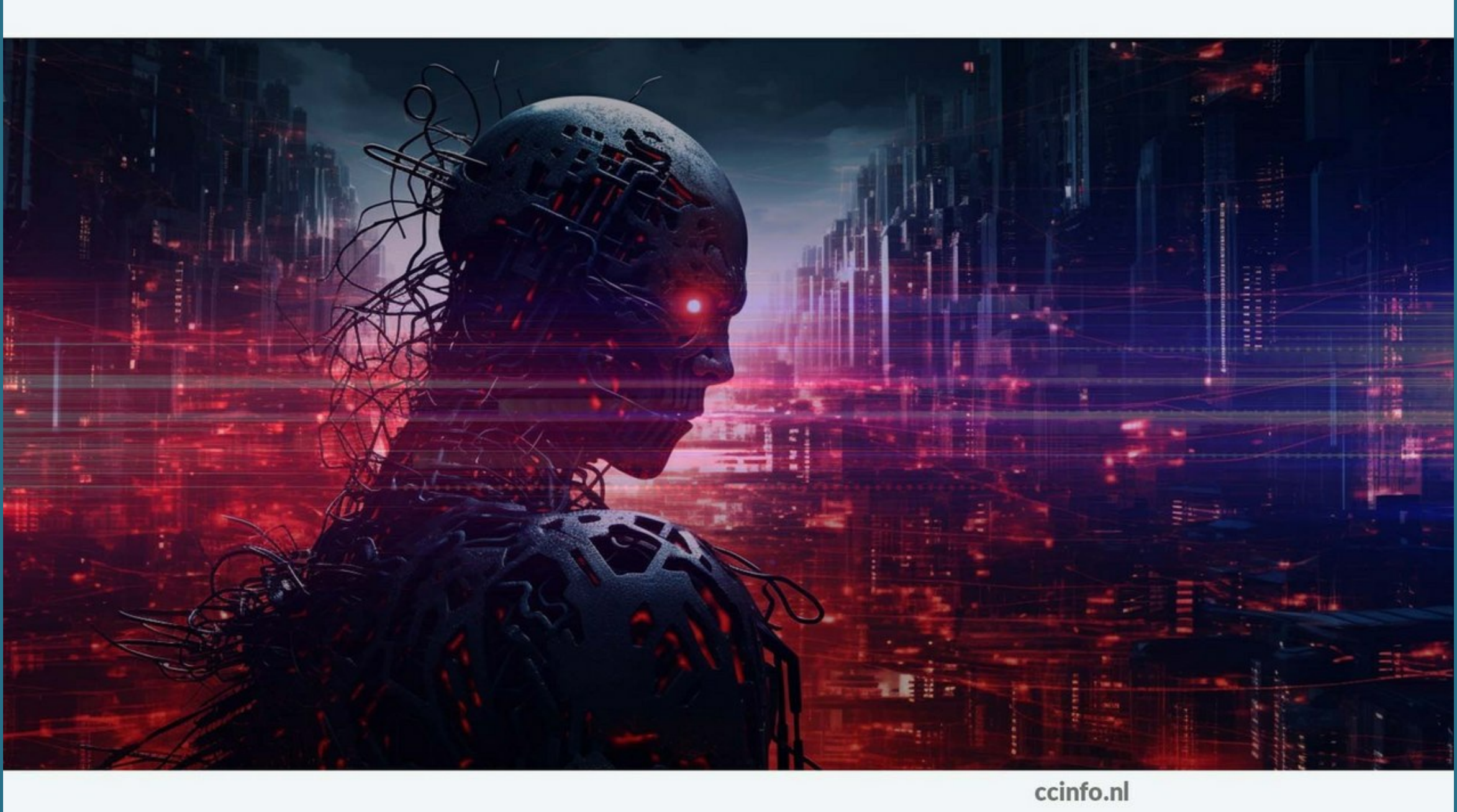
