Cybercrimeinfo.nl
Het onzichtbare zichtbaar maken

Nieuwsbrief 357

Reading in another language

Amerika stopt cyberaanvallen tegen Rusland: gevolgen en risico's voor Europa

De Verenigde Staten stoppen met offensieve cyberoperaties tegen Rusland, een drastische koerswijziging die grote gevolgen heeft voor de digitale veiligheid in Europa. Terwijl de VS Rusland niet langer als cyberdreiging zien, blijft Moskou wel actief in het aanvallen van westerse infrastructuur en instellingen. Dit roept vragen op over de veiligheid van Europa, dat nu minder inlichtingen en steun ontvangt vanuit Washington. Dreigt een verschuiving van Russische cyberaanvallen naar Europese doelen? En hoe kan Europa zich hiertegen wapenen? Lees verder om de impact van deze strategische zet te begrijpen.

Lees verder

Reading in another language

Misleidende popups vragen om nu bij te werken, hoe criminelen via nepupdates mobiele apparaten infecteren

Je smartphone geeft een melding dat een update nodig is en zonder erbij na te denken klik je op ‘Nu bijwerken’. Maar wat als die melding vals is en in werkelijkheid malware op je apparaat installeert? Cybercriminelen gebruiken steeds vaker misleidende pop-ups om Android-gebruikers te infecteren via malafide advertenties, ook wel malvertising genoemd. Deze aanvallen zijn geraffineerd en kunnen zelfs op betrouwbare websites opduiken. In dit artikel lees je hoe deze nepupdates werken, waarom vooral Android-gebruikers gevaar lopen en hoe je jezelf kunt beschermen tegen deze vorm van cybercriminaliteit.

Lees verder

Reading in another language

Russische hackers ronselen burgers online voor cyberaanvallen en sabotage

Russische hackers gebruiken steeds vaker een nieuwe strategie om westerse samenlevingen te ontwrichten. Via online platforms zoals sociale media en Telegram werven zij nietsvermoedende burgers voor sabotage en cyberaanvallen. Deze ‘wegwerpagenten’ krijgen relatief eenvoudige opdrachten en worden betaald in cryptomunten, waardoor de werkelijke opdrachtgevers verborgen blijven. Wat begint als een onschuldige taak, kan uitmonden in serieuze criminele activiteiten met verstrekkende gevolgen voor de nationale veiligheid. Hoe werkt deze rekruteringsmethode en welke impact heeft het op onze samenleving? Lees verder en ontdek de verborgen gevaren van hybride oorlogvoering.

Lees verder

Reading in another language

Vraag van de week: De impact van quantum computing op wachtwoordbeheer: Is MindYourPass toekomstbestendig?

Quantumcomputers beloven ongekende rekenkracht, maar vormen tegelijk een bedreiging voor traditionele wachtwoordbeveiliging. Encryptie-algoritmen die nu als veilig gelden, kunnen in de toekomst in een oogwenk gekraakt worden. Wat betekent dit voor wachtwoordmanagers zoals MindYourPass? Is deze technologie bestand tegen de impact van quantum computing? In dit artikel onderzoeken we de risico’s en kijken we naar innovatieve oplossingen om onze digitale identiteit veilig te houden.

Lees verder

Reading in another language

Cybercrime op het darkweb: hoeveel kost hacken echt?

Het darkweb is een duistere marktplaats waar cybercriminelen investeren in digitale wapens en gestolen gegevens. Maar hoeveel kost het eigenlijk om een hack uit te voeren? Van ransomware en zero-day exploits tot toegang tot gehackte bedrijfsnetwerken, de prijzen lopen sterk uiteen. Dit artikel geeft inzicht in de kosten en winstmodellen van cybercriminelen en laat zien waarom cyberaanvallen zo lucratief zijn. Ontdek hoe de handel in cybercrime werkt en waarom het voor bedrijven en individuen cruciaal is om zich hiertegen te wapenen.

Lees verder

Reading in another language

Gouda - Helpdesk fraude

Een 88-jarige vrouw uit Gouda werd het slachtoffer van een geraffineerde vorm van oplichting. Een fraudeur deed zich voor als bankmedewerker en wist haar te overtuigen haar sieraden af te geven, zogenaamd ter bescherming. Dit type criminaliteit, bekend als bankhelpdeskfraude, komt steeds vaker voor en maakt misbruik van het vertrouwen van slachtoffers. Hoe herkent u deze vorm van fraude en wat kunt u doen om uzelf en anderen te beschermen? Lees verder en ontdek de werkwijze van oplichters en hoe u voorkomt dat u de volgende prooi wordt.

Lees verder

Blijf op de hoogte van de nieuwste cybercrime- en darkwebtrends!

Cybercriminelen worden steeds slimmer en cyberdreigingen ontwikkelen zich razendsnel. Wil je op de hoogte blijven van de nieuwste trends op het darkweb, digitale fraude en actuele cyberaanvallen? Via ons Telegram-kanaal ontvang je direct de laatste updates, exclusieve analyses en inzichten waarmee je jouw cyberweerbaarheid vergroot. Mis niets en maak samen met ons het onzichtbare zichtbaar in de digitale wereld.

Telegram kanaal Cybercrimeinfo

AI-gids CyberWijzer: Kunstmatige intelligentie voor cyberveiligheid

De AI-gids CyberWijzer biedt een overzicht van hoe kunstmatige intelligentie (AI) kan helpen bij het verbeteren van cyberveiligheid. De gids bevat praktische tips en tools om AI effectief in te zetten tegen digitale dreigingen. Met de opkomst van cybercriminaliteit wordt AI steeds vaker gebruikt om aanvallen sneller te detecteren en te bestrijden. CyberWijzer helpt gebruikers om AI op een veilige en verantwoorde manier toe te passen, zowel voor bedrijven als particulieren. De gids behandelt onder andere het herkennen van verdachte activiteiten, het verbeteren van wachtwoordbeheer en het veilig omgaan met online data. Daarnaast is CyberWijzer zeer handig bij de implementatie van de NIS2-richtlijn, die strengere eisen stelt aan cybersecurity binnen bedrijven en organisaties. Door AI op de juiste manier te benutten, kunnen organisaties en individuen zich beter wapenen tegen cyberdreigingen.

AI CyberWijzer

Reading in another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waarin digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Als onafhankelijke organisatie, volledig gedreven door vrijwilligers, zetten wij ons in om het publiek te informeren en beschermen tegen de gevaren van het digitale tijdperk.

Jouw donatie maakt het verschil. Dit is waarom:

- **Een onafhankelijke en betrouwbare 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.
- **Bewustwording en preventie mogelijk maken**
  Met jouw donatie help je ons om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen direct bij aan het voorkomen van digitale misdrijven.
- **Ondersteuning van operationele kosten**
  Donaties worden direct gebruikt voor het hosten van onze website en het up-to-date houden van technologische middelen. Hierdoor kunnen we cybercriminelen blijven volgen en jullie informeren over de nieuwste digitale dreigingen.

Elke bijdrage, groot of klein, is van onschatbare waarde in onze strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Doneer nu via onze doneerpagina (kies zelf het bedrag dat je wilt doneren) of gebruik de onderstaande QR-code.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

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

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.

Non-profit team Cybercrimeinfo (ccinfo)

Schrijf een review

Share Tweet Share Pinterest Bluesky Mastodon