DigiVeiliger

Veilig online bankieren

Inhoudsopgave

Introductie 03

Informatie over veilig online bankieren 04

ABCD'tje 04

Denk goed na voordat je iets deelt 04

VeiligWijzer + stap voor stap 05

Voorbeelden van online oplichting 10

Tips over online veiligheid en bescherming 12

Handige websites 13

Opgelicht? 13

Hulp nodig? 14

Meer leren? 14

Met vertrouwen online 14

Tip 14

Introductie: Veilig online bankieren

In onze digitale wereld is online bankieren niet meer weg te denken. Het gemak van een betaling regelen, je saldo controleren of een overboeking doen: alles is binnen enkele klikken geregeld. Maar helaas zijn ook oplichters actief in deze wereld. Met sluwe trucs proberen ze toegang te krijgen tot je persoonlijke gegevens of geld. Daarom is het belangrijk om te weten hoe je jezelf kunt beschermen.

Dit boekje geeft meer informatie over:

- veilig online bankieren;
- hoe je verdachte berichten en telefoontjes kunt controleren;
- voorbeelden van oplichtingsmails en sms'jes;
- tips over online oplichting en veiligheid;
- handige websites;
- wat je moet doen als je toch bent opgelicht.

Blader door dit boekje en ontdek hoe je met een paar simpele maatregelen een stuk veiliger online kunt bankieren.

Informatie over veilig online bankieren

Bij het online bankieren (internetbankieren), kun je via internet bankzaken regelen. Zo kun je saldo controleren, rekeningen betalen of geld op je spaarrekening zetten.

Online bankieren heeft verschillende voordelen:

- Je hebt toegang tot een actueel overzicht van je rekening.
- Je kunt altijd en overal waar je bent geld overmaken.
- Je kunt steeds meer online regelen, zoals een nieuwe bankpas vragen.

ABCD'tje

Onthoud het ABCD'tje om zo veilig mogelijk online te zijn.

A	Alert	Wees alert, want er zijn oplichters die je op verschillende manieren kunnen benaderen en blijf op de hoogte van oplichtingstrucs
B	Bescherm	Bescherm je apparaten. Zorg ervoor dat ze goed beveiligd zijn, up-to-date zijn en dat je sterke wachtwoorden gebruikt
C	Controleer	Controleer altijd de afzender, de inhoud, de links en voer niet zomaar een actie uit
D	Deel	Deel verdachte berichten of links met de organisatie en praat hierover met bekenden. Twijfel je of het betrouwbaar is? Neem dan contact op met de organisatie

Denk goed na voordat je iets deelt!

Vraag jezelf altijd: *Zou ik deze informatie ook in het echte leven delen?* Zou je zomaar je pincode of adres aan een vreemde geven? Doe dat online ook niet. Gebruik je gezond verstand en wees kritisch op wat je online tegenkomt.

VEILIGWIJZER

Online bankieren

1. Controleer de afzender

7. Zeker? Ga door. Twijfel? Neem contact op via officiële kanalen

2. Controleer de inhoud

6. Deel geen persoonlijke gegevens

3. Let op emotionele trucs

5. Open geen verdachte bijlagen

4. Controleer websitelinks en QR-codes

1. Controleer de afzender

E-mail

Ken je de afzender?

- Controleer of het een e-mail van een bekende is.

Ken je de afzender niet?

- Kijk naar het deel achter het apenstaartje (@).
- Let op vreemde tekens, een vreemde naam of een bedrijfsnaam die verkeerd is gespeld (bijvoorbeeld info@rab0bank.nl).
- Vergelijk het e-mailadres met het e-mailadres op de officiële website van het bedrijf of met eerdere mails die je van het bedrijf hebt ontvangen.

Sms, WhatsApp of bellen

Ken je het nummer?

- Controleer of het telefoonnummer van een bekende is.

Ken je het nummer niet?

- Controleer het nummer op de officiële website van het bedrijf.

Let op! *Oplichters kunnen een bestaand nummer, zoals dat van je bank, in beeld laten verschijnen. Vaak gebruiken ze ook een naam van een medewerker. Hang op, bel zelf je bank en vraag naar de medewerker.*

Is de afzender iemand die zegt een bekende te zijn?

