

# B. bank informatie punt

## Veilig Bankieren

Samen sterk tegen online fraude

Welkom!





## Introductievideo: maak het oplichters niet gemakkelijk



# Introductie programma Toegankelijk Bankieren

Wat hebben de banken tot nu toe gedaan en waar zijn zij mee bezig?

Banken verbeter(d)en hun **dienstverlening en bereikbaarheid**:



**Communicatie**



Over hulp dichtbij, telefoonnummers etc.



**Hulp dichtbij**



Lokaal palet aan hulp en persoonlijk contact  
(sommige banken bieden ook hulp dichtbij huis)



**Telefonische ondersteuning**



Verbetering van bereikbaarheid\*



**Toegankelijke websites en mobiele apps**



Producten worden aangepast op  
toegankelijkheid



**Hulpmiddelen / Educatie**



Educatie bankmedewerkers op  
toegankelijkheid, gratis workshops door heel  
het land.

\*De ING heeft een speciaal 'Samen Digitaal' nummer, ABN Amro een 'Hulp bij bankzaken' nummer en Rabobank een 'Samen Bankieren' nummer.

# Het programma van de workshop: veilig bankieren

- ❖ Introductievideo
- ❖ Kennismaken: wat wilt u vandaag leren?
- ❖ Activiteit: kwartet spel Veilig Bankieren
- ❖ Het behandelen van de onderwerpen over Veilig Bankieren
- ❖ Afronding



