



Nieuwsbrief 354

The new reality of geopolitical and digital threats

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

De nieuwe realiteit van geopolitieke en digitale dreigingen

De wereldorde is in beweging. Met de herverkiezing van Trump in 2025 en de toenemende militaire assertiviteit van Rusland bevinden we ons in een tijdperk waarin geopolitieke spanningen en digitale dreigingen elkaar versterken. Traditionele bondgenootschappen staan onder druk, terwijl cyberoorlogsvoering steeds vaker wordt ingezet als strategisch wapen. Van gerichte cyberaanvallen op vitale infrastructures tot desinformatiecampagnes die democratieën ondermijnen, de digitale arena is nu een volwaardig strijdtoneel.

Wat betekent dit voor de veiligheid van landen, bedrijven en individuen? Hoe kunnen we ons wapenen tegen deze nieuwe dreigingen? In dit artikel duiken we dieper in de geopolitieke verschuivingen, de impact van cyberoorlogsvoering en de maatregelen die nodig zijn om ons digitaal en strategisch te beschermen.

[Lees verder](#)

Changing attack techniques in the digital world

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Veranderende aanvalstechnieken in de digitale wereld

Cyberaanvallen worden steeds geavanceerder, met malware zoals LummaStealer en FrididStealer die onopgemerkt gevoelige informatie kunnen stelen. Criminelen misbruiken social media, gekaapte websites en zelfs legitiem ogende updates om slachtoffers te besmetten. Of je nu Windows, macOS of Android gebruikt, geen enkel systeem is veilig zonder de juiste maatregelen. In dit artikel ontdek je hoe deze nieuwe dreigingen werken, welke technieken aanvallers gebruiken en, belangrijker nog, hoe je jezelf en je organisatie hiertegen kunt beschermen. Lees verder en blijf cybercriminelen een stap voor!

[Lees verder](#)

Instagram hacks: why even 2FA doesn't always protect you from digital attacks

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Instagram hacks: waarom zelfs 2FA je niet altijd beschermt tegen digitale aanvallen

Instagram accounts worden steeds vaker gehackt, zelfs als gebruikers hun beveiliging goed op orde hebben. Twee-factor-authenticatie (2FA) zou extra bescherming moeten bieden, maar cybercriminelen vinden steeds slimmere manieren om deze beveiligingslaag te omzeilen. Van phishing-aanvallen tot SIM-swapping en malware: hackers hebben meerdere methoden om toegang te krijgen tot accounts. Hoe kunnen zij 2FA omzeilen en wat kun je doen om je account beter te beschermen? In dit artikel duiken we dieper in de technieken van cybercriminelen en geven we praktische tips om jouw Instagram-account veilig te houden.

[Lees verder](#)

The role of ethical hackers in a proactive cybersecurity strategy

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

De rol van ethische hackers in een proactieve cybersecuritystrategie

In een wereld waarin cyberaanvallen steeds geavanceerder worden, is afwachten geen optie meer. Bedrijven en overheden moeten proactief handelen om hun digitale veiligheid te waarborgen. Ethische hackers, ook wel white hat hackers genoemd, spelen hierin een cruciale rol. Zij sporen kwetsbaarheden op voordat cybercriminelen dat doen en helpen organisaties zich te wapenen tegen digitale dreigingen. Maar hoe gaan ze te werk? Welke uitdagingen komen ze tegen? En waarom is preventie zoveel effectiever dan enkel reageren op incidenten? Ontdek in dit artikel hoe ethische hackers bijdragen aan een robuuste cybersecuritystrategie en waarom zij de 'rookmelders' van de digitale wereld zijn.

[Lees verder](#)

Tip of the week: extra security for your iCloud data

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Tip van de week: extra beveiliging voor je iCloud-data

Cyberdreigingen zijn overal: datalekken, ransomware en hackers liggen op de loer. Toch laat een groot deel van de Apple-gebruikers hun iCloud-data onnodig kwetsbaar. Met Geavanceerde Gegevensbescherming (ADP) introduceert Apple een extra beveiligingslaag met end-to-end encryptie, waardoor zelfs Apple geen toegang meer heeft tot jouw back-ups, foto's en notities. Maar wat betekent dit precies voor jouw digitale veiligheid? Hoe activeer je ADP en welke risico's brengt het met zich mee? In dit artikel lees je alles over hoe je jouw iCloud-gegevens beter kunt beschermen én wat Android-gebruikers als alternatief kunnen doen.

[Lees verder](#)


Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Middelburg - Helpdesk fraude

In Middelburg zijn vijf slachtoffers misleid door een oplichtster die zich voordeed als bankmedewerker. Met een geraffineerde smoes wist zij hun bankpassen in handen te krijgen en duizenden euro's buit te maken. De politie is op zoek naar deze verdachte en roept het publiek op om tips te delen. Herken jij haar? Lees verder en help mee om deze fraudeur op te sporen!

[Lees verder](#)

AI Cyberwijzer

AI Cyberguide

Cybercrimeinfo | ccinfo.nl

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



Cybercrimeinfo | ccinfo.nl

[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 (ccinfo.nl)

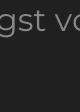
[Doneer pagina](#)
[Geen budget? Geen probleem!](#)
[Help ons de zichtbaarheid van Cybercrimeinfo te vergroten door jouw Google review!](#)
[Laat jouw stem horen: Steun ons met een Google review!](#)

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.

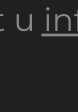
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review.**

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.

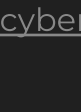
Non-profit team Cybercrimeinfo (ccinfo)

[Schrijf een review](#)


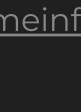
Share



Tweet



Share



Pinterest

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.