

A modern office desk with three computer monitors. The monitors display a dark-themed user interface with various panels and text. A large, semi-transparent 'MAGAZINE' watermark is centered across the middle of the image, spanning all three monitors. On the desk in front of the monitors is a keyboard and a mouse. The background shows a blurred office environment with windows.

MAGAZINE

VEILIG DIGITAAL



Jack Dorsey lanceert Bitchat – Chatten zonder internet

Block CEO en mede-oprichter van Twitter, Jack Dorsey, heeft in juli 2025 een nieuwe berichtenapp gelanceerd genaamd Bitchat. Deze experimentele messaging-innovatie trekt direct veel media-aandacht door haar unieke eigenschappen.

Bitchat belooft een revolutionaire manier om te communiceren zonder afhankelijk te zijn van internetverbindingen of mobiele netwerken.

VEILIGDIGITAAL.COM

Bitchat is een Bluetooth-berichtenapp



Bluetooth communicatie

Bitchat werkt met het Bluetooth-sigitaal van een telefoon. Hierdoor kunnen gebruikers communiceren in drukke omgevingen zoals festivals of protesten waar wifi en telefoonservice beperkt zijn - per ongeluk of door ontwerp.



Mesh-netwerk technologie

Bitchat omzeilt het probleem van het beperkte bereik van Bluetooth, meestal rond de 100 meter, door gebruik te maken van een Bluetooth-mesh-netwerk, dat berichten doorstuurt via andere gebruikers binnen bereik.



Privacy en digitale vrijheid

Jack Dorsey's lancering van Bitchat komt voort uit groeiende zorgen over online privacy en digitale controle. In een wereld waar grote technologiebedrijven steeds meer macht krijgen over onze communicatie, pleit Dorsey voor een fundamentele verandering in hoe we digitaal met elkaar verbinden.

Volledige decentralisatie en privacy

Geen persoonlijke identificatie

Bitchat vraagt gebruikers niet om accounts aan te maken of persoonlijke gegevens zoals telefoonnummers of e-mailadressen te delen. Dit maakt anonieme communicatie mogelijk.

Tijdelijke berichtenopslag

Berichten bestaan uitsluitend in het werkgeheugen van de betrokken apparaten en worden niet permanent opgeslagen, wat de privacy van gebruikers maximaal beschermt.

Geen centrale servers

Er zijn geen centrale servers die berichten verwerken of opslaan. Het netwerk bestaat volledig uit de apparaten van gebruikers die met elkaar communiceren.

End-to-end encryptie

Alle communicatie is standaard beveiligd met sterke end-to-end encryptie, waardoor zelfs als berichten onderschept worden, ze niet leesbaar zijn voor derden.

Unieke Bitchat-functies



Room-based chats

Gebruikers kunnen deelnemen aan groepsgesprekken door simpelweg dezelfde hashtag te gebruiken, wat ad-hoc communities mogelijk maakt.



"Store-and-forward"

Berichten voor offline gebruikers worden tijdelijk bewaard en later afgeleverd wanneer ze weer verbinding maken met het netwerk.



Wachtwoordbeveiliging

Voor extra privacy kunnen gebruikers hun chats beveiligen met wachtwoorden, zodat alleen geautoriseerde personen kunnen deelnemen.



Dubbele functionaliteit

Elk apparaat functioneert zowel als zender én ontvanger in het mesh-netwerk, wat de infrastructuur versterkt met elk nieuw apparaat.

Praktische toepassingen en doelgroep



Essentiële communicatie bij uitval

Bitchat biedt een levensreddende communicatiemogelijkheid tijdens natuurrampen, stroomstoringen of andere scenario's waarbij reguliere netwerken uitvallen.

Privacybewuste gebruikers

Voor journalisten, activisten en anderen die discreet moeten communiceren zonder digitale sporen achter te laten, biedt Bitchat een veiliger alternatief.

Drukbezochte evenementen

Op festivals, conferenties en sportevenementen waar mobiele netwerken vaak overbelast raken, kan Bitchat zorgen voor stabiele lokale communicatie.

Uitdagingen en beperkingen

Beperkt fysiek bereik

De standaard Bluetooth-verbinding heeft een bereik van slechts 30 meter, wat betekent dat er voldoende apparaten in elkaars nabijheid moeten zijn om het netwerk effectief te laten functioneren.

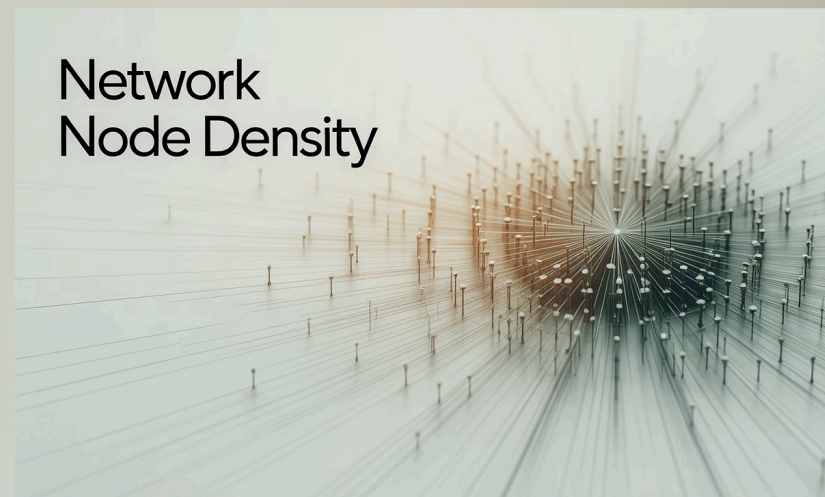
Afhankelijk van gebruikersdichtheid

Het mesh-netwerk werkt alleen optimaal wanneer er voldoende actieve Bitchat-gebruikers zijn in een bepaald gebied. In dunbevolkte gebieden kan de functionaliteit beperkt zijn.

Nog in ontwikkeling

Als bètaversie heeft Bitchat nog te kampen met kinderziektes op gebied van robuustheid, batterijverbruik en gebruiksvriendelijkheid. De app ondergaat nog intensieve testen en optimalisatie.

Network Node Density



De visie van Dorsey: impact en toekomst

"Bitchat is meer dan een app – het is een stap naar echte digitale autonomie voor iedereen, ongeacht waar ze wonen of onder welk regime." – Jack Dorsey

Dorsey's visie reikt verder dan alleen een berichtenapp. Bitchat vertegenwoordigt een fundamentele verschuiving naar meer gebruikerscontrole en minder afhankelijkheid van gecentraliseerde systemen die gevoelig zijn voor censuur en surveillance.

De open protocol-aanpak van Bitchat dient als blauwdruk voor toekomstige innovaties. Als succesvolle implementatie kan het een inspiratiebron worden voor een breed scala aan decentrale apps en diensten die privacy en gebruikersautonomie centraal stellen.



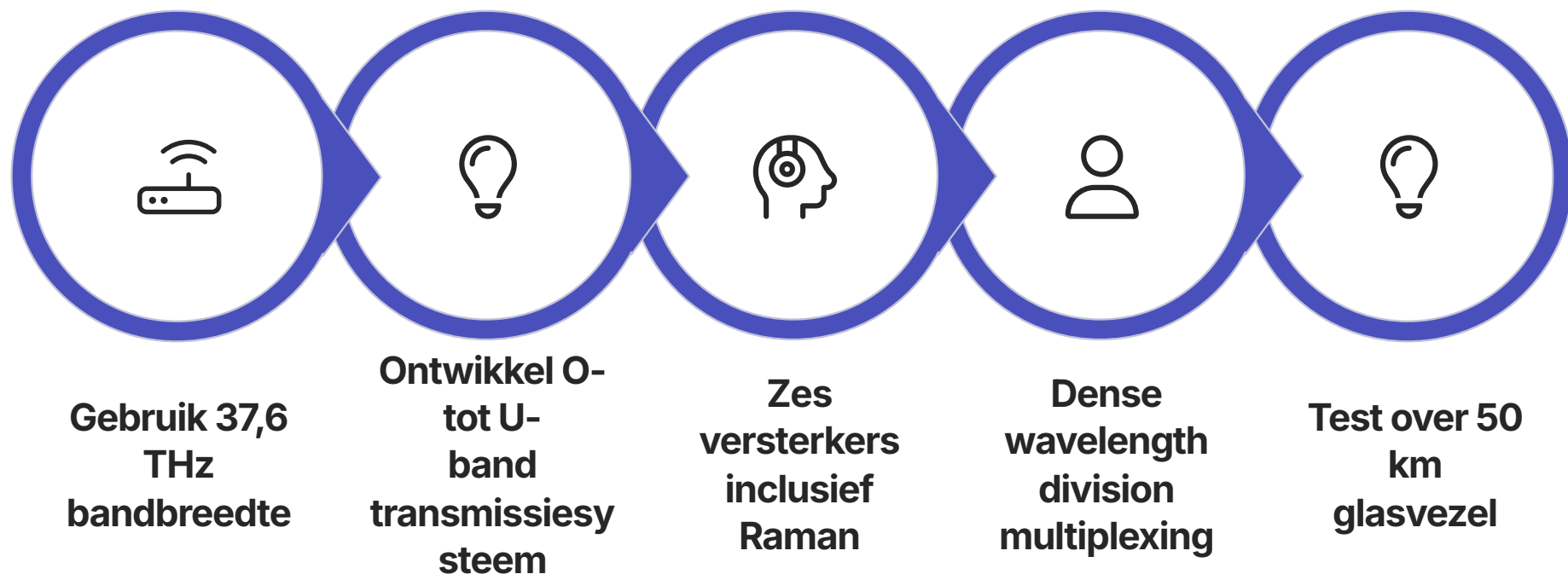
Japan vestigt nieuw snelheidsrecord voor internet: 402 terabits per seconde

Japanse onderzoekers van het National Institute of Information and Communications Technology (NICT) hebben een baanbrekend nieuw internetsnelheidsrecord gevestigd van 402 terabits per seconde (Tbps). Deze uitzonderlijke prestatie verbreekt het vorige wereldrecord van 321 Tbps dat in 2023 werd behaald. Om de indrukwekkende aard van deze snelheid te illustreren: een volledige game zoals Elden Ring (ongeveer 18GB) zou in minder dan een milliseconde kunnen worden gedownload.

VEILIGDIGITAAL.COM

Technologische innovaties achter het record

De doorbraak is bereikt door gebruik te maken van standaard commercieel verkrijgbare glasvezelkabels, dezelfde soort kabels die de backbone vormen van onze huidige netwerken. Dit is een significante ontwikkeling omdat het aantoont dat bestaande infrastructuur potentieel heeft voor enorme snelheidsverbeteringen zonder complete vervanging van de basisarchitectuur.



De onderzoekers slaagden erin om een indrukwekkende 37,6 terahertz (THz) bandbreedte te benutten over een afstand van 50 kilometer glasvezel. Een cruciaal element in dit onderzoek was de ontwikkeling van een transmissiesysteem dat gebruikmaakt van het volledige spectrum van de zogenaamde O- tot U-band. Dit systeem implementeert dense wavelength division multiplexing (DWDM), een techniek die meerdere golflengtes van licht tegelijkertijd door dezelfde glasvezel stuurt.

Een andere essentiële innovatie was de toepassing van zes verschillende soorten optische versterkers, waaronder geavanceerde Raman-amplificatie. Deze versterkers compenseren voor het verzwakken van het signaal over langere afstanden, wat normaal gesproken een van de grootste beperkingen is bij het verhogen van de transmissiesnelheid. Door deze versterkers strategisch toe te passen, konden de onderzoekers de kwaliteit van het signaal behouden terwijl ze de capaciteit drastisch verhoogden.

Praktische betekenis en beperkingen

Hoewel het nieuwe snelheidsrecord van 402 Tbps indrukwekkend is, moet worden opgemerkt dat deze technologie nog ver verwijderd is van praktische toepassingen voor de gemiddelde consument. De huidige beperking ligt niet bij de glasvezelkabels zelf, maar bij de hardware die we gebruiken om data te verwerken. Standaard consumentenhardware zoals Ethernet-poorten, routers en zelfs de snelste SSD's kunnen bij lange na niet overweg met deze enorme hoeveelheden data.

De werkelijke betekenis van deze doorbraak ligt in het aantonen dat onze bestaande glasvezelinfrastructuur veel meer potentieel heeft dan we eerder dachten. Dit kan leiden tot aanzienlijke kostenbesparingen voor netwerkproviders en telecombedrijven, aangezien het suggereert dat we mogelijk niet alle onderzeese kabels en nationale backbones hoeven te vervangen om hogere snelheden te bereiken.



De directe toepasbaarheid van deze technologie zal vooral liggen bij grootschalige datacenters, nationale internetbackbones en onderzeese kabelverbindingen - de belangrijkste infrastructuur die onze digitale wereld ondersteunt. Hier kan deze technologie helpen bij het oplossen van capaciteitsproblemen en het voorbereiden van netwerken op toekomstige dataintensieve toepassingen.

1

Voordelen

- Bestaande infrastructuur kan worden hergebruikt en geüpgraded
- Aanzienlijke kostenbesparing vergeleken met volledige vervanging
- Langere levensduur voor huidige netwerkinvesteringen
- Bereidt netwerken voor op exponentiële groei van dataverkeer

2

Beperkingen

- Consumentenhardware kan deze snelheden niet verwerken
- Complexe en dure apparatuur is nodig voor signaalversterking
- Praktische implementatie op grote schaal ligt nog jaren in de toekomst
- Volledige netwerkarchitectuur moet worden aangepast

3

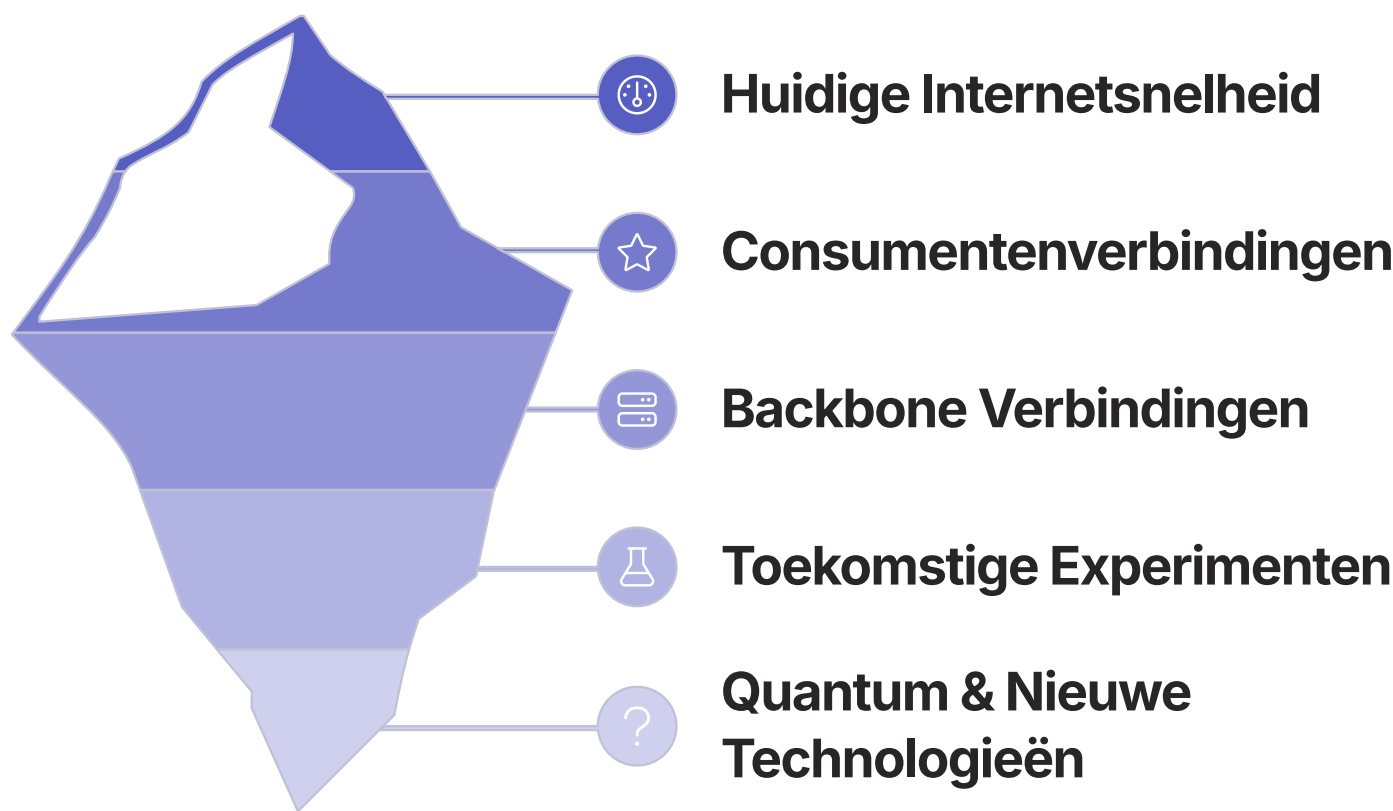
Toepassings-gebieden

- Datacenters met extreme dataverkeerbehoeften
- Internationale onderzeese kabelverbindingen
- Nationale internetbackbones en kernnetwerken
- Onderzoeksinstellingen en wetenschappelijke rekencentra

Hoewel deze technologie niet direct relevant is voor huishoudens, wijst het resultaat wel de weg naar wat algemeen wordt aangeduid als 'Beyond 5G'-diensten. Deze diensten zullen in de toekomst nog hogere eisen stellen aan de capaciteit van onze netwerken, en deze doorbraak toont aan dat onze huidige infrastructuur in principe klaar is om aan die eisen te voldoen.

Vooruitzichten en toekomst van supersnel internet

Het recente snelheidsrecord van 402 Tbps heeft verstrekende implicaties voor de toekomst van internetcommunicatie. Een van de belangrijkste conclusies is dat bestaande netwerken nog lang niet zijn uitontwikkeld. Terwijl veel telecombedrijven nadenken over volledige vervanging van hun infrastructuur, toont dit onderzoek aan dat substantiële verbeteringen mogelijk zijn binnen de bestaande architectuur door optimalisatie van transmissietechnieken.



Door nieuwe frequentiebanden te benutten en innovatieve technieken toe te passen op bestaande optische vezels, kunnen netwerken worden voorbereid op de exponentieel groeiende datavraag. Met de opkomst van kunstmatige intelligentie, virtual reality, 8K-streaming en het internet der dingen zal de hoeveelheid data die over onze netwerken stroomt alleen maar toenemen. De technologieën die zijn ontwikkeld tijdens dit onderzoek bieden een pad naar het accommoderen van deze groei zonder massale vervangingen van infrastructuur.

Jaartal	Snelheidsrecord	Technologische doorbraak
2020	178 Tbps	Verbeterde modulatietechnieken
2023	321 Tbps	Multi-core glasvezel en geavanceerde modulatie
2024	402 Tbps	O- tot U-band transmissie met DWDM
Verwacht 2030	1 Petabit/s	Geavanceerde fotonische geïntegreerde circuits

Dit onderzoek stimuleert niet alleen de ontwikkeling van ultrasnelle verbindingen voor toekomstige communicatiediensten, maar heeft ook economische voordelen. De mogelijkheid om bestaande netwerkinfrastructuur aanzienlijk langer te gebruiken betekent dat investeringen in glasvezelnetwerken een langere economische levensduur hebben dan eerder werd aangenomen. Dit kan leiden tot meer kosteneffectieve uitrol van hoogwaardige connectiviteit, wat uiteindelijk de digitale kloof kan helpen verkleinen.

Terwijl we kijken naar de toekomst van internetcommunicatie, is het duidelijk dat we nog maar aan het begin staan van wat mogelijk is met optische technologie. De Japanse doorbraak toont aan dat er nog veel onontdekt potentieel ligt in de fundamentele technologieën die ons internet aandrijven, en dat er nog vele innovaties zullen volgen die de grenzen van connectiviteit verder zullen verleggen.



Laat je niet bedriegen! Herken AI-gegenereerde videobeelden

Sinds 2023 zien we een explosieve toename van AI-gegenereerde video's online. Deze zogenaamde 'deepfakes' maken het steeds moeilijker om echt van nep te onderscheiden, wat leidt tot groeiende zorgen over desinformatie en bedrog in onze digitale omgeving.

Willem Bosgra voor [VEILIGDIGITAAL.COM](https://veiligdigitaal.com)

Klassieke herkenningmethoden

Spraakafwijkingen

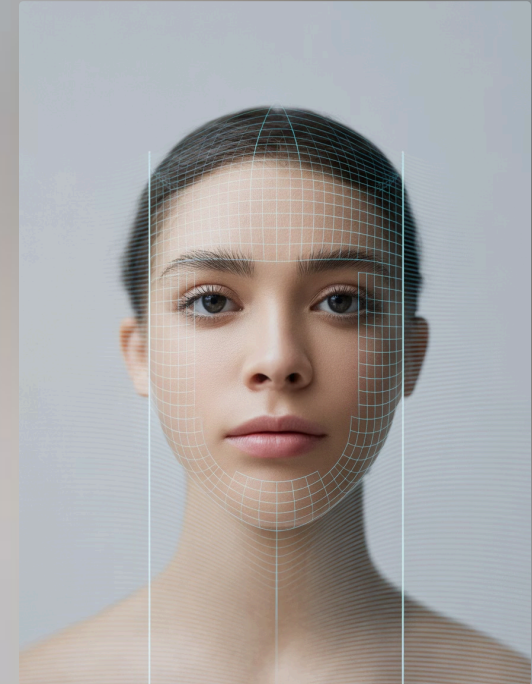
Let op onnatuurlijke stemklank, vreemde intonatie of robotachtige stemovergangen. AI heeft moeite met het perfect nabootsen van menselijke spraakpatronen, waardoor er vaak subtiele onregelmatigheden hoorbaar zijn.

Oogbewegingen

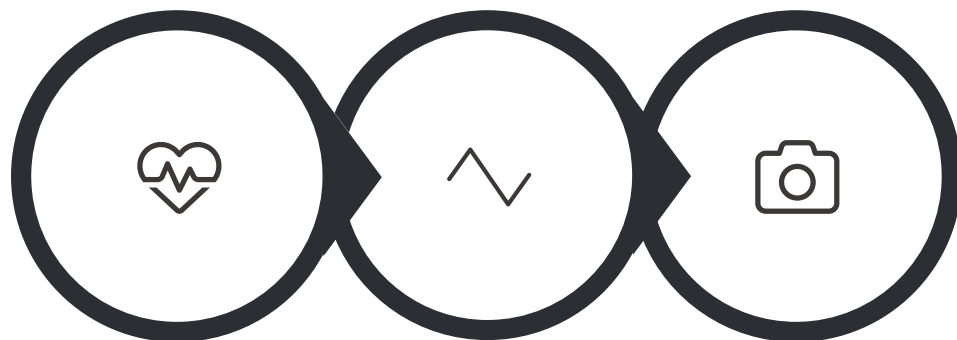
Onregelmatig knipperen of rare oogbewegingen zijn vaak zichtbaar in AI-gegenereerde beelden. Het menselijk oog knippert ongeveer 15-20 keer per minuut, terwijl AI-modellen dit natuurlijke ritme vaak niet correct weergeven.

Beeldvervormingen

Slordig afgewerkte randen of vervormde objecten in beeld zijn belangrijke aanwijzingen. Let vooral op gezichtscontouren, haarlijnen en de overgang tussen personen en achtergrond.



Innovatieve technologieën voor detectie



Hartslagpatroonanalyse

Detecteert
pulssignalen in
video

ENF Analyse

Elektrisch
netwerkfrequentie
patroon

PRNU Kamerafingerprint

Unieke sensorruis
herkenning

Hartslagpatroonanalyse

Onderzoek uit 2025 (nog onafgerond) toont aan dat AI-systemen de subtiele kleurveranderingen in gezichtshuid kunnen detecteren die overeenkomen met de hartslag - een patroon dat deepfakes niet kunnen nabootsen.

Electric Network Frequency (ENF)

Deze techniek analyseert microscopische lichtflikkering in video's, veroorzaakt door stroomnetten. Echte opnames bevatten consistente ENF-patronen die moeilijk te vervalsen zijn.

Photo Response Non Uniformity (PRNU)

Identificeert de unieke 'vingerafdruk' van camerasensoren in beeldmateriaal, waardoor vervalsingen zonder deze signatuur ontmaskerd worden.

Hoe werkt AI bij videoanalyse?



Patroonherkenning

Machine learning-algoritmes worden getraind om specifieke elementen zoals gezichten, teksten en logo's te herkennen. Ze analyseren duizenden datapunten per frame om patronen te identificeren.



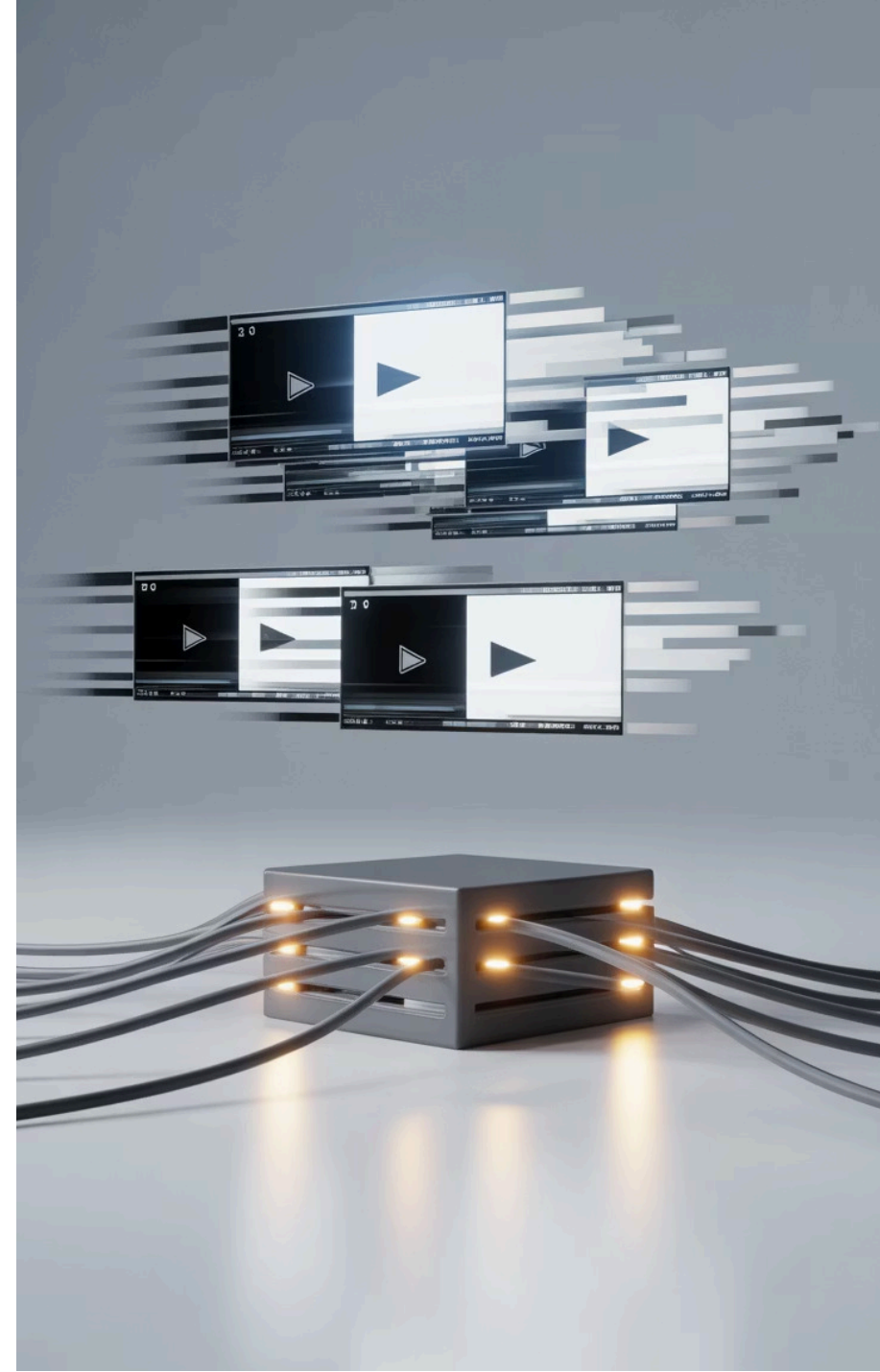
Inhoudsanalyse

AI kan razendsnel expliciete, misleidende of ongepaste inhoud markeren door deze te vergelijken met grote databases van geclassificeerde beelden. Dit helpt bij snelle screening van grote hoeveelheden videomateriaal.



Voortdurende verbetering

Doorlopend getrainde AI-engines verbeteren hun nauwkeurigheid door feedback-loops. Hoe meer voorbeelden ze analyseren, hoe beter ze worden in het herkennen van manipulaties.



Valkuilen bij het herkennen van deepfakes



Steeds betere kwaliteit

Nieuwere deepfakes zijn steeds minder zichtbaar met het blote oog. Geavanceerde AI-modellen leren snel bij en kunnen nu zelfs subtiele gelaatsuitdrukkingen en emoties nabootsen.

Technische beperkingen

Videokwaliteit en compressie bemoeilijken technische analyse. Wanneer video's worden gecomprimeerd voor sociale media, gaan vaak de subtiele aanwijzingen verloren die nodig zijn voor detectie.

Groeiende onzekerheid

Zelfs echte beelden worden soms als nep gezien. Dit 'liar's dividend' effect ondermijnt vertrouwen in alle beeldmateriaal, waardoor ook legitieme content in twijfel wordt getrokken.



Praktische tips voor consumenten

1 Combineer detectiemethoden

Vertrouw niet op één enkele aanpak. Inspecteer zowel het beeld zelf op onregelmatigheden als de audiocomponent. Maak gebruik van beschikbare online tools die speciaal zijn ontwikkeld om deepfakes te herkennen.

2 Verifieer de bron

Controleer altijd de bron en context van video's voordat je ze gelooft of deelt. Betrouwbare nieuwsbronnen verifiëren doorgaans hun materiaal, terwijl sociale media accounts zonder geschiedenis of met verdachte activiteiten meer risico vormen.

3 Behoud kritisch denken

Blijf kritisch en vertrouw niet blind op "realistische" beelden. Als iets te goed lijkt om waar te zijn of sterk afwijkt van bekend gedrag van een persoon, is gezonde scepsis op zijn plaats.

Lancering van ChatEurope: De Europese Nieuwschatbot

In juli 2025 hebben 15 toonaangevende Europese mediaorganisaties de handen ineengeslagen om ChatEurope te lanceren - een baanbrekende chatbot speciaal ontworpen om de strijd aan te gaan met online desinformatie.

Dit innovatieve platform onderscheidt zich door een unieke focus op Europese actualiteiten en volledige transparantie in nieuwsvoorziening.

VEILIGDIGITAAL.COM



Partners en Samenwerking binnen Europa



Internationale Samenwerking

Media-organisaties uit 7 Europese landen, waaronder grote spelers als dpa, Deutsche Welle, AFP en ANSA, bundelen hun journalistieke expertise.



EU-Financiering

Het project wordt gefinancierd door de Europese Unie als onderdeel van hun strategie tegen desinformatie en voor mediageletterdheid.



Media-Tech Alliantie

Unieke samenwerking tussen traditionele mediahuizen en innovatieve technologiebedrijven voor een betrouwbaar nieuwsecosysteem.

Deze gezamenlijke inspanning vertegenwoordigt een ongekennde schaal van Europese nieuwssamenwerking in het digitale tijdperk.

Techniek achter ChatEurope



1

Mistral Taalmodel

De chatbot is gebouwd op het geavanceerde taalmodel van Mistral, een vooraanstaand Frans AI-bedrijf dat bekend staat om zijn precisie en betrouwbaarheid.

2

DRUID AI Ontwikkeling

De technische implementatie komt van het Roemeense DRUID AI, dat expertise brengt in conversationele AI-interfaces.

3

Deutsche Welle Vertaalsysteem

Deutsche Welle levert geavanceerde vertaal- en transcriptietechnologie voor meertalige video-content.

**Protecting truth.
Empowering Europe.**



Protecting truth.
Empowering Europe.



Hoe ChatEurope Desinformatie Bestrijdt



Betrouwbare Bronnen

De AI levert nieuws 'zonder invloed van fake news' door uitsluitend gebruik te maken van geverifieerde berichtgeving van de deelnemende mediaorganisaties.



Bronvermelding

Bij elk antwoord worden de exacte nieuwsbronnen vermeld, waardoor gebruikers altijd kunnen nagaan waar de informatie vandaan komt.



EU-Transparantie

Een belangrijk doel is het transparanter maken van Europese besluitvorming voor burgers, waardoor het democratisch proces versterkt wordt.

Nieuwsplatform & Digitale Kanalen

Geïntegreerde Interface

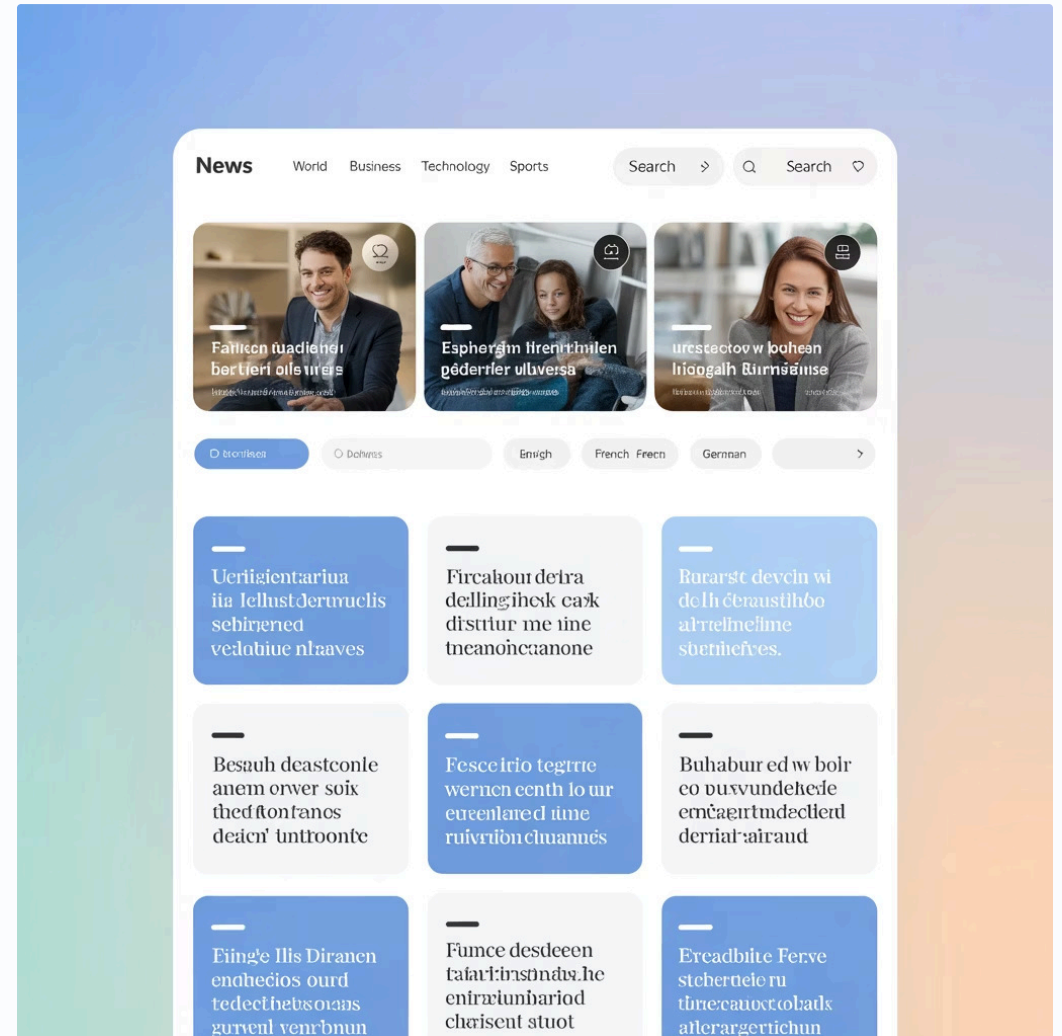
ChatEurope biedt een soepele integratie van chatbot-functionaliteit, actuele newspagina's en sociale media-kanalen in één gebruiksvriendelijk platform.

Meertalige Toegang

Dankzij geavanceerde vertaaltechnologie is het platform toegankelijk in meerdere Europese talen, wat de inclusiviteit vergroot.

Pan-Europees Nieuws

Voor het eerst biedt één platform geïntegreerd nieuws uit alle hoeken van Europa, wat bijdraagt aan een gemeenschappelijke Europese informatieruimte.



Eerste Gebruikerservaringen & Kritiek

⚠ Vroege Uitdagingen

Ondanks de ambitieuze doelstellingen kampt ChatEurope met enkele kinderziektes die kenmerkend zijn voor nieuwe AI-nieuwsplatforms.

