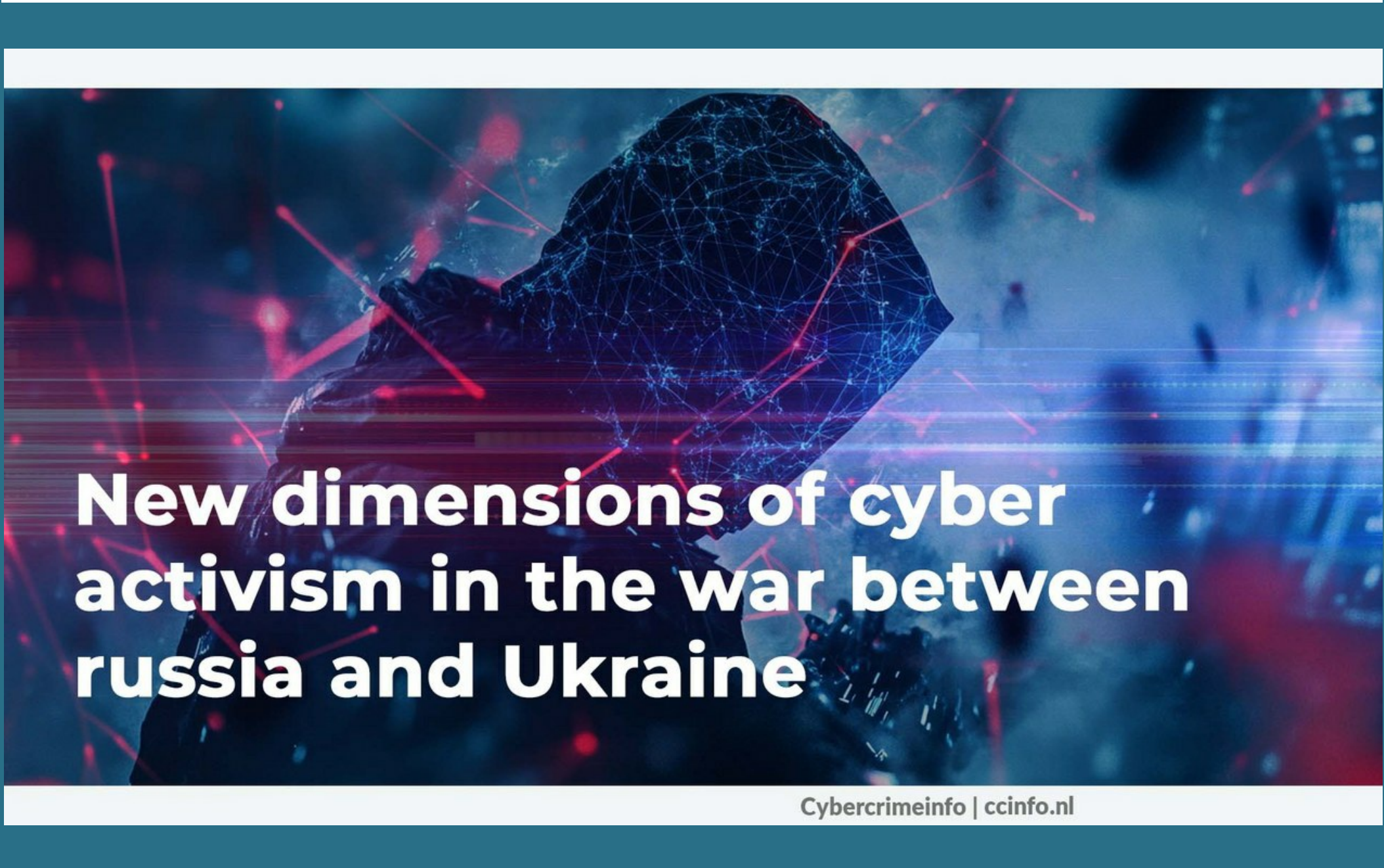
Nieuwsbrief 355

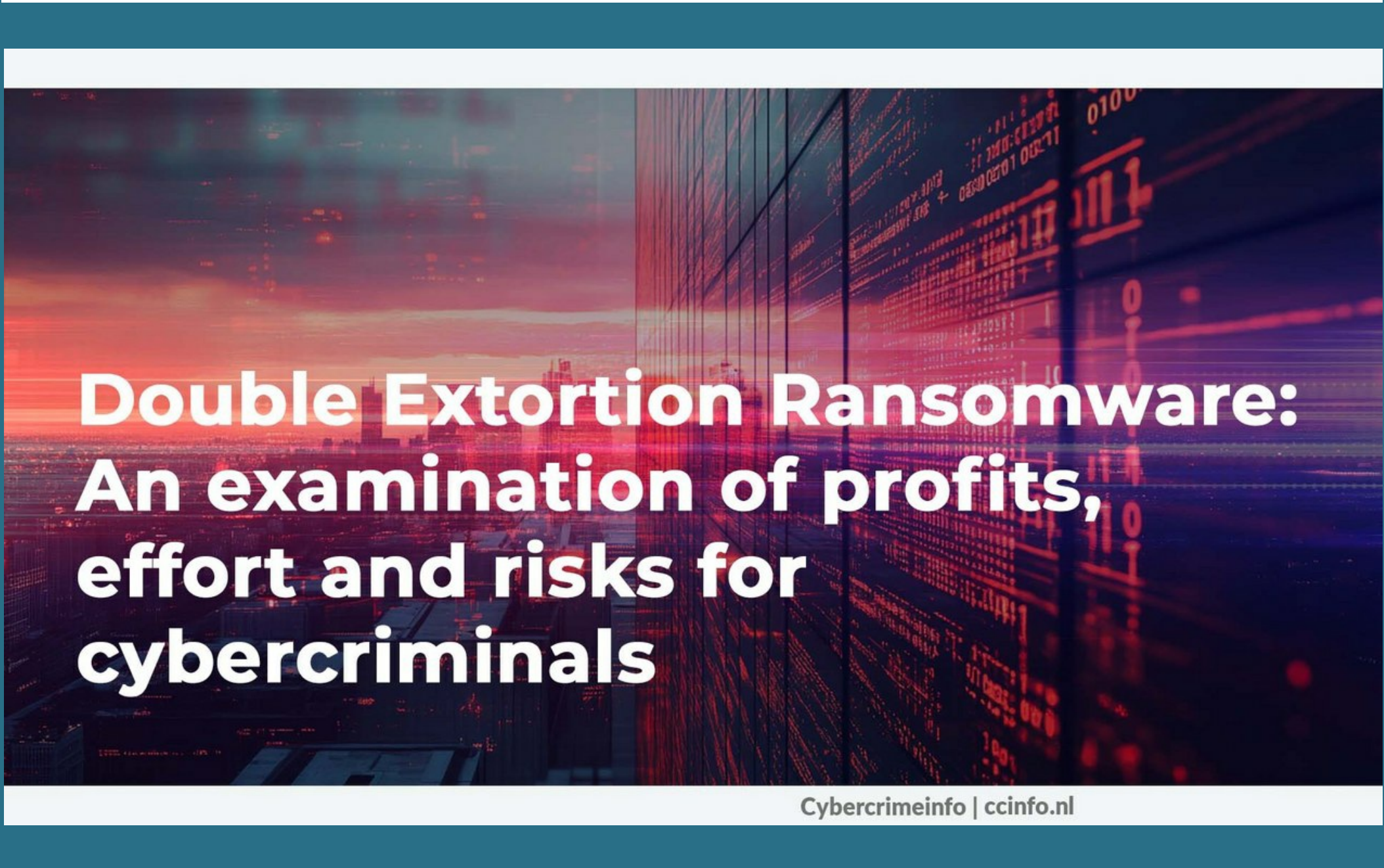


Reading in another language

Nieuwe dimensies van cyberactivisme in de oorlog tussen rusland en Oekraïne

Sinds het uitbreken van de oorlog tussen Rusland en Oekraïne is cyberactivisme uitgegroeid tot een krachtig wapen in het digitale strijdperk. Wat begon met grootschalige DDoS-aanvallen, is geëvolueerd naar een breed scala aan tactieken, waaronder ransomware, aanvallen op operationele technologie en doxing. Hacktivistische groepen spelen een steeds strategischere rol, waarbij de grens tussen cyberaanvallen en informatieoorlogsvoering vervaagt. In dit artikel duiken we dieper in de recente trends, de afname en professionalisering van hacktivistische groeperingen en de geopolitieke implicaties van deze digitale strijd. Hoe beïnvloeden deze ontwikkelingen de veiligheid van overheden en bedrijven? En welke lessen kunnen we hieruit trekken? Lees verder en ontdek hoe cyberactivisme zich blijft aanpassen in een wereld waar digitale conflicten steeds bepalender worden.

