CYBERPREVENTIE

Ik ben Louis Lombaert

- kom uit Asse
- ben geen cyberexpert
- De presentatie is een compilatie van diverse cybersessies
- ben ambassadeur cyberpreventie
- Doel: zoveel mogelijk mensen weerbaar te maken tegen aanvallen van cybercriminelen

CYBER... ???

Het voorvoegsel dat gebruikt wordt voor alles wat met internettechnologie samenhangt, en gebruikt wordt om het geheel van digitale systemen en netwerken te benoemen :

Cyberspace
de virtuele wereld van computers

Cyberactivisme
promoten of protesteren tegen toestanden of beslissingen

Cyberoorlog
hacken met politieke motieven, destabiliseren, fake-news, hybride oorlogsvoering

Cyberspionage
stiekem achterhalen van (staats)geheimen, fake news

Cyberveiligheid
voorkomen van vernietigen van gegevens en van ongeautoriseerde toegang.

Cybercriminaliteit
fraude, afpersing, terrorisme, diefstal, kindermisbruik, cyberseks, cyberpesten

Gilbert Leterme (96) was een kranige man, die nog thuis woonde en voor zijn vrouw zorgde. *Tot hij het slachtoffer werd van internetoplichters die er met zijn spaargeld vandoor gingen.* Hij brak. En hij niet alleen. Hij is in februari 2023 gestorven

Het pijnlijkste was misschien nog dat Gilbert zijn vrouw niet kon of wilde vertellen wat er aan de hand was…

Wat Gilbert overkwam, overkomt de jongste tijd veel ouderen. “Ze zijn het favoriete doelwit van criminelen geworden.” (DS 12januari 2025).

Toen Gilbert Leterme thuis in Kortrijk op 13 juli 2022 de telefoon opnam, had hij onverwacht ‘een bankmedewerker’ aan de lijn. Er was iets raars aan de hand met de rekeningen, zei die. Hij vroeg Gilbert om zijn computer op te starten en in te loggen bij de bank. Geen probleem. Gilbert regelde zijn bankzaken nog altijd zelf en hij zou wel even kijken wat er aan de hand was…


vrt
Cyberaanval luchthavens


vrt
Cyberaanval luchthavens

Voornaamste methoden van cyberaanvallen

- Emailphishing
- Smishing
- Vishing
- Spyware
- Ransomeware
- Quishing

- Computer virussen
- Adware
- Trojaans paard
- Email spoofing
- URL phishing


Phishing
Hacking
Botnets
Malware
Ransomwar
e
Bron : AbberantRealities
via Pixabay
CYBER(ON)VEILIGHEI

EMAILPHISHING

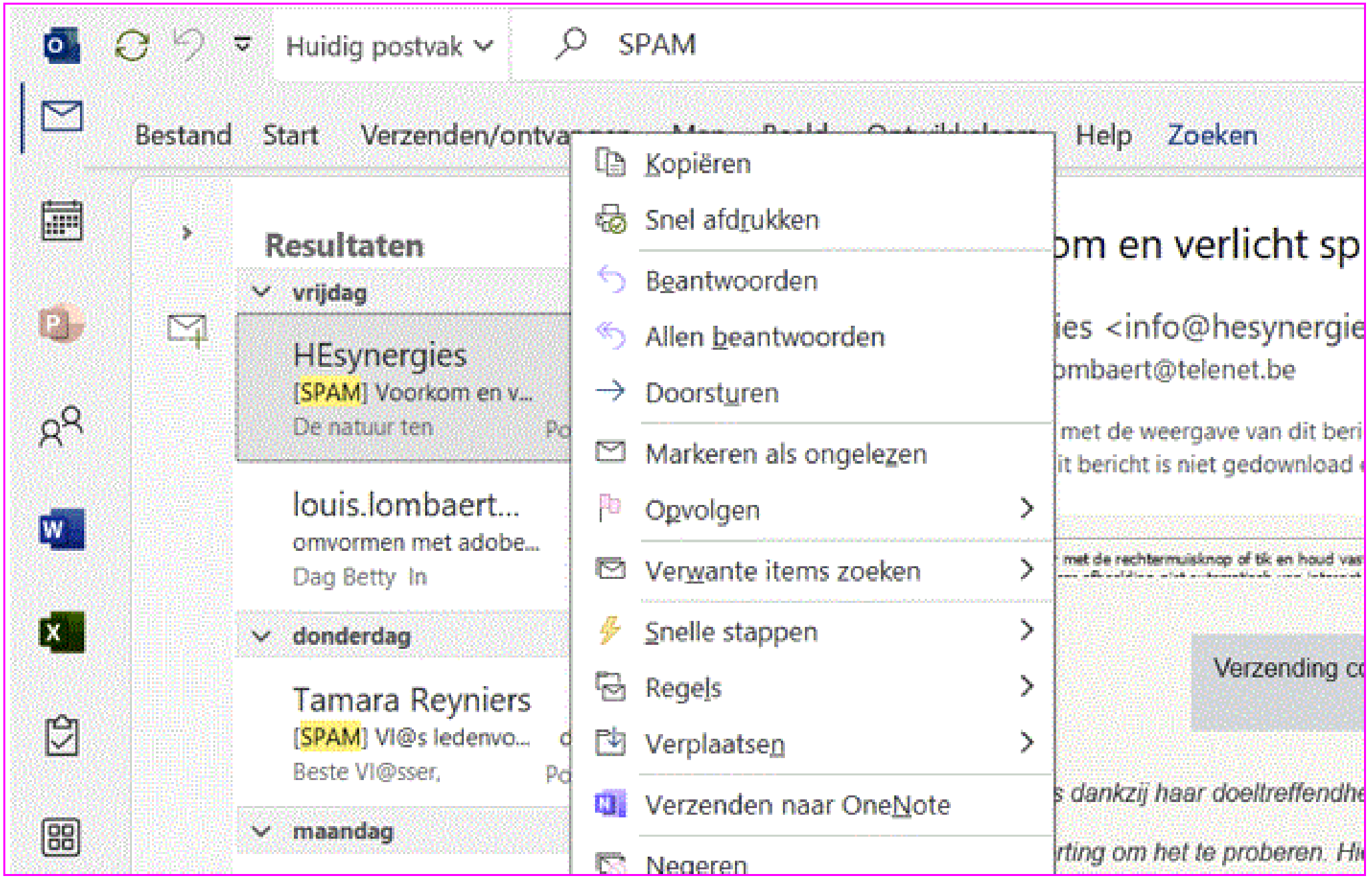
- MEEST BEKEND
  - MISLEIDENDE EMAIL VAN:
    - BANK
    - OVERHEIDSDIENST
      - Boetes
      - financiën
    - INVORDERINGEN
      - Te late betalingen
        - Onvoldoende frankering
    - MUTUALITEIT enz

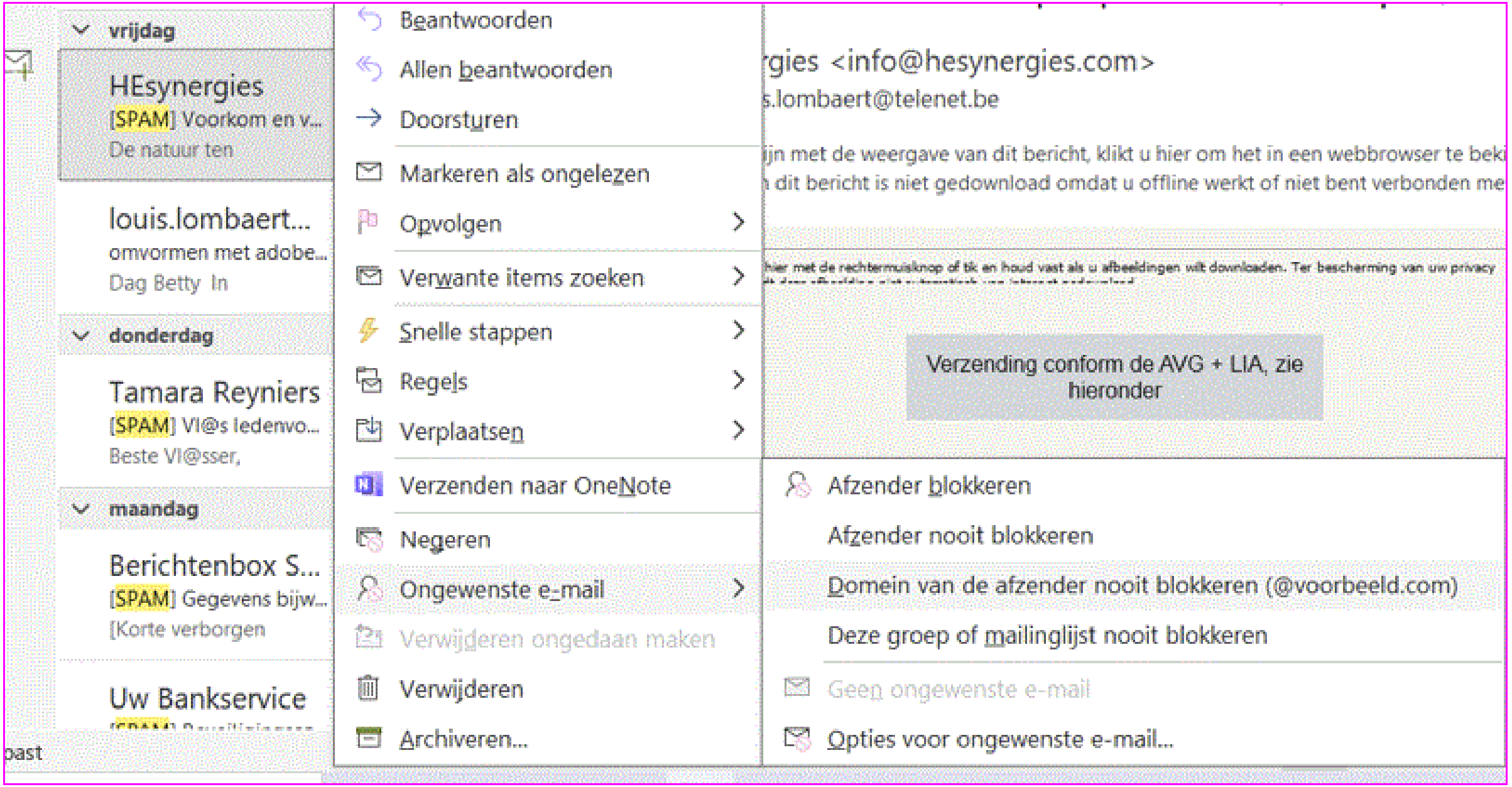
HOE VOORKOMEN ?

