



**Vlaamse actieve senioren vzw**

Puurs-Sint-Amands, 18 juni 2026





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...

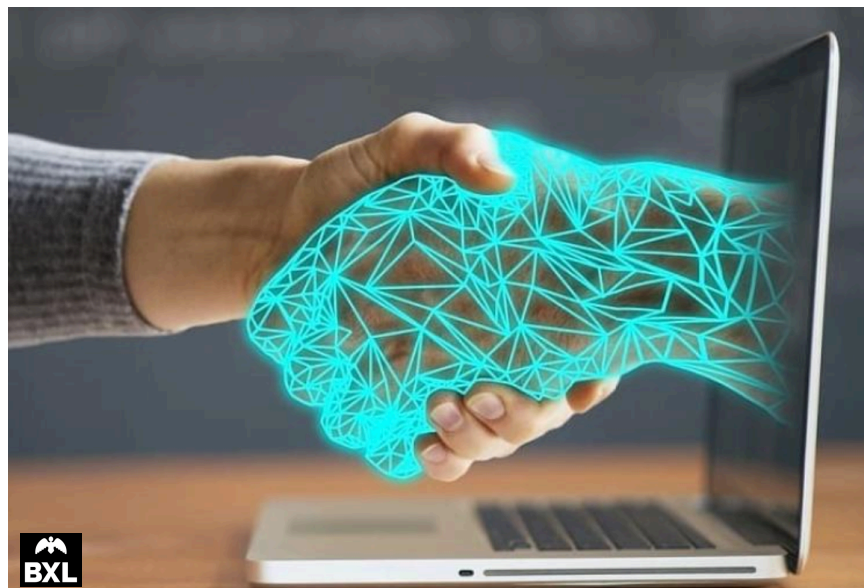
Wat Gilbert overkwam, overkomt de jongste tijd veel ouderen. “Ze zijn het favoriete doelwit van criminelen geworden.”

*(De Standaard 12 januari 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...

*“Onze papa was een sterke man”, vertellen zijn dochters. “Hij was 96 jaar, maar zijn indrukwekkende moestuin zag er nog altijd pico bello uit. Hij zorgde voor onze moeder die licht dementerend was, maar kon daarmee om. Natuurlijk was hij niet meer zo zelfstandig als vroeger. Dat hij niet meer mocht autorijden leerde hij ook mee leven. Als dat ene telefoontje er niet was gekomen, dan had hij vermoedelijk nog jaren gelukkig thuis kunnen wonen in de vertrouwde omgeving, samen met onze mama.”*





# CYBER(ON)VEILIGHEID





**VEILIG MET INTERNET OMGAAN EN WERKEN  
IS GEEN KWESTIE VAN GELUK !!!**

**ZEG NOOIT “*MIJ OVERKOMT HET NIET !*”**





# LEDENBEWUSTZIJN

## INTERNETFRAUDE - PHISHING

*“Of mij dat nooit zal overkomen ?  
Neen, dat durf ik niet zeggen. Ik geloof zelfs niet  
dat er iemand is die vandaag met zekerheid kan  
zeggen : mij overkomt dit nooit”*

*“Wij lezen verklaringen waar je tranen van in de  
ogen krijgt. Oudere mensen die hun volledige  
spaargeld kwijt zijn. Jonge gezinnen die aan het  
verbouwen zijn en al hun middelen zien  
verdwijnen”*



**Peter Peereboom**

Parketmagistraat Cybercrime

(HLN zaterdag 28 februari 2026)

*“Voor sommige slachtoffers betekent de  
oplichting dat het geld voor hun oude dag  
gewoon weg is”*



**Dimitri Antonissen**

Hoofdredacteur Het Laatste Nieuws

(HLN zaterdag 28 februari 2026)

Stel je voor dat er bij jou thuis wordt ingebroken en de  
politie meteen zegt : *“Goh, daar beginnen we niet aan.”*  
*In phishingdossiers gebeurt dat dagelijks.*

*“Een digitale inbraak verdient dezelfde prioriteit als een  
fysieke overval”, schrijft hoofdredacteur Dimitri Antonissen.*



Internetfraude is geëvolueerd van massale, onhandige spam met spellingsfouten en slecht nagmaakte logo's of foto's naar gepersonaliseerde, technologisch geavanceerde aanvallen. De modernste tendensen worden aangedreven door artificiële intelligentie (AI), zoals beeld- en spraaktechnologie,

+

De maatschappij - inclusief de senioren die gemiddeld tussen de 25 en de 30% van de bevolking uitmaken - is geëvolueerd naar een digitale samenleving (bank applicaties, tax-on-web, eBox, subsidie aanvragen, allerhande reservaties, sociale media ...).

=



**IEDERE GEBRUIKER VAN DIGITALE SYSTEMEN EN VAN DE CYBERRUIMTE IS KWETSBAAR !**





# CYBER... ???

Het voorvoegsel dat gebruikt wordt voor alles wat met internettechnologie en de digitale wereld 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

## Cybercriminaliteit

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

## Cyberveiligheid

het voorkomen van het vernietigen van gegevens en van ongeautoriseerde toegang.

Bron : Pixabay







Phishing  
Smishing  
Vishing  
Quishing  
Spoofing

Malware

Ransomware

Hacking

Botnets

Bron : AbberantRealities  
via Pixabay

**CYBER(ON)VEILIGHEID**



# BEVEILIGINGSRISICO ?



Informatie- en communicatietechnologie wordt als **middel én doelwit** gebruikt om ongeoorloofde en criminele acties te ondernemen : terrorisme en sabotage, politieke destabilisatie en fake news, fraude en diefstal, afpersing en losgeld, kindermisbruik, of maatschappelijk ontoelaatbare acties zoals cyberpesten, haattweets, sexting, dreigmails...

