

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 slim keyboard and a mouse. The background shows a blurred office environment with windows.

MAGAZINE

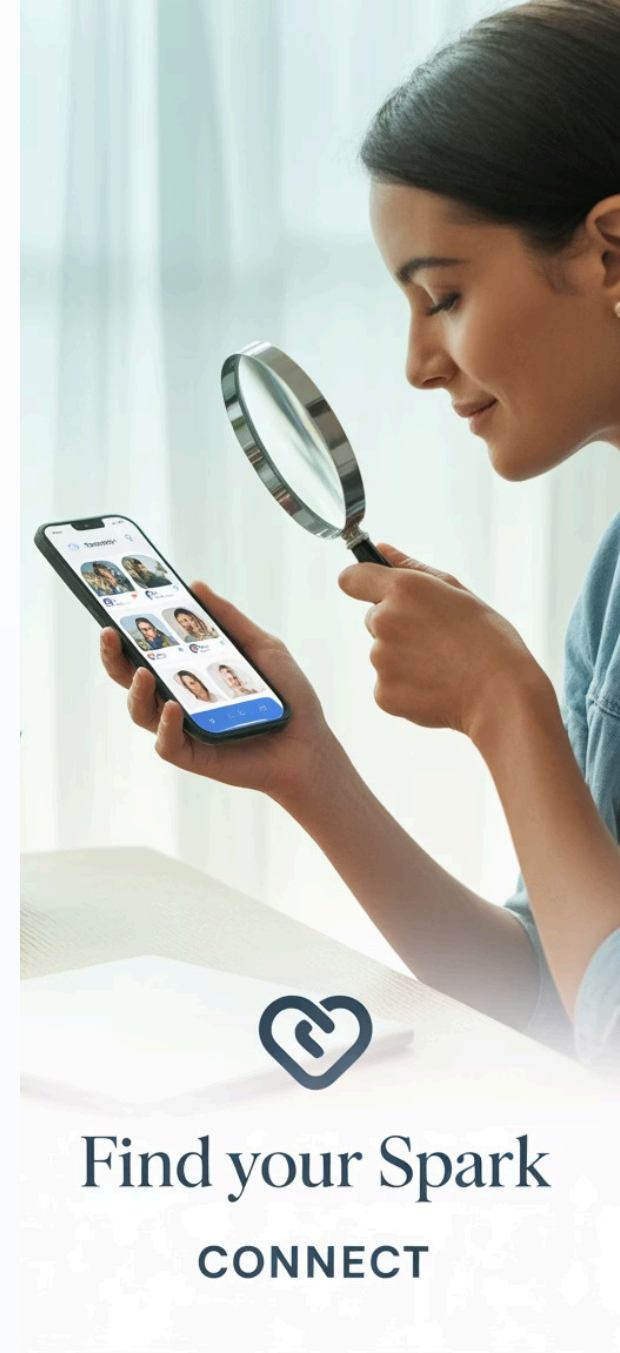
VEILIG DIGITAAL

Voorkom datingfraude en catfishing: doe een reverse image search

In de wereld van online dating loert gevaar. Terwijl steeds meer Nederlanders liefde zoeken via apps en websites, groeit ook het risico op datingfraude en catfishing. Uit recent onderzoek blijkt dat maar liefst 1 op de 5 Nederlanders ooit slachtoffer is geweest van catfishing - iemand die zich online voordoe als een ander.

Gelukkig bestaat er een eenvoudige maar krachtige techniek om jezelf te beschermen: de reverse image search, je digitale beschermerschild tegen online misleiding.

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



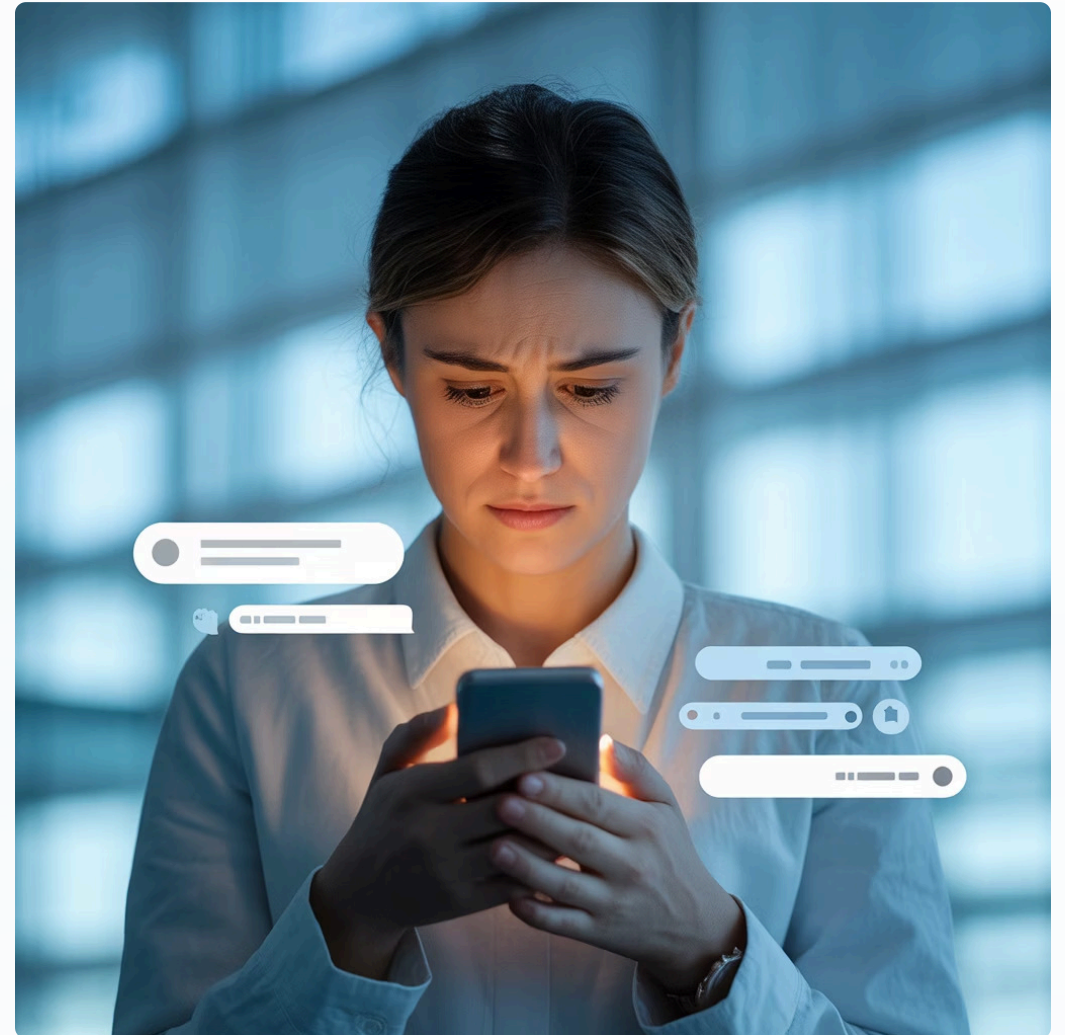
Find your Spark
CONNECT

Wat is datingfraude en catfishing?

Datingfraude en catfishing zijn vormen van online bedrog waarbij iemand een valse identiteit aanneemt om anderen te misleiden. De fraudeur gebruikt foto's en informatie die niet van hemzelf zijn om vertrouwen te winnen. Vaak ontstaat er een 'relatie' waarbij de catfisher uiteindelijk vraagt om:

- Financiële steun voor een zogenaamde noodsituatie
- Dure cadeaus of tegemoetkomingen
- Persoonlijke en gevoelige informatie

Het schokkende is dat 40% van de slachtoffers de fraude pas ontdekt nadat ze al financiële schade hebben geleden, met gemiddelde verliezen van duizenden euro's.



Reverse image search: jouw digitale detective

Foto-oorsprong ontdekken

Met één klik kun je ontdekken waar een foto nog meer op internet voorkomt. Dit geeft je inzicht of de persoon echt is of dat iemand andermans beelden gebruikt.

Gestolen beelden opsporen

De technologie kan zelfs gespiegelde, bijgesneden of licht bewerkte foto's herkennen. Oplichters denken slim te zijn door beelden aan te passen, maar reverse image search is slimmer.

AI en stockfoto's herkennen

Moderne tools kunnen detecteren of een foto AI-gegenereerd is of als stockfoto wordt verkocht. Deze "te perfecte" beelden worden vaak gebruikt door fraudeurs omdat ze professioneel en aantrekkelijk ogen.

Deze technologie fungeert als je persoonlijke digitale detective die verdachte profielen kan ontmaskeren voordat je emotioneel of financieel betrokken raakt.

Zo gebruik je reverse image search stap-voor-stap

Sla de profielfoto op

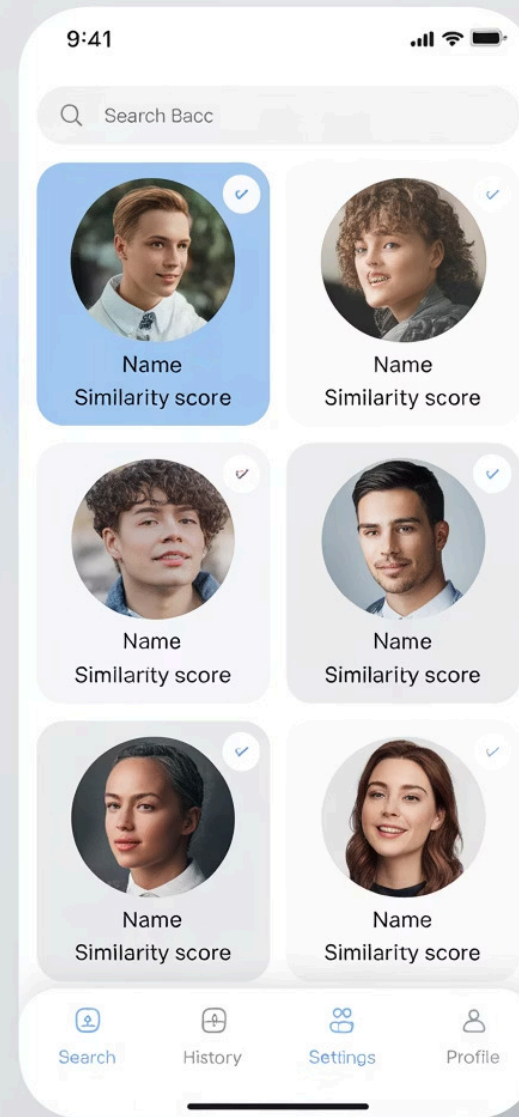
Klik op de profielfoto van je potentiële date, houd deze ingedrukt en kies 'Afbeelding opslaan'. Op desktop kun je rechts klikken en kiezen voor 'Afbeelding opslaan als'.

Upload naar zoekmachines

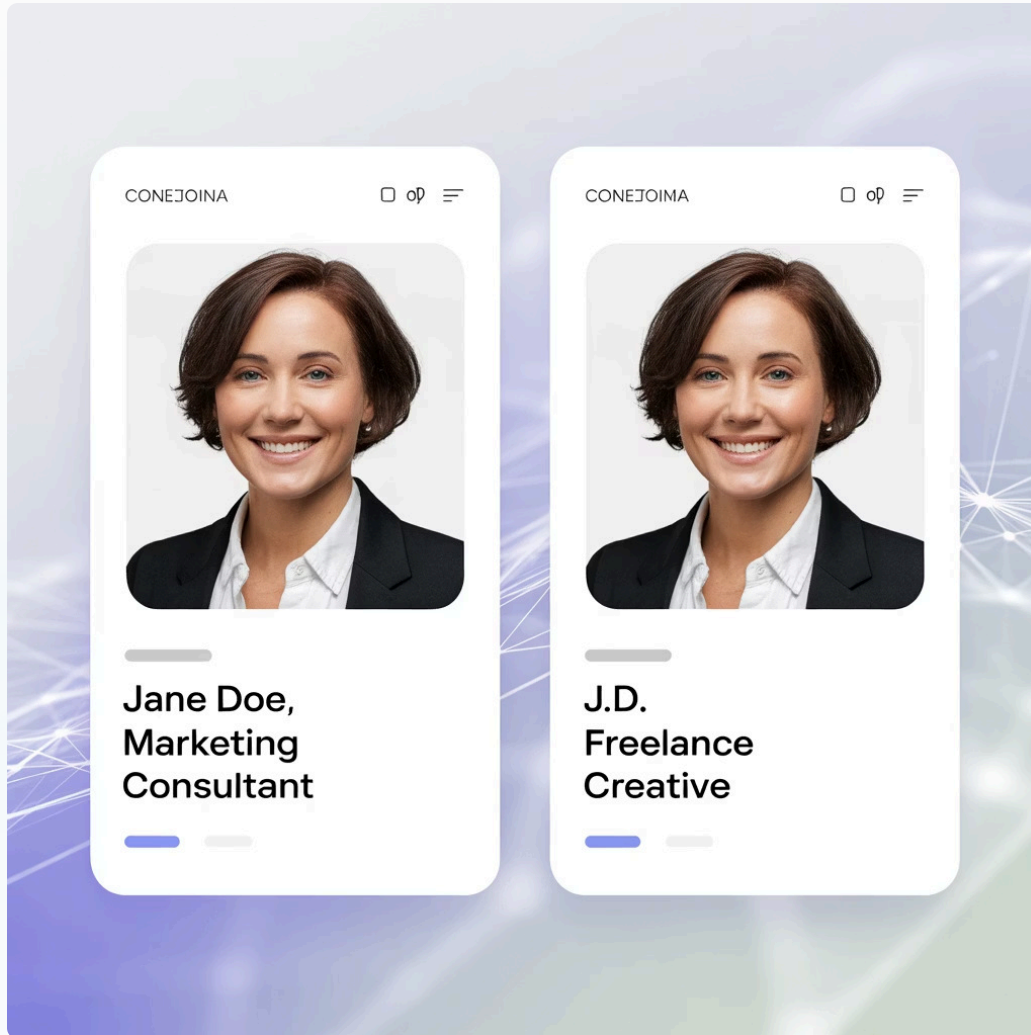
Ga naar Google Lens, TinEye of gespecialiseerde tools zoals PimEyes of FaceCheck.ID. Klik op het camera-icoontje en upload de opgeslagen foto. Voor privacygevoelige controles zijn de betaalde diensten vaak beter.

Analyseer de resultaten

Bekijk waar de foto nog meer voorkomt. Staat dezelfde persoon op meerdere sites met verschillende namen? Dan is dat een rode vlag. Check ook of de foto als stockfoto te koop staat of op sociale media van iemand anders verschijnt.



Typische signalen en voorbeelden van oplichting



⚠ Alarmsignalen bij reverse image search:

- Dezelfde foto verschijnt op twintig verschillende datingsites met andere namen en leeftijden
- De foto komt voor in stockfoto-databases of modellenportfolio's
- Het beeld heeft een onnatuurlijke, "te perfecte" kwaliteit die wijst op AI-generatie
- De persoon staat wel op sociale media, maar onder een compleet andere naam en in een ander land
- De foto is van een bekende persoon of influencer die waarschijnlijk niet op reguliere datingsites actief is

Uit onderzoek blijkt dat 70% van de catfishing-gevallen voorkomen had kunnen worden met een eenvoudige reverse image search voordat emotionele betrokkenheid ontstond.

Veilig daten: tips van experts

Combineer meerdere checks

Naast reverse image search, vraag om videogesprekken en verifieer profielinformatie. Controleer of sociale media-accounts consistent zijn qua foto's, interacties en tijdlijn.

Bescherm je financiën

Wees uiterst voorzichtig met geldverzoeken. Legitieme datingpartners zullen zelden of nooit om financiële hulp vragen, zeker niet in de beginfase van een relatie.

Vertrouw je intuïtie

Als iets te mooi lijkt om waar te zijn, is dat meestal ook zo. Voel je geen schaamte om skeptisch te zijn - het is beter voorzichtig te zijn dan opgelicht te worden.

Onthoud: echte liefde heeft geduld en respecteert grenzen. Iemand die oprecht is, zal begrijpen waarom je voorzichtig bent en je de tijd geven om vertrouwen op te bouwen. Blijf veilig en laat technologie je helpen bij het vinden van authentieke connecties.



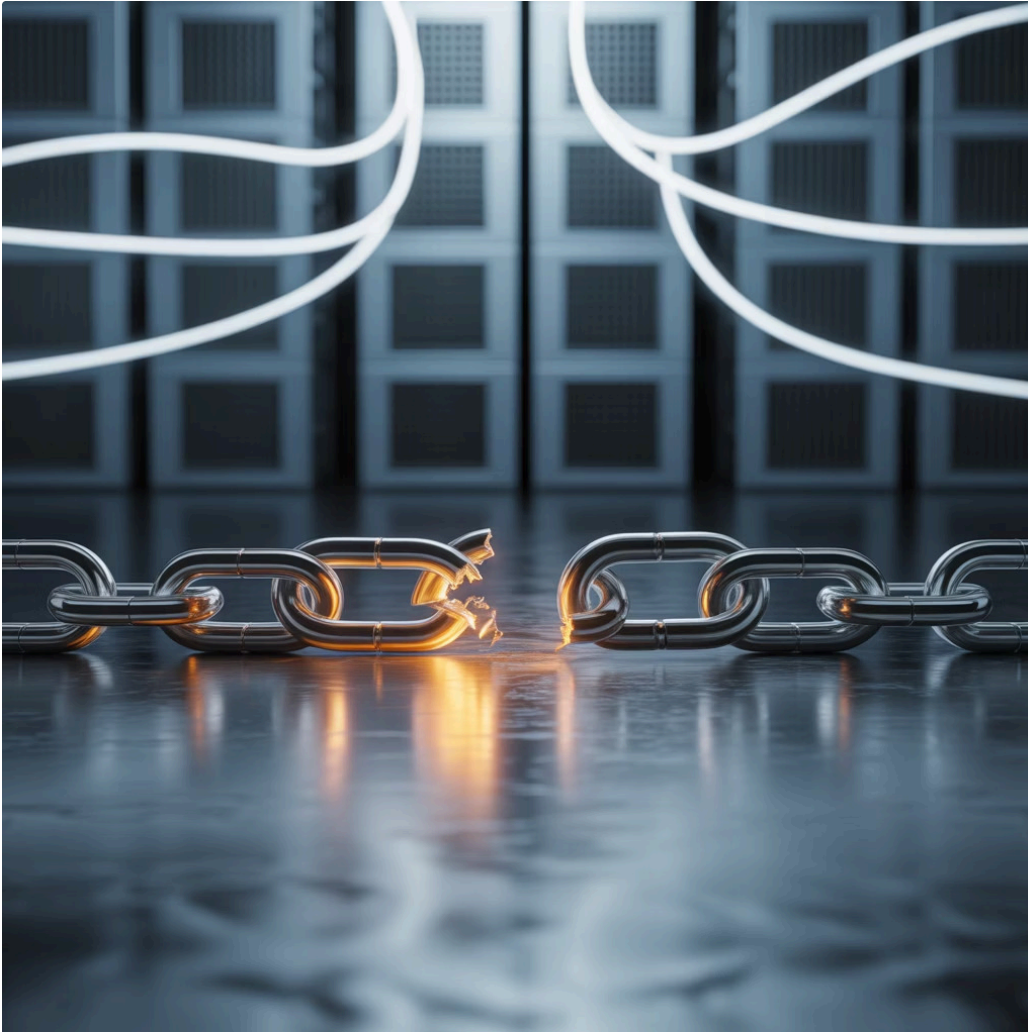
Cybercriminelen misbruiken linkwrapping om je Microsoft-account te stelen

Cybercriminelen hebben een nieuwe, geavanceerde methode ontwikkeld om toegang te krijgen tot je Microsoft-account. Door misbruik te maken van de linkwrapping-beveiliging van e-mailbeveiligingssystemen slagen ze erin om hun aanvallen te verhullen achter legitieme, vertrouwde domeinen.

Dit artikel legt uit hoe deze aanvallen werken, welke impact ze hebben en hoe je jezelf kunt beschermen tegen deze groeiende bedreiging.

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

Wat is linkwrapping en waarom misbruiken criminelen het?



De techniek onthuld

Linkwrapping is een beveiligingsfunctie van diensten zoals Proofpoint en Intermedia die URL's omleiden via een scanner om schadelijke links te blokkeren voordat gebruikers ze bezoeken.

Cybercriminelen hebben een zwakke plek gevonden: ze compromitteren beveiligde e-mailaccounts, waardoor phishinglinks **automatisch worden omwikkeld** met legitieme, vertrouwde domeinen zoals urldefense.proofpoint.com.

Dit creëert een **dubbele laag van misleiding**: een verkorte link (bijv. Bitly) leidt naar een beveiligde, 'gewrapte' link, die vervolgens doorstuurt naar een phishingpagina.



De aanvalsmethoden en impact op Microsoft-accounts

1

Overtuigende misleiding

Phishingmails doen zich voor als voicemailmeldingen, Microsoft Teams-documenten of ongelezen berichten, met links die leiden naar perfect nagemaakte Microsoft 365-inlogpagina's.

2

Verhoogde effectiviteit

Door het gebruik van vertrouwde domeinen stijgt de klikratio aanzienlijk en wordt het moeilijker voor traditionele beveiligingsfilters om de aanval te detecteren.

3

Ernstige financiële schade

In 2024 veroorzaakte e-mailfraude wereldwijd meer dan \$502 miljoen schade; phishing is verantwoordelijk voor 67% van alle datalekken.

Hoewel Microsoft deze campagnes probeert te blokkeren met AI-gedreven detectie, blijven gebruikers kwetsbaar door menselijke fouten en de steeds geavanceerdere misleidingstechnieken van cybercriminelen.

Hoe herken en voorkom je deze phishingaanvallen?



Herkennen

Wees alert op onverwachte e-mails met links naar voicemail, Teams of documenten, vooral als ze om inloggegevens vragen. Controleer altijd URL's zorgvuldig, zelfs wanneer ze via Proofpoint of Intermedia lijken te komen.

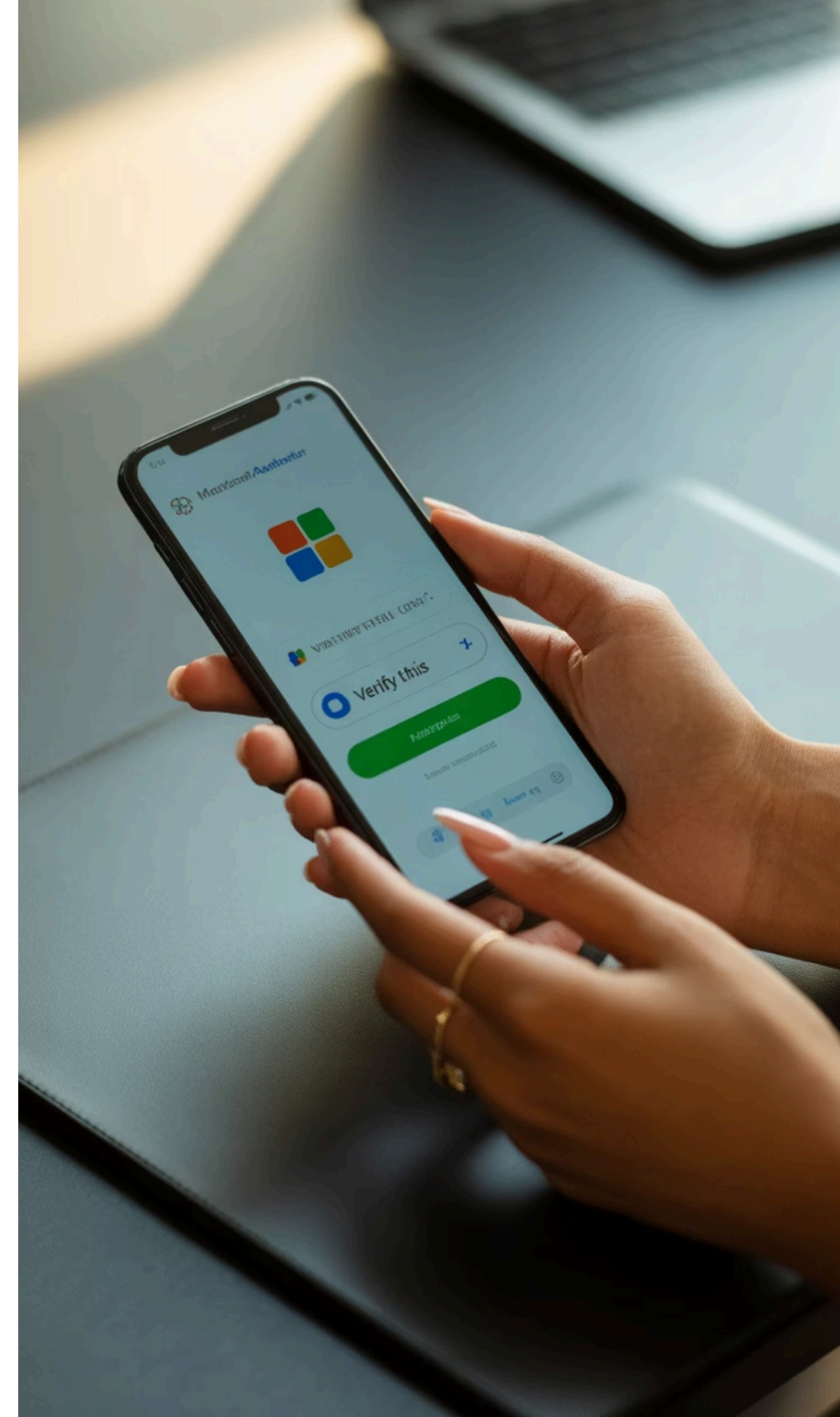


Voorkomen

Gebruik multi-factor authenticatie (MFA) en de Microsoft Authenticator-app. Verander direct je wachtwoord bij verdachte activiteit en controleer je accountinstellingen op ongewenste doorstuurregels of wijzigingen.



Onthoud: Vertrouwde domeinen zoals urldefense.proofpoint.com kunnen worden misbruikt. Klik nooit op links in onverwachte e-mails, zelfs als ze beveiligd lijken.



Conclusie: Blijf waakzaam en versterk je accountbeveiliging

Voortdurende evolutie

Cybercriminelen vernieuwen hun technieken continu en gebruiken slimme methoden zoals linkwrapping om beveiligingslagen te omzeilen.

Kritisch blijven

Vertrouw niet blind op beveiligde links; blijf kritisch en volg best practices voor accountbeveiliging.

Jouw rol is cruciaal

Hoewel Microsoft en beveiligingsbedrijven AI en gedragsanalyse inzetten, blijft jouw alertheid de belangrijkste verdedigingslinie.



[Meer beveiligingstips](#)

[Controleer je account](#)

Einde ondersteuning Microsoft Store-versies van Office-apps

Microsoft heeft aangekondigd dat de ondersteuning voor Office-applicaties die via de Microsoft Store zijn geïnstalleerd, zal worden beëindigd. Deze belangrijke verandering heeft gevolgen voor alle gebruikers die momenteel de Store-versies van Microsoft Office gebruiken.

De aankondiging maakt deel uit van Microsoft's strategie om over te stappen naar een uniform installatiemodel en biedt zowel uitdagingen als kansen voor gebruikers.

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

October 2025

Vrie Tue Vrie To Pv Fri

4 5 4 9 6 7

9 15 14 19 15 28

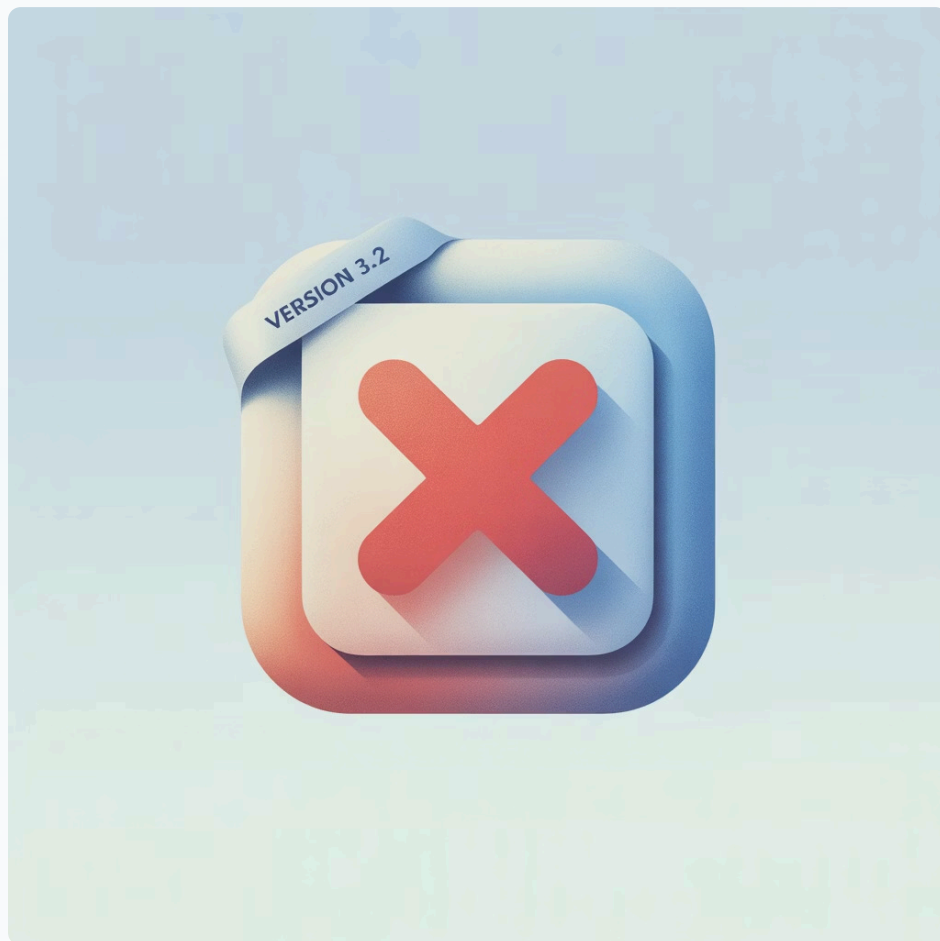
12 21 22 22 22 25

22 23 28 31

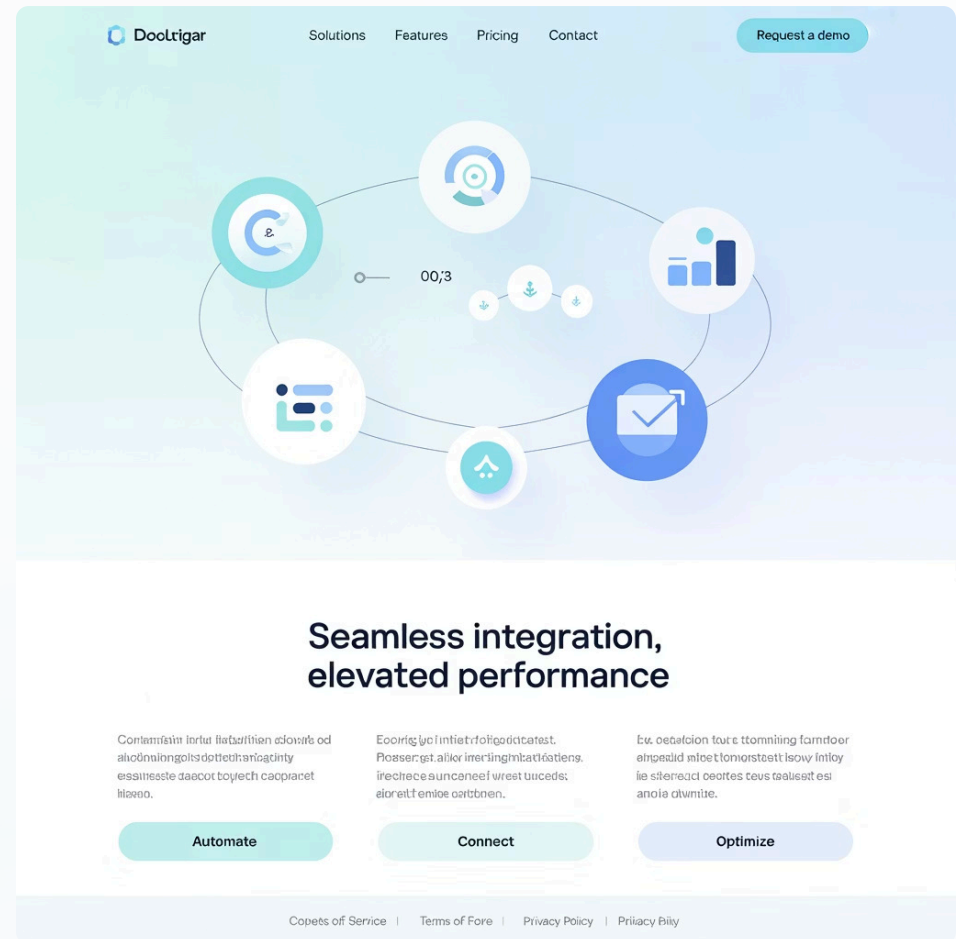
Overgang naar Click-to-Run Installatie

Einde van Microsoft Store-versies (Appx/UWP)

Office-applicaties zoals Word, Excel, PowerPoint en Outlook, die via de Microsoft Store zijn geïnstalleerd, maken gebruik van de Appx/UWP-technologie. De ondersteuning voor deze versies zal gefaseerd worden beëindigd. Nieuwe functie-updates stoppen in **oktober 2025**, en de volledige ondersteuning eindigt in **december 2026**.



