

Informatieavond fraude en oplichting

BANKHELPDESKFRAUDE / NEPAGENTEN

Dit betreft het uittreksel van de informatieavonden in Noordenveld, gehouden in mei 2025. Het is een samenvatting van de dia's die getoond zijn.



politie.nl

BANKHELPDESKFRAUDE

Wat is bankhelpdeskfraude?

- Vaak telefonisch
- Daders doen zich voor als bankmedewerkers
- Het doel is om geld en/of waardevolle spullen afhandig te maken

Hoe gaat dat in zijn werk?

Stap 1: Fraudeur belt of sms't het slachtoffer

Bij het bellen kan gebruik worden gemaakt van:

- Spoofing
- Typosquatting (Go0gle.nl of Po1itie.nl)
- Een anoniem nummer
- Een normaal nummer (06 of netnummer)
- Een zakelijk nummer (088)



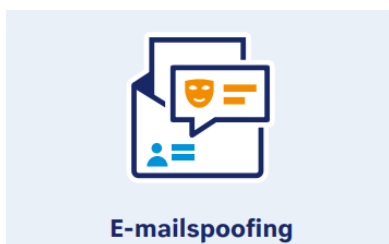
Wat is Spoofing:

- Legitieme technologie
- Door criminelen gebruikt voor

Typosquat Domain Example

www.g!thub.com
www.gougle.com — Typos
www.amozon.com — Missing an 'S'
www.victoriasecret.com
www.homdepot.com — Letters reversed

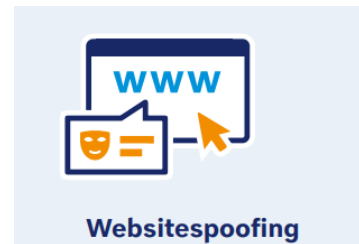
Verschillende manieren:



E-mailspoofing



Telefoonspoofing



Websitespoofing



politie.nl

Stap 2: Fraudeur geeft aan dat er iets aan de hand is met de bankrekening van het slachtoffer

Hij belooft te helpen door het vermogen van het slachtoffer veilig te stellen.

i *Tijdens het telefoongesprek maakt de fraudeur gebruik van social engineering. Dit is het psychologisch manipuleren van personen, zodat zij handelingen verrichten die niet in hun voordeel zijn. Een fraudeur zit soms uren aan de lijn met een slachtoffer.*

Stap 3: Vervolgens zijn er drie mogelijkheden



Het slachtoffer maakt zelf het geld over naar de zogenaamde veilige rekening van de bank.



De dader stuurt een koerier langs om de doorgeknipte pinpas en/of andere waardevolle spullen op te halen.



De fraudeur installeert een RAT op het (computer)systeem van het slachtoffer en voert handelingen uit met zijn of haar bankrekening.



Stap 4: Fraudeur verkrijgt het geld

- Via een geldezel (money mule)
- Vanuit een pintransactie (met opgehaalde bankpas)
- Via cryptovaluta, dit doet hij om het geldspoor te verhullen



Manipulatie:

Door bijvoorbeeld een codewoord of pincode

Hoe: Bankhelpdeskfraude voorkomen

- Je bank belt nooit dat je geld moet veiligstellen/overboeken
- Stuur nooit een pinpas op, ook niet laten ophalen
- Vraag naar de naam van de medewerker (bij twijfel)
- Laat je niet 'ompraten' met persoonlijke informatie
- Verlaag je daglimiet
- Bij ING kun je al checken wie je aan de lijn hebt



Belt ING? Check het gesprek

[< Vorige](#)Check het Gesprek



ING aan de telefoon of niet?
Vul hieronder je telefoonnummer in. Dan checken we meteen of er nu vanuit ING naar jouw nummer gebeld wordt.

Wat is je telefoonnummer?

 NL 

(+31)

Check het Gesprek



politie.nl

Diverse voorbeelden

ING LET OP!

Geldopname geweigerd. Er is zojuist een bedrag van EUR 3500 geprobeerd op te nemen aan de geldmaat op de (Ginnekenweg [46 4818](#) JG te Breda). Bent u dit niet geweest? Neem dan zo spoedig mogelijk contact op met de klantenservice ([085](#)) [666 36677](#)

<  +48 507 511 784 >

Tekstbericht
Vandaag 15:31

Uw openstaande schuld van: €448,00 is tot op heden niet betaald. Betaal dit nog voor 09-01-2024 via: <https://afbetaling-schuld.org/belastingdienst/BD58460901>

KPN NL 10:51 97%

Triodos Bank
zakelijk algemeen

 Herinnering  Bericht

 Weiger  Accepteer

INFO [SNSBANK]

Geachte klant,

We nemen contact met u op i.v.m een bedrag van 3400,00 euro dat is geprobeerd op te nemen met uw betaalpas in Texel. Wij hebben dit voor nu geannuleerd. Bent u dit **NIET** zelf geweest? Neem dan zo snel mogelijk contact met ons op via het **ONDERSTAANDE!** nummer van de Fraude Helpdesk: [+31623340718](tel:+31623340718)

Groet, SNS.



politie.nl

HELPDESKFRAUDE



Slachtoffer wordt gebeld

1. De fraudeur doet zich voor als medewerker - 'security expert' of 'technician' - van een softwarebedrijf, zoals Microsoft.
2. De fraudeur laat het slachtoffer geloven dat er problemen op de computer zijn ontdekt (bijvoorbeeld virussen, of verouderde software).



