

# Alles wat je moet weten over phishing





# Index

- 01 Mediawijs & mezelf
- 02 Wat is phishing?
- 03 Hoe werkt het?
- 04 Hoe herkennen?
- 05 Help, ik ben gefisht!
- 06 Tips voor jouw lokaal bestuur
- 07 Tot slot...



## Louis Demeulenaere

Projectmedewerker 'content, tools en events'.

- **Content:** cybersecurity, informatiegeletterdheid, ...
- **Tools:** Edubox, Beleidstool Mediawijsheid, lespakketten, ...
- **Events:** Apestaartjaren, MediaNest Studiedag, Dig it up, ...

# Mediawijs is ...

... het **Vlaamse Kenniscentrum Digitale en Mediawijsheid** van de Vlaamse overheid en imec vzw. Mediawijs helpt de inwoners van Vlaanderen en Brussel om **digitale technologie en media actief, creatief, kritisch en bewust te gebruiken en begrijpen** om deel te nemen aan onze maatschappij.

# Mediawijs in een nieuw jasje

Ontdek onze nieuwe website boordevol interessante dossiers, handige tools en actueel onderzoek.



[mediawijs.be](https://mediawijs.be)

# Dossiers

Mediawijs werkt op basis van expertise uit het veld en uit onderzoek de volgende dossiers uit. We blijven werken aan onze dossiers, houden de info up to date en vullen aan waar nodig. Heb je een vraag of opmerking? [Contacteer ons](#).

## Zoek een dossier



Auteursrechten



Complotdenken



Cyberpesten



Cybersecurity



Home > Dossiers >

# Surf safe! Alles over cybercriminaliteit

Voor een groot deel van onze dagelijkse bezigheden rekenen we op het internet: online houden we contact met vrienden en familie, regelen we onze bankzaken en kopen we eender wat we nodig hebben. Dat is handig, maar ook risicovol. Want ook cybercriminelen zitten op het internet. Zo proberen ze je geld of gegevens in handen te krijgen. Hoe bescherm je jezelf daartegen? In dit dossier ontdek je alles wat je moet weten.

Dit dossier kwam tot stand met de hulp van Centrum voor Cybersecurity België [↗](#) (Safeonweb) en Febelfin [↗](#). Vragen over cybersecurity? Contacteer onze experts [Louis Demeulenaere](#).

---

Op deze pagina: [Wat is cybercriminaliteit](#) [Veilig surfen: de basics](#) [Digitaal betalen en bankieren](#) [Wat je moet weten over phishing](#) [Soorten \(online\) fraude](#)  
[Onderzoek](#) [Tools](#) [Video's](#) [Meer weten?](#)

---





# Wat is phishing?







# Ga naar [menti.com](https://menti.com)

- code: **3187 6879**





# Wat is phishing?

- Eén van de meest voorkomende vormen van **cybercriminaliteit**.
- Slachtoffers van phishing worden opgelicht via **(online) berichten of telefoontjes**
  - aansporen om **persoonlijke gegevens** te delen
  - geld overmaken
  - verdachte bijlagen openen
  - onofficiële apps downloaden
  - ...
- Letterlijk 'vissen' naar gegevens

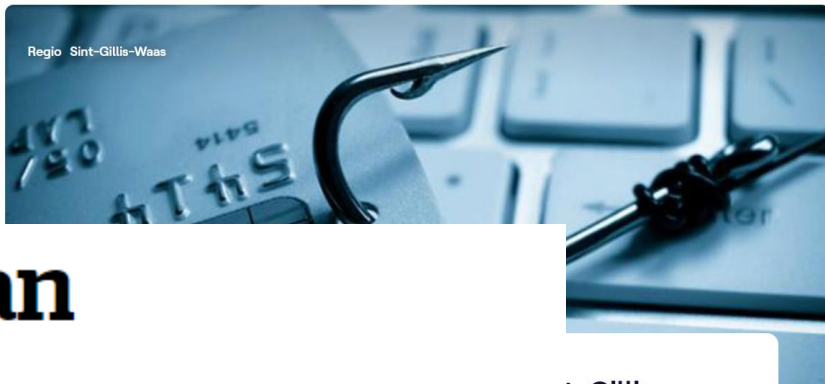




Piet den Blanken

# rschot waarschuwt voor g mails

elet! Er zi  
ot waars  
lijven bi



t-Gillis-  
elasting



n  
ut

# Phishing mail in naam van burgemeester

**ZWIJNDRECHT**

Er gaat momenteel een phishing mail rond in naam van de burgemeester van Zwijndrecht, André Van de Vyver. Phishing is een vorm van internetfraude waarbij er valse berichten worden verstuurd om inloggegevens, creditcardinformatie, pincodes of andere persoonlijke gegevens te achterhalen.



