



Nieuwsbrief 265 - Week 23-2023

The increasing severity and impact of data breaches in the Netherlands

ccinfo.nl

De toenemende ernst en impact van datalekken in Nederland

In Nederland, een van de meest gedigitaliseerde landen ter wereld, is er een groeiende ernst en impact van datalekken. Volgens de Autoriteit Persoonsgegevens heeft het aantal ernstige datalekken de afgelopen jaren een verontrustende stijging gezien. Deze lekken hebben verstrekende gevolgen, niet alleen voor individuen die slachtoffer kunnen worden van identiteitsdiefstal en fraude, maar ook voor organisaties die financiële en reputatieschade kunnen oplopen. Ondanks inspanningen om de beveiliging te verbeteren, blijft het probleem bestaan, waarbij bijna elke Nederlander op een bepaald moment slachtoffer is geweest van een datalek. Het is daarom cruciaal dat zowel individuen als organisaties actie ondernemen om de risico's en gevolgen van datalekken te minimaliseren.

[Lees verder](#)

Oekraïense hackers leggen serviceprovider voor Russische banken plat

ccinfo.nl

Hackers uit Oekraïne halen dienstverlener voor Russische banken neer

In een recente ontwikkeling binnen de cyberoerlog heeft een groep Oekraïense hackers, bekend als Cyber.Anarchy.Squad, de Russische telecoaanbieder Infotel JSC succesvol aangevallen. Deze aanval heeft een aanzienlijke impact gehad op het Russische bankwezen, wat aantoonde dat hacktivisme en cyberoerlogsvoering de kracht hebben om significante verstoringen te veroorzaken in een land's economie. Infotel JSC, gevestigd in Moskou, speelt een cruciale rol in het verbinden van de Russische Centrale Bank met andere Russische banken, online winkels en kredietinstellingen. Deze aanval onderstreept niet alleen het belang van cyberveiligheid, maar ook de noodzaak voor internationale samenwerking in de strijd tegen cybercriminaliteit.

[Lees verder](#)

Trading wildlife on the Dark Web: A worrying trend

ccinfo.nl

Handel in wilde dieren en planten op het darkweb: Een verontrustende trend

Hoewel de huidige impact van de handel in wilde dieren en planten op het darkweb wellicht niet enorm lijkt, mag het potentieel voor toekomstige schade niet worden onderschat. Met strengere reguleringen en handhaving zou deze handel gemakkelijk kunnen verschuiven naar verborgen delen van het internet, waardoor het bijna onmogelijk wordt om toezicht te houden. Het is daarom van cruciaal belang dat onderzoekers en wetshandhavers waakzaam blijven en deze activiteiten nauwlettend blijven volgen. Op deze manier kunnen we hopen te voorkomen dat de darkweb-marktplaatsen een grotere bedreiging gaan vormen voor de biodiversiteit van onze planeet.

[Lees verder](#)

Draag bij aan de toekomst van cybercriminaliteitsbestrijding en maak kans op een luxe wellness-overnachting

ccinfo.nl

Draag bij aan de toekomst van cybercriminaliteitsbestrijding en maak kans op een luxe wellness-overnachting

Cybercrimeinfo.nl kondigt met trots de lancering aan van onze 24/7 beschikbare AI Chatbot-assistent. Deze assistent beantwoordt al uw vragen over cybercriminaliteit en houdt u op de hoogte van de nieuwste trends. Wij nodigen u uit om uw mening te geven over hoe deze chatbot u kan helpen. Door deel te nemen en onze enquête in te vullen, maakt u kans op een luxe overnachting bij B&B Arendsnest in Renswoude, uitgerust met een privé jacuzzi en sauna. De meest inzichtelijke antwoorden maken kans op deze speciale prijs. Deelname kan tot en met 30 juni 2023. Veel succes!

[Lees verder](#)

