



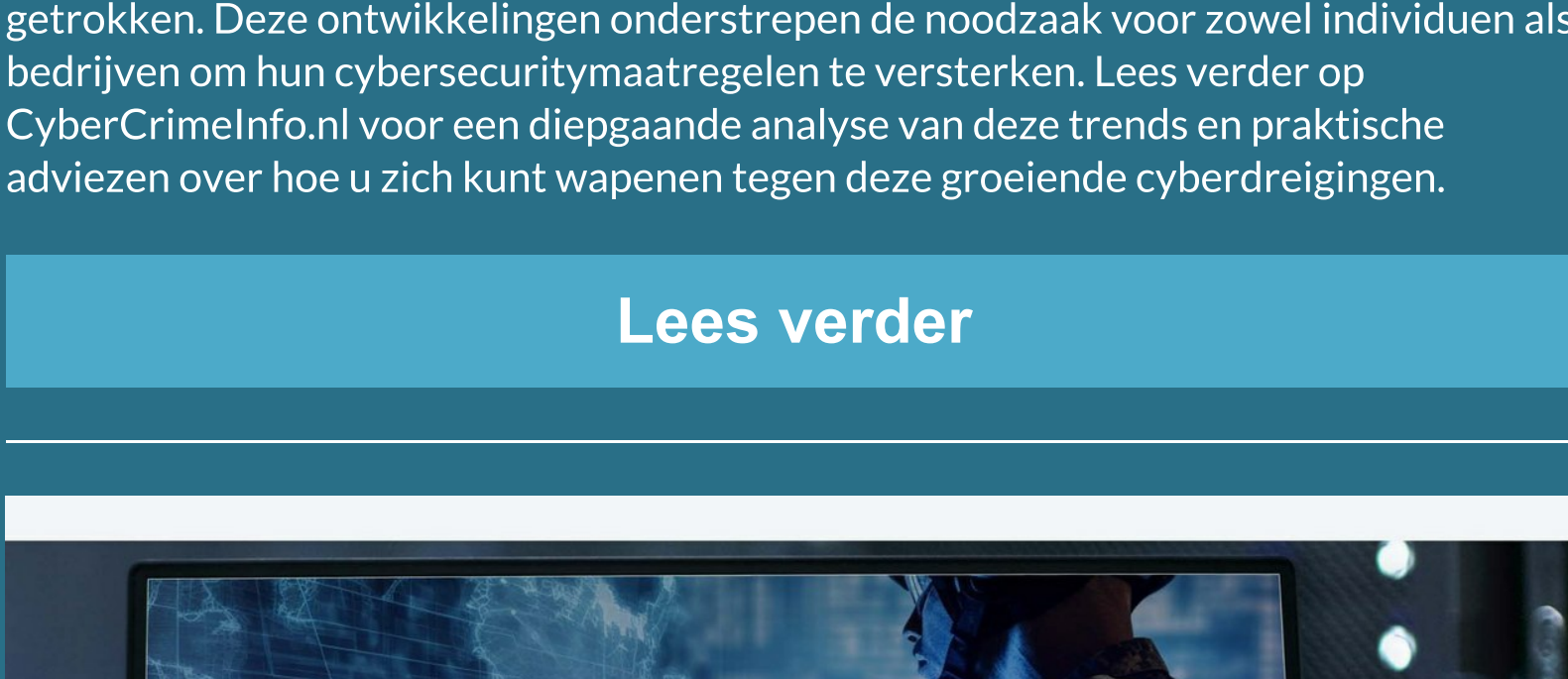
Nieuwsbrief 291 - Week 49-2023



De ongeziene dreiging: Mobiele veiligheid in 2023

In het artikel "De ongeziene dreiging: Mobiele veiligheid in 2023", gepubliceerd op CyberCrimelInfo.nl, wordt de toegenomen afhankelijkheid van mobiele apparaten in ons dagelijks leven belicht. Met de verschuiving van dataopslag naar de cloud, worden deze apparaten een aantrekkelijker doelwit voor cyberaanvallen. Dit brengt aanzienlijke veiligheidsrisico's met zich mee, niet alleen voor individuen, maar ook voor bedrijven die vaak vertrouwen op het