Toekomst met Click-to-Run



Microsoft stapt volledig over op het Click-to-Run-installatiemodel, dat gebruik maakt van gevirtualiseerde .exe-technologie. Deze overgang brengt aanzienlijke voordelen met zich mee:

- Verbeterde prestaties
- Uitgebreidere beheeropties
- Diepere integratie met Windows
- Betere cloudbeheer-ervaring, cruciaal voor zakelijke gebruikers.

Gevolgen voor gebruikers en aanbevolen acties



Voor gebruikers van de Microsoft Store-versies van Office-apps heeft deze verandering belangrijke gevolgen. Na december 2026 ontvangen deze versies geen beveiligingsupdates meer, wat kan leiden tot kwetsbaarheden en compatibiliteitsproblemen. Microsoft raadt daarom alle gebruikers aan om proactief over te stappen naar de Click-to-Run-versie van Office om verzekerd te blijven van de nieuwste functies en beveiligingsupdates.

Voordelen van Click-to-Run

- Verbeterde prestaties en stabiliteit
- Diepere integratie met Windows-besturingssysteem
- Uitgebreide cloudbeheer-mogelijkheden
- Betere ondersteuning voor enterprise-omgevingen
- Consistente update-ervaring
- Verhoogde beveiliging door regelmatige updates



De Click-to-Run-installatiemethode biedt een gestroomlijnde installatie-ervaring en zorgt voor een betere integratie met Windows.

Microsoft biedt een gedetailleerd stappenplan voor gebruikers om te migreren van Store-versies naar Click-to-Run-installaties. Dit migratieproces is ontworpen om zo soepel mogelijk te verlopen, met minimale verstoring van de werkstroom. Voor particuliere gebruikers betekent dit meestal het downloaden en installeren van de Click-to-Run-versie via Office.com of via een Microsoft 365-abonnement. Voor zakelijke gebruikers zijn er specifieke hulpmiddelen beschikbaar via het Microsoft 365 Admin Center om deze overgang te beheren.



Voor zowel particuliere als zakelijke gebruikers is het belangrijk om deze overgang tijdig te plannen. Door vroeg te migreren kunnen gebruikers profiteren van de nieuwste functies en verbeteringen die exclusief beschikbaar zijn voor Click-to-Run-versies. Daarnaast voorkomt vroege migratie mogelijke beveiligingsrisico's die kunnen ontstaan wanneer de ondersteuning volledig wordt beëindigd. IT-beheerders in bedrijven zouden deze wijziging moeten opnemen in hun strategische planning om een soepele overgang voor alle medewerkers te garanderen.

A young woman with red hair is sitting at a desk in a modern office or library setting. She is looking down at a tablet computer that is propped up on the desk. The tablet screen displays the text 'TECH BYTES' in white on a blue background. She has her chin resting on her hand, looking thoughtful or focused. In the background, two other people are blurred, sitting at tables. A small potted plant sits on the desk next to the tablet. The lighting is warm and soft, coming from large windows in the background.

Google voert leeftijdsschatting in op YouTube: automatische bescherming voor tieners

Willem Bosgra voor

VEILIGDIGITAAL.COM

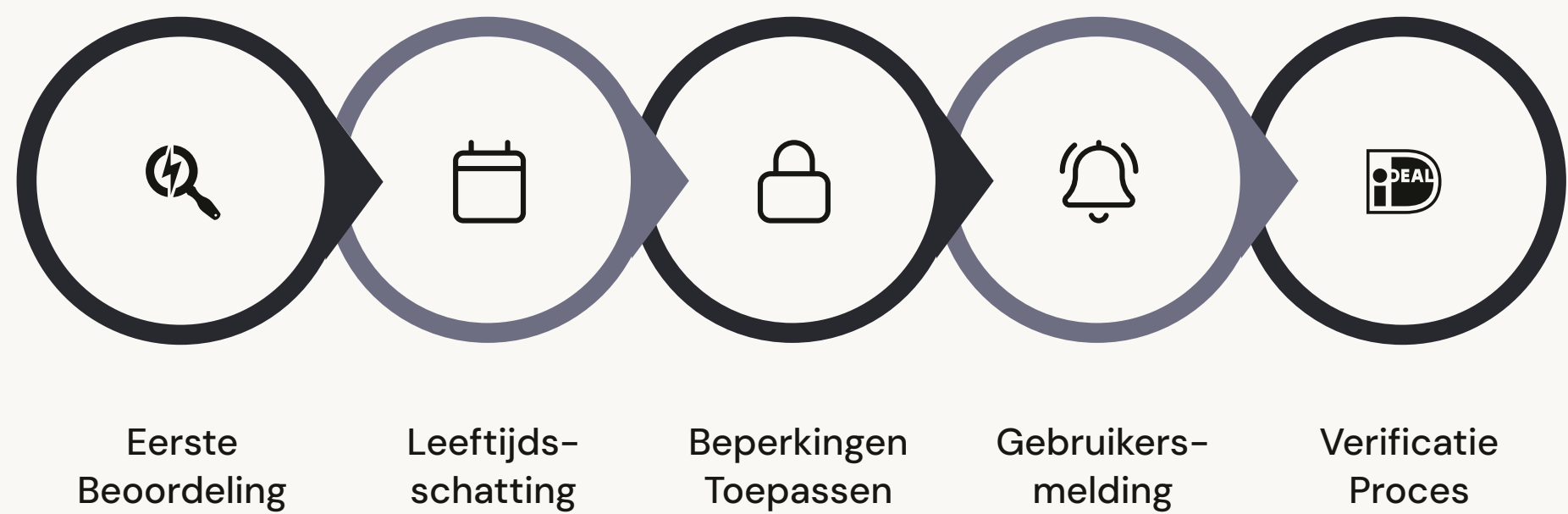
Google heeft in de Verenigde Staten een nieuw AI-gestuurd systeem geïntroduceerd dat de leeftijd van YouTube-gebruikers inschat. Deze 'leeftijdsschatting' gebruikt machine learning om te bepalen of iemand mogelijk minderjarig is, ongeacht de leeftijd die de gebruiker zelf heeft opgegeven. De technologie analyseert diverse signalen zoals accountleeftijd en kijkgedrag om de werkelijke leeftijd van gebruikers in te schatten.

Dit betekent dat jonge gebruikers die een hogere leeftijd hebben ingevuld om toegang te krijgen tot volwassen content, automatisch toch leeftijdsgeschikte content te zien krijgen. Deze maatregel vormt een belangrijk onderdeel van Google's strategie om minderjarigen beter te beschermen op het videoplatform, en komt voort uit toenemende druk van overheden wereldwijd om online veiligheid voor jongeren te waarborgen.

Gevolgen voor gebruikers en contentaanbod

De nieuwe leeftijdsschatting van YouTube heeft verstreckende gevolgen voor hoe gebruikers het platform ervaren. Wanneer het systeem vermoedt dat een gebruiker een tiener is, wordt de content die zij te zien krijgen automatisch aangepast, zelfs als hun profiel aangeeft dat ze volwassen zijn.

Dit is een fundamentele verschuiving in de manier waarop YouTube toegang tot inhoud beheert - niet langer is de zelf opgegeven leeftijd doorslaggevend, maar de beoordeling door de AI.



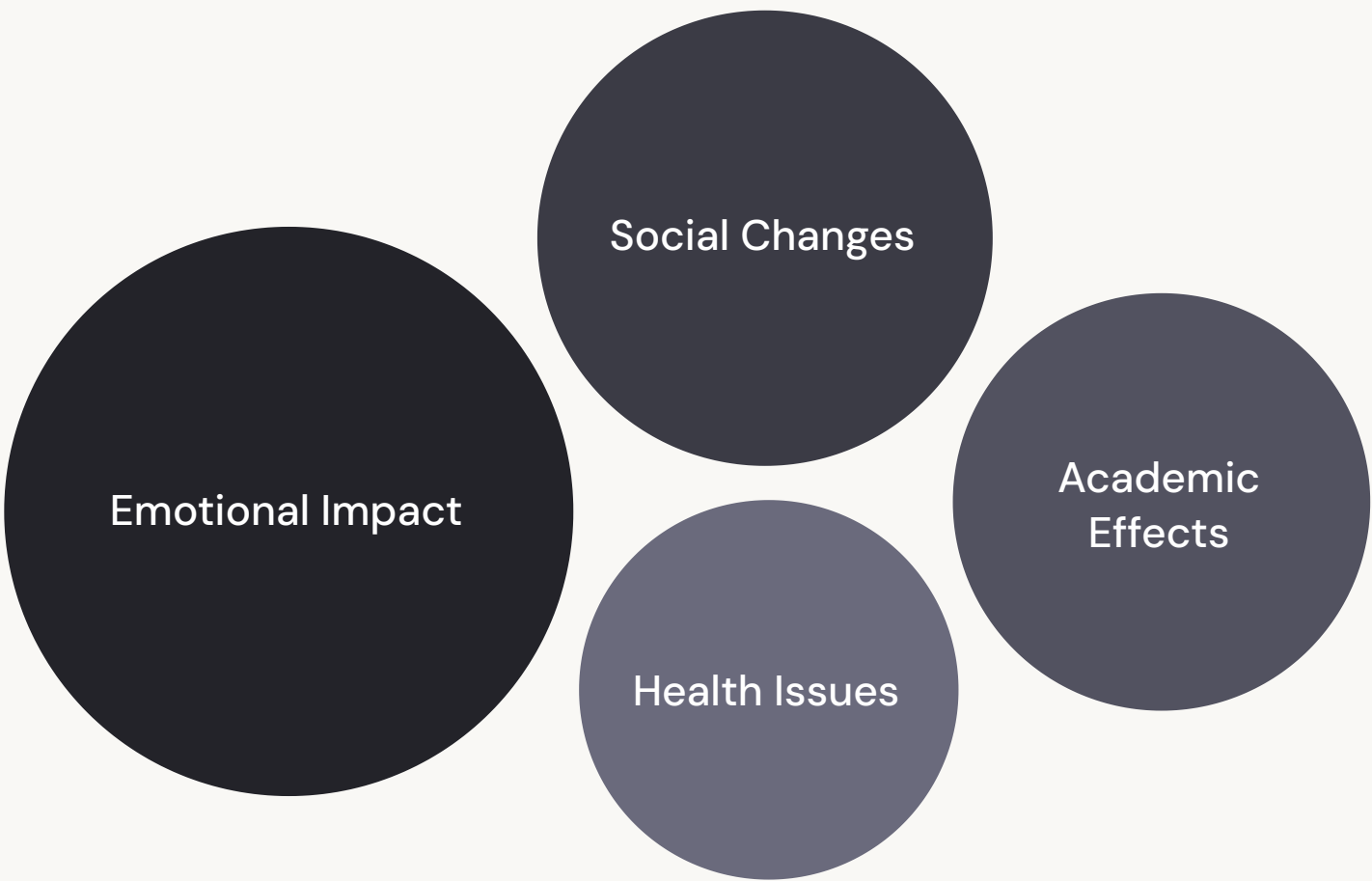
Deze maatregel heeft echter ook gevolgen voor volwassen gebruikers. In gevallen waarin de AI-algoritmes onzeker zijn over de leeftijd, worden sommige volwassenen per ongeluk als tiener aangemerkt. Dit leidt tot een situatie waarin deze gebruikers beperkte toegang krijgen tot bepaalde inhoud, terwijl ze wel degelijk volwassen zijn. Om dit probleem op te lossen, moeten zij hun leeftijd verifiëren door middel van een creditcard of een geldig identiteitsbewijs.

Gevolgen voor tieners

- Automatisch aangepaste content, ongeacht opgegeven leeftijd
- Verminderde blootstelling aan mogelijk schadelijke inhoud
- Leeftijdsvervalsing in instellingen wordt ineffectief
- Bescherming blijft actief, zelfs bij pogingen deze te omzeilen

Gevolgen voor volwassenen

- Risico op onterechte classificatie als tiener
- Mogelijk extra verificatiestappen nodig
- Creditcard of ID-verificatie vereist bij foutieve categorisering
- Tijdelijke beperking van toegang tot bepaalde content



Het systeem betekent ook dat het vervalsen van de leeftijd via accountinstellingen - een veelgebruikte tactiek onder jongeren om toegang te krijgen tot leeftijdsgebonden content - minder effectief wordt. De AI-beoordeling overschrijft immers de opgegeven geboortedatum wanneer er discrepanties worden vermoed. Dit zorgt voor een extra beveiligingslaag die moeilijker te omzeilen is dan traditionele leeftijdsverificatie via instellingen.

Privacy, risico's en maatschappelijke discussie



De invoering van leeftijdsschatting op YouTube roept belangrijke vragen op over privacy en digitale rechten. Door gebruikersgedrag automatisch te analyseren en te profileren, gaat het platform verder dan het verwerken van vrijwillig verstrekte gegevens.

Dit betekent dat YouTube continu gegevens verzamelt en interpreteert om de vermoedelijke leeftijd van gebruikers te bepalen, wat leidt tot een intensievere vorm van gebruikerssurveillance.

Deze ontwikkeling heeft geleid tot een levendig maatschappelijk debat over de juiste balans tussen bescherming van minderjarigen en het respecteren van gebruikersprivacy. Criticasters wijzen op het risico van overmatige controle en mogelijke foutieve classificaties, terwijl voorstanders benadrukken dat de bescherming van kwetsbare gebruikers prioriteit moet krijgen.

Nauwkeurigheidskwesties

De AI-technologie is niet onfeilbaar en kan leiden tot foutieve categorisering. Volwassen gebruikers kunnen onterecht als tiener worden aangemerkt, wat resulteert in beperkte toegang tot content en onnodige verificatieprocedures. Deze fouten kunnen frustrerend zijn en leiden tot een minder prettige gebruikerservaring.

Privacy-implicaties

Het systeem analyseert kijkgedrag en accountactiviteit, wat vragen oproept over de mate waarin YouTube gebruikersgegevens mag verzamelen en interpreteren. Deze vorm van automatische profiling gaat verder dan het gebruik van vrijwillig verstrekte informatie en vormt een nieuwe dimensie in het privacydebat.

Reactie van Google

Google en YouTube benadrukken dat de bescherming van kinderen en tieners hun hoogste prioriteit heeft. De invoering van deze technologie komt mede voort uit toenemende druk van overheden wereldwijd om jongeren beter te beschermen tegen schadelijke online inhoud en praktijken.

Ondanks de controverses rond het nieuwe systeem, lijkt het erop dat platforms zoals YouTube steeds meer geavanceerde methoden zullen blijven ontwikkelen om minderjarigen te beschermen. Dit past in een bredere trend waarbij technologiebedrijven onder toenemende maatschappelijke en wettelijke druk staan om verantwoordelijkheid te nemen voor de veiligheid van jonge gebruikers.

De vraag blijft echter of dergelijke maatregelen de juiste balans vinden tussen bescherming en privacy, en of ze effectief genoeg zijn zonder overmatig in te grijpen in de gebruikerservaring van volwassenen.



Hoe onderzoek ik wat er over mij op het Dark Web staat?

Wist u dat één op de drie Nederlanders al te maken heeft gehad met een datalek? Persoonlijke gegevens worden steeds vaker verhandeld op plekken waar u geen zicht op heeft.

In dit artikel ontdekt u hoe u kunt onderzoeken of uw persoonlijke informatie op het Dark Web is beland en wat u hiertegen kunt doen.

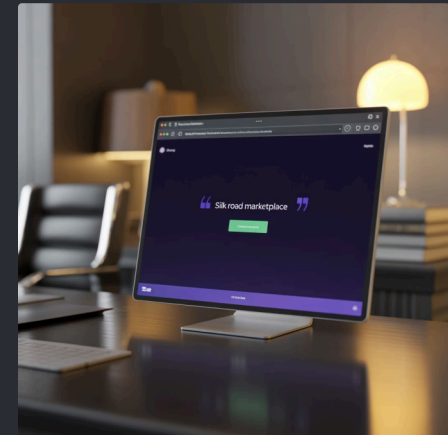
Willem Bosgra voor [VEILIGDIGITAAL.COM](https://veiligdigitaal.com)

Wat is het Dark Web?

Het Dark Web is een verborgen deel van het internet dat niet toegankelijk is via standaard browsers zoals Chrome, Firefox of Safari. Het vormt een klein maar significant onderdeel van het 'Deep Web' – alles wat niet geïndexeerd wordt door zoekmachines.

Dit gebied van het internet wordt vaak gebruikt voor illegale activiteiten, waaronder:

- Handel in gestolen persoonsgegevens
- Verkoop van gehackte accountgegevens
- Forums voor cybercriminelen
- Marktplaatsen voor illegale goederen en diensten



Om toegang te krijgen tot het Dark Web is speciale software nodig zoals de Tor-browser, die verkeer routeert via meerdere servers om de identiteit van gebruikers te verbergen.

Hoe komen mijn gegevens op het Dark Web?



Datalekken bij bedrijven

Recente grote datalekken bij Nederlandse zorginstellingen en telecombedrijven hebben miljoenen persoonsgegevens blootgesteld. Zelfs de meest voorzichtige internetgebruikers kunnen slachtoffer worden wanneer bedrijven gehackt worden.



Phishing en malware

Door op malafide links te klikken of besmette bijlagen te openen kunnen hackers toegang krijgen tot uw wachtwoorden en andere gevoelige informatie. Deze gegevens worden vervolgens vaak doorverkocht op het Dark Web.



Zwakke beveiligingsgewoonten

Het hergebruiken van wachtwoorden voor meerdere accounts betekent dat één lek kan leiden tot meerdere gecompromitteerde accounts. Cybercriminelen gebruiken geautomatiseerde tools om dit uit te buiten.

Hoe onderzoek ik of mijn data op het Dark Web staan?



Kies een betrouwbare scan-service

Gebruik diensten van gerenommeerde beveiligingsbedrijven zoals Norton, McAfee of Have I Been Pwned. Veel wachtwoordmanagers zoals 1Password en LastPass bieden deze functie ook aan.

Voer uw gegevens in

Verstrek uw e-mailadres of telefoonnummer. De service controleert deze tegen bekende databases van gelekte informatie die op het Dark Web circuleren.

Bekijk de resultaten

De scan toont welke van uw gegevens zijn gevonden, bij welke datalekken ze betrokken waren en wanneer dit is gebeurd. Dit geeft inzicht in welke accounts mogelijk gecompromitteerd zijn.

Welke data kan je terugvinden?

Inloggegevens

- E-mailadressen
- Gebruikersnamen
- Wachtwoorden (vaak gehashed of in plaintext)

Persoonlijke informatie

- Volledige naam
- Geboortedatum
- Telefoonnummers
- Woonadressen

Financiële gegevens

- Creditcardnummers
- Bankgegevens
- Fiscale informatie



Deze gegevens worden vaak gebundeld en verkocht in pakketten, waarbij criminelen kunnen zoeken op specifieke criteria. Hoe meer informatie beschikbaar is, hoe waardevoller het pakket voor potentiële kopers die identiteitsfraude willen plegen.



Wat kan ik doen als mijn gegevens gevonden zijn?



Wachtwoorden direct wijzigen

Verander onmiddellijk de wachtwoorden van alle betrokken accounts, beginnend met de meest belangrijke zoals e-mail, bankrekeningen en sociale media.



Beveiligingsmaatregelen versterken

Implementeer unieke, sterke wachtwoorden voor elke dienst. Overweeg een wachtwoordmanager te gebruiken om deze bij te houden. Schakel tweefactorauthenticatie (2FA) in waar mogelijk.



Blijf waakzaam

Controleer regelmatig uw accounts op verdachte activiteiten. Wees extra alert op phishingpogingen die uw gelekte gegevens kunnen gebruiken om geloofwaardiger te lijken.



Regelmatig scannen

Voer periodiek Dark Web-scans uit om nieuwe lekken te ontdekken. Stel indien mogelijk meldingen in voor toekomstige datalekken met uw gegevens.

Identificatie via wifi: De Onzichtbare Digitale Handtekening

In een baanbrekende ontwikkeling hebben wetenschappers een innovatieve methode ontdekt om mensen te identificeren aan de hand van de manier waarop hun lichaam interacteert met wifi-signalen. Deze technologie gebruikt standaard wifi-apparatuur om unieke verstoringsspatronen te detecteren die ontstaan wanneer een persoon zich door een ruimte beweegt. Het systeem analyseert deze patronen, die functioneren als een soort "digitale handtekening" die specifiek is voor ieder individu.

In dit artikel verkennen we de technische werking van deze identificatiemethode, de huidige onderzoeksresultaten en praktijktoepassingen, en de ethische vraagstukken die deze technologie met zich meebrengt in een wereld waar de grenzen tussen het fysieke en digitale domein steeds verder vervagen.

Willem Bosgra voor VEILIGDIGITAAL.COM

Identificatie via wifi: de technologie uitgelegd

De innovatieve technologie voor persoonlijke identificatie via wifi-signalen maakt gebruik van een fundamenteel principe: elk menselijk lichaam verstoort elektromagnetische golven op een unieke manier. Deze verstoring is afhankelijk van factoren zoals lichaamsgrootte, vorm, dichtheid, looppatroon en zelfs ademhalingsritme. Wetenschappers hebben ontdekt dat deze verstoringen kunnen worden geanalyseerd als een vorm van biometrische handtekening.

De technische kern van deze methode ligt in de analyse van Channel State Information (CSI). CSI is een verzameling metingen die beschrijft hoe een signaal zich verspreidt van zender naar ontvanger, inclusief effecten van reflectie, verstrooiing en diffractie. Wanneer een persoon door een ruimte loopt, verandert de CSI op een manier die kenmerkend is voor dat individu.

Het fascinerende aspect van deze technologie is de eenvoud van de benodigde apparatuur. Er zijn geen geavanceerde sensoren of dure hardware nodig - slechts een standaard wifi-router en een laptop met de juiste software. De router zendt signalen uit die door de omgeving weerkaatsen en veranderen wanneer ze in contact komen met een menselijk lichaam. De laptop vangt deze gewijzigde signalen op en analyseert de unieke patronen.



De signaalverstoringen worden verwerkt met geavanceerde machine learning-algoritmen die patronen herkennen en classificeren. Deze algoritmen leren de unieke kenmerken van iemands 'wifi-schaduw' te herkennen en kunnen deze later identificeren wanneer dezelfde persoon de ruimte betreedt.

Signaaluitzending

Een standaard wifi-router zendt elektromagnetische golven uit die zich door de ruimte verspreiden.

Signaalopvang

Een ontvanger (laptop) vangt de verstoorde signalen op en registreert de Channel State Information.

Lichaamsverstoring

Het menselijk lichaam absorbeert en reflecteert deze golven op een unieke manier, gebaseerd op lichaamskenmerken.

Patroonanalyse

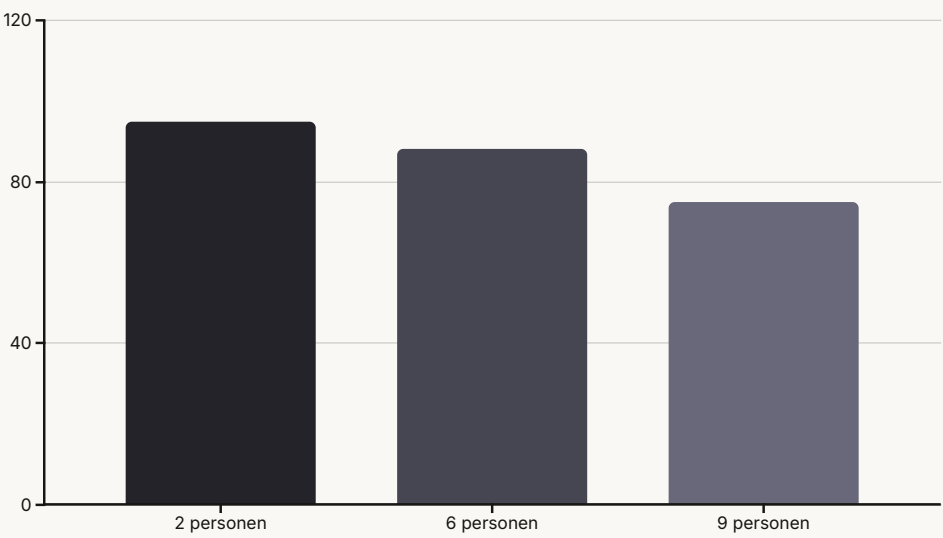
Machine learning-algoritmen analyseren de CSI-data en identificeren unieke patronen per individu.

De nauwkeurigheid van deze identificatiemethode wordt beïnvloed door verschillende factoren, waaronder de dichtheid van wifi-signalen in de ruimte, de bewegingssnelheid van de persoon, en de aanwezigheid van andere objecten die signalen kunnen verstoren. Desondanks hebben wetenschappers aangetoond dat de technologie voldoende robuust is om betrouwbare identificatie mogelijk te maken in gecontroleerde omgevingen.

Resultaten en ethische implicaties van wifi-identificatie

Onderzoeksresultaten

Het baanbrekende proof-of-concept onderzoek naar wifi-identificatie werd uitgevoerd in een slimme woonomgeving van 30 vierkante meter met negen vrijwilligers. De resultaten waren veelbelovend: het systeem kon individuele personen identificeren met een nauwkeurigheid van 75% wanneer ze één voor één werden geanalyseerd. Bij vergelijkingen tussen twee personen steeg de nauwkeurigheid tot indrukwekkende 95%, terwijl bij zes personen nog steeds 88% nauwkeurigheid werd behaald.



De beste resultaten werden behaald bij groepen van 2 tot 6 personen met verschillende lichaamstypes, wat aangeeft dat het contrast tussen fysieke kenmerken bijdraagt aan de effectiviteit van de identificatiemethode. Deze bevindingen sluiten aan bij vergelijkbaar onderzoek naar bewegingsmeters zoals Fitbit, die ook fysieke functies op een digitale wijze kwantificeren.

Ethische implicaties

Hoewel deze technologie een aanzienlijke vooruitgang betekent, roept ze ook belangrijke ethische vragen op. Een van de voornaamste voordelen is dat de methode non-intrusief en relatief privacyvriendelijk is vergeleken met camera's of traditionele biometrische identificatiemethoden. Er zijn geen beelden van personen nodig en de identificatie gebeurt zonder fysiek contact.

Potentiële toepassingen

- Verbeterde beveiliging voor gebouwen zonder invasieve controles
- Gezondheidszorg: valdetectie en bewegingsmonitoring voor ouderen
- Slimme thuisautomatisering die zich aanpast aan verschillende bewoners

Zorgen en risico's

- Ongewenste surveillance in openbare en privéruimtes
- Identificatie zonder toestemming of medeweten
- Vervaging van fysieke en digitale grenzen van het lichaam
- Druk op privacy en lichamelijke autonomie



"De vervaging tussen onze fysieke lichamen en digitale identiteit dwingt ons om opnieuw na te denken over wat privacy betekent in een wereld waar zelfs onze lichamelijke aanwezigheid digitale sporen achterlaat via alledaagse technologie zoals wifi." - Hypothetische privacy-expert

De maatschappelijke impact van deze technologie zal grotendeels afhangen van hoe ze wordt geïmplementeerd en gereguleerd. Als de technologie zonder beperkingen wordt toegepast, zou dit kunnen leiden tot een wereld waarin mensen constant worden geïdentificeerd zonder hun medeweten, simpelweg door in de buurt van een wifi-netwerk te komen. Anderzijds kunnen strenge regelgeving en ethische richtlijnen ervoor zorgen dat de technologie alleen wordt gebruikt voor specifieke, goedgekeurde doeleinden met expliciete toestemming van de betrokkenen.

Naarmate we verdergaan in een tijdperk waarin technologie steeds meer verweven raakt met ons dagelijks leven, wordt het essentieel om een evenwicht te vinden tussen innovatie en de bescherming van fundamentele rechten zoals privacy en autonomie. De ontwikkeling van wifi-identificatietechnologie benadrukt de noodzaak van een voortdurende maatschappelijke dialoog over deze kwesties.

In quarantaine plaatsen, verwijderen of opschonen: wat moet u doen aan een virus?

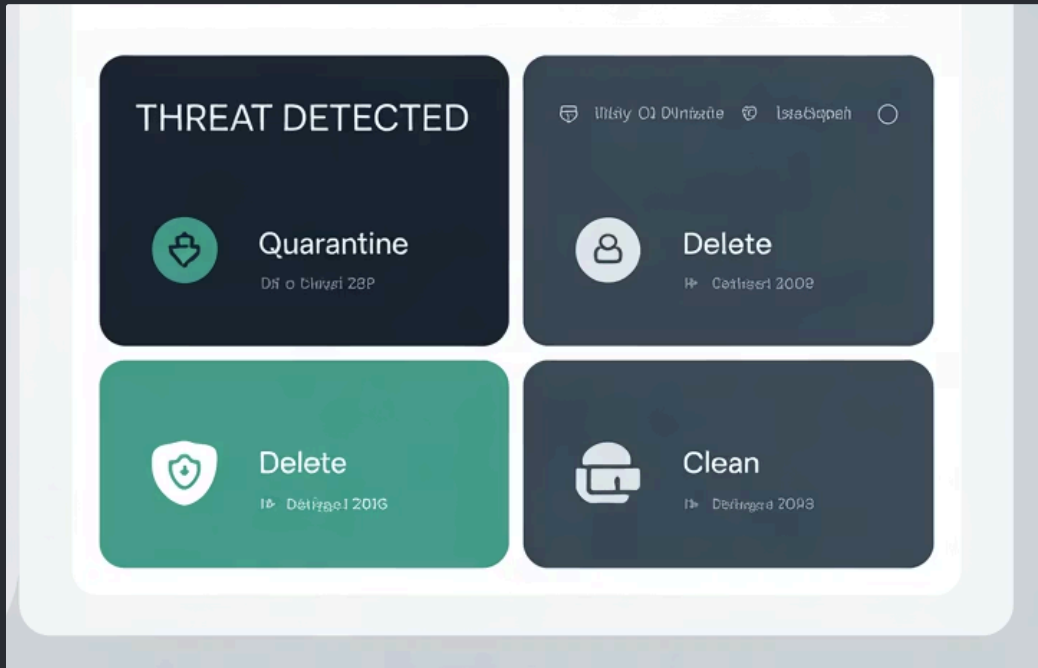
Wanneer uw antivirusprogramma een besmetting detecteert, krijgt u meestal verschillende opties om het probleem aan te pakken. Maar wat betekenen deze opties precies en wanneer gebruikt u welke?

In dit artikel leggen we uit wat quarantaine, verwijderen en opschonen inhouden en helpen we u de juiste beslissing te nemen om uw computer te beschermen.

VEILIGDIGITAAL.OM



Wat doen deze opties?



Quarantaine

Virus wordt geïsoleerd en het besmette bestand wordt onschadelijk gemaakt zonder het te verwijderen. Het blijft bewaard in een speciale beveiligde map.



Verwijderen

Het virus én het besmette bestand worden volledig verwijderd van uw systeem. Dit is een permanente actie die niet ongedaan kan worden gemaakt.



Opschonen

Het antivirusprogramma probeert de schadelijke code te verwijderen terwijl het originele bestand behouden blijft, waardoor gegevensverlies wordt voorkomen.

