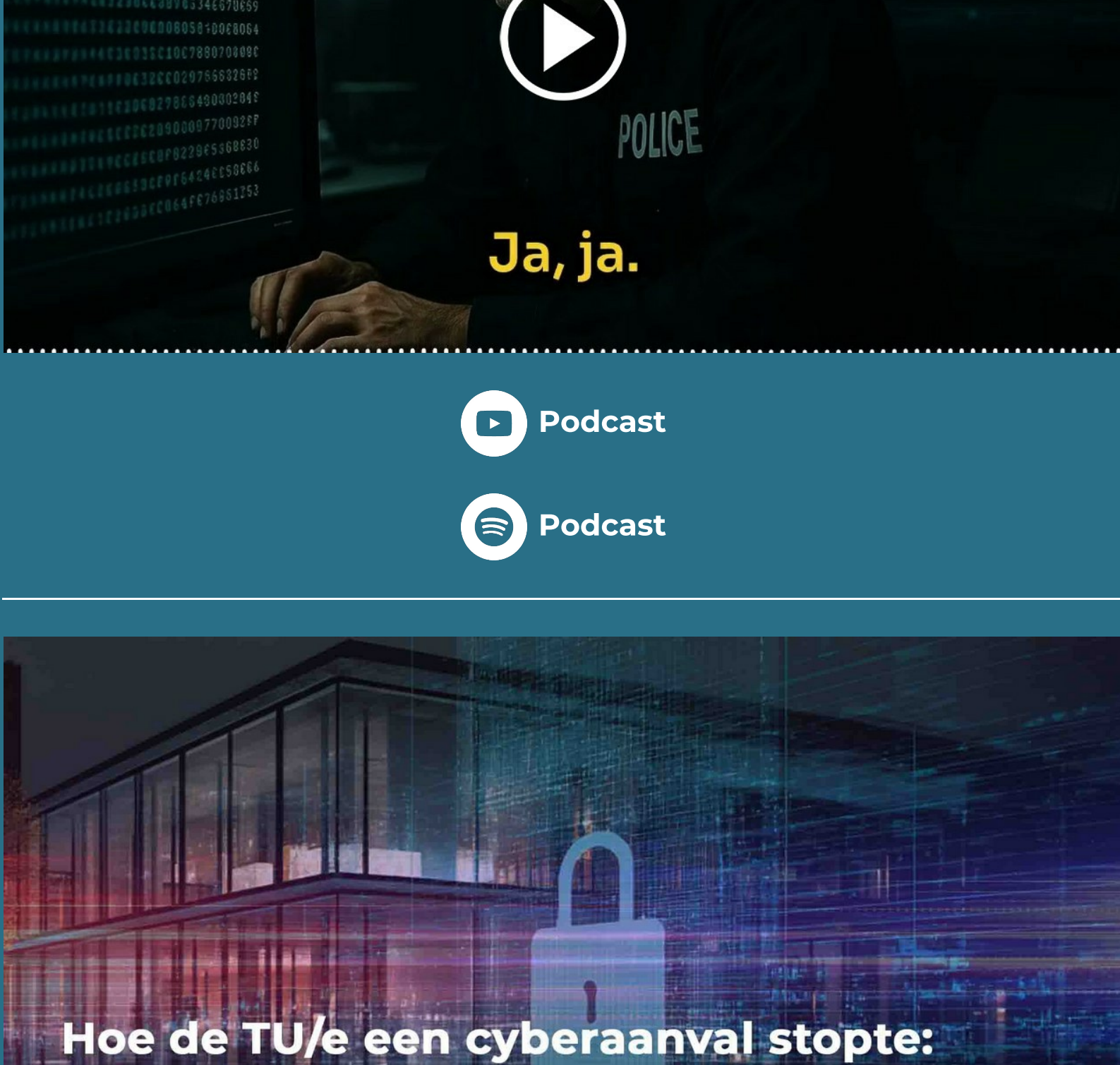




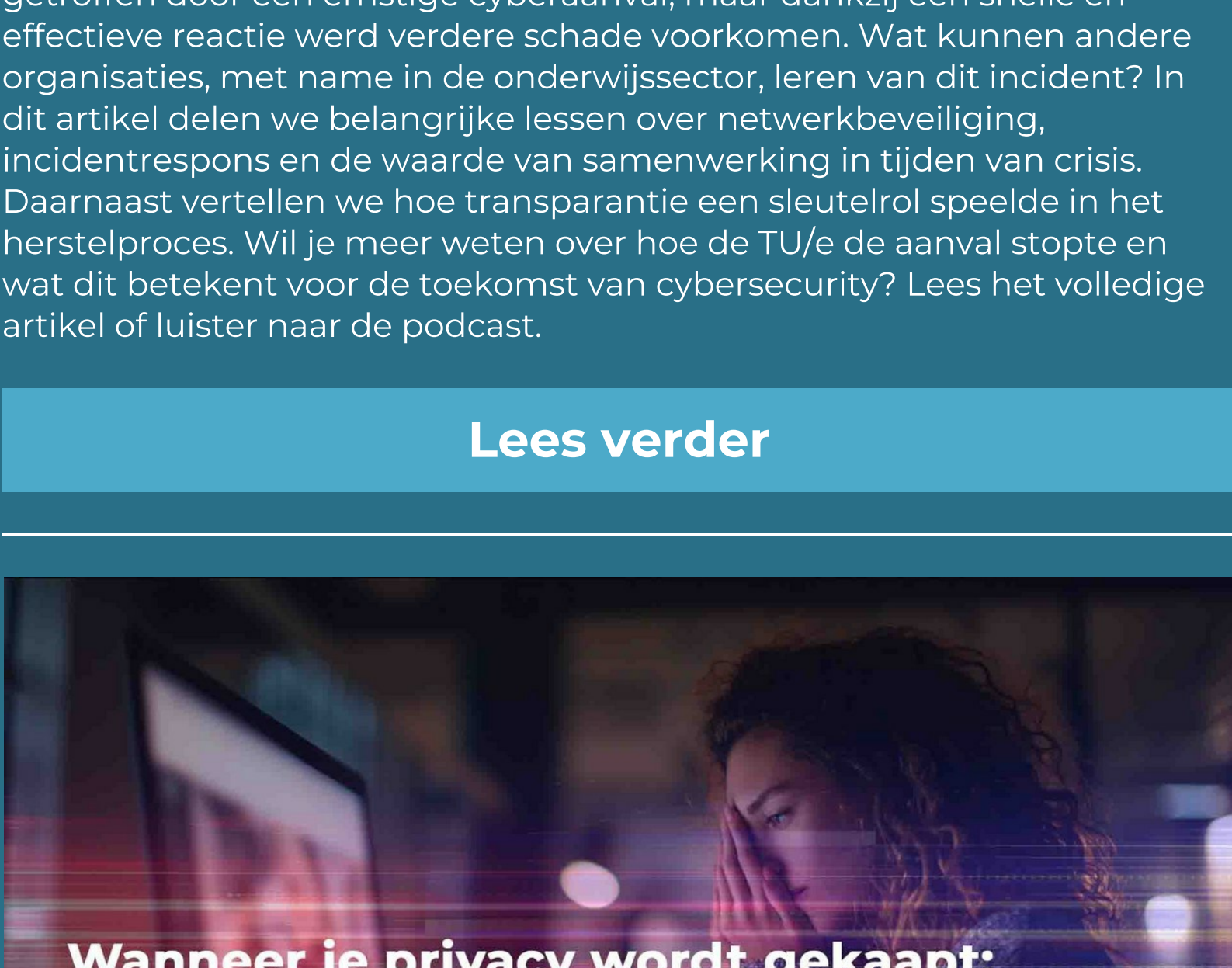
Nieuwsbrief 367



Podcast



Podcast



Hoe de TU/e een cyberaanval stopte: een les in snelle actie en transparantie

How TU/e stopped a cyber attack: a lesson in swift action and transparency



Wanneer je privacy wordt gekaapt: de verborgen gevolgen van het delen van intieme beelden