# B. bank informatie punt

## Veilig Bankieren

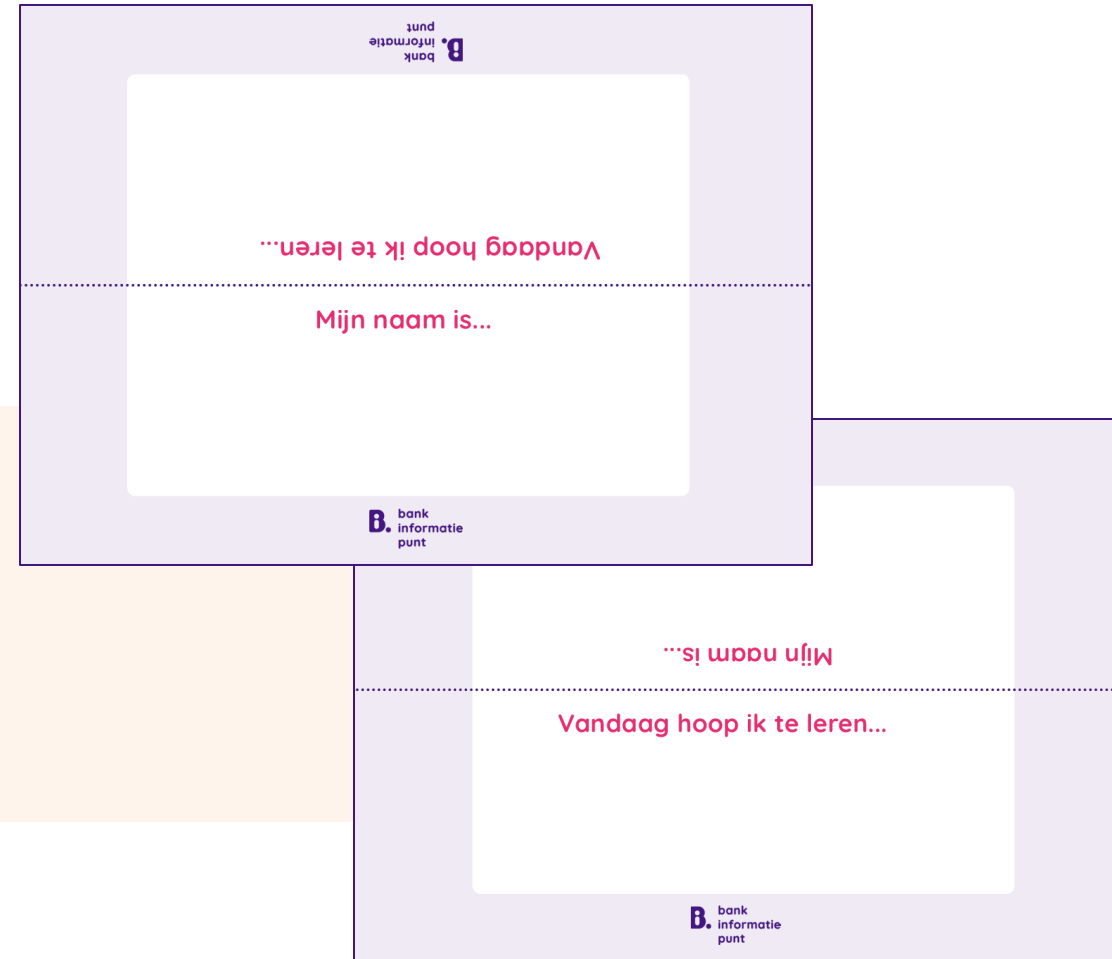
Samen sterk tegen online fraude



# Veilig bankieren: **laten we kennismaken**

Laten we starten met een **korte kennismaking**.

- Schrijf uw **naam** op het naambordje
- **Vouw** deze dubbel
- Schrijf op de achterkant wat u **vandaag hoopt te leren**
- Dit **bespreken** we daarna kort



# B. bank informatie punt

## Veilig Bankieren

Aan de slag met de informatie!



# Veilig bankieren: de thema's

Welke thema's heeft het **kwartetspel**?

1. Maatregelen banken
2. Zelf doen
3. Uw bank vraagt u nooit...
4. Fraude herkennen
5. Nepberichten
6. Niet doen
7. Na fraude

*Vandaag wisselen we af tussen inhoud en persoonlijke verhalen, zodat we ook van elkaar kunnen leren!*



# B. bank informatie punt

## Veilig Bankieren

Tijd voor kwartet!



# Veilig bankieren: **het kwartetspel**

 Uw bank  
vraagt u nooit...



1. ... om uw beveiligingscodes
2. ... om geld over te maken
3. ... om uw betaalpas aan iemand mee te geven
4. ... om uw computer over te nemen

→ Hier vindt u het **thema**, blijf deze ook herhalen tijdens het spel

→ Hier vindt u de **namen van de kaarten** die u kunt verzamelen



*U mag om de beurt vragen of iemand van een bepaald thema een kaart heeft, zo lopen we alle kaarten langs*

# Veilig bankieren: **het kwartetspel**

**B.** bank  
informatie  
punt

**B.** bank  
informatie  
punt

Instructies

**Veilig Bankieren**  
**Kwartet**



Tijdens het kwartetspel kunt u **persoonlijke verhalen delen**.  
Zo **leren we van elkaar**.

Bedenk over **welke onderwerpen u meer wilt weten**.  
Dan behandelen we die straks!

# B. bank informatie punt

## Veilig Bankieren

Veel plezier!



# Veilig bankieren: onderwerpen

**Zelf doen:**  
zo beschermt u uw gegevens



**Nepberichten:**  
phishing



**Maatregelen banken:**  
wat banken doen voor uw veiligheid



**Niet doen:**  
bankhelpdeskfraude



**Uw bank vraagt u nooit..**



**Na fraude:**  
wat als u slachtoffer bent geworden?



**Fraude herkennen:**  
herken en voorkom fraude



**Welke informatie neemt u  
mee naar huis?**



# B. bank informatie punt

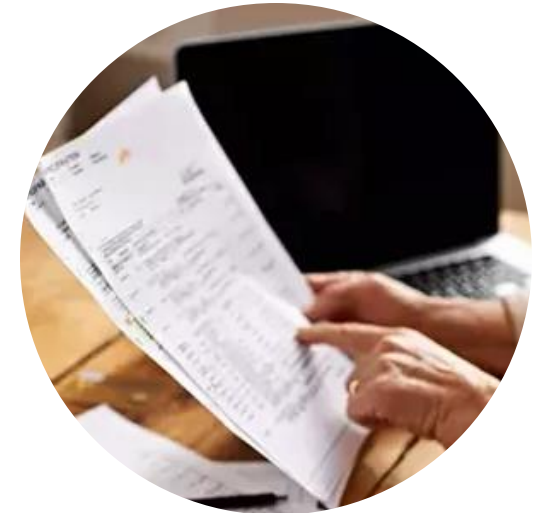
## Veiligheid en bankieren

- Zo beschermt u uw gegevens
- Wat doen banken voor uw veiligheid?
- Een bank vraagt u nooit...