...  
miljoen euro

werd in 2021 buitgemaakt via phishing.



25  
miljoen euro

werd in 2021 buitgemaakt via phishing.

2020: 34 miljoen euro



# Phishing: hoe werkt dat?





# Phishing: hoe werkt dat?

- Je wordt benaderd door een **oplichter** die zich **voordoet** als een **persoon, bedrijf, organisatie** of andere instantie.
  - via **e-mail, sms, instant messaging apps, telefoontjes of sociale media.**
  - Doel: **geld of gegevens te ontfutselen.**





# Phishing: hoe werkt dat?

- **‘Social engineering’** = Een veel gebruikte techniek bij phishing.
  - **Verzameling strategieën** om anderen **mentaal** te manipuleren.
  - **Doel:** iemand **overhalen** gevoelige informatie prijs te geven of specifieke handelingen te verrichten
- **Typerend** aan social engineering-aanvallen:
  - Er wordt op jouw **emoties** ingespeeld
  - Je wordt overhaalt om **dringend** te handelen
  - Er wordt geprobeerd je **vertrouwen** te winnen





# Hoe phishing herkennen?





# Hoe phishing herkennen?

- Steeds sluwere technieken om je ervan te overtuigen dat je met een betrouwbare partij in contact staat.
- Jezelf beschermen → **signalen** herkennen.





# Hoe phishing herkennen?

- **Het bericht komt uit het niets**
  - Is het logisch dat je dit bericht krijgt?
- **Je krijgt een vreemde vraag**
  - Je bankgegevens doorgeven via sms of e-mail?



# Hoe phishing herkennen?

- **Het is te mooi om waar te zijn**
  - Een indrukwekkende prijs of een geldbedrag hebt gewonnen?
  - En moet je daar nog even wat gegevens voor invullen?
- **Word je gepusht om iets te doen?**
  - Frons je wenkbrauwen als je gevraagd wordt om iets met spoed te doen.



# Hoe phishing herkennen?

- **De afzender komt je bekend voor, maar het mailadres klopt niet**
  - Het e-mailadres of de opmaak van de e-mail lijkt bijvoorbeeld sterk op dat van de overheid.
- **De link in het bericht klopt niet**
  - Valse berichten bevatten vaak een link waarop je moet klikken.



# Hoe phishing herkennen?

- **Je naam wordt niet gebruikt**
  - Frauduleuze berichten worden vaak tegelijk naar een groot aantal mensen gestuurd → niet gepersonaliseerd.
  - Opgelet! Ook mails met persoonlijke aansprekingen kunnen phishing zijn!
- **Je merkt taalfouten op**
  - Rare zinsconstructies of spelfouten?



# Hoe phishing herkennen?

- **Het bericht belandt in je spamfolder**
  - Een goede maatstaf om valse berichten meteen te herkennen.
  - Verdachte e-mailadressen staan vaak op de zwarte lijst van je mailprovider, waardoor ze als ongewenst beschouwd worden.
- **Het bericht bevat clickbait**
  - Aantrekkelijke en veelbelovende titels...



de post brengt je vandaag een pakje.

de post <noreply@xyz542.be>

To YOU

Sep 4 at 8:29 AM



Dag,

BOLSY heeft je een pakje met nummer 323200017959819956632040 gestuurd. Vandaag, tussen 08:00 en 17:00 komt de post het jou bezorgen. Wij hopen dat je dan aanwezig zal zijn.

Je kan de status van jouw pakje raadplegen via [onze track & trace applicatie](#). Indien je de link niet kunt openen, gelieve dan [onze tool](#) te downloaden om jouw pakje live te volgen.

Met vriendelijke groeten,  
de post.

