# Cybercrimeinfo

*"Omdat wat waardevol is, beschermd moet worden"*

## Nieuwsbrief 391

---

## Test je digitale weerbaarheid met de wekelijkse pro quiz van Cybercrimeinfo

Cybercrimeinfo daagt je elke week uit met een pro quiz, speciaal ontworpen om jouw kennis van cyberveiligheid te versterken.
Ransomware, phishing, zwakke plekken in systemen, deze quiz houdt je scherp en up-to-date met de laatste digitale dreigingen.

Je leert niet alleen bij, maar traint ook actief je digitale weerbaarheid. Zo ben je beter voorbereid op de slimmigheidjes van cybercriminelen.

Kortom: een slimme, snelle en serieuze manier om je cybersecurity skills te verbeteren. Doe mee met de quiz en blijf de cyberboeven een stap voor!

**QUIZ 45-2025**

---


## Toegang tot Nederlands bedrijf verkocht op hackforum terwijl AI wordt ingezet voor digitale manipulatie

Hackers hebben toegang tot een Nederlands bedrijf verkocht op een hackforum, waarbij ze inloggegevens via een domeinaccount deelden. Dit biedt hen de mogelijkheid om vertrouwelijke bedrijfsinformatie te stelen. Daarnaast wordt kunstmatige intelligentie (AI) steeds vaker ingezet voor digitale manipulatie, met als doel om cybercriminaliteit te vergemakkelijken. Tegelijkertijd zijn er zorgen over de veiligheid van AI-systemen, waarbij experts, zoals Zico Kolter van OpenAI, zich inzetten voor het veilig houden van AI-ontwikkeling.

**LEES VERDER**


## EU locatiegegevens te koop, AI in nep sollicitaties, 92 kwetsbare DNS servers en RMM misbruik in transport

Europese locatiegegevens van miljoenen mobiele telefoons, waaronder die van EU-functionarissen, worden te koop aangeboden op het dark web, wat een risico vormt voor spionage en chantage. In België heeft de hacker groep NoName verschillende DDoS-aanvallen uitgevoerd op belangrijke websites. Ook werd ontdekt dat cybercriminelen zich voordoen als nep sollicitanten in de crypto- en Web3-sector, met behulp van deepfake-technologie. Verder bleken er kwetsbaarheden in DNS-servers en Windows-server systemen, waardoor bedrijven in Nederland en België risico liepen op misbruik.

**LEES VERDER**


## Digitale stalking bestraft, kritieke updates na mobiele aanvallen, DDoS en nieuw afperscollectief

Een vrouw die jarenlang werd belaagd via digitale stalking, kreeg een celstraf en een contactverbod. Dit benadrukt de serieuze gevolgen van online intimidatie. Er werden verschillende beveiligingslekken ontdekt in populaire systemen, waaronder WordPress, Android, Apple, en Microsoft Teams, waarvoor updates werden uitgebracht. Er is een toename van mobiele aanvallen, waaronder phishing en betalingssysteemfraude. Een nieuw afperscollectief, "Scattered LAPSUS Hunters", is actief, met extorsie als dienst. DDoS-aanvallen verstoren publieke websites, en er is groeiende bezorgdheid over de kwetsbaarheid van mobiele apparaten en applicaties.

**LEES VERDER**


## AI gedreven ransomware, botnet exploits en gerichte aanvallen op organisaties zoals Proximus en UZ Gent

AI-gedreven ransomware en botnet-aanvallen richten zich op grote organisaties zoals Proximus, UZ Gent en Cisco, waarbij nieuwe malware gebruikmaakt van kunstmatige intelligentie om zich aan te passen en moeilijker te detecteren te zijn. Daarnaast worden kwetsbaarheden in software, zoals CentOS Web Panel en Elastic Cloud Enterprise, actief misbruikt door hackers om systemen te compromitteren. Geopolitieke spanningen beïnvloeden de digitale dreigingen, waarbij landen zoals Rusland via cyberaanvallen politieke doelen nastreven. Wetshandhaving wereldwijd werkt steeds nauwer samen om criminele netwerken aan te pakken.

**LEES VERDER**


## RTV Noord en Belgische gemeenten verstoord door cyberaanvallen en nieuwe dreigingen tegen industriële systemen en mobiele apparaten

RTV Noord werd getroffen door een cyberaanval die tijdelijke verstoringen veroorzaakte in de uitzendingen en de toegang tot systemen. In België platlegden DDoS-aanvallen gemeentelijke websites, waarbij de groep NoName verantwoordelijk zou zijn voor aanvallen op kritieke infrastructuur zoals de Haven van Antwerpen. Ondertussen werd een kwetsbaarheid in Cisco's callcenter-software ontdekt, die bedrijven blootstelt aan aanvallen. Cyberdreigingen richten zich steeds meer op mobiele apparaten en IoT-systemen, wat de kwetsbaarheid van de publieke sector benadrukt. Geopolitieke hackers zoals Sandworm verstoren ook strategische sectoren in Oekraïne, zoals de graanproductie.

LEES VERDER


## NoName057 valt Belgische militaire inlichtingendienst aan en kwetsbaarheden in Cisco firewalls bedreigen systemen

Op 7 november 2025 werden verschillende Belgische overheidswebsites aangevallen door hackergroepen zoals NoName057, die zich richtte op de militaire inlichtingendienst ADIV. Tevens werden kwetsbaarheden ontdekt in Cisco firewalls, wat Nederlandse en Belgische bedrijven in gevaar bracht. Daarnaast werden nieuwe vormen van Android-malware zoals Landfall en Fantasy Hub aangetroffen, die persoonlijke gegevens en bankinformatie stelen. Ook werden phishingaanvallen en frauduleuze advertenties op sociale media waargenomen. Hackers blijven wereldwijd actief, met China en Rusland als belangrijke dreigingen.