- UW NAAM STAAT NIET IN HET VAKJE “ AAN”
- UW NAAM STAAT TUSSEN VEEL ANDERE NAMEN
- U BENT GEEN KLANT

VOORBEELD


Resultaten
vrijdag
HEsynergies
[SPAM] Voorkom en v...
vr 19/09
De natuur ten
Postvak IN
louis.lombaert...
omvormen met adobe...
vr 19/09
Dag Betty In
Sent
donderdag
Tamara Reyniers
[SPAM] VI@s ledenvo...
do 18/09
Beste VI@sser,
Postvak IN
maandag
[SPAM] Voorkom en verlicht spierproblemen, krampen, verstuikinge...
H
HEsynergies <info@hesynergies.com>
Aan louis.lombaert@telenet.be
vr 19/09
Als er problemen zijn met de weergave van dit bericht, klikt u hier om het in een webbrowser te bekijken.
Sommige inhoud in dit bericht is niet gedownload omdat u offline werkt of niet bent verbonden met een netwerk.
Klik hier met de rechtermuisknop of tik en houd vast als u afbeeldingen wilt downloaden. Ter bescherming van uw privacy
Verzending conform de AVG + LIA, zie hieronder
Deze synergie is dankzij haar doeltreffendheid een groot succes en is in 19 landen verkrijgbaar. Wij


Huidig postvak
SPAM
Bestand
Start
Verzenden/ontva
Help
Zoeken
Resultaten
vrijdag
HEsynergies
[SPAM] Voorkom en v...
De natuur ten
louis.lombaert...
omvormen met adobe...
Dag Betty In
donderdag
Tamara Reyniers
[SPAM] VI@s ledenvo...
Beste VI@sser,
maandag
Kopiëren
Snel afdrukken
Beantwoorden
Allen beantwoorden
Doorsturen
Markeren als ongelezen
Opvolgen
Verwante items zoeken
Snelle stappen
Regels
Verplaatsen
Verzenden naar OneNote
Negeren
om en verlicht sp
ies <info@hesynergie
ombaert@telenet.be
met de weergave van dit beri
it bericht is niet gedownload
Verzending c
s dankzij haar doeltreffendhe
rting om het te proberen. H


vrijdag
HEsynergies
[SPAM] Voorkom en v...
De natuur ten
louis.lombaert...
omvormen met adobe...
Dag Betty In
donderdag
Tamara Reyniers
[SPAM] VI@s ledenvo...
Beste VI@sser,
maandag
Berichtenbox S...
[SPAM] Gegevens bijw...
[Korte verborgen
Uw Bankservice
Beantwoorden
Allen beantwoorden
Doorsturen
Markeren als ongelezen
Opvolgen
Verwante items zoeken
Snelle stappen
Regels
Verplaatsen
Verzenden naar OneNote
Negeren
Ongewenste e-mail
Verwijderen ongedaan maken
Verwijderen
Archiveren...
gies <info@hesynergies.com>
s.lombaert@telenet.be
ijn met de weergave van dit bericht, klikt u hier om het in een webbrowser te beki
dit bericht is niet gedownload omdat u offline werkt of niet bent verbonden me
Verzending conform de AVG + LIA, zie hieronder
Afzender blokkeren
Afzender nooit blokkeren
Domein van de afzender nooit blokkeren (@voorbeeld.com)
Deze groep of mailinglijst nooit blokkeren
Geen ongewenste e-mail
Opties voor ongewenste e-mail...


[SPAM] Dit hoort bij uw situatie
22 september 2025 04:31
RJV
Gegevens
RIJKSDIENST VOOR JAARLIJKSE VAKANTIE
vakantie is ons werk
Vakantiegeld Statusbericht
Referentie: VG-2025
Beste relatie,
De geplande uitbetaling kan nog niet doorgaan door een technisch knelpunt in de betaalstroom. We werken aan een oplossing. Op uw RJV-pagina ziet u steeds de voortgang en de nieuwe geplande datum.
Wat u daar terugvindt
• Huidige stand van de betaling.
• Verwachte datum van uitvoering.
• Korte toelichting in klare taal.
Antwo..
Antw. ..
Doors..
Wissen
Meer

SMARTPHONE

Markeren als spam

Markeren als ongele

Toevoegen aan VIP's

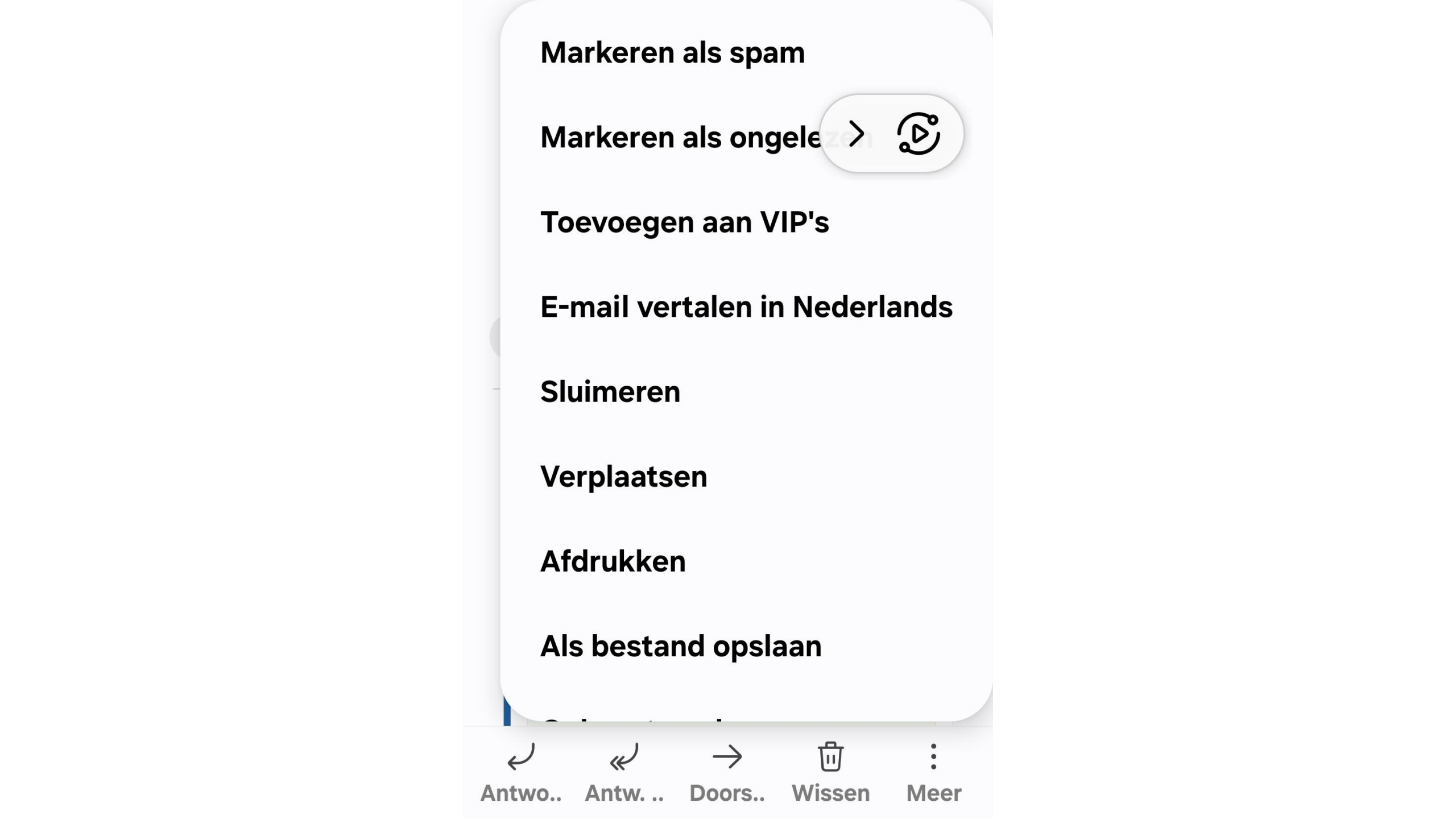
E-mail vertalen in Nederlands

Sluimeren

Verplaatsen

Afdrukken

Als bestand opslaan



SMISHING

- IDEM ALS EMAILPISHING MAAR DAN VIA:
  - SMS
  - WHATSAPP

SPYWARE

- BESCHADIGT SYSTEMEN
- STEELT DATA

RANSOMWARE

- VERSLEUTELT BESTANDEN
- LOSGELD

Malware en Ransomware: verzamelnaam voor kwaadaardige software ontworpen om computersystemen te beschadigen, te verstoren, ongeautoriseerde toegang te verkrijgen, data te vergrendelen en die pas vrij te geven na betaling van losgeld.

- Online : identiteitsfraude, oplichting bij online aankopen of betalingen
- Afpersing
- Stalking
- haatspraak en haat zaaien
- bedreigingen (politie, gerecht)
- Discriminatie
- Productie, bezit of verspreiding van kinderpornografie, auteursrechtenschendingen en Illegale kopieën, spammen.

Bron : Geralt via Pixabay

Wat?

- Opsporen zwakke plekken
- Toegang krijgen individuele gegevens

Doel

- Stelen geld
- Aankopen doen op uw rekening
- Losgeld
- Bestanden
  - Blokkeren
  - Verwijderen
  - beschadigen

Wachtwoorden hacken :
het gebruik van eenvoudige algoritmen om verschillende combinaties van letters, cijfers en symbolen te genereren, om wachtwoord combinaties te identificeren.

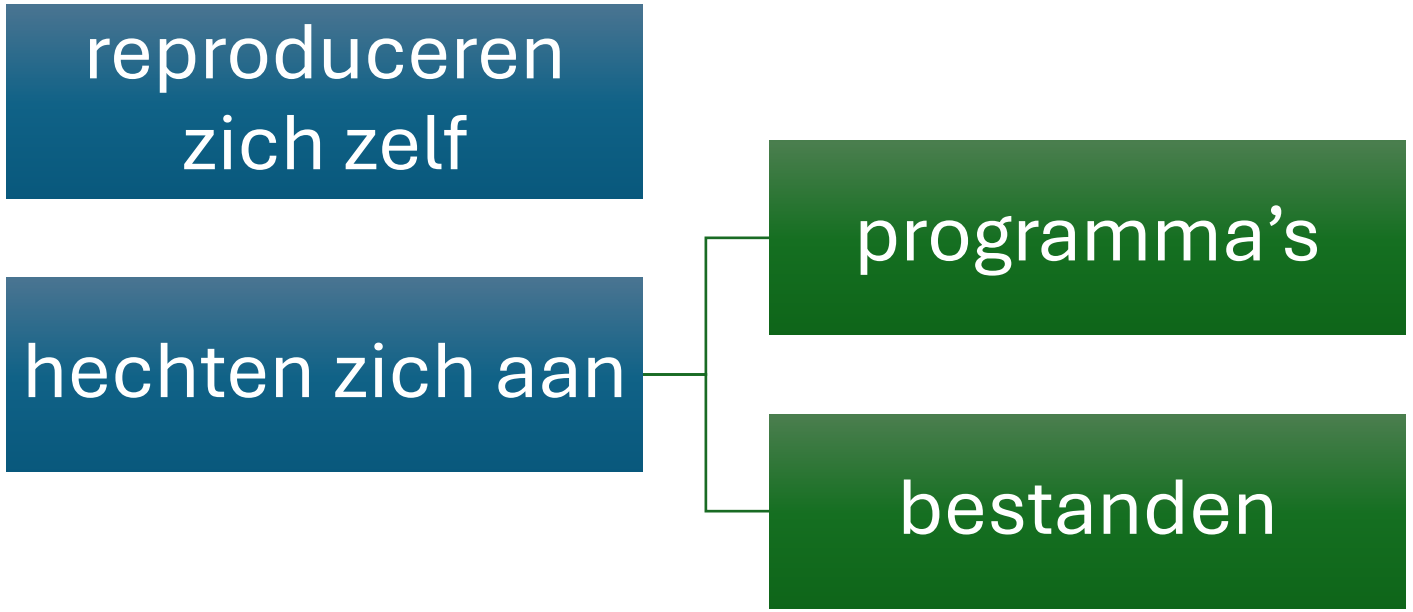
QUISHING ==

SCANT EEN QR-CODE

CLONE PHISHING

LEGITIEME EMAIL KOPIEREN EN WIJZIGEN

COMPUTERVIRUSSEN



URL -PHISHING

FRAUDEUR

- VERBERGT HET WEBADRES
- JE KAN HET WEBADRES NIET LEZEN
- GEBRUIKT EEN LINK VERKORTER
- FOUT GESPELDE NAAM VAN MERKEN / INSTELLINGEN
- OP ELKAAR GELIJKENDE LETTERS : AMAZON.COM
-  ANAZON.COM

SPOOFING

- FRAUDEUR
  - GEBRUIKT VALS EMAILADRES
  - VRAAGT OM OP LINK TE KLIKKEN
  - IN TE LOGGEN OP EEN WEBSITE
  - ACTIE TE ONDERNEMEN/ BESTANDEN DELEN

ADWARE

- Ongewenste advertenties
- Pop ups


TROJAANSPAARD
NET ALS LEGITIEME SOFTWARE MAAR BEVAT VIRUS

Waarover gaan we het hebben vandaag?

