



Nieuwsbrief 306 - Week 12-2024



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

Nieuwsbrief



Nieuwe truc van oplichters: Zij doen zich voor als medewerkers van De Nederlandse Bank DNB

Oplichters hebben weer een nieuwe methode ontdekt om mensen hun geld afhandig te maken: ze doen zich voor als medewerkers van De Nederlandsche Bank (DNB). Deze fraudeurs gebruiken valse communicatie, zoals e-mails, sms-berichten en telefoontjes, met de techniek van 'spoofing' om geloofwaardig over te komen. Ze beweren bijvoorbeeld dat er iets mis is met je bankrekening en dat snelle actie vereist is. Belangrijk om te onthouden is dat DNB nooit plotseling contact zal opnemen om persoonlijke gegevens te vragen of om directe betalingen te doen. Bij twijfel is het altijd het veiligst om zelf contact op te nemen om persoonlijke gegevens te vragen of om directe betalingen te doen. Bij twijfel is het altijd het veiligst om zelf contact op te nemen om persoonlijke gegevens te vragen of om directe betalingen te doen. Bij twijfel is het altijd het veiligst om zelf contact op te nemen om persoonlijke gegevens te vragen of om directe betalingen te doen.

Lees verder



Het hacken van wifi-wachtwoorden: patronen, risico's en preventie

Het kraken van wifi-wachtwoorden vormt een significant risico voor zowel particuliere als zakelijke netwerken. In een wereld waar draadloze verbindingen essentieel zijn, wordt het beveiligen van deze netwerken tegen ongewenste indringers cruciaal. Dit artikel belicht hoe eenvoudige en voorspelbare wachtwoordpatronen het voor kwaadwillenden makkelijker maken om toegang te verkrijgen en deelt effectieve strategieën om je netwerkbeveiliging te versterken. Het belang van sterke, unieke wachtwoorden en regelmatige updates wordt onderstreept, evenals de waarde van bewustwording over de methoden die hackers gebruiken. Voor praktische tips en diepgaande inzichten in het voorkomen van wifi-wachtwoordhacken, nodigen we je uit verder te lezen via onze link.

Lees verder



De ondergang van Nemesis: Een lichtstraal in de schaduw van het Darkweb

In de schaduwrijke krotten van het internet, ver verwijderd van het goedverlichte pad dat de meesten van ons dagelijks bewandelen, bevond zich Nemesis Market. Dit was niet zomaar een plek. Het was een bruisend centrum voor alles wat buiten de wet viel, van de handel in verboden middelen tot de verkoop van gestolen gegevens. Echter, door een indrukwekkende samenwerking van internationale wetshandhavinginstanties, waaronder de Duitse politie en het FBI, is deze markt onlangs ontmanteld. Dit markeert een significante overwinning in de voortdurende strijd tegen cybercriminaliteit. Maar de strijd is verre van voorbij. Ontdek hoe deze actie de ondergrondse wereld van illegale handel heeft geschokt en wat het betekent voor de toekomst van online veiligheid. Lees verder over de details van deze operatie en de impact ervan op de digitale misdaadwereld.

Lees verder



Slachtofferanalyse en Trends van Week 11-2024

In week 11 van 2024 zien we weer hoe veelzijdig en ingrijpend cyberaanvallen kunnen zijn, onderstreepd door incidenten die van invloed zijn op de gamingindustrie tot aan persoonlijke gegevens van miljoenen mensen. Een onthullend voorbeeld is de hack die de finale van een groot e-sportevenement uitstelde, naast een datalek dat gevoelige informatie van bijna 2,5 miljoen mensen aan het licht bracht. Deze gebeurtenissen benadrukken de constante bedreigingen in onze digitale wereld en het cruciale belang van proactieve beveiligingsmaatregelen. Van phishingpogingen bij sportevenementen tot de kwetsbaarheden in softwarebibliotheken, de variëteit aan aanvallen laat zien dat niemand volledig immuun is. Deze samenvatting raakt slechts de oppervlakte van de complexe cyberdreigingen die ons omringen. Voor een diepgaande analyse en praktische adviezen om je te beschermen tegen deze en andere cyberdreigingen, nodigen we je uit om het volledige artikel te lezen.