principe van Bring Your Own Device (BYOD). Het artikel gaat dieper in op de complexiteit van cyberaanvallen op mobiele apparaten, zoals phishing en malware, en benadrukt het belang van bewustzijn en technologische beveiliging. Verder wordt de noodzaak voor organisaties besproken om een balans te vinden tussen sterke beveiligingsmaatregelen en gebruiksgemak voor werknemers. Lees het volledige artikel voor een uitgebreide analyse en praktische tips over hoe om te gaan met deze ongeziene mobiele bedreigingen in 2023.

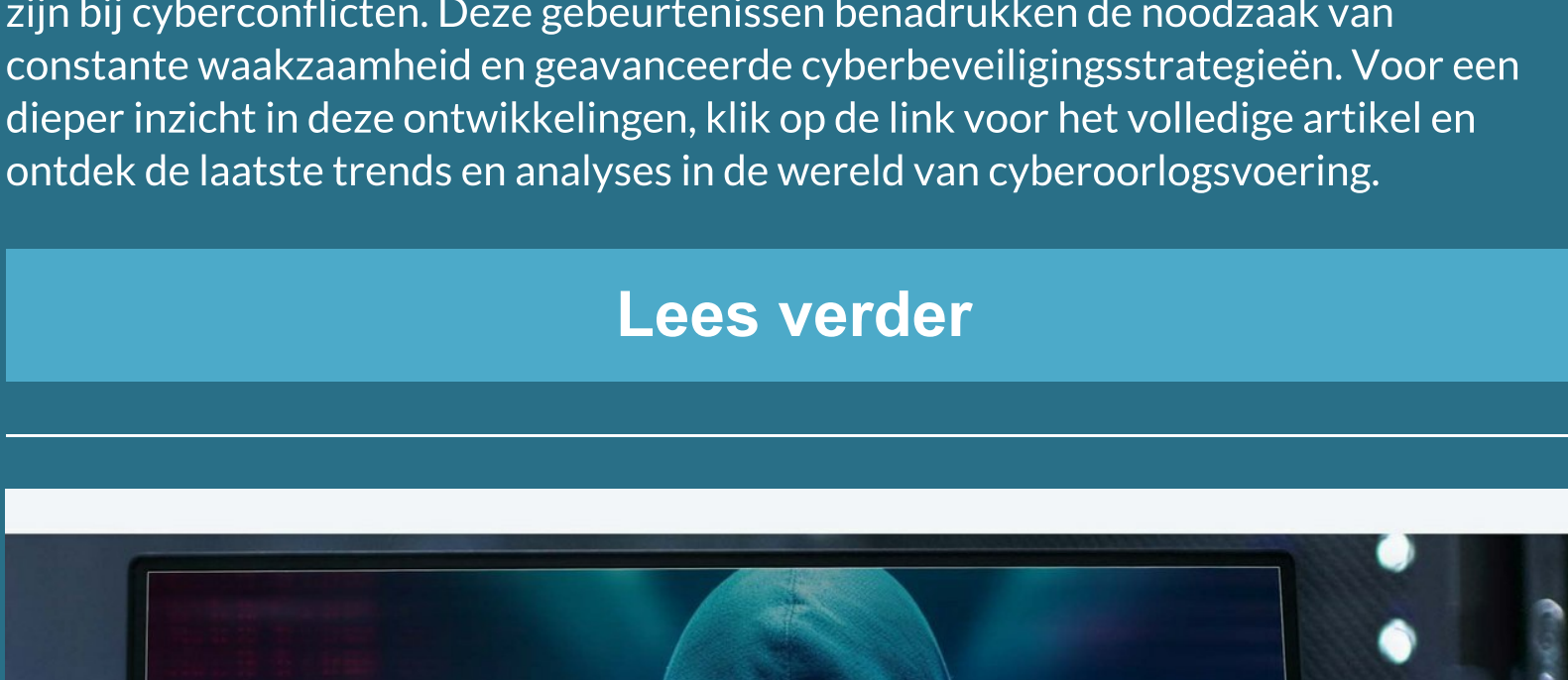
[Lees verder](#)



