



Nieuwsbrief 270 - Week 28-2023

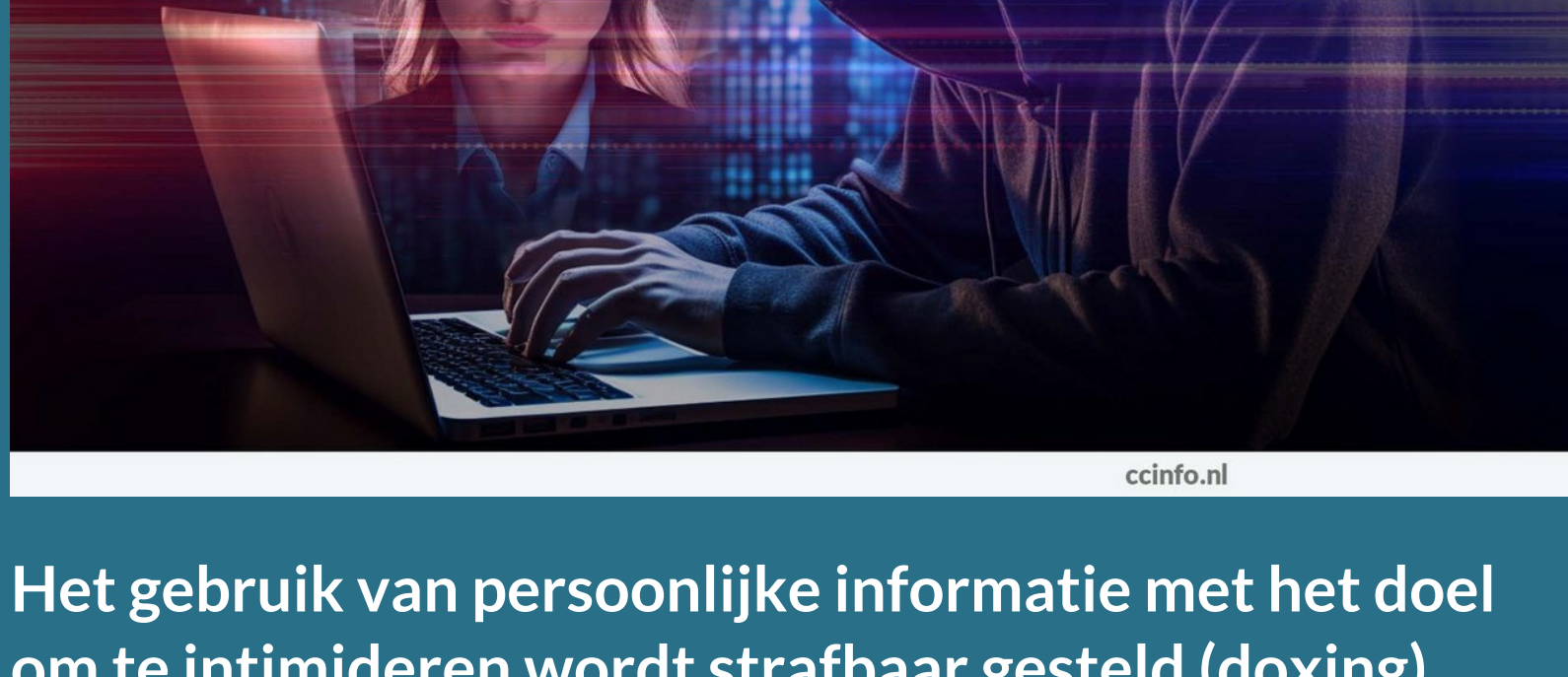


ccinfo.nl

Cybercriminelen in 2023: Aanpassingsvermogen, sextortion en misleidende leningsapps

Cybercriminelen worden steeds slimmer en gebruiken technieken om traditionele beveiligingsmaatregelen te omzeilen. Ze passen zich aan en exploiteren nieuwe technologieën, zoals het gebruik van Office-macro's en gewapende OneNote-bestanden om ongeoorloofde toegang te krijgen tot bedrijfssystemen. Ook sextortion, waarbij criminelen dreigen met het publiceren van compromitterende informatie tenzij er losgeld wordt betaald, is bezig met een comeback. Daarnaast neemt de prevalentie van misleidende leningsapps op Android toe. Deze apps misleiden kwetsbare mensen die financiële hulp nodig hebben, en de ontwikkelaars erachter profiteren van hun wanhoop. Door alert te blijven op deze trends, kunnen we beter voorbereid zijn op de steeds veranderende cyberbeveiligingslandschap.