Slachtoffer belt zelf

1. Het slachtoffer zoekt het telefoonnummer van een helpdesk en komt hierbij op een nagebootste, criminele website die lijkt op de echte website.
2. De fraudeur doet zich voor als medewerker van het bedrijf en vraagt het slachtoffer wat het probleem is.



Slachtoffer krijgt pop-up melding

1. Het slachtoffer krijgt een pop-up te zien op zijn/haar beeldscherm met hierin de boodschap dat de computer is geïnfecteerd met een 'virus'.
2. Het slachtoffer wordt gevraagd een vaak Nederlands telefoonnummer te bellen.



3. De fraudeur zegt het probleem (tegen betaling) te kunnen oplossen.

Om het probleem op te lossen moet het slachtoffer software installeren. De fraudeur kan met deze software de computer van het slachtoffer besturen, en zelfs proberen om geld over te maken via internetbankieren.



politie.nl

HULPVRAAGFRAUDE

Ook wel Whatsappfraude, vriend-in-noodfraude of betaalverzoekfraude genoemd



Wat is hulpvraagfraude?

- Fraudeurs doen een (soms overtuigend) verhaal
- Met als doel het verkrijgen van een betaling
- Doen alsof
- Vaak via Whatsapp, Facebook of SMS

Kapotte telefoon?



politie.nl



politie.nl

Facebook marketplace

- Komt ook veel voor
- In diverse vormen
- Verkoop en aankoop



Hoe kan ik hulpvraagfraude voorkomen?

- Codewoord afspreken
- Niet zomaar in gesprek gaan na afstemming
- Geldafspraken vooraf maken



NEPAGENTEN

Handelswijze

- Vaak eerst telefonisch
- Komen dan aan de deur
- Vertellen dan over een risico op inbraak

Kenmerken:

- Dragen (vergelijkbare) kleding
- Vervalst legitimatiebewijs
- Links is oud (geldig tot eind 2025); rechts is nieuw



politie.nl

Hoe zit het met legitimeren?

Bij politieambtenaren.

- Wanneer 'in burger'; altijd!
- Wanneer geüniformeerd; op verzoek
- Marechaussee; zelfde regels!



Koninklijke Marechaussee



politie.nl

Wat kun je doen?

Als je het niet vertrouwt.

Wanneer aan de telefoon:

- Hang op en bel 0900-8844

Aan de deur:

- Staat er een 'agent' voor je deur; vraag door!
- Bel 112 als je het niet vertrouwt



politie.nl

PHISHING

Wat is Phishing?

Het 'vissen' naar informatie

Diverse voorbeelden

- Valse Factuur
- DHL / PostNL / Andere bezorgdiensten
- Google Docs
- PayPal
- Dropbox
- Belastingdienst
- Ongebruikelijke Activiteit

In 7 vragen duidelijkheid over een e-mail

- Ja**
- Heeft de e-mail een persoonlijke aanhef?
 - Lijkt de e-mail foutloos geschreven?
 - Bent u klant bij het genoemde bedrijf?
 - Is de e-mail verstuurd vanuit een e-mailadres van het bedrijf zelf? (@naambedrijf.nl)
 - Is de toon van de e-mail vriendelijk en krijgt u voldoende tijd om te reageren?
 - Verwijst de e-mail naar een betrouwbare website?
(Plaats uw muis boven de link zonder te klikken.
Werkt u met een tablet? Houd dan de link langer ingedrukt)
- Ja**
- Wat zegt uw gevoel? Is de e-mail echt?



Betrouwbaar?

Van: icscreditcard@marketing.icscards.nl
Datum: maandag 1 oktober 2017 12:01
Aan: [REDACTED]strik@ziggo.nl
Onderwerp: Wijziging van de spaarrente op uw card

Bekijk de webversie



Wijziging van de spaarrente op uw Card

Geachte mevrouw Strik,

Bij een positief saldo van € 500,- of meer op uw ABN AMRO Creditcard ontvangt u spaarrente over het totale positieve saldo. Per 15 oktober 2017 wordt de spaarrente die van toepassing is op uw Card gewijzigd van 0,3% naar 0,1% effectief op jaarbasis. Het maximale positieve saldo waarover wij rente vergoeden is € 1.000.000.

Hoe kunt u sparen op uw Card?

- Maak het gewenste bedrag over naar uw Card onder vermelding van alleen uw ICS klantnummer. Uw ICS klantnummer vindt u bovenaan de pagina in Creditcard Online op www.icscards.nl/abnamro en op uw rekeningoverzicht.
- Als het spaarsaldo op uw Card € 500,- of meer bedraagt, ontvangt u automatisch spaarrente. De overboekingen en uw spaarrente worden elke maand op uw rekeningoverzicht vermeld.