Darkweb discussies ontmaskerd: Cyberdreigingen in 2024

In het artikel "Darkweb discussies ontmaskerd: Cyberdreigingen in 2024" belichten we de meest recente en verontrustende trends op het darkweb. Dit jaar zien we een verontrustende toename van gelekte naaktfoto's, vaak gestolen van sociale mediaplatforms, die een significante privacybedreiging vormen. AI-geassisteerde cyberaanvallen worden ook steeds geavanceerder, met kwaadaardige chatbots die phishing-aanvallen automatiseren. De opkomst van amateurhackers, die hun kennis en tools op het darkweb delen, vormt een nieuwe uitdaging. Daarnaast wordt de betrouwbaarheid van biometrische authenticatiemethoden steeds vaker in twijfel getrokken. Deze ontwikkelingen onderstrepen de noodzaak voor zowel individuen als bedrijven om hun cybersecuritymaatregelen te versterken. Lees verder op CyberCrimelInfo.nl voor een diepgaande analyse van deze trends en praktische adviezen over hoe u zich kunt wapenen tegen deze groeiende cyberdreigingen.

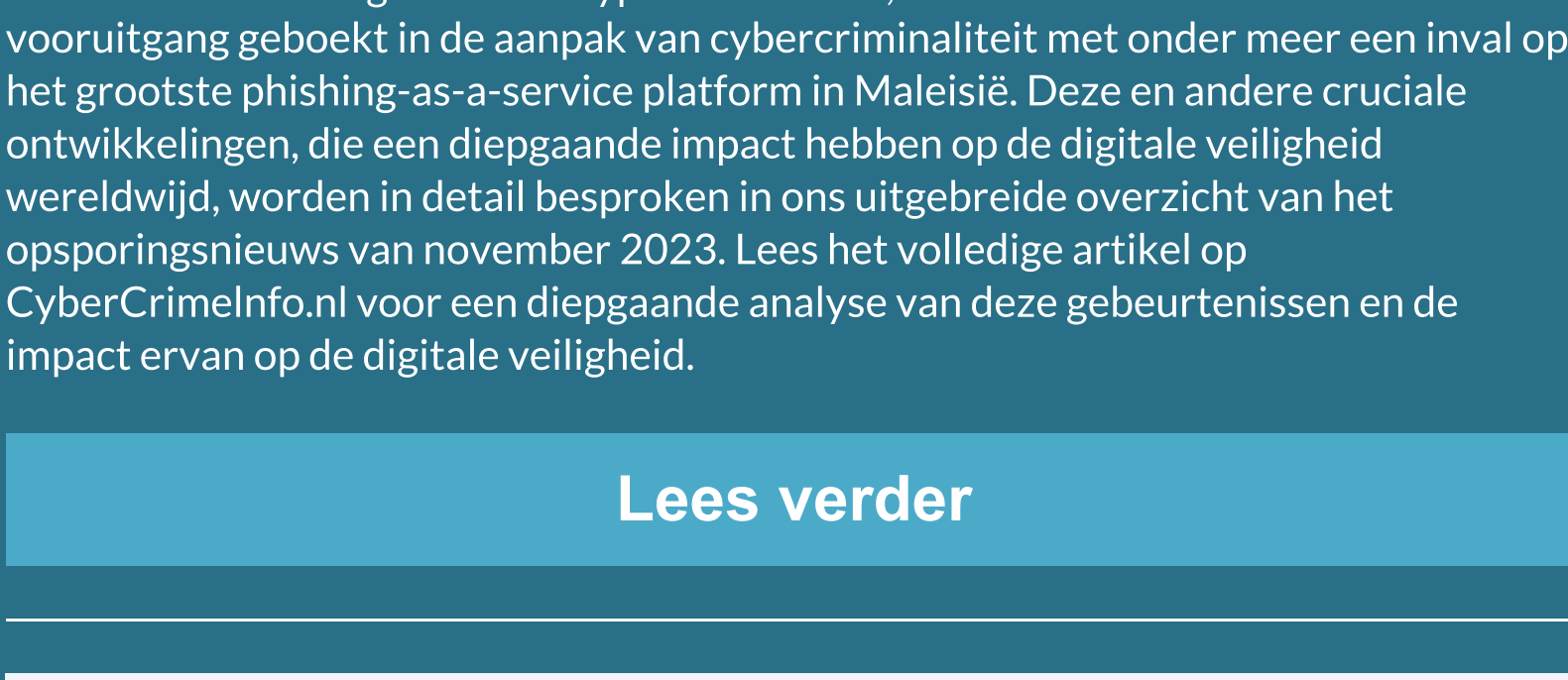
[Lees verder](#)