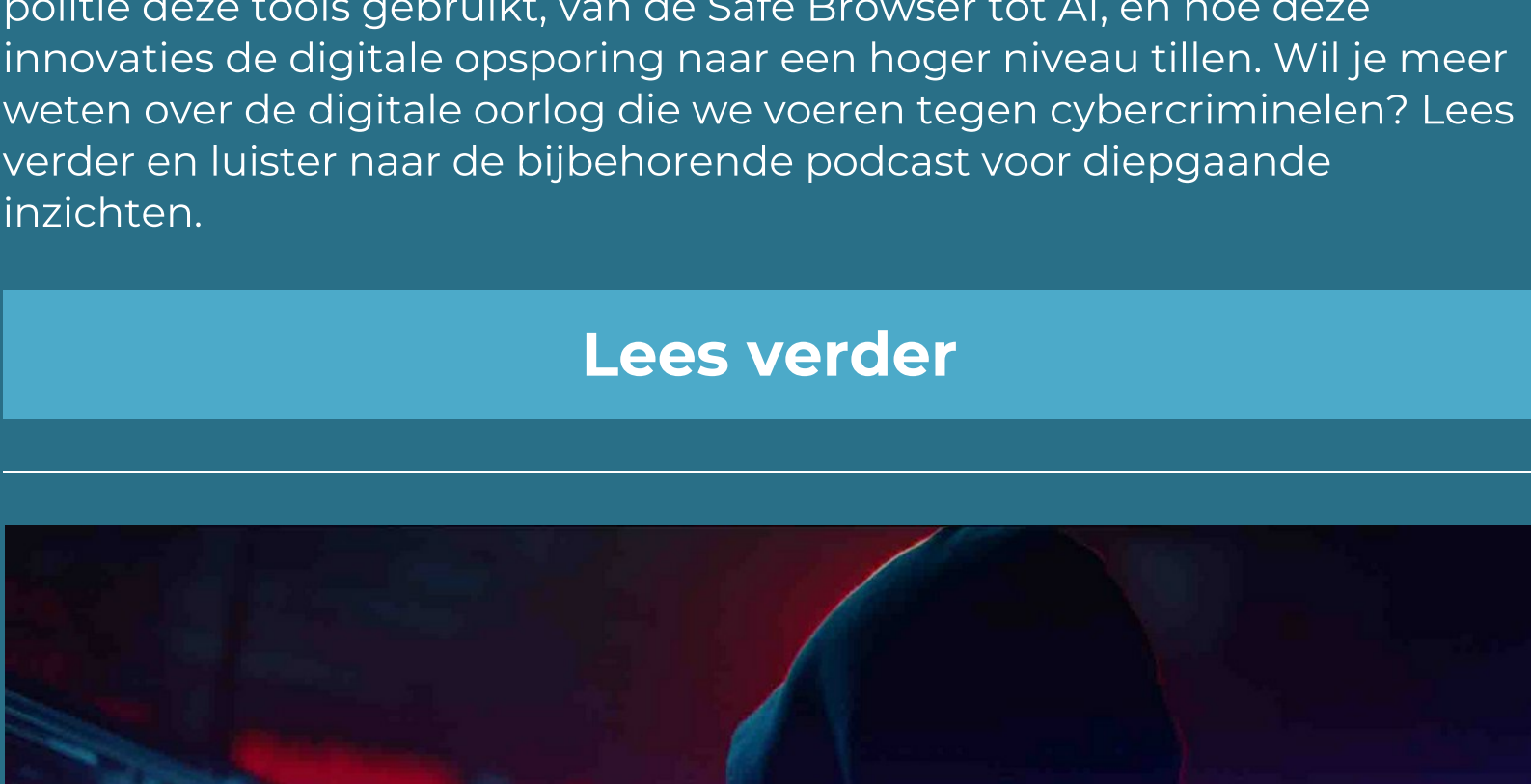
When your privacy is hijacked: the hidden consequences of sharing intimate images

[Reading in another language](#)

Wanneer je privacy wordt gekaapt: de verborgen gevolgen van het delen van intieme beelden

Het delen van intieme beelden zonder toestemming is een groeiend probleem met verwoestende gevolgen voor slachtoffers. In dit artikel duiken we dieper in de verborgen impact van niet-consensuele verspreiding van intieme beelden, ofwel NCII, en onderzoeken we hoe verschillende landen, waaronder Nederland, België en Zweden, hiermee omgaan. Wat zijn de psychologische en sociale gevolgen voor slachtoffers, en welke wetgeving biedt bescherming? Dit artikel biedt niet alleen inzichten in de huidige situatie, maar ook de stappen die nodig zijn voor een effectievere aanpak.

[Lees verder](#)



Cybercrime 2024: Hoe de politie de digitale oorlog wint met technologie en samenwerking

Cybercrime 2024: How police are winning the digital war with technology and collaboration

[Reading in another language](#)

Cybercrime 2024: Hoe de politie de digitale oorlog wint met technologie en samenwerking

In 2024 heeft de politie haar strijd tegen cybercrime drastisch versterkt door het inzetten van geavanceerde technologieën en intensieve internationale samenwerking. Deze aanpak maakt het mogelijk om complexe misdrijven zoals phishing, ransomware en cyberaanvallen sneller te detecteren en aan te pakken. In dit artikel ontdek je hoe de politie deze tools gebruikt, van de Safe Browser tot AI, en hoe deze innovaties de digitale opsporing naar een hoger niveau tillen. Wil je meer weten over de digitale oorlog die we voeren tegen cybercriminelen? Lees verder en luister naar de bijbehorende podcast voor diepgaande inzichten.