Verouderde Informatie

Gebruikers melden dat de chatbot soms verouderde antwoorden geeft over actuele onderwerpen, waardoor de betrouwbaarheid in het geding komt.

1

2

Onvolledige Politieke Berichtgeving

Bij vragen over bijvoorbeeld Duitse politiek blijkt dat ChatEurope niet altijd up-to-date is met de meest recente ontwikkelingen.

Onverwachte Antwoorden

In plaats van recente politieke gebeurtenissen te bespreken, wijdt de chatbot soms uit over minder relevante onderwerpen zoals wolvenbeleid.

3

4

Achterstand op Commerciële Platforms

Vergeleken met gevestigde commerciële AI-platforms toont ChatEurope nog duidelijke tekortkomingen in snelheid en actualiteit.



Uitdagingen en Verbeterpunten

1 Actualiteitsprobleem

Het platform heeft moeite met het snel verwerken en integreren van het allerlaatste nieuws, waardoor er een vertraging ontstaat tussen gebeurtenissen en beschikbare informatie.

2 Kwaliteitsbewaking

De partnerorganisaties hebben een systematisch monitoringsysteem opgezet om de kwaliteit van antwoorden voortdurend te controleren en bij te sturen waar nodig.

3 Technische Ontwikkeling

Er is continue technische ontwikkeling nodig om de balans te vinden tussen betrouwbaarheid en actualiteit, een uitdaging die alle AI-nieuwsplatforms delen.

Toekomstperspectief: Transparant en Betrouwbaar Europees Nieuws

Een Groeiende Alliantie

ChatEurope streeft ernaar uit te groeien tot een Europa-brede alliantie tegen desinformatie, met steeds meer deelnemende nieuwsorganisaties en verbeterde dekking.

Technologische Vooruitgang

Volgens de mediapartners ligt de focus op voortdurende innovatie en het verbeteren van betrouwbaarheid, met regelmatige updates en technologische verbeteringen.

Optimistische Verwachtingen

De verwachting is dat de prestaties van ChatEurope significant zullen verbeteren naarmate de technologie rijpt en de samenwerking tussen partners intensiveert.





Massistant: Chinese mobiele forensische tool heeft toegang tot sms-, afbeeldingen, audio en GPS-gegevens

Massistant, een geavanceerde mobiele forensische tool ontwikkeld door het Chinese bedrijf Xiamen Meiya Pico, wordt sinds 2024 op grote schaal ingezet door de Chinese politie. Deze nieuwe technologie volgt de eerdere forensische tool "MFSocket" op en biedt uitgebreide mogelijkheden voor het verzamelen van persoonlijke gegevens van mobiele apparaten.

VEILIGDIGITAAL.COM

Werking en Installatie van Massistant

De Massistant-technologie maakt gebruik van een speciale hardwaretoren die communiceert met desktopsoftware om gegevens te extraheren. Voor de werking is het essentieel dat de tool handmatig wordt geïnstalleerd op een ontgrendeld apparaat, wat betekent dat fysieke toegang tot het toestel vereist is.

Wanneer geïnstalleerd, kan Massistant op twee manieren worden gedetecteerd:

- Als zichtbare applicatie op het apparaat
- Via Android Debug Bridge voor technisch onderlegde gebruikers



De installatieprocedure vindt meestal plaats tijdens tijdelijke inbeslagnames bij grenscontroles of tijdens politiecontroles, waarbij het apparaat korte tijd uit het zicht van de eigenaar is.

Welke Gegevens Exporteert Massistant?

Communicatiegegevens

Massistant verzamelt alle sms-berichten, contactgegevens en gespreksinformatie. Ook berichten uit versleutelde apps zoals Signal kunnen worden uitgelezen, wat ernstige privacyzorgen oproept.

Mediabestanden

Alle afbeeldingen en audiobestanden op het apparaat zijn toegankelijk voor de tool. Spraakopnames, persoonlijke foto's en gedownloade media worden geëxtraheerd en opgeslagen in de forensische database.

Locatiegegevens

De tool verzamelt uitgebreide GPS-data en locatiegeschiedenis, waardoor een gedetailleerd bewegingsprofiel van de gebruiker kan worden samengesteld over langere perioden.

De verzamelde gegevens worden lokaal opgeslagen in een beveiligde omgeving en kunnen worden gebruikt voor verder onderzoek of surveillance door Chinese autoriteiten.

Juridische en Praktische Context in China

Sinds 2024 is de wetgeving in China zodanig aangepast dat er geen huiszoekingsbevel meer nodig is om mobiele apparaten te doorzoeken. Dit heeft de drempel voor gegevensextractie aanzienlijk verlaagd.

Typische scenario's waarbij Massistent wordt ingezet:

- Grenscontroles bij in- en uitreis van China
- Willekeurige politiecontroles in het openbaar
- Gerichtte controles van specifieke individuen

Tijdens deze controles kunnen apparaten tijdelijk in beslag worden genomen, vaak zonder duidelijke uitleg aan de eigenaar over wat er precies met het apparaat gebeurt.



An illustration of a person's face in profile, looking down at a smartphone. They are holding a magnifying glass over the screen. The phone screen displays 'Security Settings' and 'Potential threat detected' with a red circular warning icon. Below this, there are several settings options, some of which are partially visible and appear to be in a non-Latin script. The background is a soft-focus indoor setting with a window and a plant.

Risico's, Herkenning en Preventie

Aanhoudende Surveillance

Een verontrustend aspect van Massistant is dat de tool soms actief blijft na teruggave van het apparaat, waardoor continue monitoring mogelijk is. Dit creëert een ernstig veiligheidsrisico, vooral voor zakenreizigers en expats.

Detectie en Verwijdering

Voor technisch onderlegde gebruikers zijn sporen van de tool zichtbaar in het systeem. Hoewel verwijdering mogelijk is, zijn de gegevens op het moment van installatie al geëxporteerd, waardoor preventieve maatregelen essentieel zijn.

Beschermingsmaatregelen

Overweeg het gebruik van een "burner phone" voor reizen naar China, of zorg voor een fabrieksreset voor en na grensovergangen. Vermijd het opslaan van gevoelige informatie op apparaten die mogelijk geïnspecteerd kunnen worden.

Matanbuchus 3.0: Een Ernstige Malwarebedreiging via Microsoft Teams

Een nieuwe, geavanceerde malwarebedreiging genaamd Matanbuchus 3.0 is sinds juli 2025 actief in het cyberlandschap. Deze malware wordt specifiek verspreid via Microsoft Teams en richt zich op strategisch geselecteerde zakelijke doelwitten.

Toonaangevende cyberbeveiligingsbedrijven zoals Morphisec hebben waarschuwingen uitgebracht over deze ernstige dreiging die gebruik maakt van de vertrouwde Teams-omgeving om systemen te infiltreren.

VEILIGDIGITAAL.COM



Aanvalsmethode: Social Engineering via Teams



Contact via Teams

Aanvallers doen zich voor als medewerkers van de IT-helpdesk en benaderen slachtoffers via Microsoft Teams-gesprekken, waarbij ze vertrouwen opbouwen door het gebruik van bedrijfsjargon en interne procedures.



Quick Assist Activatie

Slachtoffers worden overtuigd om Microsoft Quick Assist te activeren, een legitiem hulpprogramma dat externe toegang tot het systeem mogelijk maakt onder het voorwendsel van "technische ondersteuning".



Malware Installatie

Zodra toegang is verkregen, voeren aanvallers verborgen PowerShell-commando's uit om Matanbuchus 3.0 te installeren, terwijl ze tegelijkertijd schijnbaar legitieme ondersteuning bieden aan het slachtoffer.

Deze aanvalsmethode is bijzonder verraderlijk omdat de aanvallers legitieme IT-hulpmiddelen misbruiken in een real-time interactie, waardoor het voor slachtoffers moeilijk is om de aanval te herkennen.

Technische Werking van Matanbuchus 3.0

Matanbuchus 3.0 functioneert als een geavanceerde loader die ransomware en andere hacktools zoals Cobalt Strike kan installeren, waardoor aanvallers uitgebreide controle over geïnfecteerde systemen verkrijgen.

Initiële Infectie

Verspreid via aangepaste Notepad++ updater en kwaadaardige DLL-bestanden die legitieme software nabootsen

Informatie Verzameling

Onderschept systeeminformatie en controleert op aanwezigheid van beveiligingssoftware

Command & Control

Maakt verbinding met C2-servers voor het ontvangen van extra payloads en instructies



Gevolgen en Risico's voor Organisaties

1

Dataverlies en Afpersing

Matanbuchus maakt volledige bestandsversleuteling mogelijk, waarbij kritieke bedrijfsgegevens ontoegankelijk worden gemaakt en vaak gecombineerd wordt met datadiefstal voor dubbele afpersing.

2

Langdurige Infiltratie

De malware installeert geplande taken en zijladingen in DLL-bestanden die traditionele detectiemethoden omzeilen, waardoor aanvallers langdurig toegang behouden tot gecompromitteerde systemen.

3

Financiële Impact

Naast directe kosten van losgeld (Matanbuchus wordt op darkwebmarktplaatsen aangeboden vanaf €10.000 per maand), ontstaan er aanzienlijke kosten voor herstelwerkzaamheden, downtime en reputatieschade.

Bescherming en Aanbevelingen

Technische Maatregelen

- Schakel Microsoft Quick Assist uit of beperk het gebruik tot geautoriseerde beheerders
- Implementeer uitgebreide monitoring van PowerShell-activiteiten en stel restrictieve uitvoeringsbeleid in
- Gebruik geavanceerde endpoint protection met gedragsgebaseerde detectie
- Voer regelmatig updates uit van alle bedrijfssoftware en -systemen

Organisatorische Maatregelen

- Train medewerkers in het herkennen van social engineering tactieken, specifiek via Teams
- Ontwikkel duidelijke protocollen voor IT-ondersteuning en externe toegang tot systemen
- Creëer een veilige meldingsprocedure voor verdachte IT-verzoeken
- Implementeer een "zero trust" beveiligingsmodel voor toegang tot kritieke systemen



Microsoft Quick Machine Recovery: Introductie

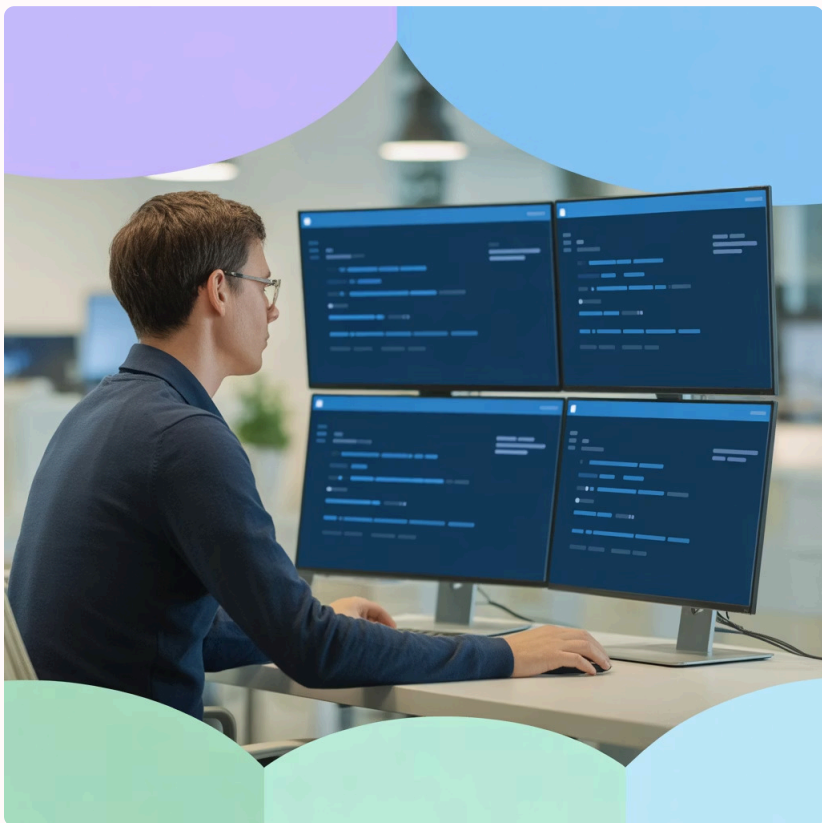
Microsoft's nieuwe "Quick Machine Recovery" technologie belooft een revolutie in het automatisch herstellen van Windows 11-systemen bij kritieke fouten. Deze innovatie, voor het eerst aangekondigd tijdens Microsoft Ignite 2024, is ontworpen om langdurige systeemuitletval te voorkomen wanneer er ernstige problemen optreden.

Na succesvolle implementatie in bedrijfsomgevingen is deze functionaliteit nu beschikbaar gemaakt in de Windows Insider Beta Channel, wat een belangrijke stap markeert richting de algemene beschikbaarheid voor consumenten wereldwijd.

VEILIGDIGITAAL.COM



Testen in de Ondernemingsomgeving



Microsoft heeft "Quick Machine Recovery" uitgebreid getest in diverse bedrijfsomgevingen wereldwijd voordat het naar de consumentenmarkt komt. Deze tests waren cruciaal om de betrouwbaarheid en effectiviteit van de technologie te waarborgen.

IT-beheerders kregen volledige controle over het inschakelen en uitbreiden van de functies, waardoor ze konden bepalen hoe en wanneer de technologie werd toegepast binnen hun organisatie. Dit omvatte mogelijkheden voor:

- Simulatie via een speciale 'test modus'
- Vooraf configureren van netwerkinstellingen
- Aangepaste implementatiestrategieën

De feedback uit deze bedrijfsomgevingen was overwegend positief, met name over de aanzienlijke tijdsbesparing bij het herstellen van systemen tijdens grootschalige storingen, wat de weg vrijmaakte voor de consumentenversie.

Werking van Quick Machine Recovery

Detectie

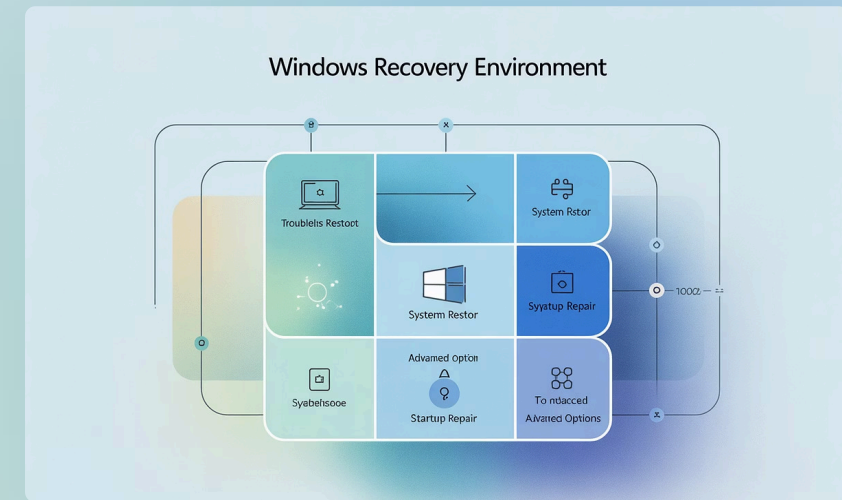
Het systeem detecteert automatisch ernstige opstartproblemen die normaal gesproken handmatige interventie zouden vereisen. Deze scanfunctie draait op instelbare intervallen, met een aanbevolen frequentie van elke 30 minuten.

Diagnose

Na detectie rapporteert het systeem het probleem en bepaalt de beste oplossing via Windows Recovery Environment (RE), een speciale herstelomgeving die onafhankelijk van het hoofdsysteem kan draaien.

Oplossing

Het systeem maakt verbinding met Windows Update om gerichte oplossingen te downloaden en toe te passen, zonder tussenkomst van de gebruiker. Het herstelproces heeft een instelbare tijdslimiet, met een aanbevolen maximum van 72 uur.



Introductie voor Consumenten

Windows Insider Preview

De functie is momenteel beschikbaar in de Insider Preview voor Windows 11 24H2, waar vroege gebruikers de technologie kunnen testen en feedback kunnen geven.

1

2

Windows 11 Home

Na de testfase wordt Quick Machine Recovery standaard geactiveerd op alle Windows 11 Home-apparaten voor consumenten, zonder dat configuratie nodig is.

Bredere uitrol

Een uitrol naar een grotere gebruikersgroep volgt na succesvolle tests. Microsoft zal de implementatie gefaseerd uitvoeren om eventuele problemen vroeg te identificeren.

3

4

Pro en Enterprise-apparaten

Voor zakelijke gebruikers behouden IT-beheerders volledige controle over de implementatie op Pro en Enterprise-apparaten, met uitgebreide configuratieopties.

Deze gestructureerde uitrolstrategie zorgt ervoor dat Microsoft de functionaliteit kan verfijnen voordat het beschikbaar komt voor alle Windows 11-gebruikers.

Voordelen voor Consumenten



De introductie van Quick Machine Recovery brengt tal van voordelen met zich mee voor de dagelijkse Windows-gebruiker, die nu minder technische kennis nodig heeft om computerproblemen op te lossen.

Minder handmatige herstellingen

Het aantal situaties waarin gebruikers zelf hun systeem moeten herstellen of technische ondersteuning moeten inschakelen wordt drastisch verminderd.

Minimale werkonderbreking

Sneller herstel na fouten betekent minder tijd waarin gebruikers niet kunnen werken of hun computer kunnen gebruiken.

Verhoogde betrouwbaarheid

Windows-systemen worden betrouwbaarder door het proactief oplossen van problemen voordat ze ernstige gevolgen hebben.

Zorgeloze ervaring

Gebruikers worden ontzorgd, zelfs bij grootschalige uitval of technische problemen die normaal gesproken expertise vereisen.

Microsoft test: Copilot AI krijgt volledige desктоptoegang

In juli 2025 begint Microsoft met het testen van een baanbrekende nieuwe functionaliteit voor hun Copilot AI-assistent: "Desktop Share". Deze innovatie geeft de AI-assistent voor het eerst de mogelijkheid om de volledige desktop en alle geopende programma's te observeren en te analyseren.

Dit markeert een significante uitbreiding van Copilot's mogelijkheden, die voorheen beperkt was tot interactie met individuele applicaties of vensters.

VEILIGDIGITAAL.COM

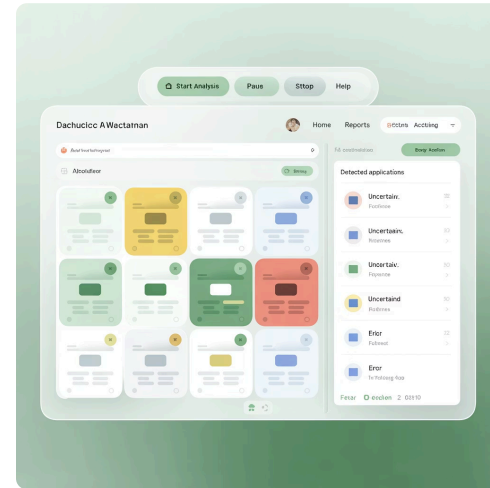
Copilot



Wat is Copilot Desktop Share?

"Vision Desktop Share" is een geavanceerde functie die Copilot in staat stelt om je volledige Windows-bureaublad te observeren en te interpreteren. In tegenstelling tot eerdere versies heeft de AI nu toegang tot alle actieve processen en open content op je desktop, inclusief meerdere vensters, documenten en applicaties tegelijkertijd.

Deze uitgebreide waarnemingscapaciteit stelt Copilot in staat om realtime inzichten te bieden, contextgebonden analyses uit te voeren en complexere vragen te beantwoorden op basis van wat er op je scherm gebeurt, zonder dat je specifieke schermafbeeldingen hoeft te delen.



Met Desktop Share kan Copilot verbanden leggen tussen verschillende geopende applicaties en de gebruiker voorzien van geïntegreerde hulp die voorheen niet mogelijk was.

Gebruikerscontrole en Opties



Standaard Uitgeschakeld

De Desktop Share-functie is standaard uitgeschakeld en werkt uitsluitend op basis van expliciete toestemming van de gebruiker. Activering gebeurt via het bril-icoon in de Copilot-composer.



Flexibele Deelkeuzes

Gebruikers hebben volledige controle over wat ze delen en kunnen kiezen tussen het delen van het volledige bureaublad of alleen specifieke vensters en applicaties.



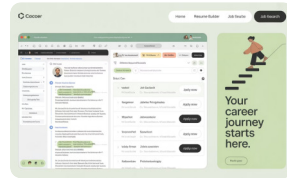
Direct Stoppen

Het delen kan op elk moment worden beëindigd door op de "Stop" of "X" knop in de Copilot-composer te klikken, waardoor de AI direct geen toegang meer heeft tot de scherm inhoud.

Deze controlemaatregelen zijn ontworpen om gebruikers volledige zeggenschap te geven over wanneer en wat Copilot kan waarnemen.

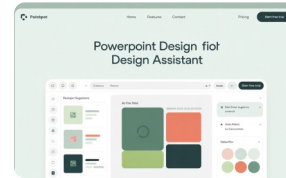


Praktische Toepassingen



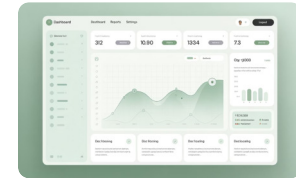
Documentverbetering

Copilot kan je CV in Word herschrijven en optimaliseren terwijl het tegelijkertijd vacature-eisen uit je browser kan analyseren om relevante aanpassingen voor te stellen.



Ontwerpbegeleiding

Bij het werken in PowerPoint of Photoshop kan Copilot realtime tips en correcties geven over layout, kleurgebruik en compositie gebaseerd op professionele ontwerpprincipes.



Software Navigatie

Directe uitleg bij onbekende games of complexe instellingsmenu's zonder dat je specifieke vragen hoeft te stellen of schermafbeeldingen moet delen.

Privacy en Ethische Vragen

Privacyrisico's

Volledige desktoptoegang vergroot de kans dat gevoelige informatie zoals bankgegevens, persoonlijke berichten of vertrouwelijke documenten zichtbaar worden voor de AI.

Gebruikerscontrole

Microsoft benadrukt dat de AI alleen kijkt wanneer de gebruiker actief toestemming geeft en alleen ziet wat bewust wordt gedeeld.

Databescherming

Vragen blijven over hoe Microsoft omgaat met de verzamelde gegevens en wie toegang heeft tot de informatie die Copilot verwerkt.





Conclusie & Impact

Vergaande Integratie

De nieuwe Desktop Share-functionaliteit vertegenwoordigt een significante stap in de integratie van AI in de Windows-omgeving en verandert fundamenteel hoe gebruikers met hun computers kunnen werken.

Gebruikersvertrouwen Cruciaal

Het succes van deze krachtige functie zal grotendeels afhangen van het vertrouwen dat gebruikers hebben in Microsoft's omgang met hun gegevens en de waargenomen meerwaarde in dagelijks gebruik.

Toekomstperspectief

De toekomst van AI-assistenten zoals Copilot hangt af van het vinden van de juiste balans tussen geavanceerde functionaliteit en robuuste privacybescherming. Microsoft's aanpak zal waarschijnlijk de standaard zetten voor de hele industrie.

Microsoft verlengt gratis Windows 10-updates tot oktober 2026

Microsoft heeft aangekondigd dat Windows 10-gebruikers nog een jaar langer gratis beveiligingsupdates kunnen ontvangen, mits zij hun PC synchroniseren met de cloud. Deze onverwachte verlenging biedt meer dan 500 miljoen gebruikers extra tijd voordat zij moeten overstappen naar Windows 11.

VEILIGDIGITAAL.COM



Het probleem: Eindigende Windows 10-ondersteuning

Huidige situatie

- Officiële ondersteuning stopt op 14 oktober 2025
- Meer dan 53% van alle Windows-gebruikers werkt nog met Windows 10
- Wereldwijd draaien ruim 500 miljoen apparaten op dit besturingssysteem

Risico's zonder updates

- Verhoogde kwetsbaarheid voor cyberaanvallen
- Nieuwe beveiligingslekken worden niet meer gedicht
- Compatibiliteitsproblemen met nieuwere software



Nieuwe aanbieding: Gratis Extended Security Updates (ESU)

Oorspronkelijk plan

Microsoft zou na oktober 2025 betaalde ESU aanbieden voor €30 per jaar of via 1.000 Microsoft Rewards-punten

Nieuwe regeling

Gratis Extended Security Updates tot 13 oktober 2026 voor particuliere gebruikers die voldoen aan de cloud-synchronisatie voorwaarde

Voor bedrijven

Commerciële gebruikers moeten nog steeds betalen voor de ESU-dienst; deze aanbieding geldt alleen voor consumenten



Voorwaarde: Synchroniseer je PC met de cloud



Microsoft-account

Log in met je Microsoft-account op je Windows 10-apparaat om toegang te krijgen tot de Windows Backup-functie



Windows Backup

Activeer deze nieuwe app om PC-instellingen, documenten, applicaties en foto's automatisch te back-uppen naar de cloud



OneDrive-opslag

Standaard krijg je 5GB gratis opslag; voor meer ruimte betaal je vanaf €1,99/maand voor 100GB extra

Praktische uitleg en aandachtspunten

Tijdslijn

- Juli 2025: Introductie nieuwe Windows Backup-app
- Augustus 2025: Volledige uitrol naar alle gebruikers
- 14 oktober 2025: Einde reguliere Windows 10-ondersteuning
- 13 oktober 2026: Einde gratis ESU-programma

Aandachtspunten

- Notificaties verschijnen automatisch in je Windows 10-instellingen
- Back-ups kunnen meer dan 5GB ruimte vereisen
- Bij onvoldoende ruimte: overweeg OneDrive-upgrade
- Bedrijven moeten alsnog betalen voor ESU

Conclusie: Veilig op Windows 10 tot oktober 2026

1 Extra tijd voor overstap

Honderden miljoenen gebruikers krijgen een extra jaar om in alle rust te beslissen over een upgrade naar Windows 11 of de aanschaf van nieuwe hardware

2 Microsoft's strategie

Door cloud-synchronisatie als voorwaarde te stellen, stimuleert Microsoft het gebruik van hun clouddiensten en verzamelt waardevolle gebruikersdata

3 Overwegingen voor gebruikers

Bepaal of je comfortabel bent met cloud-synchronisatie van je gegevens of dat je liever upgradet naar Windows 11 of overstapt naar een alternatief



Microsoft verwijdt uw wachtwoorden op 1 augustus. Dit is wat u nu moet doen

Microsoft maakt een drastische verandering in zijn beveiligingsstrategie: vanaf 1 augustus 2025 zullen wachtwoorden niet langer beschikbaar zijn in de Microsoft Authenticator app. Deze wijziging treft meer dan 75 miljoen gebruikers wereldwijd die momenteel vertrouwen op deze app voor hun wachtwoordbeheer. Bent u een van hen? Dan is het tijd om actie te ondernemen.

VEILIGDIGITAAL.COM



Tijdslijn van de veranderingen

1 juni 2025

1

Geen nieuwe wachtwoorden meer toevoegen of importeren in Microsoft Authenticator. De eerste fase waarin functionaliteit wordt beperkt.

2

Juli 2025

De autofill-functie voor wachtwoorden werkt niet meer. U kunt opgeslagen wachtwoorden niet meer automatisch laten invullen in apps en websites.

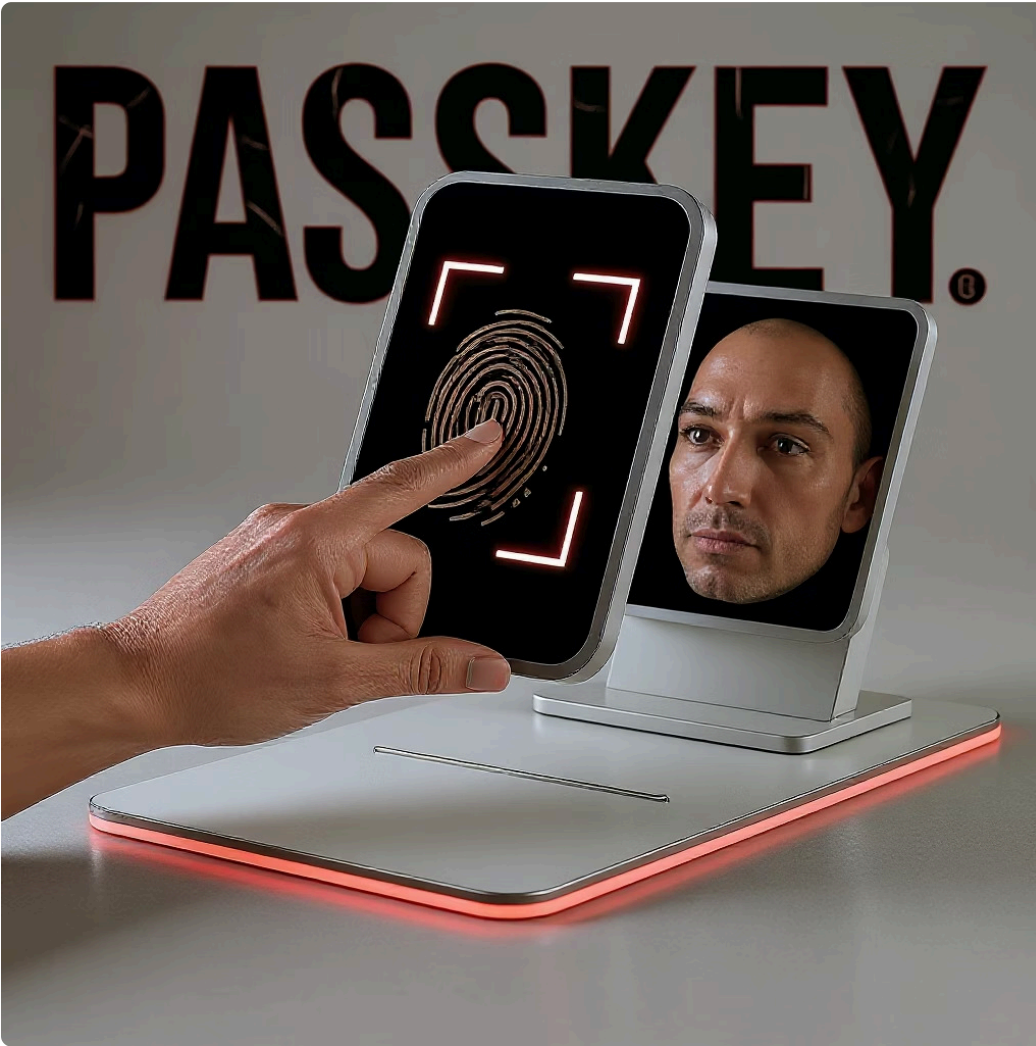
Augustus 2025

3

Alle opgeslagen wachtwoorden zijn niet meer toegankelijk in de Authenticator app. Dit markeert het definitieve einde van de wachtwoordbeheerfunctie.

Het is belangrijk deze datums in de gaten te houden en tijdig actie te ondernemen om verlies van toegang tot uw accounts te voorkomen.

Waarom deze verandering?



Microsoft werkt aan een toekomst waarin traditionele wachtwoorden vervangen worden door veiligere alternatieven.

Verschuiving naar passkeys

Microsoft zet in op wachtwoordloze technologieën zoals passkeys, die veel veiliger zijn dan traditionele wachtwoorden.

Minder beveiligingsrisico's

Paskeys verminderen het risico op phishing-aanvallen en elimineren problemen met hergebruikte wachtwoorden.

Centralisatie naar Edge

Microsoft wil wachtwoordbeheer centraliseren in de Edge-browser voor een betere gebruikerservaring en veiligheid.



Wat betekent dit voor gebruikers?

Einde van een functie

Vanaf augustus 2025 kunt u Microsoft Authenticator niet meer gebruiken als wachtwoordmanager voor het opslaan en beheren van uw inloggegevens.

Synchronisatie met Microsoft-account

Uw opgeslagen wachtwoorden worden automatisch gesynchroniseerd met uw Microsoft-account en blijven toegankelijk via de Edge-browser.

Gegevensverlies

Niet opgeslagen gegenereerde wachtwoorden en betaalgegevens worden permanent verwijderd en kunnen niet worden hersteld na de overgangsdatum.

Wat moet u nu doen?



Wachtwoorden overzetten

Zorg ervoor dat al uw wachtwoorden worden overgezet naar Microsoft Edge vóór augustus 2025. Controleer of synchronisatie is ingeschakeld met uw Microsoft-account.



Controle uitvoeren

Verifieer of alle belangrijke wachtwoorden en inloggegevens correct gesynchroniseerd zijn en toegankelijk blijven via Edge of uw Microsoft-account.



Overstappen op passkeys

Overweeg waar mogelijk over te stappen op passkeys of andere moderne authenticatiemethoden die veiliger zijn dan traditionele wachtwoorden.



Handmatig opslaan

Sla gegenereerde wachtwoorden die nog niet zijn opgeslagen tijdig handmatig op om te voorkomen dat u toegang verliest.

Samenvatting & Directe Actie

Belangrijke deadlines

1 juni 2025: Geen nieuwe wachtwoorden meer toevoegen

Juli 2025: Autofill stopt

1 augustus 2025: Volledige verwijdering wachtwoorden

Authenticator blijft bestaan voor tweefactorauthenticatie, maar verliest de wachtwoordbeheerfunctie. Plan uw migratie nu om problemen te voorkomen.

Aanbevolen alternatieve oplossingen:

- Microsoft Edge wachtwoordbeheer
- Overstap naar passkeys waar mogelijk
- Andere wachtwoordmanagers zoals LastPass, 1Password of Bitwarden

Neem de tijd om uw digitale beveiliging te herzien en te verbeteren tijdens deze overgangsperiode. Deze verandering biedt een kans om uw online beveiliging te moderniseren.



Microsoft zal het vergrendelingsscherm van Windows 11 gebruiken om widgets aan te bevelen

Microsoft introduceert een nieuwe strategische zet om widgets een prominentere plaats te geven in de Windows 11-ervaring. Via het vergrendelingsscherm zullen gebruikers binnenkort aanbevelingen voor widgets ontvangen, beginnend met 'Weather and more'-widgets in Windows 11 Build 26252.

Deze verandering markeert een belangrijke verschuiving in hoe Microsoft gebruikers wil betrekken bij de dynamische content-mogelijkheden van het besturingssysteem.

door **VEILIGDIGITAAL.COM**

Wat zijn Windows 11 Widgets?

Widgets in Windows 11 zijn interactieve informatiekaarten die realtime updates en content tonen. Ze bieden een snelle blik op belangrijke informatie zonder dat je applicaties hoeft te openen. Oorspronkelijk waren deze widgets alleen toegankelijk via de taakbalk, maar Microsoft breidt hun aanwezigheid nu uit naar het vergrendelingsscherm.

Deze dynamische elementen kunnen informatie tonen zoals:

- Actuele weersverwachtingen voor je locatie
- Recente nieuwskoppen van geselecteerde bronnen
- Aandelenkoersen en financiële updates
- Sportscores en aankomende wedstrijden
- Agenda-afspraken en herinneringen



Het widgetpaneel in Windows 11 toont verschillende informatiekaarten die kunnen worden aangepast aan de voorkeuren van de gebruiker.

Nieuwe Strategie: Widgets op het Vergrendelingsscherm



Verbeterde Zichtbaarheid

Microsoft test widgets die direct zichtbaar zijn op het vergrendelingsscherm, waardoor gebruikers informatie kunnen zien voordat ze zich aanmelden.



Weerinformatie Voorop

De eerste uitrol focust op weerwidgets, die actuele temperatuur en weersomstandigheden tonen op het vergrendelingsscherm.



Persoonlijke Aanbevelingen

Het systeem zal geleidelijk meer gepersonaliseerde widgets aanbevelen op basis van gebruikersgedrag en voorkeuren.

Deze nieuwe benadering is onderdeel van Microsofts bredere strategie om de gebruikersbetrokkenheid te verhogen door relevante informatie direct beschikbaar te maken. Door widgets prominenter te plaatsen, hoopt Microsoft dat gebruikers deze functionaliteit vaker zullen benutten.