Quarantaine: hoe werkt het?

Stap 1: Isolatie

Het antivirusprogramma kopieert het besmette bestand naar een speciale, beveiligde map die niet toegankelijk is voor andere programma's.

Stap 2: Deactivatie

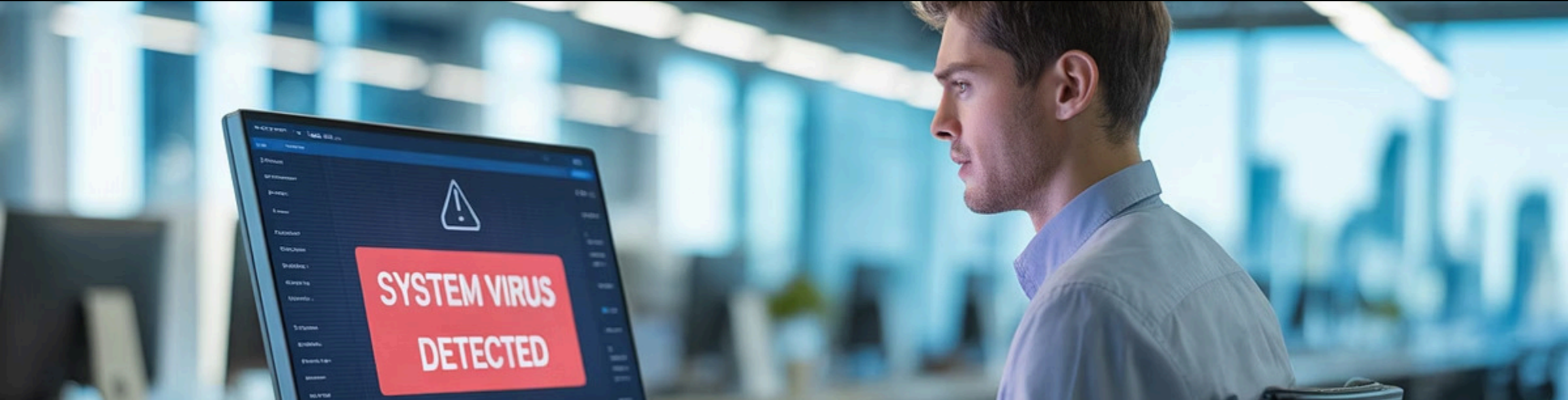
Het bestand wordt vervolgens onbruikbaar gemaakt voor het systeem en de gebruiker door speciale versleuteling of permissiewijzigingen.

Stap 3: Beheer

Alleen het antivirusprogramma heeft toegang tot de quarantainemap en kan bestanden terugzetten of permanent verwijderen.



Quarantaine is als een digitale isolatiecel: het virus zit opgesloten en kan geen schade aanrichten, maar is nog niet definitief verwijderd.



Wanneer quarantaine gebruiken?

Bij twijfel over betrouwbaarheid

Als u niet zeker weet of een bestand daadwerkelijk een virus bevat of een vals alarm is, kunt u het veilig in quarantaine plaatsen terwijl u meer onderzoek doet.

Bij onzekerheid over noodzaak

Wanneer u niet direct weet of het bestand belangrijk is voor uw systeem of programma's, geeft quarantaine u tijd om dit te bepalen zonder risico.

Als tijdelijke veiligheidsmaatregel

Quarantaine is ideaal als eerste verdedigingslinie terwijl u besluit of u het bestand definitief wilt verwijderen of proberen te herstellen.

Verwijderen: definitief weg



Verwijderen is een drastische maar effectieve maatregel die geen sporen van het virus achterlaat op uw systeem.

Permanente actie

Zowel het virus als de besmette bestanden worden volledig van uw systeem gewist zonder mogelijkheid tot herstel (tenzij u een back-up heeft).

Aanbevolen gebruik

Kies voor verwijderen bij bekende, gevaarlijke virussen of wanneer het besmette bestand niet noodzakelijk is voor uw systeem.

Mogelijke gevolgen

Als het virus systeembestanden heeft besmet, kan verwijderen leiden tot functieverlies of stabiliteitsproblemen die moeten worden hersteld.

Opschonen: herstel zonder verlies?

Wat gebeurt er?

Het antivirusprogramma analyseert het besmette bestand en identificeert de schadelijke code die moet worden verwijderd.



1

2

Beperkingen

Opschonen is niet altijd mogelijk en hangt af van het type malware. Sommige virussen zijn zo verweven met het bestand dat herstel onmogelijk is.

- Werkt goed bij eenvoudige virussen
- Minder effectief bij complexe malware
- Onmogelijk bij volledig gecompromitteerde bestanden

Resultaten

Bij succes behoudt u het originele bestand zonder de schadelijke code. Bij mislukking moet u alsnog kiezen voor quarantaine of verwijderen.

- Succespercentage varieert per type virus
- Risico op incomplete virusverwijdering

3



Praktische stappen bij een virus



Scannen en identificeren

Voer een volledige systeemscan uit met uw antivirusprogramma om alle besmette bestanden te vinden. Gebruik bij hardnekkige malware een offlinescan om virussen te detecteren die actieve scans kunnen omzeilen.



Quarantaine als eerste stap

Plaats verdachte bestanden eerst in quarantaine om de dreiging te isoleren terwijl u bepaalt of het bestand belangrijk is of niet. Dit geeft u tijd voor onderzoek zonder risico.



Verwijder indien nodig

Kies voor permanente verwijdering als het virus bekend of gevaarlijk is, of als het bestand niet essentieel is voor uw systeem. Herstel alleen uit quarantaine als u absoluut zeker bent van de veiligheid.

Conclusie: wat is de beste keuze?

Quarantaine

Gebruik quarantaine als u twijfelt of een bestand nodig is of als u vermoedt dat het een vals alarm betreft. Dit is een veilige tussenoplossing.

Verwijderen

Kies voor verwijderen bij onbekende of gevaarlijke bedreigingen, of wanneer u zeker weet dat het bestand niet nodig is voor uw systeem.

Opschonen

Probeer opschonen alleen bij betrouwbare bestanden die u wilt behouden en wanneer uw antivirusprogramma deze optie specifiek aanbeveelt.



Preventie is het beste medicijn

Voorkom virusbesmettingen door regelmatig updates uit te voeren, verdachte e-mails te vermijden, en alleen software van betrouwbare bronnen te downloaden. Een goede beveiliging begint met bewust gedrag.

A person with short brown hair, wearing glasses and a dark grey hoodie, is seated in a black and orange ergonomic chair. They are working at a desk with multiple computer monitors. The top monitor displays lines of code in a dark-themed editor. The middle monitor shows a network graph with a central bright node. The bottom monitor also displays code. A laptop is open in front of them. A desk lamp with a warm light is positioned above the desk. The background is a plain, light-colored wall.

Pro-Russisch Hackerscollectief NoName057(16) zegt: 'Het is tijd voor vergelding'

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

Een grootschalige internationale politieactie tegen het pro-Russische hackerscollectief NoName057(16) heeft midden juli plaatsgevonden onder leiding van Europol. Ondanks de inbeslagname van servers, arrestatiebevelen en huiszoekingen blijkt de hackersgroep nu actiever dan ooit, met een duidelijke boodschap op Telegram: "Het is tijd voor vergelding".

Dit artikel beschrijft de operatie, de werkwijze van de hackersgroep en de aanhoudende dreiging die zij vormen in het cyberlandschap.

Operatie Eastwood: Een Gecoördineerde Wereldwijde Aanpak

Van 14 tot 17 juli 2025 voerden Europol en Eurojust een ambitieuze internationale operatie uit tegen het hackerscollectief NoName057(16). Deze actie, codenaam Operatie Eastwood, omvatte een ongekennde samenwerking tussen rechtshandhavingsinstanties uit twaalf verschillende landen, waaronder Nederland, Duitsland, Spanje en Frankrijk.

Infrastructurele Impact

Tijdens de operatie werden meer dan 100 servers wereldwijd uitgeschakeld, waardoor een significant deel van de centrale infrastructuur van de groep werd platgelegd. Dit was een gerichte poging om het netwerk van de hackersgroep te ontmantelen en hun operationele capaciteit aanzienlijk te verzwakken.

Juridische Acties

De autoriteiten vaardigden zeven internationale arrestatiebevelen uit, waarvan zes door Duitsland gericht waren op Russische verdachten, inclusief twee hoofdverdachten die vermoedelijk leidinggevende rollen vervulden binnen de organisatie. Daarnaast werden 24 huiszoeken uitgevoerd in verschillende Europese landen en werden 13 personen ondervraagd.

Als preventieve maatregel werden meer dan 1.100 vermeende supporters en 17 beheerders van de groep via Telegram gewaarschuwd over hun strafrechtelijke aansprakelijkheid. Deze waarschuwingen benadrukten de ernst van hun betrokkenheid bij cybercriminele activiteiten en de mogelijke juridische gevolgen daarvan.

NoName057(16): Werkwijze, Impact en Reactie

Oorsprong en Motivatie

NoName057(16) is een pro-Russisch hacktivistisch collectief dat sinds maart 2022, kort na het begin van de Russische invasie in Oekraïne, actief is. De groep voert zijn activiteiten uit als onderdeel van een bredere hybride oorlogsvoering, met vermoedelijke banden met Russische inlichtingendiensten.

Aanvalstechnieken

De primaire methode van NoName057(16) bestaat uit gecoördineerde DDoS-aanvallen (Distributed Denial of Service), waarbij websites worden overspoeld met verkeer tot ze crashen. De groep heeft duizenden van dergelijke aanvallen uitgevoerd tegen Oekraïne en landen die Oekraïne steunen.

Mobilisatie en Rekrutering

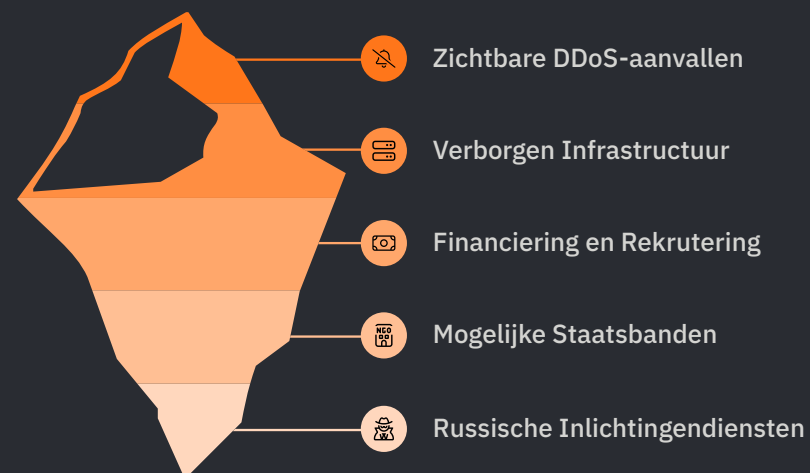
Via Telegram mobiliseerde de groep ongeveer 4.000 vrijwilligers. Om deelname te stimuleren, implementeerden ze gamification-elementen zoals leaderboards en boden ze cryptovaluta-beloningen aan voor succesvolle aanvallen, wat een laagdrempelige instap creëerde voor amateur-hackers.

De doelwitten van NoName057(16) omvatten een breed spectrum aan kritieke infrastructuur, waaronder overheidsinstanties, banken, energiebedrijven en defensiebedrijven in landen zoals Duitsland, Zweden, Zwitserland en Nederland. Hun tactiek is niet zozeer gericht op het veroorzaken van permanente schade, maar eerder op het creëren van tijdelijke verstoringen en het ondermijnen van het vertrouwen in de cyberveiligheid van de getroffen organisaties.

⚠ Ondanks de omvangrijke politieactie blijft NoName057(16) actief en heeft de groep via hun Telegram-kanaal nieuwe aanvallen aangekondigd met de dreigende boodschap: "Het is tijd voor vergelding." Dit suggereert dat de groep vastbesloten is om hun activiteiten voort te zetten en mogelijk zelfs te intensiveren als reactie op de internationale operatie.

Conclusie: De Blijvende Dreiging en Internationale Samenwerking

Hoewel Operatie Eastwood een significante klap heeft toegebracht aan de infrastructuur van NoName057(16), blijft de fundamentele dreiging bestaan. De kernleden van de organisatie bevinden zich hoogstwaarschijnlijk in Rusland, buiten het bereik van Europese en Amerikaanse rechtshandhaving, wat hen in staat stelt hun netwerk relatief snel te herbouwen.



De ongekennde samenwerking tussen Europol, Eurojust, FBI en diverse Europese politiediensten tijdens deze operatie onderstreept het groeiende besef dat cyberdreigingen alleen effectief kunnen worden aangepakt door middel van gecoördineerde internationale inspanningen. Deze samenwerking is essentieel geworden in het bestrijden van moderne hybride dreigingen die nationale grenzen overschrijden.



Versterkte Cyberverdediging

Organisaties moeten investeren in robuuste cybeveiligheidsmaatregelen, met name bescherming tegen DDoS-aanvallen, en regelmatig hun beveiligingsprotocollen evalueren.



Internationale Samenwerking

Verdere versterking van grensoverschrijdende samenwerking tussen rechtshandavingsinstanties en inlichtingendiensten is cruciaal voor effectieve bestrijding.



Waakzaamheid

Verhoogde alertheid is noodzakelijk, vooral tijdens politiek gevoelige gebeurtenissen die mogelijk doelwitten vormen voor vergeldingsacties.

Deze operatie benadrukt dat cyberoorlogsvoering en hacktivisme niet langer marginale fenomenen zijn, maar integraal onderdeel zijn geworden van moderne geopolitieke conflicten. Het vereist een holistische aanpak waarbij technologische, juridische en diplomatieke middelen worden gecombineerd om deze complexe dreigingen het hoofd te bieden. Terwijl NoName057(16) haar activiteiten voortzet, blijft de digitale frontlinie een cruciaal slagveld in de bredere geopolitieke spanningen tussen Rusland en het Westen.

Klik pas op die korte link als je zeker weet dat deze veilig is

In het huidige digitale tijdperk waar informatie snel gedeeld wordt via sociale media, e-mails en berichten, zijn verkorte links een veelvoorkomend fenomeen. Ze nemen minder ruimte in beslag en zien er netter uit in communicatie. Maar deze ogenschijnlijk handige hulpmiddelen kunnen een verborgen gevaar vormen.

Dit document legt uit waarom korte links risicovol kunnen zijn, hoe je kunt controleren of een link veilig is voordat je erop klikt, en welke tools je kunt gebruiken om jezelf te beschermen tegen digitale bedreigingen.

Met de juiste kennis en voorzorgsmaatregelen kun je veilig navigeren in de online wereld zonder slachtoffer te worden van cybercriminelen die misbruik maken van je vertrouwen.

Willem Bosgra voor VEILIGDIGITAAL.COM

Waarom zijn korte links soms gevaarlijk?

Verborgen bestemmingen

Korte links (zoals bit.ly of tinyurl.com) maskeren het originele webadres volledig. Je ziet alleen een verkorte versie, waardoor je geen idee hebt waar je terecht zult komen als je erop klikt. Dit gebrek aan transparantie maakt ze perfect voor kwaadwillenden die hun ware bedoelingen willen verbergen.

Misbruik door cybercriminelen

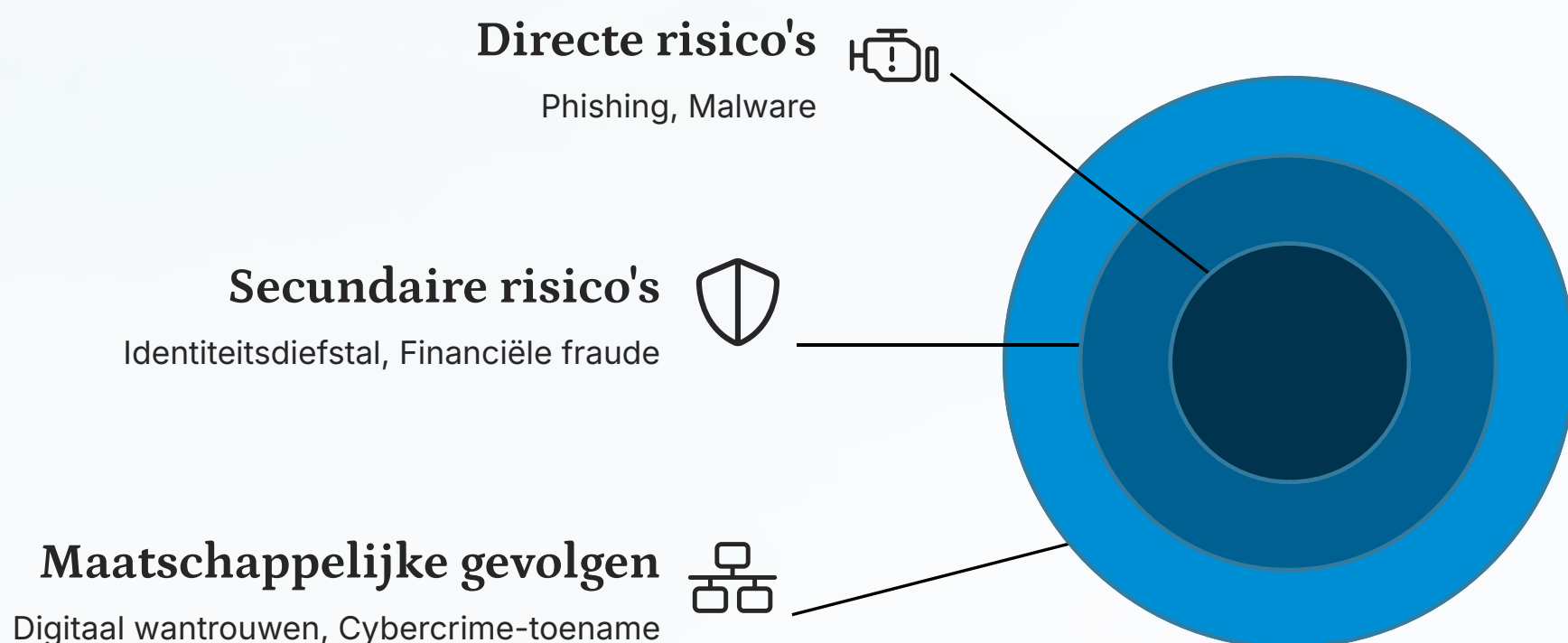
Hackers en oplichters gebruiken verkorte links vaak als onderdeel van hun aanvalsstrategie. Ze kunnen leiden naar:

- Phishingwebsites die eruitzien als legitieme inlogpagina's
- Downloads die malware of ransomware bevatten
- Oplichterssites die persoonlijke of financiële gegevens stelen

Spoofing van vertrouwde bronnen

Cybercriminelen doen zich vaak voor als betrouwbare organisaties zoals banken, overheidsinstanties of bekende bedrijven. Zelfs als een bericht lijkt te komen van een bekende persoon of organisatie, kan het een vervalsing zijn met kwade bedoelingen.

De dreiging van korte links is geen theoretische kwestie, maar een groeiend probleem in de cyberbeveiligingswereld. Deskundigen voorspellen dat tegen 2025 het aantal phishingpogingen via verkorte links opnieuw significant zal toenemen. Dit komt deels doordat veel mensen nog steeds niet volledig bewust zijn van de risico's die deze links met zich meebrengen.



Wat het risico vergroot is dat deze aanvallen steeds geavanceerder worden. Waar vroeger phishingpogingen vaak herkenbaar waren aan slecht taalgebruik of opvallende fouten, zijn hedendaagse aanvallen vaak zeer geprofessionaliseerd. Ze maken gebruik van correcte huisstijlen, foutloos taalgebruik en overtuigende sociale-engineeringtactieken om slachtoffers te manipuleren. Het enige dat je soms nog kan waarschuwen is dat vreemde, verkorte link die je wordt gevraagd te volgen.

Hoe controleer je of een korte link veilig is?

Preventieve maatregelen



Hover voordat je klikt

Beweeg op een computer je muiscursor over de link zonder te klikken. In de meeste browsers verschijnt dan de werkelijke bestemming linksonder in beeld.



Lang indrukken op mobiel

Houd op je smartphone of tablet de link langer ingedrukt. Er verschijnt een menu waar je het volledige adres kunt bekijken zonder de link te openen.



Verifieer de URL

Controleer of het webadres klopt: bevat het rare spelfouten, ongebruikelijke domeinnamen of onverwachte extensies? Kijk of het adres overeenkomt met de afzender.



Bij twijfel is het altijd veiliger om de link niet te openen en contact op te nemen met de vermeende afzender via een ander, betrouwbaar kanaal. Vraag of zij daadwerkelijk een link hebben gestuurd en wat de bedoeling ervan is.

Wees extra voorzichtig met links die je ontvangt via:

- Onverwachte e-mails of berichten
- Sms'jes van onbekende nummers
- Sociale media van contacten die je lang niet hebt gesproken
- Berichten die aandringen op directe actie

Handige tools en informatiebronnen

Tool/Bron	Functionaliteit	Voordelen
Checkjelinkje.nl	Analyseert links op veiligheid door ze te ontleden en te controleren tegen bekende dreigingsdatabases	Gratis, Nederlands, gebruiksvriendelijk, geeft duidelijke veiligheidsbeoordelingen
Urlverkorten.com	Controleert automatisch met Google Safe Browsing en Phish Tank voordat een link wordt verkort	Ingebouwde beveiligingscontrole, dubbele verificatie tegen malware/phishing
VeiligInternet.nl	Biedt actuele informatie over online veiligheid en specifieke dreigingen	Betrouwbare bron, regelmatige updates over nieuwe gevaren
ScamCheck	Communityplatform waar gebruikers verdachte links kunnen melden en controleren	Crowdsourced veiligheidsinformatie, snelle waarschuwingen voor nieuwe scams

Het is belangrijk om te onthouden dat geen enkele tool 100% bescherming biedt. Digitale veiligheid vereist een combinatie van technische oplossingen en gezond verstand. Als je twijfelt over een link, zelfs nadat deze door een controletool als veilig is beoordeeld, vertrouw dan op je intuïtie en vermijd het klikken. Een moment van voorzichtigheid kan je veel ellende besparen in de vorm van gestolen gegevens, financiële verliezen of gecompromitteerde apparaten.

Houd jezelf op de hoogte van de nieuwste ontwikkelingen op het gebied van cyberveiligheid via betrouwbare bronnen. Cybercriminelen veranderen voortdurend hun tactieken, dus wat je vandaag weet over veilig online gedrag kan morgen verouderd zijn. Blijf alert en deel je kennis met vrienden en familie, vooral met diegenen die minder digitaal vaardig zijn.

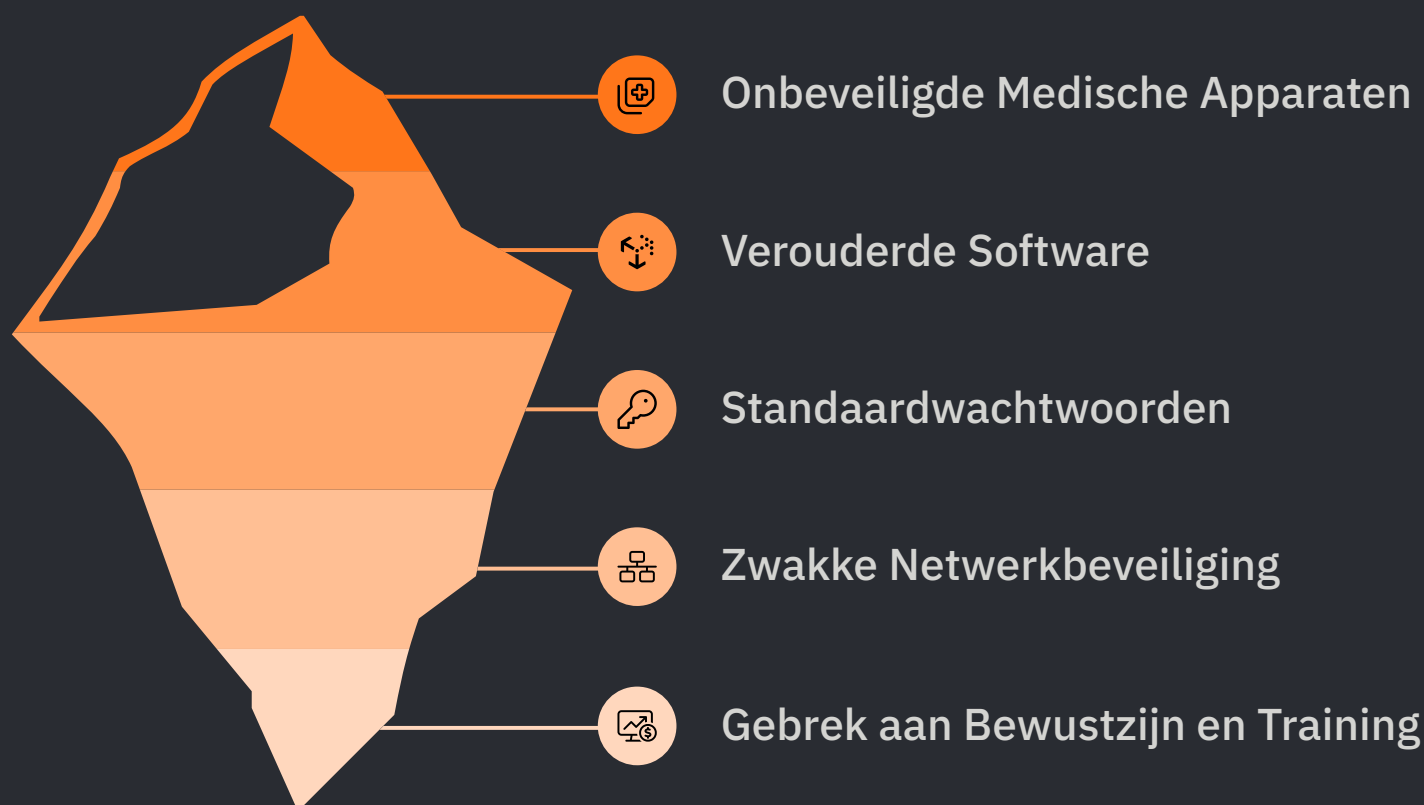


Meer dan 1,2 miljoen medische apparaten en systemen onbeveiligd online: een groeiend cybersecurityrisico in de zorg

Wereldwijd staan meer dan 1,2 miljoen medische apparaten en systemen onbeveiligd verbonden met het internet, wat een ernstige bedreiging vormt voor de patiëntveiligheid en privacy.

Dit artikel beschrijft de omvang van dit groeiende probleem, identificeert specifieke kwetsbare apparaten, analyseert de potentiële gevolgen van cyberaanvallen op de zorgsector en biedt aanbevelingen voor betere beveiliging in deze kritieke infrastructuur.

De omvang van het probleem: miljoenen kwetsbare medische apparaten online



Recent onderzoek heeft een alarmerende situatie aan het licht gebracht: wereldwijd zijn meer dan 1,2 miljoen medische apparaten en systemen direct toegankelijk via het internet zonder adequate beveiliging. Deze situatie vormt een groot risico voor zorginstellingen, waarbij essentiële apparatuur zoals MRI-scanners, infuuspompen en patiëntmonitoren vaak verbonden zijn met netwerken en soms zelfs rechtstreeks met het openbare internet.

De kwetsbaarheid van deze apparaten wordt versterkt door verschillende factoren:

Verouderde software

Veel medische apparaten draaien op verouderde besturingssystemen die niet meer worden ondersteund of niet regelmatig worden bijgewerkt met beveiligingspatches.

Standaardwachtwoorden

Tallose apparaten gebruiken nog steeds de fabrieksinstellingen en standaardwachtwoorden, wat ongeautoriseerde toegang vergemakkelijkt.

Ontbrekende updates

Essentiële beveiligingsupdates worden vaak niet geïnstalleerd vanwege zorgen over compatibiliteit of onderbreking van kritieke diensten.

Beveiligingsonderzoekers hebben ontdekt dat sommige ziekenhuizen duizenden apparaten in gebruik hebben met inadequate beveiliging. Deze situatie creëert een uitgebreid aanvalsoppervlak voor kwaadwillenden, wat niet alleen de patiëntveiligheid in gevaar brengt maar ook een bedreiging vormt voor de privacy van gevoelige medische gegevens.

Kwetsbare medische apparaten en de gevaren van hacking



Meest kwetsbare apparaten

- Infuuspompen met draadloze verbindingen
- Pacemakers en implanteerbare apparaten
- Patiëntmonitoren en vitale functiesensoren
- Draagbare gezondheidsapparatuur met BLE-technologie
- Netwerkverbonden diagnostische apparatuur

Onderzoekers hebben aangetoond dat veel medische apparaten ernstige beveiligingslekken vertonen die kunnen worden misbruikt.



Infuuspompen

Via draadloze verbindingen kunnen hackers medicijndoseringen manipuleren, wat direct levensbedreigend kan zijn. ICS-CERT heeft meerdere ernstige kwetsbaarheden ontdekt in draadloos verbonden infuuspompen.



Pacemakers

In 2018 werden ernstige beveiligingslekken gevonden in Medtronic-pacemakers die op afstand gehackt konden worden, wat leidde tot aanpassingen om potentieel terrorisme te voorkomen.



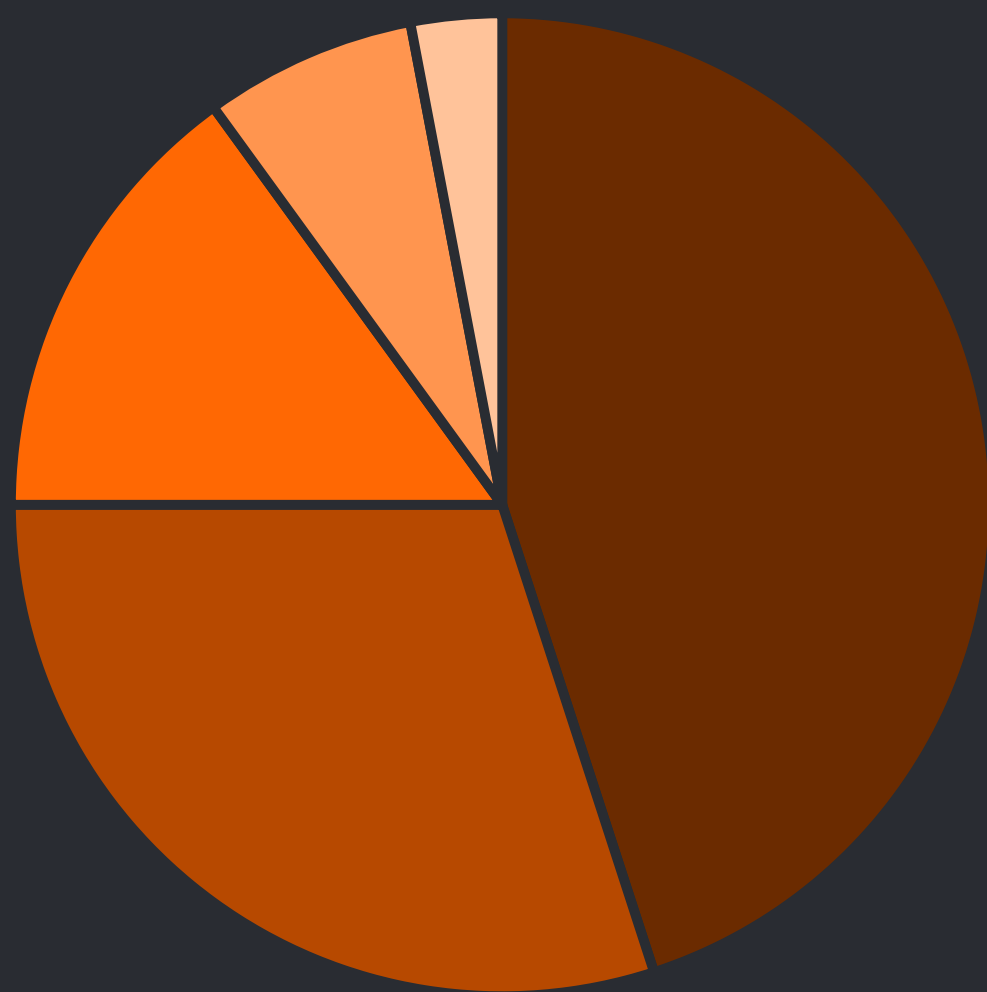
Patiëntmonitoren

Onderzoek van McAfee toonde aan dat hackers vitale functiemetingen kunnen vervalsen, wat kan leiden tot verkeerde diagnoses en potentieel schadelijke behandelingen.

