



**seniorweb**  
Westerkwartier

# FRAUDE HERKENNEN EN VOORKOMEN

**RENÉE KAMPHUIS**

**SeniorWeb Westerkwartier**

- Wat is online fraude? Hoe kunt u het zelf herkennen?
- Hoe wapent u zich tegen deze criminelen? Wat kunt u zelf allemaal doen?
- **GOUDEN REGELS**



# Soorten online fraude

---

- Phishing (nepmails)
- Helpdeskfraude (neptelefoontjes van de bank)
- WhatsApp fraude



- **Phishing (nepmails)**
- Helpdeskfraude (neptelefoontjes van de bank)
- WhatsApp fraude





<https://www.maakhetzeniettemakkelijk.nl/senioren-en-veiligheid/phishing-via-bijvoorbeeld-nepmailtjes>

# Dus bij een mailtje met een link erin ...

---

## GOUDEN REGEL: **eerst checken, dan pas klikken ...**

- Controleer de afzender (klopt dit met eerdere mails die u kreeg?)
- Controleer de aanhef (staat uw **naam** er in?)
- Wordt u gevraagd op een link te klikken, bijvoorbeeld om uw gegevens aan te passen? Of wordt u gevraagd geld over te maken? Is er haast bij?



**let dan extra goed op of alles klopt!**

- stuur een verdacht mailtje (**als bijlage**) naar

[valse-email@fraudehelpdesk.nl](mailto:valse-email@fraudehelpdesk.nl)

Bedankt voor uw e-mail aan [valse-email@fraudehelpdesk.nl](mailto:valse-email@fraudehelpdesk.nl)



Fraudehelpdesk valse-email <[donotreply@fraudehelpdesk.nl](mailto:donotreply@fraudehelpdesk.nl)>

Aan [renee@wijninga-kamphuis.nl](mailto:renee@wijninga-kamphuis.nl)

↩ Beantwoorden

↩️ Allen beantwoorden

➔ Doorsturen



wo 24-1-2024 09:54

Geachte mevrouw, heer,

Dit is een automatisch gegenereerd bericht. U ontvangt geen persoonlijk antwoord op e-mails die u doorstuurt naar [valse-email@fraudehelpdesk.nl](mailto:valse-email@fraudehelpdesk.nl). Heeft u een specifieke vraag over de ingestuurde e-mail? Gebruik dan ons [online meldformulier](#) of neem contact met ons op via telefoonnummer 088 786 73 72.

Hartelijk dank voor het toesturen van de e-mail. **De door u toegezonden e-mail is vermoedelijk een phishing-e-mail.** Wij adviseren u de verdachte e-mail uit uw mailbox te verwijderen. Heeft u op de -in de e-mail vermelde- link geklikt, gegevens ingevuld of een betaling verricht via een betaallink, neem dan contact met ons op via telefoonnummer 088 786 73 72 of kijk op onze [website](#) voor meer informatie.



- Home
- Valse e-mails**
- Maarschuwingen
- Veilig digitaal
- Meer
- Over ons

Fraude melden

LET OP (3/4): E-MAIL DAGVAARDING IN BEZIT HEBBEN KINDERPORNO > Sinds 12:21 | 17 jan 2024

- Ik heb een raar telefoontje ontvangen
- Ik heb een nare ervaring met online shoppen
- Bestaat mijn online geliefde wel echt?
- Mijn gegevens zijn in verkeerde handen gevallen
- Ik heb een vreemd bericht ontvangen
- Mij is iets anders overkomen
- Fraude? Direct melden!**
- Verdachte e-mail melden!**

### Actueel

**Onbekende webshop?**  
Check eerst de reviews  
[Lees onze tips](#)



Particulier | Zakelijk

🔍 | 088 - 7867372



Home Valse e-mails Waarschuwingen Veilig digitaal Meer Over ons


**Fraude melden**

Filter: **Alles** Op bedrijf




**Apple**  
29 jan 2024  
Uw Apple ID is geblokkeerd

Voorbeeld | [Lees meer](#)



**ICS**  
29 jan 2024  
U heeft een belangrijk bericht ontvangen

Voorbeeld | [Lees meer](#)