[Lees verder](#)



ccinfo.nl

Het gebruik van persoonlijke informatie met het doel om te intimideren wordt strafbaar gesteld (doxing)

In reactie op groeiende zorgen rondom 'doxing', het ongewenst verspreiden van iemands persoonlijke gegevens met als doel om te intimideren, heeft de Nederlandse Eerste Kamer een wetsvoorstel aangenomen dat doxing strafbaar stelt. Deze wet, die op 1 januari 2024 in werking treedt, maakt de verspreiding van persoonsgegevens met het doel om angst, ernstige overlast of hinder in de uitoefening van iemands beroep te veroorzaken, strafbaar. Bij een overtreding kunnen daders een maximale gevangenisstraf van twee jaar of een boete van maximaal 22.500 euro verwachten. Hiermee worden de privacybescherming en bestrijding van online intimidatie versterkt.

[Lees verder](#)

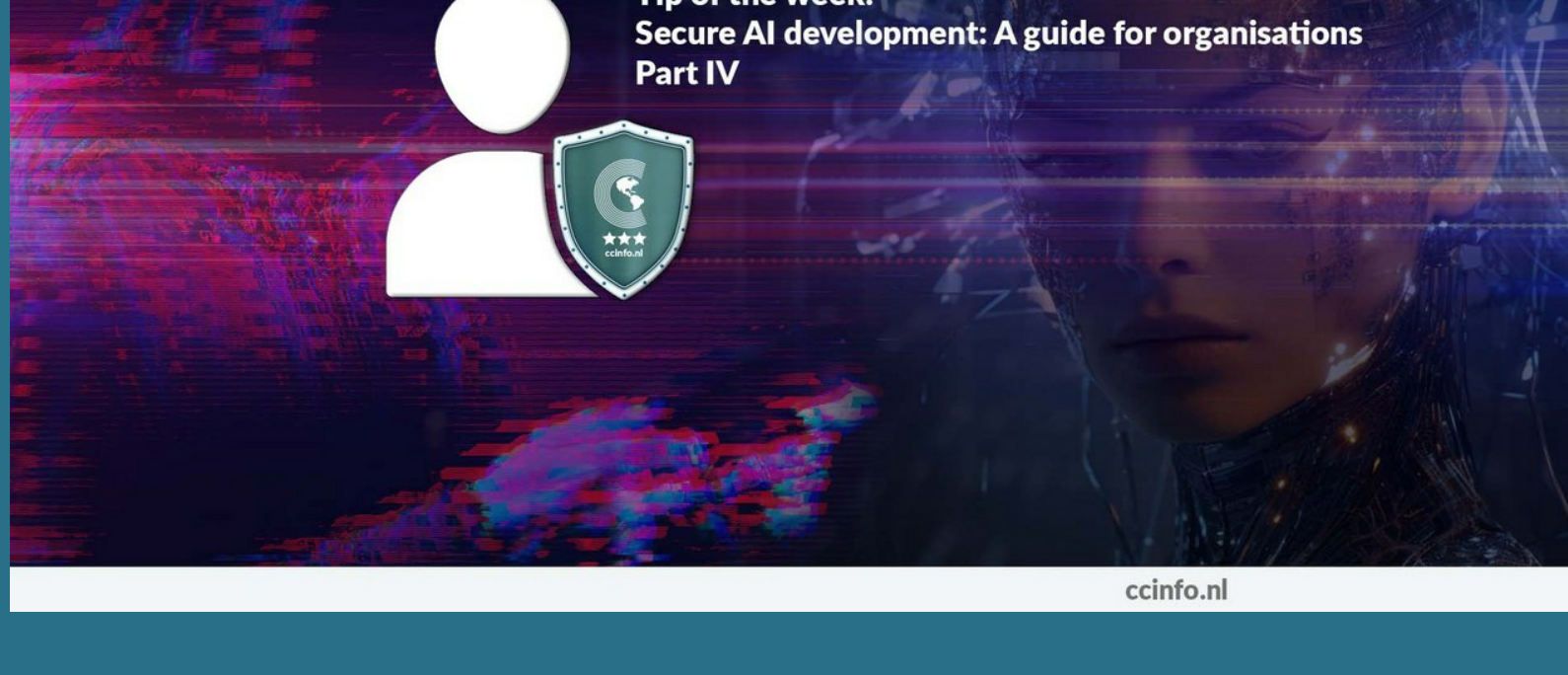


ccinfo.nl

Het Darkweb en de strijd tegen kinderporno in Nederland

Ondanks de afname van meldingen, blijft de strijd tegen kinderporno een grote uitdaging. Dit wordt verergerd door de rol van het Darkweb, een moeilijk te traceren en anonieme ruimte op het internet waar illegale activiteiten, zoals de verspreiding van kinderporno, floreert. Hoewel technologie en infrastructuur het blokkeren van sluiten van websites op het Darkweb bemoeilijkt, blijft het van cruciaal belang om deze weerzinwekkende praktijken te bestrijden. Het vergt een gecoördineerde, internationale inspanning, innovatieve technologische oplossingen en effectieve wetgeving om degenen die deze misdaden plegen op te sporen en te vervolgen.

[Lees verder](#)



ccinfo.nl

Tip van de week: Veilige AI-ontwikkeling: Een gids voor organisaties - Deel IV

In dit vierde deel van onze serie 'Veilige AI-ontwikkeling: Een gids voor organisaties' richten we ons op de beveiligingsuitdagingen van cloud-gebaseerde en open source AI-systemen. We onderstrepen het belang van een holistische beveiligingsbenadering, waarbij technische, menselijke en beleidsmatige aspecten allemaal in overweging worden genomen. Organisaties moeten niet alleen mogelijke bedreigingen identificeren en defensieve strategieën ontwikkelen, maar ook voldoen aan wetten en regelgevingen, gebruikers opleiden en menselijke vooroordelen aanpakken om sterke en veilige AI-systemen te bouwen. Blijf ons volgen voor meer inzichten en begeleiding op dit belangrijke terrein.

[Lees verder](#)