Copyright © de post | [Disclaimer](#) | [Algemene voorwaarden](#)



Mail-bijlage

1. Het bericht komt uit het niets
2. Je krijgt een vreemde vraag
3. Het is te mooi om waar te zijn
4. Word je gepusht om iets te doen?
5. De afzender komt je bekend voor, maar het mailadres klopt niet
6. De link in het bericht klopt niet
7. Je naam wordt niet gebruikt
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait

↩ Reply   ↩️ Reply to All   ➡ Forward   ⋮ More





de post brengt je vandaag een pakje.

de post <noreply@xyz542.be>

To YOU

Sep 4 at 8:29 AM



Dag,

BILSY heeft je een pakje met nummer 323200017959819956632040 gestuurd. Vandaag, tussen 08:00 en 17:00 komt de post het jou bezorgen. Wij hopen dat je dan aanwezig zal zijn.

Je kan de status van jouw pakje raadplegen via [onze track & trace applicatie](#). Indien je de link niet kunt openen, gelieve dan [onze tool](#) te downloaden om jouw pakje live te volgen.

Met vriendelijke groeten,  
de post.

Copyright © de post | [Disclaimer](#) | [Algemene voorwaarden](#)



Mail-bijlage

↩ Reply   ↩️ Reply to All   ➡ Forward   ⋮ More

1. **Het bericht komt uit het niets**
2. Je krijgt een vreemde vraag
3. Het is te mooi om waar te zijn
4. **Word je gepusht om iets te doen?**
5. **De afzender komt je bekend voor, maar het mailadres klopt niet**
6. **De link in het bericht klopt niet**
7. **Je naam wordt niet gebruikt**
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



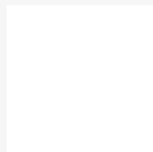
**From:** Cinema Cadeau <[CinemaCadeau@federal-gov.be](mailto:CinemaCadeau@federal-gov.be)>

**Sent:** Monday 3 January 2022 15:59

**To:** Louis Demeulenaere (imec-Vrije Universiteit Brussel) <[Louis.Demeulenaere@imec.be](mailto:Louis.Demeulenaere@imec.be)>

**Subject:** You have received a CinemaGift Card

Congratulations with your present, click [here](#) to redeem your present.



**Dear Louis Demeulenaere,**

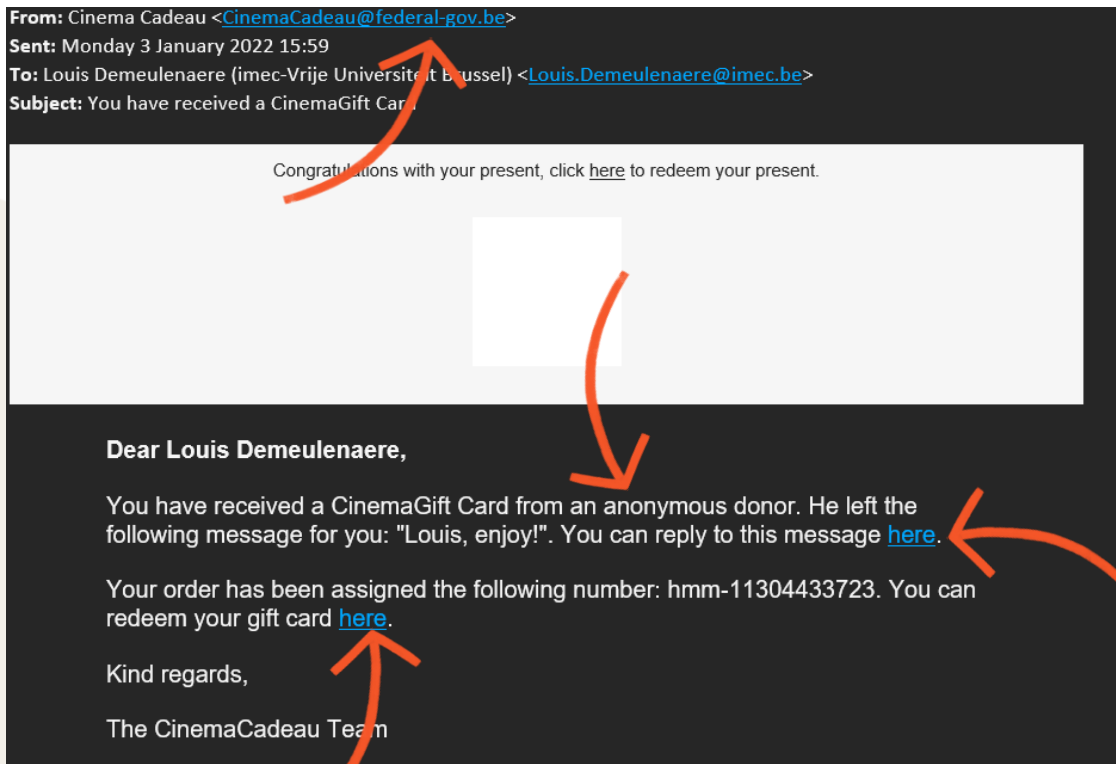
You have received a CinemaGift Card from an anonymous donor. He left the following message for you: "Louis, enjoy!". You can reply to this message [here](#).