**ICS**  
29 jan 2024  
Ongelezen bericht

Voorbeeld | [Lees meer](#)




**Kamer van Koophandel**  
29 jan 2024  
KVK-Controleer uw account gebruik

Voorbeeld | [Lees meer](#)




**Facebook Meta for Business**  
29 jan 2024  
Immediate Action Required to Prevent Permanent Account Suspension

Voorbeeld | [Lees meer](#)




**Ziggo**  
29 jan 2024  
Je Ziggo-account is inactief.

Voorbeeld | [Lees meer](#)



**Belastingdienst Berichtenbox**



**Bunq bank**



**Mijn Overheid**



Beste mevrouw Kamphuis,

Je hebt een bericht over: “**De voorwaarden rond je betaalrekening wijzigen per 1 januari 2024**”. [Lees het veilig in je app of in Mijn ING.](#)

Is een bericht extra belangrijk, dan krijg je ook een e-mail. Zoals nu. Dan mis je niets!

Met vriendelijke groet,

Annet van der Hoek  
Directeur Klantenservice



Bericht van SVB (document ontvangen)



noreply@mijn.overheid.nl  
Aan renee@wijninga-kamphuis.nl

[Als er problemen zijn met de weergave van dit bericht, klikt u hier om het in een webbrowser te bekijken.](#)

Er staat een document in uw Berichtenbox van SVB. **Log in op MijnOverheid om het bericht te bekijken.** Mogelijk moet u naar aanleiding van dit bericht actie ondernemen. Lees het daarom op tijd.

Geachte R. Kamphuis,

Er staat een document in uw Berichtenbox van SVB. Log in op MijnOverheid om het bericht te bekijken. Mogelijk moet u naar aanleiding van dit bericht actie ondernemen. Lees het daarom op tijd.

Met vriendelijke groet,

MijnOverheid

# Phishing herkennen: check de link

---

Let op de **domeinnaam** in het internetadres:

<https://www.rtvnoord.nl/nieuws/900998>

<https://mailstats.fietzersbond.nl/ls/click?upn=mHR-2FJVMwO1Ifna>

# Phishing herkennen: check de link

---

- **op uw pc:** wijs met de cursor de link aan (vooral **niet klikken**)
- **op uw tablet/telefoon:** de link indrukken en ingedrukt houden (vooral **niet tikken**)

# Phishing herkennen: check de link

Bekijk tips voor je Stofzuiger

 Coolblue <klantenservice@coolblue.nl>

Als er...

[https://trco.coolblue.nl/c10/https://www.coolblue.nl/support/product/908391?utm\\_source=vanessa&utm\\_medium=mail&utm\\_campaign=notspecified&utm\\_content=product\\_urls\\_support\\_hub&message\\_id=121c82df-1514-4ff4-99d0-de1f07e6d2e9/1/0102018d0e8581c0-dd50b618-2ff6-49ce-9be4-97671f80c560-000000/gzvcg9s1a1cd2vzkq7crglg6bl6imjbtvp6rcvo3lim=335](https://trco.coolblue.nl/c10/https://www.coolblue.nl/support/product/908391?utm_source=vanessa&utm_medium=mail&utm_campaign=notspecified&utm_content=product_urls_support_hub&message_id=121c82df-1514-4ff4-99d0-de1f07e6d2e9/1/0102018d0e8581c0-dd50b618-2ff6-49ce-9be4-97671f80c560-000000/gzvcg9s1a1cd2vzkq7crglg6bl6imjbtvp6rcvo3lim=335)

**Klik of tik om de koppeling te volgen.**

# akkoord



onderhoud ik mijn stofzuiger met za



# verdacht!



## MijnOverheid

Geachte heer/mevrouw ,

Er staat een document in uw [Berichtenbox](#) van Relactingsamenwerking Gemeenten en Waterschappen. Ga naar [MijnOverheid](#) om het bericht te bekijken. Mogelijk moet u naar aanleiding van dit bericht actie ondernemen. Lees het daarom op tijd.

Met vriendelijke groet,

MijnOverheid



### Technisch onderhoud Berichtenbox app

Vanwege technisch onderhoud is het momenteel niet mogelijk om het bericht via de Berichtenbox direct te lezen. Bekijk het bericht daarom direct via uw webbrowser.