Lees verder



Reading in another language

Double Extortion Ransomware: Een onderzoek naar de winst, inspanning en risico's voor cybercriminelen

Ransomware is een van de grootste digitale bedreigingen van deze tijd, maar cybercriminelen gaan steeds een stap verder. Met het double extortion-model eisen ze niet alleen losgeld voor het ontsleutelen van bestanden, maar dreigen ze ook met het lekken van gestolen data. Dit maakt de druk op slachtoffers nog groter en vergroot de kans op betaling. Maar hoe winstgevend is deze methode voor criminelen? Welke risico's nemen ze en hoe efficiënt zijn hun aanvallen? In dit diepgaande onderzoek, mede gebaseerd op politierapporten en cybersecurity-expertise, wordt onthuld hoe ransomwaregroepen opereren, welke factoren hun succes bepalen en wat bedrijven kunnen doen om zich te beschermen.

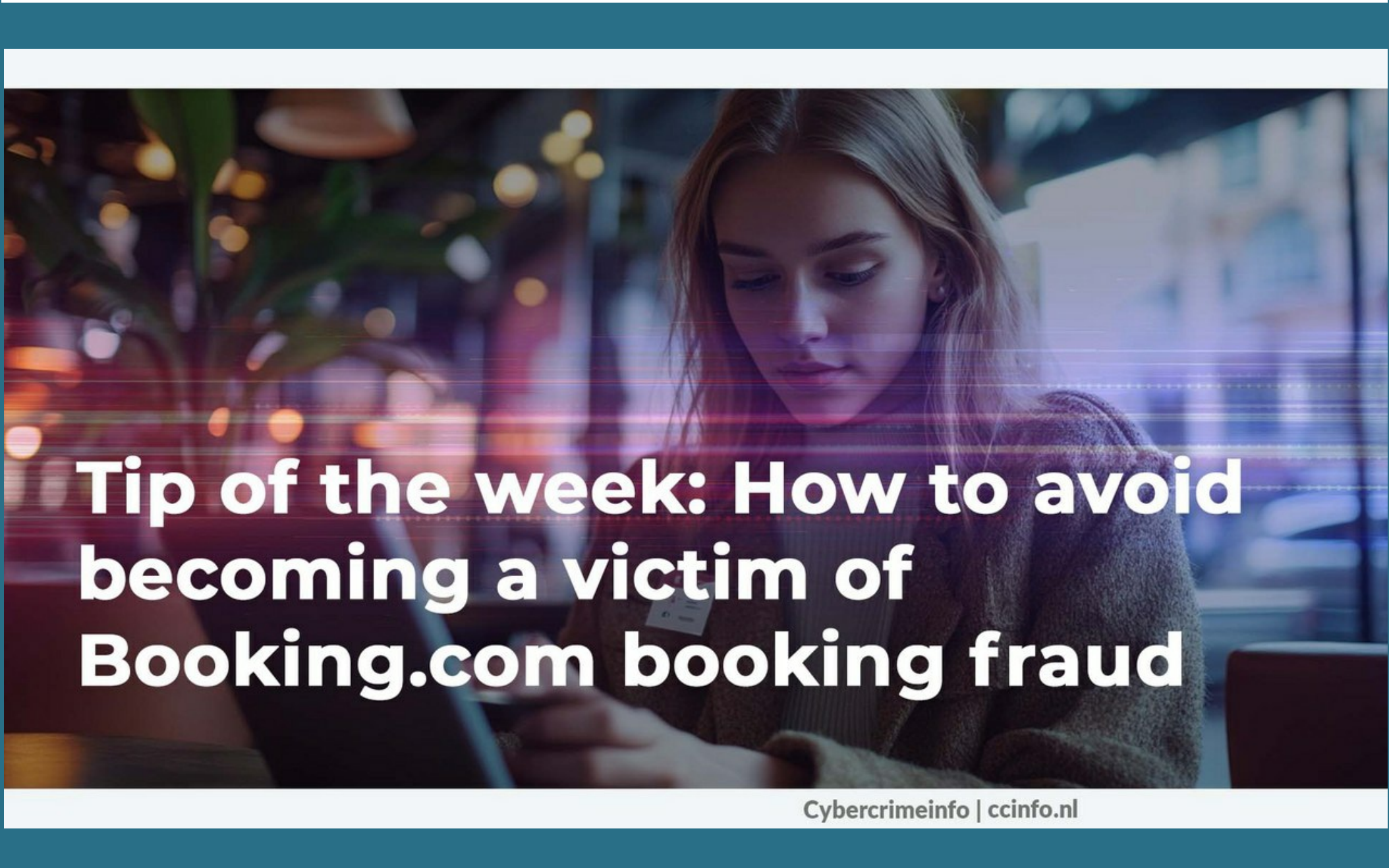
Lees verder

Reading in another language

Cyberdreigingen en digitale soevereiniteit

Europese bedrijven en overheden vertrouwen massaal op Amerikaanse clouddiensten zoals Microsoft 365 en Google Cloud. Dit biedt gemak, maar brengt ook grote risico's met zich mee. Juridische onzekerheden, cyberdreigingen en de mogelijkheid van plotselinge beleidswijzigingen zetten de digitale autonomie van Europa op het spel. Wat betekent deze afhankelijkheid voor de veiligheid van gevoelige data? En welke alternatieven zijn er om controle terug te winnen? In dit artikel duiken we in de kern van dit groeiende probleem en verkennen we strategieën om de digitale soevereiniteit van Europa te waarborgen.