Voordelen en Nadelen voor Gebruikers

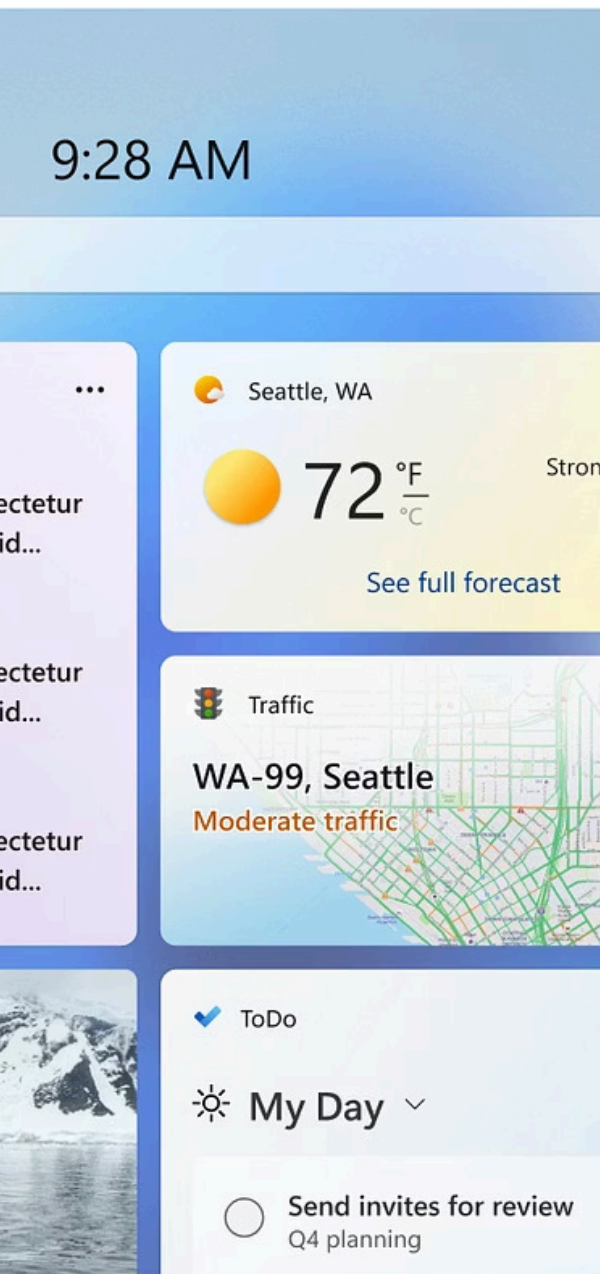
Voordelen

- Directe toegang tot actuele informatie bij het ontgrendelen
- Relevante updates zonder apps te openen
- Tijdbesparend voor frequent gecontroleerde info zoals weer
- Visueel aantrekkelijke presentatie van belangrijke gegevens
- Gepersonaliseerde content afgestemd op gebruikersvoorkeuren

De reacties van gebruikers zijn gemengd: sommigen waarderen de toegankelijkheid van informatie, terwijl anderen zich zorgen maken over de toenemende commercialisering van het vergrendelingsscherm.

Nadelen

- Potentiële afleiding bij het inloggen
- Zorgen over privacy en gegevensverzameling
- Meer reclame-achtige content op het vergrendelingsscherm
- Mogelijk vertraagde systeemprestaties
- Sommige gebruikers ervaren widgets als opdringerig en storend



Widgets op het Vergrendelingsscherm Beheren of Uitschakelen

Open Instellingen

Druk op de toetsencombinatie [Windows] + [I] om het instellingenmenu te openen.

Navigeer naar Vergrendelingsscherm

Ga naar 'Persoonlijke instellingen' en klik vervolgens op 'Vergrendelingsscherm' in het linkermenu.

Widgets Uitschakelen

Zoek de optie voor widgets of 'Weer en meer' en zet deze op 'Geen' of 'Uit'. Schakel ook de optie voor 'Extra tips op het vergrendelingsscherm weergeven' uit voor een volledig schone ervaring.

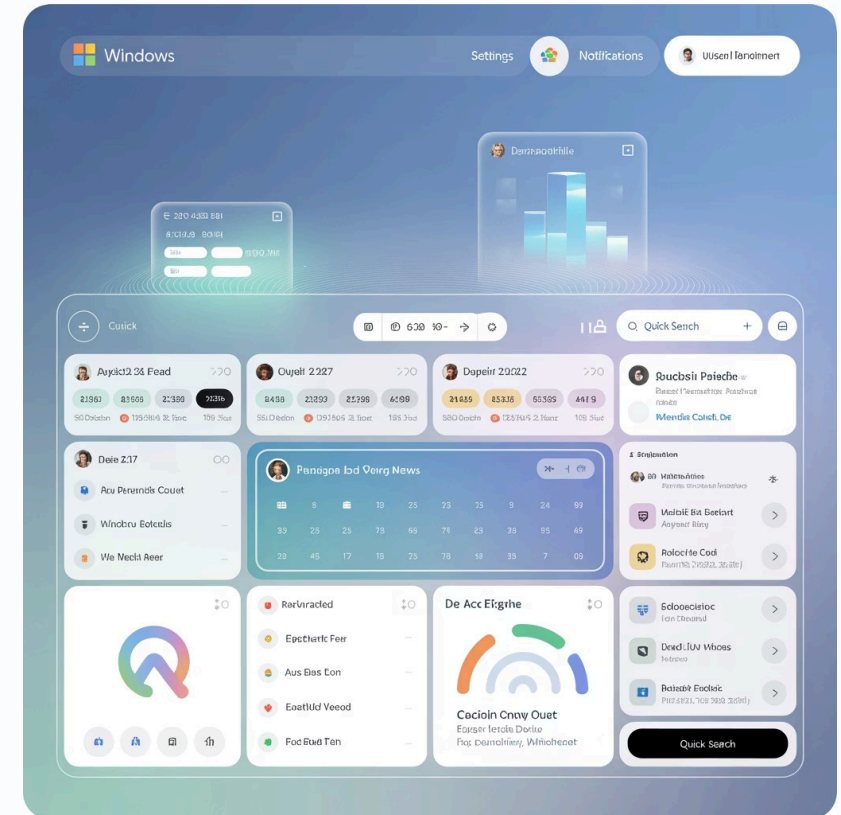
Voor gebruikers die liever een minimalistisch vergrendelingsscherm hebben, biedt Windows 11 gelukkig eenvoudige opties om de nieuwe widgetfunctionaliteit volledig naar wens aan te passen of uit te schakelen.

Conclusie & Vooruitblik

Microsoft's strategie om widgets naar het vergrendelingsscherm te brengen weerspiegelt hun bredere visie voor Windows 11: een meer gepersonaliseerde, content-rijke gebruikerservaring. Hoewel deze functie voor sommigen waardevol zal zijn, blijft het belangrijk dat Microsoft de controle bij de gebruiker laat en duidelijke opties biedt om deze functies aan te passen.

In toekomstige updates kunnen we verwachten:

- Meer gepersonaliseerde widgetaanbevelingen op basis van gebruikersgedrag
- Verbeterde integratie met Microsoft 365-diensten en -applicaties
- Uitgebreidere beheeropties voor de gebruiker
- Betere prestatie-optimalisatie om systemen niet te vertragen



De toekomst van Windows widgets zou nog meer gepersonaliseerde en interactieve ervaringen kunnen bieden, mogelijk met AI-verbeteringen.

Nederland moet weerbaar zijn in een onzekere wereld

De Nederlandse inlichtingendiensten waarschuwen voor toenemende dreigingen in een wereld die steeds onzekerder en onvoorspelbaarder wordt. Dit document behandelt de belangrijkste conclusies uit het Dreigingsbeeld Statelijke Actoren 2025 en belicht de groeiende risico's op het gebied van sabotage, spionage en digitale aanvallen.

We analyseren de verschuivende internationale machtsbalans en de concrete bedreigingen voor Nederland, om vervolgens in te gaan op de noodzakelijke maatregelen om de nationale weerbaarheid te versterken.

VEILIGDIGITAAL.COM

Samenvatting en actualiteit

Het Dreigingsbeeld Statelijke Actoren 2025 dat door de Nederlandse veiligheidsdiensten is gepresenteerd, schetst een zorgwekkend beeld van de huidige veiligheidssituatie. De AIVD, MIVD en NCTV waarschuwen gezamenlijk dat de internationale machtsbalans in hoog tempo verandert, wat leidt tot een wereld gekenmerkt door onvoorspelbaarheid en onzekerheid. Dit heeft directe implicaties voor de Nederlandse nationale veiligheid.

"De wereld bevindt zich in een fase van drastische transformatie, waarbij traditionele machtsverhoudingen onder druk staan en nieuwe dreigingen zich in hoog tempo manifesteren."

De veiligheidsdiensten zijn buitengewoon expliciet in hun waarschuwingen. Ze signaleren een verontrustende toename van sabotageactiviteiten en spionagedreigingen die direct gericht zijn tegen Nederlandse belangen. Deze dreigingen komen niet alleen uit de gebruikelijke hoek van statelijke actoren, maar worden steeds vaker uitgevoerd door zogenaamde proxy-actoren - groeperingen die handelen in opdracht van buitenlandse mogendheden zonder dat daar een directe verbinding mee te leggen is.

Verschuivende machtsbalans

De internationale machtsverhoudingen zijn fundamenteel aan het veranderen, met opkomende grootmachten die de geopolitieke status quo uitdagen en nieuwe invloedssferen creëren.

Toenemende onvoorspelbaarheid

Conflicten en spanningen tussen staten worden steeds minder voorspelbaar, wat leidt tot een verhoogd risico op misrekeningen en onbedoelde escalaties.

Concrete dreigingen

De inlichtingendiensten zien tastbare bewijzen van toenemende sabotage- en spionageactiviteiten gericht tegen Nederland en andere Europese landen.

Het rapport onderstreept dat deze ontwikkelingen niet theoretisch of toekomstig zijn, maar reeds plaatsvinden. De Nederlandse samenleving wordt nu al geconfronteerd met concrete pogingen tot beïnvloeding, digitale aanvallen en andere activiteiten die de nationale veiligheid ondermijnen. Deze situatie vereist volgens de diensten een verhoogde waakzaamheid en een grondige herbeoordeling van de huidige veiligheidsmaatregelen.

Nieuwe dreigingen en mondiale ontwikkelingen

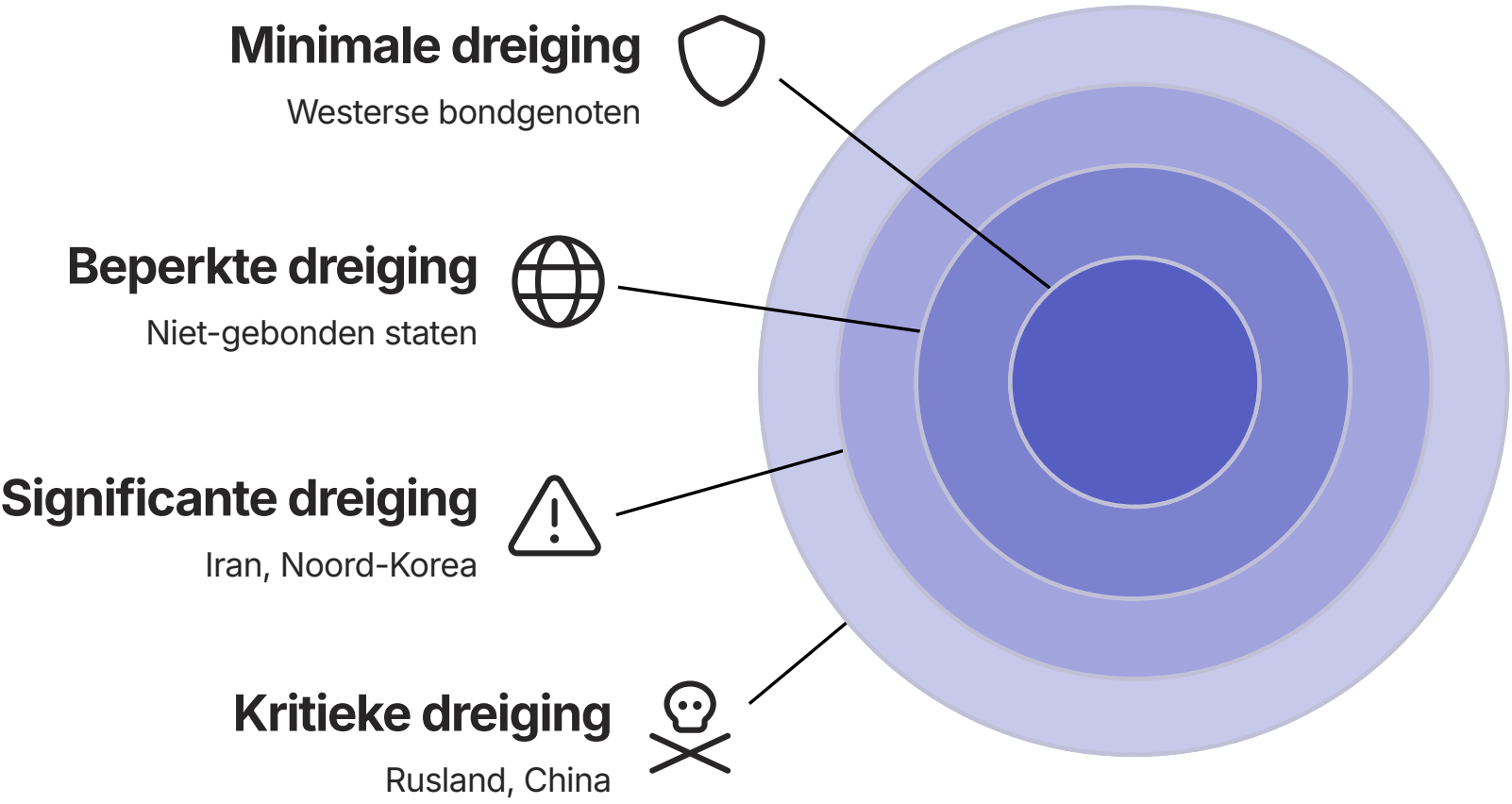
De veiligheidssituatie wordt gekenmerkt door een breder scala aan dreigingen dan voorheen. De inlichtingendiensten signaleren een significante toename van sabotagerisico's door Russische en pro-Russische actoren. Deze manifesteren zich onder meer in de vorm van DDoS-aanvallen, waarbij websites en digitale diensten tijdelijk onbereikbaar worden gemaakt door een overvloed aan nepverkeer. Dergelijke aanvallen zijn relatief eenvoudig uit te voeren maar kunnen aanzienlijke economische schade veroorzaken en maatschappelijke onrust teweegbrengen.

Naast Rusland vormen ook China en Iran in toenemende mate een bedreiging voor de Nederlandse veiligheid. Deze landen richten zich vooral op spionageactiviteiten met als doel het vergaren van geavanceerde kennis en technologie. Deze informatie wordt vervolgens gebruikt om hun eigen militaire en economische positie te versterken, vaak ten koste van Nederlandse en Europese belangen.



Een visualisatie van een DDoS-aanval, waarbij grote hoeveelheden dataverkeer worden gebruikt om digitale diensten te overspoelen en onbereikbaar te maken.

Ondanks de toegenomen spanningen achten de inlichtingendiensten een directe militaire aanval van Rusland op NAVO-grondgebied onwaarschijnlijk. Dit komt mede door de afschrikkende werking van het NAVO-bondgenootschap. Echter, indirecte en hybride dreigingen nemen wel toe, waarbij de grens tussen oorlog en vrede steeds verder vervaagt.



Een zorgwekkende ontwikkeling is de mogelijke afname van Amerikaanse steun aan Europese NAVO-landen. Door de verschuivende machtsverhoudingen en de toenemende focus van de Verenigde Staten op de Indo-Pacific regio, bestaat het risico dat Europa in toenemende mate voor zijn eigen veiligheid moet zorgen. Dit zou een fundamentele heroriëntatie van het Europese veiligheidsbeleid kunnen vereisen.

Statelijke actor	Primaire dreigingsvorm	Belangrijkste doelwitten
Rusland	Sabotage, desinformatie	Kritieke infrastructuur, politieke besluitvorming
China	Spionage, economische beïnvloeding	Hoogtechnologische bedrijven, academische instellingen
Iran	Spionage, beïnvloeding diaspora	Defensie-industrie, Iraanse oppositie in Nederland

De complexiteit van deze dreigingen wordt versterkt door het feit dat ze vaak verborgen blijven en moeilijk zijn toe te schrijven aan specifieke actoren. Dit bemoeilijkt een effectieve respons en vergroot de kwetsbaarheid van de Nederlandse samenleving. De inlichtingendiensten benadrukken daarom het belang van verhoogde waakzaamheid en investeringen in detectie- en responscapaciteiten.

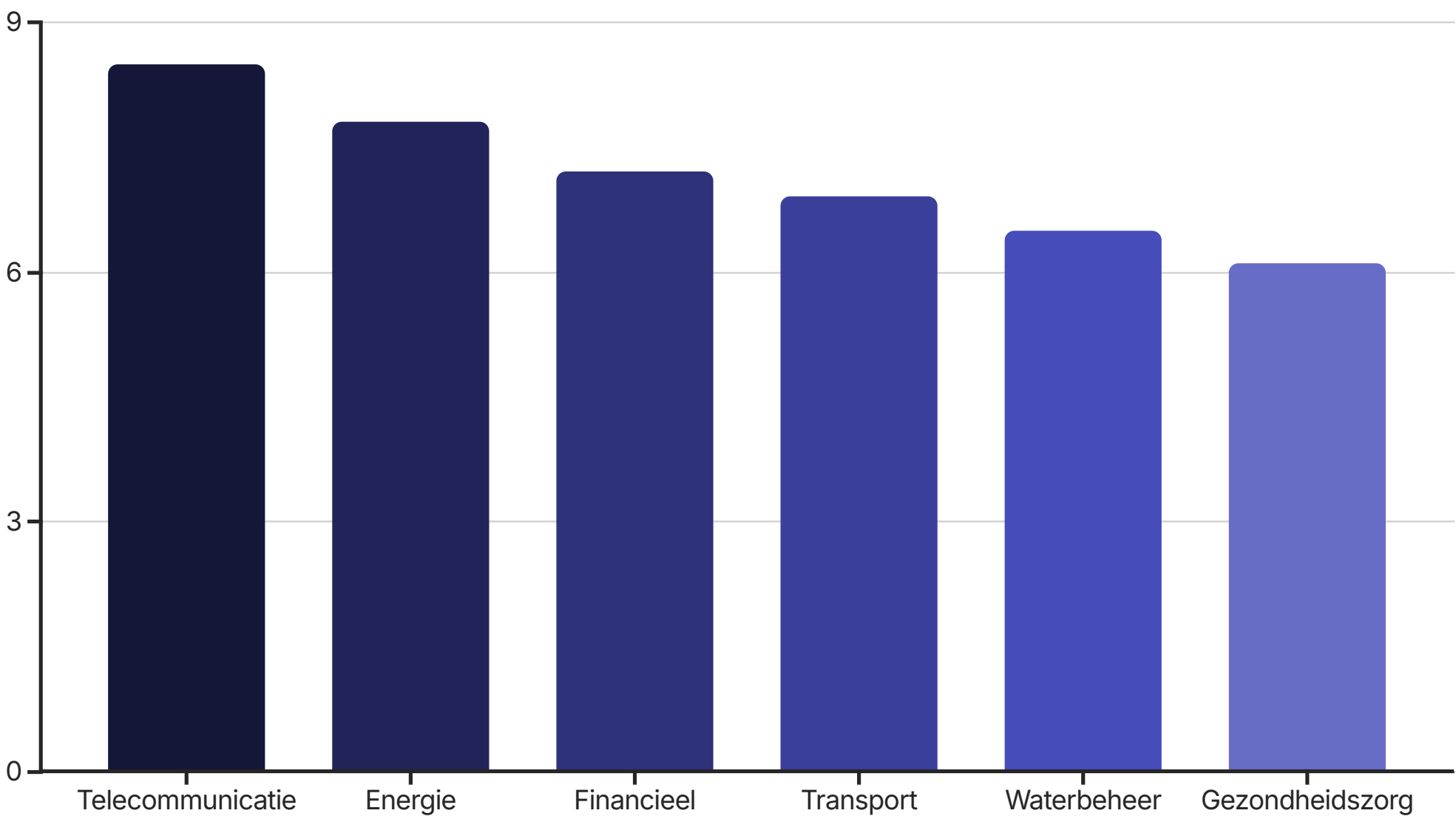
Kwetsbaarheden en concrete risico's voor Nederland

Nederland kent als hoogontwikkelde, open en digitaal verbonden samenleving specifieke kwetsbaarheden die het een aantrekkelijk doelwit maken voor buitenlandse actoren. De inlichtingendiensten identificeren verschillende cruciale infrastructuren die bijzondere bescherming behoeven vanwege hun vitale functie voor de Nederlandse samenleving en economie.

1	2
Noordzee-internetkabels De onderzeese glasvezelkabels in de Noordzee vormen een cruciale schakel in de internationale dataverbindingen. Sabotage van deze kabels zou kunnen leiden tot ernstige verstoring van internetverkeer en economische schade van mogelijk miljarden euro's.	Elektriciteitsvoorziening Het elektriciteitsnetwerk is kwetsbaar voor zowel fysieke als digitale aanvallen. Langdurige stroomuitval heeft directe gevolgen voor vrijwel alle maatschappelijke processen en kan leiden tot sociale onrust en economische ontwrichting.
3	4
Digitaal betalingsverkeer De Nederlandse economie is sterk afhankelijk van digitale betalingssystemen. Verstoring hiervan, zelfs voor korte tijd, kan het vertrouwen in het financiële systeem ondermijnen en aanzienlijke economische schade veroorzaken.	Drinkwatervoorziening De infrastructuur voor schoon drinkwater is essentieel voor de volksgezondheid. Manipulatie van waterzuiveringssystemen of distributieprocessen vormt een ernstige bedreiging voor de volksgezondheid.

De inlichtingendiensten waarschuwen specifiek voor het risico van digitale sabotage, waarbij essentiële voorzieningen tijdelijk kunnen worden verstoord. Dit type aanvallen is relatief eenvoudig uit te voeren maar kan aanzienlijke maatschappelijke impact hebben. Een kortdurende verstoring van bijvoorbeeld het betalingsverkeer of de elektriciteitsvoorziening kan al leiden tot economische schade en ondermijning van het vertrouwen in de overheid.

Er zijn concrete signalen dat buitenlandse actoren, met name Rusland, actief bezig zijn met sabotageactiviteiten en pogingen om westerse hulp aan Oekraïne te vertragen of te verstoren. Deze activiteiten vinden plaats in het grijze gebied tussen vreedstijd en oorlog, waardoor een adequate respons wordt bemoeilijkt. De diensten zien een toenemend risico op maatschappelijke ontwrichting en onrust als gevolg van buitenlandse inmenging.



Een bijzonder zorgwekkende ontwikkeling is de toenemende verwevenheid van verschillende typen dreigingen. Zo kan een cyberaanval gecombineerd worden met desinformatiecampagnes om de maatschappelijke impact te vergroten. Deze 'hybride dreigingen' zijn moeilijker te detecteren en te bestrijden, wat de kwetsbaarheid van Nederland verder vergroot.

Noodzaak tot verhoogde weerbaarheid en overheidsmaatregelen

In het licht van de toenemende dreigingen en kwetsbaarheden roepen de inlichtingendiensten op tot verhoogde alertheid en proactieve bescherming van vitale sectoren. Deze oproep is niet vrijblijvend - de diensten zijn ervan overtuigd dat Nederland in toenemende mate geconfronteerd zal worden met sabotageactiviteiten en andere vormen van buitenlandse inmenging die gericht zijn op ontwrichting van de samenleving.

"Het is niet de vraag óf, maar wanneer we ontwrichtende effecten gaan ervaren," aldus de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Om de nationale weerbaarheid te versterken, worden verschillende concrete maatregelen genomen. Een belangrijke stap is de integratie van diverse cyberwaarschuwingsdiensten tot één nationale organisatie, die naar verwachting eind 2025 operationeel zal zijn. Deze samenvoeging moet leiden tot een effectievere detectie van en respons op cyberaanvallen en andere digitale dreigingen.

Bewustwording

Vergroten van het bewustzijn bij overheidsinstanties, bedrijven en burgers over de aard en ernst van de dreigingen. Dit omvat voorlichtingscampagnes, trainingen en regelmatige dreigingsanalyses.

Detectie

Opzetten van geavanceerde detectiesystemen die vroegtijdig signalen van sabotage of spionage kunnen identificeren, inclusief de oprichting van een geïntegreerd nationaal cybersecurity centrum.

Preventie

Implementeren van preventieve maatregelen zoals verbeterde beveiligingsprotocollen, redundantie in kritieke systemen en regelmatige veiligheidsoefeningen om de weerbaarheid te testen en te verbeteren.

Respons

Ontwikkelen van snelle en effectieve responsprotocollen voor het geval er toch een aanval plaatsvindt, met duidelijke verantwoordelijkheden en communicatielijnen tussen alle betrokken partijen.

Een andere belangrijke maatregel is de oprichting van een centraal meldpunt bij het Nationaal Cyber Security Centrum, waar organisaties terecht kunnen met informatie over incidenten of vermoedens van digitale aanvallen. Door deze informatie centraal te verzamelen, kunnen patronen worden herkend en kan effectiever worden opgetreden tegen gecoördineerde aanvallen.

De overheid benadrukt dat weerbaarheid niet alleen een kwestie is van technische maatregelen, maar ook van maatschappelijke veerkracht. Het vermogen om snel te herstellen van verstoringen en het behouden van vertrouwen in overheidsinstanties zijn essentiële aspecten van een effectieve responsstrategie. Hiervoor is nauwe samenwerking nodig tussen overheid, bedrijfsleven en maatschappelijke organisaties.

Internationale samenwerking

Nederland versterkt de samenwerking met internationale partners, met name binnen de EU en NAVO, om informatie over dreigingen te delen en gezamenlijke responsstrategieën te ontwikkelen. Deze samenwerking is essentieel gezien het grensoverschrijdende karakter van veel dreigingen.

Publiek-private partnerschappen

De overheid stimuleert samenwerkingsverbanden tussen publieke en private organisaties om de weerbaarheid van kritieke infrastructuur te vergroten. Hierbij worden kennis, expertise en middelen gebundeld om effectiever te kunnen reageren op bedreigingen.

Tot slot wordt benadrukt dat verhoogde weerbaarheid geen eenmalige inspanning is, maar een continu proces van aanpassing en verbetering. De dreigingsomgeving evolueert voortdurend, wat vereist dat ook de beschermingsmaatregelen zich blijven ontwikkelen. Dit vraagt om structurele investeringen in kennis, technologie en samenwerkingsverbanden, zowel nationaal als internationaal.



Nep-gaming- en AI-bedrijven pushen malware op cryptocurrency-gebruikers

In 2025 zien we een alarmerende nieuwe golf van gerichte cyberaanvallen op cryptocurrency-gebruikers. Kwaadwillenden hebben hun pijlen gericht op de groeiende gemeenschap van crypto-enthousiastelingen door zich voor te doen als legitieme gaming- en AI-bedrijven.

Ze gebruiken populaire communicatieplatforms zoals Telegram en Discord als primaire kanalen voor het verspreiden van geavanceerde malware, waarmee ze toegang krijgen tot digitale wallets en persoonlijke gegevens van slachtoffers.

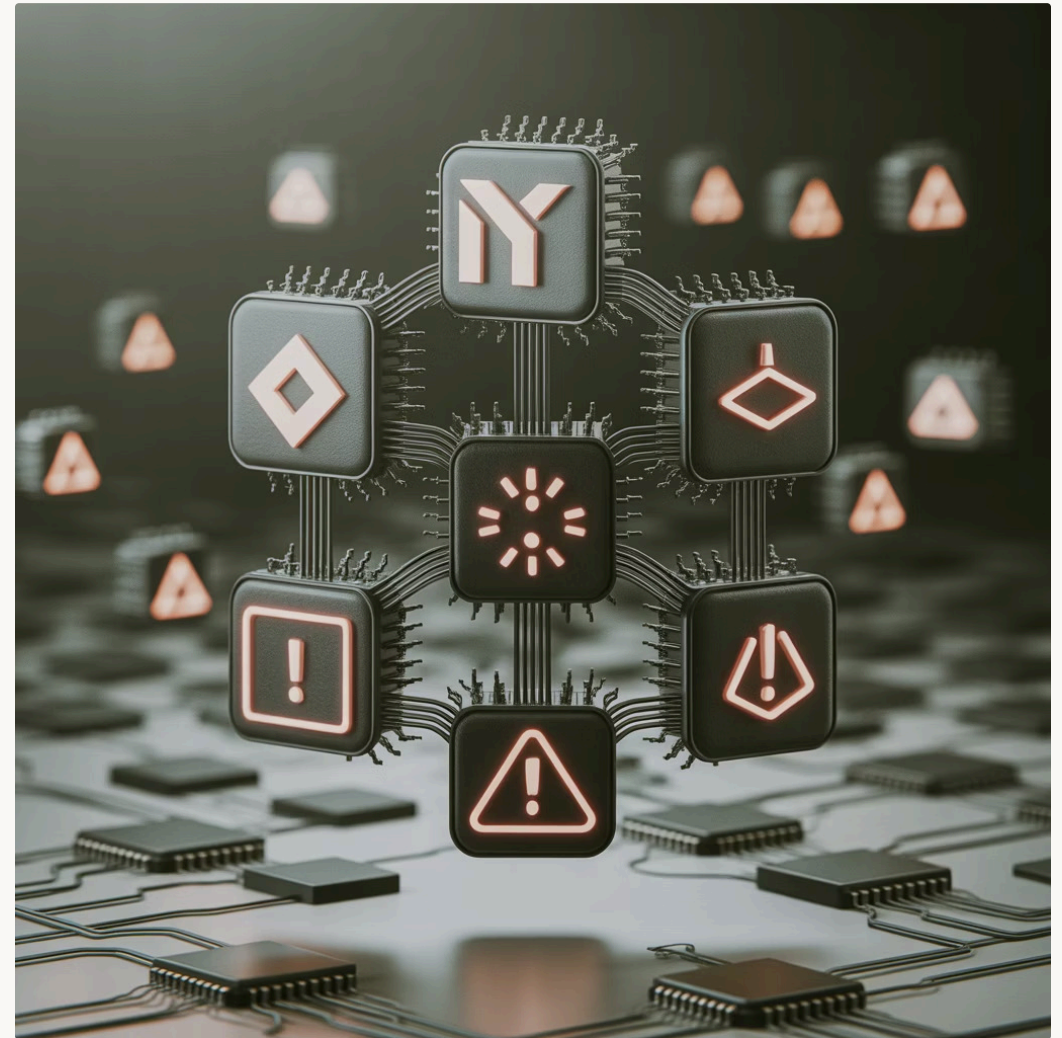
VEILIGDIGITAAL.COM

De opkomst van cybercrime via nepbedrijven

De cybercrimewereld heeft een zorgwekkende verschuiving doorgemaakt waarbij AI-technologie en deepfakes steeds vaker worden ingezet voor overtuigende oplichting. Nepbedrijven in de gaming- en AI-sector hebben ontdekt dat ze specifiek cryptocurrency-investeerders kunnen aantrekken door beloftes van innovatieve technologie, exclusieve toegang of lucratieve investeringsmogelijkheden.

Een belangrijk element in deze nieuwe golf van aanvallen is het gebruik van moeilijk te reguleren communicatieplatforms. Telegram en Discord bieden cybercriminelen een ideale omgeving door hun combinatie van:

- Anonimiteit en privacyfuncties
- Groot bereik binnen crypto-gemeenschappen
- Minimale controle op inhoud



Criminelen gebruiken deze platformen om malware te verspreiden die specifiek is ontworpen om cryptovaluta te stelen of om toegang te krijgen tot digitale wallets.

Aanvalsmethoden: zo werkt het

1

Geavanceerde phishing

Aanvallers creëren overtuigende nepaccounts en -kanalen die legitieme gaming- of AI-bedrijven nabootsen. Ze gebruiken gestolen logo's, professionele marketing en zelfs namaak-websites om slachtoffers te misleiden. Deze accounts bouwen vertrouwen op door regelmatig relevante content te delen voordat ze met malafide links komen.

2

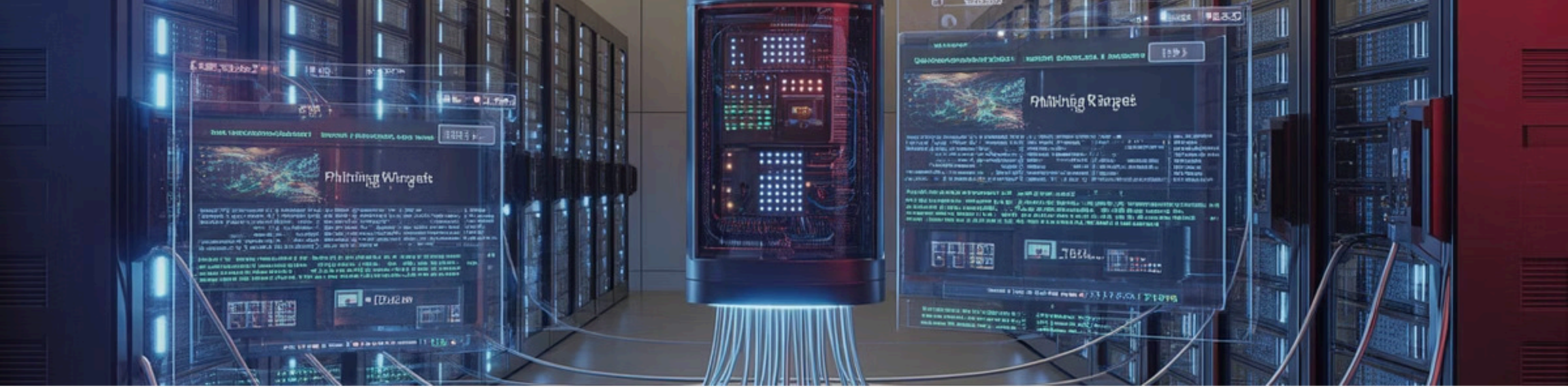
Malware-verspreiding

Criminelen bieden "exclusieve" applicaties of bots aan die zogenaamd speciale toegang geven tot gaming- of AI-functionaliteiten. Deze software bevat echter verborgen malware die cryptowallets kan leeghalen of persoonsgegevens kan stelen. Sommige malware blijft slapend aanwezig tot het een groot genoeg doelwit detecteert.

3

Gepersonaliseerde aanvallen

Door gebruik te maken van AI-analyse van publiek beschikbare data kunnen criminelen hun aanvallen personaliseren. Ze verzamelen informatie over potentiële slachtoffers via social media en forums, en passen hun benadering aan op basis van interesses, bezittingen en online gedrag van het doelwit.



AI als versneller van cybercrime

Automatische phishing op schaal

Moderne AI-systemen kunnen duizenden unieke en grammaticaal correcte phishingberichten per minuut genereren. Deze berichten worden automatisch aangepast aan de context van het doelwit en bevatten overtuigende elementen die de kans op succes vergroten.

Polymorfe malware

AI-gestuurde malware kan zichzelf constant hercoderen en aanpassen om traditionele antivirusoplossingen te omzeilen. Deze malware kan zich vermommen als legitieme software en zelfs leren van detectiepogingen om in de toekomst effectiever te worden.

Deepfake-profielen

Deepfake-technologie stelt criminelen in staat om volledig fictieve maar overtuigende online identiteiten te creëren voor hun nepbedrijven, compleet met "CEO-video's" en persoonlijke interacties die het vertrouwen van potentiële slachtoffers winnen.

Voorbeelden van recente incidenten (2025)

⊗ XAI-tokenscam

Een nepbedrijf dat zich voordeed als een AI-onderzoekslab bood een "exclusieve presale" aan van een niet-bestaande XAI-token met belofte van 50% bonus. Via een perfect geïmiteerde website verloor één slachtoffer 0,1 BTC (ongeveer €60.000) toen malware zijn wallet leeghaalde na een "investeringstransactie".

⚠ Gaming-platform shutdowns

Na een reeks spraakmakende sluitingen van legitieme crypto-gamingplatforms in 2025, ontstond er een vacuüm dat werd gevuld door scamprojecten die beweerden "de volgende grote crypto-game" te zijn. Deze nepprojecten richtten zich specifiek op gebruikers van de gesloten platforms.



ⓘ Discord-plugin malware

Consumentenrapporten hebben een verontrustende toename aangetoond van snelle malware-infecties via zogenaamde Discord-plugins voor gaming. Deze plugins beloven functies zoals automatische trading of in-game voordelen, maar installeren in werkelijkheid keyloggers die wachtwoorden onderscheppen.

Impact op crypto-gebruikers en industrie

Financiële verliezen

De geavanceerde aard van deze aanvallen heeft geleid tot steeds grotere financiële verliezen voor gebruikers. Zelfs ervaren handelaren in gevestigde cryptocurrencies zoals Bitcoin en Ethereum zijn slachtoffer geworden, met geschatte totale verliezen van meer dan €150 miljoen in het eerste halfjaar van 2025.

Vertrouwensverlies

Het cumulatieve effect van deze aanvallen heeft geleid tot een algemene daling van het vertrouwen in nieuwe crypto-projecten. Dit heeft legitieme startups in de ruimte gedwongen om aanzienlijk meer te investeren in het opbouwen van vertrouwen en het verifiëren van hun legitimiteit.



Marktvolatiliteit

Grote incidenten hebben geleid tot kortstondige maar hevige marktschommelingen wanneer nieuws over aanvallen bekend wordt. Dit heeft bijgedragen aan toenemende volatiliteit in een markt die al gevoelig is voor veranderingen in vertrouwen en sentiment.