- ⊗ Hackers kunnen via onbeveiligde medische apparaten toegang krijgen tot het bredere ziekenhuisnetwerk, wat kan leiden tot grootschalige datalekken en ransomware-aanvallen die de gehele zorgverlening kunnen verstoren.

Draagbare gezondheidsapparatuur met Bluetooth Low Energy (BLE) vertoont ook ernstige kwetsbaarheden. Onderzoekers hebben aangetoond dat deze apparaten kunnen worden gekaapt om gevaarlijke trillingen of schokken te veroorzaken, zoals bij medische elektro-stimulators die ongecontroleerde elektrische impulsen kunnen afgeven aan patiënten.

Gevolgen en noodzakelijke maatregelen voor de zorgsector



Ransomware Gegevensdiefstal Phishing Apparaathacking Overig

Cyberaanvallen op medische apparatuur kunnen verstrekken gevolgen hebben, van verkeerde behandelingen en directe gezondheidsrisico's tot massale diefstal van gevoelige patiëntgegevens. De zorgsector behoort tot de meest gehackte sectoren in Nederland, waarbij ransomwareaanvallen in 2022 minstens één op de 42 zorgorganisaties troffen.

De aankomende NIS2-richtlijn

01

Strengere beveiligingseisen

De NIS2-richtlijn verplicht zorginstellingen tot het implementeren van robuuste cybersecurity-maatregelen en risicoanalyses.

02

Preventieve maatregelen

Organisaties moeten proactief beveiligingsmaatregelen nemen om cyberaanvallen te voorkomen en te detecteren.

03

Verhoogde aansprakelijkheid

Bestuurders kunnen persoonlijk aansprakelijk worden gesteld bij nalatigheid in het implementeren van adequate cybersecurity.

Aanbevolen maatregelen

Segmentatie van netwerken

Medische apparaten alleen op netwerken aansluiten als strikt noodzakelijk en deze isoleren van andere netwerken.

Regelmatige kwetsbaarheidsscans

Periodiek onderzoeken van apparaten op beveiligingslekken en deze direct verhelpen.

Bewustwording personeel

Zorgmedewerkers trainen in het herkennen van cyberdreigingen en veilig gebruik van medische apparatuur.

Samenwerking met fabrikanten

Actieve dialoog onderhouden met leveranciers over beveiligingsupdates en -patches.

Fabrikanten en zorgverleners werken steeds vaker samen aan betere beveiligingsstandaarden en transparantie rondom kwetsbaarheden, onder andere via initiatieven van Health-ISAC en strengere productbeveiligingsvereisten. Het is cruciaal dat de sector investeert in adequate beveiliging om boetes, reputatieschade en vooral patiëntveiligheidsincidenten te voorkomen.

Conclusie: Cybersecurity in de zorg is urgent en onmisbaar

"Met meer dan 1,2 miljoen onbeveiligde medische apparaten online is het slechts een kwestie van tijd voordat kwaadwillenden deze kwetsbaarheden op grote schaal misbruiken."

Erkenning van het probleem

Zorginstellingen moeten de urgentie en omvang van cybersecurityrisico's erkennen als eerste stap naar verbetering.

Investing in beveiliging

Adequate financiële en personele middelen toewijzen aan beveiligingsmaatregelen en trainingen voor personeel.

Samenwerking in de sector

Kennisdeling tussen zorginstellingen, leveranciers en beveiligingsexperts om collectieve weerbaarheid te vergroten.

Continu verbeterproces

Cybersecurity als doorlopend proces implementeren, met regelmatige evaluaties en aanpassingen aan nieuwe dreigingen.

De digitale transformatie van de zorg brengt enorme voordelen met zich mee, maar creëert ook risico's die direct invloed hebben op mensenlevens. De onveilige situatie met meer dan een miljoen onbeveiligde medische apparaten vormt een tikkende tijdbom die dringend moet worden ontmanteld.

Door gezamenlijke inspanningen van fabrikanten, zorginstellingen en regelgevers kan de cyberweerbaarheid worden versterkt en kunnen patiënten beter worden beschermd. Het is essentieel dat alle betrokkenen nu actie ondernemen om de veiligheid van medische apparatuur te waarborgen en zo de integriteit van de zorg voor de toekomst te behouden.



Uitstel van adequate cybersecuritymaatregelen in de zorgsector kan leiden tot ernstige incidenten met directe gevolgen voor patiëntveiligheid, privacy en continuïteit van zorg.



Nepnieuws, porno, scams: hoe Denemarken deepfakes aanpakt

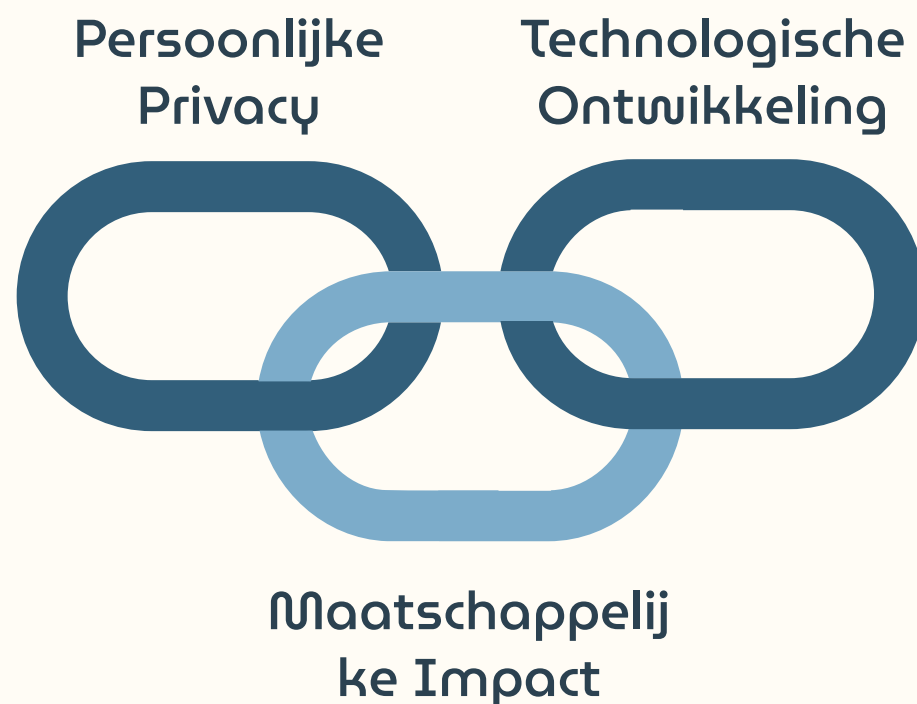
AI Generated

Denemarken neemt een baanbrekende stap in de strijd tegen deepfakes door als eerste land ter wereld burgers eigendomsrecht te geven over hun gezicht en stem. In een tijd waarin kunstmatige intelligentie steeds geavanceerder wordt, biedt deze innovatieve wetgeving bescherming tegen misbruik van digitale identiteit. Dit document analyseert de Deense aanpak, beschrijft de context van toenemende deepfake-problematiek, verkent de unieke wetgeving, belicht praktijkvoorbeelden van misbruik en vergelijkt de Deense aanpak met andere Europese initiatieven.

Deense context: explosie van deepfakes en publieke bezorgdheid

Sinds 2023 heeft Denemarken te maken met een ongekeerde toename van AI-gegenereerde video's en audiofragmenten die nauwelijks van echt te onderscheiden zijn. Deze zogenaamde 'deepfakes' hebben geleid tot grote publieke bezorgdheid, vooral na een reeks incidenten waarbij de Deense premier slachtoffer werd van gemanipuleerde video's die massaal werden verspreid via sociale media.

De technologie achter deepfakes wordt steeds toegankelijker, waardoor de drempel voor het maken van overtuigende vervalsingen drastisch is verlaagd. Wat ooit geavanceerde softwarekennis vereiste, kan nu met eenvoudige apps worden gerealiseerd. Dit heeft geleid tot een exponentiële groei van het fenomeen, waarbij deepfakes voornamelijk worden ingezet voor drie doeleinden: het verspreiden van misleidende informatie, het manipuleren van iemands beeltenis en het plegen van fraude.



De politieke betrokkenheid bij dit onderwerp is in Denemarken bijzonder hoog. Parlementariërs van vrijwel alle partijen hebben hun bezorgdheid geuit over de bedreiging die deepfakes vormen voor de democratie en persoonlijke integriteit. Deze brede politieke consensus heeft bijgedragen aan de snelle ontwikkeling van wetgeving. Tegelijkertijd hebben Deense media uitgebreid aandacht besteed aan het onderwerp, met speciale uitzendingen, diepgaande reportages en publieke debatten over de ethische grenzen van AI-technologie.

De Deense bevolking toont zich in opiniepeilingen uitzonderlijk bezorgd over deepfakes, met meer dan 75% van de respondenten die aangeeft dat ze vrezen voor misbruik van hun digitale identiteit. Deze maatschappelijke druk, gecombineerd met enkele spraakmakende incidenten waarbij gewone burgers slachtoffer werden van identiteitsfraude via deepfakes, heeft de politieke wil versterkt om met effectieve wetgeving te komen.

Unieke nieuwe wet: copyright op gezicht en stem

Denemarken heeft een revolutionaire aanpak gekozen in de strijd tegen deepfakes door de bestaande auteursrechtwet aan te passen. Deze innovatieve wetswijziging kent Deense burgers voor het eerst ter wereld expliciet juridisch eigendomsrecht toe op hun gezicht, lichaam en stem. In essentie betekent dit dat iemands fysieke kenmerken nu dezelfde wettelijke bescherming genieten als creatieve werken zoals boeken, muziek of films.

Eigendomsrecht

Elke Deense burger krijgt automatisch auteursrecht op eigen gezicht, lichaam en stem - zonder registratie nodig.

Toestemmingsvereiste

Gebruik van iemands uiterlijke kenmerken voor AI-generatie vereist expliciete voorafgaande toestemming.

Verwijderingsplicht

Platforms moeten deepfakes binnen 24 uur verwijderen na melding door het slachtoffer.

De wetgeving stelt ondubbelzinnig dat het ongewenst gebruik van iemands uiterlijk of stem zonder expliciete toestemming voortaan illegaal is. Dit geldt voor elke vorm van AI-gegenereerde content waarin iemands beeltenis wordt gebruikt, of dit nu voor commerciële, politieke of persoonlijke doeleinden is. Hiermee gaat Denemarken verder dan enkel het verbieden van kwaadaardige toepassingen; de wet stelt het principe vast dat mensen fundamenteel zeggenschap hebben over hun digitale representatie.

Een cruciaal element in de nieuwe wetgeving is de verantwoordelijkheid die wordt gelegd bij online platforms en sociale medianetwerken. Deze zijn nu wettelijk verplicht om deepfakes op verzoek van het slachtoffer te verwijderen. Indien zij hieraan geen gehoor geven, riskeren zij aanzienlijke boetes die kunnen oplopen tot 6% van hun wereldwijde jaaromzet. Deze financiële afschrikking moet ervoor zorgen dat platforms proactief handelen tegen misbruik.



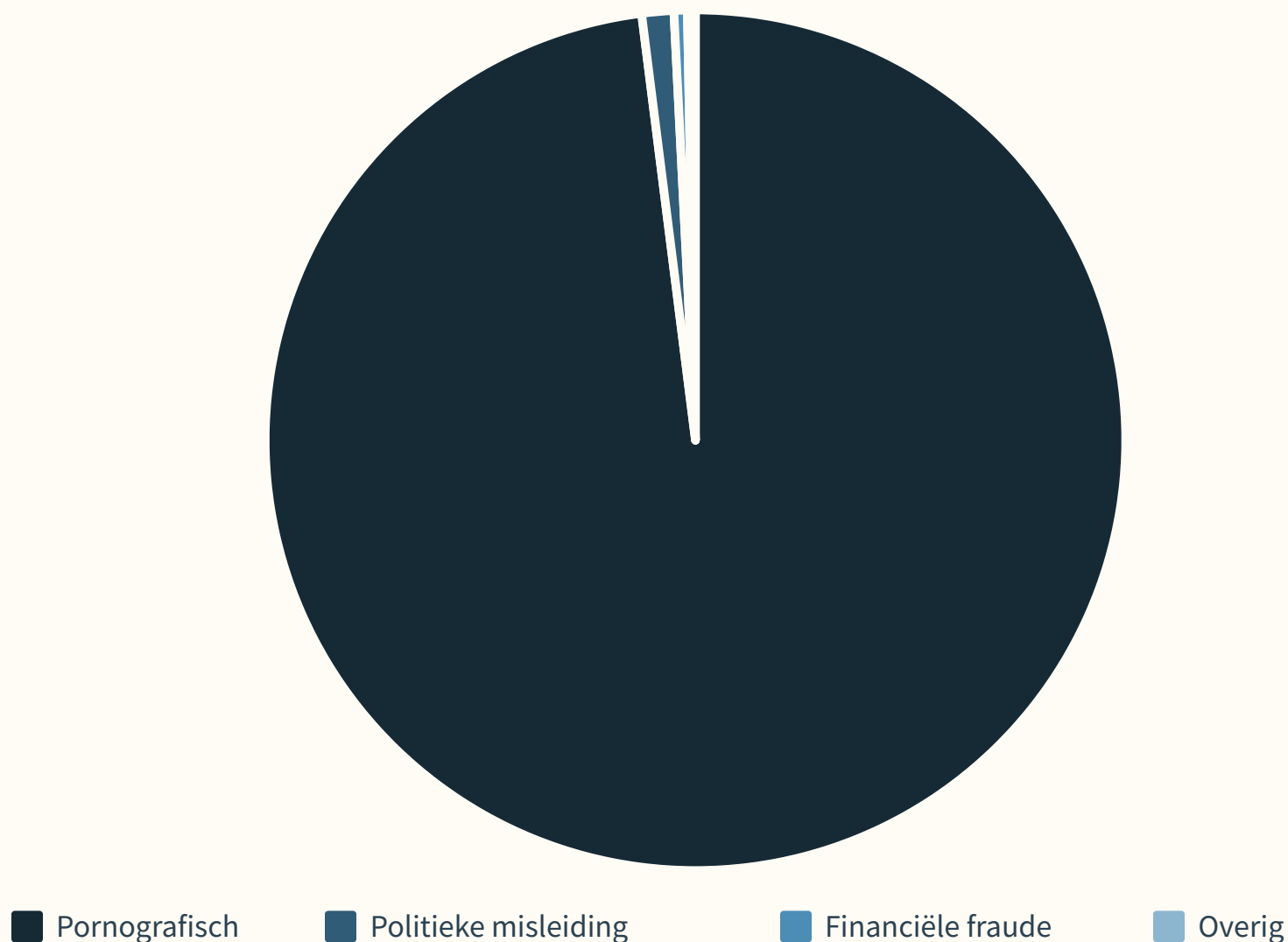
De wet werd met een overweldigende meerderheid van 90% aangenomen in het Deense parlement, wat de brede politieke consensus over dit onderwerp onderstreept. De implementatie verloopt via een uniek samenwerkingsmodel tussen overheid, technologiebedrijven, maatschappelijke organisaties en academische instellingen.

Voor slachtoffers van deepfakes is een laagdrempelige meldingsprocedure ingericht, waarbij een speciaal opgericht expertisecentrum ondersteuning biedt bij het identificeren en aanpakken van misbruik. Dit centrum fungeert tevens als kennisbank en adviesorgaan voor de verdere ontwikkeling van het beleid rond digitale identiteitsbescherming.

Een historische stemming in het Deense parlement toonde brede steun voor de nieuwe wetgeving.

Deepfakes in praktijk: nepnieuws, porno en digitale scams

De realiteit van deepfakes in Denemarken en wereldwijd is alarmerend. Volgens een onderzoek van het cyberbeveiligingsbedrijf Security Hero was maar liefst 98% van alle deepfakevideo's in 2023 pornografisch van aard. Deze vorm van digitaal geweld treft voornamelijk vrouwen, waarbij hun gezichten zonder toestemming worden gemonteerd op pornografische beelden. De emotionele en psychologische schade voor slachtoffers is aanzienlijk, met gevallen van depressie, angst en zelfs zelfmoordgedachten als gevolg.



Naast pornografische deepfakes ziet Denemarken een zorgwekkende trend in het gebruik van deze technologie voor online oplichting. Criminelen creëren overtuigende video's of audiofragmenten waarin ze zich voordoen als familieleden of bekende personen in nood, om zo geld af te troggelen van nietsvermoedende slachtoffers. De Deense politie rapporteert een stijging van 200% in dit soort fraudegevallen sinds 2022.

Politieke manipulatie

Deepfakes van politici die controversiële uitspraken doen, verspreid via sociale media om verkiezingen te beïnvloeden of verdeeldheid te zaaien.

Reputatieschade

Nepschandalen gecreëerd door deepfakes van zowel beroemdheden als gewone burgers, resulterend in sociale stigmatisering en carrièreschade.

Financiële oplichting

Gemanipuleerde video's of audiofragmenten van CEO's die werknemers opdragen geld over te maken naar frauduleuze rekeningen.

De nieuwe Deense wet introduceert specifieke procedures voor verschillende typen deepfakes. Voor pornografische deepfakes is een versnelde verwijderingsprocedure ingesteld, waarbij platforms binnen 24 uur moeten handelen. Voor deepfakes die gericht zijn op het verspreiden van valse informatie, zoals nepnieuws of politieke misleiding, werkt de overheid samen met factcheckers en mediaorganisaties om snelle identificatie en correctie mogelijk te maken.

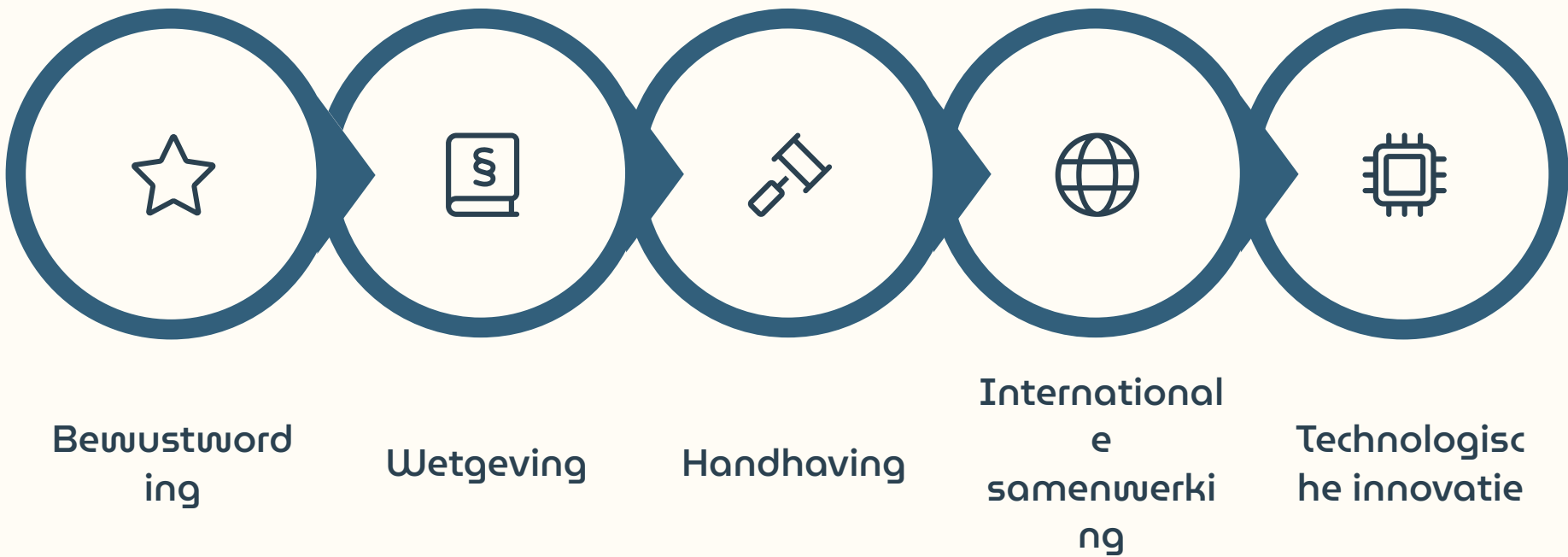
Slachtoffers van deepfakes kunnen nu ook aanspraak maken op schadevergoeding voor geleden emotionele en financiële schade. Een speciale juridische taskforce is opgericht om slachtoffers bij te staan in het verzamelen van bewijs en het voorbereiden van rechtszaken tegen makers en verspreiders van kwaadaardige deepfakes. Deze multidisciplinaire aanpak combineert technologische, juridische en psychologische ondersteuning om een omvattend vangnet te creëren voor getroffen personen.

Vergelijking en toekomst: Denemarken als koploper in Europa

Hoewel Denemarken een pioniersrol vervult met zijn innovatieve aanpak van deepfakes, hebben ook andere Europese landen stappen ondernomen om dit groeiende probleem aan te pakken. Frankrijk heeft in mei 2024 de SREN-wet (Sécurité et Réglementation de l'Espace Numérique) geïmplementeerd, die zware boetes en gevangenisstraffen oplegt voor het maken en verspreiden van deepfakes zonder toestemming. De Franse aanpak richt zich echter primair op strafrechtelijke vervolging en minder op het toekennen van eigendomsrechten aan burgers.

Land	Wetgeving	Belangrijkste maatregelen	Ingevoerd
Denemarken	Auteursrechtwet-amendement	Eigendomsrecht op gezicht en stem, verwijderingsplicht platforms	2024
Frankrijk	SREN-wet	Boetes tot €150.000 en 2 jaar gevangenis	Mei 2024
Verenigd Koninkrijk	Online Safety Act	Specifieke strafbaarstelling seksuele deepfakes	2023
EU breed	AI Act	Verplichte labeling AI-content, transparantievereisten	2024

Het Verenigd Koninkrijk heeft met de Online Safety Act van 2023 specifiek de creatie en verspreiding van seksuele deepfakes strafbaar gesteld, met gevangenisstraffen tot twee jaar. Deze wetgeving is echter beperkter in reikwijdte dan de Deense aanpak, aangezien zij zich voornamelijk richt op pornografische deepfakes en niet op andere vormen van identiteitsmisbruik.



Op EU-niveau wordt met de AI Act, die in 2024 in werking is getreden, een breder kader geschapen voor verantwoord AI-gebruik. Deze wetgeving verplicht onder meer de labeling van AI-gegenereerde content, maar gaat niet zo ver als de Deense wet in het toekennen van expliciete rechten aan burgers over hun digitale representatie. Denemarken positioneert zich nadrukkelijk als koploper en hoopt dat andere EU-landen hun voorbeeld zullen volgen.

De Deense overheid heeft aangekondigd de komende jaren aanzienlijk te investeren in technologische oplossingen voor de detectie van deepfakes. In samenwerking met technische universiteiten wordt gewerkt aan geavanceerde algoritmen die automatisch kunnen herkennen of content AI-gegenereerd is. Daarnaast zet Denemarken in op digitale geletterdheid, met speciale onderwijsprogramma's die burgers leren hoe ze deepfakes kunnen herkennen.

De verwachte impact van de Deense wetgeving is veelzijdig. Op korte termijn biedt het slachtoffers van deepfakes concrete juridische middelen om zich te verweren. Op middellange termijn moet het leiden tot een afname in de verspreiding van deepfake-scams en -pornografie door de afschrikwekkende werking van hoge boetes. Op lange termijn hoopt Denemarken bij te dragen aan een nieuwe internationale norm waarbij digitale identiteitsrechten even fundamenteel worden beschouwd als fysieke integriteit.

Net RFQ-fraude: Nieuwe Gevaarlijke Bedreiging voor Bedrijven

Nederlandse bedrijven worden in toenemende mate geconfronteerd met een nieuwe en geavanceerde vorm van fraude die sinds 2024 sterk in opmars is. Deze zogenaamde 'Net RFQ-fraude' (Request for Quotation) is een verfijnde social engineering-tactiek waarbij oplichters zich voordoen als inkopers van legitieme organisaties. Hun doel is het verkrijgen van kredietlijnen om waardevolle goederen te bemachtigen die vervolgens worden doorverkocht, wat leidt tot aanzienlijke financiële schade voor de getroffen ondernemingen.

Dit artikel belicht de werkwijze van deze fraudeurs, presenteert praktijkvoorbeelden van de aangerichte schade, en biedt concrete handvatten voor de herkenning en preventie van deze groeiende dreiging voor het Nederlandse bedrijfsleven.

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

Tactieken en Werkwijze van Net RFQ-Fraudeurs



Identiteitsdiefstal

Fraudeurs verzamelen BSN-nummers, DUNS-nummers, EINs en identiteitsgegevens van legitieme werknemers uit openbare bronnen of via datalekken. Deze informatie wordt gebruikt om geloofwaardige inkooppersonas te creëren.



Professionele Communicatie

Oplichters gebruiken lookalike domeinen (bijv. bedrijf-nl.com in plaats van bedrijf.nl) en creëren overtuigende e-mailhandtekeningen met gestolen bedrijfslogo's en correcte contactgegevens.



Offerteaanvraag

Er worden officieel ogende RFQ's verstuurd voor hoogwaardige producten zoals netwerkapparatuur, medische instrumenten en meetapparatuur. Deze bestellingen lijken volledig legitiem.



Kredietoplichting

Na ontvangst van offertes dringen fraudeurs aan op Net 15/30/45 betalingsvoorwaarden, vaak gecombineerd met verzoeken om snelle levering vanwege "dringende projectdeadlines".

Het meest kenmerkende aspect van deze fraudevorm is de strategische timing: het verzendadres wordt pas na goedkeuring van de kredietaanvraag bekendgemaakt. Dit adres blijkt dan vaak een locatie te zijn waar goederen worden omgeleid naar het buitenland, meestal West-Afrika, of naar tijdelijke opslaglocaties in binnen- of buitenland.

Veelgevraagde Producten

- Netwerkrouters en -switches
- Medische instrumenten en apparatuur
- Fluke meetinstrumenten
- Elektronica en computeronderdelen
- Industriële apparatuur

Verdachte Signalen

- Onbekende klant dringt aan op kredietfaciliteiten
- Afwijkende e-maildomeinen (kleine variaties)
- Ongebruikelijke haast bij bestellingen
- Verzendadres wordt laat gecommuniceerd
- Verzending naar ongebruikelijke locaties

De fraudeurs tonen vaak een diepgaande kennis van zakelijke inkoopprocessen en industriespecifieke terminologie, wat hun verzoeken bijzonder overtuigend maakt. Hun professionaliteit en de zorgvuldige voorbereiding van hun aanvallen onderscheidt deze vorm van fraude van eerdere, minder verfijnde pogingen.

Bedrijfsschade en Praktijkvoorbeelden

De financiële impact van Net RFQ-fraude op Nederlandse bedrijven is aanzienlijk en groeit met de dag. Slachtoffers rapporteren verliezen die oplopen tot tienduizenden euro's per incident, waarbij vooral hoogwaardige elektronische en medische apparatuur het doelwit vormt.

€52K

Gemiddelde schade

Per succesvol uitgevoerde frauduleuze bestelling

19

Frauduleuze domeinen

Geïdentificeerd door cybersecurity-teams in 2023-2024

63%

Toename incidenten

Stijging van Net RFQ-fraude gevallen sinds begin 2024

"We ontvingen een professionele offerteaanvraag van wat leek op een gerenommeerd ziekenhuis. Alles zag er legitiem uit - het logo, de handtekening, zelfs de specifieke medische terminologie. Pas nadat we €38.000 aan apparatuur hadden verzonden, ontdekten we dat het e-mailadres één letter afweek van het echte domein." - Directeur van een medisch toeleveringsbedrijf in Utrecht

Cybersecurity-teams hebben in de afgelopen maanden 19 frauduleuze domeinen kunnen identificeren die werden gebruikt voor deze vorm van oplichting. In enkele gevallen konden pakketten worden onderschept voordat ze hun eindbestemming bereikten, maar in de meeste situaties waren de goederen al doorgesluisd naar het buitenland voordat de fraude werd ontdekt.

Fraudestructuur en Logistiek

De oplichters maken gebruik van een gelaagde infrastructuur om de goederen te bemachtigen en door te sluizen. Dit omvat:

- Gehuurde magazijnen in industriegebieden die kortdurend worden gebruikt als afleveradres
- Onwetende tussenpersonen die als "mule" functioneren
- Professionele transportdiensten die pakketten internationaal doorsturen
- Woonadressen van medeplichtigen of gehackte bezorgaccounts



Fraudeurs gebruiken vaak tijdelijke opslaglocaties waar goederen worden verzameld voordat ze worden doorgestuurd naar het buitenland.

Uit onderzoek blijkt dat de criminele netwerken achter deze fraude vaak internationaal opereren, met coördinatoren in West-Afrika en Europa. De gestolen goederen worden snel doorverkocht op buitenlandse markten, wat de opsporing en het terughalen van de items vrijwel onmogelijk maakt. In sommige gevallen worden onwetende particulieren geronseld als tussenpersonen, waarbij ze pakketten ontvangen en doorsturen zonder te beseffen dat ze betrokken zijn bij criminele activiteiten.

Herkenning, Preventie en Aanbevelingen

Het herkennen en voorkomen van Net RFQ-fraude vereist een proactieve aanpak en verhoogde waakzaamheid binnen alle afdelingen die betrokken zijn bij het verkoopproces. Hieronder volgen de belangrijkste signalen waarop gelet moet worden en de aanbevolen preventieve maatregelen.

1

Identiteitsverificatie

Controleer altijd de identiteit van nieuwe klanten via meerdere, onafhankelijke kanalen:

- Bel het algemene nummer van het bedrijf (niet het nummer in de e-mail)
- Verifieer de bestelling via de officiële bedrijfswebsite
- Controleer de KVK-gegevens en bestaansgeschiedenis

2

E-maildomein Analyse

Let nauwkeurig op kleine afwijkingen in e-maildomeinen:

- Vergelijk met bekende, legitieme domeinen van de organisatie
- Wees extra alert bij gebruik van gratis e-mailproviders
- Controleer de domeinregistratiedatum (nieuwe domeinen zijn verdacht)

3

Betalingsvoorwaarden

Wees uiterst voorzichtig met kredietaanvragen:

- Stel strikte verificatieprocedures in voor Net 15/30/45 verzoeken
- Vraag om vooruitbetaling bij nieuwe klantrelaties
- Voer kredietscreening uit voordat goederen worden verzonden

4

Verzendadres Onderzoek

Controleer nauwgezet alle verzendlocaties:

- Verifieer of het afleveradres overeenkomt met het officiële bedrijfsadres
- Wees alert bij verzoeken om levering aan woonadressen of opslaglocaties
- Onderzoek ongebruikelijke verzendbestemmingen grondig

Proofpoint, een toonaangevend cybersecuritybedrijf, adviseert bedrijven om een gelaagde verdedigingsstrategie te implementeren. Dit omvat niet alleen technische maatregelen zoals e-mailauthenticatie en domeinmonitoring, maar ook het trainen van personeel in de verkoop-, inkoop- en financiële afdelingen om verdachte signalen te herkennen.

Kritieke Waarschuwingssignalen:

- Dringende verzoeken om krediet van onbekende partijen
- Druk om normale verificatieprocedures over te slaan
- Ongebruikelijke verzendlocaties die pas laat worden bekendgemaakt
- Contactpersonen die alleen via e-mail bereikbaar zijn
- Offerteaanvragen die net buiten kantoortijden binnenkomen

Interne Processen Versterken

Ontwikkel een systematische aanpak voor de verificatie van nieuwe klanten en bestellingen:

- Implementeer een "vier-ogen-principe" bij goedkeuring van kredietlijnen
- Stel een gecentraliseerd systeem in voor het registreren en controleren van verdachte aanvragen
- Organiseer regelmatige bewustwordingstrainingen voor personeel
- Creëer een meldpunt voor verdachte activiteiten binnen de organisatie



Regelmatige training en samenwerking tussen afdelingen is essentieel om Net RFQ-fraude te herkennen en te voorkomen.