- Helpdeskfraude met Anita
- Valse QR-codes uit Brugge
- Kredietkaartfraude tot mijn eigen grote spijt

We gaan beginnen met **helpdeskfraude**

“Binnen vijf minuten stond er iemand aan mijn deur om alles op te halen”: Anita (85) verloor duizenden euro’s spaargeld aan oplichters

Anita Martens kreeg wel vaker verdachte mails of telefoontjes en begrijpt niet waarom ze zich nu zo in de luren liet leggen. — © jof

ZULTE - **Anita Martens (85) uit Zulte werd afgelopen weekend slachtoffer van internetoplichters. Ze verloor duizenden euro’s spaargeld en gaf nietsvermoedend ook haar laptop, gsm en wat juwelen mee. “Ik kan nog altijd niet vatten waarom ik dat gedaan heb”, zucht Anita. “Ik wil vooral anderen waarschuwen zodat hen niet hetzelfde overkomt.”**

Jonathan Folens

Vrijdag 30 mei 2025 om 09:17

“Ik kan nog altijd niet vatten waarom ik dat gedaan heb”, zucht Anita. “Ik wil vooral anderen waarschuwen zodat hen niet hetzelfde overkomt.”

Wat zegt Anita:

“Hij sprak perfect Nederlands en zei dat mijn geld plots in Spanje zat”, begint Anita. “Ik moest mijn bankapplicatie openen en van alles doen met mijn bankkaart en kaartlezer.”

“Hij bleef maar praten en praten, ik kon er geen woord tussen krijgen. Ik begreep het allemaal niet goed.”

“Ik kan nog altijd niet vatten waarom ik dat allemaal gedaan heb. Die man aan de telefoon bleef maar ratelen, ik was precies verdoofd.”

Welke vormen kennen we?

- Bank belt, geld verdwijnt, rap rap, oei oei, we gaan u helpen!
- Microsoft belt, computer kapot, rap rap, oei oei, we gaan u helpen!
- Google belt …
- CardStop belt …

En altijd is het van rap rap, oei oei, we gaan u helpen

PHISHING (email)— SMISHING (sms)
HOE HERKENNEN ?

TAAL : kaduuk taalgebruik, spellingsfouten, rare leestekens, in een andere taal dan deze die je gewoonlijk gebruikt in uw corresponderen…

RAAR : ongewone verzoeken (vriend in geldnood ?), aanmaning tot betaling, je bent uitverkoren of hebt een prijs gewonnen reden : je kocht niets, je verwacht geen pakje, je bent geen klant bij de afzender (bank, verzekeringsmaatschappij…)…

DRINGEND EN DREIGEND : onmiddellijke actie gevraagd, u loopt een fantastische prijs mis, dreigen met boetes of gerechtelijke vervolging, afsluiten van rekeningen of verzekering, blokkeren van betaalkaarten, pakje wordt in beslag genomen, familie in financiële nood…

ONVERWACHT : bericht zonder reden : je kocht niets, je verwacht geen pakje, je bent geen klant bij de afzender (bank, verzekeringsmaatschappij…), je hebt niet om een antwoord gevraagd (energiebedrijven en-consulenten), je hebt recht op een openstaande erfenis…

Nieuwsgierigheid is een slechte raadgever : klik nooit op links of bijlagen, scan geen QR-codes, antwoord niet op een verdachte mail of verdacht bericht…

Paniek of schrik zijn ook slechte raadgevers : iemand die het goed met u voorheeft intimideert u niet, jaagt u geen schrik aan, bedreigt u niet… en zekere de politie, de douane, financiën of justitie niet…

Vertrouw niet op bedrijfs- of agentschapslogo's, of telefoonnummers : huidige technieken maken het mogelijk voor fraudeurs om logo's na te maken die niet te onderscheiden zijn van de echte, "echte" oproepnummers worden nagebootst zelfs met de naam van een echte medewerker…

Naïviteit is gevaarlijk : gratis, geschenken die zomaar uit de lucht vallen, erfenissen uit het buitenland die je te beurt vallen, snel veel geld verdienen…

Let op met sociale media : gooi niet om het even wat op sociale media : alles wat erop komt en met je persoon kan verbonden worden is potentieel voer voor fraudeurs en criminelen…

Ga niet in op de vraag : stort nooit geld ook geen (kleine) vergoedingen, geef geen bankkaartgegevens of persoonlijke informatie door en zeker nooit uw geheime code of uw bank- of kredietkaart of waardevolle objecten, laat nooit toe dat iemand uw scherm deelt, ga niet in op onverwachte verzoeken tot een videogesprek…

Wat valt er op?

	Vroeger	Nu
Taal	Vreemd accent	Zeer welbespraakt
Inhoud	Zeer technisch	Zeer aannemelijk
Timing	Overdag	Vaak ‘s avonds laat
Schade	Geld	Geld, juwelen, electronica
Werkwijze	Op afstand	Ook aan huis
Voorbereiding	Weinig of niets	Goed voorbereid, weten veel

Wat kan je doen?

- Je zou al kunnen beginnen met niet op te nemen, doe ik vaak (sorry!)
- Neem je op, hoor je die “rap rap, oei oei”, haak dan in
- Geloof niet zomaar de nummerherkenning op je toestel (spoofing)
- Vraag om zelf terug te mogen bellen naar het nummer dat je kent
- Vraag eventueel naar je laatste transacties
- Vraag of ze je bankkaartnummer en vervaldatum kunnen vertellen

Hoe had je dat kunnen vermijden?

- Wees voorzichtig met je telefoonnummer te delen
- Wees simpelweg voorzichtig met wat je deelt op sociale media
- … ook met vrienden!
  (want ook die kunnen gehackt zijn)
  en dus komt de info die je “privé” deelde alsnog in handen van vreemden
- Dus ook op vakantie opletten met wat je deelt
- Kortom: je wil niet in een dataset terecht komen

Hoe gaat men te werk?

- Men koopt eerst en vooral software
- Ofwel zit daar al data in, ofwel koopt men ook nog extra data
- “Alle Anita’s uit Zulte tussen 80 en 90 die een hond hebben”
- De software belt je op, automatisch, meerdere keren, tot je opneemt
- De beller spreekt je ofwel zelf toe, of is een computerstem
- De software geeft de nodige details aan om overtuigend te zijn
- De software geeft ook privé details afkomstig van sociale media
- Vertrouwelijk, aannemelijk, verleidelijk, gevaarlijk
- Men steelt zodoende je codes en de rest is kinderspel

Wat kunnen wij als CPA doen?

- Mensen proberen te overtuigen niet zomaar alles te geloven
- Mensen mogen wel degelijk de telefoon negeren
- Mocht er echt iets fout zijn, dan blokkeerde de bank je rekening al
- En eerlijk, als een bank belt is het meestal voor een belegging, toch?

Om dit stukje af te sluiten:

Mocht iemand je op straat aanspreken met een gelijkaardige boodschap van rap rap, oei oei, zou je dan ook meteen je bankkaart afgeven?

Volgende op de agenda zijn de **valse QR codes**

Quishing

- Of op terrastafeltjes
- Laadpalen
- …

Via de valse QR-code kom je op een phishingwebsite terecht.
Foto: stad Brugge

Stad Brugge ontdekt op tijd poging tot oplichting met valse QR-codes op parkeerautomaten

In Brugge is een poging tot fraude via de parkeerautomaten ontdekt. Op 17 automaten was een valse QR-code gekleefd. Die leidde naar een phishingwebsite, waar de gebruikers de gegevens van hun bankkaart moesten invoeren. Gelukkig werd de poging tot oplichting snel ontdekt. Er hebben zich nog geen gedupeerden gemeld.

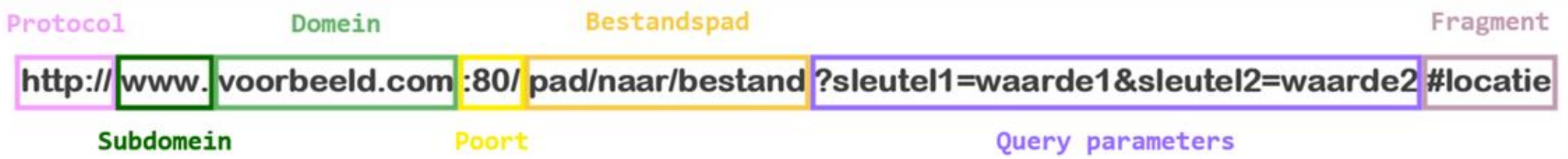
Waar komen die QR-codes vandaan?

- Dat was een uitvindsel om mensen gemakkelijk een link te bezorgen
- Lees: gemakkelijk
- Lees ook: dus ideaal om ook een stoute link te bezorgen

Waar komen die QR-codes vandaan?

- Niet altijd evident om snel even op dat kleine scherm van je telefoon te zien naar waar die link verwijst
- Links herkennen blijft dus wel handige kennis en kunde
- Ware dat nu toch wel het meest gehate stuk van de CPA opleiding ☺

De anatomie van een internetadres



HTTP vs. HTTPS

- Het zogenaamde protocol
- Versleutelde communicatie of niet

- Kan misleidend zijn want je kan ook versleuteld communiceren met een crimineel

ANALYSE VAN EEN INTERNETADRES

http= hypertext transfert protocol
geen bescherming van de gegevens

https= hypertext transfert protocol
bescherming van gevoelige informatie (versleuteld)

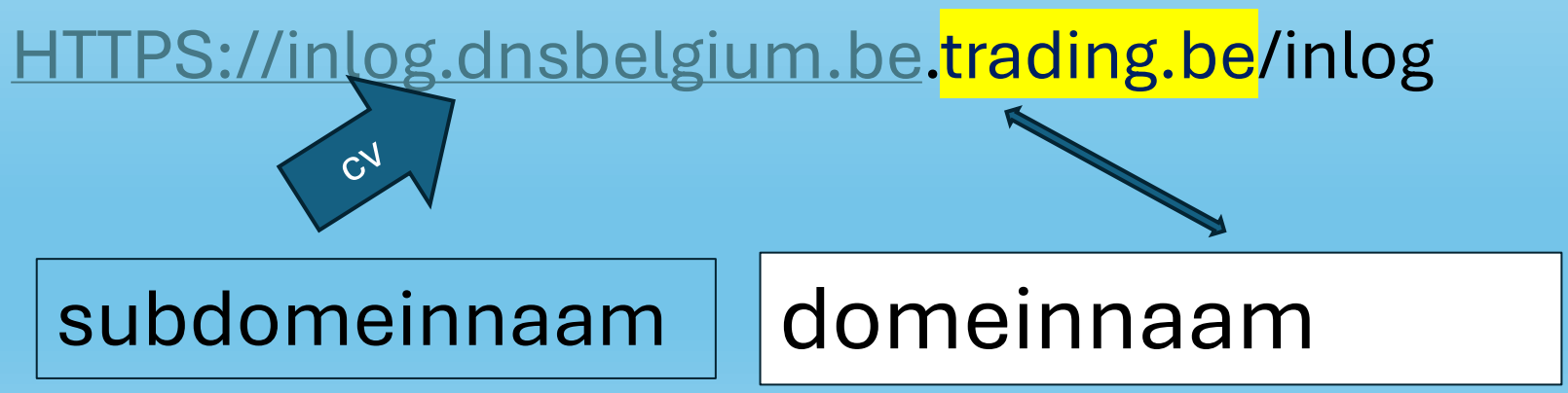
VPN= virtueel privaat network

VPN betekenis

1. **Versleuteling**
    1. Wordt onleesbaar voor derden
2. **IP – adres maskeren**
    1. Eigen IP-adres wordt vervangen door IP-adres van de VPN-server
3. **Veilige tunnel**:
    1. privé doorgang
    2. Beschermt gegevens tegen hackers
    3. Voorkomen online tracking

HOE VOORKOMEN?