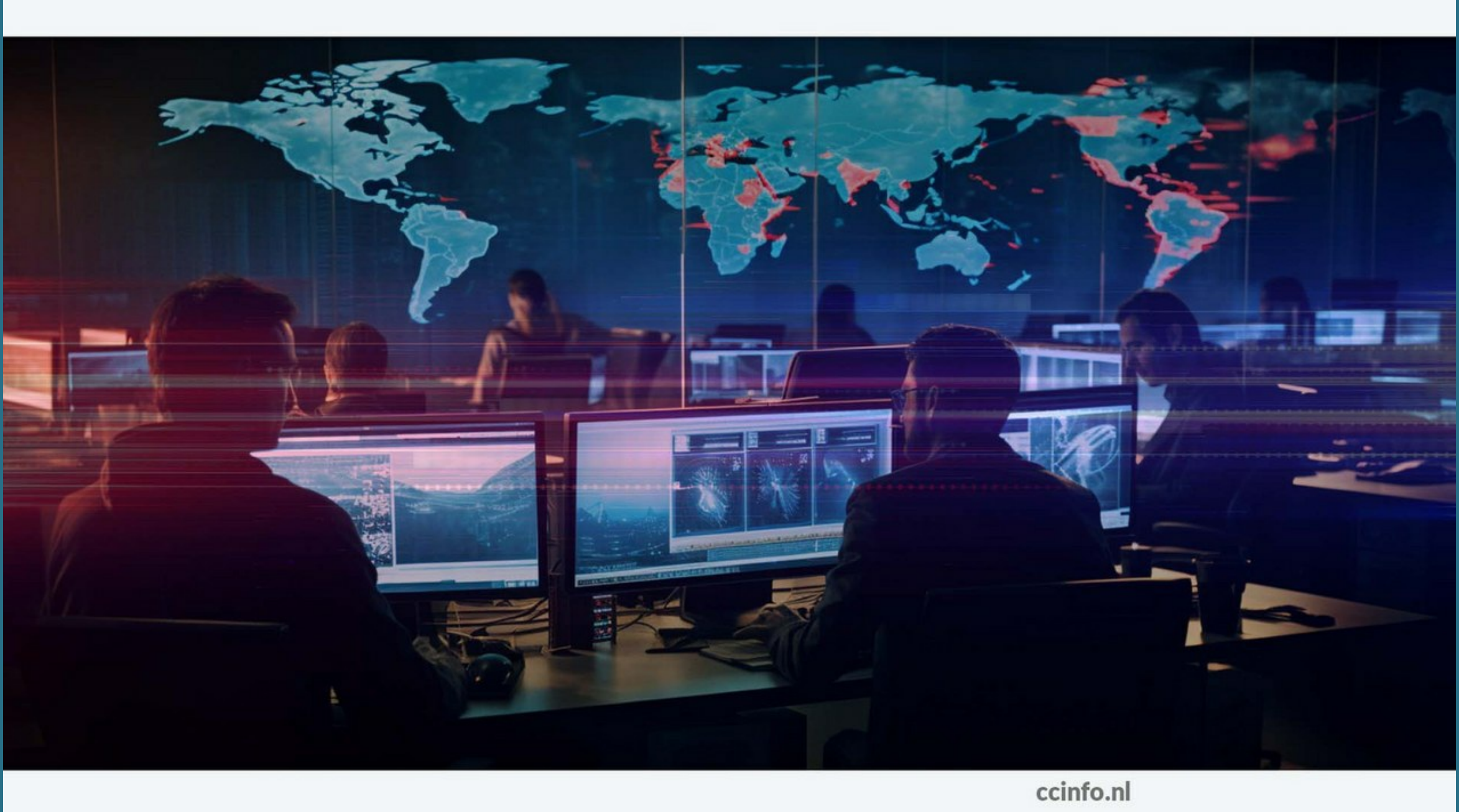
Nieuwsbrief 273 - Week 31-2023



