

# Veilig Bankieren

Samen sterk tegen online fraude



**B.** bank  
informatie  
punt

# Fraude

**Fraude is wanneer iemand u probeert op te lichten om geld of persoonlijke gegevens van u te stelen. Dit gebeurt vaak via neptelefoontjes, e-mails of berichten die van een bank, bedrijf of de overheid lijken te komen. Twee voorbeelden van fraude zijn phishing en bankhelpdeskfraude.**



## Wat is phishing?

Phishing is een vorm van fraude. U krijgt dan een bericht via e-mail, sms of WhatsApp. Daarin staat dat u snel iets moet doen, zoals op een link klikken of uw inloggegevens invullen. Maar dat bericht is nep – en is bedoeld om uw gegevens of geld te stelen.



## Wat is bankhelpdeskfraude?

Bankhelpdeskfraude is een vorm van fraude. Zogenaamde bankmedewerkers doen zich voor als mensen die bij de bank werken. Ze klinken vaak heel overtuigend en zeggen dat er iets mis is met uw rekening. Ze vragen u dan om snel iets te doen – bijvoorbeeld uw betaalpas af te geven, geld over te maken of in te loggen op een speciale website. Trap er niet in: het is een kletspraatje bedoeld om u op te lichten.

# Dit kunt u zelf doen:



## Tegen phishing

- Klik nooit zomaar op een link in een e-mail, SMS of WhatsApp bericht.
- Controleer altijd wie de afzender is.
- Log nooit in via zo'n link.
- Twijfelt u? Ga zelf naar de officiële website van de organisatie.
- Verwijder het bericht of meld het bij de Fraudehelpdesk.



## Tegen bankhelpdeskfraude

- Hang op en bel zelf uw bank via het officiële nummer of de bank app.
- Maak nooit zomaar geld over. Een bank vraagt dat nooit.
- Geef nooit uw betaalkpas, pincode, inlogcodes, wachtwoord of andere beveiligingscodes aan iemand.
- Installeer geen programma's op uw apparaat waarmee iemand op afstand mee kan kijken.



## Wat een bank nooit zal vragen

Fraudeurs passen hun werkwijze steeds aan, maar weet dat banken nooit vragen...

- naar uw pincode, inlogcodes, wachtwoorden of andere beveiligingscodes
- om geld over te maken naar een andere rekening
- om uw limiet op uw betaalrekening en betaalpas te verhogen
- om uw betaalpas of e.identifier/scanner/reader aan iemand mee te geven of op te sturen
- of ze op afstand uw computer mogen 'overnemen'.

**Let op:** een bank stuurt nooit een link via SMS, WhatsApp of e-mail waarmee u moet inloggen.





## Wat doen banken voor uw veiligheid?

Banken doen er alles aan om u veilig te laten bankieren! Hier zijn een aantal maatregelen van de bank voor uw veiligheid:

- Alle gegevens bij digitaal bankieren worden beveiligd en er kan niemand zomaar bij.
- Bij vermoeden van fraude worden rekeningen en betaalpassen geblokkeerd door de bank.
- Banken nemen maatregelen tegen websites en e-mails die zich voordoen als een bank en houden afwijkende betalingen in de gaten.
- Als het apparaat voor internet of mobiel bankieren een bepaalde tijd niet wordt gebruikt, dan wordt u automatisch uitgelogd.
- Als u een groot bedrag wilt pinnen, opnemen of overboeken, dan geldt bij een limietverhoging een wachttijd van 4 uur.

**"Toen ik werd gebeld met een heel verhaal over mijn geld, voelde ik twijfels. Dit is misschien niet pluis. Ik hing gewoon op. Liever onbeleefd dan ergens intrappen."**



## Bescherm uw gegevens

Veilig bankieren doen we samen. Wat kunt u nog meer doen om uzelf tegen fraude te beschermen?

- Bescherm uw codes: door inloggegevens geheim te houden.
- Bescherm uw pas: door deze pas bij u te houden en niet uit te lenen.
- Bekijk uw afschrijvingen: controleer uw bankrekening regelmatig.
- Beveilig uw apparatuur: door regelmatig updates uit te voeren.

Bij twijfel of vragen, **bel uw bank!** Bij voorkeur via de bank app.



## Wat te doen na fraude?

Schaam u vooral niet en bespreek het met uw naasten, vrienden of buren. Iedereen kan namelijk slachtoffer worden. Als u slachtoffer bent geworden van online fraude kunt het beste het volgende doen:

- Meld fraude direct bij uw bank
- Doe aangifte bij de politie
- Meld fraude bij de Fraudehelpdesk
- Neem contact met Slachtofferhulp Nederland (indien u daar behoefte aan hebt)



## Contactgegevens van uw bank



**ABN AMRO**

[www.abnamro.nl](http://www.abnamro.nl)

**0900 0024**

**088 226 26 12**

(zonder keuzemenu)



**ING**

[www.ing.nl](http://www.ing.nl)

**020 228 88 88**

**020 228 88 35**

(Samen Digitaal lijn)



**Rabobank**

[www.rabobank.nl](http://www.rabobank.nl)

**088 722 66 00**



**ASN Bank**

[www.asnbank.nl](http://www.asnbank.nl)

**070 365 93 35**



## Handige websites

Bezoek deze websites voor tips over veilig online bankieren:

- [www.fraudehelpdesk.nl](http://www.fraudehelpdesk.nl)
- [www.slachtofferhulp.nl](http://www.slachtofferhulp.nl)
- [www.veiligbankieren.nl](http://www.veiligbankieren.nl)
- [www.veiliginternetten.nl](http://www.veiliginternetten.nl)
- [www.voorkomfraude.nl](http://www.voorkomfraude.nl)



## Extra hulp bij bankzaken



Hulp nodig bij dagelijkse bankzaken? Of helpt u er iemand mee? Ga naar [www.bankinformatiepunt.nl](http://www.bankinformatiepunt.nl) voor meer informatie.



Moeite met digitale bankzaken? Ervaren medewerkers van de DigiHulplijn staan (gratis) voor u klaar om u te helpen.

# Veilig bankieren, dat kan iedereen!



## Vijf tips om te onthouden:

- Vertrouw op uw gevoel!
- Controleer altijd de afzender
- Klik nooit zomaar op een link
- De bank vraagt u nooit om geld over te maken
- Leen nooit uw betaalkas en pincode uit

Wilt u oefenen met het  
herkennen van fraude?  
Scan de QR-code voor  
korte interactieve video's  
over verschillende  
fraudevormen



Lukt het scannen niet? Zoek dan  
op internet naar 'CCV Echt of nep'