Lees verder

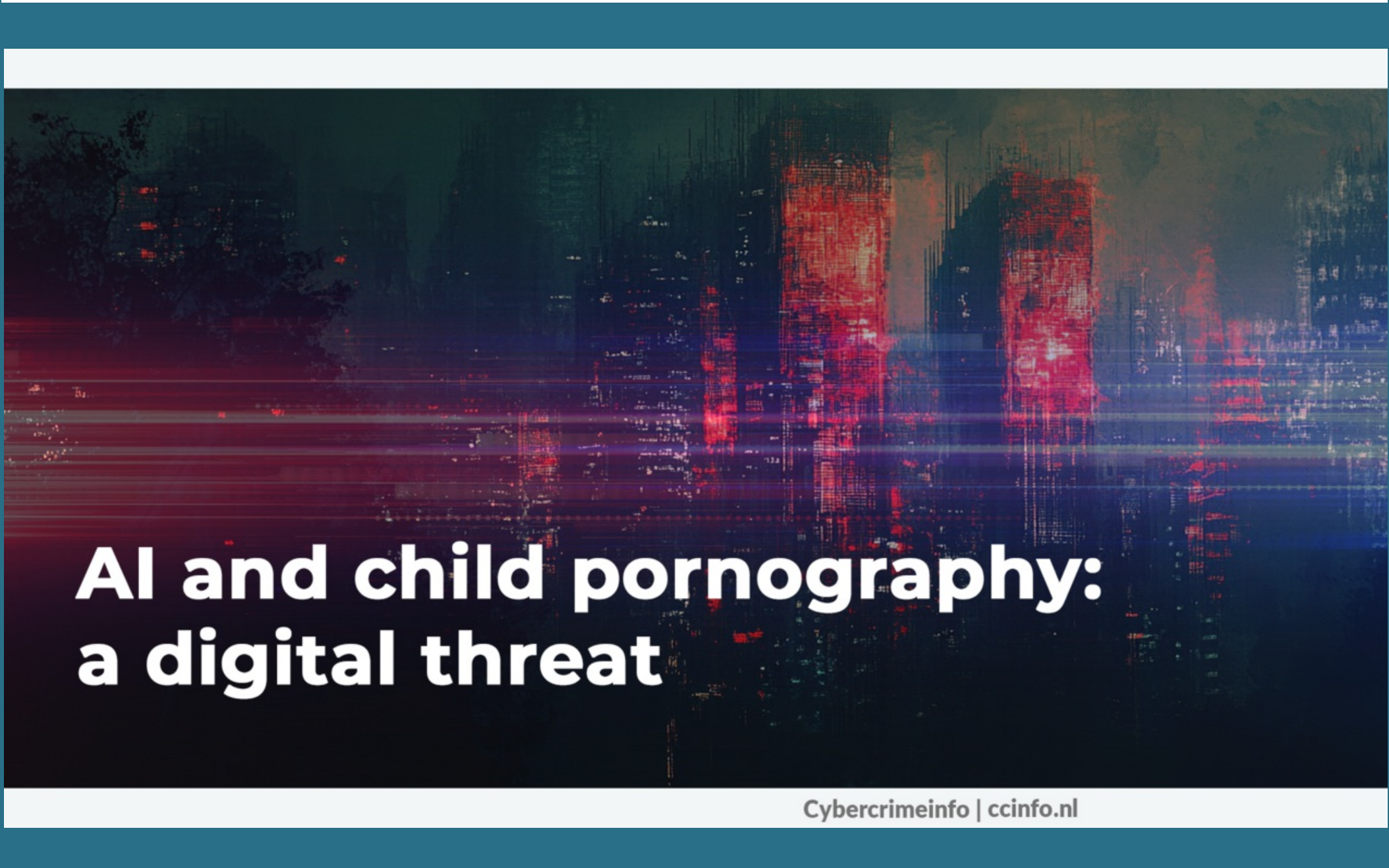


Reading in another language

Tip van de week: Hoe voorkom je dat je slachtoffer wordt van boekingsfraude op Booking.com?

De vakantieperiode komt eraan en duizenden mensen boeken enthousiast hun reis via platforms zoals Booking.com. Maar wist je dat cybercriminelen dit moment aangrijpen om nietsvermoedende reizigers op te lichten? Fraudeurs worden steeds geraffineerder en gebruiken onder andere kunstmatige intelligentie om overtuigende nepmails en phishingberichten te versturen.
Hoe herken je deze oplichtingstrucs? En belangrijker nog: hoe voorkom je dat je slachtoffer wordt? In dit artikel ontdek je de nieuwste fraudepraktijken en krijg je praktische tips om je boeking veilig te houden.