**Hacking** : toegang tot computersystemen of netwerken zonder toestemming, het vernielen of verstoren van computer systemen, het vergrendelen van systemen met vrijgave tegen betaling.

**Phishing(mail), Smishing(sms), Vishing(telefoon), Quishing(QR-code)** : met valse e-mails, websites, berichtjes, telefoon en QR-codes proberen inloggegevens of andere persoonlijke gegevens te achterhalen.

**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 -zaaien, bedreigingen (politie, gerecht), discriminatie, productie, bezit of verspreiding van kinderpornografie, auteursrechtenschendingen en illegale kopieën, spammen.







**WAT ?** : Phishing is een aanvalstechniek die vaak met veel succes ingezet wordt om een organisatie te hacken en/of gevoelige gegevens te ontfutselen van een individu of bedrijf. Specifieke doelgroepen (senioren ?) krijgen regelmatig te maken met phishingaanvallen. Phishing kan ook via sms (smishing), telefoon (vishing), QR-code (quishing) : een computer kan technisch beschermd worden, een individu niet. Phishing is de eerste stap om een een individu of organisatie aan te vallen : het slachtoffer wordt verleid om op een link te klikken, gegevens achter te laten of een bestand te openen ...

**VRIENDSCHAPSFRAUDE** : fraudeurs contacteren mensen via een vals profiel om hun vertrouwen te winnen en zo geld te ontfutselen : => meestal per mail of chatbox, verdacht online profiel, persoonlijke en financiële vragen, emotionele manipulatie... (SPOOFING)

**HULPVRAAGFRAUDE** : daders doen zich voor als een familielid of vriend om geld te ontfutselen => meestal telefonisch, dringend, geldverzoek, abnormaal taalgebruik, ongebruikelijk contactnummer online profiel, persoonlijke en financiële vragen, emotionele manipulatie... (SPOOFING)

**FALSE BANK(POLITIE)MEDEWERKERS** : fraudeurs doen zich voor als medewerkers van uw bank of de politie om geld ten goederen te ontfutselen => meestal telefonisch, onverwacht en geen tijd te verliezen, vragen codes en programma's te installeren, geld en bezittingen veilig te stellen....

**TWEEDEHANDSFRAUDE** : fraudeurs misleiden kopers of verkopers op tweedehandswebsites en online marktplaatsen => meestal per mail bieden meer dan gevraagd, eigen koerierdienst, vage beschrijving van artikel, vragen identiteit via kleine internationale transactie, ander communicatiekanalen...

**HITSCAM** : vorm van oplichting waarbij fraudeurs onder de naam van politie of justitie u bedreigen met vervolging of opsluiting tegen betaling => dreigend, significante geldsom, tijdsdruk, willekeurig en niet echt gepersonaliseerd...



## 1. Phishing (mails) en Smishing (messaging)

De tijd van e-mails vol taalfouten is definitief voorbij. Oplichters gebruiken generatieve AI om foutloze, overtuigende en natuurlijk klinkende berichten te schrijven, logo's na te bootsen...

Omdat de teksten niet-standaard zijn, vermijden ze rare tekens, gebruiken ze een normale tekstopbouw, en omzeilen ze zo vaak traditionele spamfilters.

Reële voorbeelden : criminelen sturen in België regelmatig frauduleuze berichten uit naam van vertrouwde instanties, zoals mutualiteiten (CM), banken (Argenta, Ing), de overheid (eBox, MyPension), nutsbedrijven (Fluvius, de Watergroep)...

Het gevaar : aanklikken leidt naar een gekloonde malafide website waar gevraagd wordt inloggegevens, persoonlijke gegevens en bankgegevens in te geven.

## 2. Quishing (QR-code Fraude)

Dit is een samentrekking van QR-code en phishing : oplichters versturen valse facturen, parkeerboetes of energie-afrekeningen met een gemanipuleerde QR-code.

Het gevaar : in plaats van een legitieme betaalpagina, leidt de QR-code je naar een malafide website waarmee ze je bankgegevens of betaling onderscheppen.

## 3. Evenement en reservatie hacking

Fraudeurs spelen slim in op massale events, zoals het WK voetbal. Ze zetten snel grote aantallen valse ticket- en streamingwebsites op, evenals nepvacatures voor tijdelijk personeel, om persoons- en betaalgegevens te stelen. Bij bevestigingen van reservaties van hotels en restaurants worden betalingsverzoeken omgeleid naar malafide websites.



## 4. Spoofing : nabootsing van portretten, beelden en stemmen

Criminelen maken de website van een vertrouwde partij perfect na om jou je eigen wachtwoorden of bankgegevens te laten invullen. Ze laten op jouw scherm een bekend en betrouwbaar telefoonnummer zien, zoals het officiële nummer van je eigen bank. Ze proberen je onder druk te zetten om geld over te maken of inlogcodes af te geven.

Oplichters vervalsen de afzender van een e-mail of sms-bericht. Het bericht lijkt exact afkomstig van een bekende organisatie (bijvoorbeeld een koeriersdienst), maar bevat een gevaarlijke link.