AI-gestuurde cybercriminaliteit: Een dreigende golf van phishing- en malware-aanvallen

De wereld van cyberbeveiliging is in beroering door de snelle opkomst van AI-gedreven tools die cybercriminelen in staat stellen om geavanceerdere phishing- en malware-aanvallen uit te voeren. Met tools zoals WormGPT en FraudGPT kunnen fraudeurs met gemak bedrieglijke e-mails opstellen die zelfs de meest alerte internetgebruikers kunnen misleiden. Onderzoek van SlashNext onthult dat cybercriminelen toegang hebben tot steeds geavanceerdere AI-tools, waaronder DarkBART, een duistere tegenhanger van Google's AI-chatbot. Deze trend vormt een grote uitdaging voor cybersecurity-professionals.

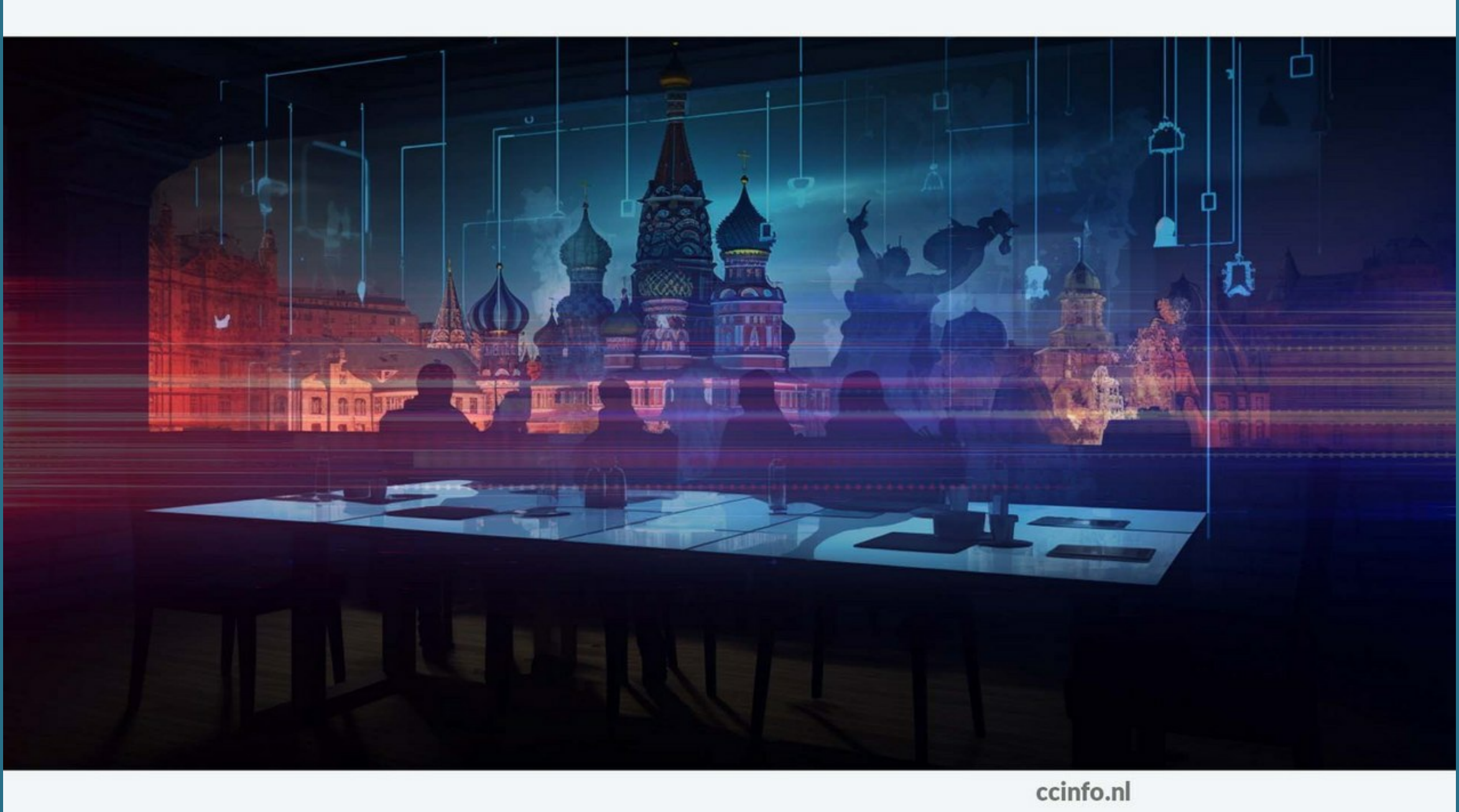
Lees verder



Operatie Narsil: Interpol verstoort netwerk van kindermisbruikwebsites

Interpol heeft onlangs met succes een grootschalige operatie afgerond, gericht op de ontwrichting van wereldwijde netwerken van kindermisbruikwebsites. Deze tweejarige operatie, genaamd Narsil, heeft de duistere hoeken van het internet in 27 verschillende landen blootgelegd. Het doel was om individuen die winst maken uit advertenties op deze schadelijke websites te identificeren en vervolgens te arresteren. Tot dusver zijn zes verdachten in verschillende landen aangehouden. Deze gezamenlijke inspanning onderstreept het belang van internationale samenwerking in de strijd tegen cybercriminaliteit en kindermisbruik.