Cyberwar nieuws 2023 oktober en november

In oktober en november 2023 heeft de wereld van de cyberoerlogvoering een reeks ingrijpende gebeurtenissen meegemaakt. De complexiteit en reikwijdte van cyberaanvallen nemen toe, waarbij zowel statelijke als niet-statelijke actoren betrokken zijn. Russische aanvallers hebben ambassades en kritieke infrastructures in verschillende landen aangevallen, terwijl Oekraïne offensieve cyberoperaties uitvoerde tegen Rusland. Tegelijkertijd maakt Hamas gebruik van cryptocurrency voor financiering en voeren ze cyberaanvallen uit, terwijl Israël en Iran ook betrokken zijn bij cyberconflicten. Deze gebeurtenissen benadrukken de noodzaak van constante waakzaamheid en geavanceerde cyberbeveiligingsstrategieën. Voor een dieper inzicht in deze ontwikkelingen, klik op de link voor het volledige artikel en ontdek de laatste trends en analyses in de wereld van cyberoerlogvoering.

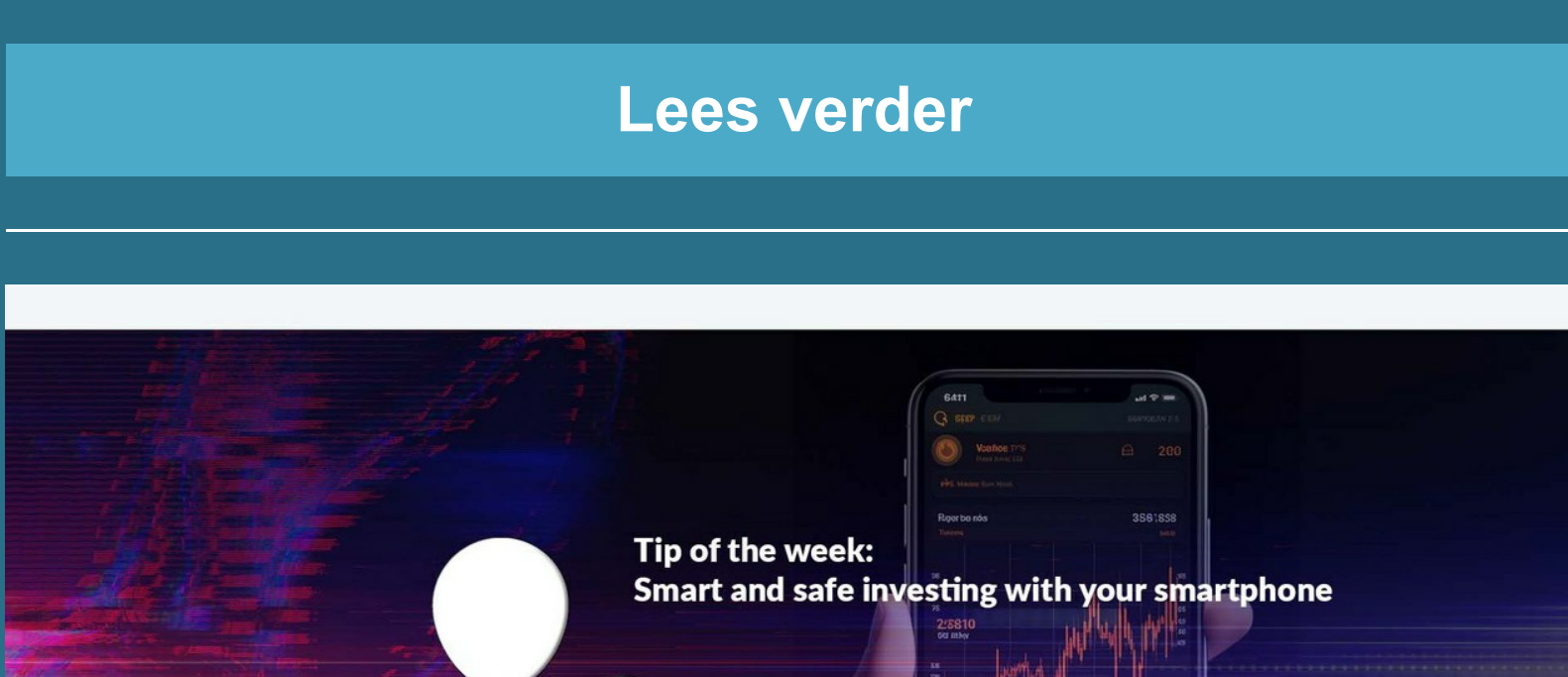
[Lees verder](#)