Artificiële Intelligentie (AI) maakt het mogelijk om de stem of het gezicht van bekenden perfect te imiteren. Oplettendheid is geboden bij telefoontjes of videobellen (FaceTime, Zoom, WhatsApp, Microsoft Teams, Google Meet, Skype, Messenger...) waarin een familie of bekenden (ogenschijnlijk) dringend vragen om een betaling of overschrijving uit te voeren.

Audio-spoofing : fraudeurs gebruiken korte audiofragmenten of gesproken boodschappen om familieleden op te bellen en hen in paniek te brengen met een smoes over een noodsituatie en de vraag om geld over te maken.

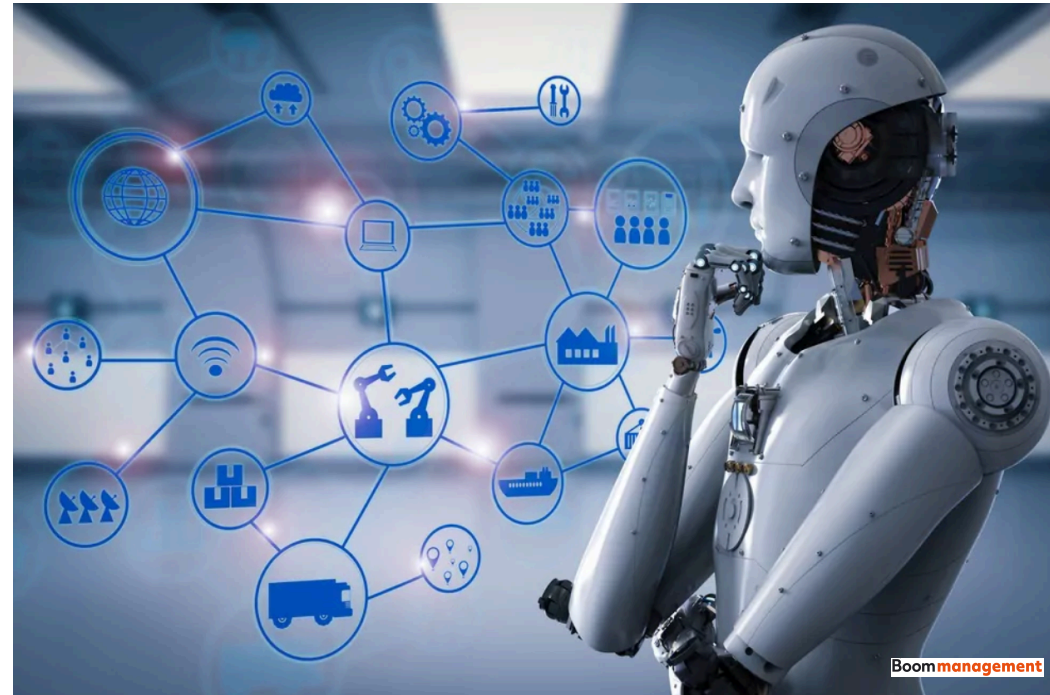
## 5. Conversatie of gesprekskaping

Bij deze vorm van fraude breken criminelen in bestaande e-mailconversaties in.

Oplichters lezen de e-mails tussen bijvoorbeeld een klant en een leverancier mee. Op het moment dat er betaald moet worden, sturen ze een e-mail uit naam van de leverancier met een gewijzigd rekeningnummer.







## **TECHNOLOGIE EVOLUEERT MAAR CYBER-ONVEILIGHEID OOK !!!**





**PHISHING (email)**  
**SMISHING (sms)**  
**QUISHING (QR-code)**

**WORDT MET DE DAG MOEILIJKER  
OM TE HERKENNEN !**

**TAAL** : kenmerken zoals kaduuk taalgebruik, spellingsfouten, rare leestekens, in een andere taal dan deze die je gewoonlijk gebruikt in uw corresponderen worden door AI-technieken quasi weggewerkt...

**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 hebt niet om een antwoord of informatie gevraagd (energiebedrijven en-consulenten), je weet van geen openstaande erfenis (de notaris zal je het wel vertellen...), je speelt nooit met de lotto maar je hebt ineens prijs....







**VISHING (telefoon, gesproken bericht)**

**WORDT MET DE DAG MOEILIJKER  
OM TE HERKENNEN !**

**TAAL** : boodschapper spreekt in een taal die z'n moedertaal niet is (zinsgebruik en vervoegingen, woordkeuzes, vreemd accent)... Met AI-technologie worden stemmen zoveel mogelijk nagebootst...

**TIJDSTIP** : na sluitingsuur, vrijdagavond, midden van de nacht, tijdens verlengd week-end, wettelijke feestdagen...

**ONGEWOON** : banken of CardStop bellen niet zelf op, maar vragen om zelf terug te bellen , en zeker niet om via de telefoon transacties uit te voeren (herstellen of blokkeren van frauduleus kaartgebruik of ongewone transacties), je hebt geen enkele zakelijke relatie met de beller (Microsoft belt je op om je computer te beveiligen of te herstellen terwijl al je apparatuur met Apple technologie werkt)...

**PANIEKZAAIEN** : niets is zo dringend of zo erg dat het direct via de telefoon moet verlopen..., als het om familie gaat, vraag dat ze zelf aan de lijn komen, vraag de plaats waar uw familielid zich bevindt, vraag het antwoord op een vraag waar alleen jouw familielid het antwoord op weet.....