# Zelf doen: zo beschermt u uw gegevens

- 
- 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.



## Wist u dat?

Regelmatige **updates** ervoor zorgen dat uw apparaat over de nieuwste beveiliging beschikt?

**Tip:** zet automatische updates aan

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

## Ook handig: tweestapsverificatie

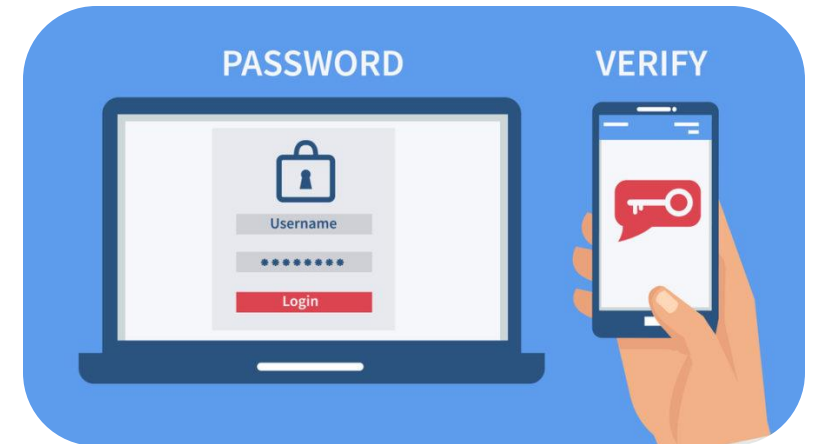
### Wat is het?

U logt in met twee stappen

Bijvoorbeeld: uw wachtwoord én uw vingerafdruk

### Waarom?

- Extra beveiliging
- Minder kans op misbruik



### Zo werkt het

U gebruikt altijd twee van deze:



**Iets wat u weet** → Wachtwoord of pincode



**Iets wat u heeft** → Telefoon of bankpas



**Iets wat u bent** → Vingerafdruk of gezichtsherkenning

# Tweestapsverificatie: in de praktijk

## Zo stelt u dit in

- 1 Ga naar instellingen van de app of website
- 2 Zoek naar 'beveiliging' of 'inloggen'
- 3 Zet tweestapsverificatie aan
- 4 Kies hoe u wilt bevestigen: code of app

## Daarna bij het inloggen:

- Voert u uw wachtwoord in
- Bevestig u met een code of melding



### Microsoft Authenticator:

Een app die codes of meldingen ontvangt om in te loggen

# Tweestapsverificatie: in de praktijk

## Waar ziet u dit in de praktijk?

### Online betalen

U bevestigt de betaling met een extra stap, zoals de bank app of een code

### Internetbankieren op de computer

U logt in en bevestigt met de bank app of een inlogapparaatje

### Betalen aan de kassa

U gebruikt uw pinpas en voert uw pincode in

### Mobiel bankieren

U logt in met een code en bevestigt met uw vingerafdruk of gezicht

# Maatregelen banken: wat doen banken voor uw veiligheid?

## Banken beschermen uw gegevens



Alle gegevens bij digitaal bankieren worden beveiligd en er kan niemand zomaar bij.

## Fraude voorkomen



Bij vermoeden van fraude worden rekeningen en betaalpassen geblokkeerd door de bank.

## Aanpak bankfraude



Banken nemen maatregelen tegen websites en e-mails die zich voordoen als een bank, en houdt afwijkende betalingen in de gaten.