Gaming-community's

Gaming-gemeenschappen zijn bijzonder kwetsbaar gebleken vanwege hun interesse in NFT's en digitale eigendommen. De combinatie van gaming, crypto en digitale verzamelobjecten creëert een drievoudige aantrekkingskracht voor criminelen, wat heeft geleid tot gerichte campagnes tegen deze gebruikersgroep.

Bescherming & tegenmaatregelen



De crypto-industrie en veiligheidsexperts hebben niet stilgezeten. In reactie op deze toenemende dreiging worden verschillende beschermingsstrategieën ontwikkeld en geïmplementeerd.

Security-awareness

Exchanges en wallet-providers investeren in uitgebreide educatieprogramma's om gebruikers bewust te maken van deze specifieke dreigingen. Platformen als Discord en Telegram implementeren strengere verificatieprocedures voor crypto-gerelateerde kanalen.

ML-fraude detectie

Geavanceerde machine learning-modellen worden ingezet om verdachte patronen in transacties en communicatie te identificeren. Deze systemen leren continu van nieuwe aanvalsmethoden en kunnen in realtime waarschuwingen geven.

Samenwerkingsverbanden

Er ontstaat een actieve samenwerking tussen cryptocurrency exchanges, cybersecurity-bedrijven en overheidsinstellingen om informatie over dreigingen te delen en gezamenlijk actie te ondernemen tegen bekende malafide actoren.

Conclusie: Wapenen tegen de AI-cybercrimegolf



Verhoogde urgentie

De toenemende verfijning van AI-gestuurde aanvallen heeft geleid tot een verhoogde urgentie voor robuuste beveiligingspraktijken in de cryptocurrency-sector. Wat voorheen als 'best practices' werd beschouwd, is nu een absolute noodzaak geworden voor alle gebruikers.



Kritische waakzaamheid

Gebruikers moeten extreme waakzaamheid betrachten bij interacties met onbekende projecten op chatplatforms, vooral als deze gerelateerd zijn aan AI of gaming. Verificatie via meerdere onafhankelijke bronnen is essentieel geworden voordat enige betrokkenheid wordt aangegaan.



Technologische evolutie

De doorlopende ontwikkeling van beschermingstechnologieën blijft cruciaal in deze wapenwedloop. Innovaties zoals gedragsgebaseerde detectie, biometrische verificatie en gedecentraliseerde identiteitsoplossingen bieden hoop voor een veiligere toekomst in het crypto-ecosysteem.

Als gemeenschap moeten we niet alleen reageren op deze dreigingen, maar proactief blijven in het ontwikkelen van betere verdedigingsstrategieën tegen de steeds evoluerende tactieken van cybercriminelen in het AI-tijdperk.



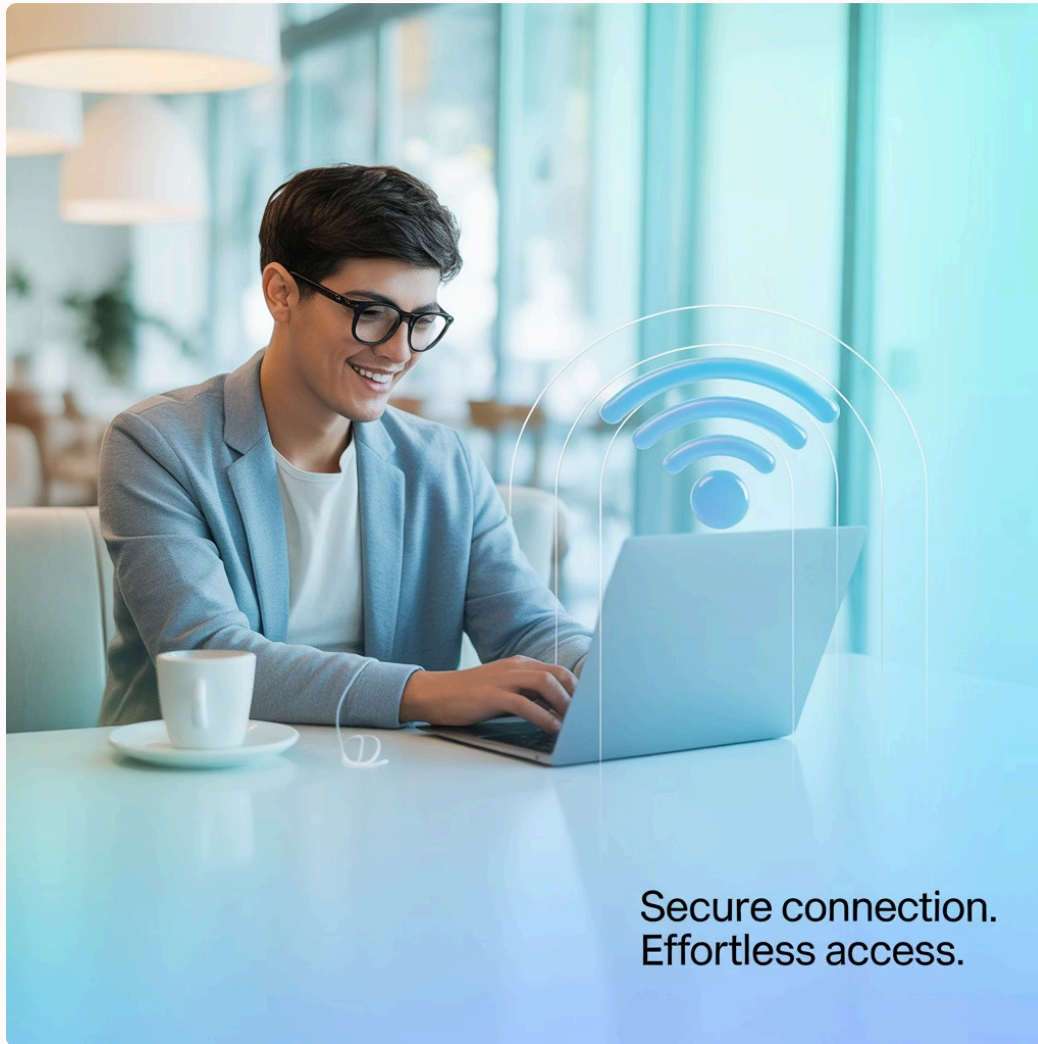
Nieuwe Bedreigingsinformatie: Ongedekte Wi-Fi Netwerken

Nieuwe bedreigingsinformatie van Zimperium onthult een alarmerende situatie: meer dan vijf miljoen ongedekte publieke Wi-Fi netwerken zijn sinds begin 2025 wereldwijd gedetecteerd.

Dit baanbrekende onderzoek biedt unieke inzichten in de toenemende dreigingen voor mobiele apparaten en de ontwikkelingen in cyberaanvallen op mobiel gebied.

VEILIGDIGITAAL.COM

Inzicht: Publieke Wi-Fi's als Grootste Mobiele Risico



De meest recente dreigingsinformatie van Zimperium bevestigt dat publieke Wi-Fi netwerken het grootste risico vormen voor mobiele apparaatbeveiliging. Volgens Zimperium's Mobile Threat Report zijn deze netwerken steeds vaker het doelwit van cybercriminelen die op zoek zijn naar gevoelige bedrijfs- en persoonlijke gegevens.

Met meer dan 5 miljoen kwetsbare netwerken wereldwijd in de eerste helft van 2025, is het risico aanzienlijk toegenomen. Deze stijging is vooral zorgwekkend omdat mobiele apparaten steeds vaker worden gebruikt voor toegang tot bedrijfsdata, wat een groter risico op datalekken met zich meebrengt.

- ⚠️ 90% van de mobiele gebruikers maakt regelmatig verbinding met publieke Wi-Fi netwerken zonder adequate beveiligingsmaatregelen.

Technologie Achter de Detectie: Danger Zone™

Realtime Risicobeoordeling

Danger Zone™ analyseert continu nabijgelegen Wi-Fi netwerken op potentiële beveiligingsproblemen, inclusief onversleutelde verbindingen en verdachte netwerkactiviteit.

Directe Waarschuwingen

Gebruikers ontvangen onmiddellijk meldingen bij het detecteren van risicovolle netwerken, waardoor datadiefstal en apparaatcompromittering kunnen worden voorkomen.

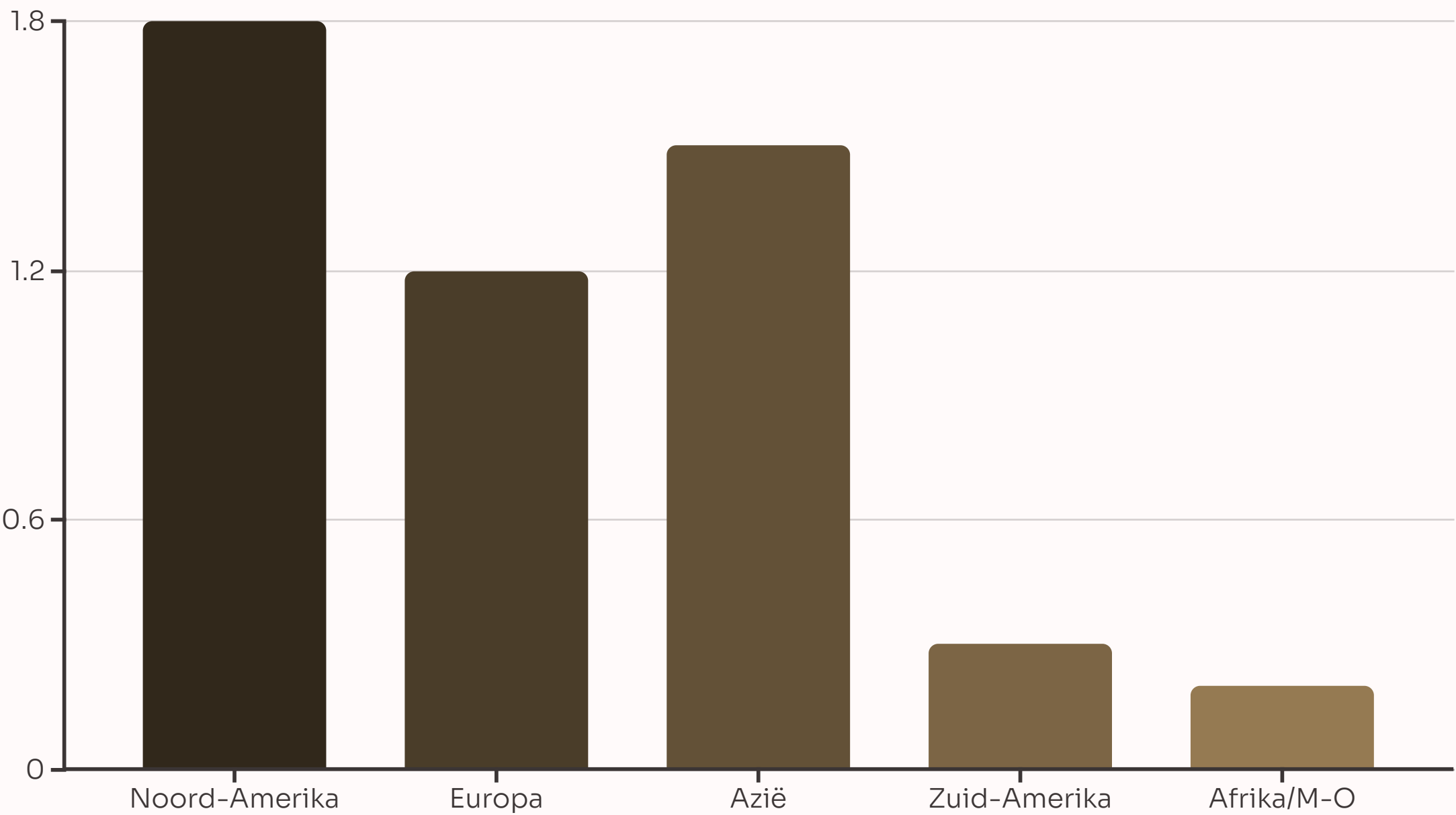
AI-Gedreven Detectie

Geavanceerde machine learning-algoritmes identificeren zelfs de nieuwste dreigingstactieken zonder negatieve impact op de gebruikerservaring of batterijduur.

De revolutionaire Danger Zone™-technologie vormt de kern van Zimperium's mobiele beveiligingsoplossing, waarmee gebruikers zich kunnen beschermen tegen de toenemende dreigingen van onveilige Wi-Fi netwerken.



Wereldwijde Verspreiding van Ongedekte Netwerken



Wi-Fi dreigingen zijn nu gemeld in meer dan 185 landen, wat een significante stijging vertegenwoordigt ten opzichte van 2024. Deze toename wordt aangedreven door de groei van mobiel werken en internationaal toerisme. Het meest zorgwekkende aspect is dat deze bedreiging universeel is en zowel grote stedelijke gebieden als landelijke locaties treft, waardoor vrijwel geen enkele regio immuun is.

Impact: Praktijkvoorbeelden en Gevolgen

1 Februari 2025

Grootschalig datalek bij Europese hotelketen waarbij gasten slachtoffer werden van man-in-the-middle aanvallen via de lobby Wi-Fi. Meer dan 30.000 klanten getroffen.

2 April 2025

Internationaal financieel congres in Amsterdam getroffen door gerichte aanval op bezoekers via gefalsificeerd 'CongressWiFi' netwerk, leidend tot diefstal van bedrijfsinloggegevens.

3 Juni 2025

Meerdere Nederlandse overheidsinstellingen rapporteren dataverlies via compromitteerde mobiele apparaten van medewerkers die publieke Wi-Fi gebruikten tijdens dienstreizen.

Deze praktijkvoorbeelden illustreren hoe cybercriminelen steeds vaker publieke Wi-Fi netwerken gebruiken als toegangspoort tot gevoelige bedrijfs- en persoonlijke gegevens, met aanzienlijke financiële en reputatieschade als gevolg.



Cybercrimineel Tactiek: Mobiel-First Aanvallen



Wi-Fi Proxying

Aanvallers creëren kwaadaardige hotspots die legitieme netwerken imiteren en al het dataverkeer onderscheppen.

Captive Portal Phishing

Valse inlogpagina's op publieke Wi-Fi's verzamelen inloggegevens van nietsvermoedende gebruikers.

App Sideload Exploits

Kwetsbaarheden in zijdelings geïnstalleerde apps worden uitgebuit via onveilige netwerkverbindingen.

In 2025 zien we een verschuiving naar steeds geavanceerdere mobiel-gerichte aanvalstactieken. Cybercriminelen richten zich specifiek op onbeschermden gebruikers met zorgvuldig ontworpen phishing-aanvallen en malware die speciaal zijn ontwikkeld voor mobiele apparaten en applicaties.

Samenvatting en Advies



"De toename van ongedekte Wi-Fi netwerken vormt een van de grootste bedreigingen voor mobiele beveiliging in 2025. Organisaties moeten nu handelen om hun gegevens te beschermen."

— Hendrik van der Meer, CISO bij Nederlandse Cybersecurity
Associatie

1 Vermijd Onbeschermd Wi-Fi

Gebruik nooit ongedekte publieke Wi-Fi-netwerken zonder adequate mobiele bescherming of VPN-verbinding.

2 Implementeer Beveiligingsoplossingen

Installeer geavanceerde security-apps zoals Zimperium zIPS op alle bedrijfs- en persoonlijke apparaten die bedrijfsgegevens verwerken.

3 Blijf Alert

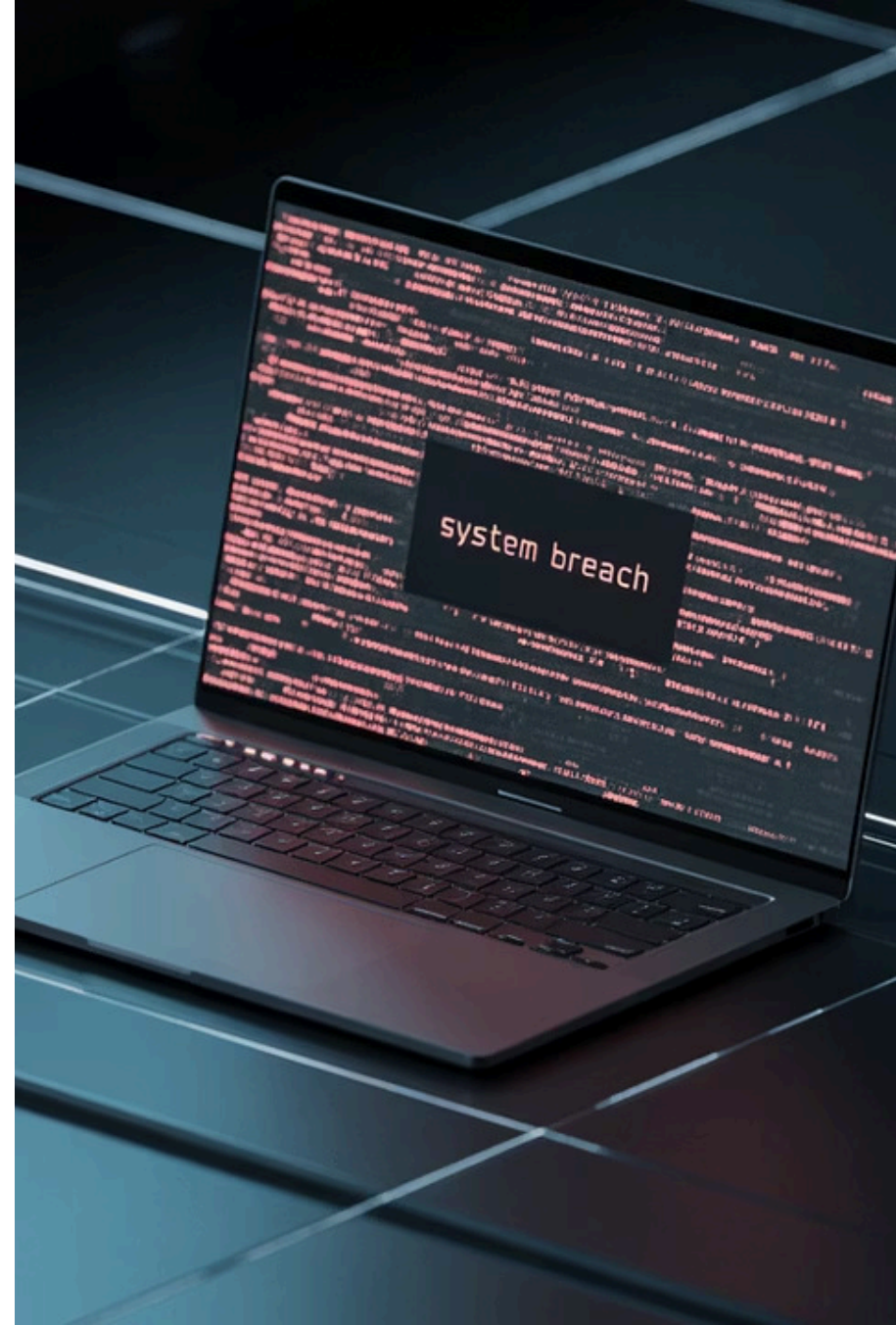
Houd rekening met de snelle evolutie van cyberbedreigingen en zorg voor regelmatige beveiligingsupdates en gebruikerstraining.

Nieuwe ransomware: Mamona – klein, snel en zelfvoorzienend

Een nieuwe, verontrustende ransomware-variant genaamd 'Mamona' is ontdekt in het voorjaar van 2025. Deze malware onderscheidt zich door zijn minimalistische aanpak en volledige offline functionaliteit, waardoor detectie bijzonder moeilijk wordt.

Mamona richt zich specifiek op Windows-systemen en heeft geen communicatie met externe servers nodig om zijn verwoestende taak uit te voeren. Door het lekken van de builder-tool is deze ransomware nu breed inzetbaar door cybercriminelen, wat de dreiging aanzienlijk vergroot.

VEILIGDIGITAAL.COM



Unieke kenmerken van Mamona



Wat Mamona echt onderscheidt van andere ransomware is zijn gebruik van volledig aangepaste encryptie-algoritmes in plaats van standaard oplossingen. Deze benadering maakt decodering zonder de sleutel vrijwel onmogelijk.

De "mute" werking betekent dat de ransomware geen netwerkverkeer genereert en geen data steelt. In plaats daarvan voert het alleen lokale acties uit, waardoor het traditionele detectiemethoden omzeilt die afhankelijk zijn van netwerkmonitoring of gedragsanalyse.

Custom Encryptie

Gebruikt eigen algoritmes die moeilijker te kraken zijn dan standaardoplossingen

"Mute" Werking

Geen communicatie met externe servers of command-and-control infrastructuur

Geen Netwerkverkeer

Laat minimale digitale sporen achter, ontwijkt netwerkgebaseerde detectie

Waarom is Mamona zo gevaarlijk?



Eenvoudige Bouwkit

De "ransomware-as-a-builder" tool maakt het zelfs voor technisch minder onderlegde criminelen mogelijk om aangepaste Mamona-varianten te creëren en te verspreiden.



Bliksemsnelle Uitvoering

Voltooit de encryptie binnen enkele seconden, waardoor reactietijd voor beveiligingssystemen minimaal is en schade al is aangericht voordat detectie plaatsvindt.



Zelfverwijdering

Na het voltooien van de encryptie verwijdt Mamona zichzelf, waardoor forensisch onderzoek aanzienlijk bemoeilijkt wordt en sporen minimaal zijn.

Deze combinatie van factoren maakt Mamona tot een bijzonder sluwe en effectieve bedreiging voor zowel individuele gebruikers als bedrijven.



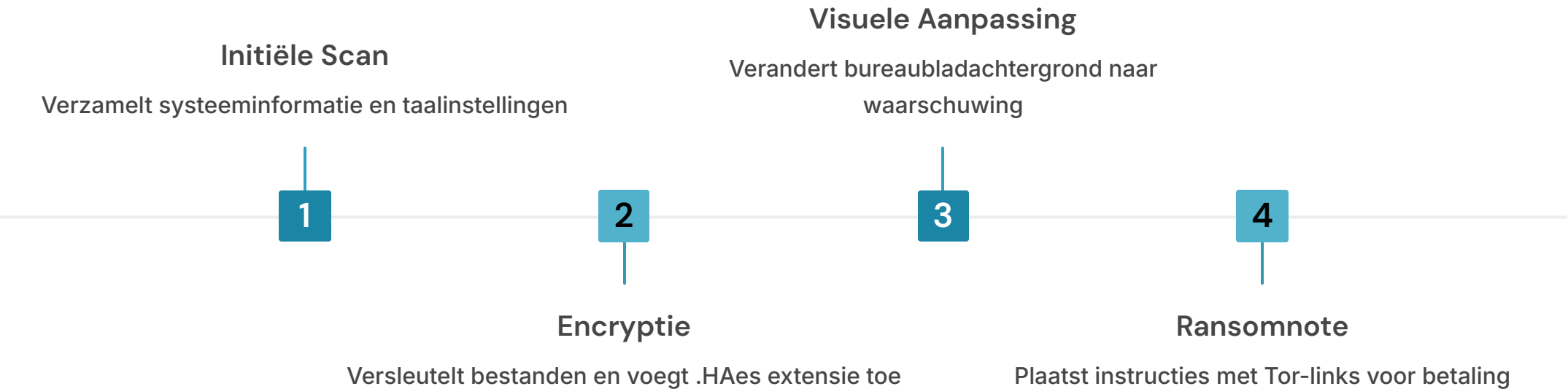
Aanvalsmethoden en impact

Bij infectie voert Mamona onmiddellijk een systematische scan uit waarbij het de systeemnaam en taalinstellingen identificeert. Vervolgens begint het bestanden te versleutelen en voegt de .HAes extensie toe aan gecompromitteerde bestanden.

De ransomware past ook de bureaubladachtergrond aan met een waarschuwingsbericht en plaatst in alle mappen een "README.HAes.txt" bestand met ransom-instructies, inclusief links naar Tor-ondersteuning en een chatchannel voor communicatie.



⚠️ Hoewel Mamona geen daadwerkelijke data-exfiltratie uitvoert, bevat het ransomnote vaak misleidende dreigementen over gestolen data om slachtoffers onder druk te zetten het losgeld te betalen.



Bescherming tegen moderne ransomware

Gedragdetectie

Implementeer actieve monitoring en sandboxing om verdachte processen te identificeren en isoleren voordat ze schade kunnen aanrichten.

Offline Back-ups

Maak regelmatig back-ups die volledig losgekoppeld zijn van het netwerk en niet toegankelijk zijn voor potentiële ransomware-aanvallen.

Security Training

Investeer in bewustwordingstraining voor medewerkers om phishing en andere aanvalsvectoren te herkennen en te vermijden.

Voor het MKB is extra waakzaamheid geboden. Een gelaagde beveiligingsaanpak is cruciaal, waarbij meerdere beschermingsmechanismen worden gecombineerd om de weerstand tegen geavanceerde bedreigingen zoals Mamona te vergroten.

- ❗ Zelfs bij de beste preventieve maatregelen is een solide herstelplan essentieel. Zorg dat uw organisatie voorbereid is op het ergste scenario met een uitgebreid incident response plan.



Norton Genie: Jouw AI-Bescherming Tegen Digitale Oplichting

In het huidige digitale tijdperk worden cyberbedreigingen steeds geavanceerder. Norton Genie is een baanbrekende AI-gedreven tool die speciaal is ontworpen om mensen te beschermen tegen online oplichting. Deze innovatieve oplossing herkent direct phishing, frauduleuze berichten, verdachte websites en misleidende social media posts.

Ontwikkeld door cybersecurity-expert Norton, is deze tool eenvoudig beschikbaar als mobiele app en via een gebruiksvriendelijke webbrowser-interface, waardoor bescherming tegen digitale bedreigingen voor iedereen toegankelijk wordt.

BY VEILIGDIGITAAL.COM



De Intelligente Technologie Achter Norton Genie

Norton Genie combineert geavanceerde kunstmatige intelligentie met Norton's uitgebreide dreigingsdatabase om een ongekend niveau van bescherming te bieden. Deze krachtige combinatie stelt de tool in staat om binnen enkele seconden frauduleuze activiteiten te identificeren.

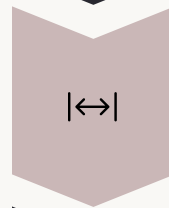
Het systeem blijft zichzelf voortdurend verbeteren door input van gebruikers te verwerken, waardoor de bescherming steeds nauwkeuriger wordt tegen nieuwe en opkomende bedreigingen.

Norton's jarenlange expertise in cybersecurity zorgt ervoor dat de AI-analyses gebaseerd zijn op real-world gegevens over actuele cyberdreigingen.



Uploaden

Gebruiker deelt verdachte berichten, e-mails of links



Analyse

AI analyseert de inhoud via geavanceerde algoritmes



Resultaat

Betrouwbaar oordeel binnen seconden beschikbaar

Praktische Toepassingen van Norton Genie

1

SMS en E-mail Verificatie

Upload eenvoudig een screenshot van verdachte berichten of kopieer de tekst om direct te controleren of het om phishing gaat

2

Link Controle

Plak verdachte URL's rechtstreeks in de tool om te controleren of de bestemming veilig is voordat je erop klikt

3

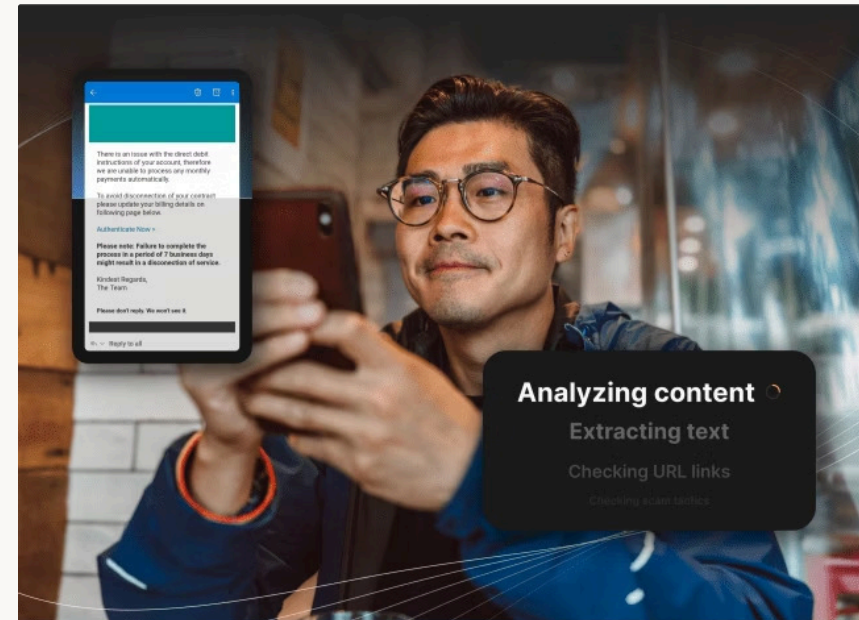
Social Media Analyse

Controleer of aanbiedingen, berichten of profielen op sociale media legitiem zijn of oplichting

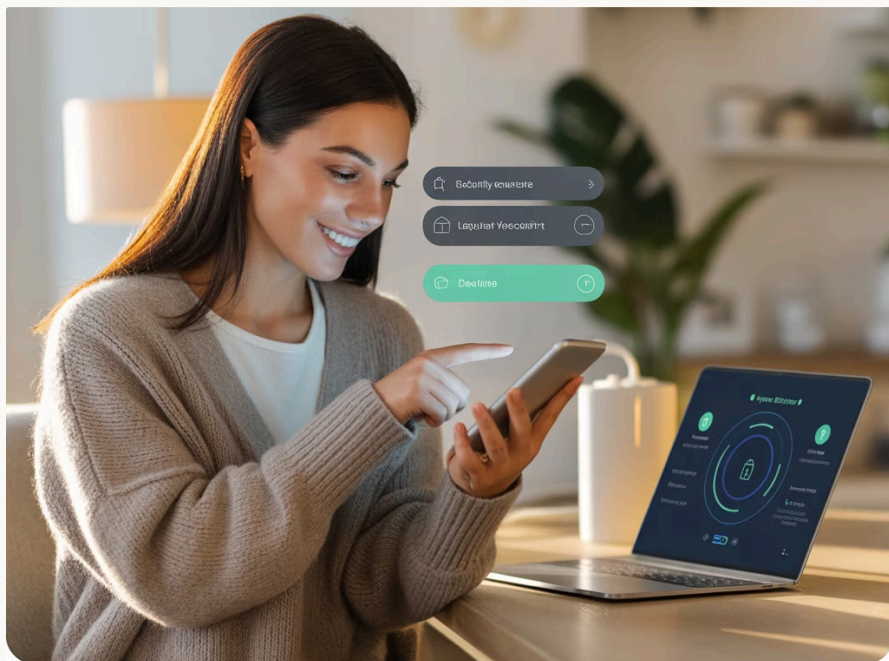
4

Persoonlijk Advies

Ontvang directe waarschuwingen en praktische tips over wat je moet doen bij gedetecteerde bedreigingen



Norton Genie in 4 Eenvoudige Stappen



“Your digital fortress”

Downloaden & Installeren

Download de Norton Genie app via de App Store of Google Play, of bezoek de officiële website voor directe toegang via je browser

Verdachte Content Delen

Kopieer en plak verdachte tekst, upload een screenshot van het bericht, of deel een verdachte URL die je wilt laten controleren

Ontvang Analyse

Binnen enkele seconden ontvang je een duidelijke beoordeling die aangeeft of de inhoud veilig is of een potentiële bedreiging vormt

Volg Advies Op

Krijg gepersonaliseerde veiligheidstips en antwoorden op eventuele vervolgvragen over de gedetecteerde bedreiging

Maximaliseer Je Digitale Veiligheid met Norton Genie

Doorlopende Bescherming

Norton Genie biedt directe beveiliging tegen de nieuwste vormen van digitale oplichting, 24/7 beschikbaar wanneer je het nodig hebt

Zelflerende Technologie

De AI-engine blijft leren en updaten met elk gebruik, waardoor de bescherming steeds effectiever wordt tegen nieuwe bedreigingen

Community Bijdrage

Door je ervaringen te delen help je de tool slimmer te maken en bescherm je daarmee indirect ook anderen tegen cybercriminaliteit

Expert Tip

"Maak het controleren van verdachte berichten met Norton Genie onderdeel van je dagelijkse digitale routine. Neem bij twijfel altijd de tijd om een bericht te verifiëren voordat je actie onderneemt."



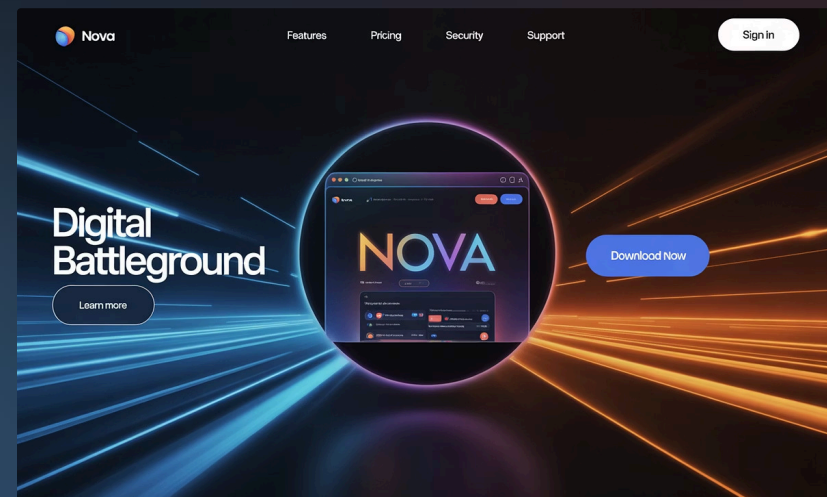
Wist je dat? Zelfs ervaren internetgebruikers worden regelmatig doelwit van geavanceerde phishing-aanvallen. Norton Genie kan subtiele aanwijzingen detecteren die voor het menselijk oog gemakkelijk te missen zijn.

OpenAI en Perplexity gaan browseroorlogen aan om het op te nemen tegen Chrome

Binnenkort staat de browserwereld een revolutie te wachten. OpenAI en Perplexity lanceren innovatieve AI-browsers die een rechtstreekse aanval inzetten op de hegemonie van Google Chrome.

Deze nieuwe generatie browsers integreert geavanceerde AI-functionaliteit in het hart van de internetervaring, waarmee ze een fundamenteel andere benadering kiezen dan de traditionele browsers.

VEILIGDIGITAAL.COM

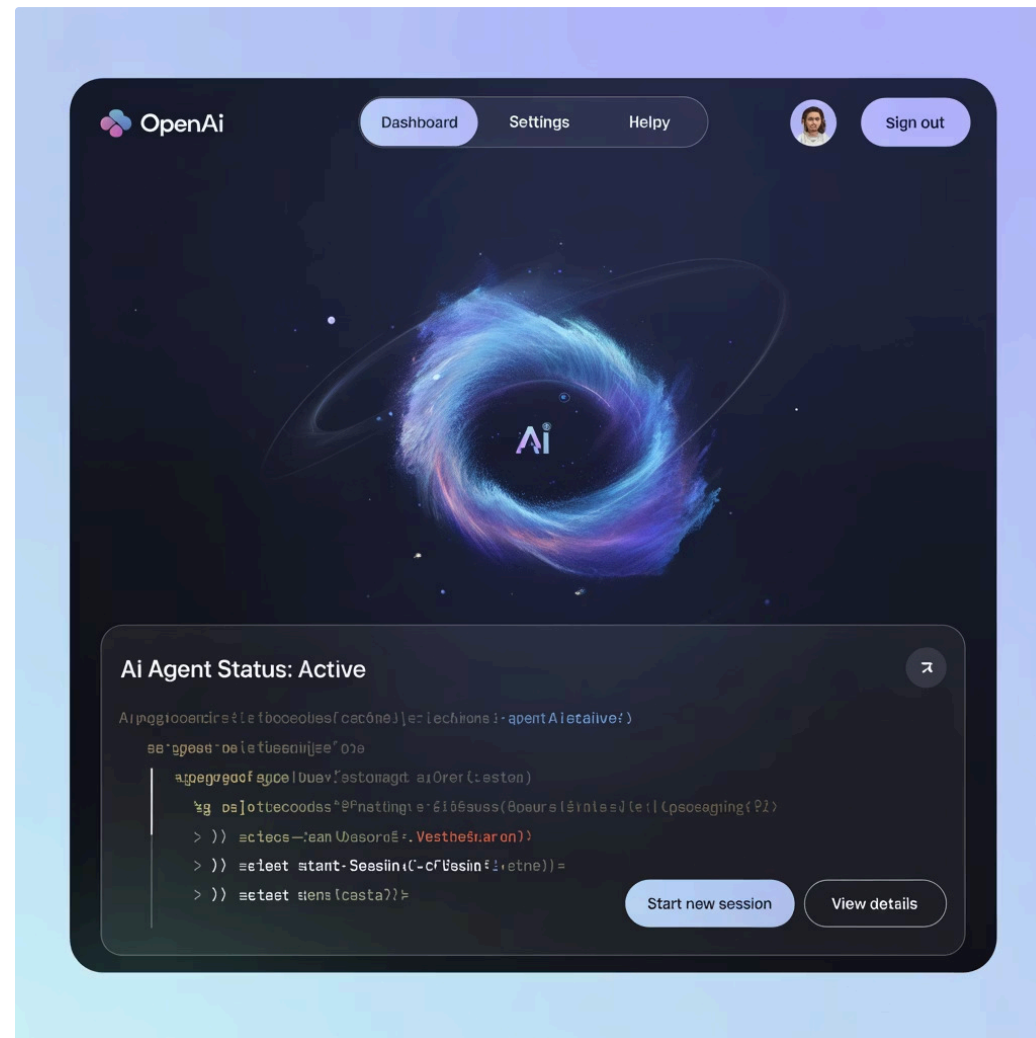


OpenAI's Gamechanger: De Chromium-AI Browser

OpenAI werkt in het diepste geheim aan een revolutionaire browser met de interne codenaam 'Operator'. Deze nieuwe browser is gebouwd op het Chromium-platform, dezelfde open-source basis als Chrome, maar met een cruciale toevoeging: volledige integratie van AI-agenten.