- BESTUDEER HET WEBADRES
- BEWEEG CURSOR OVER DE LINK
- MOBIEL TOESTEL/ DRUK LANG OP DE LINK



Zoek de derde slash!

https://www.bin-plp.be/algemeen/wat-doen-we/benno-gaat-op-pensioen/maar-zijn-vrouw-weet-het-nog-niet/

Alles na die derde slash, is overtollige ballast, heeft niets met de domeinnaam te maken

Het lange adres van hierboven kunnen we maw reduceren tot:

https://www.bin-plp.be/

Zoek de derde slash!

https://www.bin-plp.be/

De echte domeinnaam van de site staat nu vlaak voor die derde slash:

bin-plp.be

Zoek de derde slash!

https://www.bin-plp.be.phishingsite.com/

En als we datzelfde nu eens toepassen op een phishinglink, dan zien we dit:

https://www.bin-plp.be.phishingsite.com/

Domeinnamen

- bol.com
- Vrt.be
- Sporza.be
- Limburg.be
- itsme-id.com
- oxfamwereldwinkels.be
- Amazon.com

Voorbeeld

Ga naar messenslijper via google search

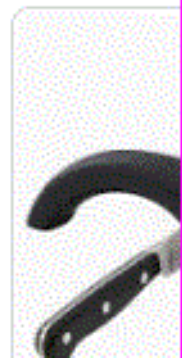
MESSENSLIJPER

Gesponsord









MESSENSLIJPER - Google Zoek

Nieuw tabblad

Nieuw tabblad

google.com/search?q=

Nieuw tabblad | Apps | Mede | edewerkers | OC... | Alle bookmarks

Google

MESSENSLIJPER

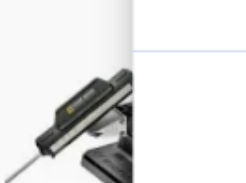
Alle | Afbeeldingen | Producte | ools

Tormek | Wüsthof | Fis

Resultaten voor **Mollem, Asse**

Gesponsord

HORL 3 -



Work Sharp

Graef Diamant

ChefsChoice

Hatori Diamond

RollEdge |

Messenslijper

Chef

Emoji's Win+Periode

Versturen naar je apparaten

Ongedaan maken Ctrl+Z

Knippen Ctrl+X

Kopiëren Ctrl+C

Plakken Ctrl+V

Plakken en gaan

Verwijderen

Alles selecteren Ctrl+A

Zoekmachines en Site Search beheren

Altijd volledige URL's bekijken

Typ hier om te zoeken

NLD 18:38 19/09/2025

PER - Google Zoek

Nieuw tabblad

Nieuw tabblad

https://www.google.com/search?q=MESSENSLIJPER&rlz=1C1GCEA_enBE939BE939

lad Apps Medewerkers | OC... Apps Account en beveiligi... Medewerke

MESSENSLIJPER

Alle Afbeeldingen Producten Productsites Video's Vacatures Vacaturesites Meer Tools

Tormek Wüsthof Fiskars ZWILLING Work Sharp

Resultaten voor **Mollem, Asse** · Regio kiezen

MESSENSLIJPER - Google Zoek

Nieuw tabblad

Nieuw tabblad

https://www.google.com/search?q=MESSENSLIJPER&rlz=1C1GCEA_enBE939BE9...

Nieuw tabblad | Apps | Medewerkers | OC... | Apps | A | Alle bookmarks

klik hierop om uw locatie al dan niet te delen

Locatietoegang toegestaan

Deze site heeft toegang tot je locatie.

- (•) Toestaan dat deze site toegang tot je locatie blijft houden
- ( ) Toegang tot je locatie altijd blokkeren voor https://www.google.com

Beheren | Klaar

Google

MESSENSLIJPER

Alle | Afbeeldingen | Producten | Productsites | Video's | Vacatures

Tormek | Wüsthof | Fiskars | ZWILLING | Work Sharp

Resultaten voor **Mollem, Asse** · Regio kiezen

Gesponsord

HORL 3 -

Work Sharp

Graef Diamant

Chef'sChoice

Hatori Diamond

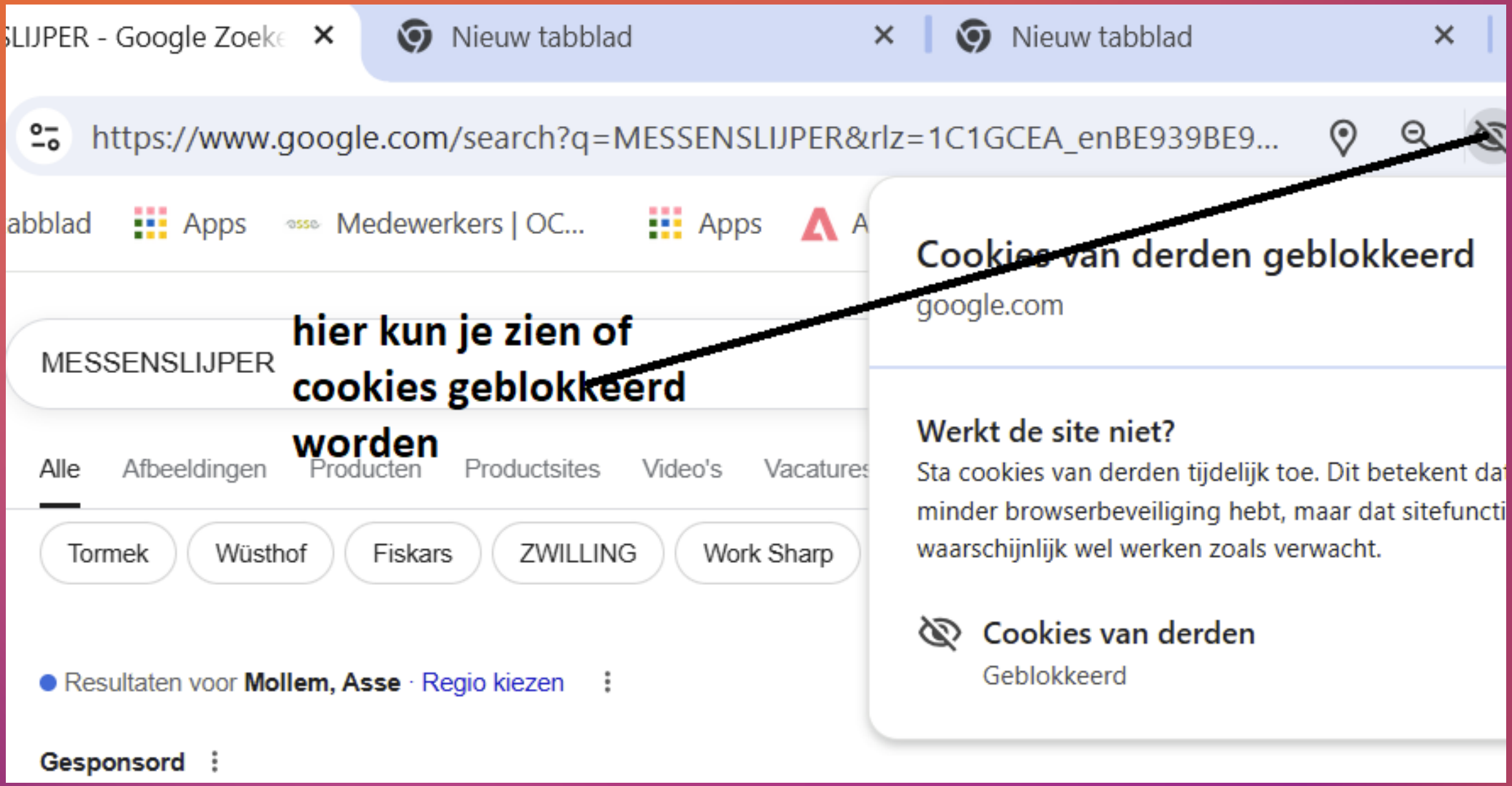
RollEdge |

Messenslijper

Chef

Typ hier om te zoeken

NLD 18:49 19/09/2025


LIJPER - Google Zoek
Nieuw tabblad
Nieuw tabblad
https://www.google.com/search?q=MESSENSLIJPER&rlz=1C1GCEA_enBE939BE9...
abblad
Apps
Medewerkers | OC...
Apps
MESSENSLIJPER
hier kun je zien of cookies geblokkeerd worden
Alle
Afbeeldingen
Producten
Productsites
Video's
Vacatures
Tormek
Wüsthof
Fiskars
ZWILLING
Work Sharp
Resultaten voor Mollem, Asse · Regio kiezen
Gesponsord
Cookies van derden geblokkeerd
google.com
Werkt de site niet?
Sta cookies van derden tijdelijk toe. Dit betekent dat
minder browserbeveiliging hebt, maar dat sitefuncti
waarschijnlijk wel werken zoals verwacht.
Cookies van derden
Geblokkeerd

Gratis e-mail checker

Controleer uw e-mail gratis met onze Free Email Checker. Test hoe Bouncer werkt en ervaar de kracht van Bouncer, in real time! Geen registratie nodig.

Enter email adress that **you want to verify**

info@lambertconstruct.be

Verify

You have 4 free verifications

Sign up and get 100 verifications for

Email checker usebouncer

Enter email adress that **you want to verify**

Email*

Verify

info@lambertconstruct.be

You should not try to send emails to this address, the current email address is disabled or does not exist anymore.