## Automatisch uitloggen



Als het apparaat voor internet of mobiel bankieren een bepaalde tijd niet wordt gebruikt, dan wordt u automatisch uitgelogd.

## Tijdslot bij aanpassen van limiet



Als u een groot bedrag wilt overboeken, dan geldt bij een limietverhoging een wachttijd van 4 uur.



# Uw bank vraagt u nooit...

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

- ⊘ 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.dentifier/scanner/reader aan iemand mee te geven of op te sturen
- ⊘ of ze op afstand uw computer mogen 'overnemen'



## **En weet...**

**Banken sturen nooit een SMS, WhatsApp of e-mail met een directe link naar een bankomgeving.**



Beste klant,

Wij informeren u dat de activatie van uw applicatie verloopt op **20 januari 2026**. Om ononderbroken gebruik te blijven maken van online bankieren, dient u uw app tijdig te heractiveren.

Voor heractivatie kunt u **op de volgende link klikken** en de instructies volgen.

[\[Heractivatie starten\]](#)

Met vriendelijke groet,  
**ABN AMRO**

# B. bank informatie punt

## Herken en voorkom fraude

- Phishing
- Bankhelpdeskfraude



# Fraude herkennen: **herken en voorkom fraude**



**Fraude draait om misleiding!**



**Online oplichting wordt steeds slimmer!**



**Herken fraude aan uw eigen emoties!**



**Wij helpen u met tips om fraude te herkennen en te voorkomen!**



# Nepberichten: wat is phishing?

## ● 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 bedoeld om uw gegevens of geld te stelen.



Beste klant,

Uw pakje kon niet geleverd worden op 07-23-2024 omdat er geen douanerechten betaald werden (3.75 €). volg de instructies op.

Dit zijn de details van uw pakket

Volg nummer : [19836386000197](#)

Verwachte levering tussen : 23-07-2024 en 25-07-2024

- Om de verzending van een pakket te bevestigen, [klik hier](#)
- U ontvangt een e-mail of SMS wanneer uw pakket op het thuisadres aankomt. Vanaf de datum van beschikbaarheid heeft u 8 dagen de tijd om het pakket af te halen. Op het moment van annulering zal u worden gevraagd om een identificatiebewijs.

Dank u voor uw vertrouwen,

**Bevestigen dat een pakket is verzonden**

Groeten,  
DHL Klantenservice.

# Phishing: voorbeelden

“Uw bankrekening wordt vandaag geblokkeerd. Klik hier om uw betaling te doen”

- U moet **snel** op een link klikken
- Er wordt **druk** gezet

“Afzender: noreply1@email.rabobank.nl”

- Het **e-mailadres (afzender) wijkt net iets** af van het echte e-mailadres
- 1 letter of cijfer kan het verschil zijn



“Stuur een kopie van uw ID om uw account te bevestigen”

- Er wordt gevraagd om **persoonlijke gegevens**



*Vertrouw op uw onderbuikgevoel. Twijfelt u? Klik niet. Moet het snel? Lijkt de afzender vreemd? Bel dan zelf uw bank.*