De browser maakt het mogelijk om complexe webtaken te automatiseren en biedt directe toegang tot gebruikersdata, wat een strategische zet is in de concurrentiestrijd met Google Chrome. De bèta-versie wordt naar verwachting in de zomer van 2025 gelanceerd voor ChatGPT Plus-gebruikers in de Verenigde Staten.

OpenAI's browser geeft de AI-gigant rechtstreeks toegang tot waardevolle gebruikersdata, waarmee het zijn afhankelijkheid van andere platforms vermindert en de positie tegenover Google versterkt.



Perplexity Comet: Directe Concurrent voor Chrome en AI Browsers

1

Exclusieve Launch

Lancering in juli 2025, aanvankelijk alleen beschikbaar voor Max-abonnees die €200 per maand betalen, waarmee Perplexity zich richt op premium gebruikers.

2

Comet Assistant

Revolutionaire AI-assistent die e-mails en agenda's automatisch samenvat, tabbladen efficiënt beheert en complexe browsertaken stroomlijnt zonder tussenkomst.

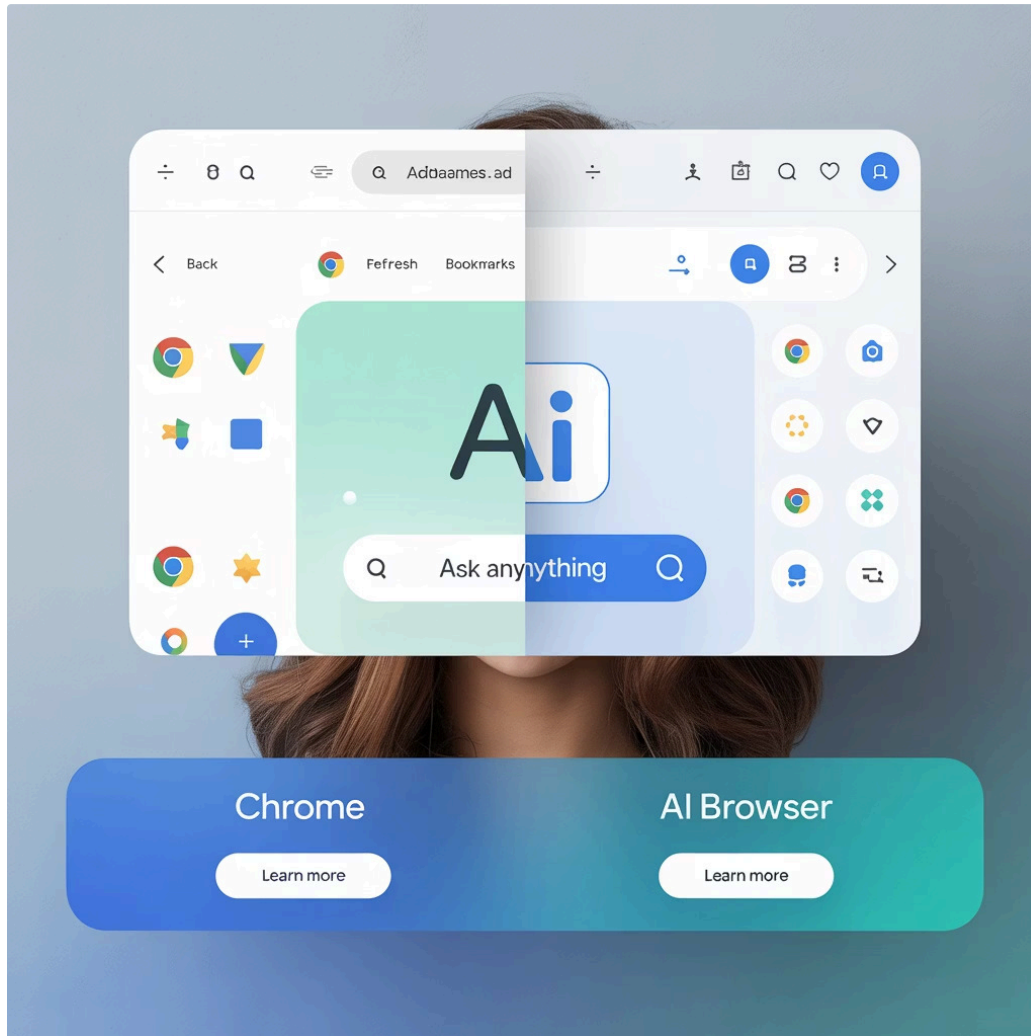
3

Geïntegreerde Zoekmachine

Perplexity's eigen zoekmachine is standaard geïnstalleerd, waardoor gebruikers geen Google meer nodig hebben en alle zoekacties direct binnen het ecosysteem blijven.

Perplexity's ultieme ambitie is om Comet te ontwikkelen tot een volledig "AI operating system" dat gebruikers aan het platform bindt en hen minder afhankelijk maakt van andere diensten.

Waarom zijn deze browsers een bedreiging voor Chrome?



AI-centrische Aanpak

In tegenstelling tot traditionele browsers plaatsen deze nieuwe platforms AI-functionaliteit in het centrum van de gebruikerservaring.

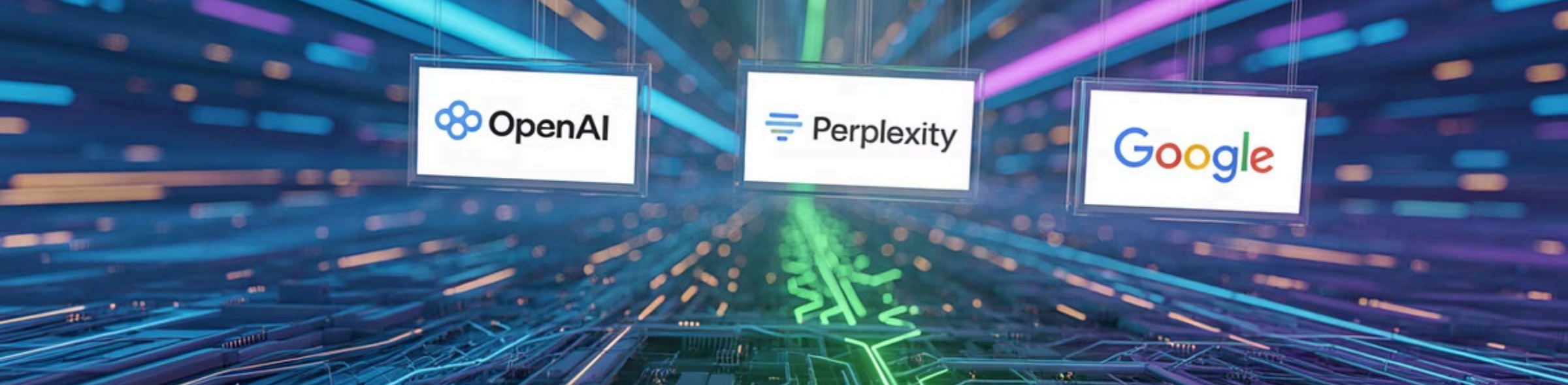
Directe Integratie

Zoekmachines en AI-assistenten zijn naadloos geïntegreerd binnen de browser, waardoor externe diensten overbodig worden.

Superieure Automatisering

De nieuwe browsers bieden geavanceerde automatisering en informatieoverzicht die klassieke browsers niet kunnen evenaren.

Google reageert al door snel AI-functies aan Chrome toe te voegen, maar loopt het risico achter de ontwikkelingen aan te lopen als het niet snel genoeg innoveert.



Toekomst: AI-browsers als nieuw slagveld



Verschuiving naar AI-integratie

De browseroorlog verplaatst zich van traditionele features naar de mate van AI-integratie en toegang tot gebruikersdata.



Directe gebruikersrelatie

OpenAI en Perplexity proberen een directe relatie met eindgebruikers op te bouwen, waarmee ze Google's tussenrol elimineren.



Cruciale race

De komende maanden worden beslissend voor wie de overhand krijgt in deze nieuwe fase van de browseroorlogen.

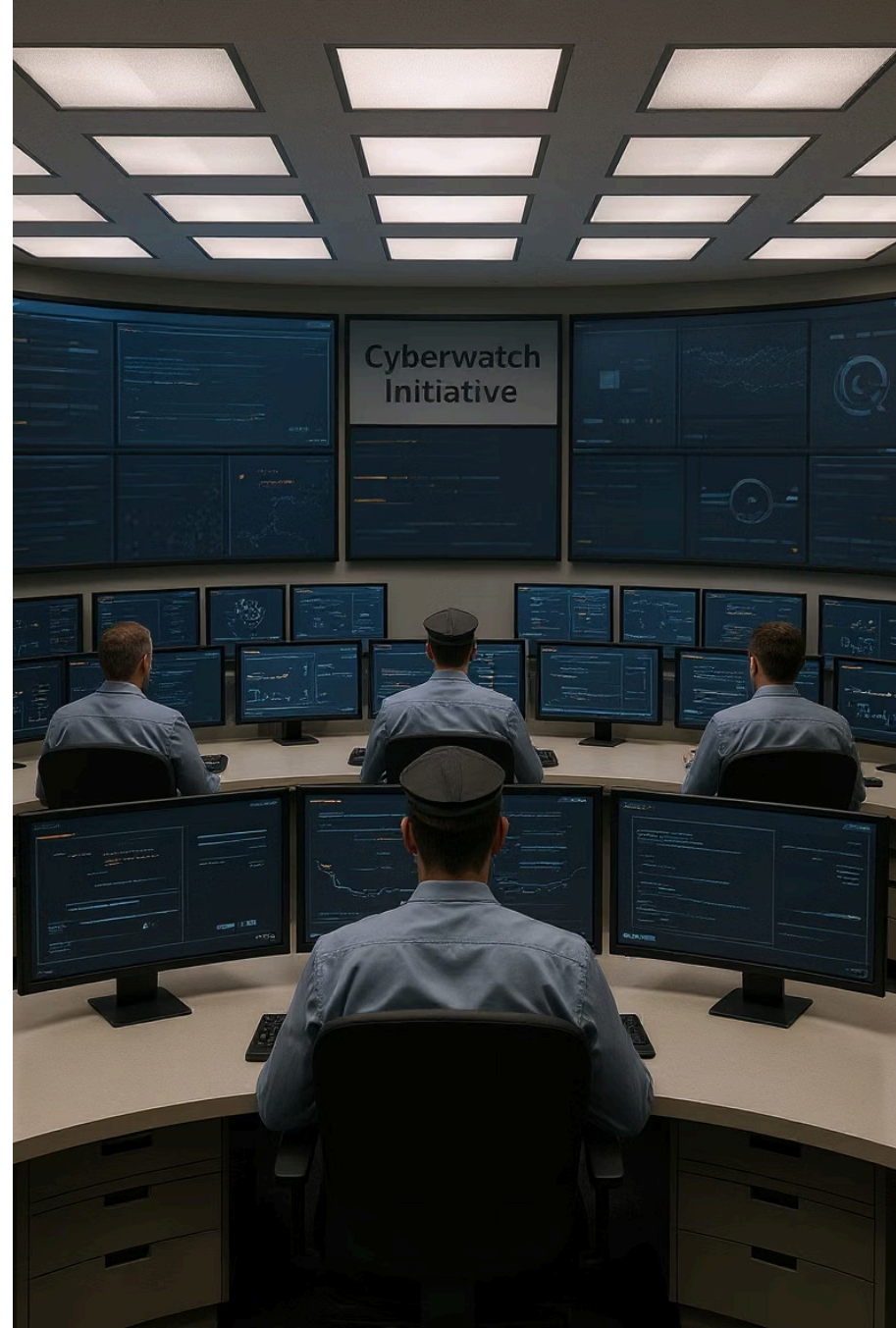
Als deze nieuwe browsers succes boeken, zou dit een fundamentele verschuiving kunnen betekenen in hoe we het internet gebruiken, met AI als centrale spil in plaats van als aanvullende functionaliteit.

Operatie Eastwood verstoort NoName057(16)

Deze maand vond een grootschalige internationale politieactie plaats tegen de pro-Russische hackersgroep NoName057(16). Deze operatie, codenaam "Eastwood", werd gecoördineerd door Europol en Eurojust en resulteerde in het offline halen van een groot deel van de infrastructuur van de groep.

De actie markeert een belangrijke stap in de strijd tegen cyberdreigingen die vanuit Rusland westerse doelen aanvallen.

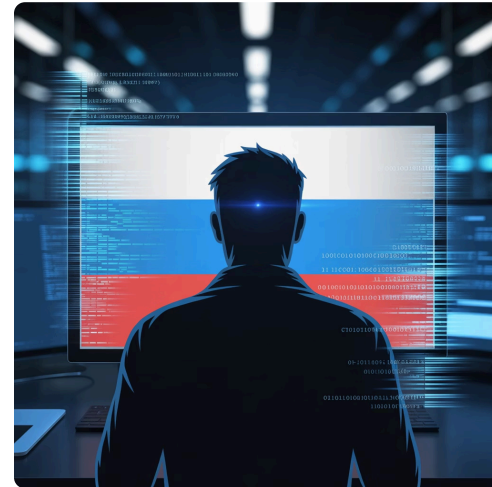
VEILIGDIGITAAL.COM



Achtergrond NoName057(16)

NoName057(16) is een pro-Russische hacktivistengroep die actief is sinds maart 2022, kort na het begin van de Russische invasie in Oekraïne. De groep heeft naam gemaakt door middel van Distributed Denial of Service (DDoS) aanvallen op westerse doelen.

Voor hun communicatie en propaganda maakt de groep intensief gebruik van Telegram-kanalen, waar ze hun activiteiten coördineren en successen vieren. Ze zijn ook bekend als de ontwikkelaar van DDOSIA, een krachtig DDoS-tool dat wordt gebruikt om websites en online diensten te overspoelen met verkeer.



De groep opereert met een duidelijke pro-Russische agenda en heeft banden met de Russische overheid, hoewel de exacte aard van deze relaties moeilijk te bewijzen is.

Activiteiten van NoName057(16)

Doelwitten

De groep voerde cyberaanvallen uit op overheden, mediaorganisaties en bedrijven in Europa, Oekraïne en de Verenigde Staten. Vooral organisaties die kritiek uitten op Rusland werden getroffen.

Methoden

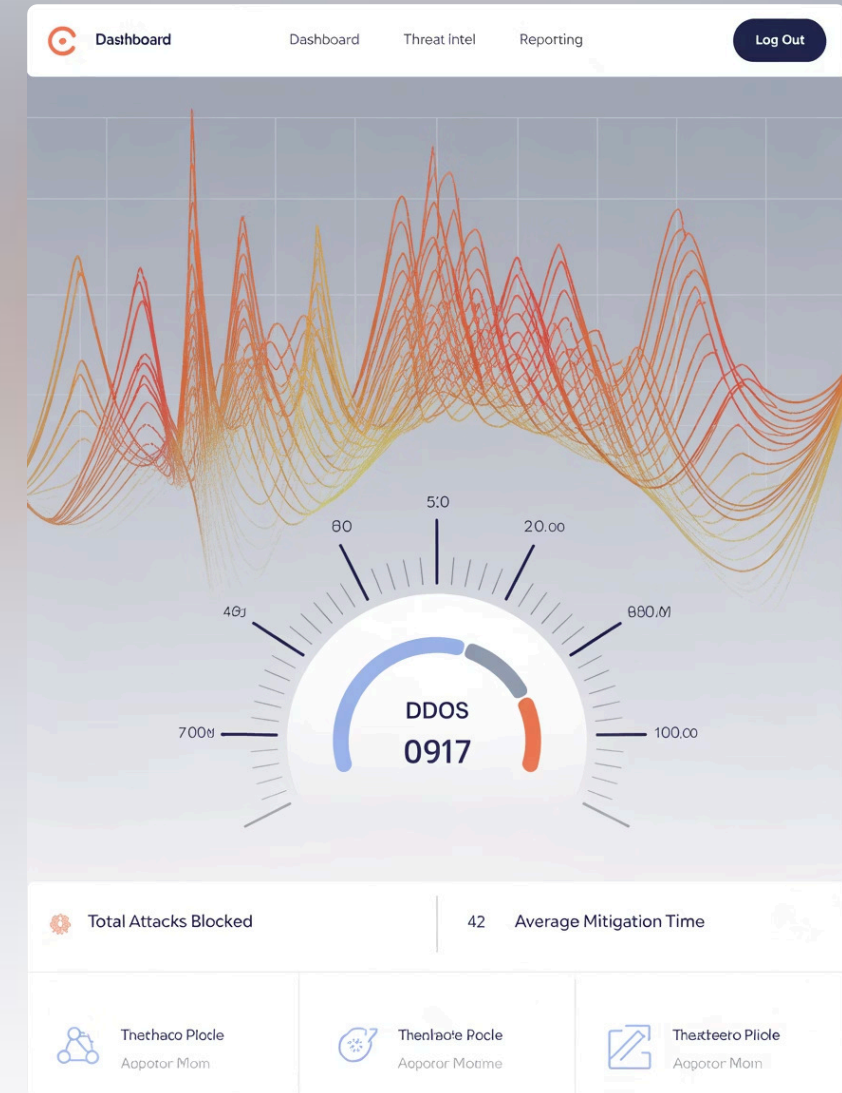
Primair gebruikte NoName057(16) DDoS-aanvallen om websites onbereikbaar te maken. Deze aanvallen werden uitgevoerd via het DDOSIA-platform dat vrijwilligers in staat stelde deel te nemen aan aanvallen.

Samenwerkingsverbanden

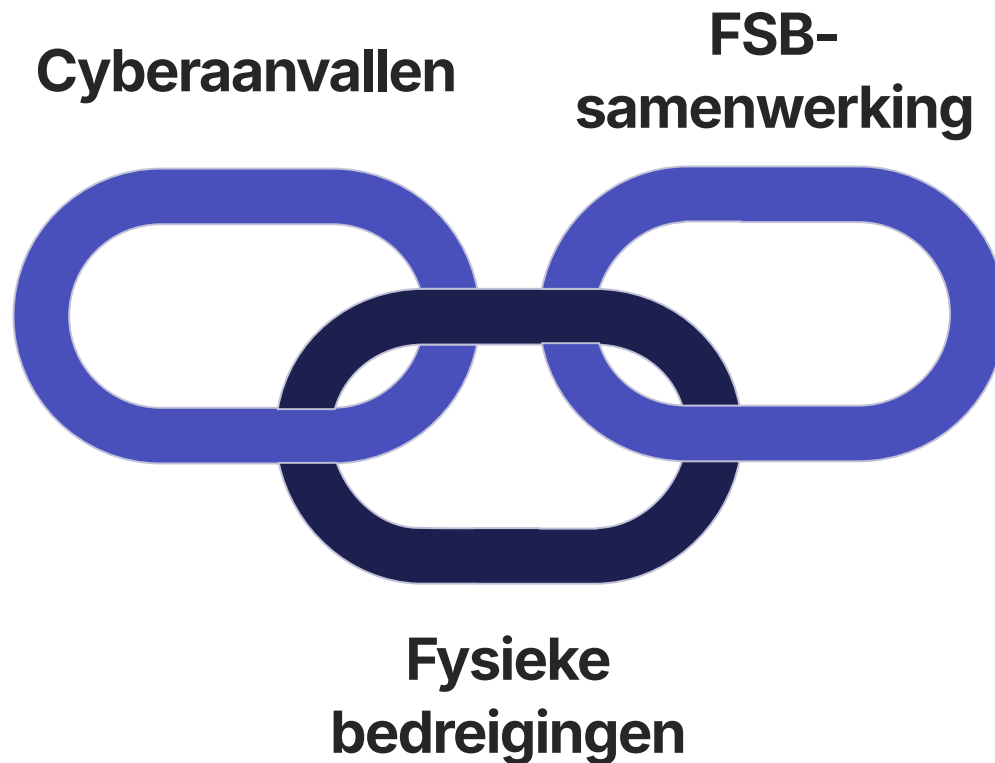
De groep werkte nauw samen met andere pro-Russische cybercollectieven zoals Killnet, waarmee ze informatie en resources deelden om hun impact te vergroten.

Intimidatie

Naast technische aanvallen bedreigde de groep individuele tegenstanders en journalisten, wat leidde tot persoonlijke veiligheidsrisico's voor critici van Rusland.



Directe aanleiding tot Operatie Eastwood



De beslissing om tot grootschalige actie over te gaan werd genomen na een duidelijke escalatie van aanvallen op Europese kritieke infrastructuur. Veiligheidsdiensten ontdekten bovendien dat de groep was begonnen samen te werken met Russische FSB-agenten bij pogingen tot fysiek geweld tegen rivalen.

Onderzoek bracht aan het licht dat honderden sympathisanten wereldwijd technische of ideologische steun leverden aan de operaties van NoName057(16), wat de dreiging vergrootte en een gecoördineerde internationale respons noodzakelijk maakte.



Internationale samenwerking en voorbereiding

1

Voorbereiding

Meer dan 20 landen bundelden hun krachten, waaronder Nederland, Duitsland, de Verenigde Staten en Frankrijk. Cybersecurity-experts werkten maandenlang samen om alle elementen van de operatie te plannen.

2

Technische ondersteuning

Specialistische organisaties zoals het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA), ShadowServer en abuse.ch leverden cruciale technische expertise voor het in kaart brengen van de infrastructuur.

3

Uitvoering

Tussen 14 en 17 juli 2025 vonden gelijktijdig 24 huiszoeken plaats en werden 13 verdachten ondervraagd in verschillende landen, wat de hoge mate van coördinatie aantoonde.

Resultaten van Operatie Eastwood

100+

Servers offline

Wereldwijd werden meer dan honderd servers die gebruikt werden door NoName057(16) offline gehaald, waardoor hun operationele capaciteit ernstig werd aangetast.

2

Arrestaties

Twee belangrijke leden werden gearresteerd in Frankrijk en Spanje tijdens gecoördineerde invallen.

7

Arrestatiebevelen

Zeven internationale arrestatiebevelen werden uitgevaardigd, waarvan zes tegen Russische staatsburgers die worden gezocht voor hun rol in de hackersgroep.

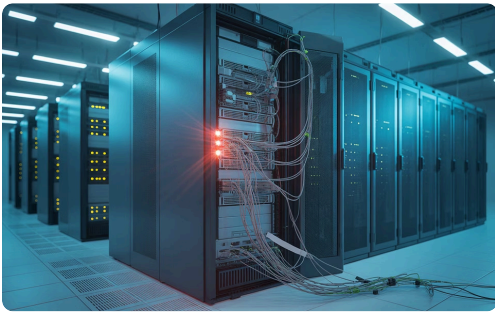
1000+

Waarschuwingen

Meer dan duizend sympathisanten ontvingen officiële waarschuwingen over de strafbaarheid van hun betrokkenheid bij cyberaanvallen.

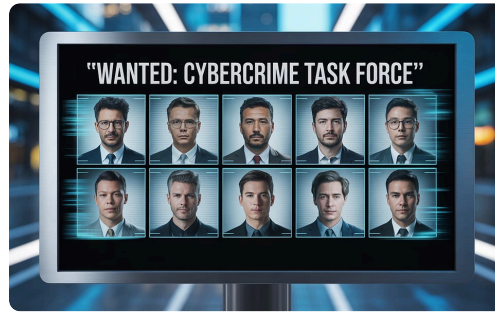


Impact en vervolg



Infrastructuur verstoord

De centrale communicatie-infrastructuur van NoName057(16) werd zwaar beschadigd, waardoor hun vermogen om gecoördineerde aanvallen uit te voeren aanzienlijk is verminderd.



Most Wanted-lijst

De kernleden van de groep zijn op de EU Most Wanted-lijst geplaatst, wat de internationale samenwerking bij het opsporen en vervolgen van deze individuen versterkt.



Toekomstige dreigingen

Hoewel de groep momenteel ernstig verzwakt is, blijft het risico bestaan dat ze hun activiteiten hervatten onder een nieuwe naam of structuur, wat voortdurende waakzaamheid vereist.

Conclusie: Wat betekent dit?

Significante overwinning

Operatie Eastwood vertegenwoordigt een grote klap voor pro-Russische cyberoperaties in Europa en toont aan dat internationale samenwerking effectief kan zijn tegen staatsgesponsorde cyberaanvallen.

Lessen voor de toekomst

Het succes van deze operatie benadrukt het belang van snelle, gecoördineerde actie en informatie-uitwisseling tussen landen bij het bestrijden van cyberdreigingen.

Blijvende waakzaamheid

Ondanks dit succes blijft voortdurende internationale digitale waakzaamheid essentieel, aangezien nieuwe pro-Russische hackersgroepen kunnen opkomen om het vacuüm te vullen dat NoName057(16) achterlaat.





Opvouwbare smartphones: beloofde toekomst of gefaalde hype?

De revolutie van opvouwbare smartphones werd met veel bombarie aangekondigd. Deze innovatieve technologie zou de manier waarop we onze mobiele apparaten gebruiken volledig transformeren.

Mediakanalen voorspelden een grote omwenteling in de smartphone-industrie, maar jaren later lijkt de realiteit anders uit te pakken dan verwacht.

VEILIGDIGITAAL.COM

Wat werd er beloofd?

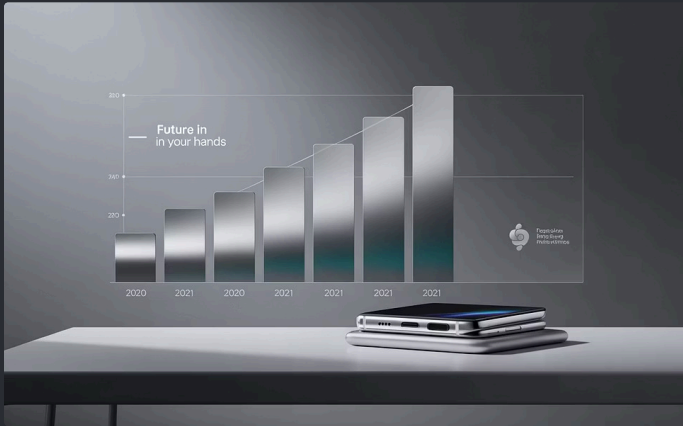
De belofte van opvouwbare smartphones was meeslepend: toestellen die naadloos konden transformeren van een compacte telefoon naar een volwaardige tablet. Fabrikanten beloofden ons het beste van twee werelden - een groter scherm voor productiviteit en entertainment, zonder de ongemakkelijke omvang van een tablet in onze zakken.

Het concept was revolutionair: waarom twee apparaten dragen als één apparaat beide functies kan vervullen? De mogelijkheden voor multitasking en een verbeterde gebruikerservaring leken eindeloos.



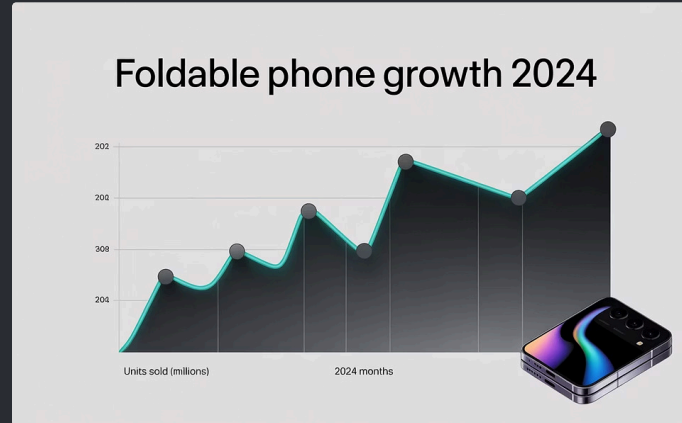
De opvouwbare technologie beloofde meer schermruimte voor werken, gamen en videostreaming zonder compromissen op gebied van draagbaarheid.

Feiten & verkoopcijfers wereldwijd



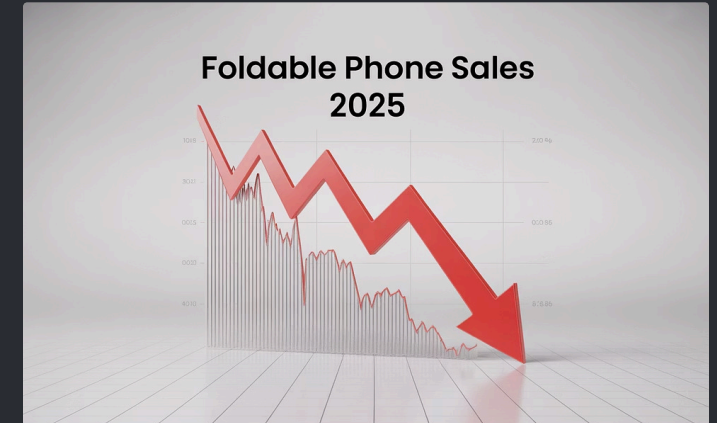
Initiële Groei (2021)

In 2021 verkocht Samsung wereldwijd vier keer meer opvouwbare smartphones dan in 2020, wat aanvankelijk een veelbelovende groei leek.



Vertraagde Groei (2024)

De huidige groei is beduidend vertraagd, met slechts een kleine toename in de wereldwijde verkoop van opvouwbare toestellen.



Verwachte Daling (2025)

Analisten voorspellen voor het eerst een negatieve groei in de markt van opvouwbare smartphones voor het komende jaar.

Hoewel de initiële verkoopcijfers hoopvol waren, lijkt de opvouwbare smartphone-markt nu tegen een plafond aan te lopen. De initiële nieuwigheid maakt plaats voor een meer kritische benadering van consumenten.

Waarom kopen mensen ze (nog) niet?



Hoge Prijzen

Vanaf €1.200 blijven opvouwbare smartphones een luxeproduct. De aanzienlijke meerprijs ten opzichte van traditionele smartphones maakt het moeilijk om de toegevoegde waarde te rechtvaardigen.



Zorgen over Duurzaamheid

De kwetsbaarheid van vouwschermen en scharnieren roept vragen op over de levensduur. Consumenten zijn bezorgd over kreukels in het scherm en de houdbaarheid van het vouwmechanisme.



Beperkte Meerwaarde

Voor de gemiddelde gebruiker bieden opvouwbare smartphones onvoldoende unieke functionaliteiten die de hogere prijs rechtvaardigen. Het grotere scherm alleen stimuleert geen massale overstap.

Groei, stagnatie of krimp?

Klein marktaandeel

Ondanks alle media-aandacht blijven opvouwbare smartphones een nichesegment binnen de totale smartphone-markt, met een aandeel van minder dan 2% wereldwijd.

Groeivertraging

De initiële explosieve groei is getemperd tot slechts 2,9% in 2024, wat wijst op een verzadiging van de early adopter-markt.

Apple als potentiële katalysator

Apple's afwezigheid in dit segment is opmerkelijk. Hun eventuele toetreding zou als 'game changer' kunnen fungeren en de markt nieuw leven in kunnen blazen.

Future-Proof your choice

Consumentenzorgen en obstakels

Praktische bezwaren

De vrees voor dure reparaties houdt veel consumenten tegen. Een beschadigd vouwscherm kan tot €600 kosten om te vervangen - bijna de helft van de aankoopprijs van het toestel zelf.

Daarnaast zijn veel potentiële kopers bezorgd over de zichtbare vouwlijn die na verloop van tijd kan ontstaan, waardoor de premium gebruikservaring wordt aangetast.

Software-uitdagingen

De softwareoptimalisatie voor vouwbare schermen blijft achter. Veel apps zijn niet ontworpen voor het veranderende schermformaat, wat resulteert in onhandige gebruikerservaringen.

Het gebrek aan werkelijk innovatieve toepassingen die de unieke vorm benutten, maakt het moeilijk om de meerwaarde van deze toestellen te demonstreren.



Rol van merken & technologie



Samsung domineert

Met de Galaxy Z-serie is Samsung marktleider, maar ook zij zien een vertraging in de groei. De Z Fold en Z Flip-modellen vertegenwoordigen meer dan 70% van alle verkochte opvouwbare toestellen wereldwijd.



Terugtrekkende merken

OnePlus en OPPO hebben hun investeringen in opvouwbare technologie verminderd na tegenvallende verkoopresultaten. Motorola blijft wel doorzetten met hun vernieuwde Razr-serie.



Toekomstige innovatie

Verwacht wordt dat nieuwe spelers en technologische doorbraken kunnen leiden tot marktherstel. Verbeterde schermtechnologie en lagere productiekosten zouden de toegankelijkheid kunnen vergroten.

Conclusie: toekomst nog onzeker



De opvouwbare smartphone blijft een fascinerend concept dat de grenzen van mobiele technologie verlegt, maar de weg naar mainstream acceptatie is langer en hobbelig dan aanvankelijk voorspeld.

Overzicht van de Beste Gratis Scam Detectors voor Je Mobiele Telefoon

Welkom bij deze uitgebreide gids over gratis scam detectors voor je smartphone. We focussen op toegankelijke beveiligingsapps voor Android die je beschermen tegen oplichting via sms, e-mail, apps en webbrowsers.

Dit artikel helpt je de juiste tools te vinden om je digitale leven veiliger te maken zonder daarvoor te hoeven betalen.

by VEILIGDIGITAAL.COM



Het Groeiende Probleem van Mobiele Scams

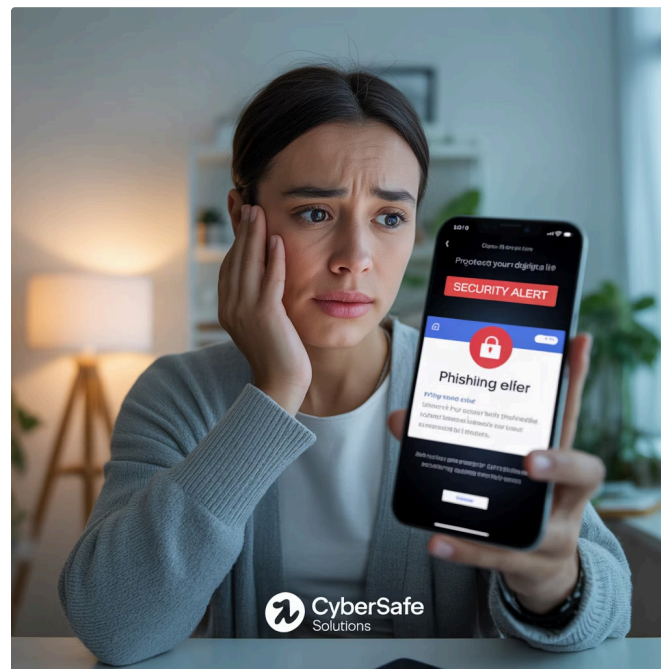
De bedreiging van mobiele oplichting neemt in hoog tempo toe.

Uit recent onderzoek blijkt dat maar liefst 71% van alle cyberaanvallen in 2024 gericht is op mobiele apparaten.

Cybercriminelen worden steeds creatiever in hun aanpak.

We zien vooral een zorgwekkende toename in:

- Geavanceerde phishing-aanvallen die legitieme websites nabootsen
- Sms-fraude (smishing) met misleidende berichten over pakketten of bankzaken
- Kwaadaardige apps die zich voordoen als nuttige tools
- Malware die persoonlijke gegevens steelt



Waarom Een Scam Detector Gebruiken?



Bescherming van Gevoelige Gegevens

Scam detectors bewaken je wachtwoorden, bankgegevens en persoonlijke informatie. Ze voorkomen dat deze in verkeerde handen vallen door verdachte activiteiten vroegtijdig te signaleren.



Signalering van Gevaarlijke Links

Deze apps analyseren links in berichten, e-mails en websites om phishing-pogingen te identificeren voordat je erop klikt, waardoor je beschermd blijft tegen frauduleuze websites.



Automatische Waarschuwingen

Ontvang directe meldingen wanneer een app verdachte activiteiten detecteert, zoals bekende scampatronen of pogingen om toegang te krijgen tot gevoelige informatie op je telefoon.