WAT ? : is het opsporen en vervolgens uitbuiten van zwakke plekken in een computersysteem of netwerk, meestal om ongeoorloofde toegang te krijgen tot individuele, bedrijfs- of organisatorische gegevens. Hun doel is : het stelen van geld en gegevens, aankopen te doen op jouw naam, informatie te verkopen of openbaar te maken tegen losgeld, bestanden te blokkeren, te verwijderen of beschadigen met vrijgave tegen een afkoopsom. Malafide hackers gebruiken verschillende technieken om hun doel te bereiken :

**Social engineering** : een manipulatietechniek waarbij gebruik wordt gemaakt van menselijke fouten om toegang te krijgen tot persoonlijke informatie (phishing scams, spam e-mails, directe berichten, nep-websites).

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

**Inficeren met malware** : infiltreren met e-mail, directe berichten en website-links met downloadbare inhoud in het gebruikers-apparaat om malware te installeren.

**Misbruik van gebrekkige beveiliging** : misbruik maken van onveilige (openbare) en onvoldoende beveiligde draadloze netwerken.

**Via de “Achterdeur”** : het inficeren van een systeem met een “Trojaans Paard”, om belangrijke gegevens te verkrijgen en te stelen zonder dat het slachtoffer het merkt.

**Zombie Computers** : een computer die gebruikt wordt om spam te versturen, en zodra het slachtoffer een schijnbaar onschuldige code heeft uitgevoerd, wordt een verbinding geopend met het systeem van de hacker.

**en verder ...** : zelfs het bespioneren en onderscheppen van e-mails, specifieke programma's volgen elke toetsaanslag, waardoor de hacker alles heeft om een systeem te infiltreren of iemands identiteit te stelen.





**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 zeker de politie, de douane, financiën of justitie niet...

**Vertrouw niet op bedrijfs- of agentschapslogo's, of telefoonnummers** : huidige technieken (AI) 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...

**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 het nummer van uw bank- of kredietkaart of waardevolle objecten, laat nooit toe dat iemand uw scherm deelt, ga niet in op onverwachte verzoeken tot een videogesprek...

**Let op met sociale media** : gooi niet om het even wat op sociale media (Facebook, WhatsApp, Instagram) : alles wat erop komt en met je persoon kan verbonden worden is potentieel voer voor fraudeurs en criminelen...





**Afzender controleren en eventueel blokkeren :** op ► staan, dan komt de echte afzender tevoorschijn. Vooral opletten voor rare combinaties, verdachte landcodes zoals **.ng** (Nigeria) of **.cc** (Cocoseilanden), namen die op niets slaan (bijv.. boifdoeou@skynet.be)

**Link controleren :** door de muis traag over link te bewegen zie je URL. Meestal zal die verschillen van de naam van de getoonde link : niet op klikken, bericht verwijderen.

### Internet bankieren :

- ➔ registreer regelmatige schuldenaars in je bankpas met hun bankrekening,
- ➔ contacteer nieuwe schuldenaars of leveranciers om hun bankrekening te verifiëren,
- ➔ banken of Card Stop vragen nooit naar je pincode per mail of telefoon,
- ➔ heb je een bankmedewerker aan de lijn die om je pin-code of persoonlijke gegevens vraagt, zeg dan dat je gaat terugbellen naar het officieel nummer van het bankkantoor dat je bekend is.