Politie cyber nieuws 2023 november

In november 2023 werd de cybercriminaliteitswereld opgeschrikt door diverse opmerkelijke gebeurtenissen en belangrijke doorbraken in opsporingsonderzoeken. In Nederland domineerde de onthulling van grootschalige bankhelpdeskfraude het nieuws, met honderden slachtoffers en de arrestatie van verdachten die een geraffineerde werkwijze hanteerden. De rechtbank in Amsterdam speelde een cruciale rol in een significante cryptofraudezaak, en internationaal werd er vooruitgang geboekt in de aanpak van cybercriminaliteit met onder meer een inval op het grootste phishing-as-a-service platform in Maleisië. Deze en andere cruciale ontwikkelingen, die een diepgaande impact hebben op de digitale veiligheid wereldwijd, worden in detail besproken in ons uitgebreide overzicht van het opsporingsnieuws van november 2023. Lees het volledige artikel op CyberCrimelInfo.nl voor een diepgaande analyse van deze gebeurtenissen en de impact ervan op de digitale veiligheid.

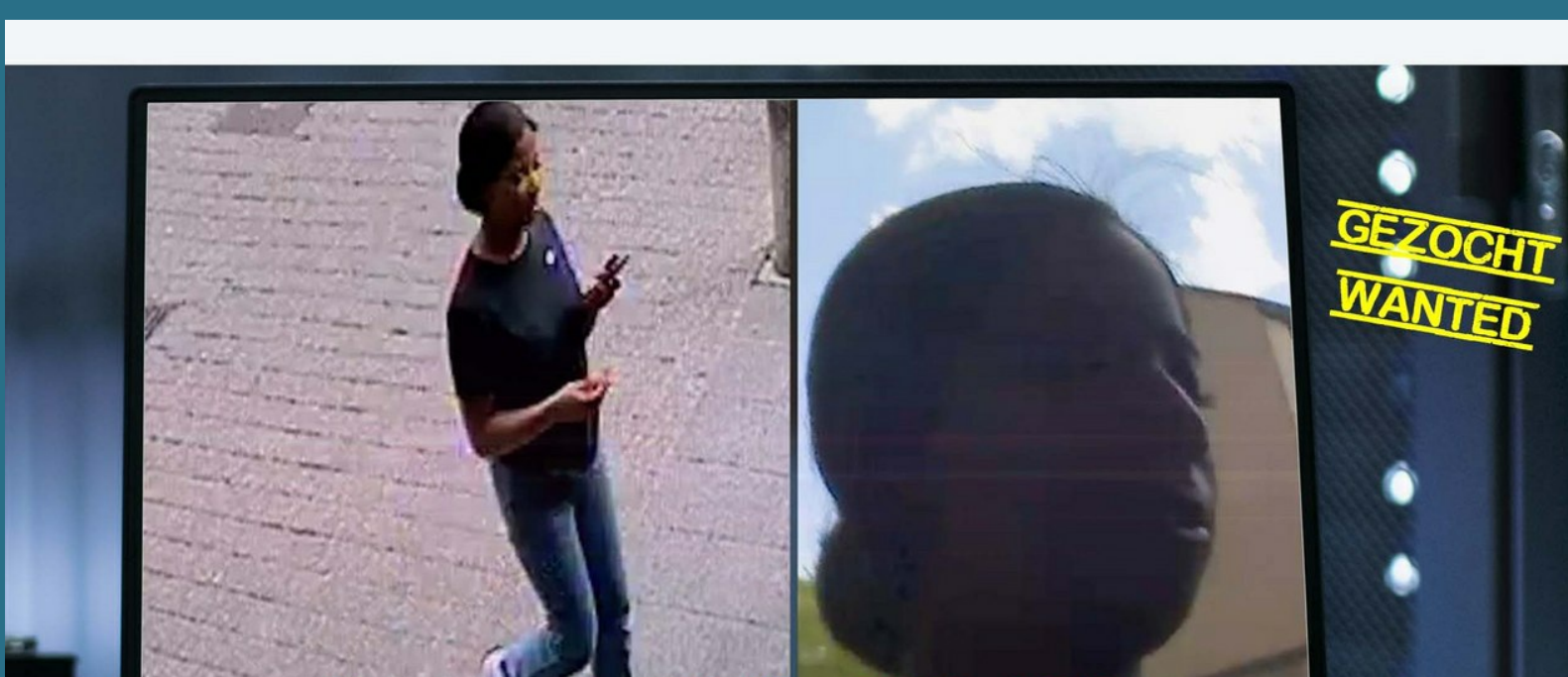
[Lees verder](#)



Overzicht van slachtoffers cyberaanvallen week 48-2023

In week 48 van 2023 zagen we wereldwijd een opmerkelijke toename in de frequentie als de verwijzing van cyberaanvallen. Deze week werd gekenmerkt door diverse incidenten, van gerichte ransomware-aanvallen op vooraanstaande bedrijven tot geavanceerde phishing- en malware campagnes. In Nederland werden