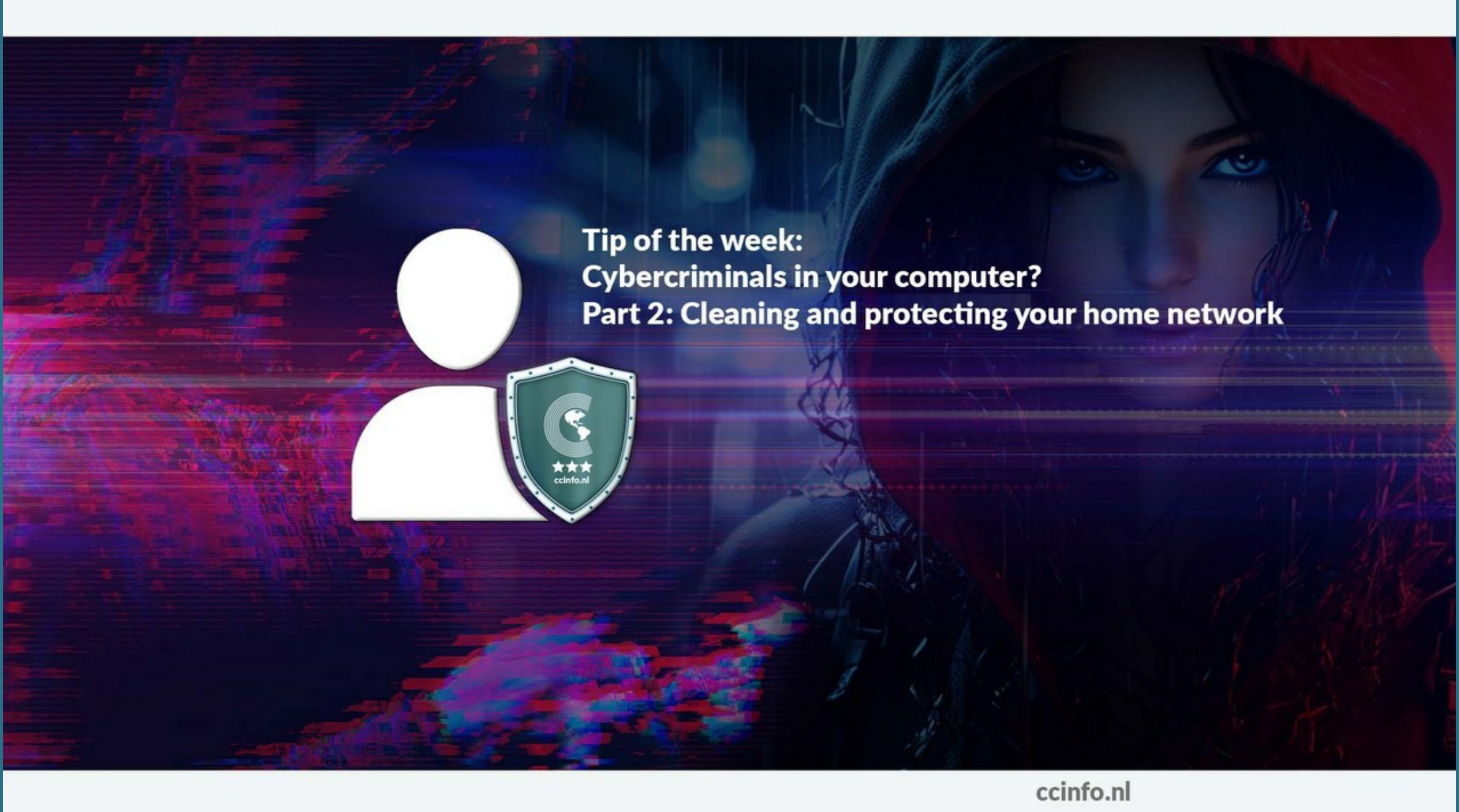
Lees verder



Verstrengelingen tussen AfD en Rusland: Leaks op het darkweb onthullen diepere connecties

In recente onthullingen afkomstig van het darkweb zijn verontrustende connecties tussen de Duitse extreemrechtse partij, Alternative für Deutschland (AfD) en Rusland blootgelegd. Documenten, die het daglicht hebben gezien na hun ontdekking in de verborgen hoeken van het internet, suggereren een diepe verwevenheid van financiële en politieke belangen. Geruchten over een mogelijke invloed van Rusland op de Duitse politiek zijn niet nieuw. Echter, deze nieuwe lekken bieden potentieel solide bewijs van de vermeende banden en laten de spanningen in Europa stijgen. Terwijl veiligheidsdiensten hun onderzoeken voortzetten, blijft de impact van het darkweb op de wereldpolitiek een punt van zorg.

Lees verder



Tip van de week: Cybercriminelen in je computer? Deel 2: Het reinigen en beschermen van je thuisnetwerk

Thuisnetwerken zijn vaker het doelwit van cyberaanvallen vanwege hun veelal lagere beveiligingsniveaus in vergelijking met bedrijfsnetwerken. Het identificeren van geïnfecteerde apparaten en het isoleren daarvan is cruciaal om verdere verspreiding van malware te