# Phishing: **wat kunt u zelf doen?**

**Check altijd eerst de afzender (het e-mailadres, of het nummer)**

**Klik nooit zomaar op een onbekende link**

**Deel nooit vertrouwelijke gegevens met onbekende personen**

**Bescherm eigen gegevens op social media, door dit op privé te zetten**

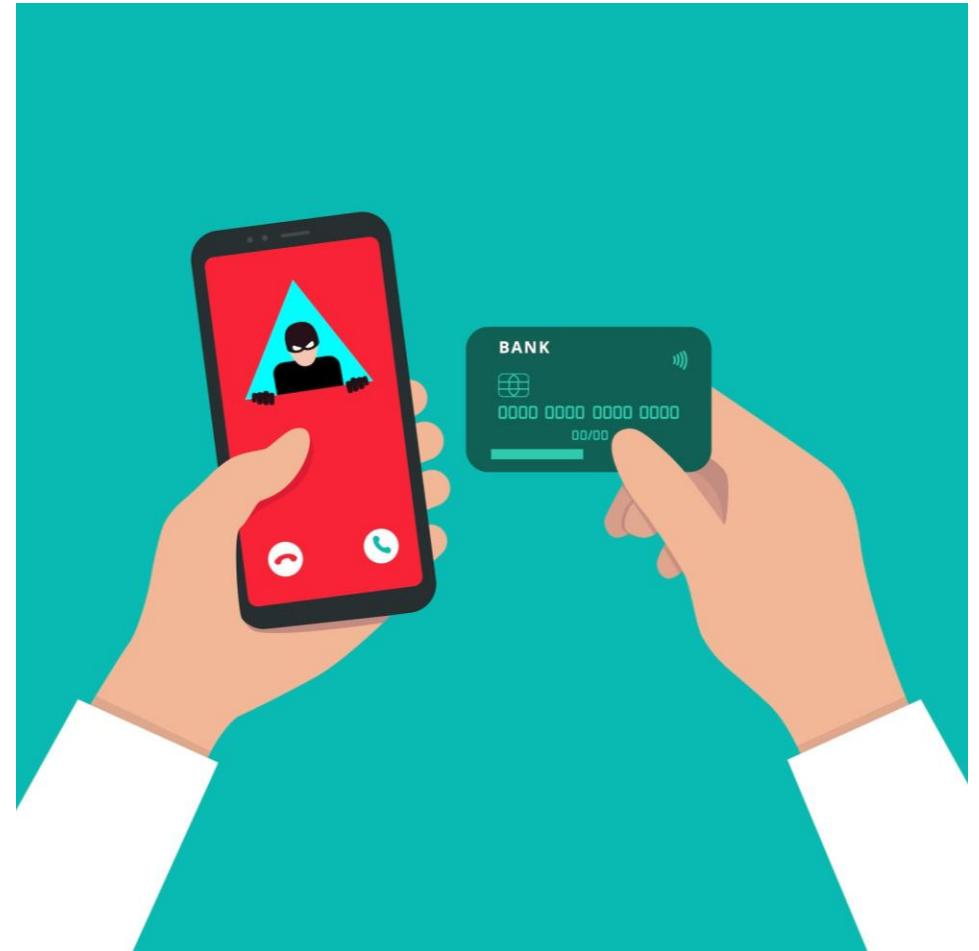
**Bij twijfel, altijd het officiële telefoonnummer van uw bank of instantie bellen**



# Wat is bankhelpdeskfraude?

## ● Bankhelpdeskfraude:

Bij bankhelpdeskfraude **doen** criminelen **alsof** ze van uw bank of een andere bekende instantie zijn. Vaak klinkt het heel **dringend**. Ze willen u **bang maken** zodat u snel doet wat zij zeggen. Zo proberen ze uw geld of gegevens te **stelen**.



# Bankhelpdeskfraude: voorbeelden



“Ik ben van de bank. Uw geld is in gevaar.”

- Er wordt **angst** gebruikt
- U moet **snel** handelen



“Het is belangrijk om uw geld zo snel mogelijk over te maken naar een veilige rekening, om het veilig te stellen”

- U moet zelf **geld overmaken**



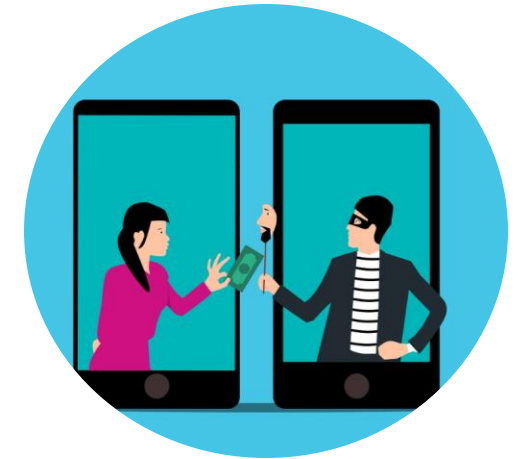
“Ik kom uw betaalpas ophalen”

- U moet uw **pas afgeven**



“Installeer dit programma zodat ik kan helpen”

- Ze willen uw **apparaat (op afstand) overnemen**
- U moet iets **downloaden** (zoals Anydesk, Teamviewer of LogMeIn)



## Let op

De oplichter **wint uw vertrouwen** en vraagt daarna om **actie**. U moet helemaal niks. Hang op en **bel zelf uw bank**. De bank vindt het niet erg als u (te) voorzichtig bent.