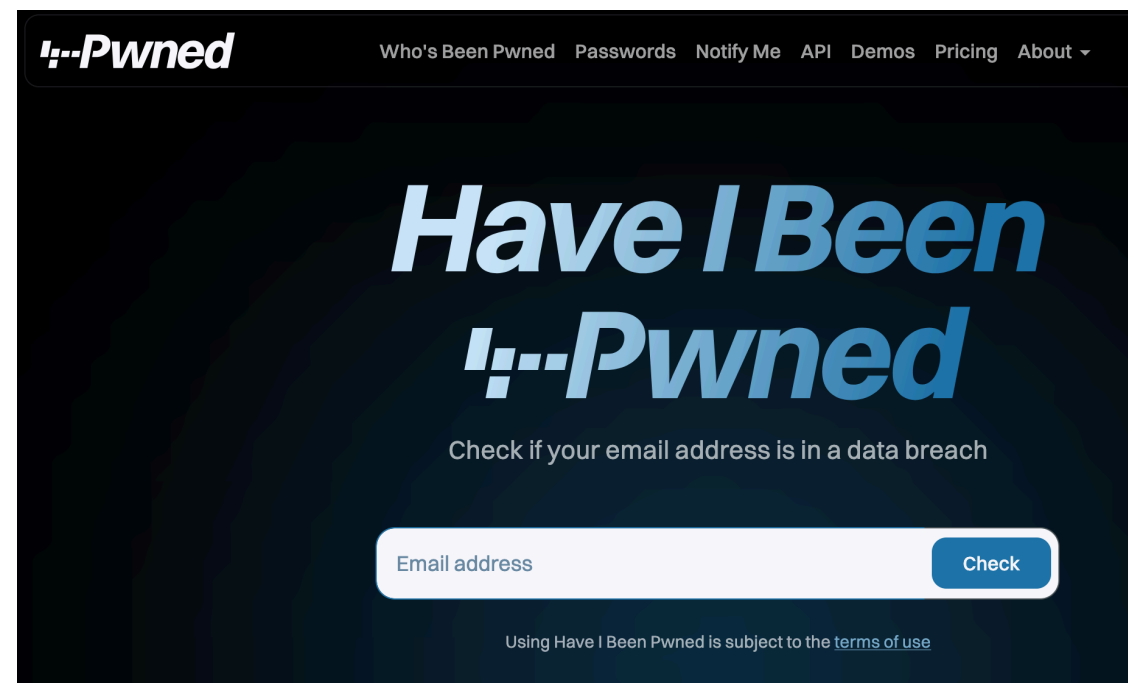




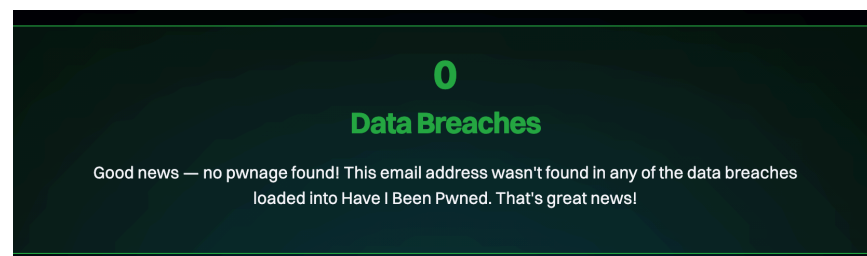
Je ontvangt een e-mail over login poging met een nieuw apparaat,  
Je merkt verdachte activiteiten op : bijv. laatste films gezien op Netflix,  
Je vrienden vertellen je dat ze een vreemde e-mail van je hebben ontvangen,  
Je merkt een frauduleuze betaling op je account op,  
Je ontvang dagelijks vreemde emails (phishing).

## DAN KAN JOUW E-MAIL ADRES GEHACKT GEWEEST ZIJN !!!

surf naar [www.haveibeenpwned.com](https://www.haveibeenpwned.com) en geef je email adres in

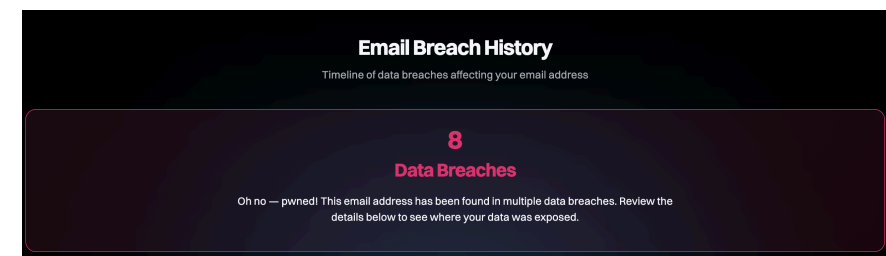


dan kan je 2 verschillende antwoorden krijgen



jouw email-adres is noch gehackt noch misbruikt geweest,  
en is (voorlopig) veilig voor verder gebruik

OF



jouw email-adres is gehackt of misbruikt geweest

➤ onmiddellijk email-adres wijzigen,  
en het oude email-adres verwijderen.





## WAT IS CYBERSECURITY ???

Cybersecurity, of cyberbeveiliging, is het geheel aan maatregelen en technologieën dat wordt ingezet om computersystemen, netwerken, apparaten en gegevens te beschermen tegen digitale aanvallen, gericht op het verkrijgen, wijzigen of vernietigen van gevoelige informatie, het afpersen van gebruikers of het verstoren van bedrijfsprocessen.

BEVEILIGINGSBEWUSTZIJN  
EN -TRAINING

NETWERK- EN  
EINDPUNTBEVEILIGING

BESCHERMING VAN  
GEGEVENS

TOEGANGSBEHEER  
EN NALEVING

Bron : Geralt via Pixabay





# CYBERSECURITY OF -BEVEILIGING



Bron : Schlüsseldienst via Pixabay

Cybersecurity omvat verschillende domeinen elk met een eigen focus en methode : netwerkbeveiliging, informatiebeveiliging, operationele beveiliging, applicatiebeveiliging, cloudbeveiliging en eindgebruiker-educatie.

Beveiliging voor al van deze domeinen helpt organisaties, bedrijven en individuen zich te beschermen tegen cyberaanvallen.

**Netwerk- en eindpuntbeveiliging** : het net van verbonden computers, servers, mobiele apparaten en andere elektronische systemen en individuele apparaten tegen cyberaanvallen (malware, virussen, ransomware, phishing en andere online bedreigingen) **door het installeren van firewalls, en het opsporen (IDS) en verhinderen van indringing (IPS).**

**Bescherming van gegevens** : beschermen van persoonlijke informatie, financiële gegevens, bedrijfsgeheimen en andere gevoelige gegevens tegen diefstal, ongeautoriseerde toegang of verlies **door versleuteling** om te voorkomen dat ze bij een mogelijke indringing leesbaar zijn.

**Toegangsbeheer en naleving** : het beheren en **beperken van toegang** tot systemen en gegevens tot niet-geautoriseerde gebruikers, het vaststellen van beleidsregels, procedures en normen, en ervoor zorgen dat deze worden nageleefd, inclusief relevante wet- en regelgeving. **Zero Trust** : het beveiligingsmodel waarbij geen gebruiker als vanzelfsprekend wordt vertrouwd, en dat vereist dat **elke toegang wordt gevalideerd**, ongeacht waar de gebruiker zich bevindt.

**Beveiligingsbewustzijn en -training** : essentieel om gebruikers op te leiden over cyberdreigingen en hoe ze deze kunnen voorkomen door het **herkennen van phishing**. Incidentrespons en -beheer : **reageren op een cyberincident**, inclusief het **identificeren van de oorzaak**, het minimaliseren van de **schade**, en het **herstellen** van de systemen.