- Bel dan het 'oude' nummer van hem of haar om dit te controleren.

2. Controleer de inhoud

Let op de aanhef.

- Bekende afzenders of organisaties gebruiken vaak je naam.
- Wees extra voorzichtig bij een algemene aanhef, zoals ‘Geachte heer/mevrouw’ of ‘Beste klant’.

Let op! *Oplichters kunnen je naam en andere persoonlijke gegevens al hebben. Vertrouw hier niet zomaar op!*

Kijk naar het taalgebruik.

- Let op taal- en spelfouten of vreemde zinnen.

Gebruik je gezond verstand.

- Verwacht je dit bericht? Is het logisch dat je het ontvangt?
- Is het te mooi om waar te zijn? Vaak is het dat ook.
- Vraagt iemand om geld? Let goed op, ook bij bekende afzenders.

3. Let op emotionele trucs

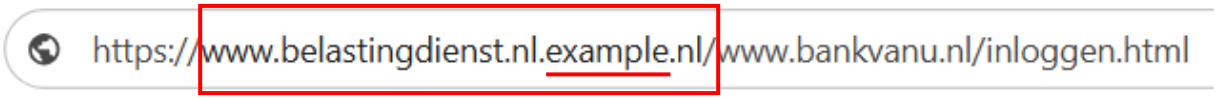
Oplichters spelen met je emoties om je snel te laten reageren, bijvoorbeeld:

Angst	Uw computer heeft een virus. Bel het onderstaande nummer van Microsoft om uw bestanden te redden.
Tijdsdruk	U heeft een openstaande rekening. Betaal binnen 2 dagen, anders zal er een deurwaarder langskomen.
Schuldgevoel	U heeft een verkeerd e-mailadres ingevuld, waardoor wij u niet konden bereiken. Hierdoor wachten wij al geruime tijd totdat u de betaling heeft voldaan.
Hebzucht	De ANWB stelt een noodpakket beschikbaar ter waarde van € 200. Vraag hier gratis uw pakket aan.
Vertrouwen	Uw bank heeft een beveiligingsupdate. Klik hier om deze te installeren en uw account te beschermen tegen oplichters.
Medelijden	Ik moet een rekening betalen, maar ik heb niet genoeg geld. Kun je voorschieten?

4. Controleer websitelinks en QR-codes

Bekijk de website.

- Ga met je muis staan op de link, maar klik hier niet op.*
- Controleer of de link begint met https:// (de ‘s’ moet erbij staan).
- Kijk naar het webadres (domein):
  - dit is het gedeelte tussen https:// en de eerste /
  - kijk naar het deel tussen de laatste twee punten



- Staat de bedrijfsnaam in het domein? Let dan op spelfouten!

Heb je de link geopend?

- Kijk dan of er een slotje (of ander icoon) in de adresbalk staat.

*Bij een QR-code controleer je ook de link voordat je er op tikt. Hoe je dit doet, hangt af van je telefoon. Tik bijvoorbeeld op het pictogram met het rode kader om de volledige link te zien (zie de voorbeelden hieronder).

5. Open geen verdachte bijlagen

Controleer het bestandstype.
De naam van een bijlage eindigt met een punt en drie letters.

- Een **veilige** bijlage eindigt vaak op:
  voor tekstbestanden: .pdf
  voor afbeeldingen: .jpg en .png

6. Deel geen persoonlijke gegevens

Wees voorzichtig met je gegevens.

- Geef **nooit** je pincode, gebruiksnaam, wachtwoord of andere inloggegevens aan iemand die je niet vertrouwt.
- Betrouwbare bedrijven vragen **nooit** om deze persoonlijke gegevens via telefoon, e-mail, sms of WhatsApp.

Bij twijfel: neem contact op met de organisatie.

- Bel het bedrijf om te controleren of de vraag echt is.

Let op! *Oplichters kunnen een website waar je je gegevens moet invullen er heel echt laten uitzien. Controleer altijd goed de link (zie stap 4).*

7. Zeker? Ga door. Twijfel? Neem contact op via officiële kanalen

Heb je alle stappen doorlopen en klopt alles?