bedrijven als Skalar.com en Smidts Autogroep het doelwit, waarbij de Medusa Locker Ransomware werd gebruikt. Ook in België werden bedrijven, zoals IRC Engineering en de online retailer Medi-Market, niet gespaard. Deze reeks aanvallen laat zien hoe cruciaal het is voor bedrijven om hun digitale beveiligingsmaatregelen voortdurend te evalueren en te versterken. Om een gedetailleerd overzicht te krijgen van deze en andere recente cyberaanvallen, inclusief inzichten en tips voor het verbeteren van digitale beveiliging, nodigen wij u uit om verder te lezen op onze website.

[Lees verder](#)



Tip van de week: Slim en veilig beleggen met je smartphone

In het digitale tijdperk waarin smartphones een integraal onderdeel van ons leven vormen, is mobiel beleggen steeds populairder geworden. Echter, met deze toename in populariteit komen ook nieuwe veiligheidsrisico's. Ons nieuwste artikel op Cybercrimeinfo.nl gaat dieper in op hoe je slim en veilig kunt beleggen met je smartphone. We bespreken de cruciale aspecten van mobiele veiligheid, zoals het gebruik van sterke wachtwoorden, het regelmatig bijwerken van apps en besturingssystemen, en het alert zijn op phishing en malware. Verder behandelen we specifieke risico's en beschermingsstrategieën bij mobiel beleggen, en het belang van netwerkbeveiliging. Deze informatie is essentieel voor iedereen die zijn financiële activiteiten via een smartphone beheert.