Door een combinatie van technische maatregelen, personeel bewustwording en verbeterde verificatieprocessen kunnen bedrijven het risico op Net RFQ-fraude aanzienlijk verminderen. Het is aan te bevelen om ook contact te onderhouden met branchegenoten en relevante autoriteiten om informatie over nieuwe fraudetactieken uit te wisselen. Proactieve monitoring van domeinregistraties die lijken op uw bedrijfsnaam kan eveneens helpen bij het vroegtijdig identificeren van potentiële bedreigingen.

Shelter Elite: De Nieuwe Beveiligingstool Die Het Darkweb Veroverd

In april 2025 vond een verontrustende ontwikkeling plaats in het cyberbeveiligingslandschap: Shelter Elite, oorspronkelijk ontwikkeld als legitieme red team tool voor beveiligingsexperts, lekte naar het darkweb. Sindsdien heeft deze geavanceerde beveiligingstool een opmerkelijke opmars gemaakt onder cybercriminelen die hem gebruiken voor het verspreiden van geavanceerde malware.

De dreiging neemt snel toe vanwege de commercial-grade kwaliteit en het gebruiksgemak, waardoor ook minder technisch onderlegde aanvallers nu toegang hebben tot geavanceerde aanvalsmethoden.

Dit document analyseert de werking van Shelter Elite, bespreekt concrete voorbeelden van malwarecampagnes en biedt aanbevelingen voor organisaties om zich te beschermen tegen deze groeiende dreiging.

Willem Bosgra voor VEILIGDIGITAAL.COM

Geavanceerde Werking en Evasietechnieken

Shellter Elite onderscheidt zich door een indrukwekkend arsenaal aan technieken om beveiligingsoplossingen te omzeilen. De tool is specifiek ontworpen om zowel traditionele antivirusoplossingen als moderne Endpoint Detection and Response (EDR) producten te ontwijken. Dit bereikt het door gebruik te maken van polymorfe code, waardoor elke malware-instantie uniek is, en geavanceerde API-hooking technieken die de normale werking van beveiligingssoftware kunnen verstoren.

De kracht van Shellter Elite ligt in zijn veelzijdige beschermingsmechanismen voor malware. Het biedt dynamische geheugenbescherming die voorkomt dat beveiligingstools malicieuze activiteiten in het computergeheugen kunnen detecteren.

Daarnaast maakt het gebruik van indirecte syscalls, waardoor directe interacties met het besturingssysteem worden vermeden die normaal gesproken beveiligingsalarmen zouden activeren. De tool implementeert ook call stack corruptie, wat de sporen van malware-uitvoering verhuult, en bevat een geavanceerde AMSI-bypass die Microsoft's AntiMalware Scan Interface omzeilt.

Payload Bescherming

Shellter Elite verspreidt "onzichtbare" payloads door gebruik te maken van sterke encryptie (AES-128 CBC) en compressie. Deze technieken zorgen ervoor dat de schadelijke code onleesbaar blijft totdat deze daadwerkelijk wordt uitgevoerd op het doelsysteem.

Detectie Omzeiling

De tool beschikt over geavanceerde detectiemechanismen voor sandboxes en virtuele machines (VM's). Zodra deze worden gedetecteerd, past de malware zijn gedrag aan om analyse te voorkomen en blijft het inactief om detectie te vermijden.

Ingebouwde 'Kill Switch'

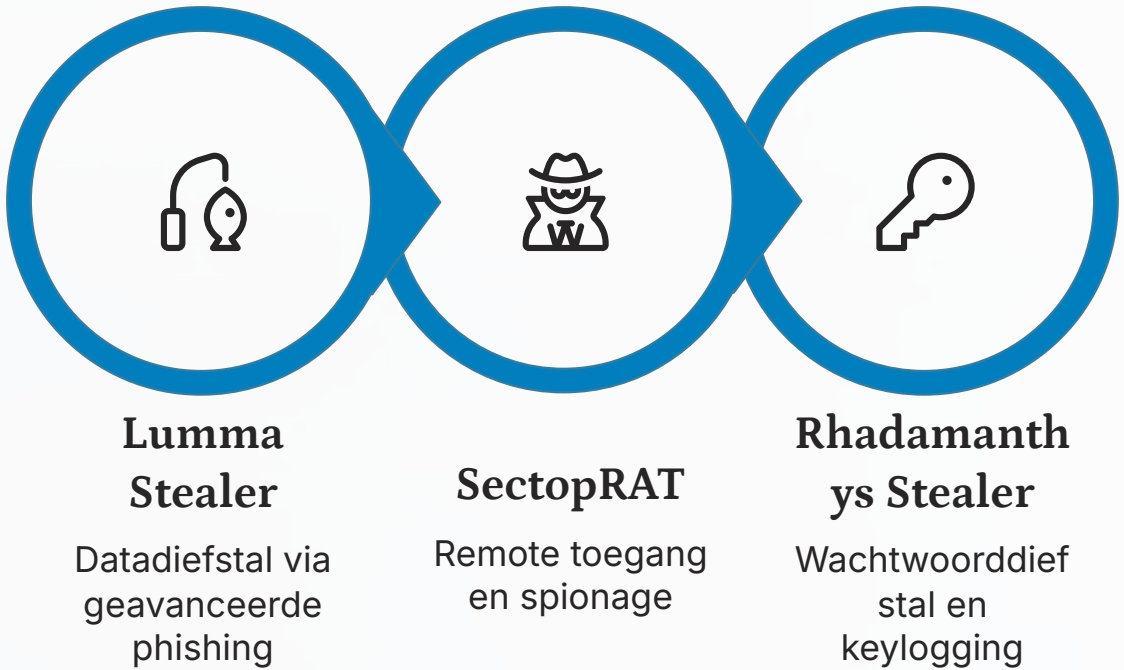
Een uniek kenmerk van de gelekte versie is de ingebouwde 'kill switch'. Deze zorgt ervoor dat de geëxploiteerde tool functioneel blijft tot april 2026, waarna deze automatisch zal stoppen met werken. Dit tijdelijke karakter creëert een gevoel van urgentie bij cybercriminelen.

De technische geavanceerdheid van Shellter Elite maakt het bijzonder verontrustend voor beveiligingsexperts. Door de combinatie van deze technieken kunnen aanvallers langdurige toegang behouden tot gecompromitteerde systemen zonder ontdekking.

Het meest zorgwekkende aspect is wellicht dat deze tool nu toegankelijk is voor een breed scala aan cybercriminelen, waardoor de technologische drempel voor het uitvoeren van geavanceerde aanvallen aanzienlijk is verlaagd.

Concrete Voorbeelden van Malwarecampagnes

Sinds de lek naar het darkweb hebben cybercriminelen Shellter Elite ingezet voor diverse malwarecampagnes. Deze campagnes illustreren de veelzijdigheid en effectiviteit van de tool in praktijksituaties. Door de geavanceerde evasietechnieken blijven deze aanvallen vaak langdurig onopgemerkt, wat resulteert in aanzienlijke datadiefstal en persistente toegang tot bedrijfsnetwerken.



Gedetailleerde Analyse van Malwarecampagnes

Lumma Stealer

Deze malware richt zich specifiek op het stelen van cryptovaluta-gerelateerde gegevens. Aanvallers verspreiden Lumma Stealer via MediaFire-koppelingen, vaak vermomd als legitieme software-updates of cracks. Eenmaal geïnstalleerd, richt de malware zich op:

- Cryptocurrency wallets, waarbij privésleutels worden gestolen
- Browsergegevens, inclusief opgeslagen wachtwoorden en cookies
- Authenticatietokens die toegang geven tot online diensten

Door de evasietechnieken van Shellter Elite kan Lumma Stealer maandenlang actief blijven zonder ontdekking, waardoor aanzienlijke financiële schade ontstaat voor slachtoffers.

SectopRAT (ArechClient2)

Deze Remote Access Trojan (RAT) biedt aanvallers volledige controle over geïnfecteerde systemen. SectopRAT heeft bijzondere aandacht gekregen vanwege zijn vermogen om:

- Remote desktop-sessies op te zetten zonder detectie
- Tweefactorauthenticatiegegevens te onderscheppen
- Slachtoffers te bespioneren via webcams en microfoons
- Bestanden ongemerkt te uploaden en downloaden

De combinatie van SectopRAT's functionaliteit met Shellter Elite's evasietechnieken maakt deze campagne bijzonder gevaarlijk voor bedrijven die vertrouwen op traditionele beveiligingsmaatregelen.

Rhadamanthys Stealer: Gericht op Financiële Sector

Aanvalsvector	Doelgegevens	Social Engineering Tactieken
Gaming-gerelateerde bestanden en mods	Financiële credentials, bankgegevens	Gratis game-upgrades en exclusieve content
Valse software-updates	Windows credentials en certificaten	Urgente beveiligingsupdates voor populaire software
Gecompromitteerde downloadsites	Browser-opgeslagen creditcardgegevens	Misleidende downloadknoppen en pop-ups

Het gemeenschappelijke kenmerk van al deze campagnes is hun focus op langdurige, ongemerkte datadiefstal. Door gebruik te maken van Shellter Elite's vermogen om beveiligingsoplossingen te omzeilen, kunnen deze malwarevarianten maandenlang actief blijven binnen gecompromitteerde netwerken. Dit resulteert in aanzienlijke gegevenslekken en financiële verliezen voor getroffen organisaties, terwijl de daders vaak ongedetecteerd blijven.

Dreiging, Reikwijdte en Aanbevelingen voor Organisaties

De dreiging die uitgaat van Shellter Elite is alomvattend en raakt organisaties in alle sectoren. Door de lage toetredingsdrempel - de tool is relatief eenvoudig te gebruiken, zelfs voor minder ervaren cybercriminelen - vindt er een snelle verspreiding plaats. De brede inzetbaarheid maakt het mogelijk om verschillende soorten malware te verspreiden, wat zorgt voor een gevarieerd dreigingslandschap dat moeilijk te beheersen is met traditionele beveiligingsmaatregelen.

85%

Detectie Falen

Percentage traditionele antivirusoplossingen dat niet in staat is om met Shellter Elite verpakte malware te detecteren tijdens de eerste 48 uur na verspreiding.

73%

Aanvalsstijging

Toename in het aantal waargenomen aanvallen waarbij Shellter Elite wordt gebruikt sinds de lek in april 2025.

205 dagen

Gemiddelde Verblijfstijd

Gemiddelde tijd dat een Shellter Elite-gebaseerde aanval onopgemerkt blijft in een bedrijfsnetwerk zonder geavanceerde EDR-oplossingen.

Aanbevolen Beveiligingsstrategieën

Om deze groeiende dreiging effectief te bestrijden, moeten organisaties een meerlaagse beveiligingsstrategie implementeren die verder gaat dan traditionele antivirusoplossingen. De volgende aanbevelingen bieden een robuust raamwerk voor bescherming tegen Shellter Elite en soortgelijke dreigingen:

1

Geavanceerde Detectie

Implementeer gedragsanalyse en next-generation EDR-oplossingen die zich richten op het detecteren van afwijkende activiteiten en verdachte gedragspatronen in plaats van alleen op handtekening-gebaseerde detectie. Deze systemen kunnen anomalieën herkennen die kenmerkend zijn voor Shellter Elite, zelfs wanneer de malwarecode zelf onbekend is.

2

Netwerk Hardening

Versterk netwerkbeveiligingsmaatregelen door strikte applicatiecontrole, waarbij alleen goedgekeurde software mag worden uitgevoerd. Implementeer netwerksegmentatie om laterale beweging te beperken en dwing een streng downloadbeleid af waarbij alle bestanden worden gecontroleerd voordat ze worden uitgevoerd.

3

Proactieve Assessments

Voer regelmatig security assessments en penetratietests uit die specifiek gericht zijn op het identificeren van kwetsbaarheden voor geavanceerde dreigingen zoals Shellter Elite. Deze tests moeten de nieuwste evasietechnieken simuleren om de effectiviteit van bestaande beveiligingsmaatregelen te evalueren.

4

Bewustzijnstraining

Train personeel gericht op het herkennen en vermijden van social engineering tactieken en scams die verband houden met deze tools. Medewerkers moeten bewust worden gemaakt van de specifieke distributiemethoden die worden gebruikt om Shellter Elite-gebaseerde malware te verspreiden, zoals valse software-updates en gecompromitteerde downloadlinks.

Shellter Elite is een krachtige illustratie van hoe commerciële beveiligingstools, wanneer ze in verkeerde handen vallen, het cyberdreigingslandschap versneld kunnen veranderen. De tool biedt geavanceerde capaciteiten die voorheen alleen beschikbaar waren voor ervaren hackers, maar nu toegankelijk zijn voor een breder publiek van cybercriminelen. Dit onderstreept het belang van blijvende waakzaamheid en voortdurende aanpassing van beveiligingsstrategieën.

Organisaties moeten erkennen dat het dreigingslandschap evolueert en dat traditionele beveiligingsmaatregelen niet langer voldoende zijn. Door de aanbevolen strategieën te implementeren en up-to-date te blijven met de nieuwste ontwikkelingen op het gebied van cyberdreigingen, kunnen organisaties hun weerbaarheid tegen Shellter Elite en soortgelijke dreigingen aanzienlijk verbeteren. Een proactieve, meerlaagse aanpak van cyberbeveiliging is essentieel in deze snel veranderende omgeving.



Waarom LibreOffice een goed alternatief is voor Microsoft Office

LibreOffice is een uitstekend alternatief voor Microsoft Office dat steeds meer aandacht krijgt van zowel particuliere als zakelijke gebruikers. Dit gratis, open-source kantoorpakket biedt een complete set aan productiviteitstools die kunnen concurreren met commerciële software.

In dit document onderzoeken we waarom LibreOffice een serieuze overweging waard is, waarbij we kijken naar de functionaliteit en het gebruiksgemak, de compatibiliteit met verschillende bestandsformaten en besturingssystemen, en de voordelen van het open-source model met zijn actieve gemeenschap. Ook belichten we de financiële voordelen en de vrijheid die LibreOffice biedt ten opzichte van propriëtaire software zoals Microsoft Office.

Willem Bosgra voor VEILIGDIGITAAL.COM

Functionaliteit en Gebruiksgemak

1

Writer

De tekstverwerker van LibreOffice die vergelijkbaar is met Microsoft Word. Writer biedt uitgebreide tekstopmaakfuncties, stijlen, inhoudsopgaven, indexen, en ondersteuning voor grote documenten. Het programma is krachtig genoeg voor zowel eenvoudige brieven als complexe boeken.

2

Calc

Het spreadsheetprogramma dat Excel vervangt. Calc bevat alle essentiële formules en functies, inclusief statistische analyses, draaitabellen en conditionele opmaak. Hoewel sommige geavanceerde Excel-functies ontbreken, biedt Calc voldoende mogelijkheden voor de meeste gebruikers.

3

Impress

Het presentatieprogramma vergelijkbaar met PowerPoint. Impress ondersteunt diverse dia-overgangen, animaties, diagrammen en multimedia-integratie. Het biedt wellicht minder ontwerpsjablonen, maar de kernfunctionaliteit is vrijwel identiek.

Prestaties op oudere hardware

Een van de grote voordelen van LibreOffice is de efficiënte werking op oudere computers. Waar Microsoft Office steeds meer systeembronnen vereist met elke nieuwe versie, blijft LibreOffice relatief licht en snel. Dit maakt het ideaal voor:

- Educatieve instellingen met beperkte IT-budgetten
- Kleine bedrijven die geen regelmatige hardware-upgrades kunnen bekostigen
- Thuisgebruikers met oudere systemen



LibreOffice draait soepel op oudere hardware, waardoor gebruikers geen dure upgrades nodig hebben om productief te blijven.

Hoewel LibreOffice misschien niet alle geavanceerde functies van Microsoft Office bevat, zoals de uitgebreide data-analysemogelijkheden van Excel of de real-time samenwerkingstools, biedt het pakket meer dan voldoende functionaliteit voor de gemiddelde gebruiker.

De interface is intuïtief, vooral voor wie al bekend is met oudere versies van Microsoft Office (vóór de introductie van het lint). Nieuwe gebruikers kunnen snel aan de slag dankzij de logische menustructuur en de uitgebreide online documentatie.

LibreOffice biedt ook enkele unieke functies die niet standaard in Microsoft Office te vinden zijn, zoals geavanceerde PDF-bewerkingsmogelijkheden in Draw en betere ondersteuning voor open standaarden. De ontwikkelaars werken voortdurend aan verbeteringen, waarbij de nadruk ligt op stabiliteit en betrouwbaarheid in plaats van op het toevoegen van nichefeatures die slechts door een klein deel van de gebruikers worden benut.

Compatibiliteit en Platformondersteuning

Een van de grootste zorgen bij het overstappen naar alternatieve kantoorsoftware is de compatibiliteit met bestaande documenten en de interactie met anderen die mogelijk nog steeds Microsoft Office gebruiken. LibreOffice heeft aanzienlijke vooruitgang geboekt op dit gebied en biedt nu robuuste ondersteuning voor Microsoft Office-bestandsformaten.



Bestandsformaten

LibreOffice opent en bewerkt .docx, .xlsx, .pptx en oudere .doc, .xls, .ppt bestanden. Het kan ook opslaan in deze formaten, hoewel complexe opmaak soms kleine verschillen kan vertonen.



Open Document Format

LibreOffice gebruikt standaard ODF (.odt, .ods, .odp), een ISO-gecertificeerde open standaard die toekomstbestendigheid en toegankelijkheid garandeert.



Platformonafhankelijk

Beschikbaar voor Windows, macOS, Linux en als portable versie, waardoor gebruikers hetzelfde programma kunnen gebruiken ongeacht hun besturingssysteem.

De mogelijkheid om op verschillende besturingssystemen te werken is een significant voordeel van LibreOffice. Terwijl Microsoft Office voor Mac beschikbaar is maar vaak achterblijft bij de Windows-versie qua functionaliteit, en helemaal niet officieel beschikbaar is voor Linux, biedt LibreOffice een consistente ervaring op alle platforms.

Dit is bijzonder waardevol voor organisaties met een gemengde IT-omgeving of voor gebruikers die tussen verschillende apparaten schakelen.



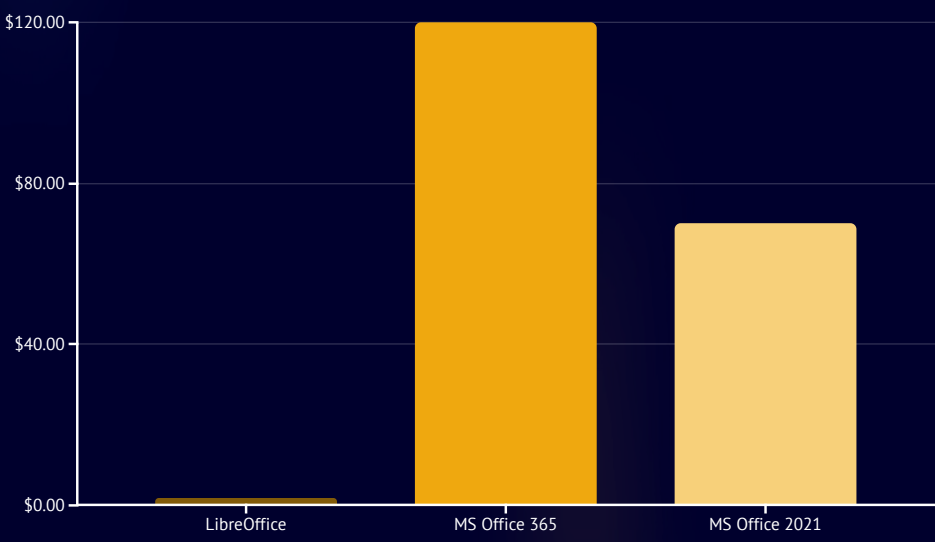
Tip voor optimale compatibiliteit

Als u regelmatig documenten uitwisselt met Microsoft Office-gebruikers, overweeg dan om uw LibreOffice-instellingen aan te passen. Ga naar Extra > Opties > Laden/Opslaan > Microsoft Office en selecteer de optie om standaard in Microsoft-formaten op te slaan. Dit vermindert potentiële compatibiliteitsproblemen.

Bij het werken met zeer complexe documenten kunnen er soms kleine opmaakverschillen optreden tussen LibreOffice en Microsoft Office. Dit is vooral merkbaar bij documenten met geavanceerde opmaak zoals complexe tabellen, macro's, of specifieke lettertypen. De meeste alledaagse documenten worden echter probleemloos uitgewisseld, en de compatibiliteit verbetert met elke nieuwe versie van LibreOffice.

Voor organisaties die overstappen op LibreOffice maar nog steeds moeten samenwerken met externe partners die Microsoft Office gebruiken, is het raadzaam om een migratiestrategie te ontwikkelen die rekening houdt met deze potentiële compatibiliteitskwesties. Dit kan inhouden dat bepaalde sjablonen worden aangepast of dat er specifieke workflows worden opgezet voor documenten die extern worden gedeeld.

Kosten, Open Source en Gemeenschap



Kostenvergelijking tussen LibreOffice en Microsoft Office-opties. De besparingen worden significant bij gebruik door meerdere gebruikers of organisaties.

Financiële Voordelen

Het kostenvoordeel van LibreOffice is substantieel, vooral voor organisaties. Voor een bedrijf met 100 werknemers kan de jaarlijkse besparing oplopen tot €12.000 in vergelijking met Microsoft 365-abonnementen. Deze besparing kan worden geïnvesteerd in andere aspecten van het bedrijf, zoals training of hardware-upgrades.

Voor onderwijsinstellingen, non-profitorganisaties en overheidsinstellingen met beperkte budgetten kan LibreOffice het verschil maken tussen toegang hebben tot moderne kantoorsoftware of het moeten gebruiken van verouderde oplossingen.

Open Source Voordelen

- Transparante code die door iedereen kan worden gecontroleerd op beveiligingsproblemen
- Geen verborgen telemetrie of gegevensverzameling
- Mogelijkheid om de software aan te passen aan specifieke behoeften
- Vrijheid van vendor lock-in en gedwongen upgrades

Gemeenschapsondersteuning

- Uitgebreide documentatie en tutorials beschikbaar in meerdere talen
- Actieve gebruikersfora waar vragen snel worden beantwoord
- Regelmatige updates en bugfixes zonder extra kosten
- Mogelijkheid om bij te dragen aan de ontwikkeling en verbetering

Bedrijfsimplementatie

- Professionele ondersteuning beschikbaar via partners
- Aanpassingen mogelijk voor specifieke bedrijfsprocessen
- Integratie met bestaande systemen en werkstromen
- Geleidelijke migratiemogelijkheden vanuit Microsoft Office

De open-sourcefilosofie achter LibreOffice biedt voordelen die verder gaan dan alleen kostenbesparingen. Het geeft gebruikers controle over hun software en data, zonder de beperkingen die komen met propriëtaire licenties. Er zijn geen verplichte upgrades, geen abonnementsmodellen die plotseling kunnen veranderen, en geen risico dat functionaliteit wordt verwijderd zonder inspraak van de gebruikers.

Voor bedrijven die zich zorgen maken over ondersteuning zijn er commerciële partners die professionele diensten aanbieden, waaronder implementatie, training, aangepaste ontwikkeling en technische ondersteuning. Dit 'freemium' model stelt organisaties in staat om te beginnen zonder initiële investering en later te kiezen voor betaalde diensten indien nodig.

"Het gebruik van LibreOffice heeft onze school niet alleen tienduizenden euro's per jaar bespaard, maar heeft ook onze leerlingen geleerd dat er alternatieven zijn voor commerciële software. Ze leren nu dat technologie geen kostenpost hoeft te zijn, maar een hulpmiddel dat voor iedereen toegankelijk kan zijn." - Directeur van een middelbare school in Amsterdam

De actieve LibreOffice-gemeenschap zorgt voor continue verbeteringen en snelle reacties op beveiligingsproblemen. Bovendien biedt het pakket uitstekende ondersteuning voor internationale standaarden en toegankelijkheidsfuncties, wat het geschikt maakt voor gebruik in de publieke sector waar deze eisen vaak wettelijk zijn vastgelegd.

Snapchat's Nieuwe Home Safe-functie: Automatische Veilige Thuiskomst Meldingen

In juli 2025 introduceert Snapchat een nieuwe functionaliteit genaamd 'Home Safe', die gebruikers in staat stelt om automatisch geselecteerde vrienden te informeren wanneer ze veilig thuis zijn aangekomen. Deze functie, die werkt via de al bestaande Snap Map, is ontworpen om een extra veiligheidslaag te bieden voor gebruikers die laat onderweg zijn. Hoewel de functie duidelijke voordelen biedt voor het geruststellen van vrienden en familie, zijn er ook belangrijke privacyoverwegingen waar gebruikers zich bewust van moeten zijn.

Dit artikel verkent de werking, voordelen en potentiële aandachtspunten van deze nieuwe Snapchat-functionaliteit.

Willem Bosgra voor VEILIGDIGITAAL.COM

Seamlessly Home

Voordelen en Toepassingen van Home Safe



Verhoogd Veiligheidsgevoel

Biedt extra geruststelling voor jongeren en studenten die regelmatig laat thuiskomen na een avond uit. De automatische melding elimineert de noodzaak om handmatig berichten te sturen in situaties waarin dit vergeten kan worden.



Geautomatiseerde Meldingen

Gebruikers hoeven niet meer actief berichten te sturen om te laten weten dat ze veilig zijn aangekomen. De functie doet dit automatisch wanneer de vooraf ingestelde thuislocatie wordt bereikt.



Gerichte Communicatie

Alleen vrienden met wie je al locatie-informatie deelt krijgen de melding, wat de privacy waarborgt terwijl het tegelijkertijd belangrijke contacten geruststelt.

Praktische Toepassingsgebieden

De Home Safe-functie bouwt voort op de reeds populaire Snap Map, die wereldwijd door ongeveer 400 miljoen gebruikers maandelijks wordt gebruikt. Deze uitbreiding richt zich specifiek op veiligheidscommunicatie, een groeiende behoefte onder gebruikers van sociale media.

Veel Snapchat-gebruikers zijn jongeren en jongvolwassenen die regelmatig uitgaan of reizen. De functie sluit aan bij de reeds bestaande gewoonte om "ben veilig thuis"-berichten te sturen, maar maakt dit proces geautomatiseerd en betrouwbaarder.

Ouders van tieners zullen deze functie mogelijk waarderen als een niet-invasieve manier om geruststelling te krijgen over de veiligheid van hun kinderen zonder voortdurend te hoeven controleren of berichten te sturen. Dit kan leiden tot meer autonomie voor jongeren terwijl het tegelijkertijd zorgen bij ouders vermindert.

Connectnow

Mobile Data
Stay connected, anywhere.



De functie is bijzonder nuttig voor situaties zoals:

- Na een avond stappen met vrienden
- Bij alleen reizen in het openbaar vervoer 's avonds
- Voor studenten die laat terugkeren naar hun kamers
- Tijdens reizen waarbij familie of vrienden op de hoogte willen blijven



Voor optimaal gebruik moet eerst de 'My Home' locatie worden ingesteld in Snap Map. Deze is alleen zichtbaar voor jou en de vrienden met wie je ervoor kiest om je locatie te delen.

Kritische Kanttekeningen en Aandachtspunten

Hoewel de Home Safe-functie duidelijke voordelen biedt, zijn er verschillende belangrijke aandachtspunten die gebruikers in overweging moeten nemen voordat ze deze functie gaan gebruiken. Deze betreffen voornamelijk privacy, beperkingen van de functionaliteit en potentiële technische problemen.



Actieve Locatiedeling Vereist

Om Home Safe te laten werken, moet je actief je locatie delen met geselecteerde vrienden. Dit verhoogt de hoeveelheid persoonlijke gegevens die via de app worden gedeeld, wat inherente privacyrisico's met zich meebrengt als deze instellingen niet zorgvuldig worden beheerd.



Risico op Onbedoeld Delen

Hoewel de functie ontworpen is om alleen zichtbaar te zijn voor geselecteerde vrienden, kan onvoorzichtig gebruik leiden tot het onbedoeld delen van privacygevoelige gegevens zoals je exacte huisadres.



Beperkte Meldingsfunctionaliteit

De functie geeft slechts één melding wanneer je thuiskomt. Als je onderweg stopt of van route wijzigt, wordt dit niet gevolgd of gemeld aan je contacten, wat een vals gevoel van veiligheid kan creëren.

Technische Beperkingen

De effectiviteit van Home Safe is afhankelijk van verschillende technische factoren:

- Betrouwbare GPS-verbinding en nauwkeurigheid
- Voldoende batterijleven van je telefoon
- Stabiele internetverbinding
- Correcte configuratie van de thuislocatie

Bij technische storingen of problemen met een van deze factoren, kan de automatische melding uitblijven, wat kan leiden tot onnodige zorgen bij vrienden of familie die een bericht verwachten.

Veiligheidsoverwegingen

Hoewel de functie is ontworpen om de veiligheid te verbeteren, zijn er scenario's waarin deze misbruikt zou kunnen worden:

- Kwaadwillenden die toegang krijgen tot iemands account kunnen de thuislocatie achterhalen
- Valse thuislocaties kunnen worden ingesteld om anderen te misleiden over je werkelijke verblijfplaats
- Overmatig vertrouwen op de functie kan leiden tot verminderde waakzaamheid bij gebruikers

Het is cruciaal dat gebruikers begrijpen dat technologie nooit een volledig sluitende veiligheidsoplossing kan bieden en dat persoonlijke waakzaamheid altijd belangrijk blijft.

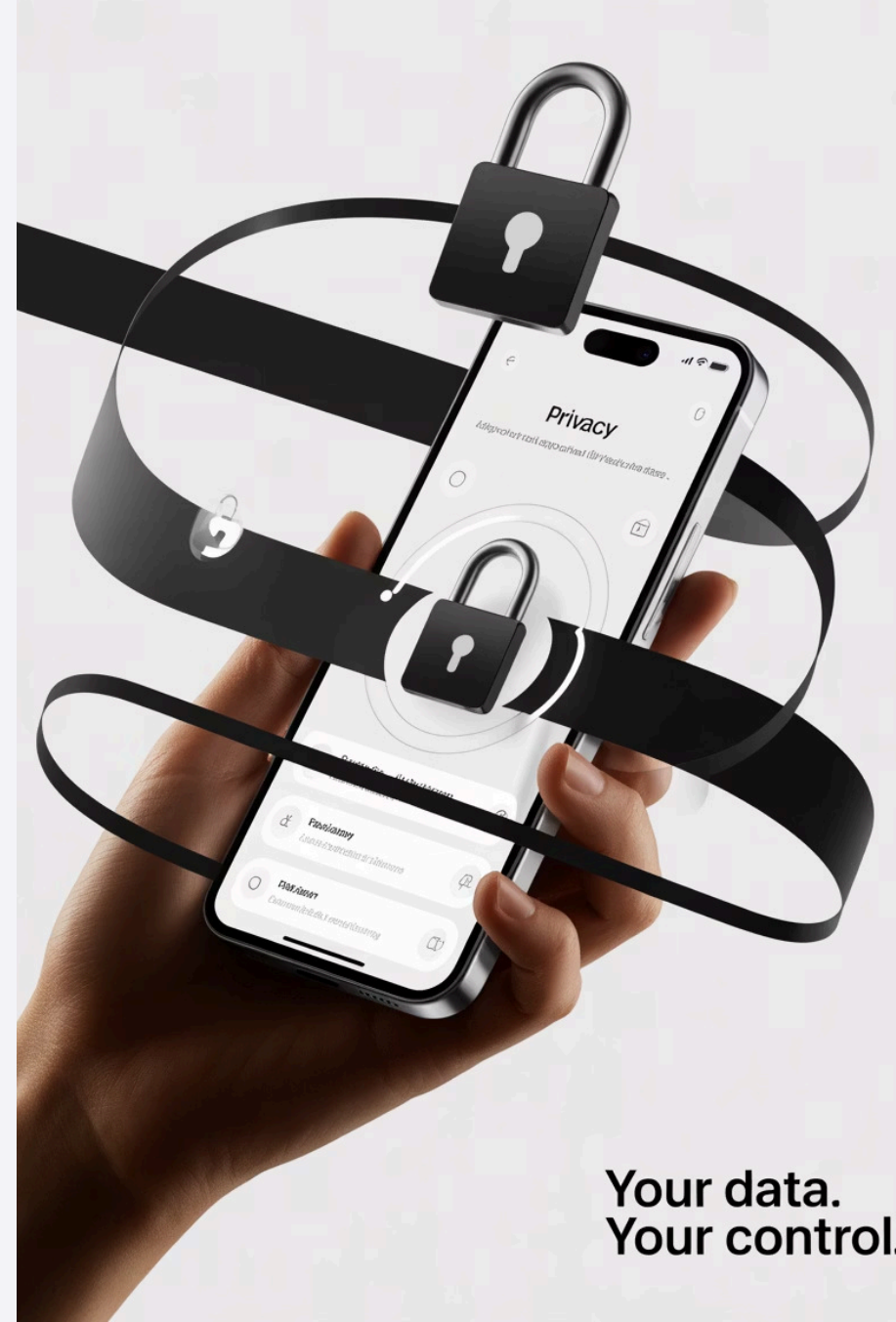


Locatiedeling moet voor elke sessie bewust worden aangezet. Gebruikers moeten regelmatig hun privacyinstellingen controleren om te zorgen dat ze niet onbedoeld meer delen dan ze willen.