**géén naam genoemd in de aanhef**

**een (verdachte) link naar de Berichteninbox en/of naar MijnOverheid**

**<https://rebrand.ly/39t858p>**

**een melding dat u gebruik moet maken van uw browser**



# verdacht!

Beste Heer/Mevrouw,

Uw openstaande schuld met kenmerk RMCK029 is na meerdere herinneringen nog r  
2023 zal de gerechtsdeurwaarder overgaan tot executieaal beslaglegging. U kunt be  
door het gehele bedrag direct te voldoen.

Via onderstaande knop kunt u het openstaande bedrag direct voldoen met [iDeal](#).


Betaal openstaande schuld


<https://bunq.me/o/5I1DQRYMnexjmONkvw21j9>

**Iedereen kan bij de bank Bunq zelf makkelijk een betaalverzoek maken – je krijgt dan een bunq.me link**



# Voorbeelden van nepmails

Van KVK <yiram.hernandez@dti-consultores.com> 

Aan Wim Wijninga 

Onderwerp **Aanvullende informatie vereist**

---

**KVK** 

[yiram.hernandez@dti-consultores.com](mailto:yiram.hernandez@dti-consultores.com)

De QR code verwijst naar [gg.gg/16rdtx](https://gg.gg/16rdtx) 

---

**Aanvullende informatie vereist**

Geachte ondernemer,

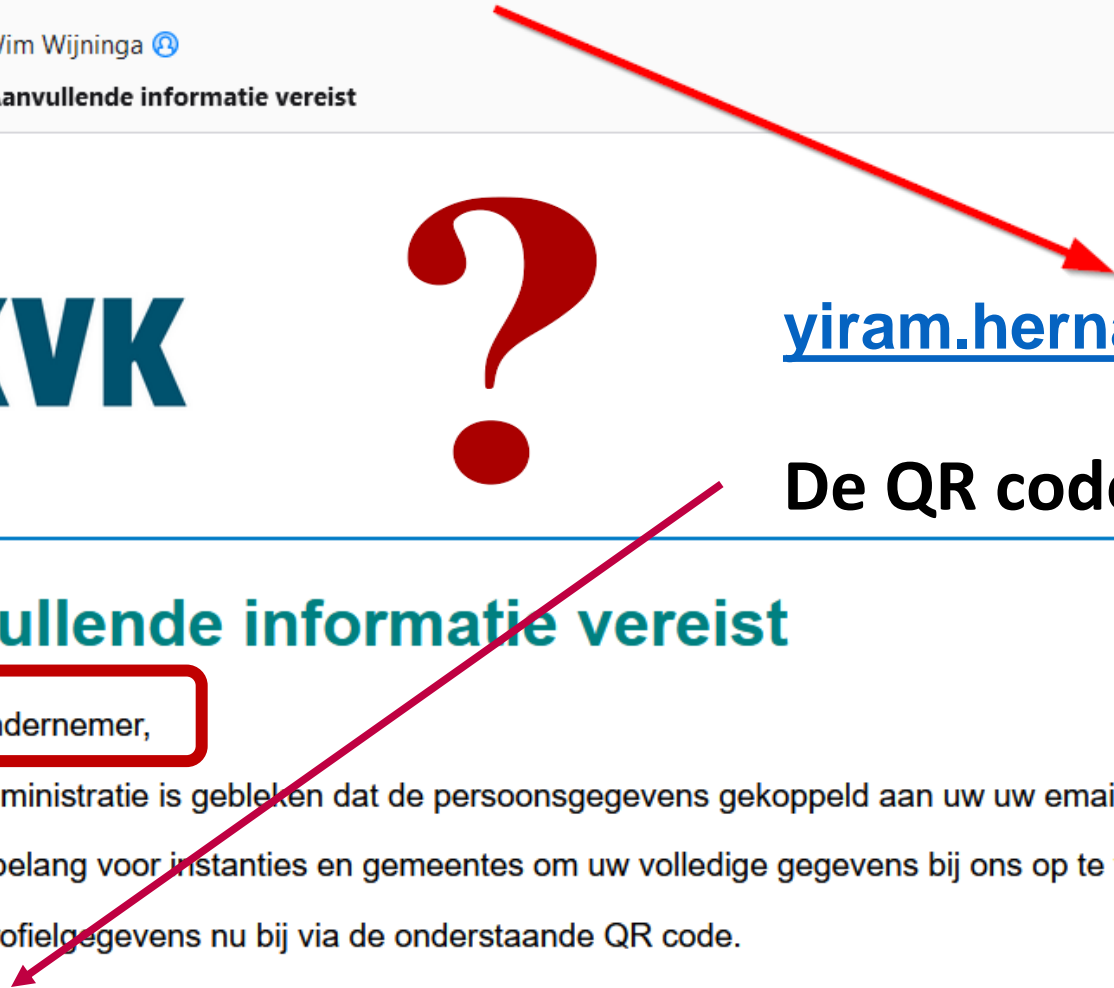
Uit onze administratie is gebleken dat de persoonsgegevens gekoppeld aan uw emailadres niet volledig zijn ingediend.