Top Gratis Scam Detector Apps: Overzicht

Bitdefender Mobile Security

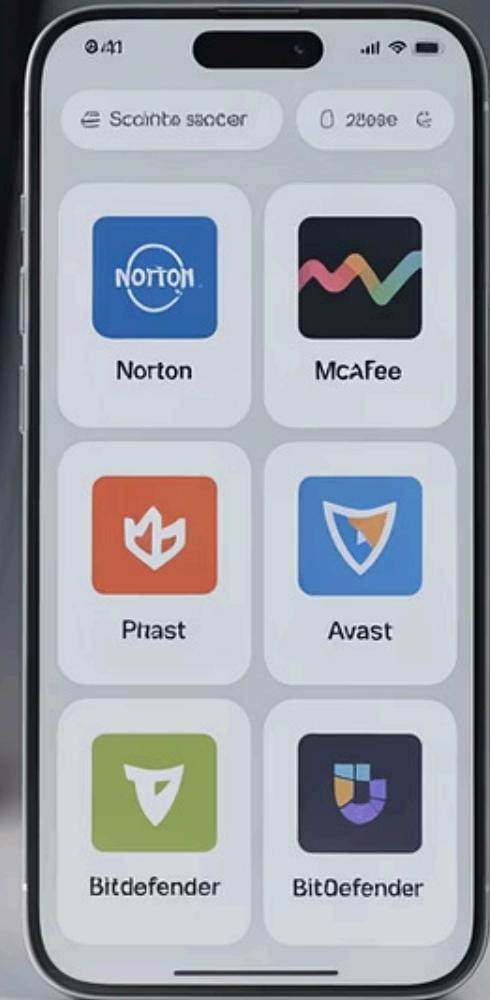
Biedt een krachtige gratis basisversie met uitstekende bescherming tegen phishing en scams. Bekend om zijn minimale impact op batterijduur en systeemprestaties.

TotalAV Mobile Security

Een veelzijdig gratis beveiligingspakket met gebruiksvriendelijke interface. Uitstekend voor beginners met weinig technische kennis maar met behoefte aan degelijke bescherming.

Andere Noemenswaardige Apps

Lookout, AVG en Avast bieden ook degelijke gratis versies met verschillende sterke punten, van anti-diefstal tot geavanceerde scanmogelijkheden.



Bitdefender Mobile Security: Sterk in Scamdetectie



Uitblinker in Real-time Bescherming

- Geavanceerde webbescherming die gevaarlijke websites blokkeert voordat je ze bezoekt
- Intelligente analyse van berichten en notificaties om verdachte links te identificeren
- Real-time scam alerts bij verdachte activiteiten
- Minimale impact op batterijduur (minder dan 2%)

De gratis versie biedt basisbescherming, waaronder een volledige netwerk-scan die kwetsbaarheden in je Wi-Fi-verbinding opspoot en een anti-phishing module die je beschermt tegen de meest voorkomende online oplichting.

TotalAV Mobile Security: Gebruiksvriendelijk en Compleet



Intuïtieve Interface

Speciaal ontworpen voor gebruikers zonder technische achtergrond. Duidelijke, eenvoudige navigatie en begrijpelijke beveiligingsrapporten maken deze app toegankelijk voor iedereen.



Veilige Browser & Wi-Fi Scanner

De ingebouwde veilige browser blokkeert schadelijke websites en advertenties. De Wi-Fi checker waarschuwt je wanneer je verbonden bent met een onveilig netwerk dat kwetsbaar is voor man-in-the-middle aanvallen.



Datalek Scanner

Controleert of je e-mailadres voorkomt in bekende datalekken. Als je gegevens zijn gelekt, krijg je direct advies over welke wachtwoorden je moet wijzigen om je accounts te beveiligen.

Zelfs zonder premium-abonnement biedt TotalAV een verrassend complete set functies die de meeste gebruikers voldoende bescherming bieden tegen alledaagse scams en bedreigingen.

Andere Gratis Opties: Lookout, AVG, Avast

App	Sterke Punten	Beperkingen
Lookout	Uitstekende diefstalbescherming met locatietracking, effectieve detectie van rootkits en systeemwijzigingen	Beperkte scamdetectie in gratis versie, sommige beveiligingsfuncties vereisen premium
AVG	Betrouwbare basis malware- en phishingbescherming, app vergrendeling, foto kluis voor privéfoto's	Advertenties in gratis versie, minder geavanceerde real-time bescherming
Avast	Krachtige virusscanner, netwerkscan voor Wi-Fi-kwetsbaarheden, anti-phishing bescherming	Zwaarder voor systeembronnen, kan telefoon vertragen op oudere modellen

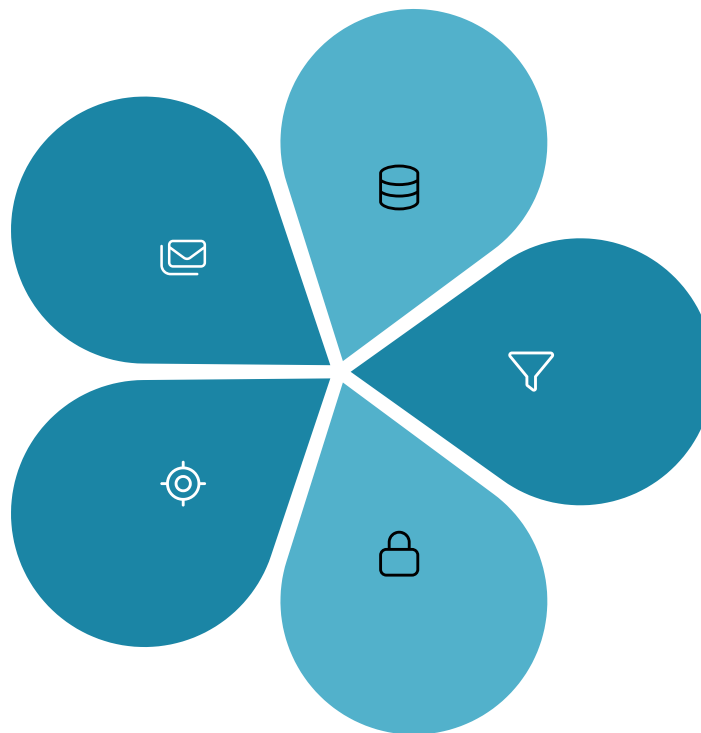
Belangrijkste Functies om te Vergelijken

Real-time Waarschuwingen

Directe notificaties bij detectie van phishing, sms-fraude of andere scampogingen, zodat je meteen kunt reageren.

Anti-diefstal

Functionaliteit om je telefoon te lokaliseren, vergrendelen of op afstand te wissen als deze wordt gestolen.



Databescherming

Monitoring van persoonlijke gegevens en waarschuwingen bij datalekken waarin je informatie is aangetroffen.

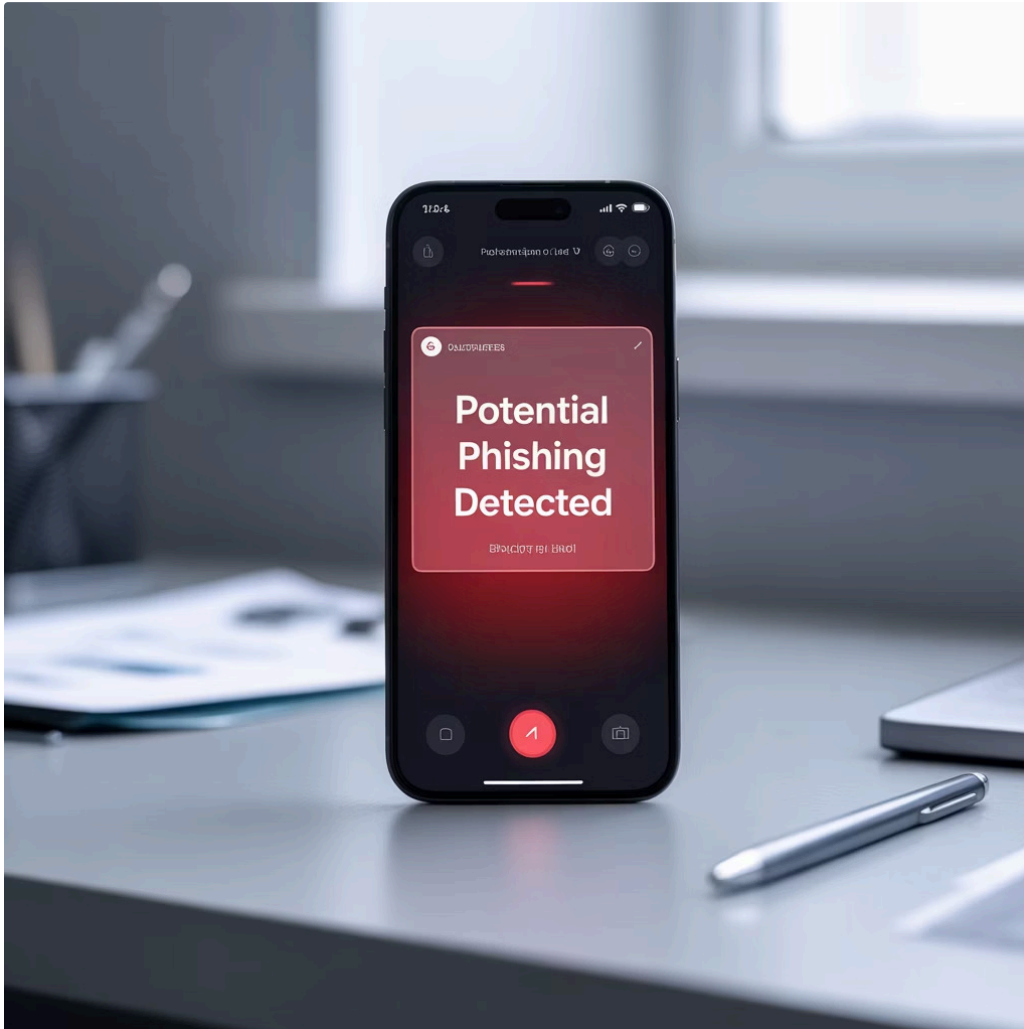
Web Filtering

Veilige browsers en filteroplossingen die schadelijke websites blokkeren en onveilige downloads tegenhouden.

App Controle

Mogelijkheid om onbekende apps te blokkeren en bestaande apps te scannen op verdacht gedrag of malware.

Gebruiksvoorbeelden: Herkenning en Waarschuwing



In onafhankelijke tests blijkt dat Bitdefender 100% van de geteste web scams detecteert en blokkeert, wat aanzienlijk beter is dan het industriegemiddelde van 94%.

TotalAV onderscheidt zich door de snelheid waarmee het datalekken identificeert - gebruikers ontvangen binnen seconden een waarschuwing wanneer hun e-mailadres in een nieuw datalek wordt aangetroffen.

Alle besproken apps tonen duidelijke en opvallende notificaties wanneer ze risicovolle links detecteren:

- Rode waarschuwingsschermen die je actief blokkeren
- Pushnotificaties die je waarschuwen voor verdachte sms-berichten
- Contextgebonden uitleg over waarom iets als scam is gemarkeerd

Conclusie:

Onze Aanbevelingen

Bitdefender voor Beste Scam Detectie

Kies Bitdefender als je prioriteit ligt bij effectieve bescherming tegen web- en berichtscams. De gratis versie biedt al uitstekende beveiliging zonder merkbare impact op je toestel.

TotalAV voor Gebruiksgemak

TotalAV is ideaal voor wie een eenvoudige interface zoekt en extra waarde hecht aan datalek-monitoring. Perfect voor minder technische gebruikers die toch volledige bescherming willen.

Belangrijke Tips

Onthoud dat geen enkele app 100% bescherming biedt. Blijf alert, update je apps regelmatig en overweeg een combinatie van beschermingsmaatregelen voor optimale veiligheid.





PerfektBlue: Bluetooth-aanval op Infotainmentsystemen

Een nieuwe, ernstige kwetsbaarheid bedreigt de infotainmentsystemen van meer dan 1,4 miljoen voertuigen wereldwijd.

Deze aanval, genaamd "PerfektBlue", richt zich specifiek op Mercedes, Volkswagen en Skoda modellen en stelt kwaadwillenden in staat om toegang te krijgen tot gevoelige voertuigsystemen via Bluetooth-verbindingen.

VEILIGDIGITAAL.COM

Hoe werkt de PerfektBlue-aanval?

De PerfektBlue-aanval maakt gebruik van een fundamentele zwakte in de Bluetooth-implementatie van MIB3-infotainmentsystemen. Wanneer de Bluetooth-functie van een voertuig is ingeschakeld, kunnen aanvallers zonder enige vorm van authenticatie toegang krijgen tot het systeem.

Deze kwetsbaarheid stelt hackers in staat om op afstanden tot 10 meter verbinding te maken met het voertuig, zelfs zonder fysieke toegang tot het voertuig zelf. Het enige wat nodig is, is dat Bluetooth is ingeschakeld - wat bij veel moderne auto's de standaardinstelling is.



Zodra de aanvaller binnen bereik komt, kan deze automatisch verbinding maken met het infotainmentsysteem zonder dat de bestuurder hiervan op de hoogte is of toestemming hoeft te geven.

Gevonden kwetsbaarheden: feiten & cijfers

12

Unieke kwetsbaarheden

Vastgesteld door onderzoeksteam
PCAutomotive in verschillende automerken en
modellen

1.4M+

Getroffen voertuigen

Wereldwijd aantal auto's met kwetsbare
infotainmentsystemen

5+

Jaren bekend

Ethische hackers waarschuwen al sinds 2018
voor vergelijkbare beveiligingsproblemen

De kwetsbaarheden zijn aangetroffen in diverse modellen van Volkswagen en Skoda, waarbij vooral het MIB3-systeem een primair doelwit vormt. Onderzoekers hebben aangetoond dat deze problemen consistent aanwezig zijn in meerdere voertuiggeneraties.

Wat kunnen hackers doen na toegang?

1

Malafide code uitvoeren

Hackers kunnen schadelijke code installeren die bij elke systeemstart automatisch wordt uitgevoerd, waardoor ze permanente toegang behouden tot het infotainmentsysteem.

2

Gegevens uitlezen en manipuleren

Toegang tot GPS-locaties, rijsnelheid en opgeslagen contactgegevens. Deze informatie kan worden uitgelezen of gemanipuleerd voor tracking of identiteitsfraude.

3

Audio en microfoon compromitteren

Meeluisteren via de ingebouwde microfoon van het voertuig of het audiosysteem manipuleren, wat kan leiden tot afleiding tijdens het rijden.

4

Schermen en interfaces overnemen

Screenshots maken van wat de bestuurder ziet en de inhoud van schermen wijzigen, wat potentieel gevaarlijke situaties kan veroorzaken.

Demo's en reactie autofabrikanten



Onderzoekers hebben een live demonstratie uitgevoerd op een Skoda Superb III, waarbij ze volledige controle over het infotainmentsysteem verkregen zonder fysieke toegang tot het voertuig.

"De aanval geeft geen toegang tot kritieke rijfuncties zoals stuur, gas of rem. Het blijft beperkt tot het infotainmentsysteem."

Reactie van fabrikanten:

- Volkswagen en Skoda beweren de kwetsbaarheden te hebben verholpen via software-updates
- Mercedes onderzoekt nog in hoeverre hun systemen getroffen zijn
- Experts twifelen of alle problemen daadwerkelijk zijn opgelost

Conclusie & aanbevelingen

Groeiende aanvalsvector

Moderne infotainmentsystemen vormen een steeds aantrekkelijker doelwit voor hackers door de toenemende connectiviteit en functionaliteit. De PerfektBlue-aanval laat zien dat zelfs grote autofabrikanten kwetsbaar blijven.

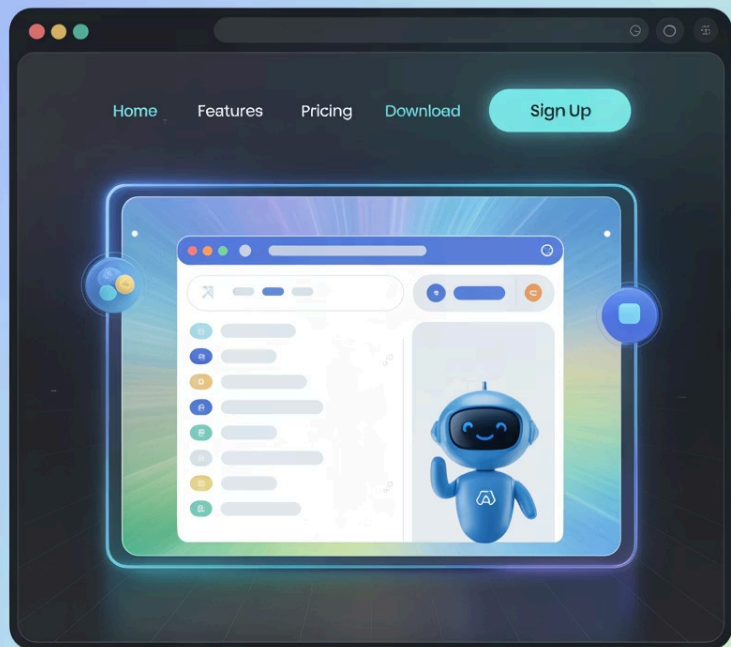
Fabrikantverantwoordelijkheid

Autofabrikanten moeten prioriteit geven aan cybersecurity en regelmatige updates uitbrengen. Er is behoefte aan een industriebrede standaard voor beveiligingsprotocollen in voertuigsystemen.

Gebruikersmaatregelen

Schakel Bluetooth standaard uit wanneer deze niet wordt gebruikt. Houd de software van uw infotainmentsysteem up-to-date en reageer snel op beveiligingsupdates van de fabrikant.

Naarmate auto's steeds meer verbonden raken met de digitale wereld, wordt cybersecurity een cruciale factor in de algemene veiligheid van voertuigen. De PerfektBlue-kwetsbaarheid is een wake-up call voor zowel fabrikanten als consumenten.



Perplexity's AI Comet Browser komt naar Windows

De eerste AI-gestuurde webbrower van Perplexity is binnenkort beschikbaar voor Windows-gebruikers, na de succesvolle bètalancering voor Mac in juni 2025.

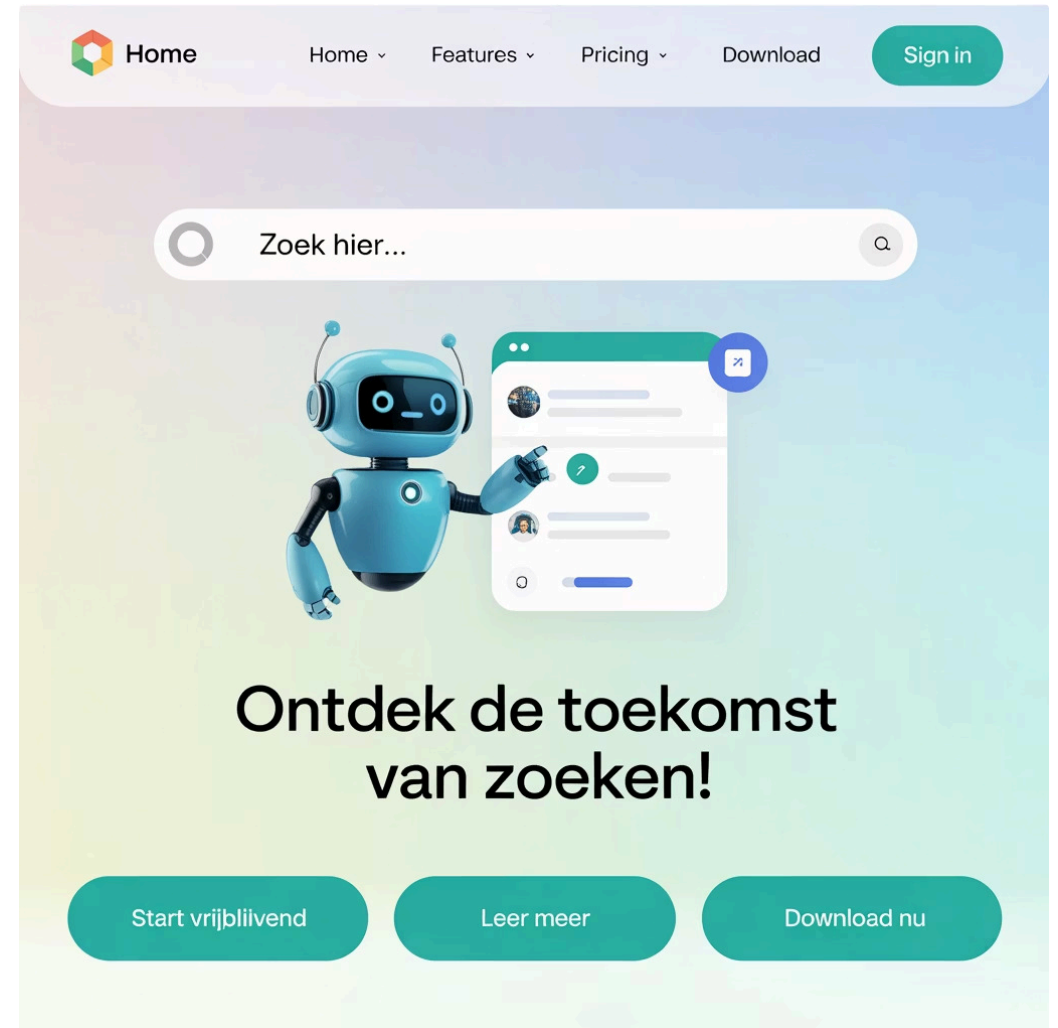
Deze innovatieve browser integreert geavanceerde AI-functionaliteiten direct in je browsingervaring.

VEILIGDIGITAAL.COM

Wat is Comet? Overzicht en Doel

Comet is een revolutionaire webbrowser die een ingebouwde AI-assistent combineert met traditionele browserfunctionaliteiten. Na de succesvolle bètalancering voor Mac-gebruikers met Apple Silicon, maakt Perplexity zich nu op voor de Windows-markt.

Het centrale concept achter Comet is "agentic search" - een slimmere, proactievere manier van zoeken die verder gaat dan gewone zoekmachines. De browser anticipeert op je behoeften en helpt je efficiënter informatie te vinden en te verwerken.



Belangrijkste AI-functies in Comet



Contextuele Antwoorden

Stel direct vragen aan je browser en ontvang intelligente, contextuele antwoorden zonder naar een aparte zoekmachine te gaan.



Automatische Kortingen

De browser scant je winkelwagen en zoekt proactief naar beschikbare kortingscodes of betere aanbiedingen.



E-mail Assistent

Vindt ongelezen e-mails en openstaande acties, waardoor je inbox beter georganiseerd blijft.

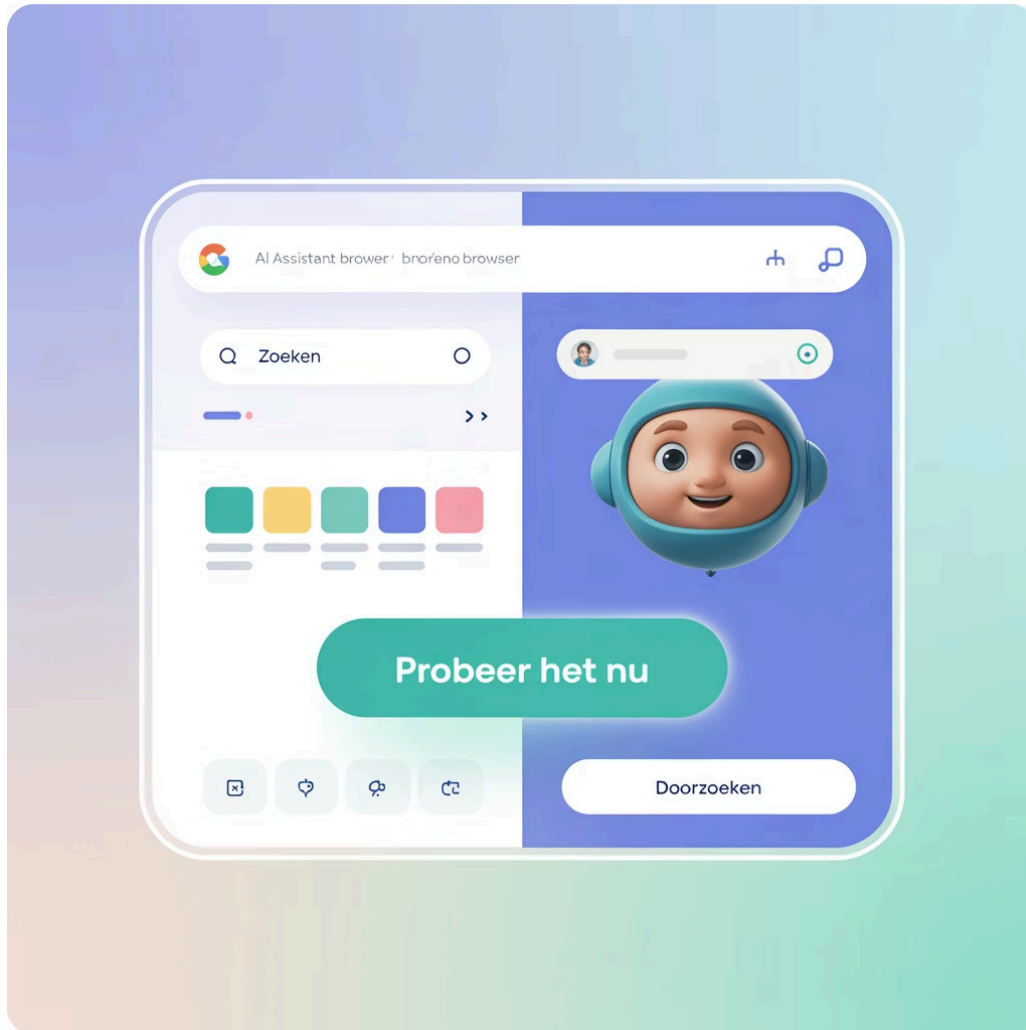


"Try-on" Functie

Upload een foto van jezelf en zie direct hoe geselecteerde kleding je zou staan, zonder fysiek te passen.



Uniek: Agentic Search en Assistent-ervaring



Nieuwe Browsing-Paradigma

Comet vervangt de traditionele zoekbalk met een intelligente assistent die je browsing-ervaring stuurt. In plaats van passief zoekresultaten te tonen, biedt Comet proactieve hulp om snel relevante antwoorden te vinden.

Deze aanpak plaatst Comet in directe concurrentie met andere innovatieve browsers zoals Opera Neon, en met AI-initiatieven van Google en OpenAI die de manier waarop we online zoeken willen herdefiniëren.

Privacy & Discussiepunten

1 Personalisatie vs. Privacy

De CEO van Perplexity suggereerde aanvankelijk het gebruik van gebruikersdata buiten de app voor personalisatie, maar heeft deze uitspraak later genuanceerd na zorgen over privacy.

2 Opt-out Mogelijkheden

Perplexity heeft beloofd dat gebruikers kunnen kiezen om niet deel te nemen aan gepersonaliseerde advertenties, wat een belangrijke stap is voor gebruikerscontrole.

3 Transparantiebelofte

Het Comet-team benadrukt hun toewijding aan transparantie over datagebruik en privacyopties voor alle gebruikers.



Vooruitblik & Impact

Uitbreiding naar Meer Platforms

Terwijl de Windows-bèta nu in testfase is, werkt Perplexity ook aan een Android-versie van Comet om hun bereik verder uit te breiden.

Houd de officiële communicatiekanalen van Perplexity in de gaten voor updates over de publieke lancering en nieuwe functionaliteiten die worden toegevoegd aan deze veelbelovende AI-browser.

Revolutie in Informatiezoeken

Comet heeft het potentieel om een gamechanger te worden in hoe mensen informatie zoeken en met AI samenwerken in hun dagelijkse online activiteiten.



Your conversations,
your privacy

End-to-end encryption you and ensure your messages stay private
retains the privacy of your messages and ensures your privacy.

Download Now

Privacyvriendelijke WhatsApp Alternatieven

WhatsApp staat onder toenemende druk vanwege privacyzorgen, waardoor steeds meer Nederlanders op zoek gaan naar veiligere alternatieven. Dit artikel biedt een uitgebreid overzicht van berichtenapps die prioriteit geven aan jouw privacy door end-to-end-encryptie en dataminimalisatie. Ontdek welke app het beste bij jouw behoeften past.

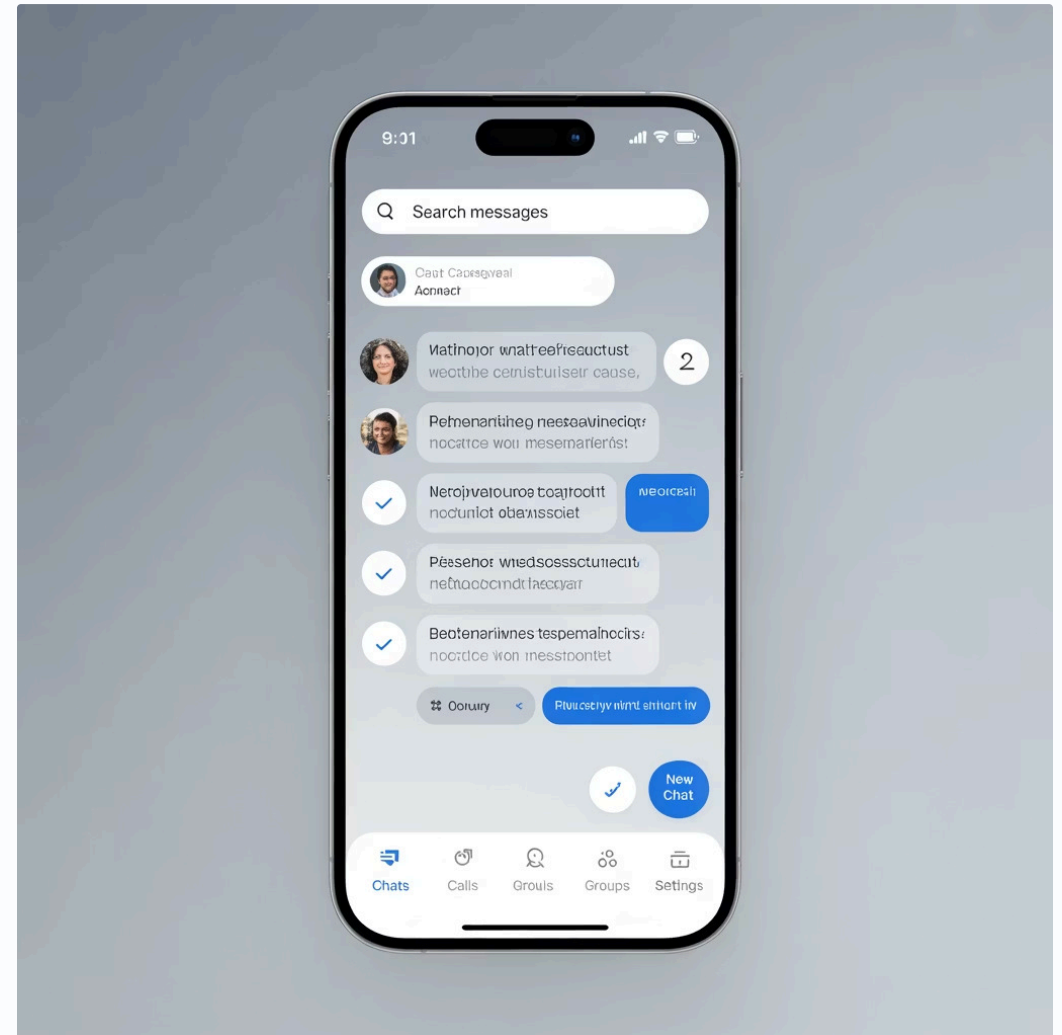
VEILIGDIGITAAL.COM

Signal: De Privacykampioen

Signal wordt alom erkend als de meest privacyvriendelijke berichtenapp op de markt. Deze app wordt beheerd door een non-profitorganisatie en is volledig open source, wat betekent dat de code door iedereen gecontroleerd kan worden op veiligheidslekken.

De app verzamelt vrijwel geen gebruikersgegevens en beperkt metadata tot het absolute minimum. Alle communicatie is standaard beschermd met end-to-end-encryptie, inclusief foto's, video's en groepsgesprekken.

Extra privacyfuncties zoals Face ID-beveiliging, verdwijnende berichten en een eenvoudige overstapprocedure vanuit WhatsApp maken Signal tot de eerste keuze voor privacybewuste gebruikers.



Telegram: Snel en Gebruiksvriendelijk



Wereldwijde Populariteit

Telegram heeft meer dan 700 miljoen gebruikers wereldwijd en staat bekend om zijn snelheid en gebruiksvriendelijkheid. Dit maakt het gemakkelijker om vrienden en familie over te halen ook over te stappen.



Beperkingen

Reguliere chats worden niet standaard end-to-end versleuteld, wat een belangrijke beperking is ten opzichte van Signal. Alleen de 'geheime chats' bieden volledige encryptie.

Telegram slaat een goed evenwicht tussen gebruiksgemak en privacy, maar is minder strikt dan Signal in het standaard toepassen van encryptie.



Privacyfuncties

Je kunt je telefoonnummer verbergen voor andere gebruikers en gebruik maken van geheime chats met end-to-end-encryptie. Zelfvernietigende berichten en de mogelijkheid om verzonden berichten te wissen bieden extra privacy.





Your data. Your control

Download Now

9:07



Threema: Maximale Anonimiteit

"Threema biedt het hoogste niveau van privacy zonder compromissen, tegen een kleine eenmalige betaling."

Volledige Anonimiteit

Threema vereist geen telefoonnummer of e-mailadres. Je krijgt een unieke Threema-ID waarmee anderen je kunnen vinden, zonder persoonlijke gegevens prijs te geven.

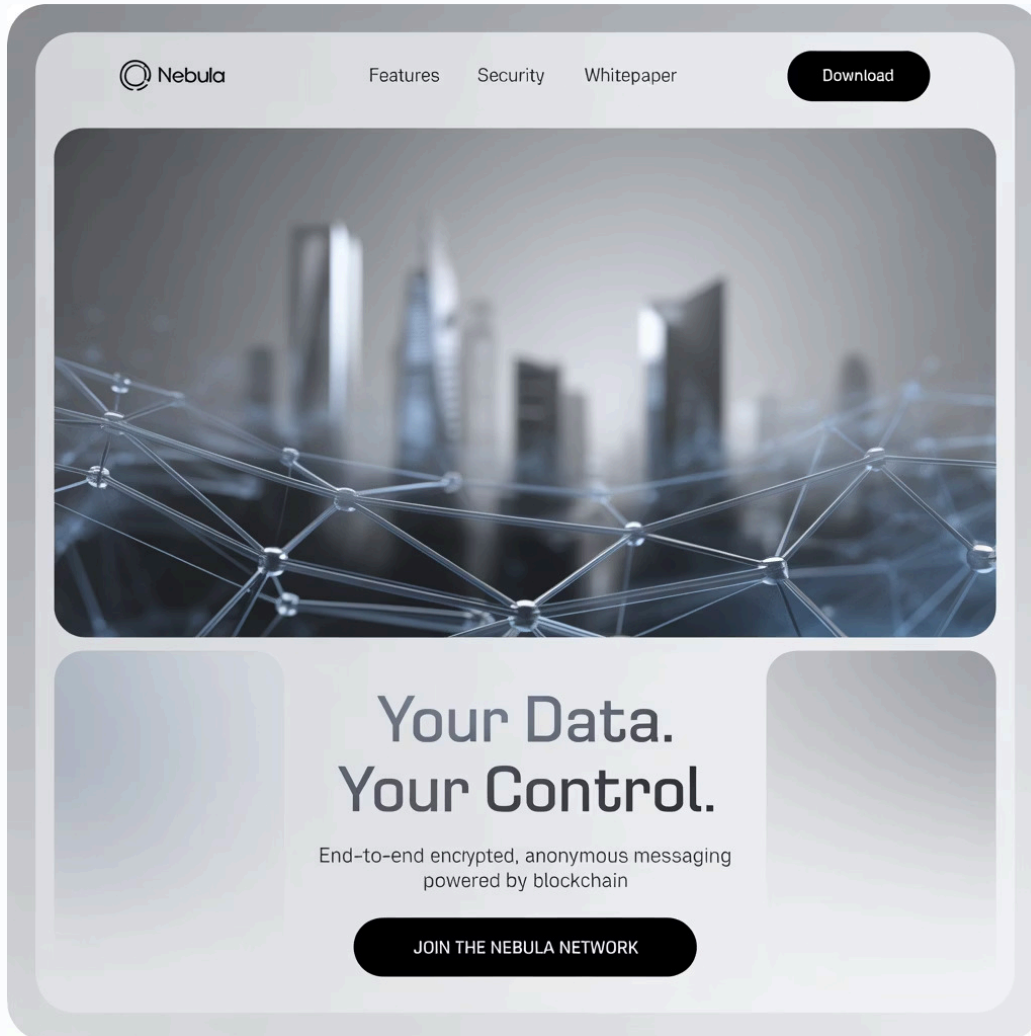
Zwitserse Kwaliteit en Veiligheid

De app wordt gehost op Zwitserse servers en valt onder de strenge Zwitserse privacywetgeving. Alle aspecten van de communicatie zijn end-to-end versleuteld, inclusief statusberichten, groepschats en zelfs spraakgesprekken.