Status	Reason
Undeliverable	REJECTED EMAIL

Domain

Name	lambertconstruct.be
Accept all	no
Disposable	no
Free	no

Account

Role	yes
Disabled	yes
Full mailbox	no

URL-shortner
URL-VERKORTER

Link naar de kapper

- Zogenaamde URL shorteners:
  - bit.ly
  - t.co
  - youtu.be
- Let op: dit was vroeger heel nobel en handig
- Tegenwoordig is dit vaak een handige manier om een link naar een phishingsite te verbergen achter een mooie korte link

Voorbeeld korte url’s

http://bit.ly/hetfeestjevannico → www.nicojoos.be/evenementen/feestje/schrijfjein.php

http://bit.ly/ikbeneensloeber → www.phishingsite.oplichting.be/jegeldkwijt

Conclusie:

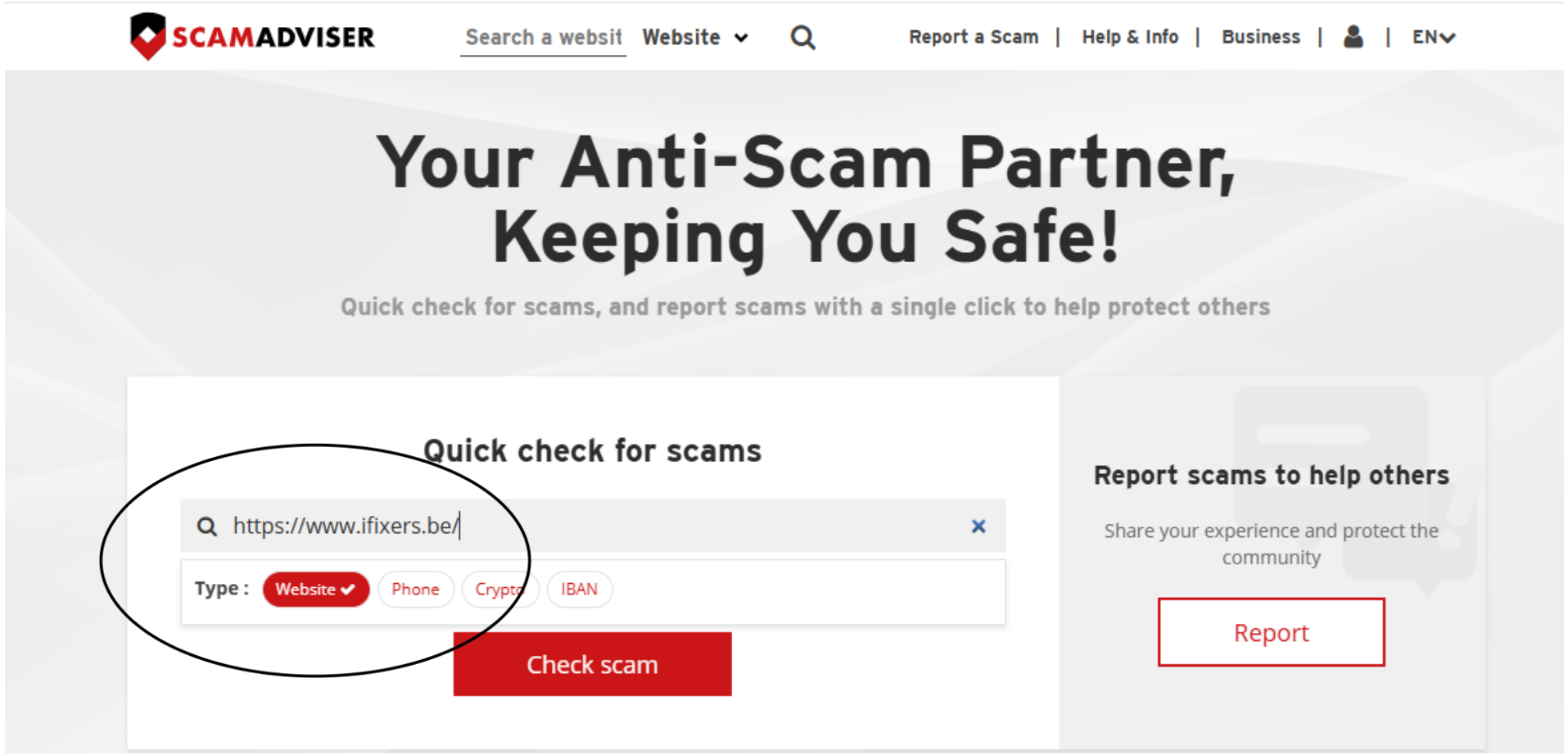
Een QR-code is een grafische en fancy evolutie van zo’n url shortener om een link te bezorgen

Check de link met scamadvisor

Ga naar

https://www.scamadviser.com/

VOORBEELD


SCAMADVISER
Search a websit
Website
Report a Scam | Help & Info | Business | EN
Your Anti-Scam Partner, Keeping You Safe!
Quick check for scams, and report scams with a single click to help protect others
Quick check for scams
https://www.ifixers.be/
Type :
Website
Phone
Crypto
IBAN
Check scam
Report scams to help others
Share your experience and protect the community
Report

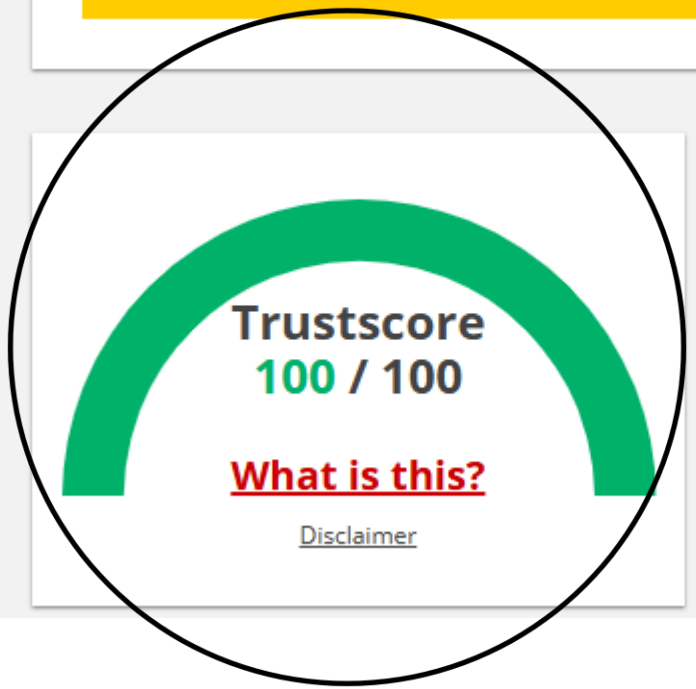
SCAMADVISER Search a websi Website Report a Scam | Help & Info | Business | | EN

www.ifixers.be Reviews

Visit the site

is www.ifixers.be legit or a scam?

Scanning in progress, check back again later

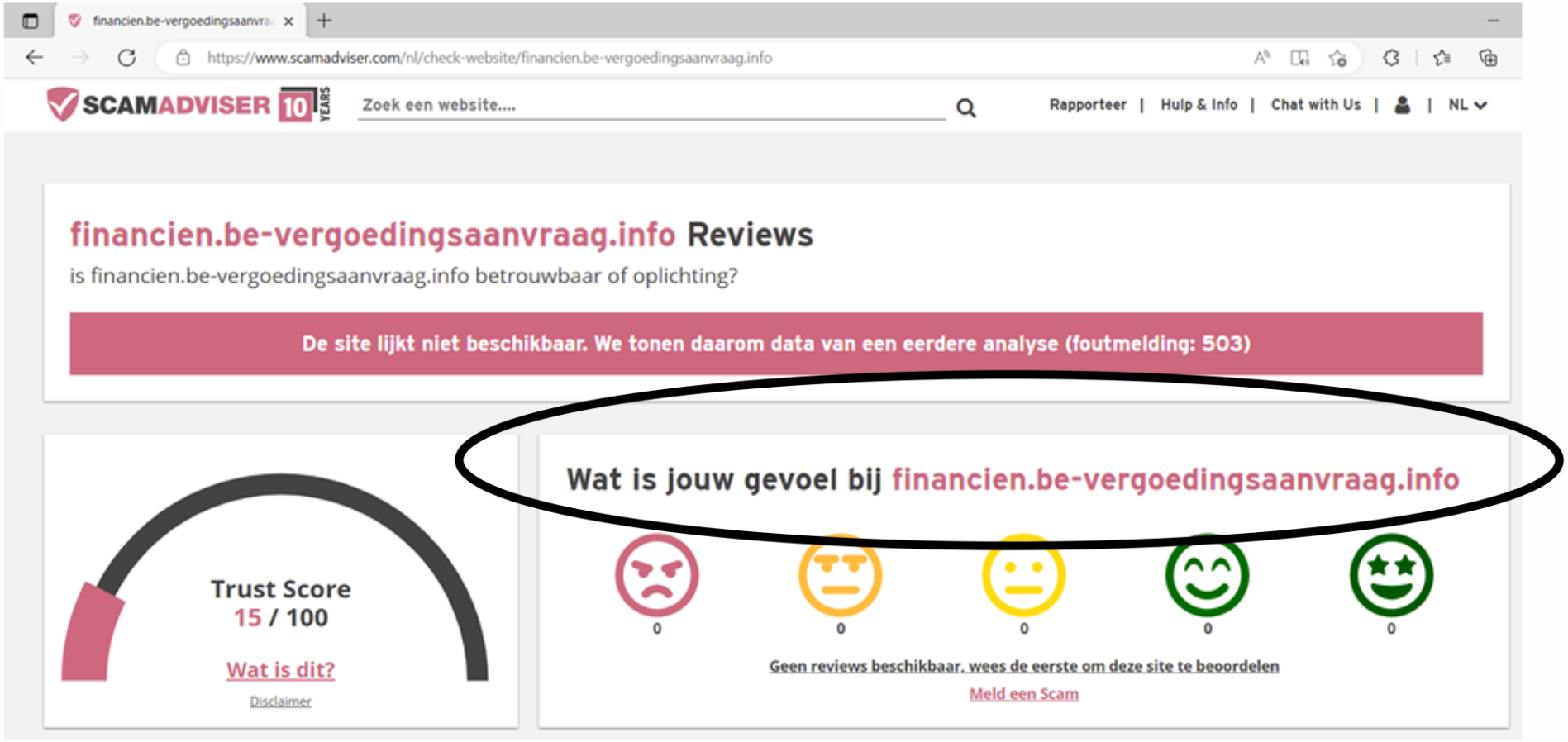


Your Go-To Tools for Online Safety

Protect yourself online with our expert-vetted tools and the official ScamAdviser App

1. **ScamAdviser App - iOS** : Your personal scam detector, on the go! Check website safety, report scams, and get instant alerts. Available on iOS
2. **ScamAdviser App - Android** : Your personal scam detector, on the go! Check website safety, report scams, and get instant alerts. Available on Android.

Check de link



Zijn alle QR codes dan potentieel slecht?

- Ja maar …
- Een QR code in het openbaar: wees voorzichtig
  - Bvb de parkeermeters in Brugge
  - Maar ook op de terrastafeltjes, bvb in Gent (dus ook op vakantie!)
  - Op de laadpaal
  - Op een affiche, flyer, enz

Moet je opletten bij bank app QR codes?

- Nee maar
- Let wel dat die van een betrouwbare bron komen
  - En kijk ook naar de bevestiging op je eigen telefoon (bedrag, begunstigde)
  - Van wie komt die QR code? Je huisarts, je beste vriendin, 2dehands koper?

Installeer geen apps via een QR-code

- QR codes kunnen naar een app verwijzen
- Helaas is de app store geen garantie meer zoals vroeger
- Installeer daarom geen apps via een QR code
- Zoek de app zelf op en verifieer de uitgever

Quishing = Phishing

- Phishing als in “vissen naar” zit verborgen achter die foute QR code

- De gevaren zijn:
  - Dat je op een valse site terecht komt waar men info wil ontfutselen
  - Dat je een valse app installeert (malware)
  - Dat je een paswoord vrijgeeft
  - Dat men identiteitsfraude kan plegen met de verkregen info
  - Dat je een betaling doet of abonnement neemt bij een malafide partij

Hoe te beschermen?

- Scan enkel QR codes waarvan je de uitgever kent
- Inspecteer een QR code ook visueel (Zeker als je parkeert in Brugge!)
- Bekijk de link waar je naartoe wordt gestuurd
- Deel nooit info tenzij je zeker bent van de site
- Hou je eigen toestel steeds up to date

Ik beken

Ik ben een beetje onvoorzichtig geweest

Situatieschets

- Buitenland
- Cyber security event
- UK
- Met de auto
- Een beetje laat, druk verkeer
- En ze rijden daar links!
- Parking volzet
- Dan maar een andere parking
- De stress loopt op
- Lokale parkeerapp moeten installeren
- En wat een geluk dat ik een VISA kaart had!