[Lees verder](#)



Nieuwegein - Bankhelpdesk fraude

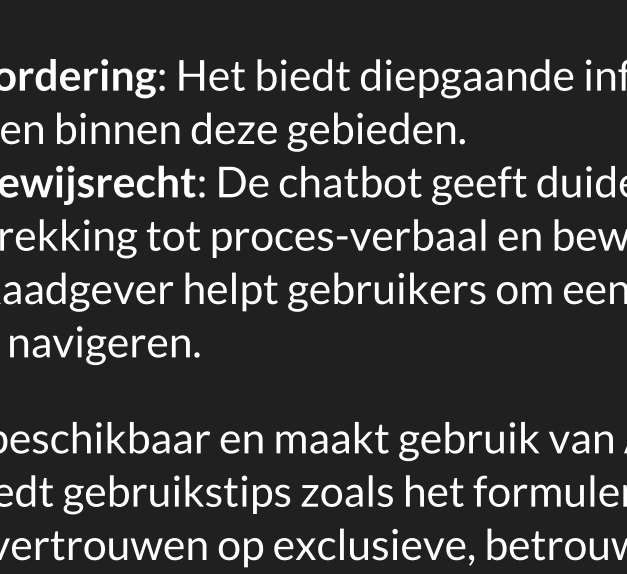
In Nieuwegein is een ernstig geval van bankhelpdesk fraude gebeurd, waarbij een 84-jarige vrouw slachtoffer werd. Ze kreeg een telefoontje van een persoon die zich voordeed als bankmedewerker, met de waarschuwing over een dreigend financieel gevaar. Ondanks aanvankelijke twijfels, overhandigde de vrouw uiteindelijk haar pinpas en waardevolle spullen. Kort daarna werd er met haar gestolen pinpas honderden euro's opgenomen. De politie heeft een signalement van de vermoedelijke dader vrijgegeven en roept getuigen op om informatie te delen. Dit voorval onderstreept het belang van alert blijven op dergelijke frauduleuze praktijken.

[Lees verder](#)

AI Gids CyberWijzer

De **AI Gids CyberWijzer** is een geavanceerde AI Chatbot, aangeboden door Cybercrimeinfo. Deze chatbot gebruikt een aangepaste versie van ChatGPT-4 om betrouwbare en actuele informatie te verstrekken over cybercriminaliteit, het darkweb en cybersecurity. CyberWijzer is exclusief verbonden met de Cybercrimeinfo-database, waardoor het een veelzijdige bron is voor een breed scala aan doelgroepen. Deze omvatten beginners, gevorderden, cybercrime experts, CISO's, ondernemers, burgers, kinderen, IT professionals, studenten, juridische professionals, beleidsmakers, ontwikkelaars, malware analisten, en ICS en OT beheerders. Het biedt informatie over onderwerpen zoals cyberveiligheid, financiële fraude, ransomware, netwerkbeveiliging, en meer.

CyberWijzer is ontworpen om intuïtief en veilig te zijn, met eenvoudige navigatie en heldere uitleg. Het waarborgt privacy en veiligheid door geavanceerde encryptie en naleving van privacyregulering.



[Download QR code](#)