Betaalde Service

Threema kost eenmalig €2,99, wat sommige gebruikers kan afschrikken. Het betekent wel dat er geen advertenties of dataverkoop nodig zijn om de dienst te financieren.

Session: Decentraal en Volledig Anoniem



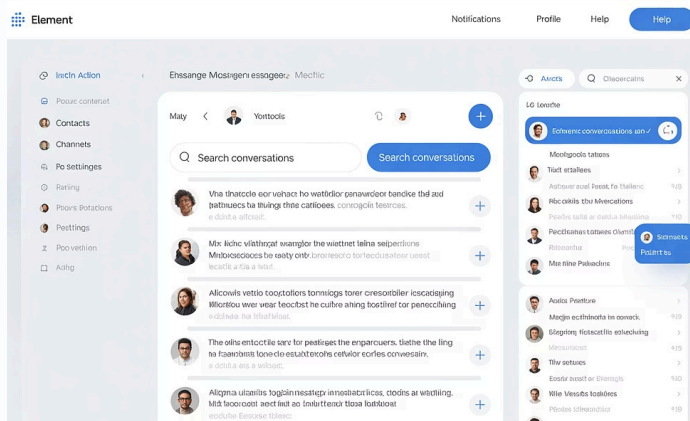
Revolutionaire Privacybescherming

Session is een relatief nieuwe speler die privacy naar een volledig nieuw niveau tilt:

- Geen telefoonnummer, e-mail of persoonlijke gegevens vereist
- Volledig open source en transparant
- Gebouwd op innovatieve blockchaintechnologie
- Gedecentraliseerd netwerk zonder centrale servers die kunnen worden gehackt
- Onion-routing principe (vergelijkbaar met Tor) maakt berichten onmogelijk te traceren

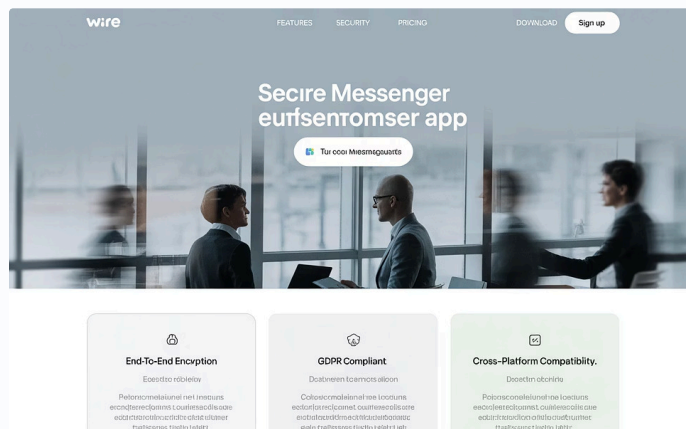
Session is ideaal voor gebruikers die maximale anonimiteit zoeken zonder compromissen.

Andere privacygerichte opties



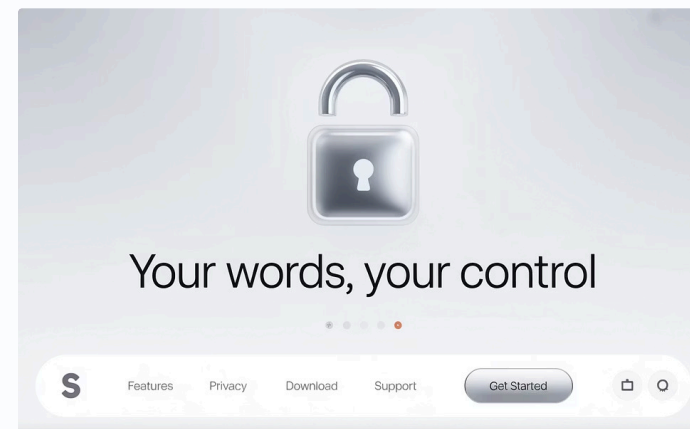
Element

Gebouwd op het open Matrix-protocol, waarmee je kunt chatten via eigen servers. Ideaal voor teams die hun communicatie volledig willen beheren. Biedt end-to-end-encryptie en volledige controle over je gegevens.



Wire

Een Europese oplossing die volledig voldoet aan de GDPR. Wire is open source, biedt end-to-end-encryptie en is beschikbaar voor alle platformen. Populair onder professionals en bedrijven die waarde hechten aan privacy.



Surespot

Een minimalistische app die zich volledig richt op versleutelde communicatie. Surespot is gratis, anoniem te gebruiken en heeft een eenvoudige interface. Perfect voor wie een no-nonsense privacyoplossing zoekt.

Praktisch Vergelijk: Belangrijke Kenmerken



Signal

- Telefoonnummer nodig: Ja
- Open source: Ja
- End-to-end encryptie: Ja
- Gratis: Ja



Telegram

- Telefoonnummer nodig: Nee (optioneel)
- Open source: Gedeeltelijk
- End-to-end encryptie: Alleen geheime chats
- Gratis: Ja



Threema

- Telefoonnummer nodig: Nee
- Open source: Ja
- End-to-end encryptie: Ja
- Gratis: Nee (€2,99)



Session

- Telefoonnummer nodig: Nee
- Open source: Ja
- End-to-end encryptie: Ja
- Gratis: Ja

De keuze voor een app hangt af van je persoonlijke voorkeuren en behoeften. Overweeg naast privacy ook gebruiksgemak, beschikbaarheid in je sociale kring, en extra functies die voor jou belangrijk zijn.

Zelfs de meest privacyvriendelijke app kan geen volledige bescherming bieden als je toestel zelf gecompromitteerd is. Houd je besturingssysteem en apps altijd up-to-date.



Conclusie: Welke past bij jou?

Voor Maximale Privacy

Signal en Threema bieden de meest robuuste bescherming. Signal is gratis maar vereist een telefoonnummer, terwijl Threema betaald is maar volledige anonimiteit biedt.

Voor Volledige Anonimiteit

Session en Threema maken het mogelijk om te communiceren zonder je identiteit prijs te geven. Perfect voor journalisten, activisten of iedereen die anoniem wil blijven.

Voor Grote Groepen en Functionaliteit

Telegram biedt meer functies en ondersteuning voor grote groepen, maar met beperkingen op het gebied van standaard encryptie. Activeer altijd geheime chats voor gevoelige gesprekken.

Onthoud dat de meest privacyvriendelijke app nutteloos is als niemand in je netwerk deze gebruikt. Overweeg je privacy-eisen af te wegen tegen de populariteit van de app in je sociale kring. Blijf je altijd bewust van je digitale voetafdruk!



PerfektBlue: Bluetooth-aanval op Infotainmentsystemen

Een nieuwe, ernstige kwetsbaarheid bedreigt de infotainmentsystemen van meer dan 1,4 miljoen voertuigen wereldwijd.

Deze aanval, genaamd "PerfektBlue", richt zich specifiek op Mercedes, Volkswagen en Skoda modellen en stelt kwaadwillenden in staat om toegang te krijgen tot gevoelige voertuigsystemen via Bluetooth-verbindingen.

VEILIGDIGITAAL.COM

Hoe werkt de PerfektBlue-aanval?

De PerfektBlue-aanval maakt gebruik van een fundamentele zwakte in de Bluetooth-implementatie van MIB3-infotainmentsystemen. Wanneer de Bluetooth-functie van een voertuig is ingeschakeld, kunnen aanvallers zonder enige vorm van authenticatie toegang krijgen tot het systeem.

Deze kwetsbaarheid stelt hackers in staat om op afstanden tot 10 meter verbinding te maken met het voertuig, zelfs zonder fysieke toegang tot het voertuig zelf. Het enige wat nodig is, is dat Bluetooth is ingeschakeld - wat bij veel moderne auto's de standaardinstelling is.



Zodra de aanvaller binnen bereik komt, kan deze automatisch verbinding maken met het infotainmentsysteem zonder dat de bestuurder hiervan op de hoogte is of toestemming hoeft te geven.

Gevonden kwetsbaarheden: feiten & cijfers

12

Unieke kwetsbaarheden

Vastgesteld door onderzoeksteam
PCAutomotive in verschillende automerken en
modellen

1.4M+

Getroffen voertuigen

Wereldwijd aantal auto's met kwetsbare
infotainmentsystemen

5+

Jaren bekend

Ethische hackers waarschuwen al sinds 2018
voor vergelijkbare beveiligingsproblemen

De kwetsbaarheden zijn aangetroffen in diverse modellen van Volkswagen en Skoda, waarbij vooral het MIB3-systeem een primair doelwit vormt. Onderzoekers hebben aangetoond dat deze problemen consistent aanwezig zijn in meerdere voertuiggeneraties.

Wat kunnen hackers doen na toegang?

1

Malafide code uitvoeren

Hackers kunnen schadelijke code installeren die bij elke systeemstart automatisch wordt uitgevoerd, waardoor ze permanente toegang behouden tot het infotainmentsysteem.

2

Gegevens uitlezen en manipuleren

Toegang tot GPS-locaties, rijsnelheid en opgeslagen contactgegevens. Deze informatie kan worden uitgelezen of gemanipuleerd voor tracking of identiteitsfraude.

3

Audio en microfoon compromitteren

Meeluisteren via de ingebouwde microfoon van het voertuig of het audiosysteem manipuleren, wat kan leiden tot afleiding tijdens het rijden.

4

Schermen en interfaces overnemen

Screenshots maken van wat de bestuurder ziet en de inhoud van schermen wijzigen, wat potentieel gevaarlijke situaties kan veroorzaken.

Demo's en reactie autofabrikanten



Onderzoekers hebben een live demonstratie uitgevoerd op een Skoda Superb III, waarbij ze volledige controle over het infotainmentsysteem verkregen zonder fysieke toegang tot het voertuig.

"De aanval geeft geen toegang tot kritieke rijfuncties zoals stuur, gas of rem. Het blijft beperkt tot het infotainmentsysteem."

Reactie van fabrikanten:

- Volkswagen en Skoda beweren de kwetsbaarheden te hebben verholpen via software-updates
- Mercedes onderzoekt nog in hoeverre hun systemen getroffen zijn
- Experts twifelen of alle problemen daadwerkelijk zijn opgelost

Conclusie & aanbevelingen

Groeiende aanvalsvector

Moderne infotainmentsystemen vormen een steeds aantrekkelijker doelwit voor hackers door de toenemende connectiviteit en functionaliteit. De PerfektBlue-aanval laat zien dat zelfs grote autofabrikanten kwetsbaar blijven.

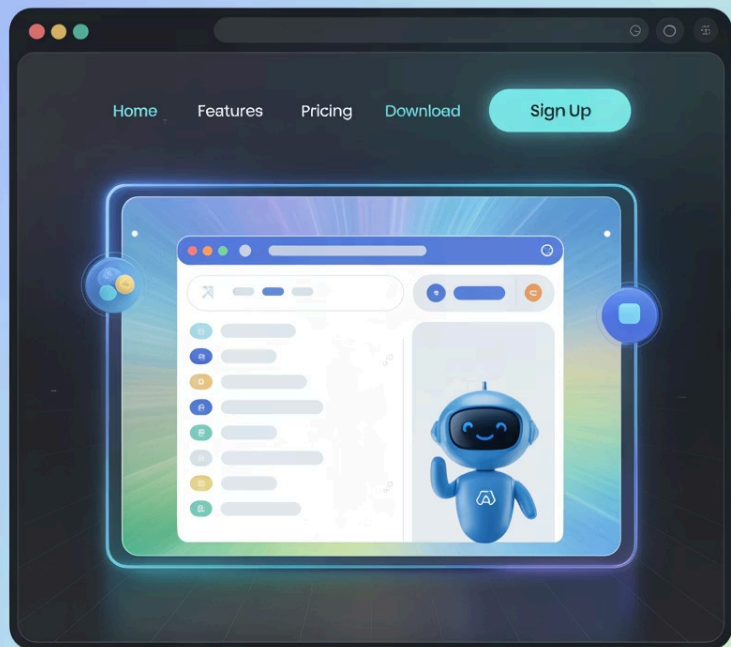
Fabrikantverantwoordelijkheid

Autofabrikanten moeten prioriteit geven aan cybersecurity en regelmatige updates uitbrengen. Er is behoefte aan een industriebrede standaard voor beveiligingsprotocollen in voertuigsystemen.

Gebruikersmaatregelen

Schakel Bluetooth standaard uit wanneer deze niet wordt gebruikt. Houd de software van uw infotainmentsysteem up-to-date en reageer snel op beveiligingsupdates van de fabrikant.

Naarmate auto's steeds meer verbonden raken met de digitale wereld, wordt cybersecurity een cruciale factor in de algemene veiligheid van voertuigen. De PerfektBlue-kwetsbaarheid is een wake-up call voor zowel fabrikanten als consumenten.



Perplexity's AI Comet Browser komt naar Windows

De eerste AI-gestuurde webbrower van Perplexity is binnenkort beschikbaar voor Windows-gebruikers, na de succesvolle bètalancering voor Mac in juni 2025.

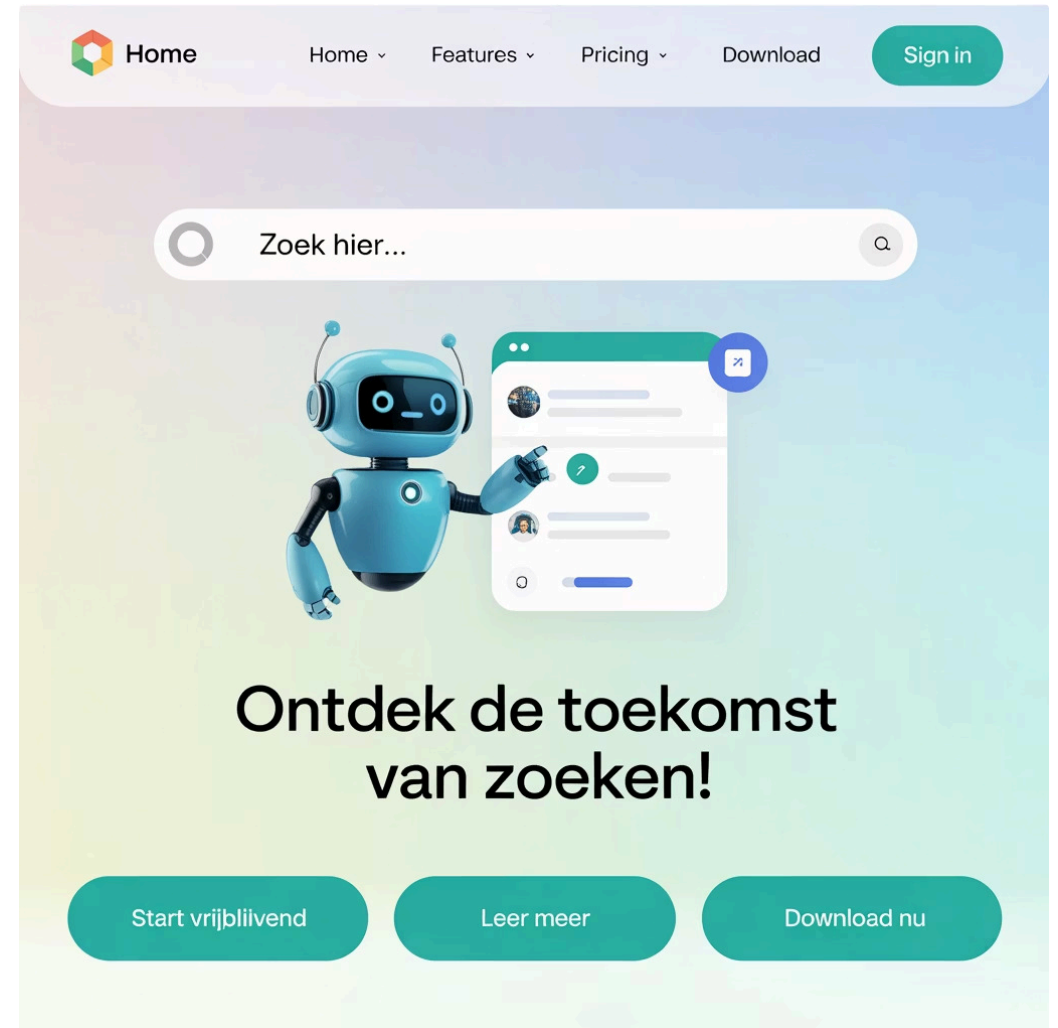
Deze innovatieve browser integreert geavanceerde AI-functionaliteiten direct in je browsingervaring.

VEILIGDIGITAAL.COM

Wat is Comet? Overzicht en Doel

Comet is een revolutionaire webbrowser die een ingebouwde AI-assistent combineert met traditionele browserfunctionaliteiten. Na de succesvolle bètalancering voor Mac-gebruikers met Apple Silicon, maakt Perplexity zich nu op voor de Windows-markt.

Het centrale concept achter Comet is "agentic search" - een slimmere, proactievere manier van zoeken die verder gaat dan gewone zoekmachines. De browser anticipeert op je behoeften en helpt je efficiënter informatie te vinden en te verwerken.



Belangrijkste AI-functies in Comet



Contextuele Antwoorden

Stel direct vragen aan je browser en ontvang intelligente, contextuele antwoorden zonder naar een aparte zoekmachine te gaan.



Automatische Kortingen

De browser scant je winkelwagen en zoekt proactief naar beschikbare kortingscodes of betere aanbiedingen.



E-mail Assistent

Vindt ongelezen e-mails en openstaande acties, waardoor je inbox beter georganiseerd blijft.

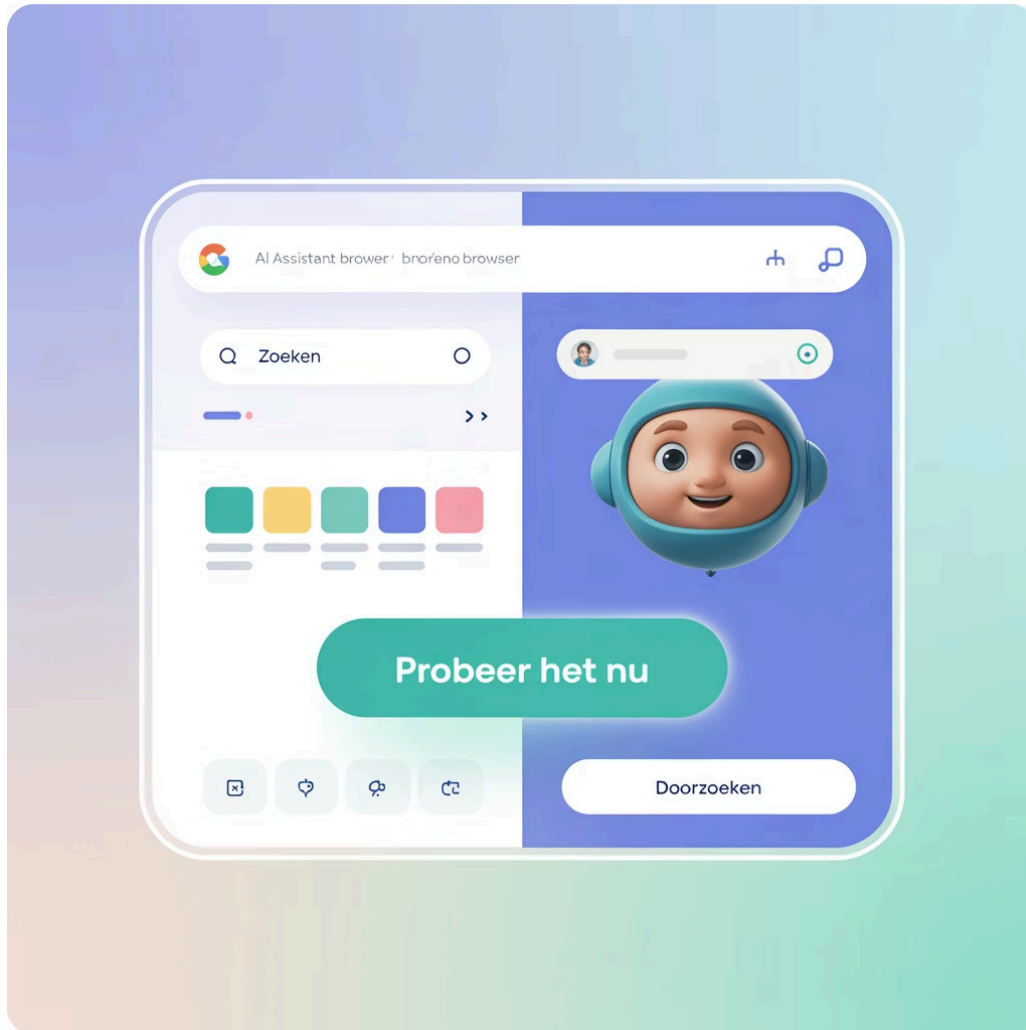


"Try-on" Functie

Upload een foto van jezelf en zie direct hoe geselecteerde kleding je zou staan, zonder fysiek te passen.



Uniek: Agentic Search en Assistent-ervaring



Nieuwe Browsing-Paradigma

Comet vervangt de traditionele zoekbalk met een intelligente assistent die je browsing-ervaring stuurt. In plaats van passief zoekresultaten te tonen, biedt Comet proactieve hulp om snel relevante antwoorden te vinden.

Deze aanpak plaatst Comet in directe concurrentie met andere innovatieve browsers zoals Opera Neon, en met AI-initiatieven van Google en OpenAI die de manier waarop we online zoeken willen herdefiniëren.

Privacy & Discussiepunten

1 Personalisatie vs. Privacy

De CEO van Perplexity suggereerde aanvankelijk het gebruik van gebruikersdata buiten de app voor personalisatie, maar heeft deze uitspraak later genuanceerd na zorgen over privacy.

2 Opt-out Mogelijkheden

Perplexity heeft beloofd dat gebruikers kunnen kiezen om niet deel te nemen aan gepersonaliseerde advertenties, wat een belangrijke stap is voor gebruikerscontrole.

3 Transparantiebelofte

Het Comet-team benadrukt hun toewijding aan transparantie over datagebruik en privacyopties voor alle gebruikers.



Vooruitblik & Impact

Uitbreiding naar Meer Platforms

Terwijl de Windows-bèta nu in testfase is, werkt Perplexity ook aan een Android-versie van Comet om hun bereik verder uit te breiden.

Houd de officiële communicatiekanalen van Perplexity in de gaten voor updates over de publieke lancering en nieuwe functionaliteiten die worden toegevoegd aan deze veelbelovende AI-browser.

Revolutie in Informatiezoeken

Comet heeft het potentieel om een gamechanger te worden in hoe mensen informatie zoeken en met AI samenwerken in hun dagelijkse online activiteiten.



Your conversations,
your privacy

End-to-end encryption you and ensure your messages stay private
retains the privacy of your messages and ensures your privacy.

Download Now

Privacyvriendelijke WhatsApp Alternatieven

WhatsApp staat onder toenemende druk vanwege privacyzorgen, waardoor steeds meer Nederlanders op zoek gaan naar veiligere alternatieven. Dit artikel biedt een uitgebreid overzicht van berichtenapps die prioriteit geven aan jouw privacy door end-to-end-encryptie en dataminimalisatie. Ontdek welke app het beste bij jouw behoeften past.

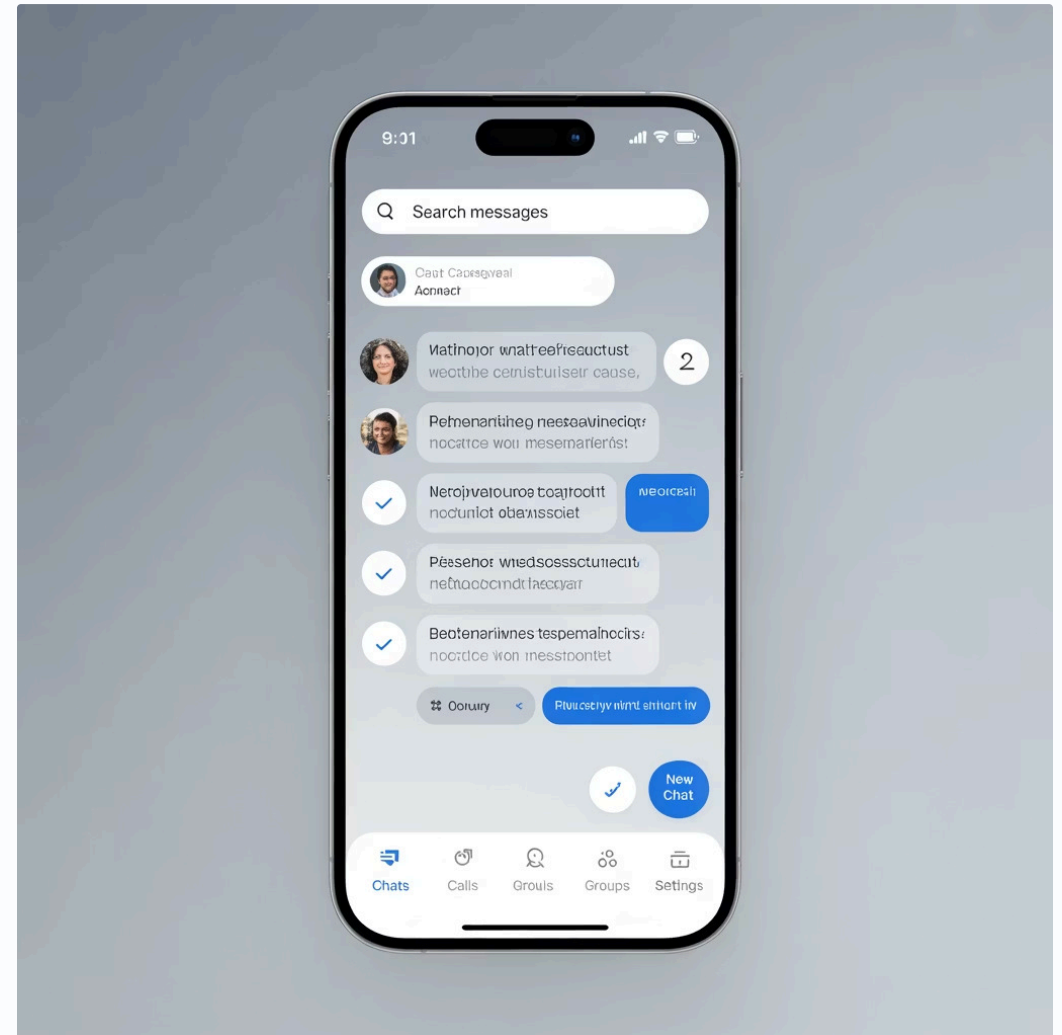
VEILIGDIGITAAL.COM

Signal: De Privacykampioen

Signal wordt alom erkend als de meest privacyvriendelijke berichtenapp op de markt. Deze app wordt beheerd door een non-profitorganisatie en is volledig open source, wat betekent dat de code door iedereen gecontroleerd kan worden op veiligheidslekken.

De app verzamelt vrijwel geen gebruikersgegevens en beperkt metadata tot het absolute minimum. Alle communicatie is standaard beschermd met end-to-end-encryptie, inclusief foto's, video's en groepsgesprekken.

Extra privacyfuncties zoals Face ID-beveiliging, verdwijnende berichten en een eenvoudige overstapprocedure vanuit WhatsApp maken Signal tot de eerste keuze voor privacybewuste gebruikers.



Telegram: Snel en Gebruiksvriendelijk



Wereldwijde Populariteit

Telegram heeft meer dan 700 miljoen gebruikers wereldwijd en staat bekend om zijn snelheid en gebruiksvriendelijkheid. Dit maakt het gemakkelijker om vrienden en familie over te halen ook over te stappen.



Beperkingen

Reguliere chats worden niet standaard end-to-end versleuteld, wat een belangrijke beperking is ten opzichte van Signal. Alleen de 'geheime chats' bieden volledige encryptie.

Telegram slaat een goed evenwicht tussen gebruiksgemak en privacy, maar is minder strikt dan Signal in het standaard toepassen van encryptie.



Privacyfuncties

Je kunt je telefoonnummer verbergen voor andere gebruikers en gebruik maken van geheime chats met end-to-end-encryptie. Zelfvernietigende berichten en de mogelijkheid om verzonden berichten te wissen bieden extra privacy.





Your data. Your control

Download Now

9:07



Threema: Maximale Anonimiteit

"Threema biedt het hoogste niveau van privacy zonder compromissen, tegen een kleine eenmalige betaling."

Volledige Anonimiteit

Threema vereist geen telefoonnummer of e-mailadres. Je krijgt een unieke Threema-ID waarmee anderen je kunnen vinden, zonder persoonlijke gegevens prijs te geven.

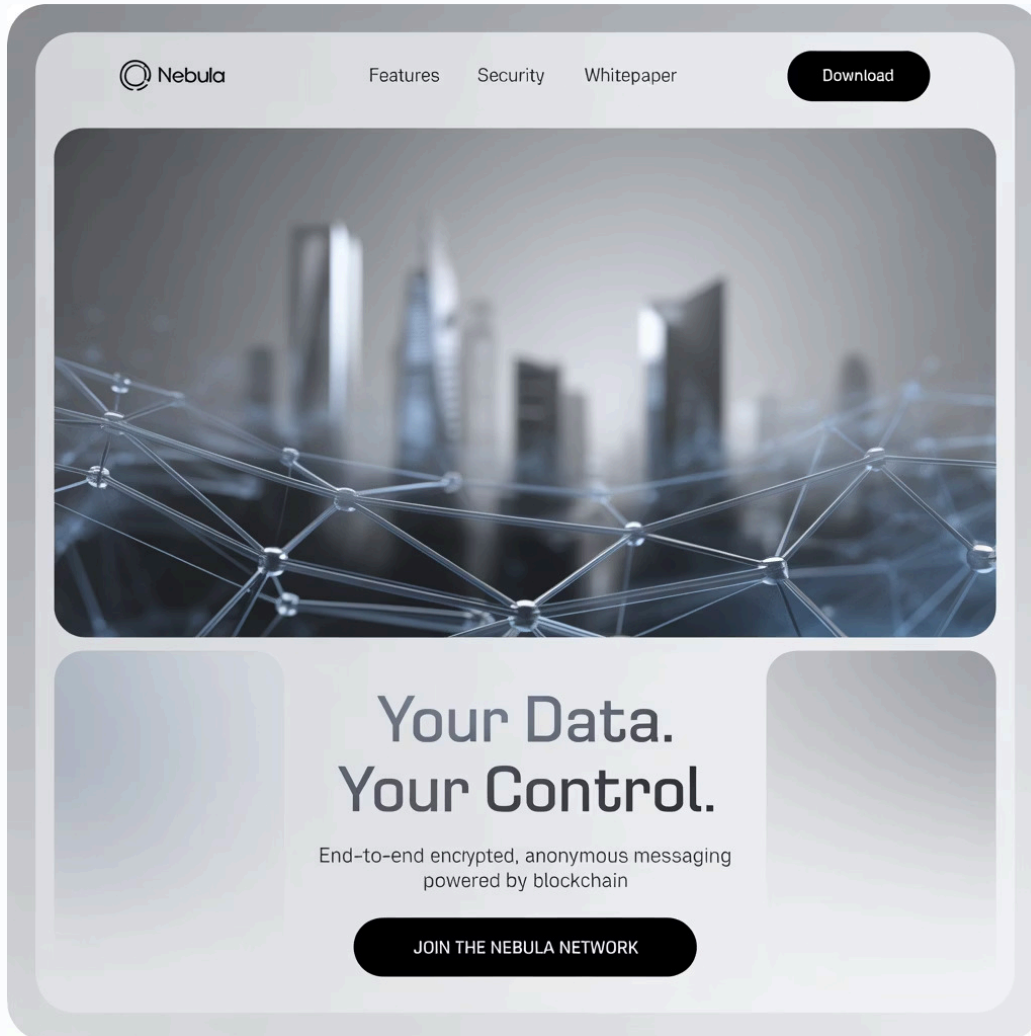
Zwitserse Kwaliteit en Veiligheid

De app wordt gehost op Zwitserse servers en valt onder de strenge Zwitserse privacywetgeving. Alle aspecten van de communicatie zijn end-to-end versleuteld, inclusief statusberichten, groepschats en zelfs spraakgesprekken.

Betaalde Service

Threema kost eenmalig €2,99, wat sommige gebruikers kan afschrikken. Het betekent wel dat er geen advertenties of dataverkoop nodig zijn om de dienst te financieren.

Session: Decentraal en Volledig Anoniem



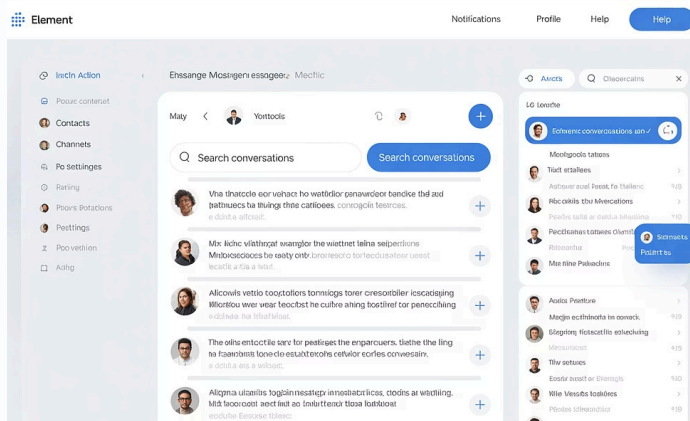
Revolutionaire Privacybescherming

Session is een relatief nieuwe speler die privacy naar een volledig nieuw niveau tilt:

- Geen telefoonnummer, e-mail of persoonlijke gegevens vereist
- Volledig open source en transparant
- Gebouwd op innovatieve blockchaintechnologie
- Gedecentraliseerd netwerk zonder centrale servers die kunnen worden gehackt
- Onion-routing principe (vergelijkbaar met Tor) maakt berichten onmogelijk te traceren

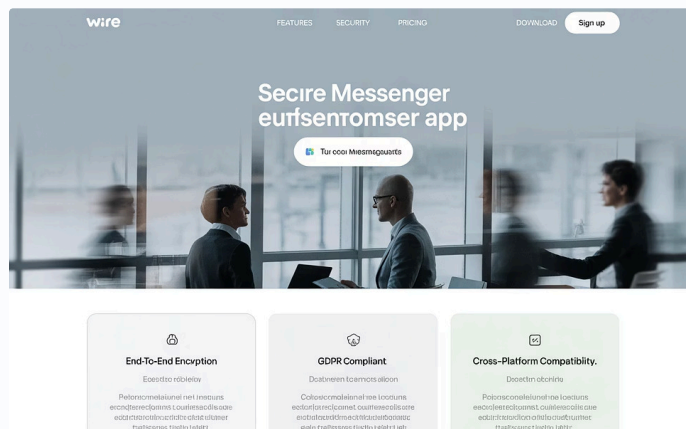
Session is ideaal voor gebruikers die maximale anonimiteit zoeken zonder compromissen.

Andere privacygerichte opties



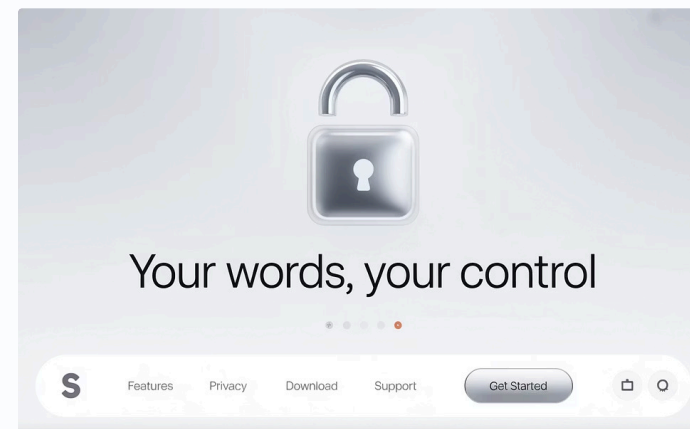
Element

Gebouwd op het open Matrix-protocol, waarmee je kunt chatten via eigen servers. Ideaal voor teams die hun communicatie volledig willen beheren. Biedt end-to-end-encryptie en volledige controle over je gegevens.



Wire

Een Europese oplossing die volledig voldoet aan de GDPR. Wire is open source, biedt end-to-end-encryptie en is beschikbaar voor alle platformen. Populair onder professionals en bedrijven die waarde hechten aan privacy.



Surespot

Een minimalistische app die zich volledig richt op versleutelde communicatie. Surespot is gratis, anoniem te gebruiken en heeft een eenvoudige interface. Perfect voor wie een no-nonsense privacyoplossing zoekt.