Lees verder

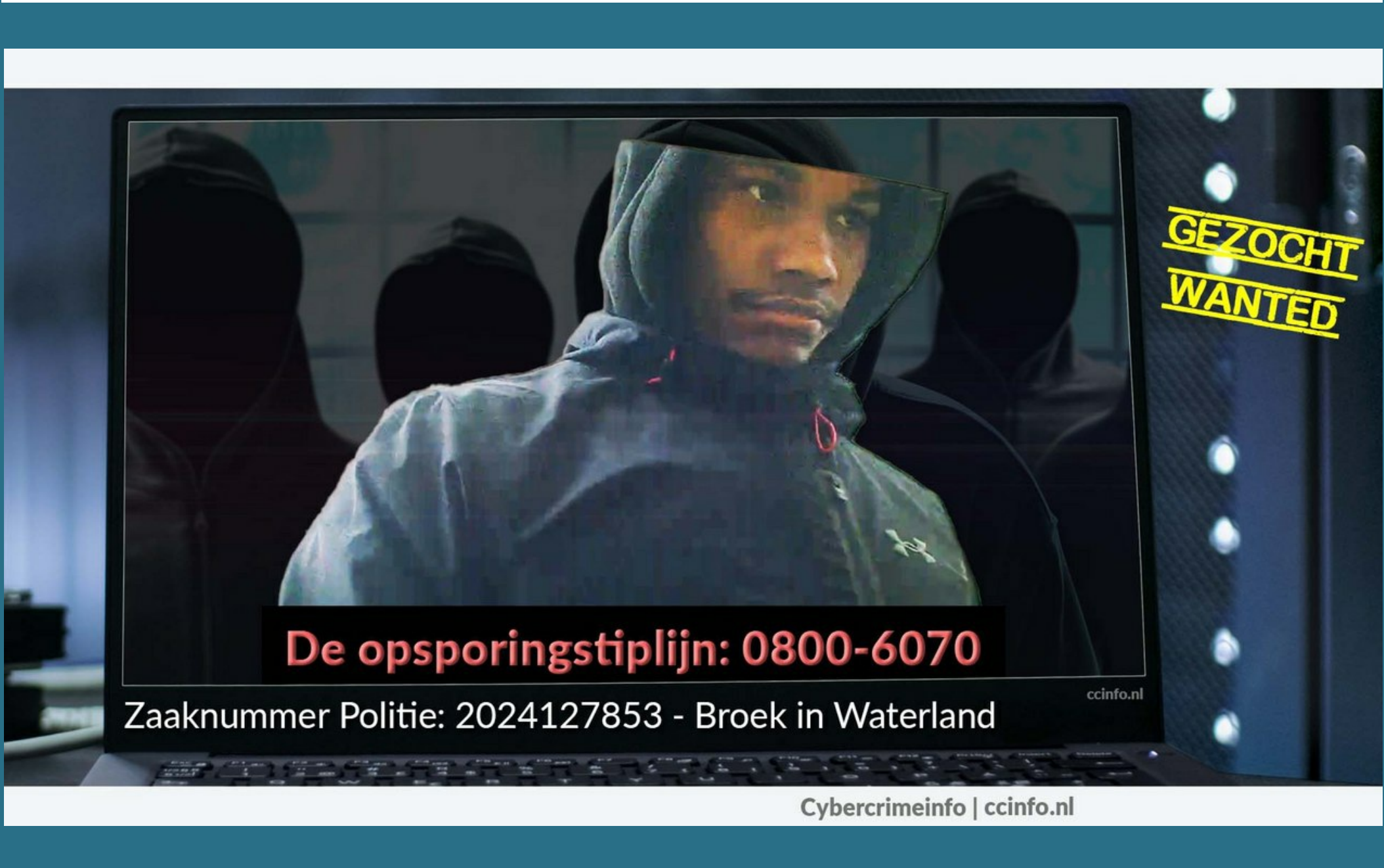


Reading in another language

AI en kinderpornografie: een digitale dreiging

De opkomst van kunstmatige intelligentie (AI) brengt niet alleen innovaties, maar ook ernstige misbruikkansen met zich mee. Criminelen zetten AI steeds vaker in om expliciete beelden te genereren, zonder dat er direct fysiek misbruik aan te pas komt. Dit maakt de opsporing complex en vergroot de uitdaging voor wetshandhavers wereldwijd.
Hoe werkt deze technologie? Wat doen internationale opsporingsdiensten om deze dreiging aan te pakken? En welke juridische en technologische maatregelen zijn nodig om dit groeiende probleem te bestrijden? In dit artikel duiken we in de schaduwzijde van AI en kinderpornografie en belichten we de wereldwijde strijd tegen deze digitale misdaad.