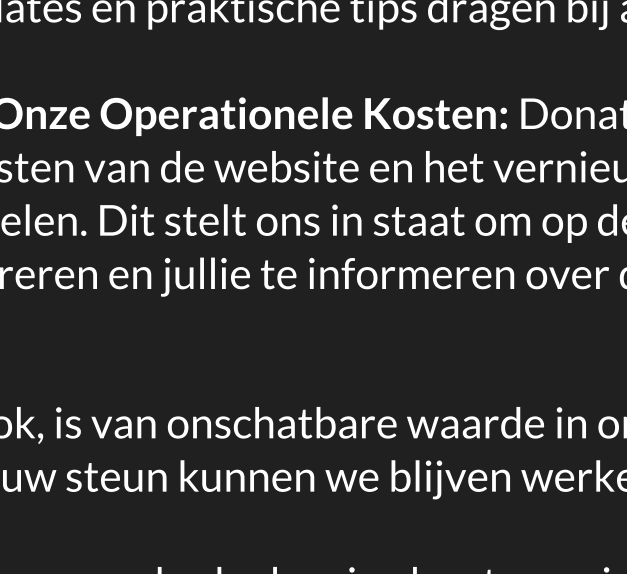
AI Gids RechtRaadgever

De **AI Gids RechtRaadgever** is een chatbot ontwikkeld voor gebruik in het gebied van strafrecht en strafvordering. Het is ontworpen om efficiënte, snelle en nauwkeurige antwoorden te bieden in het steeds veranderende digitale landschap. Deze chatbot dient als een essentiële bron voor opsporingsambtenaren, hulpofficieren en iedereen die geïnteresseerd is in strafrecht. De expertisegebieden van RechtRaadgever omvatten:

- **Strafrecht en Strafvordering:** Het biedt diepgaande informatie over een breed scala aan onderwerpen binnen deze gebieden.
- **Proces-verbaal en Bewijsrecht:** De chatbot geeft duidelijke en accurate antwoorden met betrekking tot proces-verbaal en bewijsrecht.
- **Wetteksten:** RechtRaadgever helpt gebruikers om eenvoudig door complexe juridische materie te navigeren.

RechtRaadgever is 24/7 beschikbaar en maakt gebruik van AI-technologie die continue leert en verbetert. Het biedt gebruikstips zoals het formuleren van duidelijke, specifieke vragen en het vertrouwen op exclusieve, betrouwbare bronnen. De chatbot garandeert een vertrouwelijke omgeving met privacybescherming, en moedigt gebruikers aan om te experimenteren met verschillende vragen om de capaciteiten van de chatbot te leren kennen.

De chatbot is gebruiksvriendelijk en veilig, met gemakkelijke navigatie, duidelijke antwoorden, geavanceerde encryptie en privacybescherming.



[Download QR code](#)

Waarom jouw donatie aan Cybercrimeinfo.nl essentieel is

Beste lezer,

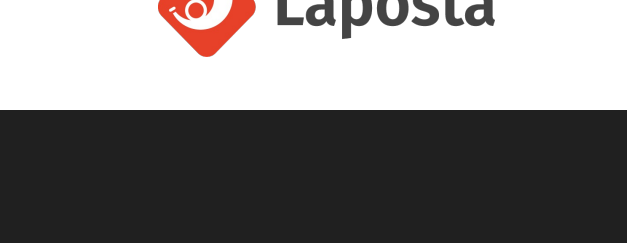
In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo.nl een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk. Jouw donatie maakt het verschil. Hier is waarom:

1. **Onafhankelijke en Belangrijke Bron van Informatie:** Cybercrimeinfo.nl is geen onderdeel van de Nederlandse Politie. Het is ontworpen om efficiënte, snelle en nauwkeurige antwoorden te bieden in het steeds veranderende digitale landschap. Deze chatbot dient als een essentiële bron voor opsporingsambtenaren, hulpofficieren en iedereen die geïnteresseerd is in strafrecht. De expertisegebieden van RechtRaadgever omvatten:
- **Strafrecht en Strafvordering:** Het biedt diepgaande informatie over een breed scala aan onderwerpen binnen deze gebieden.
- **Proces-verbaal en Bewijsrecht:** De chatbot geeft duidelijke en accurate antwoorden met betrekking tot proces-verbaal en bewijsrecht.
- **Wetteksten:** RechtRaadgever helpt gebruikers om eenvoudig door complexe juridische materie te navigeren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen. We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de [WhyDonate pagina](#) of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo.nl



[Download QR code](#)

Share Tweet Share Pinterest

Deze e-mail is verzonden aan {{email}}. • Als u geen e-mails meer wilt ontvangen, kunt u zich [hier afmelden](#). • Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.