Your order has been assigned the following number: hmm-11304433723. You can redeem your gift card [here](#).

Kind regards,

The CinemaCadeau Team

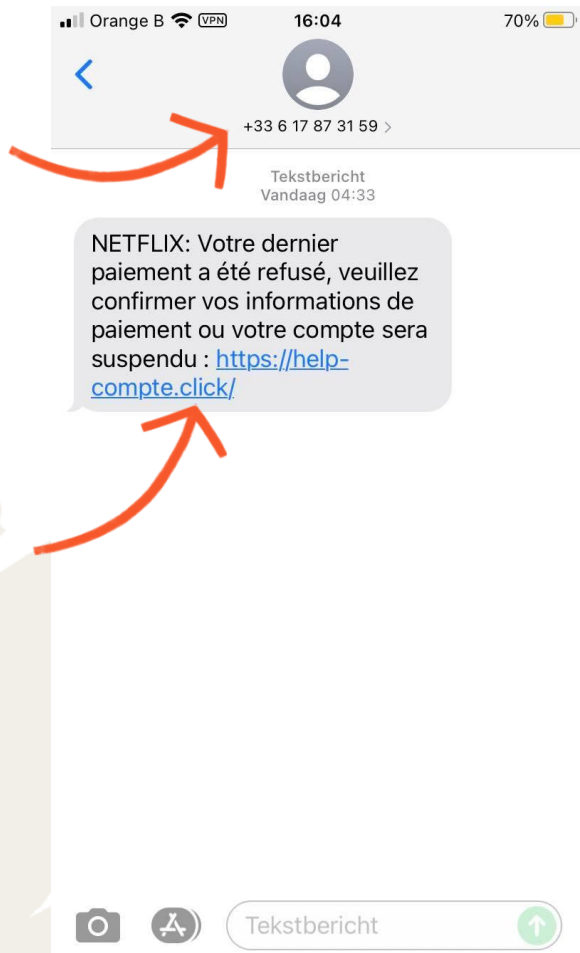
1. Het bericht komt uit het niets
2. Je krijgt een vreemde vraag
3. Het is te mooi om waar te zijn
4. Word je gepusht om iets te doen?
5. De afzender komt je bekend voor, maar het mailadres klopt niet
6. De link in het bericht klopt niet
7. Je naam wordt niet gebruikt
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



1. **Het bericht komt uit het niets**
2. Je krijgt een vreemde vraag
3. **Het is te mooi om waar te zijn**
4. **Word je gepusht om iets te doen?**
5. De afzender komt je bekend voor, maar het mailadres klopt niet
6. **De link in het bericht klopt niet**
7. Je naam wordt niet gebruikt
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



1. Het bericht komt uit het niets
2. Je krijgt een vreemde vraag
3. Het is te mooi om waar te zijn
4. Word je gepusht om iets te doen?
5. De afzender komt je bekend voor, maar het mailadres klopt niet
6. De link in het bericht klopt niet
7. Je naam wordt niet gebruikt
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



1. **Het bericht komt uit het niets**
2. Je krijgt een vreemde vraag
3. Het is te mooi om waar te zijn
4. **Word je gepusht om iets te doen?**
5. **De afzender komt je bekend voor, maar het mailadres klopt niet**
6. **De link in het bericht klopt niet**
7. **Je naam wordt niet gebruikt**
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



From: Twitter <[twitter@mobile-invoicer.com](mailto:twitter@mobile-invoicer.com)>

Sent: Wednesday 1 December 2021 21:19

To: Louis Demeulenaere (imec-Vrije Universiteit Brussel) <[Louis.Demeulenaere@imec.be](mailto:Louis.Demeulenaere@imec.be)>

Subject: Your phone number has been used!



