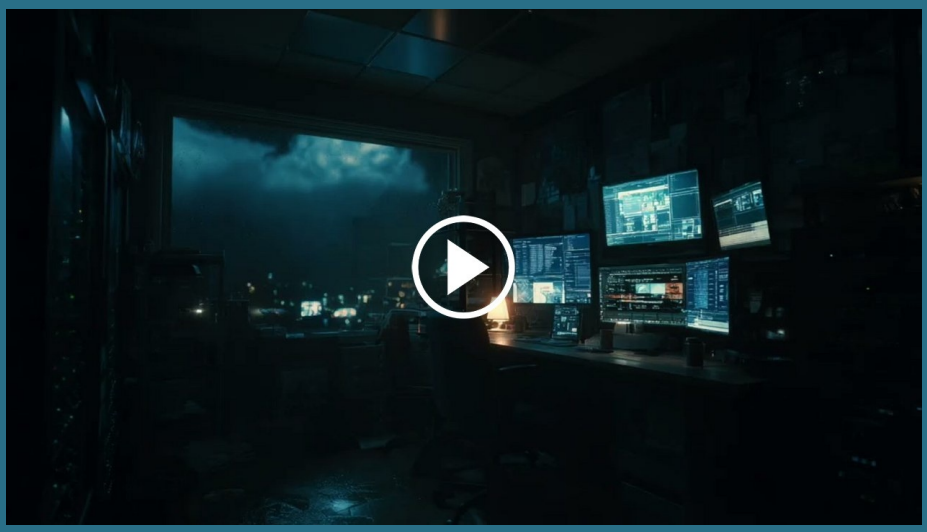
Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

Nieuwsbrief 378



Podcast

Podcast

Reading in another language

Halfjaarcijfers Fraudehelpdesk, de sluiproutes van oplichters van zoekresultaat tot financiële nachtmerrie

De eerste helft van 2025 laat een scherpe stijging zien in het aantal meldingen van digitale en telefonische fraude, waarbij oplichters steeds geraffineerdere methoden inzetten om slachtoffers te misleiden. Van misleidende verkoop en verborgen abonnementen tot nep-helpdesks en valse vacatures, de tactieken worden gevarieerder en moeilijker te doorzien. Hoewel de totale financiële schade nauwelijks veranderde, groeit de impact op slachtoffers merkbaar, zowel financieel als emotioneel. De cijfers van de Fraudehelpdesk schetsen een zorgwekkend beeld van een speelveld waar fraudeurs slim inspelen op zoekresultaten,

sociale media en telefonische benaderingen, en tonen de dringende noodzaak voor betere bescherming en bewustwording.

Lees verder

Reading in another language

Cyberaanvallen juli 2025: Van ransomware tot overheidshacks, wat betekent het voor België en Nederland?

De maand juli 2025 liet zien hoe kwetsbaar zowel bedrijven als overheidsinstellingen in België en Nederland zijn voor digitale dreigingen. Van gerichte ransomware aanvallen op zorginstellingen en bouwbedrijven tot het misbruiken van kwetsbaarheden in kritieke overheidssystemen, de incidenten tonen een zorgwekkende toename in omvang en complexiteit. Ook internationale aanvallen, zoals de diefstal van militaire gegevens en het misbruik van zeroday lekken, hebben directe gevolgen voor onze regio. In dit overzicht wordt duidelijk welke dreigingen het meest opvielen, wat hun impact was en waarom een sterke digitale verdediging belangrijker is dan ooit.

Lees verder

Reading in another language

Cyberoorlog juli 2025: Hoe digitale dreigingen de wereldorde herschikken

Juli 2025 liet opnieuw zien hoe het digitale strijdtoneel een beslissende

factor is geworden in internationale conflicten. Statelijke actoren, hacktivistische groeperingen en cybercriminelen voerden aanvallen uit die variëren van grootschalige DDoS-aanvallen tot geavanceerde malwarecampagnes, vaak met directe gevolgen voor kritieke infrastructuur. Nieuwe technieken, waaronder het gebruik van AI in malware, maken dreigingen moeilijker te detecteren en vergroten de impact op geopolitiek en economie. In dit overzicht leest u welke incidenten de afgelopen maand het digitale machtsspel hebben beïnvloed en welke risico's deze ontwikkelingen met zich meebrengen voor de veiligheid van landen en organisaties wereldwijd.

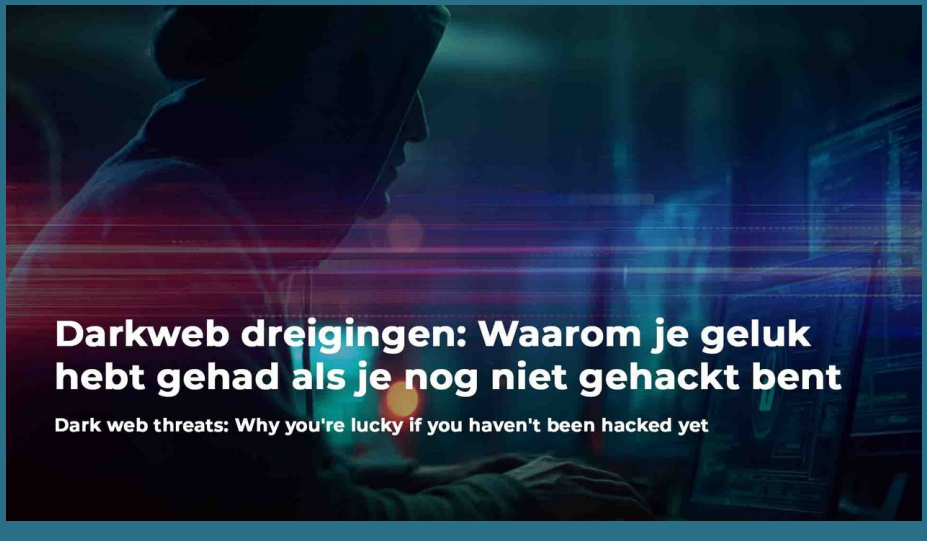
Lees verder

Reading in another language

Vraag van de week: Is lokaal uitgevoerde AI de nieuwe dreiging voor cybercriminaliteit?