- Als alles veilig lijkt kun je verdergaan.

Twijfel je? Neem dan contact op via de officiële kanalen.

- Bel of stuur een e-mail naar het bedrijf om te controleren of het bericht echt is.

Let op! *Soms staan er contactgegevens in het 'verdachte' bericht. Gebruik deze gegevens nooit! Zoek altijd de contactgegevens op via de officiële website van de organisatie.*

Als het bericht nep is:

- Blokkeer het e-mailadres of het telefoonnummer.
- Stuur eventueel het bericht door naar fraudehelpdesk.nl.
- Verwijder het bericht.

Digimail

Controleer uw melding

Rabobank
contact@mijnrabobank.nl

Rabobank

Controleer uw melding

Geachte klant,

Er staat een nieuw bericht voor u klaar in uw beveiligde omgeving. Dit bericht bevat belangrijke updates over uw account. Wij adviseren u het zo spoedig mogelijk te bekijken om volledig op de hoogte te blijven en, indien nodig, tijdig te reageren.

Klik hier om te koppelen

Met vriendelijke groet,
Rabobank

Uitleg voorbeeld

Er staat geen typefout in de naam. Maar de Rabobank stuurt mails met als afzender: @email.rabobank.nl, niet @mijnrabobank.nl. Ook al lijkt de afzender betrouwbaar, controleer altijd de andere stappen!

- In de mail staat een emotionele truc om zo spoedig mogelijk het bericht te bekijken. Zo willen ze dat je snel iets doet.
- Een bank kan mails sturen met informatie. Ze sturen geen mails met links om in te loggen in je persoonlijke omgeving. Log altijd in door zelf naar de website te gaan.
- Er is een standaard aanhef. In **echte** e-mails van de bank word je vaak aangesproken met meneer/mevrouw + je achternaam.
- De opmaak lijkt op een e-mail van de Rabobank: het logo klopt en de kleuren zijn juist. Maar oplichters kunnen mails namaken.

Uitleg voorbeeld

De afzender is een onbekend nummer. Vaak staat bij een sms van de bank wel ABN AMRO, Rabobank, ASN Bank of een andere bank. **Let op!** Oplichters kunnen ook een betrouwbaar nummer overnemen. Controleer altijd de andere stappen.

- Er wordt ingespeeld op emotie: Je wordt bang gemaakt dat iemand heeft geprobeerd veel geld over te maken.
- Het telefoonnummer kan onbetrouwbaar zijn. Zoek daarom altijd het nummer van de bank op via de officiële website.

Uitleg voorbeeld

Op websites, zoals Marktplaats, zijn ook oplichters actief. Ze lokken je eerst uit de Marktplaats-omgeving naar een app, zoals WhatsApp.

Vaak doen ze alsof ze zelf zijn opgelicht of dat er andere problemen zijn waardoor een betaling via de Marktplaats-omgeving niet kan.

De betaal-link klopt niet. Een tikkie begint altijd met: https://tikkie.me/pay.

Tips over online veiligheid en bescherming

Werk je apparaten bij
Zorg ervoor dat je telefoon, computer en alle apps up-to-date zijn. Je hebt dan de nieuwste en veiligste versie.

Gebruik sterke wachtwoorden
Een sterk wachtwoord bestaat uit hoofdletters, kleine letters, cijfers, symbolen en minstens 12 tekens. Gebruik voor elk account een ander wachtwoord.

Wachtwoordmanager
Een wachtwoordmanager is een app op je telefoon en/of computer waarin je wachtwoorden veilig worden opgeslagen. Je hoeft alleen het hoofdwachtwoord te onthouden.

Tweestapsverificatie
Zet tweestapsverificatie aan. Dit biedt extra beveiliging.
Met dit extra slot moet iemand je wachtwoord weten en je telefoon in handen hebben om in te loggen.

Openbare wifi
Gebruik geen gevoelige informatie op openbare wifi, zoals bankieren.

Antivirusprogramma
Bescherm je computer tegen virussen.