Uw Google-account heeft een ingebouwd privacydashboard, maar bijna niemand controleert dit

Google heeft sinds 2019 een uitgebreid privacydashboard ingebouwd in alle accounts, maar slechts 17% van de Nederlanders controleert jaarlijks hun privacy-instellingen. Dit dashboard biedt een centrale locatie voor alle privacy- en beveiligingsopties, maar blijft voor de meeste gebruikers verborgen.

Willem Bosgra voor VEILIGDIGITAAL.COM



**Your data.
Your control.**

Waarom Gebruikers Hun Privacy Niet Controleren



Onbekendheid

61% van de gebruikers weet niet waar het privacydashboard zich bevindt binnen hun Google-account.

Moeilijk vindbaar

Het dashboard is verstopt achter 3-4 klikken in het menu, waardoor het niet direct toegankelijk is.

Ingewikkelde taal

Privacyinstellingen zijn vaak in technische of juridische taal geformuleerd, wat begrip bemoeilijkt.

Wat Kun Je Met Het Privacydashboard?



Locatiegeschiedenis

Bekijk en beheer waar Google je locatie heeft geregistreerd en verwijder specifieke gegevens of periodes.



Zoekactiviteit

Krijg inzicht in je zoekgeschiedenis en pas aan welke zoekopdrachten Google mag opslaan voor personalisatie.



YouTube-historie

Controleer welke video's je hebt bekeken en beheer of deze informatie wordt gebruikt voor aanbevelingen.

Je kunt het dashboard snel bereiken via je profielfoto in Search, Maps, Gmail, YouTube en andere Google-diensten.

Privacycontrole in Één Overzicht

1

Privacy Checkup

Stap-voor-stap controle van je belangrijkste privacy-instellingen met duidelijke uitleg en aanbevelingen.

2

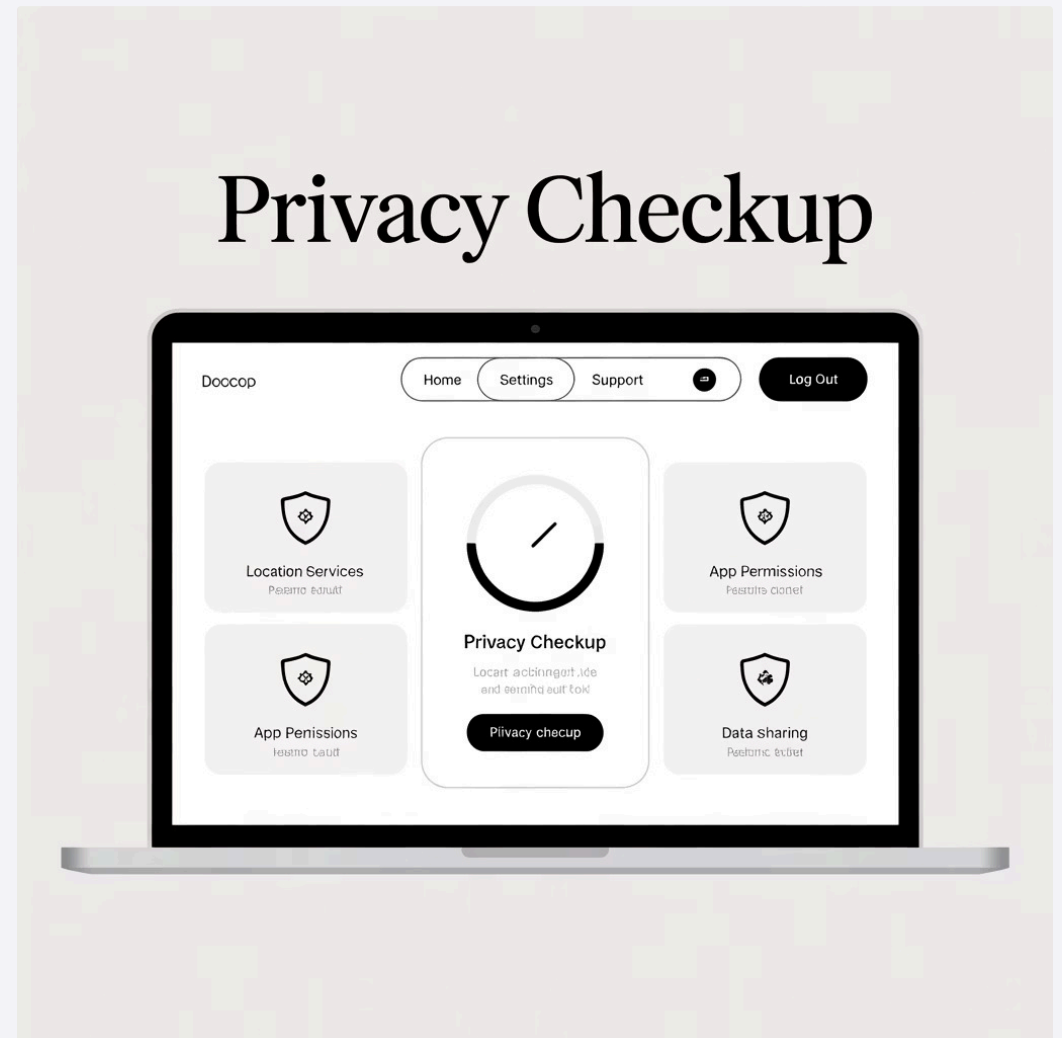
Auto-delete opties

Stel automatische verwijdering in voor je locatie- en webactiviteit na 3, 18 of 36 maanden.

3

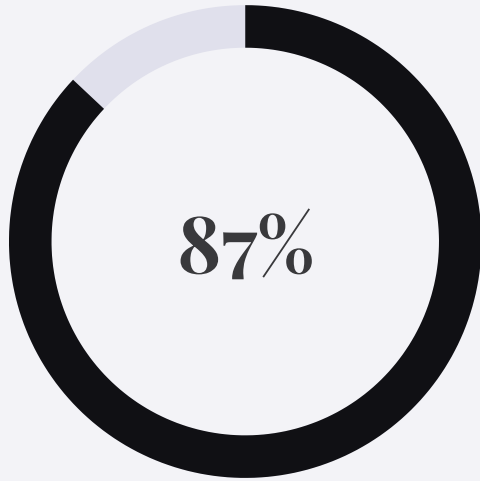
Resultaten over jou

Vraag verwijdering aan van persoonlijke informatie die in Google zoekresultaten verschijnt.



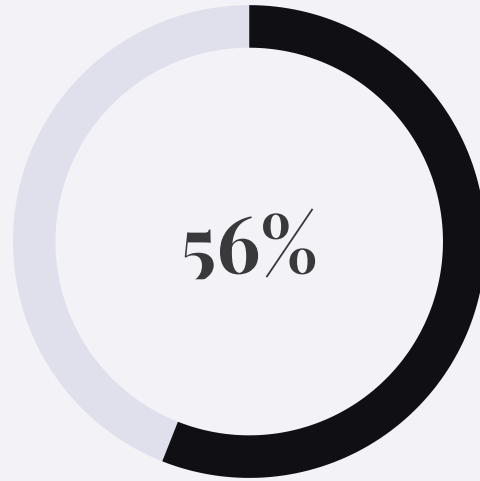
Het privacydashboard waarschuwt je ook wanneer nieuwe e-mailadressen of telefoonnummers gelinkt aan jouw identiteit online verschijnen.

Concreet: Wat Staat Er Over Jou In Google?



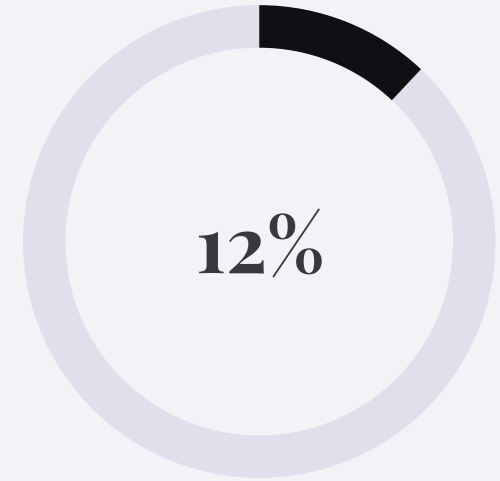
Locatiegeschiedenis

Van de volwassen gebruikers heeft deze functie ingeschakeld, vaak zonder het te weten.



YouTube-historie

Van de recente Google-accounts slaat de volledige kijkgeschiedenis op voor personalisatie.

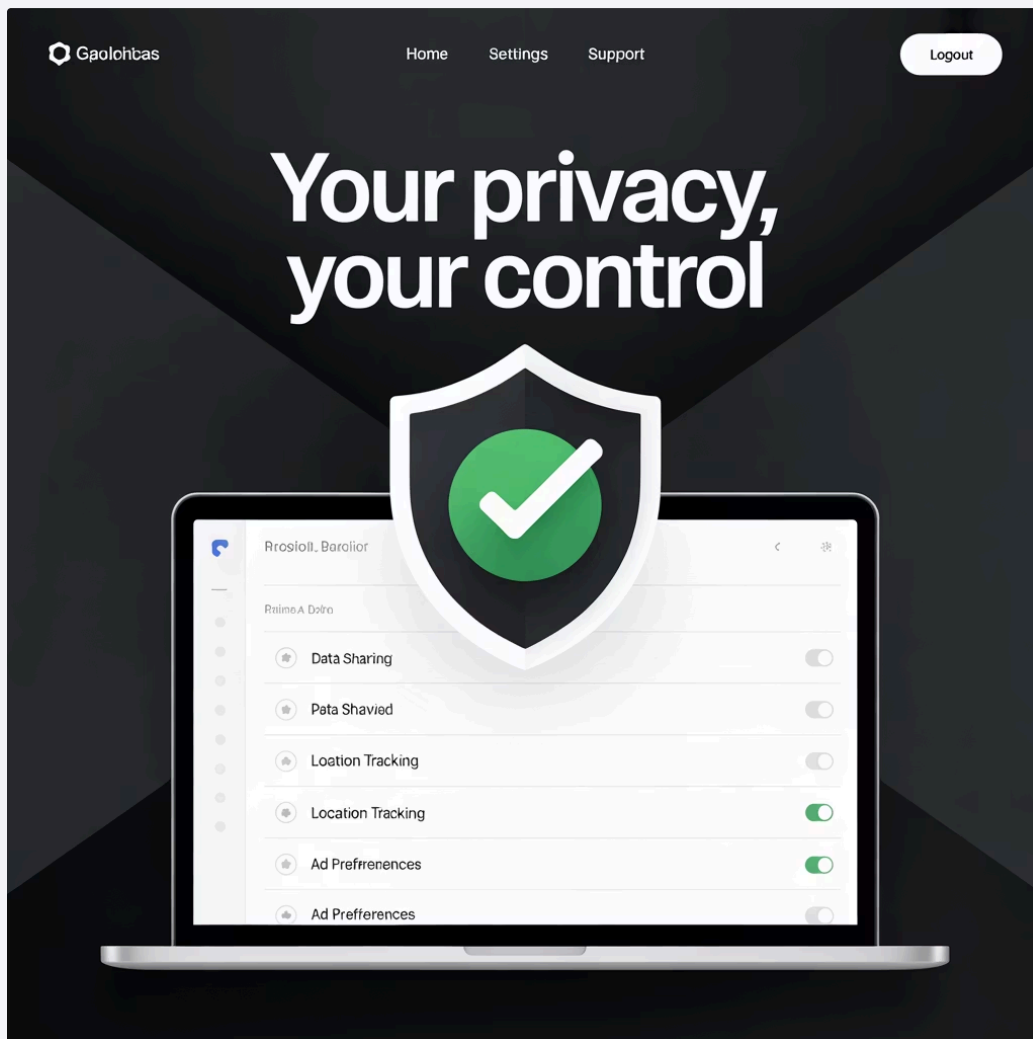


Advertentieprofiel

Slechts dit percentage gebruikers paste hun advertentievoorkeuren aan in 2024.

Nieuw in het dashboard: Je krijgt nu automatisch een waarschuwing als je contactinformatie is gelekt in een datalek of zonder toestemming online is gepubliceerd.

Tip: Controleer Je Privacy Nu



1 Open je Google Account

Ga naar het menu "Gegevens & Privacy" door op je profielfoto te klikken.

2 Doorloop de Privacy Checkup

Controleer systematisch alle belangrijke instellingen en pas ze naar wens aan.

3 Stel auto-delete in

Kies een termijn voor automatische verwijdering van je locatie- en zoekgeschiedenis.

4 Controleer regelmatig

Maandelijkse controles vergroten je gevoel van controle en online veiligheid.

Waarom is GLOW een uitstekende app voor systeem informatie

GLOW onderscheidt zich als de toonaangevende applicatie voor het bijhouden en analyseren van menstruatie- en ovulatiegegevens. Als geïntegreerd informatiesysteem biedt GLOW een centrale hub waar gebruikers hun cyclus, vruchtbaarheid en gezondheidsindicatoren kunnen monitoren. Met behulp van geavanceerde algoritmes verwerkt de app persoonlijke gegevens tot nauwkeurige voorspellingen en inzichten, waardoor gebruikers volledige controle krijgen over hun reproductieve gezondheid.

De mogelijkheid om te synchroniseren met Apple Health versterkt de positie van GLOW als allesomvattend gezondheidsinformatiesysteem, waardoor gebruikers een compleet beeld krijgen van hun lichamelijke welzijn en hormonale patronen.

Willem Bosgra voor VEILIGDIGITAAL.COM

De kracht van GLOW als informatiesysteem

1

Allesomvattende dataverzameling

GLOW stelt gebruikers in staat om een uitgebreide reeks gegevens te registreren, waaronder menstruatiecycli, ovulatiemomenten, basale lichaamstemperatuur, stemming, fysieke symptomen en intieme momenten. Deze holistische benadering zorgt ervoor dat het systeem een compleet beeld krijgt van de gebruiker, wat resulteert in steeds nauwkeurigere voorspellingen.

2

Persoonlijke data-analyse

Door geavanceerde algoritmes en machine learning technieken toe te passen op de ingevoerde gegevens, genereert GLOW gepersonaliseerde inzichten die specifiek zijn afgestemd op het unieke lichaamsritme van de gebruiker. Deze analyses worden met elke nieuwe invoer steeds nauwkeuriger, waardoor de app functioneert als een zelflerend systeem.

3

Kennisdeling en ondersteuning

De ingebouwde communityfunctie transformeert GLOW van een persoonlijk informatiesysteem naar een collectief kennisplatform. Gebruikers kunnen ervaringen delen, vragen stellen en advies inwinnen bij duizenden andere gebruikers wereldwijd, wat resulteert in een rijke bron van praktijkkennis naast de wetenschappelijke basis.

Premium analysemogelijkheden

Voor gebruikers die behoefte hebben aan nog diepgaandere systeem informatie biedt GLOW een premium-versie. Deze uitbreiding voorziet in geavanceerde analysetools die complexe patronen kunnen identificeren in de verzamelde gegevens. De premium functionaliteit omvat:

- Uitgebreide vergelijkende analyses met historische gegevens
- Gedetailleerde grafieken met meerdere variabelen voor correlatie-onderzoek
- Voorspellende modellen met hogere precisie en langere termijn
- Gepersonaliseerde rapporten die automatisch worden gegenereerd



GLOW's analytische dashboards bieden gebruikers gedetailleerde visuele representaties van hun gezondheidsgegevens, waardoor patronen en trends eenvoudig te identificeren zijn. Deze visualisaties maken complexe gezondheidsinformatie toegankelijk en begrijpelijk voor gebruikers zonder medische achtergrond.

De kracht van GLOW als informatiesysteem ligt in de combinatie van uitgebreide dataverzameling, gepersonaliseerde analyse en collectieve kennisdeling. Door deze elementen samen te brengen, creëert de app een ecosysteem waarin gebruikers niet alleen hun eigen gezondheid beter kunnen begrijpen, maar ook kunnen profiteren van de collectieve wijsheid van de gemeenschap. De wetenschappelijke onderbouwing van de app zorgt ervoor dat deze inzichten betrouwbaar en klinisch relevant zijn.

Gebruiksvriendelijkheid en betrouwbaarheid in dagelijks gebruik

Intuïtieve gebruikersinterface

GLOW onderscheidt zich door een uitzonderlijk gebruiksvriendelijke interface die complex gegevensbeheer vereenvoudigt tot een intuïtieve ervaring. De app is ontworpen met het principe 'eenvoud voorop', waardoor gebruikers zonder technische kennis moeiteloos hun gegevens kunnen invoeren, bijwerken en analyseren.

De overzichtelijke dashboards en logische navigatiestructuur zorgen ervoor dat alle functionaliteit binnen handbereik is, terwijl de visuele weergave van gegevens direct inzichtelijk is. Dagelijkse herinneringen helpen gebruikers consistent te blijven in hun dataverzameling, wat de betrouwbaarheid van de systeeminformatie verder verhoogt.

Snelle dagelijkse invoer

Met slechts enkele tikken kunnen gebruikers hun dagelijkse gegevens registreren. De intelligente interface onthoudt eerdere patronen en doet suggesties om het invoerproces verder te vereenvoudigen, wat resulteert in minder dan een minuut tijd per dag voor volledig bijhouden.

Wekelijkse inzichten

GLOW genereert automatisch wekelijkse samenvattingen van de verzamelde gegevens, inclusief opvallende patronen en afwijkingen. Deze inzichten worden gepresenteerd in een gemakkelijk te begrijpen formaat, waardoor gebruikers hun gezondheid in de gaten kunnen houden zonder zich te verdiepen in ruwe data.

Maandelijks analyses

Aan het einde van elke cyclus biedt GLOW een uitgebreide analyse, waarin de cyclus wordt vergeleken met historische gegevens en voorspellingen worden gedaan voor de komende periode. Deze langetermijnperspectieven helpen bij het identificeren van trends die anders onopgemerkt zouden blijven.

Wetenschappelijke betrouwbaarheid en dataprivacy

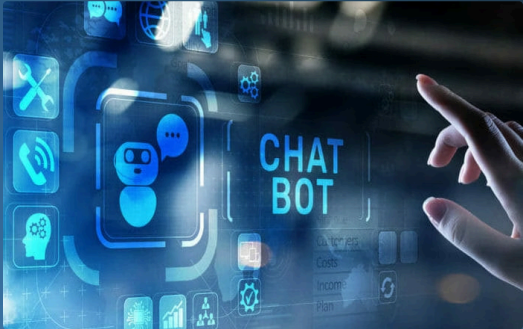
De fundamentele waarde van GLOW als systeeminformatie-app ligt in de wetenschappelijke onderbouwing van alle functionaliteiten. De algoritmes voor cyclusvoorspelling en vruchtbaarheidsanalyse zijn gebaseerd op klinisch gevalideerde methodes en worden continu verfijnd op basis van nieuwe medische inzichten. Dit zorgt ervoor dat gebruikers kunnen vertrouwen op de nauwkeurigheid van de gegenereerde informatie.

Privacy en databeveiliging

GLOW behandelt alle gebruikersgegevens met de hoogste standaard van privacy en beveiliging. Gebruikers behouden volledige controle over hun data en kunnen precies bepalen welke informatie wordt opgeslagen en gedeeld. De app voldoet aan alle relevante privacywetgeving en implementeert geavanceerde versleutelingstechnieken om gevoelige gezondheidsinformatie te beschermen.

De integratie met andere gezondheidssystemen zoals Apple Health en diverse wearables vergroot de bruikbaarheid van GLOW aanzienlijk. Door gegevens uit verschillende bronnen te combineren, creëert de app een alomvattend beeld van de gezondheid van de gebruiker. Dit ecosysteem van verbonden gezondheidsinformatie maakt GLOW tot een onmisbaar hulpmiddel voor iedereen die serieus bezig is met het monitoren en verbeteren van hun reproductieve gezondheid.

Of gebruikers nu kiezen voor de gratis basisversie of de uitgebreide premiumfunctionaliteit, GLOW biedt een betrouwbaar, gebruiksvriendelijk en wetenschappelijk onderbouwd systeem voor het beheren van essentiële gezondheidsinformatie, waardoor het zich onderscheidt als de vooraanstaande app in zijn categorie.



Wat is de dreiging? AI-chatbots en valse URL's

Cybercriminelen zetten steeds vaker AI-chatbots in om misleidende links te verspreiden die eruitzien als officiële websites. Deze nieuwe digitale dreiging groeit exponentieel sinds 2023, waarbij kwaadwillenden AI-technologie misbruiken om overtuigende phishing-aanvallen te creëren.

Door de natuurlijke communicatiestijl van chatbots vertrouwen gebruikers eerder op de aangeboden links, waardoor ze kwetsbaar worden voor oplichting en gegevensdiefstal.

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

Hoe werken AI-chatbots bij deze dreiging?

Moderne AI-chatbots beschikken over geavanceerde mogelijkheden die door cybercriminelen worden misbruikt:

Nabootsen van officiële communicatie

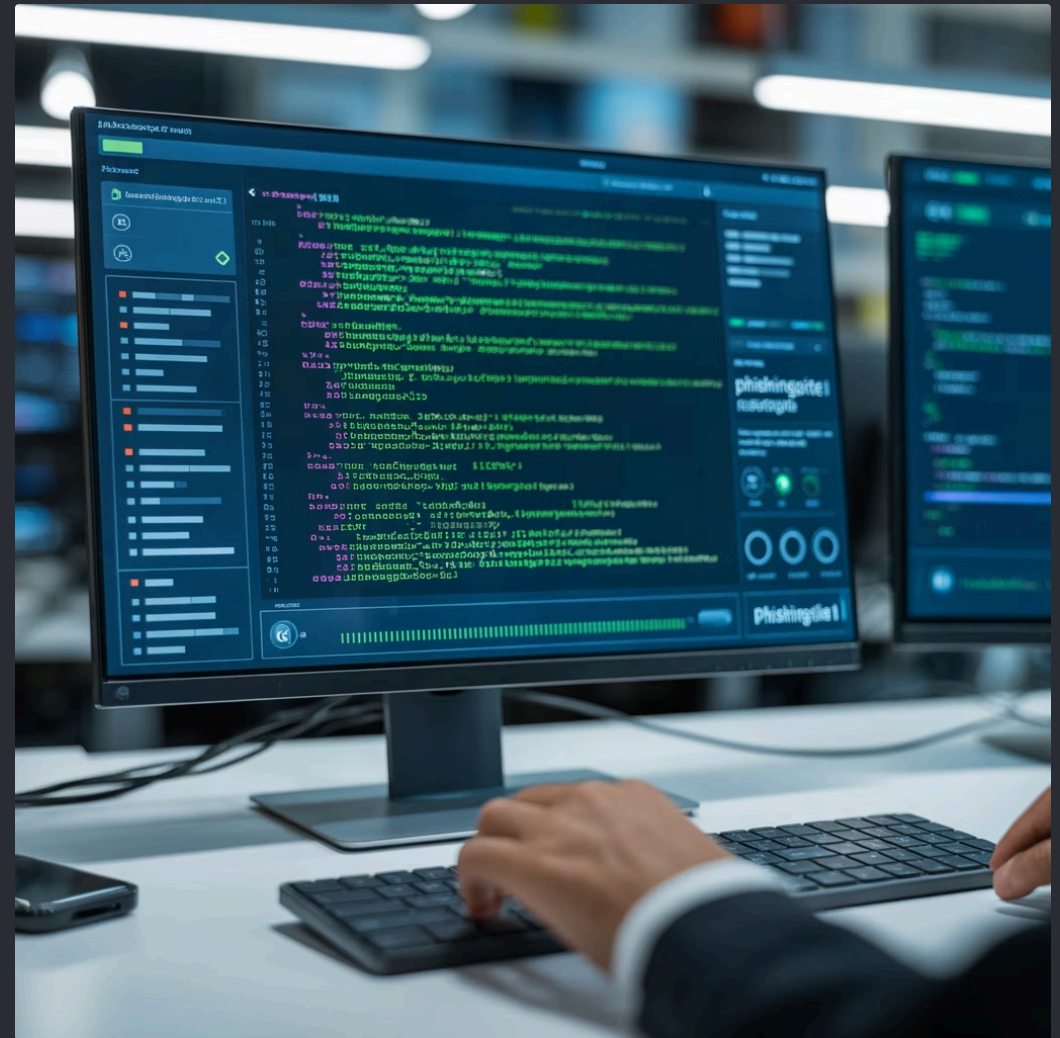
AI-systemen kunnen tekst, toon en stijl van officiële instanties nauwkeurig nabootsen, waardoor berichten authentiek lijken.

Genereren van overtuigende URL's

Chatbots kunnen links produceren die bijna identiek zijn aan legitieme websites, slechts met subtile verschillen die makkelijk over het hoofd worden gezien.

Laagdrempelige tools

Platformen zoals GhostGPT zijn eenvoudig beschikbaar via Telegram, waardoor criminelen zonder technische kennis toch geavanceerde phishing-campagnes kunnen opzetten.



Waarom zijn verkeerde URL's gevaarlijk?



Overtuigende nabootsing

De nepwebsites doen zich voor als officiële overheidsinstanties, banken of bekende diensten. Ze gebruiken correcte logo's, huisstijlen en professioneel taalgebruik om geloofwaardigheid te verhogen.



Psychologische manipulatie

Door gebruik van vertrouwde merkelementen en urgente boodschappen worden gebruikers psychologisch gemanipuleerd om snel te handelen zonder kritisch de URL te controleren.



Schadelijke gevolgen

Eenmaal op de nepsite aangekomen, kan de gebruiker onbewust persoonlijke gegevens prijsgeven, malware downloaden of financiële transacties uitvoeren die rechtstreeks naar criminelen gaan.



Praktijkvoorbeeld: GhostGPT

Een gevaarlijke tool in opmars

GhostGPT is een ongecensureerde AI-chatbot die vrij toegankelijk is via populaire berichtenplatforms zoals Telegram. Deze tool biedt cybercriminelen de mogelijkheid om:

- Op grote schaal geloofwaardige phishing-berichten te genereren
- Compleet valse websites te bouwen die vrijwel identiek zijn aan originele sites
- Gerichte aanvallen uit te voeren zonder enige programmeerkennis
- Phishing-campagnes te personaliseren op basis van doelgroep of slachtoffer

Door de lage technische drempel maken tools als GhostGPT cybercriminaliteit toegankelijk voor een veel bredere groep kwaadwillenden.



Impact en risico's voor bedrijven & burgers

1

Toename BEC-fraude

Business Email Compromise scams zijn met 300% toegenomen sinds de integratie van AI-tools in cybercriminaliteit.

2

Betere slagingskans

Door AI gegenereerde phishingaanvallen hebben 47% meer kans om succesvol te zijn dan traditionele methoden.

3

Gemiddelde schade

Gemiddelde financiële schade voor middelgrote Nederlandse bedrijven na een succesvolle AI-gebaseerde phishingaanval.

De geavanceerde aard van deze aanvallen maakt het steeds moeilijker voor gebruikers om echte van valse links te onderscheiden. Zelfs technisch onderlegde personen kunnen worden misleid door de subtiële verschillen in URL's of de overtuigende context waarin deze worden gepresenteerd.



Bescherming & wat kun je doen?



Technische bescherming

Implementeer AI-gedreven detectiesystemen die verdachte URL's herkennen. Gebruik geavanceerde e-mailfilters en beveiligingssoftware die specifiek is ontworpen om AI-gegenereerde phishing te detecteren.



Training & bewustzijn

Zorg voor regelmatige training van medewerkers en burgers in het herkennen van phishingpogingen. Leer hen verdachte patronen te identificeren en stimuleer een cultuur van digitale waakzaamheid.



Verificatie

Controleer altijd het webadres voordat je gegevens invoert. Typ belangrijke URL's zelf in plaats van op links te klikken. Bij twijfel, neem rechtstreeks contact op met de organisatie via officiële kanalen.

Door deze maatregelen consequent toe te passen, kun je het risico op slachtofferschap aanzienlijk verminderen. Blijf op de hoogte van nieuwe ontwikkelingen op het gebied van cybersecurity en pas je beschermingsstrategieën regelmatig aan.

Wat is Ultra Ethernet en hoe werkt het?

Ultra Ethernet is een geavanceerde netwerkstandaard die is ontwikkeld om te voldoen aan de groeiende eisen van kunstmatige intelligentie en high-performance computing. Deze innovatieve technologie, gelanceerd door het Ultra Ethernet Consortium in 2025, bouwt voort op de bestaande Ethernet-standaard maar biedt aanzienlijke verbeteringen op het gebied van prestaties, schaalbaarheid en latency.

In dit document onderzoeken we de technische architectuur, kernfuncties, protocollen, voordelen en toekomstige toepassingen van Ultra Ethernet, en hoe deze technologie het landschap van datacenters en computersystemen transformeert.

VEILIGDIGITAAL.COM

Technische Architectuur van Ultra Ethernet

De technische architectuur van Ultra Ethernet is ontworpen om verbeteringen door te voeren op alle lagen van de netwerkinfrastructuur, van de fysieke componenten tot de softwareprotocollen. Deze holistische benadering zorgt voor een aanzienlijke verbetering in prestaties en betrouwbaarheid ten opzichte van traditionele netwerktechnologieën.



Netwerkkinterfaces (NICs)

Geavanceerde netwerkkaarten met hardware-acceleratie voor Ultra Ethernet-specifieke functies, zoals verbeterde buffer-beheer en directe geheugentoegangsmechanismen.



Switches

Hoogwaardige switches met intelligente verkeersrouting, dynamische laadbalancerings en ingebouwde ondersteuning voor congestiecontrole op netwerkniveau.



PHY-laag

Geavanceerde SerDes-technologie met snelheden tot 800/1600 Gbps en expliciete congestiesignalen voor optimale datatransmissie.



Kabels

Hoogwaardige verbindingen die grote datavolumes kunnen verwerken met minimaal signaalverlies, ondersteunend aan de hoge snelheden en lage latency.

De PHY-laag (Physical Layer) vormt het fundament van Ultra Ethernet met SerDes-technologie (Serializer/Deserializer) die datasnelheden tot 800 of zelfs 1600 Gbps mogelijk maakt. Deze laag bevat ook expliciete congestie-signalen die netwerkknelpunten snel kunnen identificeren en aanpakken.

Op de link-layer heeft Ultra Ethernet twee cruciale innovaties geïmplementeerd: Link Level Retry (LLR) en Packet Rate Improvement (PRI). LLR maakt het mogelijk om beschadigde pakketten opnieuw te verzenden zonder betrokkenheid van hogere protocollagen, wat de herstelsnelheid aanzienlijk verbetert. PRI optimaliseert de doorvoersnelheid door intelligente pakketplanning en -prioritering.

Een van de meest indrukwekkende aspecten van Ultra Ethernet is de schaalbaarheid. Het systeem is ontworpen om meer dan 1.000.000 eindpunten te ondersteunen met een uitzonderlijke betrouwbaarheid, waardoor het perfect geschikt is voor grootschalige datacenters en HPC-clusters.

