



Nieuwsbrief 311



De afgebeelde personen in de foto's en video's zijn gecreëerd met AI en bestaan niet echt.

Nieuwsbrief



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.



De stille oorlog: Hoe Nederland zich beschermt tegen cyberaanvallen

In een tijdperk waarin digitale bedreigingen een steeds groter deel van de internationale veiligheidszorgen innemen, staat Nederland voorop in de verdediging tegen complexe cyberaanvallen. Het meest recente AIVD-rapport belicht hoe vooral China een grote uitdager is met zijn geavanceerde cyberactiviteiten gericht op het onderscheppen van bedrijfsgeheimen en het destabiliseren van kritieke infrastructuur. Dit onderstreept het belang van tijdige beveiligingsupdates en robuuste monitoringssystemen binnen bedrijven. Ontdek meer over de strategieën die Nederland toepast om deze dreigingen het hoofd te bieden op onze website.

Lees verder



De stille oorlog: Ruslands complexe beïnvloeding van Europa

Ontdek de stille oorlog die zich afspeelt binnen de grenzen van Europa, waarbij Rusland via complexe cyberoperaties invloed uitoefent. Dit artikel belicht de Russische acties, van politieke beïnvloeding en spionage tot digitale sabotage, die gericht zijn op het ondermijnen van westerse democratieën. Recente arrestaties in verband met voorbereide aanslagen en politieke complotten onderstrepen de ernst en nabijheid van deze dreigingen. Voor een diepgaande analyse van deze kwesties en meer over de reacties van Europese veiligheidsdiensten, lees verder op onze website.

Lees verder



Dreigingen op het darkweb: Onthulling van de verkoop van bedrijfsbroncodes

In de schaduwrijke wereld van het darkweb wordt cruciale informatie, zoals broncodes van bedrijven, openlijk verhandeld. Recentelijk werd onthuld dat de broncodes van 150 bedrijven voor een bedrag van \$7.000 worden aangeboden. Deze onthulling benadrukt de ernstige risico's voor de cybersecurity van bedrijven, van datalekken tot omvangrijke beveiligingsinbreuken. In ons artikel verkennen we hoe deze handel plaatsvindt en welke stappen je kunt ondernemen om je gegevens te beschermen.

Lees verder



Slachtofferanalyse en Trends van Week 16-2024

In week 16 van 2024 heeft een malware-ontwikkelaar een bijzondere aanpak gekozen in de strijd tegen cybercriminaliteit door een honeypot-malware te creëren die zich richt op personen die online zoeken naar illegaal kindermisbruikmateriaal. Deze tactiek heeft een nieuwe ethische discussie opgeworpen over privacy en de grenzen van digitale zelfjustitie. Tegelijkertijd rapporteren we een opmerkelijke daling in het aantal bedrijven dat losgeld betaalt aan ransomware-aanvallers, een teken van verbeterde beveiligingsprotocollen en verminderd vertrouwen in de belofte van cybercriminelen. Lees verder over deze en andere recente ontwikkelingen in ons volledige artikel over de cyberaanvallen van de afgelopen week.

Lees verder



Vraag van de week: Mijn gegevens staan op darkweb, wat nu?

Ontdek hoe je kunt reageren als je erachter komt dat jouw persoonlijke informatie, zoals je paspoort of identiteitskaart, op het darkweb te vinden is. Dit scenario is niet langer fictie maar een harde realiteit voor veel mensen na een groot datalek bij het Nederlandse bedrijf Nexperia. Lees over de eerste noodzakelijke stappen die je moet ondernemen om je gegevens te beschermen, van het informeren van je gegevensgever tot het beveiligen van je financiële accounts.

Lees verder



Uden - Bankhelpdesk fraude

In Uden is een 86-jarige vrouw slachtoffer geworden van bankhelpdeskfraude. Op 14 november 2022 werd zij telefonisch benaderd door een oplichter die zich voordeed als bankmedewerker. De crimineel overtuigde haar om haar bankpas en pincode af te geven, wat resulteerde in het plunderen van haar bankrekening. Beveiligingsbeelden tonen een verdachte die het geld opneemt met haar bankpas. Herkent u deze persoon, of heeft u meer informatie? Uw hulp kan cruciaal zijn in het opsporen van de daders. Bescherm onze gemeenschap tegen deze criminele praktijken. Voor meer informatie, klik hier om verder te lezen.

Lees verder

Help ons de toekomstige beats van Cybercrimeinfo vorm te geven!

Hey Cybercrimeinfo fans,

Wij zijn altijd op zoek naar manieren om onze muzikale creaties beter af te stemmen op wat jullie, onze luisteraars, willen horen. Daarom hebben we jouw hulp nodig! We willen graag weten welke stijl van muziek jullie het liefst meer zouden willen horen. Jouw mening is cruciaal om ons te leiden in onze volgende projecten.

Stem hier

Test je cyberveiligheid: Verbeter je kennis met onze interactieve quizen

Ontdek de wereld van cybersecurity en het darkweb met onze interactieve quizen op CyberCrimeInfo.nl. Geschikt voor iedereen, van beginners tot experts, bieden deze quizen een manier om je kennis op je eigen tempo te vergroten. Na elke quiz ontvang je een gedetailleerde feedback op je antwoorden, en met een perfecte score kun je speciale erkenning verdienen. Ben je klaar om je vaardigheden te testen en te zien hoe je het doet tegenover anderen? Begin vandaag nog aan je leerreis door je toegangscode aan te vragen!

Naar quizen

De Perfecte Score Club!

Topscorer			
Johan	10	16-maart-2024	
Maxim	9	16-maart-2024	
Philip Savaete	9	17-maart-2024	
Kenan	7	20-maart-2024	
Thijs	7	09-april-2024	

Maximaal te behalen punten: 16.

Aantal deelnemers tot nu toe: **605**

[Totaal overzicht](#)

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 beheersers. 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, hulpverleners en iedereen die geïnteresseerd is in strafrecht. De expertisegebieden van RechtRaadgever omvatten:

- **Strafrecht en Strafverordening:** 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 continu 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 essentieel is

Beste lezer, In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo 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 is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
2. **Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
3. **Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

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

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Om de online vindbaarheid van onze website Cybercrimeinfo (ccinfo) op Google te verbeteren, zijn recensies zeer waardevol. Zou je de tijd willen nemen om een beoordeling te plaatsen op Google? Dit is heel eenvoudig te doen via deze link: [Schrijf een review](#). Jouw steun betekent veel voor ons!

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.