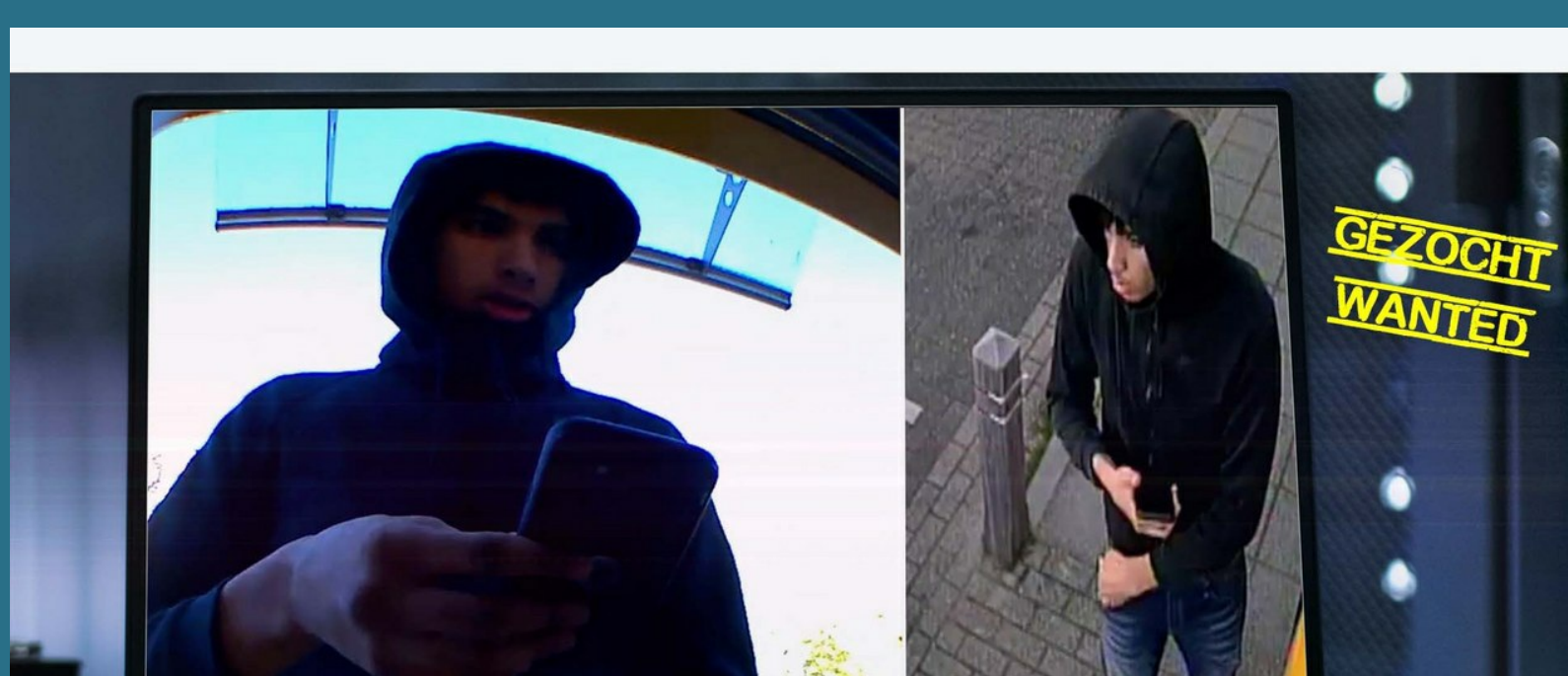


ccinfo.nl

Overzicht cyberaanvallen week 27-2023

In week 27 van 2023 was de cyberbeveiligingswereld opnieuw getuige van een reeks geavanceerde aanvallen, waarbij zowel grote multinationals als regionale entiteiten getroffen werden. Het Nederlandse Wolters Kluwer viel ten prooi aan een CLOP-ransomware-aanval, terwijl Shell te maken kreeg met een ernstige aanval op hun MOVEit Transfer-systeem. Tegelijkertijd zorgde een verwoestende ransomware-aanval ervoor dat de operaties in de haven van Nagoya, de grootste containerhaven van Japan, werden verstoord. In Europa hadden verschillende overheidsinstanties te maken met een geraffineerde SmugX-phishingcampagne, gelanceerd door Chinese hackers. Ten slotte verspreide de nieuwe 'Big Head' ransomware neppe Windows-updatewaarschuwingen, met als doel om onoplettende gebruikers te misleiden. Deze gebeurtenissen tonen nogmaals aan hoe essentieel het is dat organisaties hun cyberbeveiligingsmaatregelen voortdurend verbeteren en updaten.

[Bekijk het weekoverzicht](#)



ccinfo.nl

Deurne - Bankhelpdesk fraude

In Deurne werd een 86-jarige vrouw het slachtoffer van een frauduleuze methode bekend als 'spoofing'. Een vermeende nebankmedewerker nam telefonisch contact op en claimde problemen met haar bankrekening, 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.