Praktisch Vergelijk: Belangrijke Kenmerken



Signal

- Telefoonnummer nodig: Ja
- Open source: Ja
- End-to-end encryptie: Ja
- Gratis: Ja



Telegram

- Telefoonnummer nodig: Nee (optioneel)
- Open source: Gedeeltelijk
- End-to-end encryptie: Alleen geheime chats
- Gratis: Ja



Threema

- Telefoonnummer nodig: Nee
- Open source: Ja
- End-to-end encryptie: Ja
- Gratis: Nee (€2,99)



Session

- Telefoonnummer nodig: Nee
- Open source: Ja
- End-to-end encryptie: Ja
- Gratis: Ja

De keuze voor een app hangt af van je persoonlijke voorkeuren en behoeften. Overweeg naast privacy ook gebruiksgemak, beschikbaarheid in je sociale kring, en extra functies die voor jou belangrijk zijn.

Zelfs de meest privacyvriendelijke app kan geen volledige bescherming bieden als je toestel zelf gecompromitteerd is. Houd je besturingssysteem en apps altijd up-to-date.



Conclusie: Welke past bij jou?

Voor Maximale Privacy

Signal en Threema bieden de meest robuuste bescherming. Signal is gratis maar vereist een telefoonnummer, terwijl Threema betaald is maar volledige anonimiteit biedt.

Voor Volledige Anonimiteit

Session en Threema maken het mogelijk om te communiceren zonder je identiteit prijs te geven. Perfect voor journalisten, activisten of iedereen die anoniem wil blijven.

Voor Grote Groepen en Functionaliteit

Telegram biedt meer functies en ondersteuning voor grote groepen, maar met beperkingen op het gebied van standaard encryptie. Activeer altijd geheime chats voor gevoelige gesprekken.

Onthoud dat de meest privacyvriendelijke app nutteloos is als niemand in je netwerk deze gebruikt. Overweeg je privacy-eisen af te wegen tegen de populariteit van de app in je sociale kring. Blijf je altijd bewust van je digitale voetafdruk!

Roblox rolt video-selfie-leeftijdsschatting uit om de veiligheid van tieners te vergroten

Vanaf juli 2025 introduceert Roblox een baanbrekende AI-veiligheidsfunctie specifiek gericht op gebruikers tussen 13 en 17 jaar. Deze innovatieve technologie maakt gebruik van video-selfies om de leeftijd van tieners nauwkeuriger te bepalen, met als doel hun online ervaring veiliger te maken.

Deze maatregel zal miljoenen gebruikers wereldwijd beïnvloeden en markeert een belangrijke stap in de bescherming van jonge gamers op het populaire platform.

VEILIGDIGITAAL.COM



Waarom deze stap?

Roblox is een enorm populair platform met maar liefst 77,7 miljoen dagelijkse gebruikers, waarvan een aanzienlijk deel - ongeveer 40% - jonger is dan 12 jaar. Deze jonge demografische samenstelling brengt specifieke veiligheidsuitdagingen met zich mee.

De afgelopen jaren hebben critici herhaaldelijk vragen gesteld over de veiligheid van tieners op het platform. Online risico's zoals predatoren, pesten en blootstelling aan ongepaste content vormen reële bedreigingen voor jonge gebruikers.

Bovendien ervaren gaming- en socialemediaplatforms zoals Roblox toenemende druk van zowel bezorgde ouders als toezichthouders om de veiligheid van minderjarigen beter te waarborgen.



Protect their world.
Manage their play.





Hoe werkt video-selfie-leeftijdsschatting?

1

Video-selfie maken

Gebruikers maken een korte video-selfie rechtstreeks via de Roblox-app. Dit proces is ontworpen om laagdrempelig en gebruiksvriendelijk te zijn, zodat tieners het gemakkelijk kunnen doorlopen.

2

AI-analyse

Geavanceerde AI-technologie analyseert de video en schat de leeftijd op basis van gelaatstrekken en natuurlijke bewegingen. Het systeem is specifiek getraind om nauwkeurige schattingen te maken voor de leeftijdscategorie 13-17 jaar.

3

Verificatie en alternatieven

Deze methode is vooral gericht op tieners die nog geen geldig ID-bewijs hebben. Het dient als aanvulling op de bestaande verificatiemethoden via officiële documenten, zoals identiteitskaarten of paspoorten.

Privacy en effectiviteit

Aanvullende verificatie

De AI-leeftijdsschatting is geen volledige vervanging van reguliere ID-controle, maar een aanvullende laag van verificatie. Voor bepaalde functies zal nog steeds officiële identificatie vereist zijn.

Nauwkeurigheid

De effectiviteit in het correct inschatten van leeftijden is nog niet volledig bewezen. Roblox erkent dat het systeem continu verbeterd zal worden op basis van resultaten en feedback.

Gegevensbescherming

Er blijven vragen over welke beelden worden opgeslagen of verwijderd. Roblox belooft transparantie over datagebruik en -opslag, conform strengste privacyregels.

Ouderlijke controle

Ouders krijgen via nieuwe tools meer inzicht in de schermtijd en contacten van hun kinderen, zodat zij beter toezicht kunnen houden op online activiteiten.

Voorbeelden & extra maatregelen



Uitgebreide veiligheidsmaatregelen

- Nieuwe notificatie-instellingen die tieners waarschuwen voor potentieel onveilige interacties
- Verbeterde privacy-instellingen die standaard op het hoogste beschermingsniveau staan
- Geavanceerde schermtijdlimieten die ouders kunnen instellen
- Optie voor tieners om 'trusted connections' aan te wijzen voor minder gefilterde chatgesprekken
- Educatieve initiatieven over online veiligheid binnen het platform
- Oprichting van een Teen Council die gebruikersinspraak faciliteert

Impact & vooruitblik



Voortrekkersrol

Roblox positioneert zich als pionier in AI-veiligheidsinnovatie specifiek gericht op jongeren. Het platform zet een nieuwe standaard voor de gaming- en sociale media-industrie.



Monitoring

De effectiviteit van de nieuwe maatregelen blijft onder nauwlettend toezicht van ouders, veiligheidsexperts en toezichthoudende instanties.



Bredere impact

Als deze aanpak succesvol blijkt, kan het als voorbeeld dienen voor andere sociale platforms en gaming-omgevingen die met vergelijkbare veiligheidsuitdagingen kampen.

Door deze innovatieve leeftijdsverificatiemethode te combineren met uitgebreide veiligheidsfuncties, streeft Roblox ernaar een veiligere online omgeving te creëren waar tieners kunnen spelen, creëren en socialiseren zonder onnodige risico's.



Ruil Google in voor Proton: Waarom en Hoe?

In een wereld waar digitale privacy steeds belangrijker wordt, biedt Proton een veilig alternatief voor de alomtegenwoordige Google-diensten. Google domineert al jaren met zijn gratis producten, maar de zorgen over hoe zij omgaan met onze persoonlijke gegevens nemen toe.

Vanuit Zwitserland presenteert Proton een complete suite van privacy-gerichte alternatieven die beloven onze digitale vrijheid te beschermen.

[VEILIGDIGITAAL.COM](https://veiligdigitaal.com)

Privacy: Het Kernverschil

Google's Bedrijfsmodel

Google's verdienmodel is gebouwd op het verzamelen en monetiseren van gebruikersdata. Ze scannen uw e-mails, zoekgeschiedenis en online activiteiten om gepersonaliseerde advertenties te tonen.

De gratis diensten die Google aanbiedt worden in feite "betaald" met uw persoonlijke gegevens, die vervolgens worden verkocht aan adverteerders.

Proton's Filosofie

Proton opereert met een fundamenteel andere filosofie - een "zero-access" beleid waarbij alle gebruikersgegevens volledig versleuteld zijn. Zelfs Proton zelf kan uw data niet lezen of analyseren.

Daarnaast profiteert Proton van de strenge Zwitserse privacywetgeving, die veel meer bescherming biedt dan de Amerikaanse wetten waaronder Google valt.



Google vs Proton: Functievergelijking



E-mail

Gmail biedt veel opslagruimte en slimme functies, maar scant uw e-mails. Proton Mail beschermt uw communicatie met end-to-end encryptie en heeft een gebruiksvriendelijke interface.



Opslag

Google Drive biedt ruime opslag en naadloze integratie. Proton Drive garandeert dat al uw bestanden versleuteld zijn, zowel tijdens opslag als bij het delen.



Agenda

Google Calendar is veelzijdig en eenvoudig te delen. Proton Calendar biedt dezelfde kernfuncties, maar zonder dat iemand kan meekijken naar uw afspraken.



Extra's

Google biedt meer aanvullende diensten, maar Proton onderscheidt zich met Proton VPN, waarmee u veilig en anoniem kunt surfen zonder extra kosten.

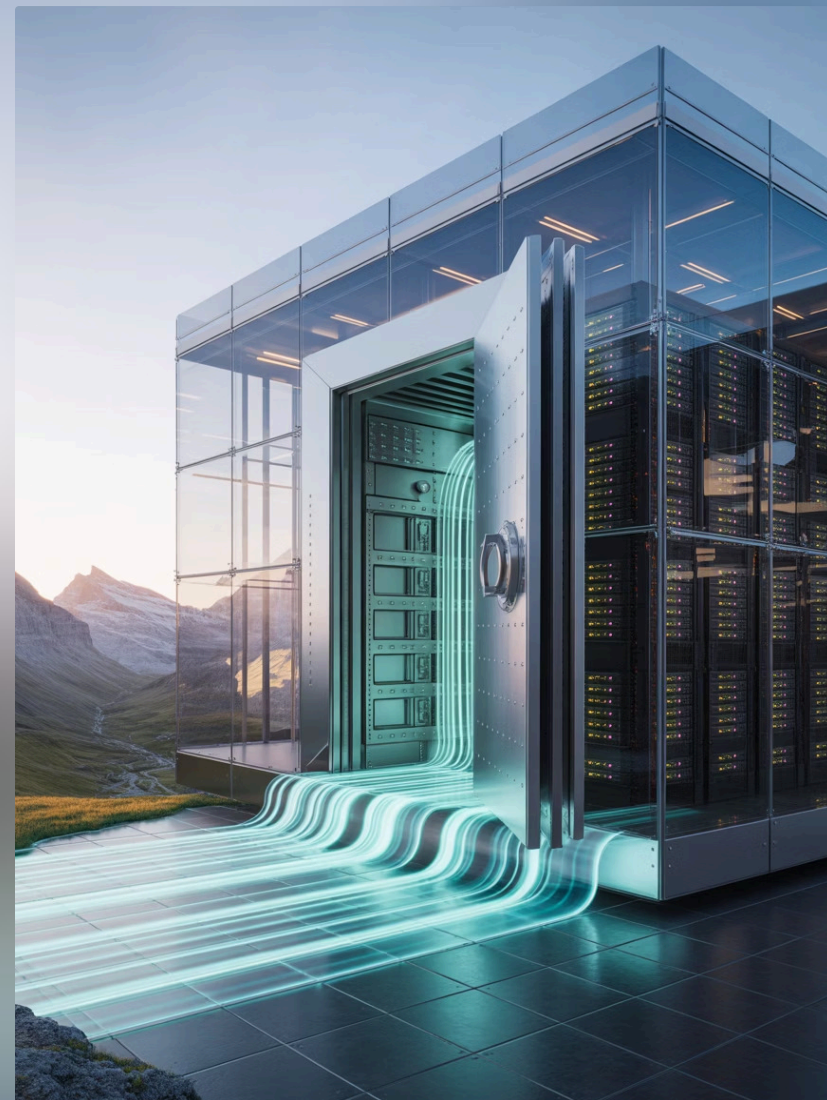
Veiligheid en Data-eigendom

Proton's Veiligheidsvoordelen

- End-to-end encryptie voor alle communicatie en bestanden
- Geen logboeken van gebruikersactiviteit
- Minimale opslag van metadata
- Open-source code voor maximale transparantie
- Beschermd door strenge Zwitserse privacywetten

Google's Beperkingen

- Encryptie alleen tijdens verzending, niet tijdens opslag
- Uitgebreide metadata-verzameling voor advertentiedoeleinden
- Valt onder Amerikaanse wetgeving met ruimere surveillancemogelijkheden
- Verplichte medewerking aan overheidsverzoeken zonder kennisgeving



Gebruikerservaring en Overstap

De overstap van Google naar Proton vraagt om aanpassing, maar wordt steeds eenvoudiger. Proton heeft de afgelopen jaren significant geïnvesteerd in het verbeteren van de gebruikerservaring en het uitbreiden van functionaliteiten.

Een volledige migratie kost tijd, maar kan stapsgewijs worden uitgevoerd, beginnend met het overzetten van e-mail en contacten. Proton biedt hiervoor steeds betere importtools aan.

1

Exporteer data

Gebruik Google Takeout om al je gegevens te downloaden

2

Maak Proton-account

Begin met het gratis plan om te testen

3

Importeer gegevens

Gebruik Proton's importtools om je data over te zetten



Voor Wie is Proton een Goede Keuze?



Journalisten & Activisten

Bescherm gevoelige bronnen en communicatie tegen surveillance. Proton's versleuteling zorgt ervoor dat niemand kan meelesen met uw berichten of documenten.



Bedrijven & Professionals

Garandeer de vertrouwelijkheid van bedrijfsinformatie, klantgegevens en intellectueel eigendom. Proton's zakelijke oplossingen bieden robuuste bescherming tegen industriële spionage.



Privacy-bewuste Gebruikers

Voor iedereen die controle wil over persoonlijke gegevens en niet wil dat hun online activiteit wordt gevolgd of gecommercialiseerd door grote techbedrijven.

Uitdagingen bij Overstappen

1 Beperkte Integraties

Proton's ecosysteem heeft minder verbindingen met externe diensten dan Google's uitgebreide netwerk van integraties.

2 Leercurve

Wennen aan nieuwe interfaces en workflows kost tijd, vooral als u jarenlang Google-producten hebt gebruikt.

3 Functionaliteitsverschillen

Sommige geavanceerde Google-functies zijn nog niet beschikbaar bij Proton, al wordt dit verschil steeds kleiner.



Conclusie: Veiligheid of Gemak?

Proton: Privacy Voorop

- Maximale privacybescherming door end-to-end encryptie
- Groeiend aanbod van geïntegreerde diensten
- Beschermd door robuuste Zwitserse wetgeving
- Transparant bedrijfsmodel zonder datamining

Google: Gemak & Integratie

- Uitgebreider ecosysteem met meer functies
- Betere integratie met externe diensten
- Gebruiksvriendelijke interfaces en AI-assistentie
- Gratis, maar betaald met uw persoonlijke gegevens



De keuze tussen Proton en Google komt uiteindelijk neer op wat u belangrijker vindt: maximale privacy of maximaal gebruiksgemak. De kloof tussen beide wordt echter steeds kleiner naarmate Proton zijn diensten blijft verbeteren.

Voor wie privacy waardeert, biedt Proton een steeds aantrekkelijker alternatief dat de moeite van het overstappen meer dan waard is.

Spioneert iemand op jouw Facebookaccount? Zo kom je er achter

Tegenwoordig is Facebook niet alleen een plek om contact te houden met vrienden en familie, maar ook een potentieel doelwit voor hackers en mensen die je activiteiten willen bespioneren. Wereldwijd worden dagelijks duizenden accounts gehackt of ongeautoriseerd bekeken.

In dit artikel leer je hoe je kunt ontdekken of iemand zonder jouw toestemming toegang heeft tot je Facebookaccount en wat je daartegen kunt doen.

 by VEILIG DIGITAAL



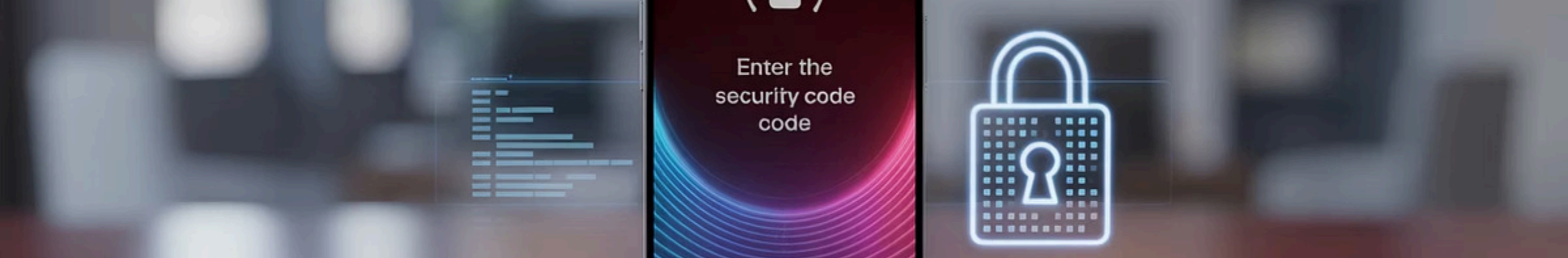
Tekenen van een gecompromitteerd account

Verdachte signalen

- Onverklaarbare wijzigingen in je profielgegevens of contactinformatie
- Berichten of reacties die je niet zelf hebt geschreven
- Vreemde vriendschapsverzoeken die zijn verzonden vanaf jouw account
- Meldingen over inlogpogingen vanaf onbekende locaties
- Je wachtwoord werkt plotseling niet meer



Als je een of meer van deze tekenen herkent, is het mogelijk dat iemand ongeautoriseerde toegang heeft tot je Facebookaccount. Hoe sneller je dit opmerkt, hoe beter je jezelf kunt beschermen tegen mogelijke schade.



Waarom is Two-Factor Authentication essentieel?

Basis beveiliging

Een sterk wachtwoord is je eerste verdedigingslinie, maar biedt onvoldoende bescherming tegen geavanceerde hackmethoden.

Extra beveiligingslaag

2FA voegt een tweede verificatiestap toe: naast je wachtwoord heb je ook een tijdelijke code nodig die naar je telefoon wordt gestuurd.

Bewezen effectiviteit

Onderzoek toont aan dat 2FA meer dan 99% van geautomatiseerde aanvallen en 66% van gerichte aanvallen kan blokkeren.

Stappen om je Facebookaccount te beveiligen



Sterk wachtwoord instellen

Gebruik een uniek wachtwoord van minimaal 12 tekens met hoofdletters, kleine letters, cijfers en speciale tekens. Vermijd persoonlijke informatie zoals namen of geboortedata.



Two-Factor Authentication activeren

Ga naar Instellingen > Beveiliging en aanmelding > Tweestapsverificatie gebruiken. Kies voor sms-codes of een authenticator-app voor extra veiligheid.



Regelmatige controles uitvoeren

Controleer wekelijks je recente activiteit en inloggeschiedenis om ongeautoriseerde toegang snel te detecteren.



Privacy-instellingen aanpassen voor meer veiligheid

Belangrijke privacy-instellingen

- Bepaal wie je berichten kan zien (Openbaar, Vrienden, Alleen ik)
- Beperk wie je kan taggen in foto's en berichten
- Schakel tagcontrole in om goedkeuring te geven voordat tags zichtbaar worden
- Beperk zoekmachines in het indexeren van je profiel
- Controleer welke apps toegang hebben tot je accountgegevens

Deze instellingen vind je onder Instellingen > Privacy in je Facebookaccount.



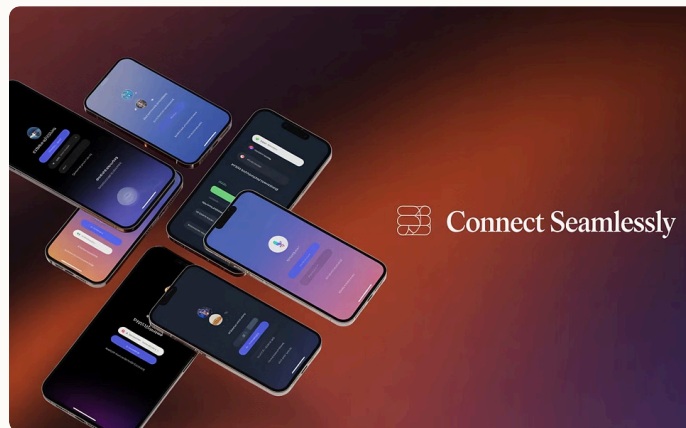
Door je privacy-instellingen aan te passen, verklein je de kans dat ongewenste personen toegang krijgen tot je persoonlijke informatie en activiteiten.

Inlogactiviteit controleren



Locaties controleren

Bekijk waar er is ingelogd op je account. Onbekende locaties zijn een duidelijk waarschuwingssignaal. Ga naar Instellingen > Beveiliging en aanmelding > Waar je bent aangemeld.



Apparaten beheren

Controleer welke apparaten toegang hebben tot je account. Zie je onbekende telefoons, tablets of computers? Verwijder deze direct met de optie "Afsluiten".



Verdachte activiteit melden

Bij onbekende inlogpogingen, klik op "Dit ben ik niet" om Facebook te waarschuwen en je account extra te beveiligen. Je wordt dan door beveiligingsstappen geleid.

Reageren op een gehackt account

Directe acties bij een gehackt account

1. Wijzig onmiddellijk je wachtwoord via een vertrouwd apparaat
2. Controleer en herstel gewijzigde accountgegevens zoals e-mail en telefoonnummer
3. Meld het gehackte account bij Facebook via facebook.com/hacked
4. Controleer je betalingsgegevens op ongeautoriseerde aankopen
5. Waarschuw vrienden dat je account is gehackt
6. Scan je apparaten op malware met actuele antivirussoftware



Hoe sneller je reageert op een gehackt account, hoe kleiner de schade zal zijn. Bij ernstige problemen kun je contact opnemen met de Facebook Helpdesk voor extra ondersteuning.

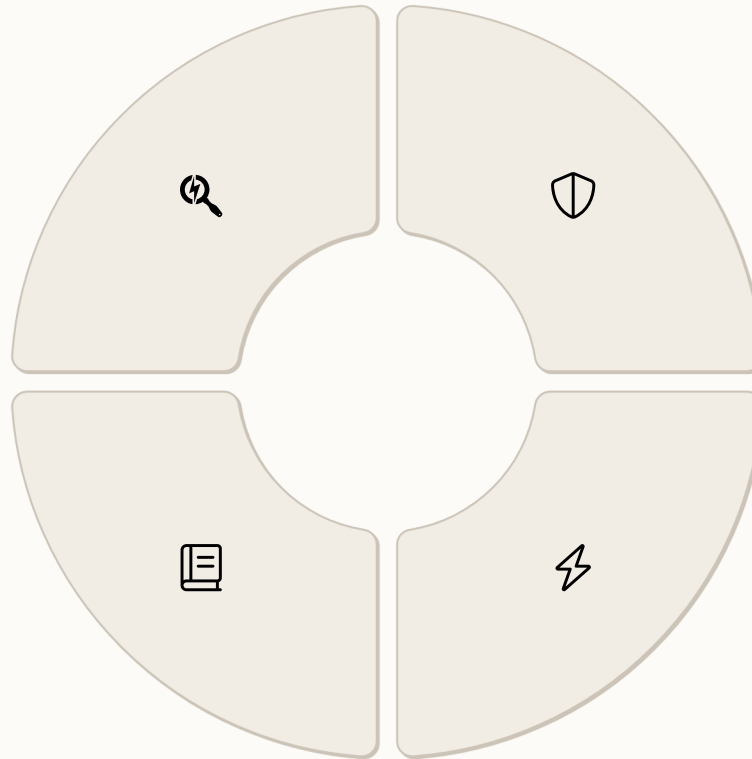
Samenvatting en conclusie

Regelmatige controles

Controleer wekelijks je inlogactiviteit en accountgebeurtenissen om vreemde activiteiten snel op te sporen.

Blijf geïnformeerd

Houd je kennis over online veiligheid up-to-date en volg Facebook's beveiligingsadviezen voor de nieuwste beschermingsmethoden.



Preventieve maatregelen

Gebruik sterke wachtwoorden, activeer 2FA, en pas je privacy-instellingen aan om je account te beschermen.

Snelle reactie

Bij verdachte activiteit, onderneem direct actie: wijzig wachtwoorden, meld het probleem en herstel je accountgegevens.



Steeds meer meldingen van spoofing: criminelen misbruiken 06-nummers

Nederland kampt met een explosieve stijging van telefonische oplichting, waarbij criminelen steeds vaker gebruikmaken van een techniek genaamd 'spoofing'.

Hierbij wordt specifiek misbruik gemaakt van Nederlandse 06-nummers om potentiële slachtoffers te misleiden en op te lichten.

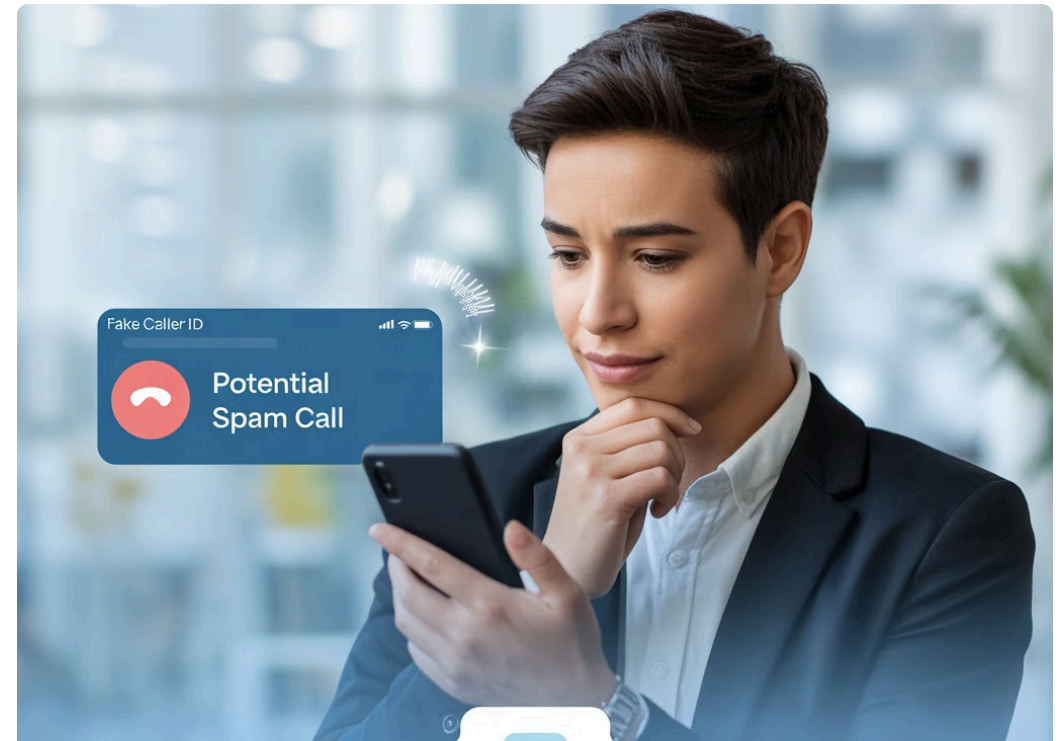
VEILIGDIGITAAL.COM

Wat is spoofing met 06-nummers?

Spoofing is een geavanceerde criminele techniek waarbij oplichters het telefoonnummer dat op uw toestel verschijnt manipuleren. Bij deze vorm van oplichting ziet het slachtoffer een ogenschijnlijk betrouwbaar Nederlands 06-nummer op het scherm verschijnen.

De criminelen doen zich vervolgens voor als een medewerker van een bekende instantie zoals uw bank, de Belastingdienst, of zelfs als een familielid of vriend om uw vertrouwen te winnen.

Het gebruik van Nederlandse nummers verhoogt de geloofwaardigheid van de oproep aanzienlijk, waardoor slachtoffers eerder geneigd zijn de oplichters te vertrouwen.



ShieldDid

"Protect Your Identity"

Stijging aantal meldingen in 2025

10.000

Meldingen Q1 2025

Aantal meldingen bij de Fraudehelpdesk in het eerste kwartaal van 2025

3.000

Meldingen Q1 2024

Aantal meldingen in dezelfde periode vorig jaar

333%

Stijging

Meer dan een verdriedubbeling van het aantal meldingen vergeleken met 2024

Deze dramatische toename toont aan dat spoofing een snel groeiend probleem is in Nederland, waarmee steeds meer mensen worden geconfronteerd.

Werkwijze van criminelen



Diefstal van 06-nummers

Criminelen maken gebruik van eerder buitgemaakte telefoonnummers om geloofwaardig over te komen.



Misleiding

Ze bellen namens uw bank, de Belastingdienst, politie of andere bekende organisaties.



Gegevensverzameling

Ze vragen naar persoonlijke gegevens, bankgegevens of proberen u apps te laten installeren.



Emotionele druk

Ze zetten slachtoffers onder druk door urgentie te creëren of angst aan te jagen.

Recente incidenten en impact

Moeilijke opsporing

De politie heeft grote moeite om de daders van spoofing op te sporen en te vervolgen vanwege de complexe digitale sporen.

Ernstige schade

Slachtoffers lopen vaak aanzienlijke financiële schade op en ervaren daarnaast emotionele gevolgen zoals schaamte en angst.

Recente arrestaties

Onlangs zijn er enkele jongeren aangehouden voor gerelateerde phishingpraktijken, maar dit betreft slechts een klein deel van het probleem.



Iedereen kan slachtoffer worden van spoofing. De criminelen kiezen hun doelwitten vaak willekeurig en richten zich zowel op ouderen als jongeren, hoogopgeleiden als laagopgeleiden.

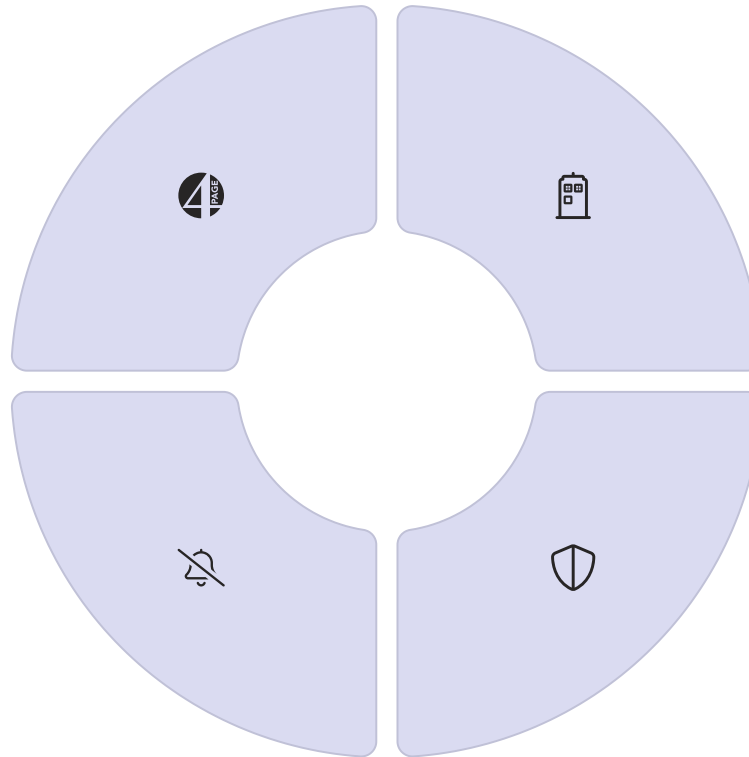
Maatregelen en preventie

Samenwerking

Telecomproviders en banken werken aan systemen voor realtime controle van verdachte telefoonnummers om spoofing tegen te gaan.

Alert blijven

Blijf altijd op uw hoede bij onverwachte telefoontjes, zelfs als deze afkomstig lijken van bekende Nederlandse nummers.



Voorlichting

De politie en Fraudehelpdesk waarschuwen burgers proactief via campagnes over de gevaren van spoofing.

Gegevens beschermen

Deel nooit persoonlijke gegevens, inlogcodes of andere gevoelige informatie via de telefoon, ook niet als het een bekend nummer lijkt.



SwissTransfer: Grote Bestanden Versturen Tot 50GB

SwissTransfer biedt een eenvoudige en veilige oplossing voor het delen van grote bestanden. Deze gratis service stelt gebruikers in staat om bestanden tot 50GB te versturen zonder registratie, waarbij alle data veilig wordt opgeslagen op Zwitserse servers.



by **VEILIG DIGITAAL**

Belangrijkste Voordelen

Ruime Capaciteit

Met SwissTransfer kunt u tot 50GB per overdracht versturen, aanzienlijk meer dan wat veel concurrerende diensten bieden.

De service ondersteunt tot 500 transfers per dag, perfect voor intensief zakelijk gebruik.



De downloadlinks blijven 30 dagen geldig, waardoor ontvangers voldoende tijd hebben om hun bestanden te downloaden.

Veiligheid & Privacy



SSL-Encryptie

Alle bestandsoverdrachten zijn beveiligd met SSL-encryptie, waardoor uw gegevens beschermd blijven tijdens het transport.



Wachtwoordbeveiliging

Voeg een extra beveiligingslaag toe door uw transfers te beschermen met een wachtwoord dat alleen u en de ontvanger kennen.



Zwitserse Wetgeving

Profiteer van de strenge Zwitserse privacywetgeving die zorgt voor optimale bescherming van uw persoonlijke gegevens.

Gebruiksgemak & Praktische Tips

SwissTransfer is ontworpen met gebruiksgemak als prioriteit. Zonder account kunt u direct beginnen met het uploaden en delen van uw bestanden.

Meerdere Deelmethoden

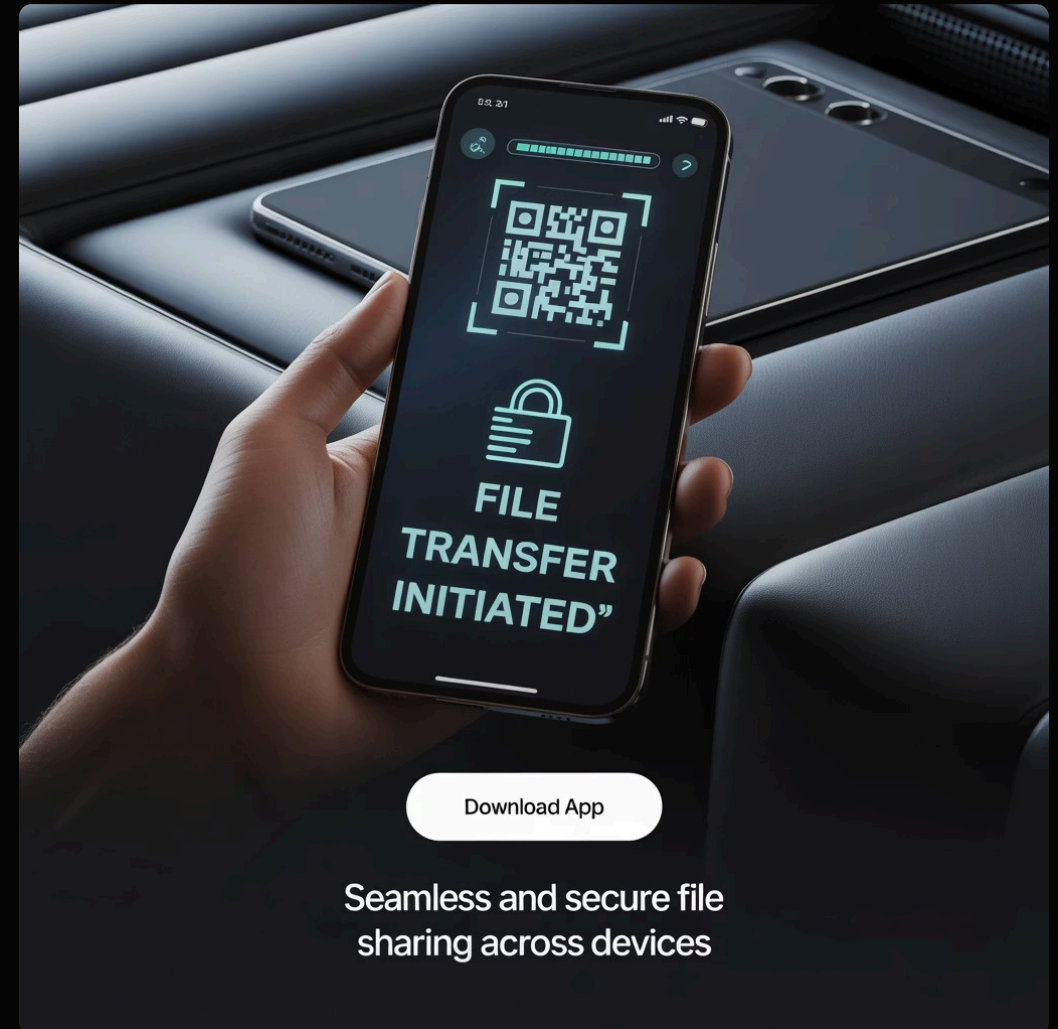
Verstuur bestanden via e-mail, genereer downloadlinks of deel een QR-code voor snelle toegang.

Browserintegratie

Installeer extensies voor Chrome of Firefox voor naadloze integratie met uw browser.

Mobiele Toegang

Gebruik de Android-app om onderweg toegang te hebben tot al uw bestanden.



SwissTransfer download:

www.swisstransfer.com