Cybercrimeinfo.nl (ccinfo.nl) Bekijk de webversie

Nieuwsbrief 285 - Week 43-2023

ccinfo.nl

Wat te doen bij een hackpoging en hoe jezelf te beschermen

Zekerheid op het internet is geen luxe, maar een noodzaak. Word je geconfronteerd met een hackpoging, dan is snelle en effectieve actie cruciaal. In ons diepgaande artikel op CyberCrimeInfo.nl bieden we een uitgebreide handleiding over wat te doen bij een hackpoging en hoe je jezelf kunt beschermen tegen toekomstige cyberaanvallen. Ontdek welke directe stappen je moet nemen, zoals het verbreken van de internetverbinding en het wijzigen van wachtwoorden, maar ook hoe je op de lange termijn je digitale veiligheid kunt waarborgen. Leer over het herkennen van eerste signalen, het omgaan met gecompromitteerde accounts en preventieve maatregelen voor de toekomst. Lees het volledige artikel voor gedetailleerde uitleg en advies.

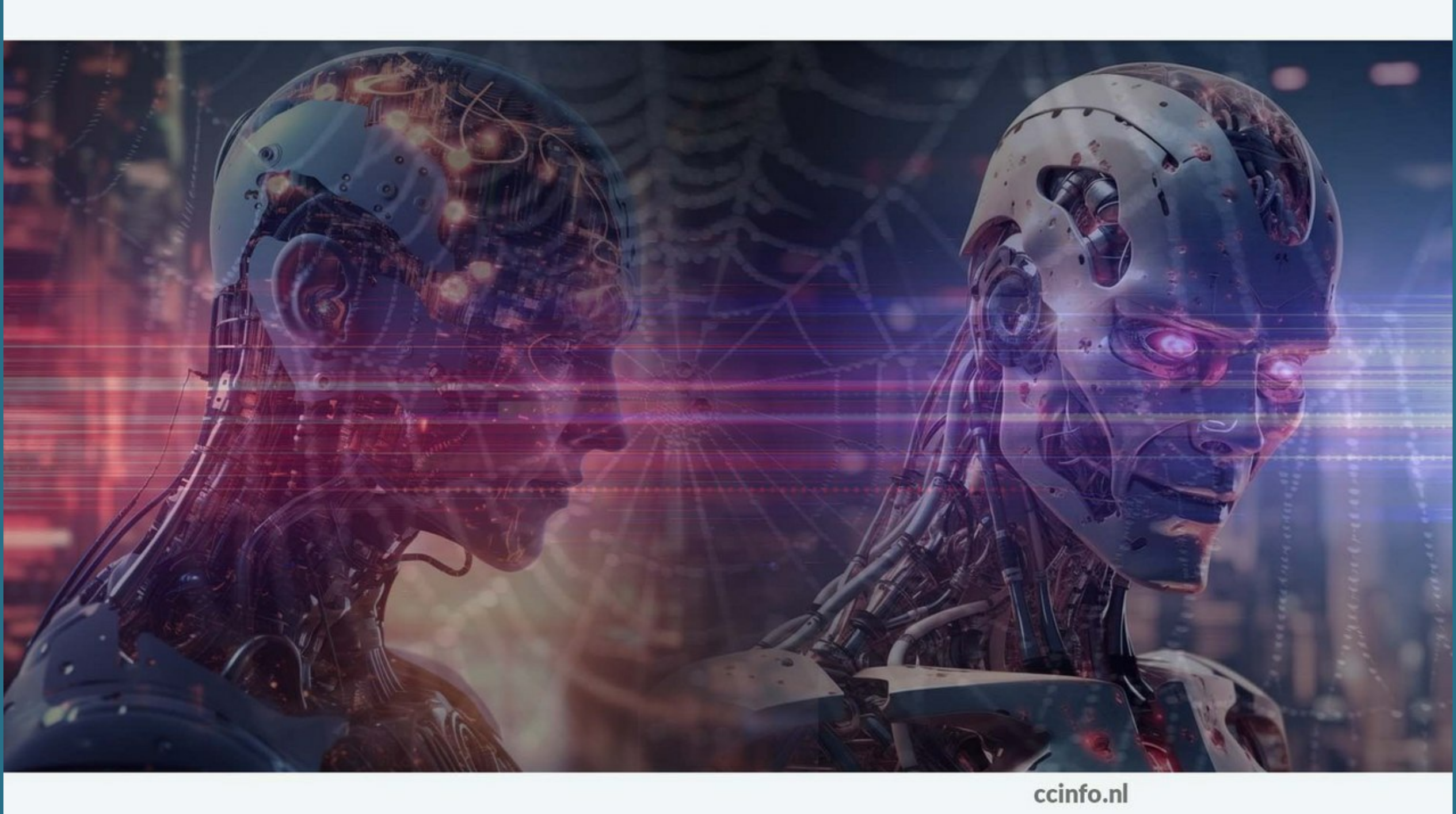
Lees verder

ccinfo.nl

De opkomende golf van massale Ransomware-aanvallen in 2023

In 2023 zien we een verontrustende opmars van massale ransomware-aanvallen, die nu verder gaan dan enkel het gijzelen van data. Deze aanvallen richten zich ook op het verstoren van toeleveringsketens, waardoor het herstelproces complexer en kostbaarder wordt. Cybercriminelen gebruiken geavanceerdere methoden zoals spear phishing en exploiteren beveiligingslekken om hun malware te verspreiden. Zelfs als losgeld wordt betaald, vaak in cryptocurrencies, is er geen garantie dat gegevens worden hersteld. Lees in ons uitgebreide artikel op CyberCrimeInfo.nl over deze evoluerende cyberdreiging en de beste praktijken voor preventie. Blijf waakzaam en voorop in de strijd tegen ransomware.

Lees verder



ccinfo.nl