Lees verder

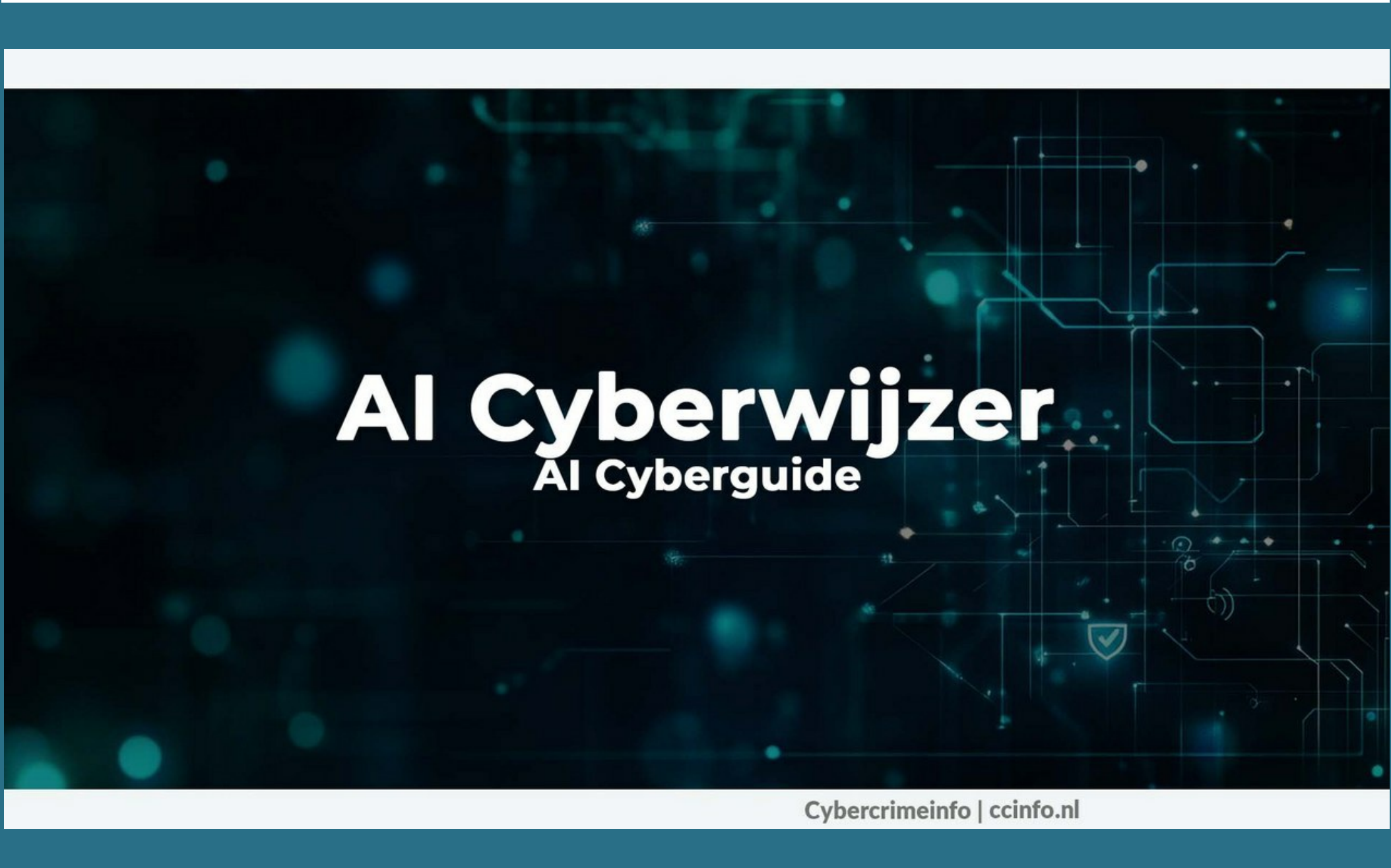


Reading in another language

Middelburg - Helpdesk fraude

In Broek in Waterland is een 81-jarige vrouw het slachtoffer geworden van een geraffineerde vorm van oplichting: bankhelpdeskfraude. Een nep-bankmedewerker wist haar zover te krijgen haar bankpas en geld af te geven, waarna er direct werd gepind. De dader is vastgelegd op camerabeelden, herken jij hem?
De politie roept op om mee te helpen bij de opsporing. Lees verder en ontdek hoe deze fraude in zijn werk gaat, hoe je jezelf en anderen kunt beschermen, en hoe je tips kunt doorgeven. Samen kunnen we deze criminelen stoppen!

Lees verder



AI-gids CyberWijzer: Kunstmatige intelligentie voor cyberveiligheid

De AI-gids CyberWijzer biedt een overzicht van hoe kunstmatige intelligentie (AI) kan helpen bij het verbeteren van cyberveiligheid. De gids bevat praktische tips en tools om AI effectief in te zetten tegen digitale dreigingen. Met de opkomst van cybercriminaliteit wordt AI steeds vaker gebruikt om aanvallen sneller te detecteren en te bestrijden. CyberWijzer helpt gebruikers om AI op een veilige en verantwoorde manier toe te passen, zowel voor bedrijven als particulieren. De gids behandelt onder andere het herkennen van verdachte activiteiten, het verbeteren van wachtwoordbeheer en het veilig omgaan met online data. Daarnaast is CyberWijzer zeer handig bij de implementatie van de NIS2-richtlijn, die strengere eisen stelt aan cybersecurity binnen bedrijven en organisaties. Door AI op de juiste manier te benutten, kunnen organisaties en individuen zich beter wapenen tegen cyberdreigingen.