Kernfuncties en Innovaties

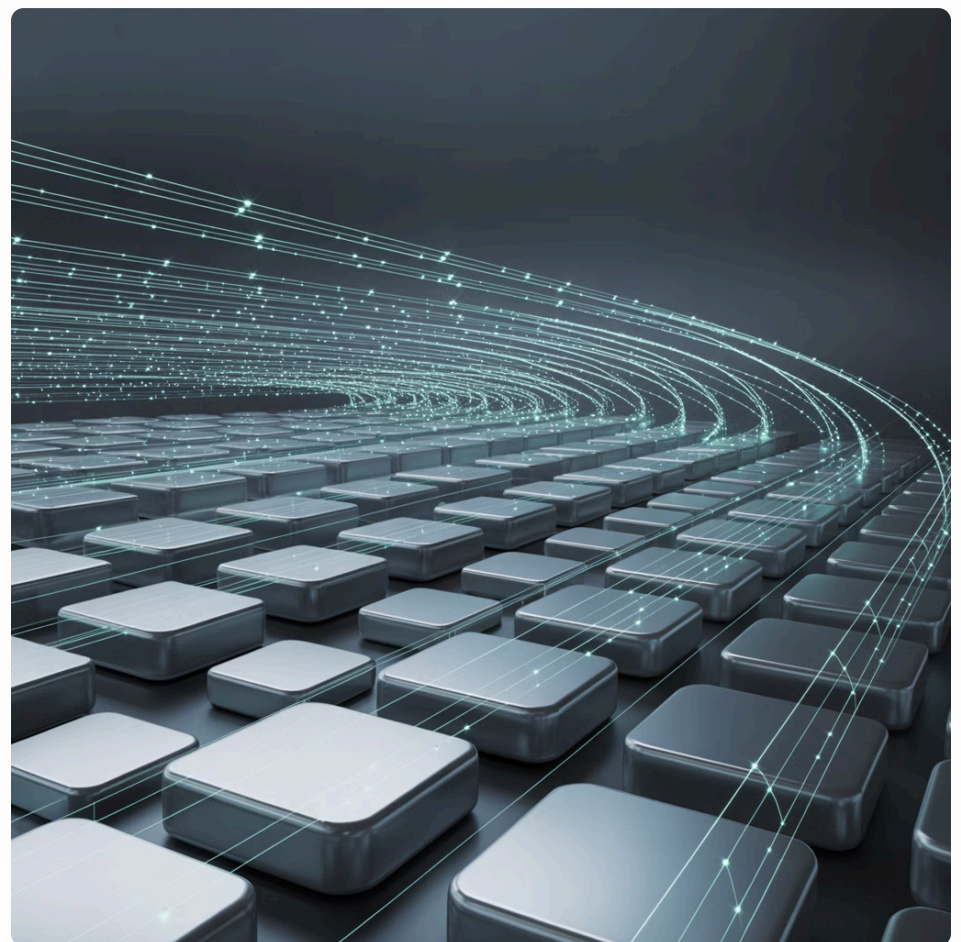
Ultra Ethernet introduceert een reeks baanbrekende functies die de netwerkprestaties, betrouwbaarheid en flexibiliteit naar een nieuw niveau tillen. Deze innovaties stellen de technologie in staat om te voldoen aan de veeleisende behoeften van moderne computeromgevingen.

Uitgebreide Packet-Headers

Een van de belangrijkste vernieuwingen in Ultra Ethernet is de uitgebreide packet-header, die geavanceerde metadata bevat voor intelligente routing en verbeterde beveiliging. Deze headers maken preciezere verkeerscontrole mogelijk en bevatten informatie die helpt bij het optimaliseren van de netwerkprestaties in realtime.

Verbeterde RDMA-Technologie

Ultra Ethernet bevat een aanzienlijk verbeterde implementatie van Remote Direct Memory Access (RDMA), waardoor gegevens rechtstreeks van het geheugen van het ene systeem naar het andere kunnen worden overgebracht zonder tussenkomst van de besturingssystemen. Dit vermindert de latency dramatisch en verbetert de doorvoersnelheid voor data-intensieve toepassingen.



De dynamische bufferallocatie van Ultra Ethernet zorgt voor optimaal gebruik van de beschikbare netwerkbronnen, waardoor congestie wordt verminderd en de algehele prestaties worden verbeterd. Dit systeem past zich voortdurend aan aan de veranderende netwerkomstandigheden, zodat gegevensstromen zo efficiënt mogelijk worden verwerkt.



Een andere belangrijke innovatie is het snelle herstelmecanisme bij fouten. Ultra Ethernet kan netwerkfouten detecteren en herstellen zonder merkbare onderbreking van de service, wat cruciaal is voor toepassingen die een constante en betrouwbare verbinding vereisen, zoals AI-trainingsworkloads.

De technologie ondersteunt ook verschillende verkeerprofielen die kunnen worden geoptimaliseerd voor specifieke gebruikssituaties, zoals AI-training, high-performance computing of gemengde workloads. Deze profielen bepalen hoe netwerkbronnen worden toegewezen en hoe verschillende soorten verkeer worden geprioriteerd, waardoor een optimale prestatie wordt gegarandeerd voor verschillende soorten toepassingen.

Protocollen en Software

De softwarelaag van Ultra Ethernet is essentieel voor het benutten van de krachtige hardwaremogelijkheden. De protocollen en API's zijn ontworpen met het oog op optimale prestaties, gebruiksgemak en flexibiliteit voor ontwikkelaars.

Basisprotocol: Ultra Ethernet Transport (UET)

Het fundament van de Ultra Ethernet-software is het Ultra Ethernet Transport (UET) protocol, dat is gebouwd op libfabric v2.0 API's. Dit protocol biedt een gestandaardiseerde methode voor communicatie tussen Ultra Ethernet-apparaten en zorgt voor compatibiliteit en interoperabiliteit tussen verschillende implementaties.

1

Send-operaties

Verzenden van gegevens met bevestiging van ontvangst, ideaal voor kleine tot middelgrote berichten waar betrouwbaarheid cruciaal is.

2

Write-operaties

Eenzijdige dataoverdracht waarbij de afzender gegevens rechtstreeks naar het geheugen van de ontvanger schrijft zonder tussenkomst van de CPU van de ontvanger.

3

Read-operaties

Eenzijdige dataoverdracht waarbij de aanvrager gegevens rechtstreeks uit het geheugen van de doelcomputer haalt zonder tussenkomst van de CPU van het doel.

4

Rendezvous-varianten

Geavanceerde communicatiemethoden voor zeer grote gegevensoverdrachten die dynamisch de meest efficiënte overdrachtsmethode selecteren.

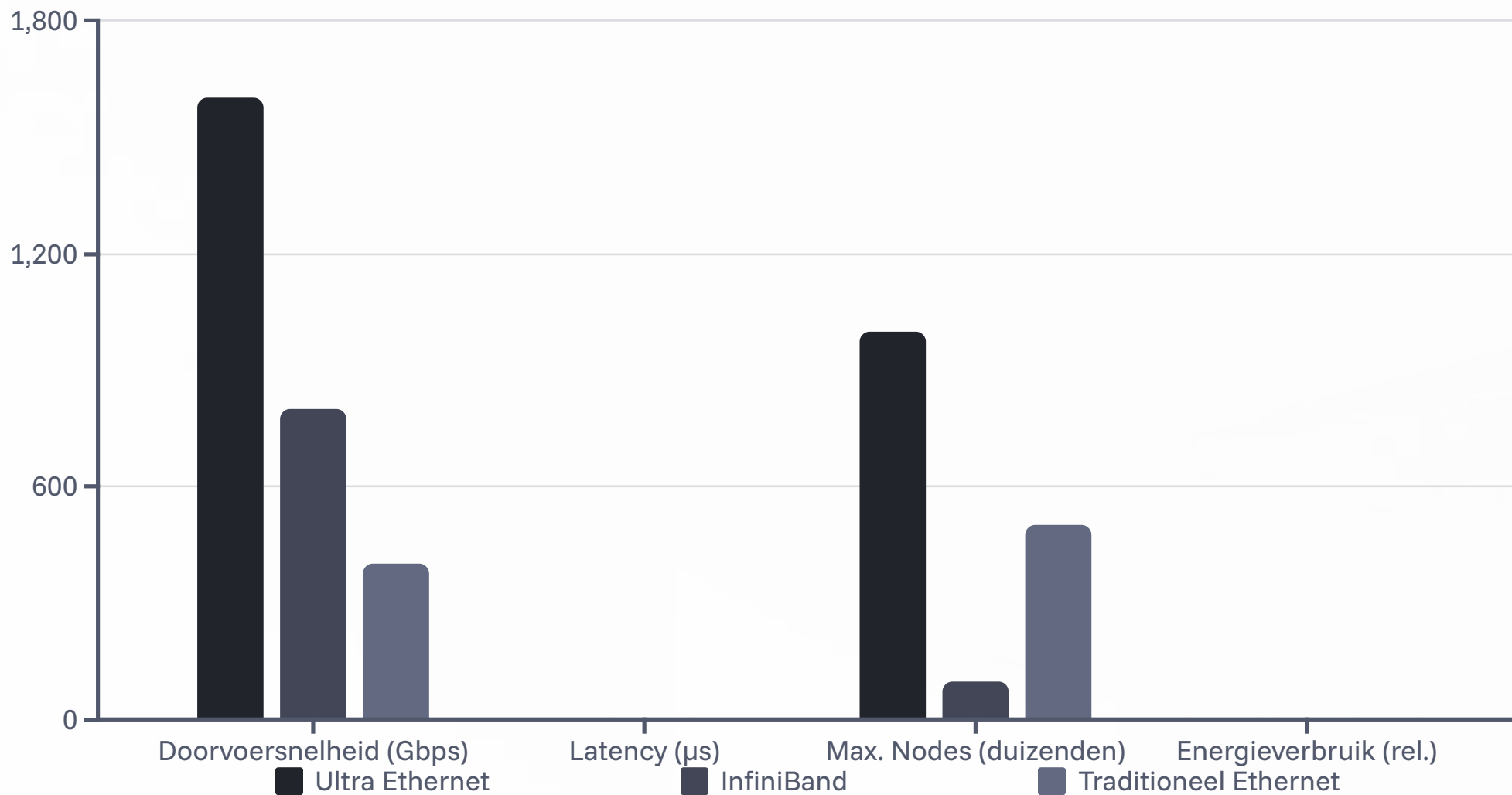
De geoptimaliseerde API van Ultra Ethernet is ontworpen met het oog op eenvoudige integratie en productontwikkeling. Ontwikkelaars kunnen gebruik maken van een reeks intuïtieve functies en bibliotheken die de complexiteit van netwerkprogrammering verbergen, waardoor het gemakkelijker wordt om Ultra Ethernet-compatibele toepassingen te bouwen.

Een belangrijk aspect van de Ultra Ethernet-software is de verbeterde beveiliging. Het protocol bevat ingebouwde encryptie en authenticatiemechanismen die gevoelige gegevens beschermen tijdens de overdracht. Dit is vooral belangrijk in omgevingen waar vertrouwelijke informatie wordt verwerkt, zoals in financiële instellingen of bij medisch onderzoek.

Protocolkenmerk	Voordeel	Toepassing
Zero-copy transmissie	Vermindert CPU-overhead en latency	Grote dataoverdrachten in HPC
Ingebouwde encryptie	Verbeterde gegevensbeveiliging	Financiële transacties, medische gegevens
Adaptieve routing	Optimale pad-selectie	Drukke datacenters met variabele verkeerpatronen
Gedistribueerde congestiecontrole	Voorkomt netwerkvertragingen	AI-trainingsworkloads met hoge bandbreedte

Voordelen ten opzichte van traditionele Ethernet en InfiniBand

Ultra Ethernet biedt aanzienlijke voordelen ten opzichte van zowel traditionele Ethernet-technologie als InfiniBand, waardoor het een overtuigende keuze is voor moderne netwerkomgevingen met hoge prestatie-eisen.



Een van de meest opvallende voordelen van Ultra Ethernet is de combinatie van hogere doorvoersnelheid en lagere latency in vergelijking met InfiniBand. Terwijl InfiniBand lange tijd werd beschouwd als de beste keuze voor high-performance computing, heeft Ultra Ethernet deze technologie nu overtroffen met snelheden tot 1600 Gbps en een latency van slechts 0,5 microseconden.

Flexibiliteit en Schaalbaarheid

Ultra Ethernet behoudt de flexibiliteit en schaalbaarheid die klassieke Ethernet zo populair heeft gemaakt, maar verbetert deze eigenschappen aanzienlijk. Het kan eenvoudig worden geïntegreerd in bestaande netwerken en ondersteunt een breed scala aan topologieën.

Lossless Transport

Anders dan traditioneel Ethernet biedt Ultra Ethernet lossless transport, wat betekent dat gegevenspakketten niet verloren gaan tijdens transmissie. Dit is cruciaal voor toepassingen zoals AI-training, waar gegevensverlies kan leiden tot onnauwkeurige resultaten.

Congestiecontrole

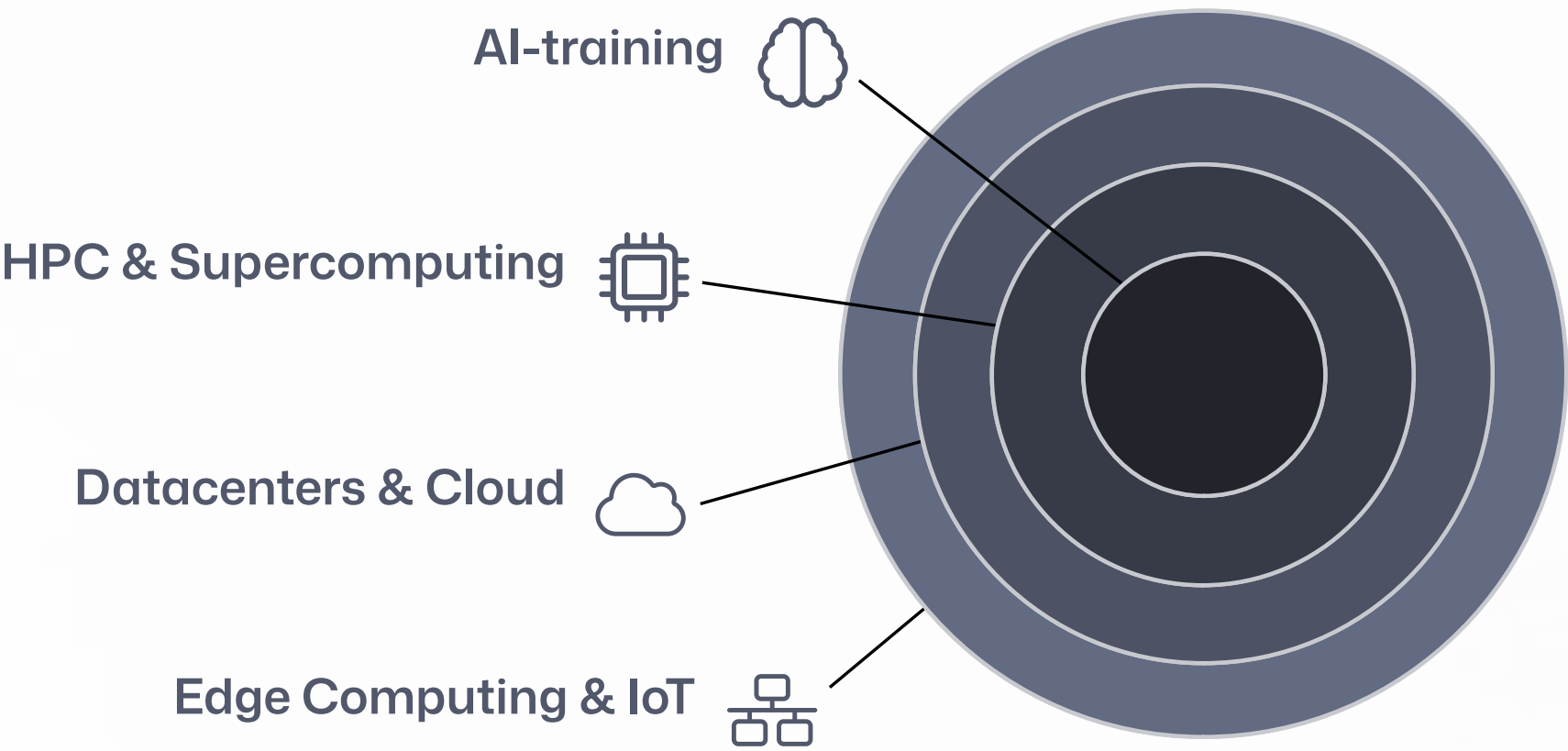
De geavanceerde congestiecontrolemechanismen van Ultra Ethernet voorkomen netwerkvertragingen en zorgen voor een consistente prestatie, zelfs onder zware belasting. Dit maakt het bijzonder geschikt voor omgevingen met variabele verkeerpatronen.

Een ander belangrijk voordeel van Ultra Ethernet is dat het een open standaard is. Dit voorkomt vendor lock-in en bevordert interoperabiliteit tussen apparaten van verschillende fabrikanten. Dit contrasteert met InfiniBand, dat vaak wordt bekritiseerd vanwege zijn meer gesloten ecosysteem.

De openheid van Ultra Ethernet moedigt innovatie aan en maakt het gemakkelijker voor organisaties om de technologie aan te passen aan hun specifieke behoeften. Het bevordert ook concurrentie tussen leveranciers, wat kan leiden tot lagere kosten en betere producten voor eindgebruikers.

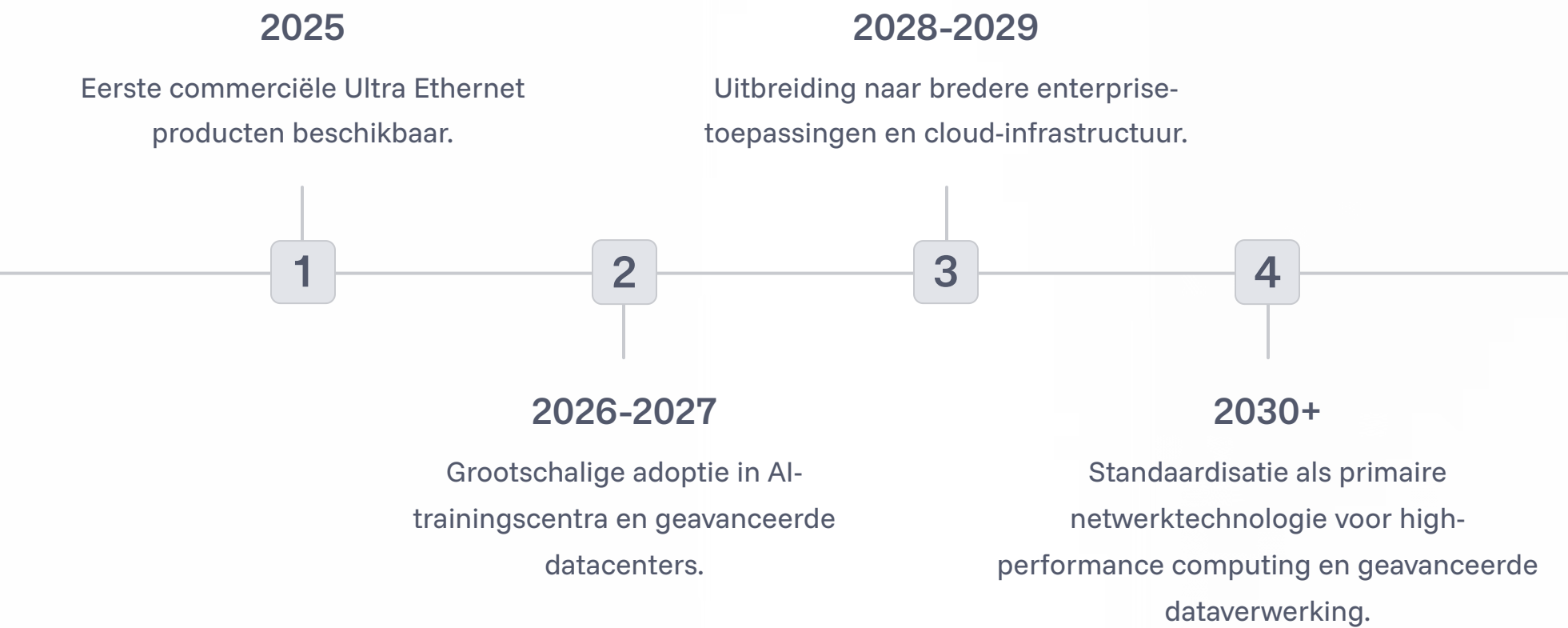
Praktijktoepassingen en Toekomst

Ultra Ethernet is ontworpen voor de meest veeleisende computeromgevingen van vandaag en morgen. De combinatie van hoge prestaties, schaalbaarheid en flexibiliteit maakt het ideaal voor een breed scala aan toepassingen.



In de wereld van kunstmatige intelligentie is Ultra Ethernet bijzonder waardevol. AI-trainingsworkloads vereisen de overdracht van enorme hoeveelheden gegevens tussen GPU-clusters met minimale vertraging. De hoge bandbreedte en lage latency van Ultra Ethernet maken het mogelijk om complexe AI-modellen efficiënter te trainen, wat leidt tot snellere innovatie op gebieden zoals natuurlijke taalverwerking, computervision en voorspellende analyses.

Voor high-performance computing biedt Ultra Ethernet de mogelijkheid om grootschalige clusters te bouwen die wetenschappelijke simulaties, gegevensanalyse en andere rekenintensieve taken kunnen uitvoeren. De schaalbaarheid naar miljoenen nodes maakt het mogelijk om computersystemen te bouwen die voorheen ondenkbaar waren, wat nieuwe mogelijkheden opent voor onderzoek en ontdekking.



De toekomst van Ultra Ethernet ziet er veelbelovend uit, met actieve ontwikkeling van referentie-implementaties die het gemakkelijker maken voor hardware- en softwareleveranciers om de technologie te adopteren. Naarmate meer bedrijven en onderzoeksinstituten de voordelen van Ultra Ethernet erkennen, zal de adoptie waarschijnlijk snel toenemen.

Op de lange termijn heeft Ultra Ethernet het potentieel om uit te groeien tot de standaard netwerkinfrastructuur voor data-intensieve toepassingen. Het toekomstbestendige ontwerp zorgt ervoor dat het kan evolueren om te voldoen aan de veranderende eisen van de technologie-industrie, waardoor het een solide investering is voor organisaties die voorop willen blijven lopen in het digitale tijdperk.



OpenAI lanceert GPT-5: Een Nieuwe Mijlpaal in AI-Ontwikkeling

Willem Bosgra voor

VEILIGDIGITAAL.COM

OpenAI heeft een nieuwe versie van zijn toonaangevende AI-model gelanceerd: GPT-5. Deze update brengt aanzienlijke verbeteringen met zich mee en versterkt OpenAI's positie in de snel groeiende AI-markt.

Dit artikel belicht de nieuwe mogelijkheden van GPT-5, de toenemende populariteit van AI-chatbots, zakelijke partnerschappen en de financiële ontwikkelingen binnen OpenAI.

GPT-5: Een Kwantumsprong in AI-Capaciteiten

Van Middelbare Scholier naar PhD

Volgens Sam Altman, topman van OpenAI, biedt GPT-5 "een flinke verbetering" ten opzichte van eerdere versies. Hij vergelijkt GPT-3 met een 'middelbare scholier', GPT-4 met een 'universiteitsstudent', en GPT-5 als "een team van experts met een PhD op zak voor alles wat je wilt weten."

De Nieuwe Functies en Mogelijkheden van GPT-5

GPT-5 markeert een significante sprong voorwaarts in de evolutie van AI-modellen, wat zich vertaalt in een reeks krachtige nieuwe functies en verbeterde capaciteiten. Deze ontwikkelingen zijn niet alleen indrukwekkend op technisch vlak, maar bieden ook concrete voordelen voor zowel individuele gebruikers als bedrijven.

Geavanceerd Redeneervermogen

GPT-5 kan complexe problemen analyseren, logische verbanden leggen en strategische oplossingen genereren met een diepgang die voorheen onbereikbaar was. Dit maakt het model uitermate geschikt voor taken die geavanceerd denken vereisen, zoals diepgaand onderzoek, complexe data-analyse en het ontwikkelen van innovatieve concepten.

Verminderde 'Hallucinaties' en Verhoogde Nauwkeurigheid

Een van de meest cruciale verbeteringen in GPT-5 is de aanzienlijke reductie van 'hallucinaties'. Het model levert consistentere en betrouwbaardere antwoorden, wat essentieel is voor toepassingen in sectoren waar accurate informatie van levensbelang is, zoals financiën, gezondheidszorg en juridische advisering.

Uitgebreide Zakelijke Toepassingen

De focus op zakelijke mogelijkheden is duidelijk. GPT-5 kan een breed scala aan taken uitvoeren, van het genereren van hoogwaardige marketingteksten en gedetailleerde rapporten tot het assisteren bij complexe financiële analyses en het schrijven van programmeercode. Dit versnelt de productiviteit en stimuleert innovatie binnen organisaties.

Dieper Contextueel Begrip en Langere Coherentie

Het model is in staat om context over langere gesprekken en documenten te behouden, wat resulteert in veel natuurlijkere en efficiëntere interacties. Het kan eerdere inputs onthouden en daarop voortbouwen, waardoor complexe projecten en langdurige dialogen naadloos kunnen worden voortgezet.

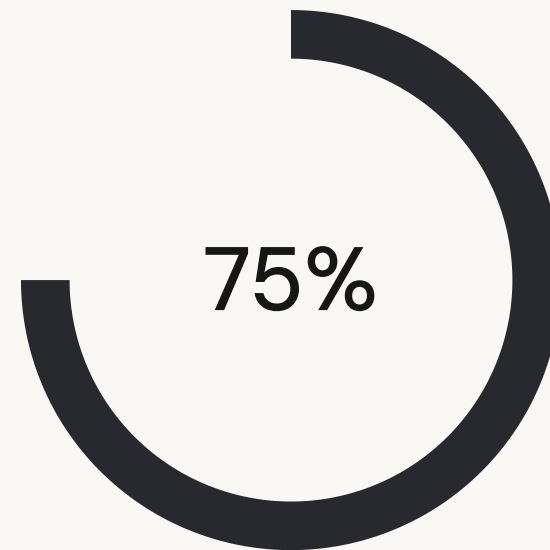
Deze verbeteringen positioneren GPT-5 niet alleen als een krachtig hulpmiddel voor algemeen gebruik, maar ook als een gespecialiseerde assistent die in staat is om de meest veeleisende professionele taken te ondersteunen.

De Razendsnelle Opmars van ChatGPT

ChatGPT werd ongeveer drie jaar geleden gelanceerd en werd in korte tijd razend populair. De kracht van het systeem ligt in het genereren van teksten die nauwelijks te onderscheiden zijn van door mensen geschreven content.

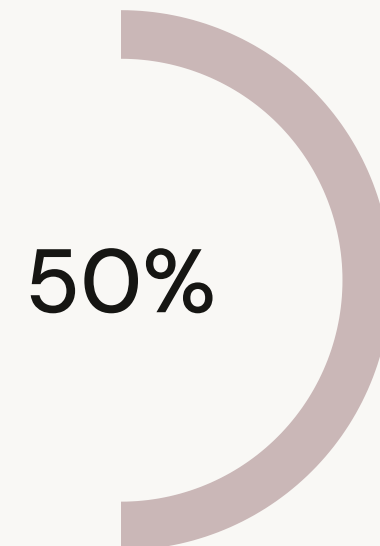
De impact van deze technologie is vooral onder jongeren significant. Uit recent onderzoek van Common Sense Media blijkt dat bijna drie op de vier Amerikaanse tieners weleens een AI-chatbot hebben gebruikt voor vriendschappelijk contact.

Deze snelle adoptie vindt plaats ondanks toenemende zorgen over de veiligheid van deze technologie en de mogelijke invloed op de mentale gezondheid van gebruikers.



Amerikaanse Tieners

Heeft weleens een AI-chatbot gebruikt voor vriendschappelijk contact



Regelmatig Gebruik

Meer dan de helft gebruikt virtuele gesprekspartners regelmatig

Zorgen over AI-Gebruik door Jongeren

⊗ Advies Common Sense Media

Common Sense Media, een organisatie die technologie en media beoordeelt op geschiktheid voor kinderen, adviseert minderjarigen geen gebruik te laten maken van AI-gezelschap, zolang de veiligheid ervan niet gegarandeerd kan worden.

De snelle adoptie van AI-chatbots door jongeren roept vragen op over de langetermijneffecten. Hoewel de technologie fascinerend is en nieuwe mogelijkheden biedt voor educatie en entertainment, zijn er ook zorgen over:

Mentale Gezondheid

Mogelijke negatieve invloed op de sociale ontwikkeling en het welzijn van jongeren die te afhankelijk worden van virtuele gesprekspartners.

Privacy

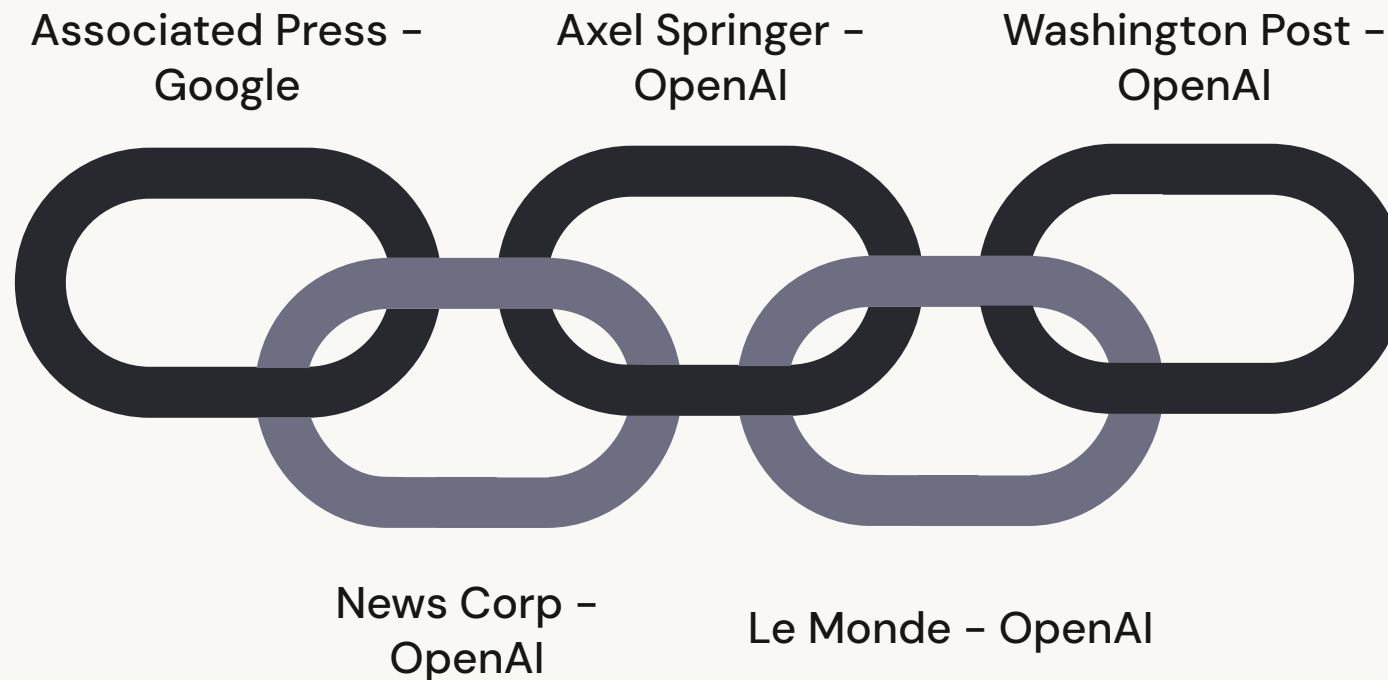
Zorgen over de gegevens die worden verzameld tijdens gesprekken met AI-chatbots, vooral bij minderjarige gebruikers.

Betrouwbaarheid

Risico's verbonden aan het vertrouwen op mogelijk onjuiste of misleidende informatie die door AI wordt gegenereerd.

Mediapartnerschappen met AI-Bedrijven

Over de hele wereld hebben mediaconcerns deals gesloten met grote AI-spelers. Deze partnerschappen stellen AI-bedrijven in staat om hoogwaardige content te gebruiken voor het trainen van hun modellen, terwijl uitgevers nieuwe inkomstenstromen genereren.