De donkere kant van AI: hoe malafide taalmodellen het Darkweb veranderen

In een recent gepubliceerd artikel op CyberCrimeInfo.nl verkennen we de verontrustende opkomst van malafide taalmodellen op het darkweb. Deze AI-gedreven tools, zoals WormGPT en FraudGPT, zijn niet alleen toegankelijk maar ook gevaarlijk effectief in het faciliteren van cybercriminaliteit. Van het genereren van overtuigende phishing-aanvallen tot het creëren van gepersonaliseerde social engineering-strategieën, deze taalmodellen stellen zelfs minder technisch onderlegde personen in staat om geavanceerde cyberaanvallen uit te voeren. Dit verlaagt de drempel voor het plegen van cybermisdrijven en roept ernstige vragen op over de toekomst van cybersecurity. Lees het volledige artikel om te begrijpen welke uitdagingen en ethische vraagstukken dit met zich meebrengt.

Lees verder

ccinfo.nl

Overzicht van slachtoffers cyberaanvallen week 42-2023

In de afgelopen week van oktober 2023 zijn er opmerkelijke cyberaanvallen en beveiligingsincidenten geregistreerd die variëren van grote bedrijven tot overheidsinstellingen. Het supportsysteem van Okta, een belangrijke speler in de IT-beveiliging, is gecompromitteerd, en gevoelige klantgegevens zijn buitgemaakt. Het Internationaal Strafhof in Den Haag is eveneens aangevallen, met sterke indicaties van spionageactiviteiten. Daarnaast zijn er significante datalekken gemeld in zowel de gezondheidszorg als het bedrijfsleven, waaronder een lek bij genetisch onderzoeksbureau 23andMe. In de Benelux zijn onder andere KBS Accountants en De Groot Groep getroffen door verschillende vormen van ransomware. Lees verder voor een uitgebreid overzicht en aanbevelingen om uw cyberbeveiliging te versterken.