## CYBERONVEILIGHEID EN DIGITALE FRAUDE IS GEEN “GAZETTENPRAAT”





De laatste weken hebben zogenaamde medewerkers van Proximus en Argenta het ene na het andere slachtoffer gemaakt. Ook Jan Tuerlinckx (88) en Kris Deckers (83) uit Leopoldsburg verloren al hun spaargeld. “Mijn vader is het vertrouwen in de mensheid kwijtgeraakt” zegt zijn zoon Bert.

foto : © Raymond Lemmens)

Zoon Bert : “Een paar weken geleden werd mijn vader opgebeld door een nummer dat schijnbaar van Proximus was. Een computerstem zei hem dat zijn simkaart te oud was en vroeg om zijn gegevens door te geven. Toevallig zat ik naast mijn vader, dus ik beval hem meteen om zijn telefoon neer te leggen.”

“Maar een paar dagen later kreeg hij plots een mail van het mailadres ‘*vlaanderen.be@gmail.com*’. De inhoud en lay-out waren perfect nagemaakt. Mijn vader moest een bijlage openen en zijn gegevens invullen. Zo gaf hij onder meer zijn bankrekeningen door. Een paar uur later werd hij gebeld, zagezegd door een medewerker van Argenta. Die sprak over verdachte transacties op zijn rekeningen. Mijn vader moest enkele handelingen uitvoeren en onder meer via **Itsme** inloggen.” “Mijn ouders waren al hun spaargeld kwijt, 12.000 euro, door transacties van telkens 900 euro. Er bleef nog 300 euro over op hun rekening”





Sinds oktober 2025 moeten Belgische en Europese banken bij alle overschrijvingen een zogenoemde IBAN-naamcontrole uitvoeren. De verplichte controle werd ingevoerd in de strijd tegen phishing. Dat betekent dat nagegaan moet worden of de naam van de begunstigde overeenkomt met het rekening- of IBAN-nummer. Is dat niet zo, dan krijgt de klant de kans om zijn mogelijke fout aan te passen of de overschrijving te annuleren.

**In geen tijd hebben oplichters al een manier gevonden om de sinds eind vorig jaar verplichte IBAN-naamcontrole bij overschrijvingen te omzeilen.**

Fraudeurs vragen nu hun slachtoffers om geen overschrijving meer te doen, maar om met een betaalkaart te betalen. “Zo omzeilen ze de IBAN-naamcontrole”, aldus Ombudsfina, want betalingen met betaalkaart worden niet automatisch onderworpen aan zo’n controle.

Concreet vragen de oplichters om een betaling met je betaalkaart te doen via een linkje of een online platform. Vaak is hun excuus dat de betaling dringend moet gebeuren, maar dat er “een probleem is met hun bankapp om een overschrijving te aanvaarden”.





Phishingaanval blijft gasten van Vlaamse hotels treffen. Horeca Vlaanderen ontving de afgelopen week heel wat meldingen van hotels over een phishingaanval, gericht op hun hotelgasten. Bijna honderd Vlaamse hotels lieten de voorbije week aan Horeca Vlaanderen weten dat hun gasten getroffen werden door een bredere phishingcampagne die nog steeds verder raast.

Daarbij ontvangen gasten berichten via WhatsApp of andere communicatiekanalen waarin correcte reserveringsgegevens worden vermeld, zoals hun naam, boekingsreferentie of verblijfsdata. Vervolgens worden zij doorgestuurd naar een valse betaalpagina met als doel betalingsgegevens te stelen.

Meer dan een derde van de getroffen hotels geeft aan dat zij in de afgelopen dagen elk meer dan 25 meldingen van verdachte berichten van hun gasten ontvingen. De impact is daarbij duidelijk voelbaar in de dagelijkse werking van de hotels.

Naast de directe gevolgen voor de hotels, wordt de ondersteuning door hun channel manager – de softwaretool voor het beheer van de verschillende online verkoopkanalen – door een groot deel van de respondenten als onvoldoende ervaren.

## OOK SENIORENVERENIGINGEN ZIJN NIET VEILIG !!!



Neos Zutendaal voor duizenden euro's opgelicht.

Oplichters deden zich voor als bankmedewerkers en haalden duizenden euro's van de rekening van de seniorenvereniging.

Neos Zutendaal werd recent geconfronteerd met een geraffineerde vorm van phishing. Een bestuurslid van de vereniging werd telefonisch gecontacteerd door onbekenden die zich voordeden als medewerkers van de bank. Wat begon als een ogenschijnlijk geruststellend telefoontje over een verdachte overschrijving naar het buitenland, eindigde in een financiële kater voor de vereniging. Volgens de oplichters was er een groot bedrag onderweg naar een buitenlandse rekening. Ze zouden alles in orde brengen om de zogezegde frauduleuze transactie tegen te houden. In werkelijkheid slaagden ze erin om duizenden euro's van de rekening van NEOS Zutendaal weg te sluizen. Het gestolen geld is dat van de 160 Neos-leden die ingeschreven hadden voor twee uitstappen.





# Casussen

uit het dagelijks leven gegrepen ...





