Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

Nieuwsbrief 366

Podcast

Reading in another language

LockBit gehackt: Het onmogelijke gebeurt en onthult een duistere wereld van ransomware

In een onverwachte wending werd LockBit, een van de grootste en meest gevreesde ransomwaregroepen ter wereld, zelf het slachtoffer van een hack. Dit incident onthult niet alleen de interne werking van de groep, maar biedt ook een zeldzaam kijkje in de onderhandelingsstrategieën en financiële praktijken van cybercriminelen. De gelekte gegevens werpen een nieuw licht op de dreiging van ransomware en bieden belangrijke lessen voor organisaties die zich willen wapenen tegen dergelijke aanvallen. Wat betekent dit voor de toekomst van cybercriminaliteit en wat kunnen we leren van de onthullingen? Lees verder om meer te ontdekken over de impact van deze historische gebeurtenis.

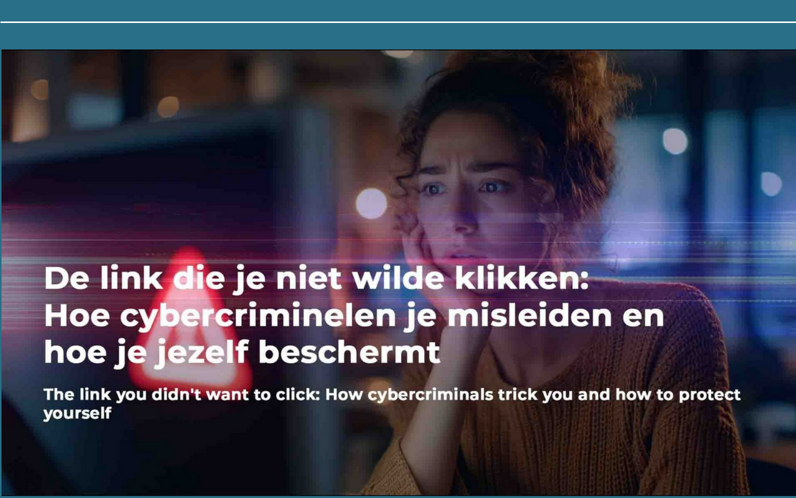
Lees verder

Reading in another language

Cyberdreigingen in de luchtvaart, hoe veilig is de lucht boven ons?

De luchtvaartsector is steeds meer afhankelijk van digitale systemen, wat nieuwe kwetsbaarheden met zich meebrengt. Cyberdreigingen zoals datadiefstal, ransomware en GPS-storingen kunnen de veiligheid van luchtvaartoperaties ernstig ondermijnen. Geopolitieke spanningen spelen hierin een steeds grotere rol, waardoor de risico's verder toenemen. Dit artikel onderzoekt de huidige cyberdreigingen in de luchtvaart, de impact van geopolitieke ontwikkelingen, en de maatregelen die genomen worden om de sector te beschermen. Hoe veilig is de lucht boven ons? Lees verder voor een diepgaande blik op de uitdagingen en oplossingen.

Lees verder



Reading in another language

De link die je niet wilde klikken: Hoe cybercriminelen je misleiden en hoe je jezelf beschermt

In de digitale wereld van vandaag worden cybercriminelen steeds slimmer in het misleiden van gebruikers. Via technieken zoals phishing, clickjacking en clickfix proberen ze je onbewust naar schadelijke websites te lokken of zelfs je persoonlijke gegevens te stelen. Dit artikel onthult hoe deze aanvallen werken en biedt concrete tips om jezelf te beschermen tegen deze geavanceerde bedreigingen. Lees verder om te ontdekken hoe je je kunt wapenen tegen deze digitale valstrikken.

Lees verder

Reading in another language

De digitale revolutie van criminaliteit: Hoe het OM de strijd aangaat

De digitale criminaliteit groeit in rap tempo, en met deze toename neemt ook de complexiteit van de dreigingen toe. Het Openbaar Ministerie (OM) speelt een cruciale rol in de strijd tegen deze misdrijven, en in 2024 wordt er flink ingezet op geavanceerde technologieën en gespecialiseerde teams. In dit artikel duiken we in de ontwikkelingen, trends en strategieën die het OM toepast om deze nieuwe golf van cybercriminaliteit te bestrijden. Wat zijn de grootste uitdagingen en wat kunnen we in de toekomst verwachten van de aanpak van digitale misdrijven? Lees verder voor een diepere kijk op deze digitale revolutie.

Lees verder

Reading in another language

Hoe een cyberaanval op de NWO het darkweb bereikte: de jacht op een internationale cybercrimineel

In 2021 werd de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO) getroffen door een ernstige ransomware-aanval, waarbij gevoelige data werd gestolen en het darkweb bereikte. Wat aanvankelijk leek op een lokale dreiging, ontvouwde zich als een internationale jacht op een cybercrimineel die verantwoordelijk was voor de aanval. Dit artikel werpt een licht op de arrestatie van de verdachte in Moldavië, de wereldwijde samenwerking die tot deze doorbraak leidde en de rol die het darkweb speelt in het verspreiden van gestolen informatie. Ontdek hoe grensoverschrijdende samenwerking de strijd tegen cybercriminaliteit vooruit helpt en welke impact dergelijke aanvallen kunnen hebben op wetenschappelijke instituten en de bredere samenleving.

Lees verder

Reading in another language

Rotterdam - Helpdesk fraude

In Rotterdam werd onlangs een vrouw bijna het slachtoffer van een sluwe bankhelpdeskfraude. Een man die zich voordeed als bankmedewerker probeerde haar te overtuigen dat er verdachte transacties op haar rekening stonden en vroeg om haar pinpas op te halen. Gelukkig weigerde ze hem binnen te laten, maar de verdachte is nog steeds onvindbaar. Herken jij deze man? Lees verder en ontdek hoe deze vorm van cybercriminaliteit werkt en hoe je jezelf kunt beschermen tegen dergelijke oplichting.

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.

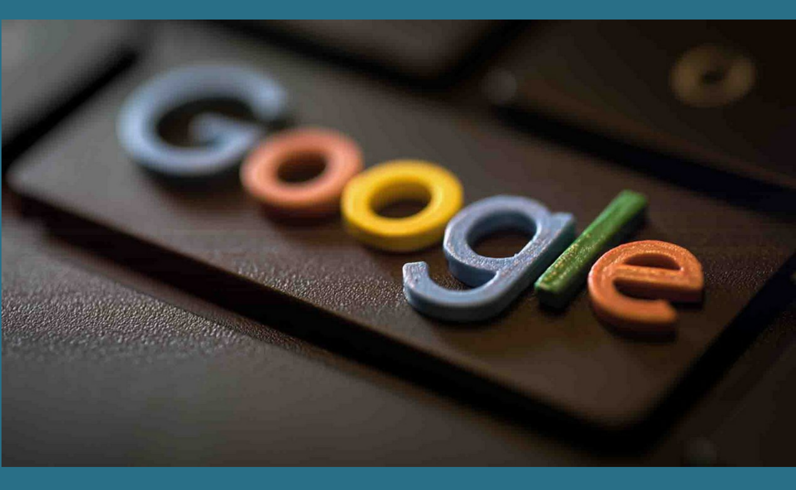
Met vriendelijke groet,
Het team van Cybercrimeinfo

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

Deze e-mail is verstuurd aan [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.