AI-technologie ontwikkelt zich razendsnel en biedt ongekende mogelijkheden, maar de opkomst van lokaal uitgevoerde modellen zonder toezicht opent de deur naar nieuwe vormen van cybercriminaliteit. Waar grote aanbieders nog controlemechanismen hebben ingebouwd, kunnen deze lokale systemen volledig vrij worden ingezet, ook voor schadelijke doeleinden. Van geavanceerde phishingcampagnes tot onzichtbare malware en levensechte deepfakes, de risico's stapelen zich op. In dit artikel onderzoeken we hoe deze technologie werkt, welke gevaren ze met zich meebrengt en waarom waakzaamheid belangrijker is dan ooit.

Lees verder



Reading in another language

Darkweb dreigingen: Waarom je geluk hebt gehad als je nog niet gehackt bent

Het darkweb is een onzichtbare ontmoetingsplaats voor cybercriminelen, waar nieuwe kwetsbaarheden, aanvalstechnieken en gestolen gegevens snel worden gedeeld. Wat voor veel organisaties een theoretisch risico lijkt, wordt hier in korte tijd omgezet in een concreet plan voor een aanval. In besloten groepen worden beveiligingslekken besproken die vaak nog niet publiekelijk bekend zijn, waardoor bedrijven en overheden zonder het te weten een aantrekkelijk doelwit vormen. Dit artikel neemt je mee in de actuele dreigingen die in deze digitale onderwereld circuleren, laat zien welke systemen in Nederland en België direct gevaar lopen en benadrukt waarom snel patchen het verschil kan maken tussen veiligheid en een kostbare inbraak.

Lees verder

Reading in another language

Zaandam - Helpdesk fraude

In Zaandam is een vrouw slachtoffer geworden van een geraffineerde vorm van bankhelpdeskfraude waarbij criminelen zich voordeden als bankmedewerkers en meer dan tienduizend euro buitmaakten via valse pinbetalingen. Het slachtoffer werd langdurig aan de lijn gehouden, onder druk gezet en misleid met overtuigende verhalen over een dreigend veiligheidsrisico. De politie is op zoek naar de verdachte en roept het publiek op om mee te helpen bij de opsporing. Dit incident laat zien hoe geraffineerd en overtuigend deze vorm van oplichting kan zijn en benadrukt het belang van alertheid bij onverwachte telefoontjes of verzoeken om bankgegevens.

Lees verder

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.

AI Chatbots Cybercrimeinfo

AI Chatbots | Ontdek **CyberWijzer**, **RechtRaadgever** en **NIS2Wijzer**, 24/7 beschikbaar voor hulp bij cybercriminaliteit, strafrecht en NIS2-wetgeving. Als je hulp nodig hebt bij het installeren of gebruiken van MindYourPass, gebruik dan AI Gids **VeiligSlot**. De AI **HRMWijzer** bevindt zich momenteel in de testfase van ontwikkeling en biedt richtlijnen en informatie over verschillende aspecten van HRM binnen de politie.

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.

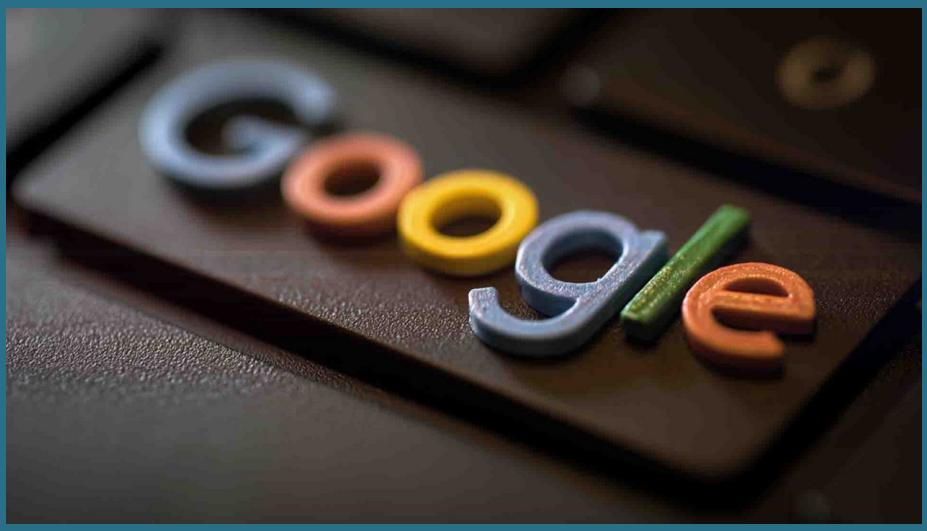
Met vriendelijke groet,
Het team van Cybercrimeinfo

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