Heeft u vragen?

Neem dan per e-mail contact met ons op via service@icscards.nl. Als u het niet eens bent met de wijzigingen in het rentepercentage, dan kunt u uw ABN AMRO Credit Card opzeggen. Hiervoor verwijzen we u naar de Algemene Voorwaarden.

[Meer informatie over sparen en de Algemene Voorwaarden](#)

Met vriendelijke groet,
International Card Services BV



mogelijk

Uw ABN AMRO Credit Card wordt uitgegeven door International Card Services BV (ICS).

Let op! Ga voorzichtig om met uw persoonlijke gegevens. Medewerkers van ICS zullen nooit naar uw gebruikersnaam, wachtwoord en/of pincode vragen. Niet via e-mail, telefoon of op welke andere manier dan ook.



politie.nl

Van: info@uwvernieuwde.nl
Datum: 05/02/2018 12:25
Aan: francie. [REDACTED]@gmail.com
Onderwerp: Introductie vernieuwde bankieren



Introductie vernieuwde mobiel bankieren

Geachte ING Rekeninghouder,

Als klant van de ING wilt u duidelijk en tijdig geïnformeerd worden over veranderingen over onze diensten en producten. We brengen u graag op de hoogte van onze nieuwste ontwikkelingen.

Op basis van feedback van onze klanten ontwikkelen we steeds nieuwe en betere beveiligingssoftware voor het internet bankieren. Door altijd gebruik te maken van de meest recente versie, ervaart u het gemak van de nieuwste functionaliteiten en weet u zeker dat u voldoet aan de laatste veiligheidsstandaarden.

De ING spendeert veel tijd aan het beveiligen van mijn ING, recent heeft de ING een nieuwe beveiligingsupdate ontwikkeld. Naar aanleiding hiervan dient uw rekening geüpdate te worden. Op dit moment maakt u nog geen gebruik van onze vernieuwde omgeving.

Wij betreuen dit omdat u nu niet volop van ons systeem gebruik kunt maken. Momenteel maken we al verschillende stappen om de nieuwe omgeving volledig naar de consument te brengen, zoals met de nieuwe ING Mobiel Bankieren app, die momenteel voor iedereen beschikbaar is. Op dit moment willen wij uw Mijn ING omzetten naar onze nieuwe beveiligde omgeving.

Mobiel Bankieren

Gemak en veiligheid gaan goed hand in hand. Dat merkt u in de nieuwste versie van de Mobiel Bankieren app. Inloggen zit u letterlijk in de vingers. Als u dat wilt, logt u in en betaalt u met uw vingerafdruk. Snel en simpel. Zoals een overboeking doen, betalen met IDEAL, een beleggingsorder plaatsen en instellingen wijzigen. Zo gaat bankieren in de app nog sneller en eenvoudiger.

We vragen u daarom om uw gegevens te verifiëren, zodra uw gegevens geverifieerd zijn maakt uw automatisch gebruik van onze verbeterde software.

[Mijn ING Online bijwerken >](#)

Voordelen van de vernieuwde beveiligingsupdate

De vernieuwde beveiligingsupdate beschikt over verschillende, nieuwe functies waaronder een beveiliging tegen skimming (fraude), meer controle om misbruik van betaalpassen tegen te gaan en zelfs een nieuw systeem die kansen op storingen bijna niet meer mogelijk maakt.

Voordelen beveiligingsupdate:

- Vernieuwde beveiliging tegen skimming
- Meer controle door ING personeel
- Versnelde mobiel bankieren koppeling

Let op: u dient uw Mijn ING binnen ontvangst van deze mail te updaten. Anders worden uw rekeningen beperkt uit veiligheids-overwegingen.

Annet van der Hoek
Directeur klantenservice



Nee



politie.nl

& Verder

- Niet zomaar op linkjes klikken
- Laat bij twijfel iemand meekijken

Voorbeeld: bekeuring gekregen?

U ontvangt **enkel per post** een brief van het CJIB

U ontvangt geen mail

U ontvangt geen sms / telefoon

U ontvangt geen Whatsapp

TOCH OPGELICHT?

Zelf doen

- Bankpassen en andere bankzaken
- Logingegevens wijzigen
- Melding maken bij de bank
- Valse mail melden

Aangifte bij de politie

- Verzamel bewijs!

Denk aan chats, facturen, printscreens en bankafschriften

- (Online) aangifte doen
- Bel voor advies 0900-8844



politie.nl

CONTACT MET DE POLITIE

Spoed 112

voor doven en slechthorenden

0800 – 8112

Geen spoed, wel politie?

0900 – 8844

voor doven en slechthorenden

0900 – 1844

Informatie en aangifte doen

0900 – 8844

voor doven en slechthorenden

0900 – 1844

Opsporingstiplijn

0800 – 6070

Meld Misdaad Anoniem

0800 – 7000

geen onderdeel van de politie

politie.nl

Te vinden op sociale media



politie.nl