Hi Louis,

Your phone number has been added to another account.

Is this still your phone number? If not, please update your account [with your current phone number](#).

NOTE: your account can no longer perform [SMS commands](#) nor receive [certain SMS notifications](#).

Only the account most recently linked to this phone number will have these features.

#### How do I know this email is from Twitter?

When you click on a link, the address should start with "twitter.com." Emails from Twitter will never ask for sensitive information.

1. Het bericht komt uit het niets
2. Je krijgt een vreemde vraag
3. Het is te mooi om waar te zijn
4. Word je gepusht om iets te doen?
5. De afzender komt je bekend voor, maar het mailadres klopt niet
6. De link in het bericht klopt niet
7. Je naam wordt niet gebruikt
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



From: Twitter <[twitter@mobile-invoicer.com](mailto:twitter@mobile-invoicer.com)>  
Sent: Wednesday 1 December 2021 21:19  
To: Louis Demeulenaere (imec-Vrije Universiteit Brussel) <[Louis.Demeulenaere@imec.be](mailto:Louis.Demeulenaere@imec.be)>  
Subject: Your phone number has been used!

Hi Louis,

Your phone number has been added to another account.

Is this still your phone number? If not, please update your account [with your current phone number](#).

NOTE: your account can no longer perform [SMS commands](#) nor receive [certain SMS notifications](#).

Only the account most recently linked to this phone number will have these features.

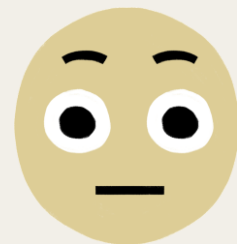
**How do I know this email is from Twitter?**

When you click on a link, the address should start with "twitter.com." Emails from Twitter will never ask for sensitive information.

1. Het bericht komt uit het niets
2. **Je krijgt een vreemde vraag**
3. Het is te mooi om waar te zijn
4. Word je gepusht om iets te doen?
5. **De afzender komt je bekend voor, maar het mailadres klopt niet**
6. **De link in het bericht klopt niet**
7. Je naam wordt niet gebruikt
8. Je merkt taalfouten op
9. Het bericht belandt in je spamfolder
10. Het bericht bevat clickbait



**Help, ik ben gephisht!**

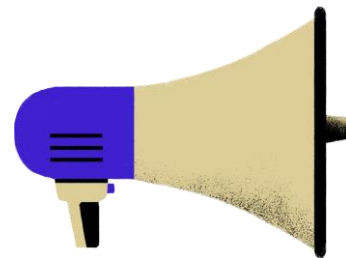






# Help, ik ben gefhisht!

- **Heb je je wachtwoord gedeeld?** Verander dit dan zo snel mogelijk in een **sterk wachtwoord**.
- **Heb je een betaling gedaan of bankgegevens doorgegeven?** Contacteer onmiddellijk je **bank** én **Card Stop**.
- **Waarschuw mensen in je omgeving.** Schaam je niet over wat er gebeurd is: je bent écht niet de enige.
- **Meld het bericht.** Via [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be) kan je frauduleuze berichten anoniem rapporteren.





# Concrete tips voor jouw lokaal bestuur



# Concrete tips voor jouw lokaal bestuur

- Accounts werknemers → beveiligd met sterke wachtwoorden en multifactorauthenticatie.
- Sensibilisering & training van personeel
- Opvolging cyberincidenten



**Tot slot...**





# Phishing?

## 8 checks om phishing te voorkomen

Cybercriminelen sturen je soms een valse sms, e-mail of bellen je op om je vertrouwelijke gegevens te pakken te krijgen. Wil je weten of een bericht betrouwbaar is? Doe deze 8 checks!