voorkomen. Daarnaast is regelmatige scanning en bijwerken van software essentieel. Het veranderen van netwerkwachtwoorden en het inschakelen van netwerkfirewalls verhogen de verdedigingslinie tegen potentiële dreigingen. Met proactieve maatregelen kan men zich wapenen tegen de voortdurend evoluerende cyberdreigingen en een veilige digitale omgeving creëren.

Lees verder

Politie cyber nieuws 2023 juli

In juli 2023 bleef de cybercriminaliteit een prominent thema in Nederland en daarbuiten. Eén van de opmerkelijke zaken was de arrestatie van een man in Nederland voor het illegaal onttrekken van €125.000 uit cryptowallets. Tevens is er een onderzoek gaande naar een datadiefstal veroorzaakt door een MOVEit-lek. Ook in Amsterdam werd een jonge verdachte, van slechts 21 jaar oud, gearresteerd voor een phishing-aanval die hem meer dan €400.000 opleverde. Op internationaal niveau werd een lid van de Lapsus$ groep, verantwoordelijk voor cyberaanvallen op grote namen zoals Uber en Rockstar Games, aangeklaagd. In de strijd tegen het darkweb werd een centrale figuur van de Silk Road-drugsmarkt veroordeeld tot 20 jaar cel. Deze incidenten onderstrepen het aanhoudende gevaar en de complexiteit van cyberdreigingen in de moderne wereld.