1 maand later …

FACEBK *UNF7W3GN22 6 650-54348…	-1,90	
Zaterdag 22 juni 2024	EUR	
FACEBK *M5L324CN22 6 650-543480…	-1,90	
Zaterdag 22 juni 2024	EUR	
FACEBK *Y8LWZ4CP22 6 650-543480…	-1,35	
Zaterdag 22 juni 2024	EUR	
FACEBK *RNLWH58P22 6 650-543480…	-1,90	
Zaterdag 22 juni 2024	EUR	
FACEBK *7LBWH58P22 6 650-543480…	-1,90	
Zaterdag 22 juni 2024	EUR	
FACEBK *FYZ224CN22 6 650-543480…	-1,90	
Zaterdag 22 juni 2024	EUR	
FACEBK *LBMFQ3UN22 6 650-54348…	-1,38	
Vrijdag 21 juni 2024	EUR	

En wat deed de bank?

Die belde niet

Die mailde niet

Die blokkeerde mijn kaart (tijdelijk)

En stuurde mij een bericht in de bank app

Met de vraag contact op te nemen

Wat bleek

- Het ging niet om Facebook transacties
- Had niets met Facebook te maken
- Dan had er zelfs “META” moeten staan
- Het was fraude
- Omdat het IT systeem achter de parkeerapp gehackt was
- Data werd gestolen, verkocht, misbruikt
- En dus ook mijn VISA kaart nummer
- En daarmee werden kleine bedragen afgehaald
- Klein genoeg om onder de radar te blijven

Welke vormen bestaan er

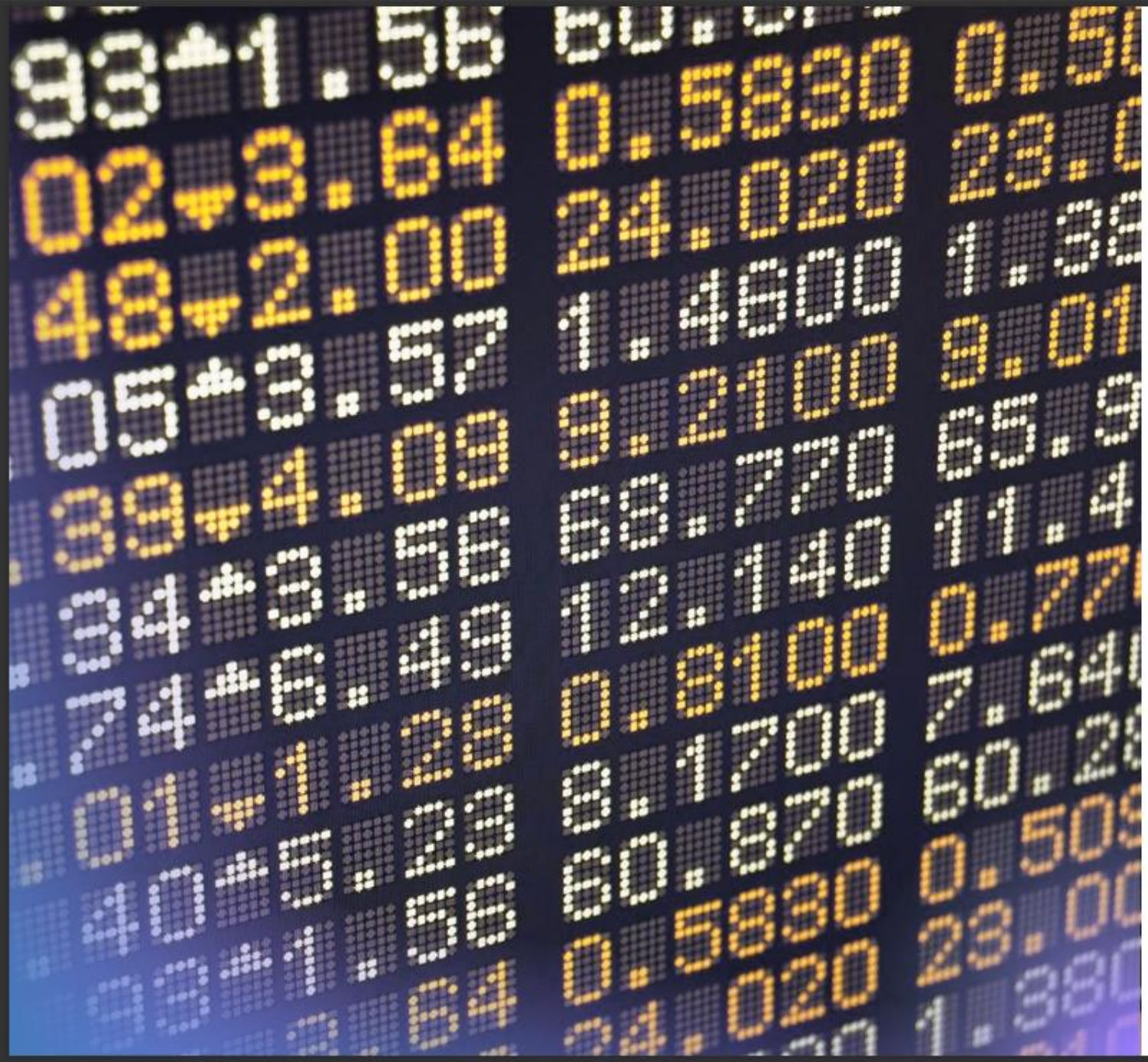
- Met fysieke kaart: gestolen of gekopieerd
- Zonder de fysieke kaart: data gestolen
- Account werd overgenomen
- Kaart werd verkregen adhv gestolen identiteitsgegevens
- Kaart werd gekopieerd via een terminal bvb
- Phishing of malware om kaartgegevens te ontfutselen

Hoe te vermijden

- Hou je account regelmatig in de gaten
- Gebruik sterke wachtwoorden, uniek, multifactor
- Hou je fysieke kaart goed bij
- Hou het veilig bij het online shoppen
- Gebruik bvb geen publieke wifi
- Let erop dat je https verbindingen gebruikt
- Let op phishing
- Gebruik de anti fraude functionaliteiten van je bank
- Zorg dat je bank steeds je contactgegevens heft
- Bekijk je afrekeningen steeds goed
- Neem de juiste stappen bij vermoeden van fraude

Nog een beetje advies

- Wees steeds voorzichtig waar je je kaartnummer achterlaat
- Sla je kaartgegevens niet op in een webshop
- Geef je kaart niet zomaar mee met een vreemde
- Schakel enkel de landen in die je ook effectief nodig hebt
- Zet je limiet zo laag mogelijk
- En verhoog je limiet slechts tijdelijk indien nodig (via de app)
- Gebruik tijdelijke of eenmalige virtuele kaarten



Geklikt, betaald, bedrogen, en dan?

- Rustig blijven
- Cardstop
- Bank
- Politie
- Meldpunt

Card Stop

+32(0)78 170 170

- **Je kan op voorhand een lijst aanmaken van de officiële websites en telefoonnummers van de instanties waarmee jij te maken hebt**

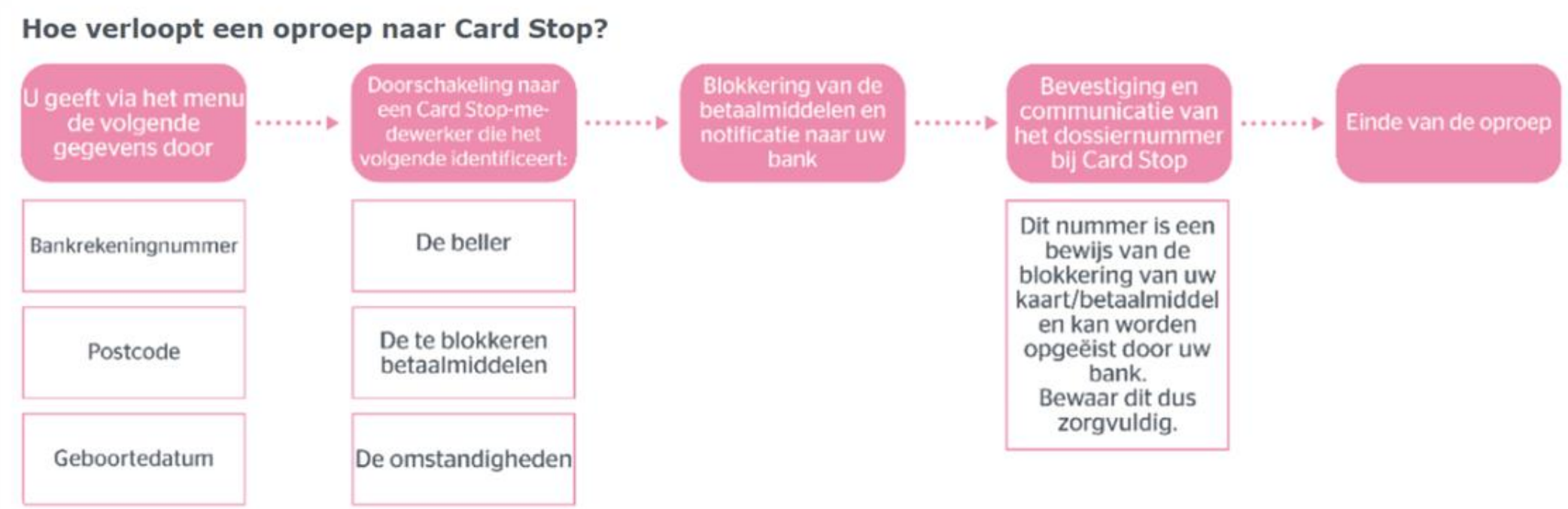
- **Card Stop**

- **Bel naar het nummer +32 (0)78 170 170.**
- **Je kiest de taal waarin je het gesprek wil voeren.**
- **Een stemcomputer zal je vragen om je bankrekening of kaartnummer in te toetsen.**
- **Je wordt vervolgens doorverbonden met een van onze Card Stop assistenten die alle verdere stappen onderneemt om je betaalmiddelen te blokkeren.**
- **Tot slot zal de stemcomputer je informatie geven over de vervanging van je betaalmiddel en zal je de referentie van dit gesprek krijgen. Noteer deze zorgvuldig. Deze kan je worden opgevraagd door je bank of de politie bij aangifte.**

- **Vergeet niet je rekening te blokkeren rechtstreeks via de bank!**

Card Stop

PROCEDURE



Safe On Web .be

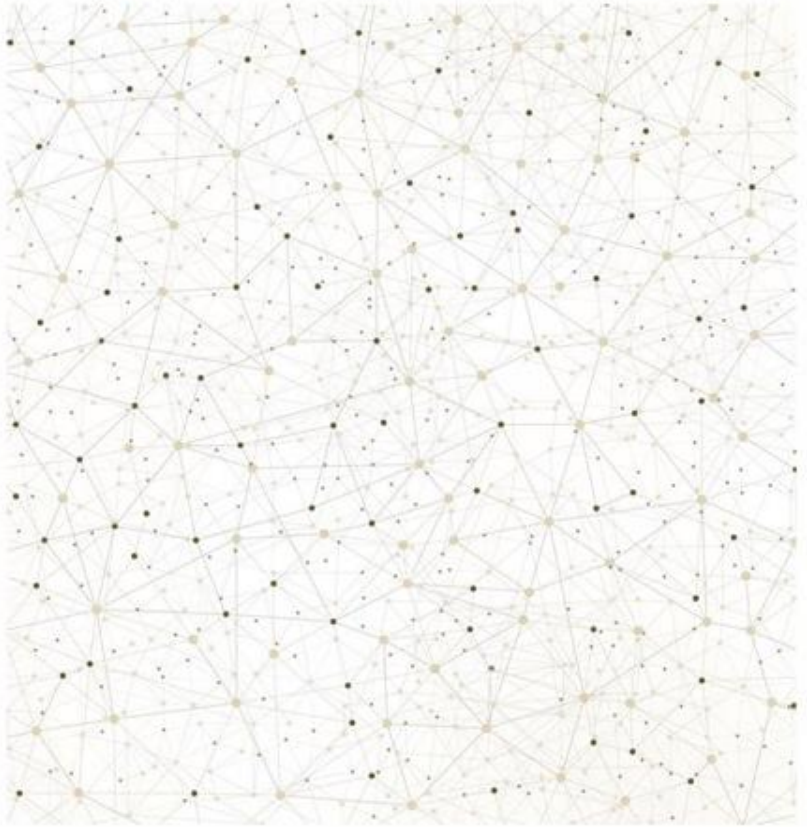
- SafeOnWeb: https://www.safeonweb.be/nl

- Stuur een phishingbericht door naar verdacht@safeonweb.be.
- Ook screenshots van verdachte SMS'jes kunnen hiernaar doorgestuurd worden
- Ook QR codes

- Zij controleren de links en bijlages van deze berichten.
- Verdachte links laten zij blokkeren.