### #1 Komt het bericht onverwacht?

Krijg je zonder reden een bericht van iemand met een onverwachte vraag?

### #2 Is het bericht te mooi om waar te zijn?

Zomaar een reis gewonnen of gratis pensioen kassa? Dat is het waarschijnlijk bedrog ...

### #3 Vraagt iemand persoonlijke gegevens?

Een officiële instantie zal je nooit per e-mail of telefoon naar je wachtwoord of bankgegevens vragen.

### #6 Naar waar leidt de link?

Wil je schermen waar de link naartoe leidt? Zelfs met je muis over de link en ontdek de volledige url.

### #5 Ken je de afzender?

Komt het meldje van een vreemd e-mailadres? Of staat de naam van het bedrijf er niet in? Let op! Ook echte e-mailadressen kunnen misbruikt worden om zulke mails te sturen.

### #4 Is het bericht dringend?

Zeg het bericht dat je iets meten moet doen?

### #7 Word je persoonlijk aangesproken?

Mails die beginnen met beste, mevrouw, meneer ... zijn vaak niet te vertrouwen als ze niet gevolgd worden door je naam.

### #8 Bevat het bericht veel taalfouten?

Ook taalfouten of vreemde afzenderadressen kunnen wijzen op een vervalscht bericht.



Meer weten? Surf naar [www.safeonweb.be](http://www.safeonweb.be) en [www.mediawijs.be/cybersecurity](http://www.mediawijs.be/cybersecurity)

# 3 tips om jouw accounts te beschermen

Bijna iedereen heeft wel één of meerdere accounts op sociale media of websites. Wil je niet dat iemand aan je profiel en informatie kan? Volg dan deze tips.

#1



## Gebruik een wachtwoordkluis

Deze kluis helpt je om sterke wachtwoorden te maken en verzamelt ze op 1 plaats. Zo moet je maar 1 wachtwoord onthouden.

#2

## Schakel tweestaps-verificatie in

Gebruik een sterk wachtwoord in combinatie met een andere manier van aanmelden zoals een vingerafdruk, gezichtsherkenning of een bevestiging via sms of app.



#3



## Zorg voor een sterk wachtwoord

- ✓ Gebruik minstens 15 tekens met cijfers, hoofd- en kleine letters en symbolen.
- ✓ Verander je wachtwoorden regelmatig.
- ✓ Bedenk een zin met leestekens.
- ✗ Gebruik niet overal hetzelfde wachtwoord en schrijf het zeker nergens op.
- ✗ Vermijd woorden en namen die makkelijk te raden zijn.
- ✗ Gebruik daarom ook geen geheime vragen om je wachtwoord te herstellen.

Meer weten? Surf naar [www.safeonweb.be](http://www.safeonweb.be) en [www.mediawijs.be/cybersecurity](http://www.mediawijs.be/cybersecurity)



## Wees slimmer dan een phisher



Download de Safeonweb app >



## Zomaar een app gedownload?



OK

is niet altijd oké!

Download alleen van erkende app stores

Meer tips op [safeonweb.be](https://safeonweb.be)





# DOE DE Phishingtest

Herken jij verdachte berichten op tijd?

## Weet jij waarop je moet letten bij internetfraude?

In de phishingtest checken we hoe oplettend jij bent bij verdachte mails en berichten. Ontdek zelf hoe gemakkelijk je in de val van internetcriminelen trapt. Ben jij een expert in het herkennen van verdachte berichten? Of kan je nog wat training gebruiken?

[Doe de test](#)

## Geen tijd voor de test?

Leer phishing herkennen

[Ontdek hier onze tips](#)

## Heb je een verdachte mail of een verdacht bericht ontvangen?

Stuur hem door naar [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be) en verwijder hem daarna.

Als je dit bericht op het werk kreeg, moet je de procedures die daar gelden voor phishing opvolgen, bv. doorsturen naar de ICT-dienst.

[Wat is verdacht@safeonweb.be?](mailto:Wat is verdacht@safeonweb.be?)

# Bedankt!

Meer weten?  
[mediawijs.be/cybersecurity](https://mediawijs.be/cybersecurity)



[louis.demeulenaere@mediawijs.be](mailto:louis.demeulenaere@mediawijs.be)