Van: Mijn doccle **boifdoeou@skynet.be**  
Onderwerp: U heeft een openstaande opdracht  
Datum: 7 juli 2025 om 00:51  
Aan:

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

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 : gkldfghhgeuijnie.com

Met vriendelijke groeten,  
Het Doccle-team



Ontdek onze apps • Contacteer ons • Lees onze blog

© 2025 Doccle

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



Van: Central Rede  
Onderwerp: ARGENTA : Herinnering: Uw kaartlezer werkt binnenkort niet meer  
Datum: 8 jun 2025, 19:23:32  
Aan:

► centralrede@lopes.com.br

afzender is niet "@argenta.be"

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

## Herinnering: Vraag uw nieuwe kaartlezer aan

Beste klant,

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

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 enkel geldt voor klanten die kiezen voor een vervangtoestel.

**dringend ???** vanaf 8 mei, maar mail dateert van 8 juni



**dreigement** : niet reageren kost geld of veroorzaakt problemen

### Kaartlezer aanvragen

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

Voor vragen kunt u terecht op [www.argenta.be](http://www.argenta.be) of bel ons tijdens kantooruren.

© 2025 Argenta Bank – Dit is een automatisch verzonden e-mail. Bezoek [www.argenta.be](http://www.argenta.be) voor meer informatie.

**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 ► [kankali@dattymaterials.com](mailto:kankali@dattymaterials.com)  
Onderwerp: Mogelijk recht op sociale compensatie voor water – check het even  
Datum: 10 juni 2025 om 00:53  
Aan:

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](#)

### Hulp nodig?

Onze klantendienst helpt je graag verder:

 078 35 35 99

 [klantenservice@dewatergroep.be](mailto:klantenservice@dewatergroep.be)

Met vriendelijke groeten,

**Het team van De Watergroep**

Volg ons op [Facebook](#) | [LinkedIn](#)

[Privacyverklaring](#) | [Mijn Watergroep](#)

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

systeem van doorsturen veroorzaakt verdere verspreiding van deze frauduleuze mail.

ga naar zelf naar de website [www.dewatergroep.be](http://www.dewatergroep.be) om te weten wat de voorwaarden en mogelijkheden zijn 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

alle getoonde links worden omgeleid naar valse websites





Van: CM-Zorgkas  
Onderwerp: Uw zorgkas komt eraan  
Datum: 6 november 2024 om 23:07  
Aan:

► info@miankararestaurant.com

afzender is niet "cm zorgkas"  
de zorgkas verzendt mails met \*\*\*\*@cm.be

's nachts 23:07 uur (andere tijdszone) ???



## Uw zorgkas komt eraan

Beste,

Uw zorgkas wordt binnenkort uitbetaald.

### Eenvoudige toegang tot uw dossier

Het **bedrag** kan u online raadplegen via Mijn CM. Log u in via onderstaande knop of via de Mijn CM-app.

Aanmelden

niet aanklikken !!!

De **details** van de betaling (zoals de periode, het aantal dagen en de inhouding voor bedrijfsvoorheffing) vindt u in de bankmededeling van de overschrijving.

### Betaalkalender en informatie

Wanneer wordt uw zorgkas overgeschreven? Op onze website vindt u een handige [betaalkalender](#) en leest u algemene informatie over [wat u moet doen bij ziekte of een ongeval](#).

Wil u deze e-mails niet meer ontvangen? [Schrijf u hier uit](#).  
Met vriendelijke groeten

Uw CM-team



### Download onze handige Mijn CM-app voor iPhone of Android

De Mijn CM-app is het digitale kantoor voor CM-leden: altijd en overal beschikbaar om uw praktische zaken op te volgen.



Als u nog vragen hebt, aarzel niet om [contact](#) met ons op te nemen.

Deze e-mail en elk meegeleverd bestand zijn vertrouwelijk en uitsluitend voor de bestemming bedoeld. Als u deze e-mail per vergissing hebt ontvangen, breng ons dan onmiddellijk op de hoogte.

contact niet aanklikken : wordt omgeleid !

De zorgkas wordt niet uitbetaald, wel het zorgbudget !  
Een zorgbudget wordt alleen uitbetaald aan :  
zwaar zorgbehoevenden, ouderen met een zorgnood,  
en mensen met een handicap.

alle getoonde links worden omgeleid naar valse websites

niet aanklikken

ook niet uitschrijven !!!



de **Landelijke Pensioendienst** bestaat niet,  
de **Federale Pensioendienst** wèl !  
<https://www.sfpd.fgov.be>

**Van:** LandelijkePensioendienst ► [LandelijkePensioendienst@mail.tpu66.Com](mailto:LandelijkePensioendienst@mail.tpu66.Com)  
**Onderwerp:** Raadpleeg nu uw persoonlijk overzicht en ontdek het bedrag van uw extra pensioenbonu  
**Datum:** 26 juni 2025 om 23:49 's nachts om 23:49uur ???  
**Aan:**



Geachte heer / mevrouw,

Wij informeren u graag dat er nieuwe gegevens beschikbaar zijn over uw pensioenrechten. Deze informatie kunt u raadplegen via het online portaal van de Landelijke Pensioendienst.

In uw dossier vindt u onder andere:

- en overzicht van uw loopbaan zoals geregistreerd bij de sociale zekerheid
- Uw opgebouwde pensioenrechten in de verschillende stelsels (werknemer, zelfstandige, ambtenaar)
- De verwachte pensioendatum op basis van uw persoonlijke situatie
- Een raming van het maandelijkse pensioenbedrag

U kunt uw dossier veilig raadplegen via [[www.landelijkepensioendienst.be](http://www.landelijkepensioendienst.be)] met uw elektronische identiteitskaart, itsme® of een andere erkende digitale sleutel.

niet aanklikken !!!  
de getoonde link wordt  
omgeleid naar valse websites

gegevens van de elektronische  
identiteitskaart en itsme worden  
gehackt.