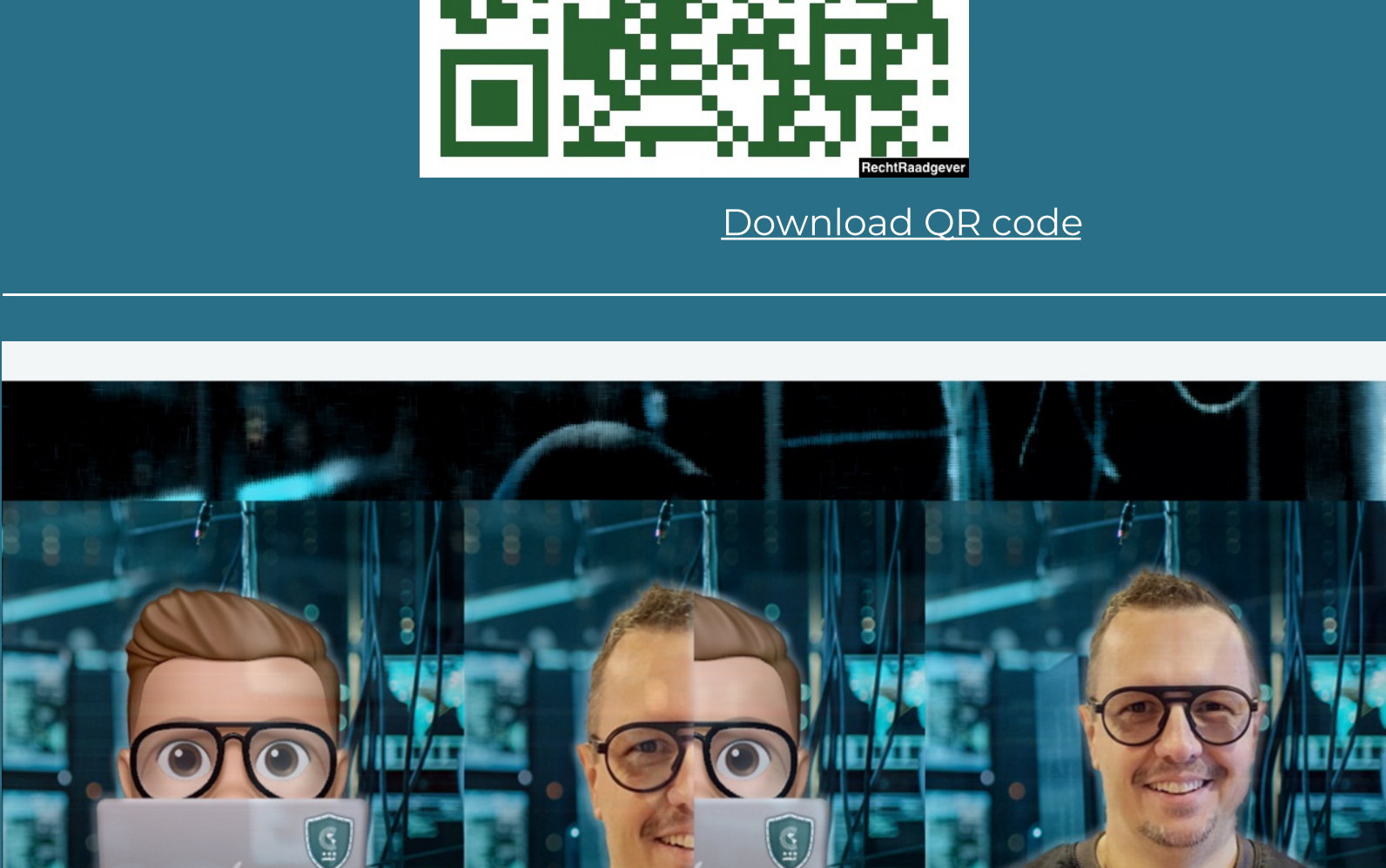
Lees verder



Tip van de week: Een praktische gids voor risicomanagement (NIS2 en ISO27001)

In de digitale wereld van vandaag is het beheren van de risico's die onze informatie veiligheid bedreigen cruciaal dan ooit. Met een toename van cyberaanvallen en datalekken is het van groot belang dat zowel individuen als organisaties een gestructureerde aanpak volgen om hun gegevens te beschermen. Dit artikel biedt een praktische gids voor risicomanagement, gericht op de implementatie van NIS2 en ISO27001 normen. Je vindt er waardevolle inzichten en strategieën voor het effectieve beveiligen van cyberdreigingen. Van het identificeren van de grootste risico's tot het implementeren van maatregelen om deze tot een acceptabel niveau te verminderen, wij lopen met je door de essentiële stappen van dit kritieke proces. Voor een diepgaande kijk op hoe je jouw informatie veilig kunt houden in een wereld vol digitale gevaren, lees verder.

Lees verder



Ontdek en verbeter je cybersecurity kennis met quizen

CyberCrimelnl.nl biedt een unieke kans voor iedereen met interesse in cybersecurity om hun kennis te testen en te verbeteren via een reeks boeiende quizen. Het platform is erop gericht om zowel beginners als gevorderden te voorzien van diepgaande inzichten in digitale veiligheid, met een sterke nadruk op privacy. Door simpelweg je naam en e-mailadres in te vullen, ontvang je binnen 24 uur een unieke toegangscode. Wees gerust, deze persoonlijke informatie wordt strikt gebruikt om de deelname aan de quizen mogelijk te maken en wordt niet voor reclamedoeleinden ingezet.

Deze toegangscode opent de deur naar diverse quizen, waar je kunt ontdekken hoeveel je weet en wat er nog te leren valt over cruciale cybersecurityonderwerpen. Na het indienen van je antwoorden krijg je vaak binnen 48 uur gedetailleerde feedback, wat een rijke leerervaring garandeert. Voor degenen die uitblinken, is er de 'Perfect Score Club'; een perfecte score levert niet alleen een plek op de topperslijst op maar geeft ook erkenning binnen de CyberCrimelnl.nl gemeenschap. Dit initiatief onderstreept het belang van voortdurende educatie en het bijblijven met de nieuwste ontwikkelingen in de strijd tegen digitale criminaliteit, alles in een veilige en reclamevrije omgeving.

Lees verder

De Perfecte Score Club!

Topscore			
Johan	10	16-maart-2024	
Maxim	9	16-maart-2024	
Philip Savaete	9	17-maart-2024	
Sjoerd Water	6	18-maart-2024	

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 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 privacyreggeving.

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 continu leert en verbetert. Het biedt steun 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. Jijzelf maakt het verschil. Hier is waarom:
- Onafhankelijke en Belangrijke Bron van Informatie:** Cybercrimeinfo.nl is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
 - 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.
 - 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.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.