Het is van belang voor instanties en gemeentes om uw volledige gegevens bij ons op te vragen indien nodig. Wij verzoeken u z

Werk uw profielgegevens nu bij via de onderstaande QR code.



**verdacht!**





**Bij twijfel: niet klikken !!!**

## Wat als u (per ongeluk) toch op een phishing-link heb geklikt?

- Sluit het e-mailprogramma af
- Laat de virusscanner een uitgebreide scan uitvoeren en schadelijke software verwijderen
- Wijzig voor de zekerheid (belangrijke) wachtwoorden – zeker die van uw bank (op een ander apparaat)
- Gebruik een ander apparaat voor internetbankieren totdat u zeker weet dat er geen schadelijke software op uw pc staat

# Soorten online fraude

---

- Phishing (nepmails)
- **Helpdeskfraude (neptelefoontjes van de bank)**
- WhatsApp fraude





<https://www.maakhetzeniettemakkelijk.nl/senioren-en-veiligheid/spoofing>

# Een bankmedewerker zal u nóóit vragen om:

---

- een betaalpas op te sturen of mee te geven (ook niet aan de deur)
- een pincode, inloggegevens of code van een scanner door te geven
- geld over te maken
- via een link in een SMS of e-mail in te loggen in internetbankieren of in de app van de bank
- software te downloaden waarmee ze de computer op afstand kunnen overnemen om u zogenaamd te 'helpen'

## Bent u er onverhoopt toch ingetrapt?

- Neem dan zo snel mogelijk contact op met uw bank
- Zoek hiervoor zélf het nummer van uw bank op
- Doe aangifte

# Soorten online fraude

---

- Phishing (nepmails)
- Helpdeskfraude (neptelefoontjes van de bank)
- **WhatsApp fraude**





<https://www.maakhetzeniettemakkelijk.nl/senioren-en-veiligheid/hulpvraagfraude-via-bijvoorbeeld-whatsapp>



- ook wel “vriend in nood fraude” genoemd –
- de oude telefoon is onbruikbaar
- er is sprake van een acute noodsituatie
- er moet geld overgemaakt worden
- en de tijdsdruk is hoog (anders gebeurt er iets ergs)

Dus:

- Maak nooit zomaar geld over
- Bel de bekende op **het bij u bekende** nummer
- Wacht tot u de bekende **écht hebt gesproken**

- bij links in een e-mailbericht: **EERST CHECKEN, DAN KLIKKEN**
- bij een 'raar' telefoontje of een e-mail van de bank die u niet helemaal vertrouwt:

**BEL ALTIJD EERST NAAR HET BIJ U BEKENDE NUMMER**

- bij een 'vriend in nood' verzoek via WhatsApp:

**NIET GEBELD – GEEN GELD**



# websites met meer informatie

---



**Veiliginternetten.nl – deels specifiek gericht op senioren:**

[https://veiliginternetten.nl/senioren-en-online-veiligheid/#locatie\\_b](https://veiliginternetten.nl/senioren-en-online-veiligheid/#locatie_b)

**en**

<https://veiliginternetten.nl/uitlegvideos/>

**SeniorWeb:**

<https://www.seniorweb.nl/online-veiligheid-en-privacy>

**BIJ TWIJFEL: DOE NIETS !**



**Dank voor uw aandacht !**