- Samenwerking met de grote Belgische providers
- Snelheid is belangrijk!
- Vorig jaar 10 miljoen mails!

- Het gaat om de links, niet altijd de sites …
- Hoe meer, hoe beter. Een beetje de coyote of waze van de flitscontroles.



ENGLISH NEDERLANDS FRANÇAIS DEUTCH

Other official information and services: www.belgium.be .be

Warning
Malicious website.

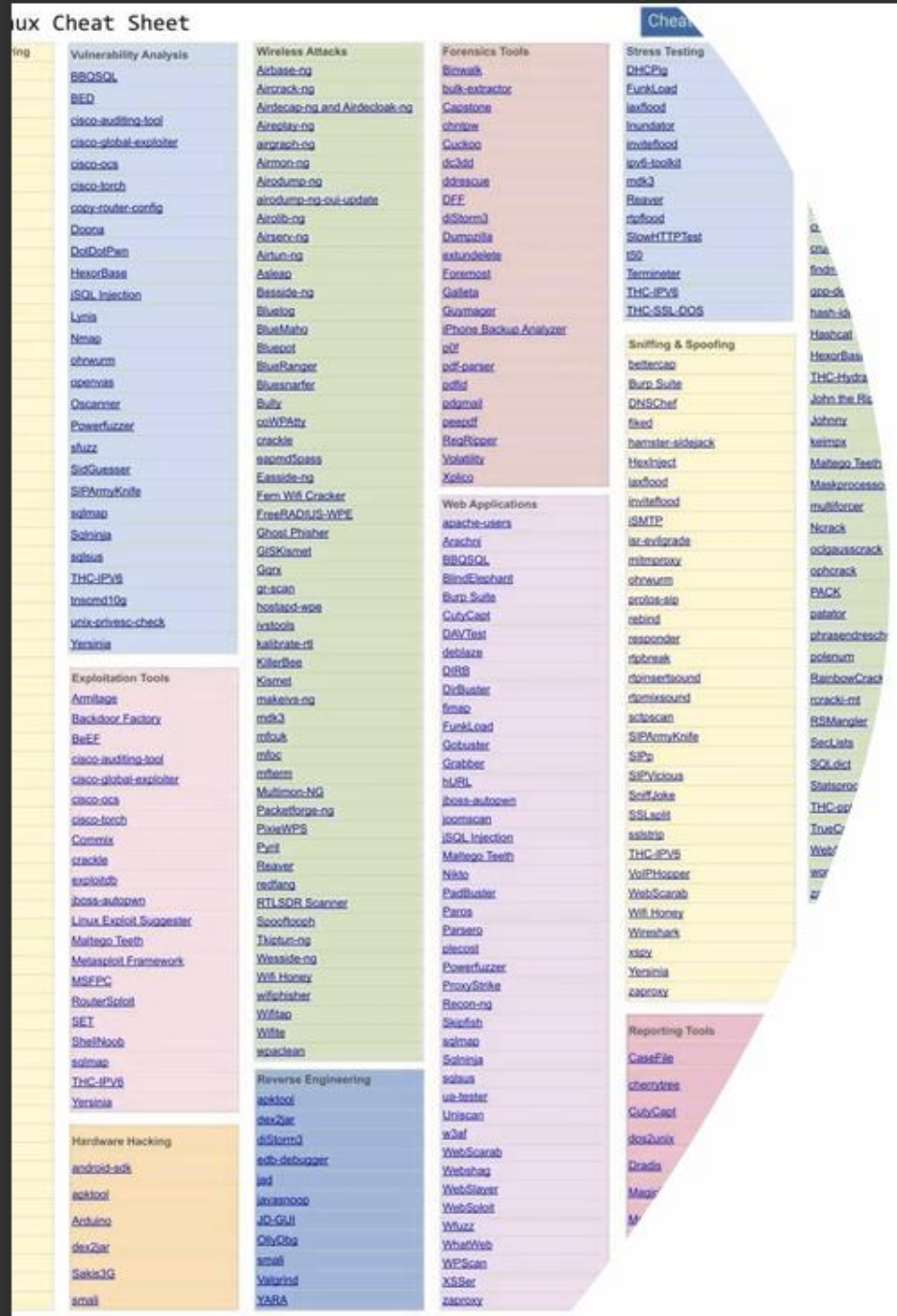
The website you want to visit is probably malicious.

Learn more

CENTRE FOR
CYBERSECURITY
BELGIUM

- https://www.cyberpreventie.be/
- **De website bevat actuele informatie, campagnes, preventiefilmpjes en educatieve pakketten (op initiatief van WVL4)**

- https://www.cybersimpel.be/nl
- **Naast praktisch advies en tips zijn er ook lespakketten terug te vinden: https://www.cybersimpel.be/nl/toolkit (op initiatief van Google en Test-Aankoop)**

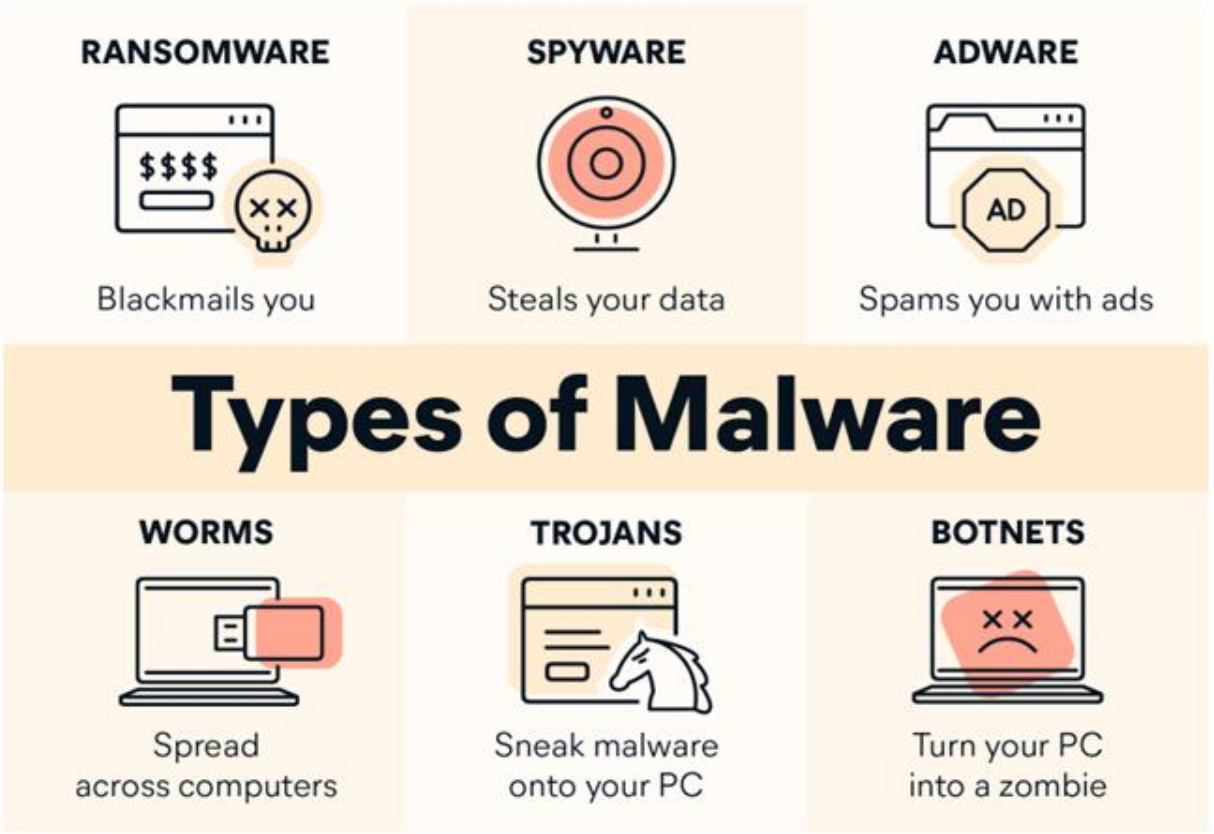


De standaard gereedschapskist voor een hacker is gratis en publiek te downloaden en bevat minstens 300 tools

Tweestapsverificatie is het meest krachtige instrument dat we hebben om een account te beschermen

10 eenvoudige tips zijn voldoende om 99% van de online fraude gevallen te voorkomen

1 op de 10 toestellen, verbonden met het internet, bevat malware



Veiligheid is een mythe

Weerbaarheid is cruciaal

Wat kunnen wij zelf doen?

1. COMPLEXE WACHTWOORDEN

Lettertekens >	6	7	8	9
Alleen kleine letters	0 s	2 s	50 s	20 min
Kleine letters en hoofdletters	5 s	4 min	3,5 uur	ca. 8 dagen
Kleine letters, hoofdletters, getallen	13 s	14 min	ca. 15 uur	ca. 40 dagen
Ook leestekens	3 min	ca. 5 uur	ca. 18 dagen	ca. 5 jaar

Wat kunnen wij zelf doen?

2. **TWEESTAPSVERIFICATIE**

- U LOGT IN
- U KRIJGT EEN CODE VIA EMAIL OF SMS
- DIE U VERVOLGENS GEBRUIKT
- OM DEFINITIEF GEGEVENS UIT TE WISSELEN VIA HET HTTPS-PROTOCOL

Wat kunnen wij zelf doen?

3. **REGELMATIG UW SYSTEEM UPDATEN** ZOWEL

- PC
- SMARTPHONE (minstens 1X per maand volledig uitschakelen)

GEBEURT AUTOMATISCH OM AANPASSINGEN

- HACKING
- MALWARE
- VIRUSSEN

TE ONDERSCHEPPEN

Wat kunnen wij zelf doen?

4.**ANTIVIRUS**

Windows 11 heeft eigen antivirus

supplementaire dure antivirus is overbodig

Vertraagt uw systeem

4.1 ZET UW FIREWALL AAN

- WIINDOWS 10
- NIET MEER ONDERSTEUND VANAF OKTOBER

Wat kunnen wij zelf doen?

5. **OPLETTEN MET DOWNLOADEN VAN APPLICATIES**

- GOOGLE PLAY STORE
- AMAZONE APP STORE
- SAMSUNG GALAXY STORE
- HUWAEI APP GALERY
- F.DROID

Wat kunnen wij zelf doen?

6. **CONTROLEREN EN ANALYSEREN VAN WEBSITES**

ZIE VOORGAANDE DIA’S

Wat kunnen wij zelf doen?