CYBER ATTACKS

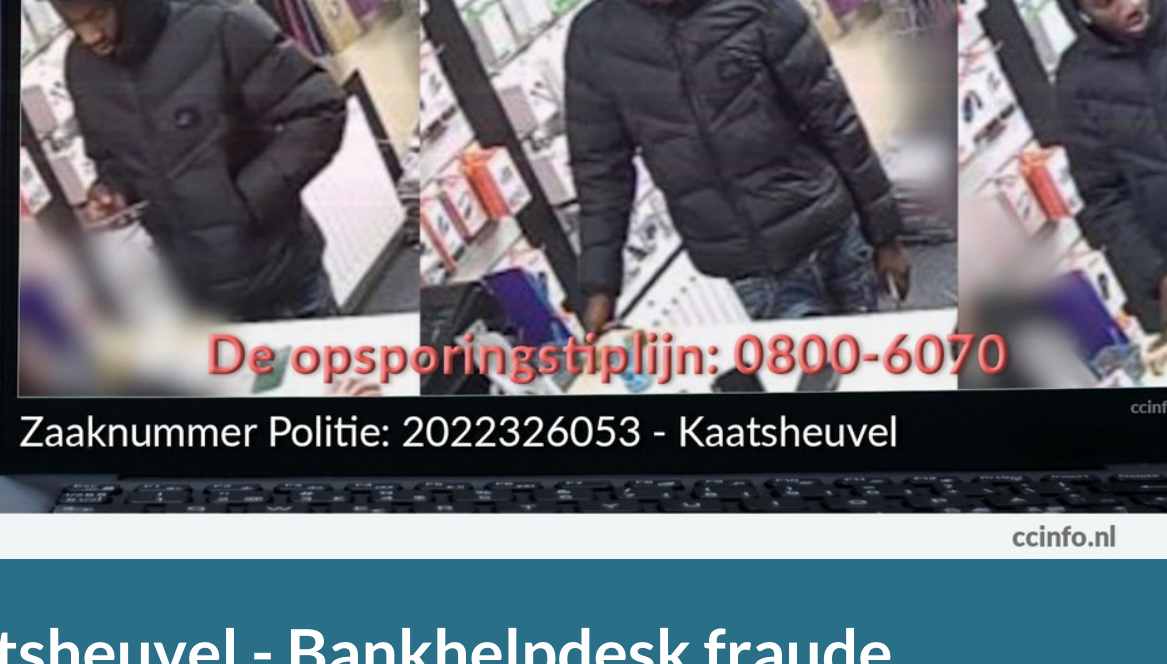
WEEK OVERVIEW
22-2023

ccinfo.nl

Overzicht cyberaanvallen week 22-2023

In week 22 van 2023 zagen we een verscheidenheid aan cyberaanvallen die de veiligheid van talloze instellingen en individuen wereldwijd in gevaar brachten. Het begon met een zware slag voor Atomic Wallet, waarbij cybercriminelen meer dan \$35 miljoen aan cryptocurrency wisten te stelen. De kwetsbaarheid van MOVEit Transfer werd ook op grote schaal misbruikt. De scholengemeenschap OSG Hengelo en de gemeente Meierijstad waren beiden het slachtoffer van aanzienlijke aanvallen - de eerste door een ransomware-aanval en de laatste door CEO-fraude, waarbij €37.000 werd buitgemaakt. Deze incidenten benadrukken opnieuw het onophoudelijke gevaar van cyberaanvallen en de noodzaak om cyberbeveiligingsmaatregelen continu te verbeteren.

[Bekijk het weekoverzicht](#)



ccinfo.nl

Kaatsheuvel - Bankhelpdesk fraude

De Nederlandse politie is dringend op zoek naar een man die verdacht wordt van cybercrime, meer specifiek bankhelpdeskfraude, in Kaatsheuvel. De verdachte, wiens identiteit op dit moment nog niet bekend is bij het publiek, zou mensen hebben gebeld en zich hebben voorgedaan als een medewerker van een bankhelpdesk. Hij overtuigde zijn slachtoffers om hun bankgegevens en pinpassen aan hem te overhandigen. De politie heeft het publiek om hulp gevraagd bij het opsporen van de verdachte en roept iedereen op om werkzaam te zijn bij het ontvangen van telefoontjes die op dergelijke fraude kunnen duiden. Zaaknummer: 2022326053.

[Lees verder](#)



"De Cybercrimeinfo AI Chatbot - Elke dag getraind, elke dag beter in de strijd tegen digitale criminaliteit."

De Cybercrimeinfo AI Bot staat altijd voor u klaar om uw vragen te beantwoorden over cybercriminaliteit, het darkweb en cybersecurity. Deze chatbot is exclusief verbonden met de Cybercrimeinfo-database en heeft toegang tot data van het internet. Alle informatie die de bot biedt, is grondig gecontroleerd en is 100% betrouwbaar.

Wat deze chatbot maakt, is de wekelijkse update van informatie over cyberaanvallen, kwetsbaarheden, opsporingsnieuws en betrouwbare artikelen over cybersecurity, cybercrime en het darkweb. Hierdoor heeft u altijd toegang tot een unieke, actuele cyberassistente die 24/7 beschikbaar is.

Overweegt u de 'Cybercrimeinfo chatbot' te implementeren in uw bedrijf of op uw website, zodat uw medewerkers toegang hebben tot alle Cybercrimeinfo-gegevens en gepersonaliseerd advies kunnen ontvangen? Bezoek dan de website van onze belangrijkste sponsor, 'Digiweerbaar.nl BV'.

Als u nog niet bekend bent met onze AI Chatbot, kunt u bij Digiweerbaar.nl een account aanvragen om deze gratis 2 dagen te testen.

Als u echter meer worstelt met juridische vraagstukken en het handelingskader binnen het Strafrecht en de Strafvordering bij de bestrijding van (digitale) criminaliteit, dan is de 'AI Chatbot SR/SV' een juridisch assistent die 24/7 beschikbaar is en zeker nuttig kan zijn.

[Meer informatie over onze AI Chatbot vindt u hier](#)



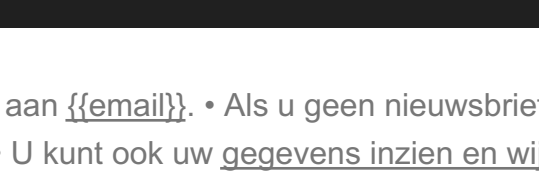
Steun Cybercrimeinfo zodat we kunnen blijven bestaan

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