# Niet doen:

## wat moet u niet doen bij bankhelpdeskfraude?

**Ga niet het gesprek aan.**  
Hang op en bel uw bank



Krijgt u een onbekend telefoontje? Hang op en bel zelf uw bank.

**Maak nooit zomaar geld over**



Een bank vraagt u nooit om geld over te maken.

**Leen nooit uw betaalpas uit**



Geef nooit uw betaalpas en pincode aan iemand mee.

**Deel nooit uw gegevens.**  
Houdt uw gegevens geheim



Geef nooit persoonlijke gegevens weg zoals inlogcodes, wachtwoorden, pincode etc.

**Geef nooit uw apparaten uit handen.**  
Houdt zelf controle over uw apparaten



Een bank vraagt u nooit om een programma te installeren, waarmee zij op afstand uw computer, tablet of smartphone kunnen bedienen.

# B. bank informatie punt

## Contact met uw bank

Iemand spreken van uw eigen bank?



# Liever iemand spreken?

 Vindt u het prettiger om iemand persoonlijk te spreken? Dat kan!

**Tip:** bel vanuit de bank app, zo weet de bankmedewerker direct wie hij/zij aan de telefoon heeft



ABN AMRO  
www.abnamro.nl  
0900 0024  
088 226 26 12  
(zonder keuzemenu)

ING  
www.ing.nl  
020 228 88 88  
020 228 88 35  
(Samen Digitaal)

Rabobank  
www.rabobank.nl  
088 722 66 00  
(Samen Bankieren)

ASN  
www.asnbank.nl  
070 356 93 35

 Of vind een locatie in uw buurt. Op onze website staan locaties van de banken:  
<https://bankinformatiepunt.nl/locaties-in-de-buurt/>

**Voor al uw digitale vragen is er daarnaast dit handige gratis nummer:**



# B. bank informatie punt

## Wat als u slachtoffer bent geworden?

- Schaam u vooral niet
- Contact belangrijke instanties



# Na fraude: ik ben slachtoffer van online fraude, wat nu?



**Schaam u vooral niet** en bespreek het met uw naasten, vrienden of burens.  
Iedereen kan namelijk slachtoffer worden.

Bent u slachtoffer geworden van online fraude?

Wij vertellen u wat u het beste kunt doen!

## Na fraude: ik ben slachtoffer van online fraude, wat nu?

### Meld fraude direct bij uw bank



Dit kan via de bank app, telefonisch, per e-mail. Of zoek op de website naar 'fraude melden'.

### Doe aangifte bij de politie



Doe aangifte bij de politie via [www.politie.nl](https://www.politie.nl), of bel naar 0900-8844.

### Meld fraude bij de Fraudehelpdesk



Benader de Fraudehelpdesk voor gratis advies om schade te beperken, of fraude te voorkomen. Ga naar [www.fraudehelpdesk.nl](https://www.fraudehelpdesk.nl) of bel 088-786 73 72.

### Neem contact op met Slachtofferhulp



Als u daar behoefte aan heeft, neem contact op met Slachtofferhulp Nederland voor emotionele, praktische en juridische hulp.

# B. bank informatie punt

## Tot slot

Welke informatie neemt u mee naar huis?



## 1 Vertrouw op uw gevoel!

Heeft u het gevoel dat iets niet klopt? Dan is dat waarschijnlijk ook zo.

**Stop** dan direct en ga voor uzelf de bekende weg:

- Belt uw bank dat uw rekening in “gevaar” is? → Bel dan het nummer dat bij u bekend is.
- Ontvangt u een WhatsApp-berichtje van uw dochter die snel geld nodig heeft? → Bel zelf uw dochter.

