bellen je niet om geld over te maken. Word je uit het niets gebeld door de bank, met een verhaal over 'geld veiligstellen'? Hang op. Twijfel je? Bel zelf de bank.

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