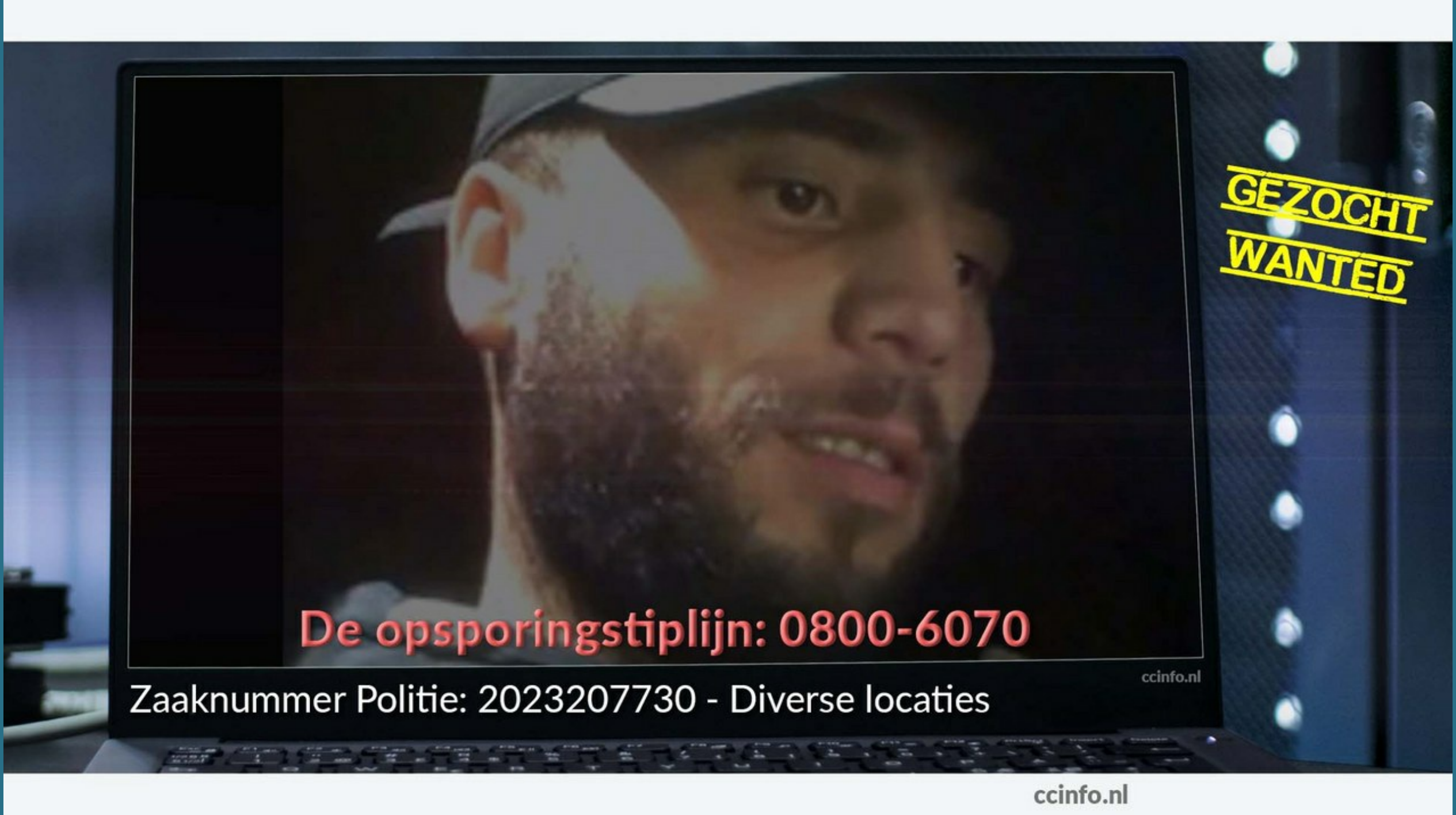
Lees verder

ccinfo.nl

Tip van de week: Bouw een veilige bedrijfscultuur als medicijn tegen cybercriminaliteit

In een wereld waar cybercriminaliteit steeds geavanceerder wordt, is technologie alleen niet voldoende om je organisatie te beschermen. Onze nieuwste publicatie op CyberCrimeInfo.nl belicht het cruciale belang van een sterke 'security culture' binnen bedrijven als effectief medicijn tegen cyberaanvallen. We ontrafelen de drie pijlers voor het opbouwen van een effectieve veiligheidscultuur: organisatie, techniek, en vooral mensen. Want onthoud: de mens is vaak de zwakste schakel in uw cybersecuritystrategie. Ontdek praktische tips en technieken om een cultuur te creëren waarin iedere medewerker zich verantwoordelijk voelt voor de veiligheid van de organisatie.

Lees verder



ccinfo.nl

Diverse locaties - Uden, Eindhoven, Zeeland - Bankhelpdesk fraude

Waarschuwing: Oplichting via bankhelpdesk neemt toe in Uden, Eindhoven en Zeeland. Een 47-jarige man uit Sint Oedenrode is onlangs slachtoffer geworden van deze vorm van fraude. Hij werd benaderd door een nep-bankmedewerker die hem verzocht Anydesk te installeren en zijn bankpassen aan een 'koerier' te overhandigen. Dezelfde avond werden er grote geldbedragen opgenomen in diverse steden. De politie is dringend op zoek naar tips die kunnen helpen bij het opsporen van de daders. Beschikt u over informatie of herkent u de betrokken personen?

Lees verder

CyberWijzer, uw persoonlijke cybersecurity expert!

"Elke dag getraind, elke dag sterker in de strijd tegen criminaliteit."

Heb je je ooit afgevraagd wat onze CyberWijzer AI Chatbot zo uniek maakt? Het antwoord is simpel: deze bot is niet zomaar een bot. Of je nu een beginner bent op het gebied van cyberveiligheid of al jaren ervaring hebt, CyberWijzer heeft voor iedereen een passend antwoord. Bovendien bieden we nu uitgebreide informatie over virussen en malware, inclusief instructies voor het verwijderen ervan.
Ben je nieuwsgierig geworden? Bekijk dan de voorbeeldvragen 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