7.**ONGEVRAAGDE HELPDESKMEDEWERKERS**

NOOIT OP INGAAN !!!

Wat kunnen wij zelf doen?

8. SOCIALE MEDIA

- ZO WEINIG MOGELIJK PRIVATE GEGEVENS

Wat kunnen wij zelf doen?

9.OPENBARE WIFI

- GEVAAR VOOR HACKERS
- MELDING
- UW TELEFOON OF PC IS ZICHTBAAR VOOR ANDERE GEBRUIKERS

Casussen

uit het dagelijks internet-verkeer…

Doccle is een online platform waar je documenten van verschillende bedrijven, zoals facturen en loonbrieven, veilig en centraal kunt ontvangen, beheren en betalen. Het is een digitale brievenbus die helpt om je administratie te organiseren en te vereenvoudigen. **Doccle gebruikt het webdomein doccle.be**

Doccle is een initiatief van CM, Telenet en Acerta, en inmiddels werken er meer dan 135 bedrijven mee. Het is een Belgisch platform met meer dan 2,5 miljoen gebruikers

boifdoeou@skynet.be

Van: **Mijn doccle**
Onderwerp: U heeft een openstaande opdracht
Datum: 7 juli 2025 om 00:51
Aan:

Hallo,

Je hebt via Doccle een nieuw document van **KBC** ontvangen.
Ga naar Doccle om met het document aan de slag te gaan.

dè hamvraag :
ben je wel klant bij de KBC ???

U heeft een openstaande opdracht

Ga naar Doccle

niet aanklikken, wel even op de link gaan staan, dan zie je de (valse) url waar je naar omgeleid wordt : gkldfghhgeuijjnie.com

Met vriendelijke groeten,
Het Doccle-team

Ontdek onze apps • Contacteer ons • Lees onze blog

© 2025 Doccle

niet aanklikken :
ontdek de blog niet, contacteren ze niet, lees de blog niet !!!
de getoonde link wordt omgeleid naar valse websites

Van: Central Rede
▸ centralrede@lopes.com.br
Onderwerp: ARGENTA : Herinnering: Uw kaartlezer wer
niet meer
Datum: 8 jun 2025, 19:23:32
Aan:

Herinnering: Vraag uw nieuwe kaartlezer aan

Beste klant,

U heeft nog geen nieuwe kaartlezer aangevraagd. Vanaf **08 mei 2025** werkt uw huidige kaartlezer niet meer voor bepaalde toepassingen die verouderde modellen gebruiken.

Vraag voor die datum een nieuwe kaartlezer aan indien u merkt dat sommige functies niet meer beschikbaar zijn. Daarna kost dit **€15,95,** wat enke
een vervangtoestel.

Kaartlezer aanvrage

Heeft u al een nieuwe kaartlezer ontvangen? Dan mag u dit bericht negeren.

Voor vragen kunt u terecht op www.argenta.be of bel ons tijdens kantooruren.

© 2025 Argenta Bank – Dit is een automatisch verzonden e-mail. Bezoek www.argenta.be voor meer i

afzender is niet “@argenta.be”

verzonden op een zondag tussen 7 en 8 ’s avonds !!!

onverwacht : de bank heeft mij daarover niets verteld, en ik heb geen eerste bericht ontvangen !

dringend ??? vanaf 8 mei, maar mail dateert van 8 juni 😮 🐟

dreigement : niet reageren kost geld of veroorzaakt problemen

niet aanklikken : alle getoonde links worden omgeleid naar valse websites

Argenta zal nooit e-mails versturen met een link om aan te melden op een website.

Van: **De watergroep** kankanli@dattymaterials.com
Onderwerp: Mogelijk recht op sociale compensatie voor water – check het even
Datum: 10 juni 2025 om 00:53
Aan: vanborsel ongenae@skynet.be

kankali@dattymaterials.com

afzender is niet “de watergroep”

’s nachts verzonden (andere tijdszone) ???

💧 Heb je recht op een sociale compensatie voor je waterfactuur?

meestal kent de watergroep dit automatisch toe

Beste klant,

Wist je dat je misschien recht hebt op een **sociale compensatie** voor je waterfactuur?

De Watergroep helpt klanten door een deel van de kosten voor drinkwater en afvalwater te verlagen. Deze compensatie is bedoeld voor onze klanten..

Wat moet ik doen?

1. Bekijk de voorwaarden
2. Bij goedkeuring krijg je automatisch korting op je waterfactuur

Bekijk je mogelijkheden

ga naar zelf naar de website www.dewatergroep.be om te weten wat de voorwaarden en mogelijkheden zijn in in plaats van door de klikken.

Gebruik het 078 nummer niet, het is omgeleid en frauduleus
Het algemene contactnummer van de Watergroep is 02 238 96 99

Hulp nodig?
Onze klantendienst helpt je graag verder:
📞 078 35 35 99
✉️ klantenservice@dewatergroep.be

Met vriendelijke groeten,
Het team van De Watergroep

Volg ons op Facebook | LinkedIn

Privacyverklaring | Mijn Watergroep

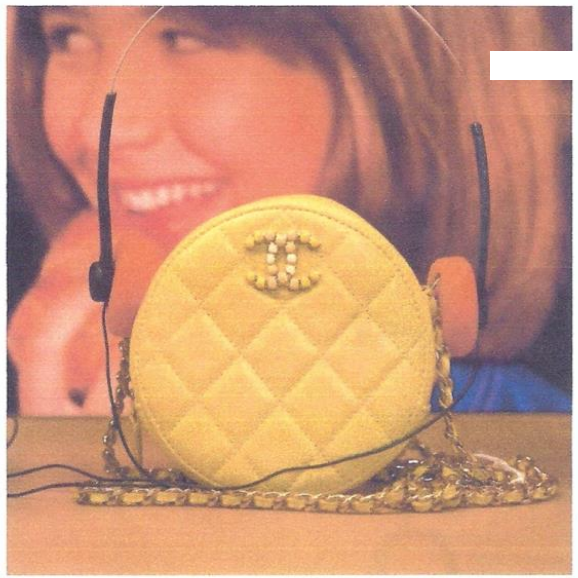
alle getoonde links worden omgeleid naar valse websites

💡 Tip: ken je iemand die hier misschien ook recht op heeft? Stuur deze e-mail gerust door.

systeem van doorsturen veroorzaak verdere verspreiding van frauduleuze mails.

Aan:

LUXE®



[ENDS TODAY] 90% off Chanel Purse!

New Arrivals Today

$356.00 $385.00

LUXE®

Handbags

Jewelry

Watches

You received this email because you are a LUXE. LLC email subscriber
To be removed from our mailing list, please click here to unsubscribe

© 2024 LUXE. LLC 1 Penn Plaza, 52nd Street, New York, NY 10022

IVO's 25.09.2025

►chanelens@luxemail.top

luxemail.top is een webdomein met registratie in CN (China)

de officiële website van Chanel is www.chanel.com
Chanel-afzenders gebruiken "...@chanel.com"

niet aanklikken !!! - link naar valse websites.

TE MOOI OM WAAR TE ZIJN !

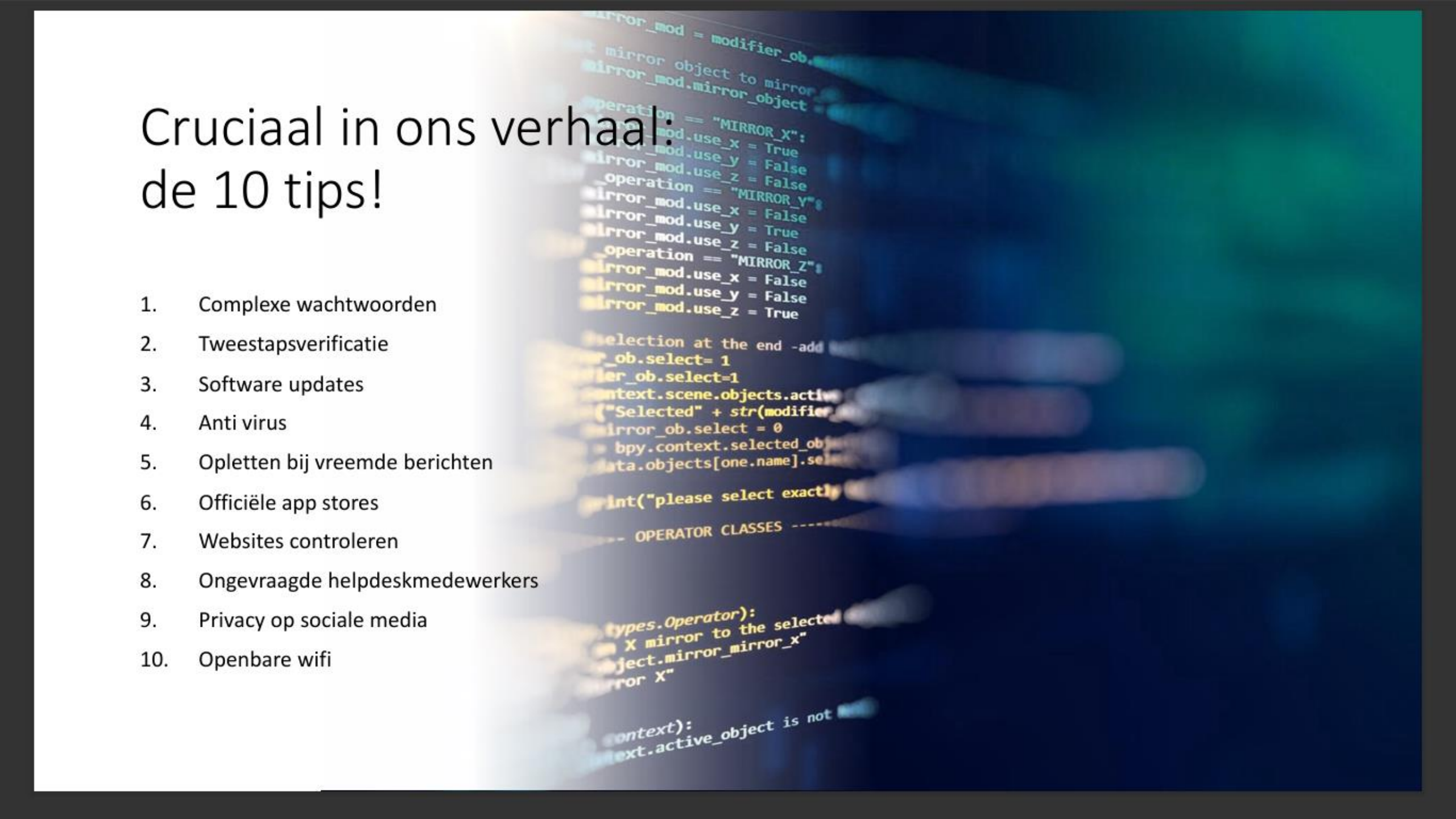
klassieke Chanel "flap bags" kosten nieuw tussen de 6.000 en de 11.000 €, en tweedehands in goede staat ongeveer 70-75% van die prijs…
voor zowat 400€ heb je die echt niet !!!

niet aanklikken !!! - link naar valse websites.

niet aanklikken om uit te schrijven - link naar valse websites.

Cruciaal in ons verhaal: de 10 tips!

1. Complexe wachtwoorden
2. Tweestapsverificatie
3. Software updates
4. Anti virus
5. Opletten bij vreemde berichten
6. Officiële app stores
7. Websites controleren
8. Ongevraagde helpdeskmedewerkers
9. Privacy op sociale media
10. Openbare wifi



Nog vragen?