## 2 Controleer altijd de afzender

## 3 Klik nooit zomaar op een link

## 4 De bank vraagt u nooit om geld over te maken

## 5 Leen nooit uw betaalpas en pincode uit

**Door verhalen en ervaringen te blijven  
delen, leren we van elkaar!**

**Met deze tips kan iedereen veilig  
bankieren!**

**Het doen van digitale bankzaken biedt  
controle over uw rekening.**

**U bent er sneller bij als het misgaat.**

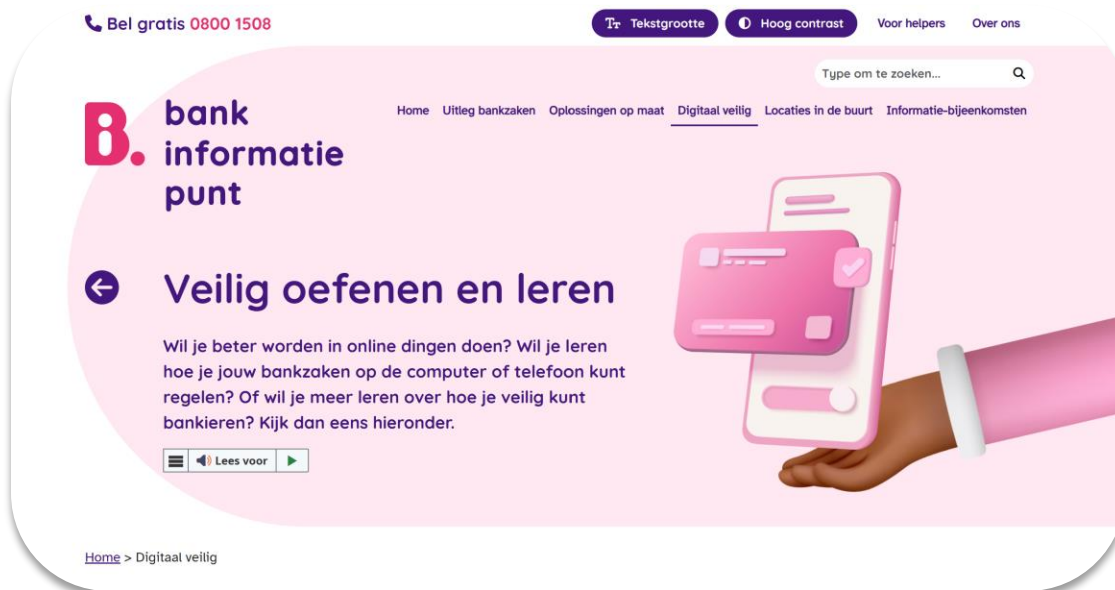
**En u kunt handig een bankmedewerker  
bellen via de app als u onraad voelt.**

**Samen voorkomen we fraude.**

# Veilig bankieren, dat kan iedereen!

Wilt u meer leren over het doen van dagelijkse bankzaken?

Neem een kijkje op [Digitaal veilig - Bankinformatiepunt](#)



# Overzicht van andere handige hulp- en oefenwebsites:

## Digihandig.nl



Voor **digitaal** oefenen

## Steffie.nl



Voor **makkelijke uitleg**  
(ook over andere zaken)

## Oefenen.nl



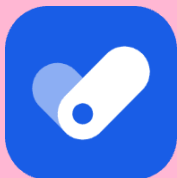
Voor **oefenen** met  
taal, rekenen en  
internetten

## Veiligbankieren.nl



Voor **informatie** over  
fraude en veilig  
bankieren

## checkjelinkje.nl



Voor het **controleren**  
van de veiligheid van  
linkjes en URL's

## Opgelicht.avrotros.nl



Voor **alerts en nieuws**  
over oplichting

## voorkomfraude.nl



Voor het **herkennen**  
**en voorkomen** van  
fraude

**B.** bank  
informatie  
punt

**Bedankt voor uw aandacht.  
Nog vragen? Stel ze gerust!**



ABN·AMRO

asn  bank

ING 



Rabobank