Met vriendelijke groet,





Van: Chanel  
Onderwerp: ☒ It's Confirmed: 90% OFF Chanel  
Datum: 30 jun 2025, 16:42:46

▶chanelens@luxemail.top

LUXE®



[ENDS TODAY] 90% off Chanel Purse!

New Arrivals Today



\$356.00



\$385.00

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 !!!**

LUXE®

Handbags

Jewelry

Watches



You received this email because you are a LUXE, LLC email subscriber.  
To be removed from our email list, please click here: [unsubscribe](#)

© 2024 LUXE, LLC 1 East 57th Street, New York, NY 10022

niet aanklikken !!! - link naar valse websites.

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

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

de officiële website van Chanel is  
[www.chanel.com](http://www.chanel.com)  
Chanel-afzenders gebruiken “...@chanel.com”





Van: Uw Testament - Bma  
Onderwerp: Wees er zeker van dat uw erfenis op de juiste manier verdeeld wordt  
Datum: 21 juni 2025 om 07:29  
Aan:

news@news.rokblue.com



[Bekijk in uw browser](#)

[Bestel hier DE GRATIS BROCHURE](#) voor schenken en nalaten

niet aanklikken - de getoonde link wordt omgeleid naar valse websites



Het opstellen van een testament is een essentiële stap om er zeker van te zijn dat uw erfenis op de juiste manier verdeeld wordt, zowel onder uw dierbaren als goede doelen die belangrijk voor u zijn. Door nu alvast na te denken over uw nalatenschap, geeft u uzelf de kans om een blijvende impact op de wereld te maken.

Bestel nu de [GRATIS gids](#) die u op weg helpt in de wetgeving rond testamenten en legateren aan een goed doel.

[BESTEL NU DE GRATIS GIDS](#)

De gratis gids "[Goed Geregeld Goed Gegeven](#)" is een uitgave van testament.be, een groepscampagne van méér dan 150 goede doelen.

U ontvangt deze e-mail \_\_\_\_\_ is een I omdat u zich via een van onze partners heeft geregistreerd voor informatie, aanbiedingen of promotionele communicatie. Tijdens de registratie heeft u aangegeven interesse te hebben in relevante producten of diensten. Dit domein behoort tot Blue Media Ads GmbH, gevestigd aan de Luitpoldstraße 74a, D-91052 Erlangen, Duitsland. Wij werken samen met zorgvuldig geselecteerde partners binnen de EU en daarbuiten om u de best mogelijke aanbiedingen te kunnen tonen. Wilt u geen e-mails meer ontvangen? U kunt zich op elk moment uitschrijven via de afmeldlink onderaan deze e-mail. [Afmelden](#)

vzw testament.be coördineert de nationale campagne, en met meer dan honderd deelnemende ngo's, goede doelen en maatschappelijke organisaties is testament.be uitgegroeid tot de grootste nationale groepscampagne ooit, om een goed doel in je testament op te nemen....

afzender is niet de domeinnaam  
testament.be

links niet aanklikken !!!  
de getoonde links wordt omgeleid naar valse websites  
ook niet op "afmelden" aanklikken....

BlueMediaAds GmbH is een legaal planning en marketing bureau, met domeinnaam [www.blumediaads.com](http://www.blumediaads.com)

Maar de afzender (zombiecomputer of botnet) verschuilt zich achter BlueMediaAds GmbH om eventueel illegaal verkregen emailadressen te gebruiken om "legaal" spam te versturen.

surf naar [www.testament.be](http://www.testament.be)  
om een brochure te krijgen,  
dat is veiliger !





## WORDEN FINANCIËLE INSTELLINGEN EN BANKEN (EINDELIJK) OP HUN VERANTWOORDELIJKHEDEN GEWEZEN ?

In zijn vonnis oordeelt de Antwerpse kortgedingrechter dat banken slachtoffers van phishing toch meteen moeten vergoeden voor de geleden schade. Geert Lenssens, advocaat gespecialiseerd in bankzaken, spreekt in de krant van een “baanbrekend” precedent.

Bron : HBVL 3 juni 2026

De zaak draaide rond een bejaard koppel dat voor net geen 50.000 euro was opgelicht. Het tweetal had het geld overgeschreven naar een valse bankmedewerker in Portugal. Banken weigeren in dergelijke gevallen meestal een terugbetaling, omdat klanten een grove nalatigheid plegen door het geld zelf over te schrijven naar een frauduleuze ontvanger.

De kortgedingrechter in Antwerpen gaf de betrokken bank in dit geval echter ongelijk. In haar vonnis stelde de rechtbank dat uit eerdere Europese rechtspraak blijkt dat een financiële instelling het geld in eerste instantie altijd moet terugstorten aan slachtoffers van phishing. Pas daarna, als de bank meent dat de klant een zware nalatigheid beging, kan ze een procedure starten om het geld terug te vorderen.





## HOUDT UW OGEN OPEN

ZIET U IETS VERDACHTS? 



## ZET UW VOELSPRIETEN OP

DENK NA VOORDAT  
U KLIKT OF DEELT!



## VOEL HET AAN UW ELLEBOGEN...

DEEL GEEN GEVOELIGE INFO! 



**SAMEN ALERT, SAMEN VEILIG OP INTERNET!**



DENK NA • CHECK • BESCHERM • DEEL VERSTANDIG



## DANK U