Bekijk het weekoverzicht

Overzicht cyberaanvallen week 30-2023

De recente cyberaanvallen hebben de wereld weer op scherp gezet. In week 30 van 2023 heeft de ransomwaregroep Clop meerdere organisaties, waaronder Nederlandse IT-bedrijven zoals Softtech.nl en internationale conglomeraten zoals Toyota Boshoku in België, op de knieën gekregen. Tegelijkertijd hebben twaalf Noorse ministeries te maken gehad met een cyberaanval via een zerodaylek. Verder heeft de Android Stalkerware Spyhide wereldwijd 60.000 telefoons gecompromitteerd. De ALPHV ransomware voegde een nieuwe draai toe aan zijn tactiek met een datalek-API en een nieuwe malware, 'Stikstof', benut advertenties voor zijn misdaden.

Bekijk het weekoverzicht

Heerenveen - Bankhelpdesk fraude

In Heerenveen is een 77-jarige vrouw het slachtoffer geworden van een geraffineerde vorm van bankhelpdeskfraude. Ze werd urenlang aan de telefoon gehouden door iemand die zich voordeed als bankmedewerker. Deze persoon wist het vertrouwen van de vrouw te winnen door te beweren dat er gefraudeerd was met haar betaalrekeningen. Hierdoor werd ze overgehaald haar bankpassen aan een zogenaamde koerier te geven. Kort daarna werden er grote bedragen van haar rekening afgeschreven. Daarnaast gaf ze enkele sieraden af om in een bankkluis te bewaren. Ze leed hierdoor een groot financieel en emotioneel verlies. De politie zoekt nu getuigen en informatie om de daders te vinden.

Lees verder

AI chatbot assistent Cybercrime en Cybersecurity

"De AI chatbot assistent: elke dag getraind, elke dag sterker in de strijd tegen criminaliteit."

In het huidige digitale tijdperk, waarin cybercriminaliteit steeds vaker voorkomt, is toegang tot betrouwbare informatie en ondersteuning van cruciaal belang. De Cybercrimeinfo AI chatbot staat te allen tijde voor u klaar om uw vragen over cybercriminaliteit, het darkweb en cybersecurity te beantwoorden. Deze chatbot is direct verbonden met de Cybercrimeinfo-database en haalt geen informatie van het internet. De informatie die de bot verschaft, is uitvoerig gecontroleerd en is volledig betrouwbaar.
Wat deze chatbot onderscheidt, zijn de wekelijkse updates over cyberaanvallen, kwetsbaarheden, opsporingsberichten en betrouwbare artikelen aangaande cybersecurity, cybercriminaliteit en het darkweb. Zo hebt u altijd en overal toegang tot een actuele en betrouwbare cyberassistent die 24/7 beschikbaar is

PS: Wist u dat we ook een 'AI chatbot assistent voor Strafrecht en Strafvordering - Hulpofficier en Opsporingsambtenaar' hebben? Gezien de voortdurende ontwikkelingen in de criminaliteit, is het van essentieel belang om up-to-date te blijven met moderne technologieën die efficiënte, snelle en nauwkeurige oplossingen bieden. De AI Chatbot voor Strafrecht en Strafvordering is ontworpen om uitgebreide informatie te bieden over strafrecht en strafvordering. Of u nu opsporingsambtenaar of hulpofficier bent, deze chatbot staat altijd voor u klaar.

AI Chatbot

Steun Cybercrimeinfo zodat we kunnen blijven bestaan

Om deze website te runnen en iedereen te kunnen blijven voorzien van het laatste nieuws, tips en tricks over digitale criminaliteit, zijn wij op zoek naar donateurs. Hiervan kunnen we onder andere nieuwe apparatuur aanschaffen, want deze hele site draait op vrijwilligers. Kortom, wij kunnen niet zonder jouw steun! Help je mee in de strijd tegen cybercrime?
Iedere donatie, hoe klein ook, is van harte welkom. Alvast bedankt namens het hele team van Cybercrimeinfo.

Doneren kan al vanaf 5 euro!

Doneer

Share Tweet Share Pinterest