Back-up
Maak regelmatig een kopie van belangrijke bestanden.

Scan de QR-codes om de webpagina met tips te bekijken.

Handige websites

fraudehelpdesk.nl
veiliginternetten.nl
politie.nl
checkjelinkje.nl
veiligbankieren.nl
bankinformatiepunt.nl

rabobank.nl/veiligbankieren
abnamro.nl/veiligbankieren

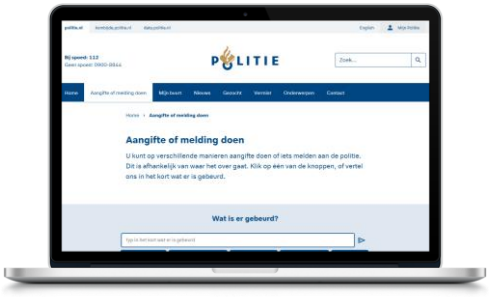
hetccv.nl/tool-cyberweerbaarheid
https://hetccv.nl/hulp-bij-online-criminaliteit/
opgelicht.nl
seniorweb.nl
slachtofferhulp.nl

ing.nl/veiligbankieren
asnbank.nl/veiligbankieren

Opgelicht?

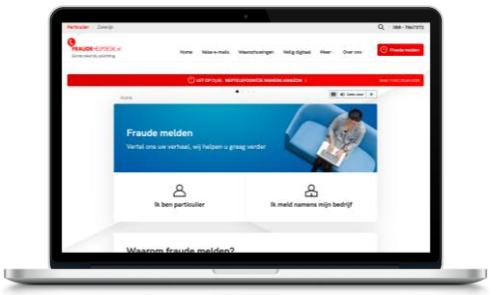
Doe dan aangifte bij de politie.

- Bel 0900-8844
- Ga naar het politiebureau
- Doe online aangifte via: politie.nl/aangifte-of-melding-doen



Meld het bij de Fraudehelpdesk.

- Bel 088-786 73 72
- Ga naar fraudehelpdesk.nl
- Zij geven ook tips wat je moet doen, zoals:
  - bankrekening blokkeren
  - computer controleren op virussen
  - wachtwoord wijzigen



Neem contact op met de organisatie waar je bent opgelicht (bijvoorbeeld bij je bank of Marktplaats).

Door deze stappen te volgen help je anderen ook veilig online te blijven.

Hulp nodig?

Heb je hulp nodig, bijvoorbeeld bij een wachtwoordmanager of tweestapsverificatie? Daarvoor kun je terecht bij de bibliotheek. Bezoek een spreekuur waar anderen je helpen met digitale vragen.

Je kunt ook contact opnemen met de DigiHulplijn:

- Bel 0800-1508
- Mail naar vragen@digihulp.nl
- Stel je vraag via WhatsApp (scan de QR-code)

Meer leren?

Ga naar digiveiliger.nl voor meer oefeningen en tips.
Of bezoek de lokale bibliotheek voor hulp en workshops over online bankieren of online veiligheid.

Met vertrouwen online

Je weet nu beter waar je allemaal op moet letten om zo veilig mogelijk online te zijn. Krijg je een bericht? Denk dan aan het ABCD'tje:
Alert – **B**escherm – **C**ontroleer – **D**eel

Vertrouw op je gezond verstand. Twijfel je over een bericht? Neem dan rustig de tijd om het te controleren met de VeiligWijzer. Je kunt altijd bellen of mailen naar het bedrijf waar je een bericht van krijgt om te controleren of het echt is.

Tip

Bel de bank vanuit de bank-app. Zo weet je zeker dat je de juiste mensen aan de lijn krijgt. En de bank weet direct dat ze jou aan de lijn hebben.

Notities

DigiVeiliger

Veilig online bankieren

Dit boekje is een samenvatting van de les ‘Veilig online bankieren’.
Het bevat de belangrijkste tips en aandachtspunten om veilig online te bankieren. Dit is handig om nog eens rustig door te lezen.

Gebruik dit boekje als geheugensteuntje:
bij twijfel, altijd eerst even checken!

zeker online

© Stichting Digisterker