AI CyberWijzer

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. Als onafhankelijke organisatie, volledig gedreven door vrijwilligers, zetten wij ons in om het publiek te informeren en beschermen tegen de gevaren van het digitale tijdperk.

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.

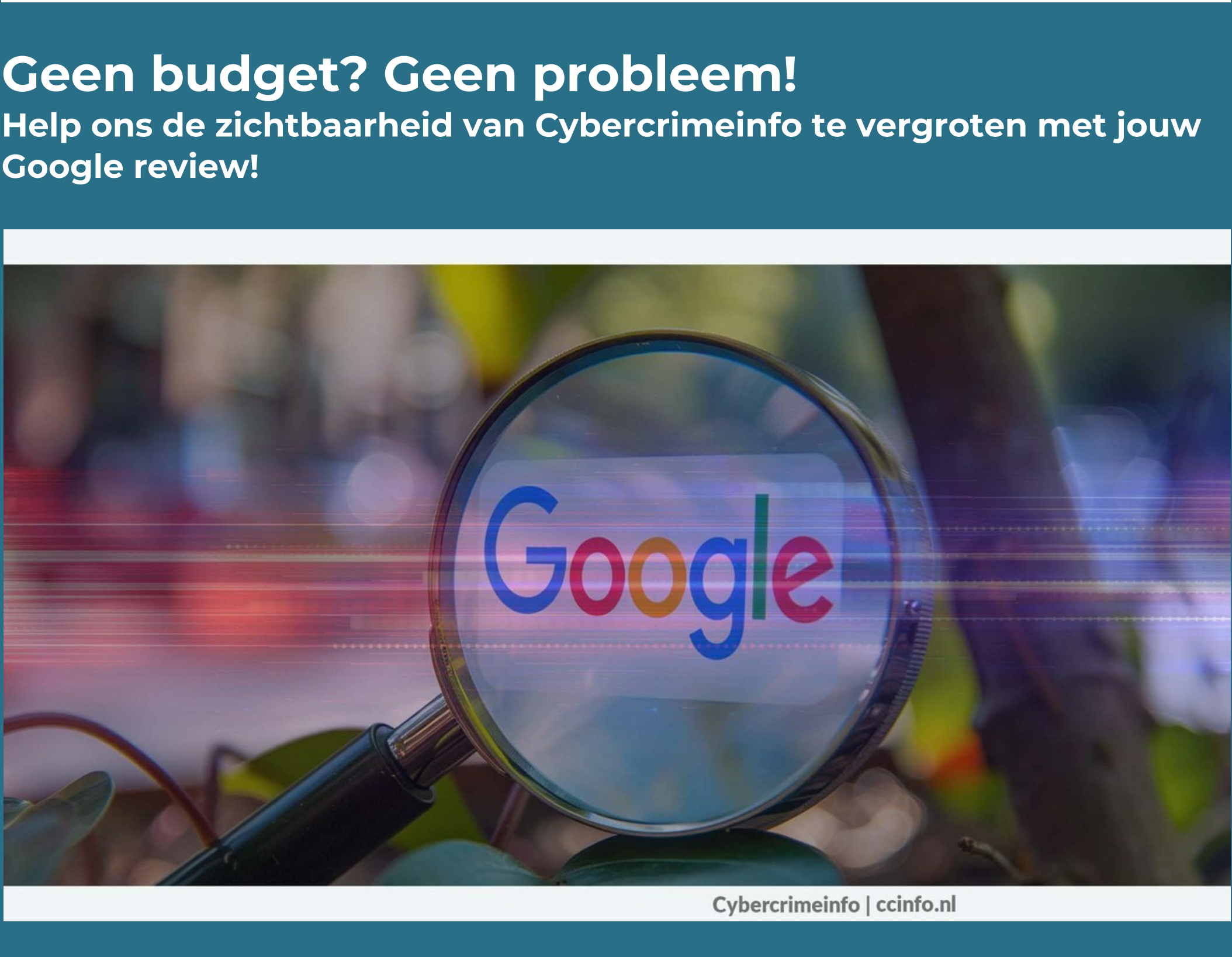
Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (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