**LEES VERDER**

---


## Krimpen aan den IJssel - Bankhelpdeskfraude

Op 1 mei 2025 werd een 77-jarige man uit Krimpen aan den IJssel slachtoffer van bankhelpdeskfraude. Na het ontvangen van een sms van een vermeende bank, die melding maakte van een mislukte overboeking, belde de man naar het opgegeven

nummer en werd hij door een oplichter geholpen die zich voordeed als bankmedewerker. De man werd gevraagd zijn bankapp te gebruiken en zijn pincodes te delen. Later moest hij zijn pinpassen, sieraden en contant geld in een envelop overhandigen voor een koerier. De politie is op zoek naar de verdachte die met de gestolen pinpassen geld opnam.

## LEES VERDER

---

Luister naar de discussiepodcast over het nieuws van de afgelopen week.

**Luister de podcast nu op Youtube**

**Luister de podcast nu op Spotify**

---

**Meer leren over cybercrime? Ontdek de verschillende vormen en begrippen**

In de Cybercrimeinfo Bibliotheek vind je een uitgebreide verzameling van termen en verschillende vormen van cybercriminaliteit. Van phishing en malware tot ransomware en andere digitale dreigingen, we leggen elke vorm duidelijk uit. Zo krijg je inzicht in wat deze aanvallen inhouden, hoe ze werken en welke risico's ze met zich meebrengen.

Of je nu op zoek bent naar uitleg over specifieke cybercrime termen of meer wilt leren over de verschillende soorten digitale bedreigingen, onze bibliotheek biedt de kennis die je nodig hebt om jezelf beter te beschermen.

Verdiep je in de wereld van cybercrime en vergroot je digitale weerbaarheid.

## BEKIJK DE BIBLIOTHEEK

---

**Beantwoorde vragen en tips voor digitale weerbaarheid**

Op deze pagina vind je antwoorden op veelgestelde vragen, nuttige tips en praktische hulpmiddelen om je digitale veiligheid te verbeteren. Of je nu meer wilt weten over bescherming tegen cyberdreigingen of jezelf beter wilt wapenen tegen online gevaren, wij bieden de informatie die je nodig hebt.

## BEKIJK DE TIPS

---

**Veelgestelde vragen over digitale veiligheid en cybercrime**

Op Cybercrimeinfo vind je antwoorden op de meest gestelde vragen over cybersecurity en cybercrime. Leer hoe je jezelf en je organisatie kunt beschermen tegen digitale dreigingen, van phishing en malware tot ransomware en DDoS-aanvallen. We bieden duidelijke uitleg en praktische tips om je digitale veiligheid te versterken.

## ONTDEK DE ANTWOORDEN

**Vergroot je kennis en vaardigheden**

Wil je je kennis over cybersecurity en het darkweb uitbreiden? Bij de Leerplek van Cybercrimeinfo vind je een breed aanbod van cursussen, tutorials en quizzen die je helpen up-to-date te blijven met de nieuwste technieken en dreigingen. Of je nu net begint of al een expert bent, onze interactieve leeromgeving biedt de uitdaging die je nodig hebt om jezelf verder te ontwikkelen.
Test je kennis met uitdagende quizzen en verdien toegang tot de exclusieve Perfecte Score Club. Voor opsporingsambtenaren bieden we binnenkort speciaal op maat gemaakte quizzen aan.

**TEST JE KENNIS**

---


**Contact met Cybercrimeinfo**

Heb je een vraag of probleem? Vul het formulier in en stel je vraag. We reageren zo snel mogelijk, maar houd er rekening mee dat het door de hoge aantallen vragen soms enkele dagen kan duren.

**STEL JE VRAAG**

---

**Steun Cybercrimeinfo en help de strijd tegen cybercriminaliteit**

Elke dag zetten wij ons in om je op de hoogte te houden van de laatste cyberdreigingen en trends. Onze missie is om jou en anderen te beschermen tegen de groeiende risico's in de digitale wereld. Maar we kunnen dit niet alleen. Jouw steun maakt het verschil.
Door te doneren help je ons waardevolle informatie te blijven leveren, nieuwe tools te ontwikkelen en de bewustwording over cybercriminaliteit te vergroten. Elke bijdrage, groot of klein, draagt bij aan de bescherming van digitale veiligheid.
Wil je ons steunen?

Samen maken we de online wereld een stukje veiliger.
Bedankt voor je steun!

**❤ STEUN ONS NU**

---

## Dagelijks cyber journaal van Cybercrimeinfo

Het Dagelijks Cyber Journaal biedt dagelijkse updates over de belangrijkste cyberdreigingen en incidenten in België en Nederland. Dit is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar geen tijd hebben om alles bij te houden. Het biedt een efficiënte manier om snel up-to-date te blijven zonder uren te spenderen aan het zoeken naar relevante informatie. De updates zijn beschikbaar in zowel tekst als via een dagelijkse podcast op Spotify en YouTube.

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag).
Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Achternaam

Inschrijven


## Inschrijven

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

**INSCHRIJVEN**

Share Tweet Share Pinterest Bluesky Mastodon