[Lees verder](#)



Actuele cyberassistente die 24/7 beschikbaar is!

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

De Cybercrimeinfo AI Chatbot staat altijd paraat om uw vragen te beantwoorden over cybercriminaliteit, het darkweb en cybersecurity. Deze chatbot is exclusief verbonden met de Cybercrimeinfo-database en vertrouwt alleen op zorgvuldig gecontroleerde informatie uit deze bronnen. Alle informatie die de bot biedt, is grondig gecontroleerd en betrouwbaar. Hoewel de chatbot gespecialiseerd is in cybercriminaliteit, cybersecurity en het darkweb, kan hij voor vragen buiten dit domein toegang hebben tot internetbronnen om u van relevante en actuele informatie te voorzien. Wat de chatbot echt uniek maakt, is de werkelijke update van informatie over cyberaanvallen, kwetsbaarheden, opsporingsnieuws en betrouwbare artikelen over cybersecurity, cybercrime en het darkweb. Klik hieronder om het volledige artikel te lezen op onze website.

[AI Chatbot](#)



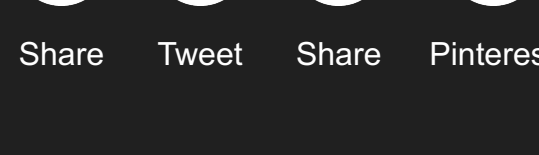
Steun Cybercrimeinfo zodat we kunnen blijven bestaan

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

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