[Lees verder](#)



De wereld strijdt terug, operation endgame en de jacht op ransomware

The world fights back, operation endgame and the hunt for ransomware

[Reading in another language](#)

De wereld strijdt terug, operation endgame en de jacht op ransomware

De strijd tegen ransomware heeft een nieuwe mijlpaal bereikt met de wereldwijde operatie "Endgame". Deze gecoördineerde actie leidde tot het uitschakelen van honderden servers en miljoenen aan beslagleggingen, terwijl de jacht op de meest gezochte cybercriminelen in volle gang is. Wat zijn de resultaten van deze operatie en wat betekent dit voor de toekomst van digitale veiligheid? In dit artikel en de bijbehorende podcast duiken we dieper in de impact van Operation Endgame en de samenwerking tussen internationale autoriteiten in de strijd tegen cybercriminaliteit.

[Lees verder](#)



De jacht op darkweb criminelen: Hoe operatie RapTor 270 arrestaties wereldwijd mogelijk maakte

The hunt for darkweb criminals: How Operation RapTor enabled 270 arrests worldwide

[Reading in another language](#)

De jacht op darkweb criminelen: Hoe operatie RapTor 270 arrestaties wereldwijd mogelijk maakte

Operatie RapTor markeert een cruciale stap in de strijd tegen cybercriminaliteit op het darkweb. Dankzij internationale samenwerking werden maar liefst 270 verdachten wereldwijd gearresteerd, waaronder vier in Nederland. Deze operatie verstoren de netwerken van criminelen die zich verschuilen in de schaduwen van het internet, waar de handel in illegale goederen floreert. Wil je weten hoe deze operatie werd uitgevoerd en welke impact dit heeft op de toekomst van darkwebcriminaliteit? Lees het volledige artikel en luister naar de podcast voor alle details.

[Lees verder](#)



[Reading in another language](#)

Velsbroek - Helpdesk fraude

Op 21 maart 2025 werd een 79-jarige vrouw slachtoffer van bankhelpdeskfraude in Velsbroek, een vorm van oplichting die helaas steeds vaker voorkomt. De verdachte, een jongeman van ongeveer 18 jaar, wordt gezocht nadat hij met de gestolen bankpas geld opnam en een robotgrasmaaier kocht. In dit artikel bespreken we niet alleen de details van deze zaak, maar geven we ook inzicht in de verschillende vormen van bankhelpdeskfraude, zoals vishing, smishing en tech support scams. Luister ook naar de podcast voor een diepere duik in de werkwijzen van cybercriminelen en hoe je jezelf kunt beschermen tegen deze oplichting.

[Lees verder](#)



Blijf alert, luister

DE CYBERCRIME PODCAST



Abonneer je op onze podcast via



YouTube



Spotify

De Cybercrime Podcast van Cybercrimeinfo

Wil je altijd op de hoogte blijven van het laatste cybernieuws? Abonneer je dan op **De Cybercrime Podcast**. Je ontvangt dagelijks een korte update met betrouwbare informatie over actuele dreigingen, trends en praktische adviezen. De inhoud is zorgvuldig samengesteld door Cybercrimeinfo en eenvoudig te volgen via AI-gegenereerde Nederlandse stemmen. Luister waar en wanneer je wilt via **YouTube** of **Spotify** en versterk je digitale weerbaarheid. Abonneren is gratis en zo geregeld.



[Reading in another language](#)

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waarin digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Jouw donatie maakt het verschil. Dit is waarom:

- **Een onafhankelijke en betrouwbare bron van informatie**
Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
- **Bewustwording en preventie mogelijk maken**
Met jouw donatie help je ons om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen direct bij aan het voorkomen van digitale misdrijven.
- **Ondersteuning van operationele kosten**
Donaties worden direct gebruikt voor het hosten van onze website en het up-to-date houden van technologische middelen. Hierdoor kunnen we cybercriminelen blijven volgen en jullie informeren over de nieuwste digitale dreigingen.

Elke bijdrage, groot of klein, is van onschatbare waarde in onze strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Doneer nu via onze doneerpagina (kies zelf het bedrag dat je wilt doneren) of gebruik de onderstaande QR-code.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo | ccinfo.nl

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te vinden.
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review**.
Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol! Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo (ccinfo)

Schrijf een review

Share

Tweet

Share

Pinterest

Bluesky

Mastodon

Deze e-mail is verzonden naar [email].

Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier](#) afmelden.

U kunt ook uw [gegevens](#) [inzien](#) en [wijzigen](#).

Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.