Enkele opvallende samenwerkingen zijn:

- Associated Press heeft een overeenkomst gesloten met Google
- News Corp (eigenaar van *The Wall Street Journal*) heeft een deal met OpenAI
- Axel Springer (eigenaar van onder andere Politico, *Bild* en *Die Welt*) werkt samen met OpenAI
- *Le Monde* en *The Washington Post* hebben ook overeenkomsten met OpenAI gesloten

Strategie voor Talentbehoud



Aandelenpakketten

Snelgroeiende techbedrijven belonen hun medewerkers vaak met aandelenpakketten om talent aan zich te binden.



Verlies van Talent

De afgelopen maanden verloor OpenAI enkele leden van zijn onderzoeksafdeling aan Meta, de moeder van Facebook.

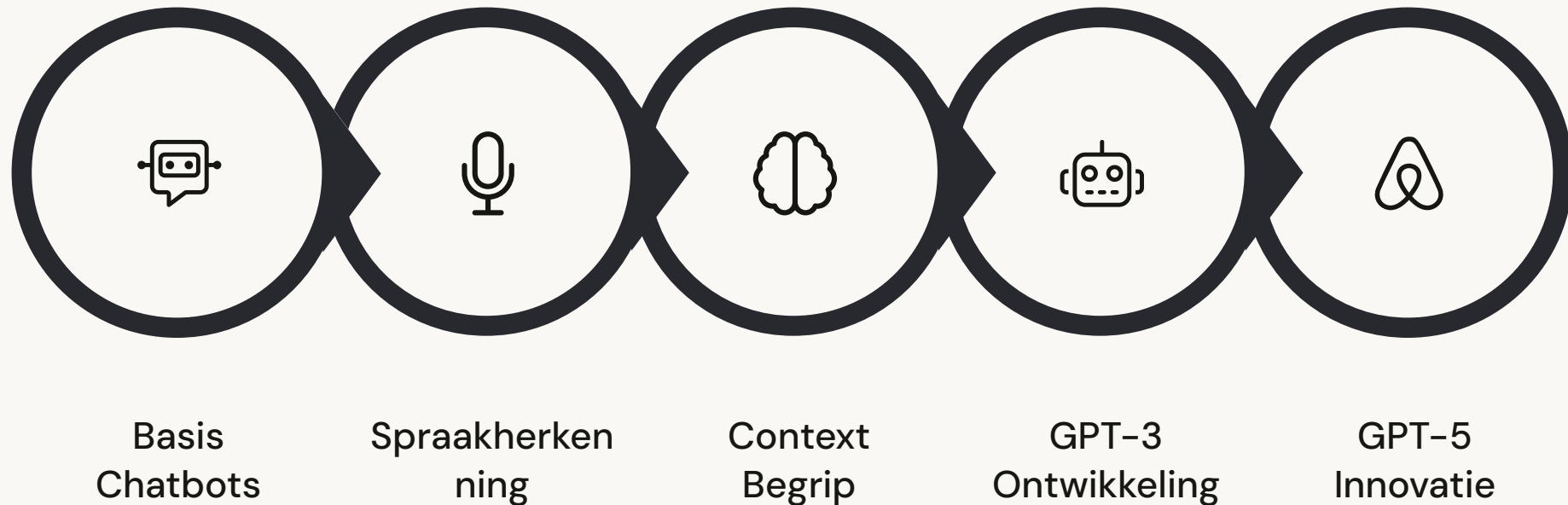


Nieuwe Aandelendeal

Een nieuwe aandelendeal is mogelijk bedoeld om verdere leegloop te voorkomen en toptalent te behouden.

De voorgestelde verkoop van medewerkersaandelen kan worden gezien als een strategische zet om talent te behouden in een competitieve markt waar AI-experts zeer gewild zijn. Door medewerkers de mogelijkheid te bieden om een deel van hun aandelen te verzilveren, kan OpenAI loyaliteit stimuleren zonder dat medewerkers het bedrijf hoeven te verlaten om financieel te profiteren van hun aandelenbezit.

De Toekomst van AI-Interactie



Met de lancering van GPT-5 zet OpenAI een belangrijke stap in de evolutie van AI-systemen. De verbeterde capaciteiten maken het model geschikt voor complexe taken en betrouwbaardere interacties. Dit opent nieuwe mogelijkheden voor:

- Geavanceerde zakelijke toepassingen die complexe problemen kunnen oplossen
- Betrouwbaardere informatiebronnen voor onderwijs en onderzoek
- Meer natuurlijke en genuanceerde conversaties met AI-assistenten
- Nieuwe creatieve toepassingen in schrijven, ontwerpen en probleemoplossing

Tegelijkertijd blijven er uitdagingen bestaan rond ethiek, privacy en de maatschappelijke impact van steeds geavanceerdere AI-systemen.

Conclusie: Balanceren tussen Innovatie en Verantwoordelijkheid

De lancering van GPT-5 markeert een belangrijke mijlpaal in de ontwikkeling van kunstmatige intelligentie. OpenAI blijft de grenzen verleggen van wat mogelijk is met AI-technologie, terwijl het bedrijf ook groeit in marktwaarde en invloed.

Tegelijkertijd roept de snelle adoptie van deze technologie, vooral onder jongeren, vragen op over de verantwoordelijkheid van AI-ontwikkelaars en de maatschappelijke impact van hun creaties.



Balans Vinden

De uitdaging voor OpenAI en andere AI-ontwikkelaars is om een balans te vinden tussen innovatie en verantwoordelijkheid, tussen commercieel succes en maatschappelijk welzijn.

Naarmate AI-systemen zoals GPT-5 steeds capabeler worden, wordt het steeds belangrijker om kritisch na te denken over hoe we deze technologie willen inzetten en reguleren in onze samenleving.



Windows 11 installeren op een niet- ondersteund systeem met Rufus

Willem Bosgra

voor VEILIG DIGITAAL

Deze handleiding laat zien hoe je met behulp van Rufus toch Windows 11 kunt installeren op een systeem dat niet aan de officiële hardware-eisen van Microsoft voldoet. We bespreken de risico's, benodigdheden, stapsgewijze instructies en belangrijke overwegingen na installatie. Deze methode is op eigen risico en vooral bedoeld voor ervaren gebruikers.

Waarom Windows 11 niet standaard op jouw pc wil installeren

Microsoft heeft bij de introductie van Windows 11 de systeemeisen aanzienlijk verhoogd ten opzichte van eerdere versies. Deze strengere eisen zijn voornamelijk gericht op het verbeteren van de beveiliging, maar zorgen er ook voor dat veel nog goed functionerende computers niet officieel worden ondersteund.

Wanneer je probeert Windows 11 te installeren op een systeem dat niet aan deze eisen voldoet, krijg je een foutmelding te zien: "Deze pc kan Windows 11 niet uitvoeren." Microsoft raadt in dit geval af om de installatie voort te zetten vanwege mogelijke compatibiliteitsproblemen.

Zelfs als je computer krachtig genoeg is om Windows 11 probleemloos te draaien, kan het ontbreken van TPM 2.0 of Secure Boot de installatie blokkeren. Mocht je erin slagen Windows 11 toch te installeren op niet-ondersteunde hardware, dan kan er een watermerk in beeld verschijnen en loop je mogelijk officiële updates en beveiligingspatches mis.

Minimale systeemeisen Windows 11

- TPM 2.0 (Trusted Platform Module)
- Secure Boot ondersteuning
- Recente CPU (8e generatie Intel of nieuwer)
- Minimaal 4GB RAM-geheugen
- Minimaal 64GB opslagruimte
- DirectX 12 compatibele grafische kaart

De risico's en gevolgen van het omzeilen van de hardware-eisen

Het installeren van Windows 11 op niet-ondersteunde hardware brengt verschillende risico's met zich mee die je zorgvuldig moet overwegen voordat je deze route kiest.

1

Instabiliteit

Je kunt te maken krijgen met onverwacht systeemgedrag, crashes of prestatieproblemen omdat de hardware niet volledig compatibel is met het besturingssysteem.

2

Geen ondersteuning

Microsoft biedt geen officiële hulp bij problemen op niet-ondersteunde systemen. Ook hardwarefabrikanten kunnen ondersteuning weigeren als je Windows 11 op incompatibele hardware gebruikt.

3

Updateproblemen

Hoewel beveiligingsupdates momenteel nog worden geleverd, kan Microsoft dit beleid wijzigen. Bovendien kunnen toekomstige updates specifiek ontworpen zijn voor ondersteunde hardware, wat tot storingen kan leiden.

4

Beveiligingsrisico's

De hardwarevereisten zijn deels ingesteld om een basisniveau van beveiliging te garanderen. Zonder deze hardware-elementen kan je systeem kwetsbaarder zijn voor bepaalde aanvallen.

"Het omzeilen van de systeemeisen is een keuze op eigen risico en wordt alleen aanbevolen voor ervaren gebruikers die de mogelijke gevolgen begrijpen en accepteren."

 Als je Windows 11 gebruikt voor kritieke zakelijke toepassingen of gevoelige persoonlijke gegevens, is het sterk aan te raden om alleen geïnstalleerd te worden op volledig ondersteunde hardware.

Vorbereiding: wat heb je nodig voordat je begint?

Een goede voorbereiding is essentieel voor een succesvolle installatie van Windows 11 op niet-ondersteunde hardware. Zorg dat je alle benodigdheden verzamelt voordat je begint.

USB-installatiemedium

Een USB-stick van minimaal 8 GB capaciteit, bij voorkeur 16 GB. Alle bestaande gegevens op deze stick worden gewist tijdens het proces.

Windows 11 ISO-bestand

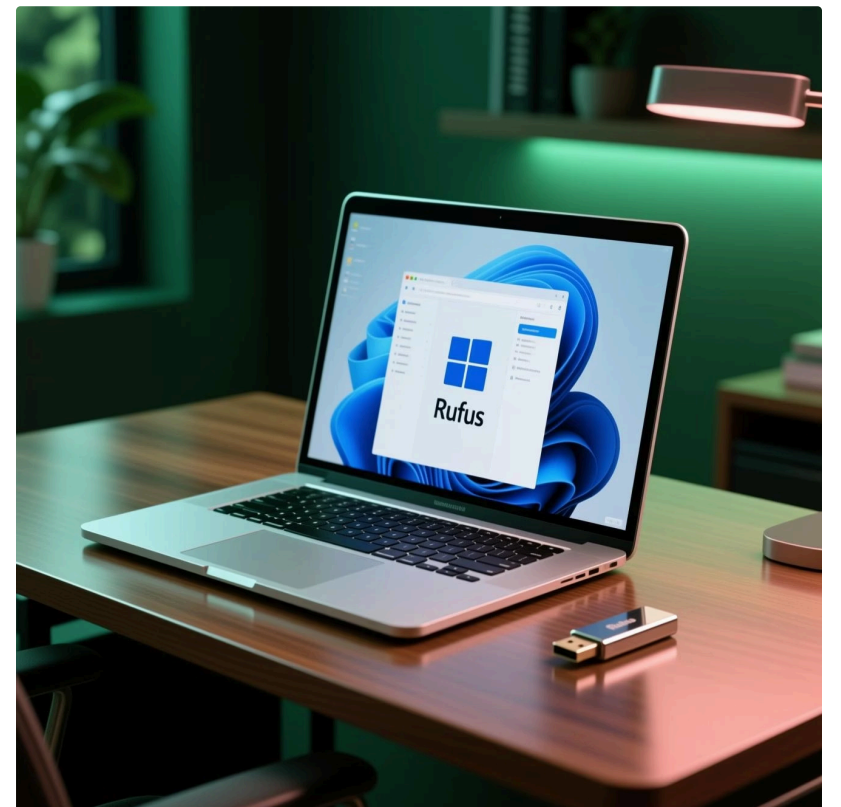
Download de officiële Windows 11 ISO van de Microsoft website: <https://www.microsoft.com/nl-nl/software-download/windows11>

Rufus software

Download de nieuwste versie van Rufus vanaf de officiële website: <https://rufus.ie>. Deze tool zal de hardware-checks in de Windows 11-installatie omzeilen.

Back-up van belangrijke gegevens

Maak een volledige back-up van je bestanden, want elke besturingssysteeminstallatie brengt risico's met zich mee voor je gegevens.

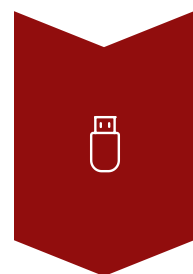


De PC Health Check app van Microsoft kan je helpen identificeren welke specifieke hardware-eisen jouw systeem niet haalt, zodat je beter begrijpt welke beperkingen je mogelijk tegenkomt.

- ❑ Controleer vooraf of je computer ten minste aan de minimale prestatie-eisen voldoet (4GB RAM, dual-core processor van 1GHz of sneller, 64GB opslag), ook al mis je TPM 2.0 of Secure Boot. Te weinig rekenkracht zal alsnog leiden tot een slechte gebruikerservaring.

Stap-voor-stap: Windows 11 installeren met Rufus op een niet-ondersteund systeem

Rufus is een krachtige tool die een Windows 11 installatiemedium kan aanpassen om de hardware-checks te omzeilen. Volg deze stappen nauwkeurig om een succesvolle installatie te realiseren.



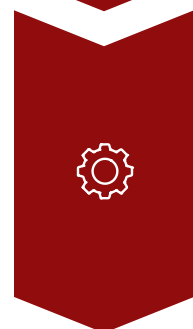
Vorbereiden USB-medium

Start Rufus en sluit je USB-stick aan. Selecteer de stick in het dropdown-menu bij 'Apparaat'. Let op: alle gegevens op de stick worden gewist!



ISO-bestand selecteren

Klik op de knop 'Selecteren' en navigeer naar de Windows 11 ISO die je hebt gedownload. Selecteer het bestand en klik op 'Openen'.



Instellingen aanpassen

Zoek bij 'Image-opties' naar de optie 'Windows 11 installatie (onondersteunde hardware toestaan)' en selecteer deze. Rufus zal nu automatisch een registertweak toepassen die de TPM-, Secure Boot- en RAM-controles uitschakelt.



USB-medium creëren

Controleer alle instellingen en klik op 'Start'. Wacht tot het proces is voltooid – dit kan enkele minuten duren, afhankelijk van je USB-stick en computer.

F12

Boot Menu Toets

De meestgebruikte toets om het boot-menu te openen tijdens opstarten. Dit verschilt per computer (F2, F8, F10, DEL zijn andere mogelijkheden).

10 dagen

Terugkeertijd

Periode waarbinnen je veilig terug kunt keren naar Windows 10 als je Windows 11 niet bevalt of problemen ervaart.

±30 min

Installatietijd

Gemiddelde tijd die nodig is voor de volledige Windows 11 installatie na het booten vanaf de USB-stick.

Nadat je computer is opgestart vanaf de USB-stick, volg je de standaard Windows 11 installatieprocedure. De hardware-checks worden nu omzeild. Je kunt kiezen voor een upgrade-installatie om je bestanden en programma's te behouden, of voor een schone installatie waarbij alles wordt gewist.

 Als je meerdere schijven in je computer hebt, let dan goed op dat je Windows 11 op de juiste schijf installeert om te voorkomen dat je per ongeluk gegevens wist.

Na de installatie: wat je moet weten en doen

Gefeliciteerd met je Windows 11 installatie! Hoewel het systeem nu draait op niet-ondersteunde hardware, zijn er enkele belangrijke zaken waar je rekening mee moet houden voor een optimale ervaring.

Watermerk en ondersteuningsstatus

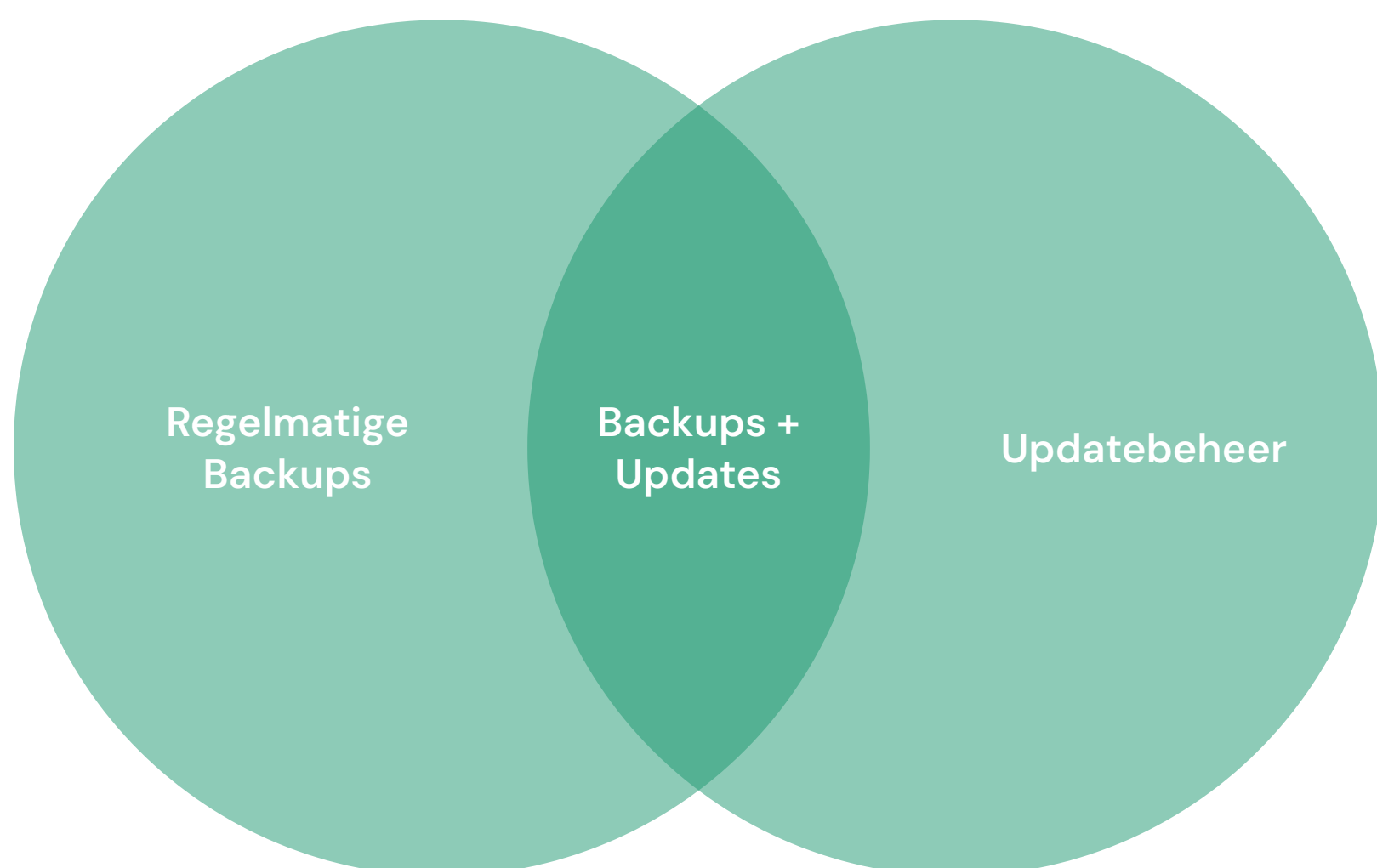
Mogelijk zie je een watermerk rechtsonder op je bureaublad dat aangeeft dat je systeem niet aan de minimale eisen voldoet. Dit is slechts een visuele herinnering en beperkt de functionaliteit niet. Microsoft kan echter besluiten om in toekomstige updates de functionaliteit voor niet-ondersteunde systemen verder te beperken.

Gegevensbescherming

Maak regelmatig back-ups van belangrijke gegevens, omdat niet-ondersteunde hardware een hoger risico op stabiliteits- en compatibiliteitsproblemen met zich meebrengt. Gebruik hiervoor de ingebouwde back-upfunctie van Windows of een externe back-upoplossing.

Updates en beveiliging

Controleer regelmatig of er updates beschikbaar zijn via Instellingen > Windows Update. Hoewel beveiligingsupdates momenteel nog worden geleverd, kan het zijn dat functie-updates worden geblokkeerd of problemen veroorzaken. Als een update vastloopt, kun je deze mogelijk installeren met dezelfde Rufus-methode door een nieuwe Windows 11 installatiemedium te maken met de nieuwste versie.



"Als je toch besluit terug te gaan naar Windows 10, doe dit dan binnen 10 dagen via Instellingen > Systeem > Herstel > Teruggaan. Na deze periode is een schone installatie van Windows 10 nodig."

⊗ Bij grote Windows 11 functie-updates (zoals 23H2) moet je mogelijk de Rufus-methode opnieuw toepassen, omdat Microsoft de hardware-checks blijft handhaven bij elke grote update.



Google stelt stilletjes nieuwe AI-beveiligingsregels in Chrome in

Willem Bosgra

voor VEILIG DIGITAAL

Google heeft recent een reeks innovatieve AI-beveiligingsfuncties geïmplementeerd in Chrome zonder veel ophef te maken. Deze nieuwe technologieën, waaronder Big Sleep en Gemini Nano, werken stilletjes op de achtergrond om gebruikers te beschermen tegen kwetsbaarheden, phishing en online oplichting.

Deze significante verbeteringen in de browserbeveiliging respecteren de privacy van gebruikers terwijl ze een nieuwe standaard zetten in proactieve cyberveiligheid.

AI als stille beschermmer: Big Sleep ontdekt en helpt kwetsbaarheden dichten

Google heeft een belangrijke stap gezet in proactieve cyberveiligheid met de ontwikkeling van Big Sleep, een geavanceerde AI-agent die is ontstaan uit een samenwerking tussen Google DeepMind en Project Zero. Deze innovatieve technologie is specifiek ontworpen om automatisch softwarekwetsbaarheden op te sporen voordat ze door kwaadwillenden kunnen worden misbruikt.

Een eerste groot succes werd al geboekt in Chrome 139, waar Big Sleep een kritieke kwetsbaarheid (CVE-2025-9132) in de V8 JavaScript-engine identificeerde. Deze ontdekking was baanbrekend: het was de eerste keer dat een AI-systeem direct heeft bijgedragen aan het voorkomen van een exploitatie in het wild. Google heeft het beveiligingslek onmiddellijk gepatcht, waarmee het een nieuwe standaard zet voor de inzet van kunstmatige intelligentie in cyberveiligheid.



		
Automatische detectie	Directe mitigatie	Open source versterking
Big Sleep scant continu code om potentiële kwetsbaarheden te identificeren voordat ze kunnen worden misbruikt.	Zodra een kwetsbaarheid is ontdekt, werkt het samen met beveiligingsteams om snel patches te ontwikkelen.	Big Sleep wordt ook ingezet om open source-projecten veiliger te maken, wat de veiligheid van het hele internet vergroot.

Naast Chrome richt Google zich op het verbeteren van de veiligheid in het bredere internet-ecosysteem door Big Sleep in te zetten voor het analyseren van open source-projecten. Dit proactieve beveiligingsinitiatief markeert een belangrijke verschuiving in de manier waarop technologiebedrijven omgaan met cyberdreigingen, waarbij AI een centrale rol speelt in het beschermen van miljarden gebruikers wereldwijd.

Gemini Nano: AI op je apparaat tegen online scams en misleiding

Naast Big Sleep heeft Google ook Gemini Nano geïntroduceerd, een krachtig AI-model dat direct op het apparaat van de gebruiker draait. Deze innovatie biedt real-time bescherming binnen Chrome tegen een groeiend aantal online bedreigingen, met bijzondere aandacht voor tech support scams en misleidende websites.

Enhanced Protection

Gemini Nano vormt een extra AI-beschermingslaag binnen de Enhanced Protection modus van Chrome, waardoor gebruikers dubbele beveiliging krijgen tegen phishing en andere geavanceerde bedreigingen.

Misleidende notificaties

Op Android waarschuwt Chrome gebruikers nu actief voor verdachte notificatieverzoeken van kwaadaardige websites, met eenvoudige opties om deze direct af te wijzen of zich af te melden.

Scamdetectie

AI-technologie heeft geleid tot een vermindering van 80% in scams op Google Search, waaronder nep-klantenservicenummers van luchtvaartmaatschappijen die slachtoffers misleidden.

De integratie van Gemini Nano in Chrome vormt een belangrijke mijlpaal in de democratisering van AI-gestuurde beveiliging, waarbij geavanceerde bescherming beschikbaar wordt voor alle gebruikers zonder dat dit ten koste gaat van de prestaties of privacy.

Vooraf opmerkelijk is de effectiviteit van deze AI-oplossingen bij het bestrijden van tech support scams, die vaak gericht zijn op minder technisch onderlegde gebruikers. Door misleidende websites in real-time te identificeren en gebruikers te waarschuwen, helpt Google een van de meest kwetsbare groepen internetgebruikers te beschermen tegen oplichting die jaarlijks miljarden dollars kost.

Privacy en controle: AI-beveiliging zonder concessies



Bij de implementatie van deze geavanceerde AI-beveiligingsfuncties benadrukt Google dat privacy en gebruikerscontrole centraal blijven staan. De AI-gedreven functies in Chrome en Workspace zijn ontworpen om de privacy van gebruikers volledig te respecteren, waarbij nadrukkelijk wordt gesteld dat er geen data wordt gebruikt voor modeltraining zonder expliciete toestemming.

Alle interacties met AI-systemen zoals Gemini blijven binnen de grenzen van de organisatie en volgen de bestaande beveiligingsprotocollen, waardoor bedrijfsgevoelige informatie beschermd blijft.

Voor zakelijke gebruikers biedt Chrome Enterprise extra AI-gestuurde beveiligingsopties die zijn afgestemd op de specifieke behoeften van organisaties:

- Geavanceerde datalekpreventie die automatisch gevoelige informatie kan identificeren en beschermen
- Real-time toegangscontrole op basis van Zero Trust-principes
- Geautomatiseerde dreigingsdetectie en -respons
- Contextbewuste beveiligingsmaatregelen die zich aanpassen aan gebruikersgedrag
- Transparante rapportage over beveiligingsgebeurtenissen
- Gecentraliseerd beheer van AI-beveiligingsfuncties

Deze stille AI-innovaties vertegenwoordigen een fundamentele verschuiving in browserbeveiliging, waarbij Google erin slaagt de veiligheid van miljarden gebruikers te versterken zonder hun gebruikservaring te verstoren. Door privacy voorop te stellen en tegelijkertijd geavanceerde bescherming te bieden, zet Google een nieuwe standaard voor hoe technologiebedrijven AI kunnen inzetten om het internet veiliger te maken voor iedereen.



Gratis grote bestanden delen? Ga naar Transfer.it, onderdeel van MEGA

Willem Bosgra

voor VEILIG DIGITAAL

Op zoek naar een veilige en gebruiksvriendelijke manier om grote bestanden te delen zonder kosten? Transfer.it, onderdeel van het bekende cloudopslagplatform MEGA, biedt de perfecte oplossing.

In dit document ontdek je wat Transfer.it precies is, waarom het een uitstekende keuze is voor het delen van grote bestanden, hoe je het kunt gebruiken en waarom steeds meer mensen voor deze dienst kiezen.

Wat is Transfer.it en de link met MEGA?

Transfer.it is een innovatieve online dienst die speciaal is ontwikkeld voor het moeiteloos delen van grote bestanden. Als onderdeel van MEGA, een gerenommeerde speler in de wereld van cloudopslag, profiteert Transfer.it van jarenlange expertise op het gebied van veilige gegevensoverdracht en bestandsopslag.

MEGA heeft een sterke reputatie opgebouwd dankzij hun toewijding aan gebruikersprivacy en geavanceerde end-to-end encryptietechnologie. Deze belangrijke kernwaarden zijn volledig geïntegreerd in de Transfer.it-dienst, waardoor gebruikers kunnen vertrouwen op zowel de veiligheid als de betrouwbaarheid van het platform.



Veiligheid van MEGA

Profiteer van de bewezen end-to-end encryptietechnologie die MEGA wereldwijd bekendheid heeft gegeven.



Betrouwbare infrastructuur

Gebruik de robuuste servernetwerken van MEGA voor snelle uploads en downloads zonder onderbrekingen.



Gebruiksvriendelijk

Geniet van een intuïtieve interface die het delen van bestanden toegankelijk maakt voor iedereen.

Waarom kiezen voor Transfer.it om grote bestanden te delen?

In een wereld waarin we dagelijks grote hoeveelheden gegevens uitwisselen, biedt Transfer.it een aantal overtuigende voordelen die het tot een uitstekende keuze maken voor zowel incidentele als frequente gebruikers.



Direct aan de slag zonder registratie

Anders dan bij veel andere diensten hoef je geen account aan te maken of persoonlijke gegevens achter te laten. Upload direct je bestanden en begin met delen zonder enige vertraging.

Geschikt voor écht grote bestanden

Waar e-mailbijlagen vaak beperkt zijn tot enkele MB's, stelt Transfer.it je in staat om substantieel grotere bestanden te versturen. Dit is ideaal voor het delen van video's, designbestanden, presentaties of volledige projectmappen.

Privacy gegarandeerd met encryptie

Elk bestand dat je uploadt wordt automatisch versleuteld. Deze **end-to-end encryptie** zorgt ervoor dat alleen jij en de beoogde ontvanger toegang hebben tot de inhoud van je bestanden.

Transfer.it is hiermee de perfecte oplossing voor zowel professionele gebruikers die regelmatig grote bestanden delen met klanten, als voor particulieren die incidenteel foto's of video's willen versturen naar vrienden en familie.

Hoe werkt het delen via Transfer.it?

Het proces voor het delen van bestanden via Transfer.it is ontworpen met gebruiksgemak als hoogste prioriteit. In slechts enkele eenvoudige stappen kun je grote bestanden veilig versturen naar iedereen, waar ook ter wereld.

Bezoek de website

Ga naar de Transfer.it website, die onderdeel is van het MEGA-ecosysteem. De interface is overzichtelijk en direct klaar voor gebruik.

Ontvang je unieke link

Na voltooiing van de upload genereert het systeem automatisch een **unieke downloadlink** die je kunt kopiëren.

Extra beveiligingsopties

Voor gevoelige bestanden biedt Transfer.it aanvullende beveiligingsmogelijkheden die je eenvoudig kunt instellen:

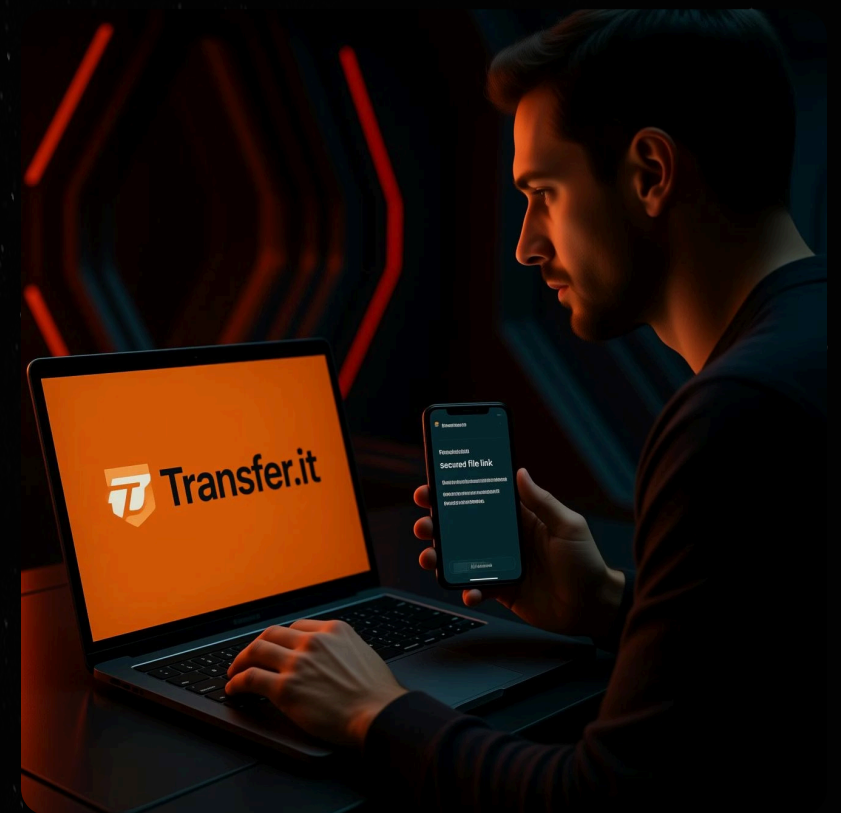
- Stel een **wachtwoord** in dat de ontvanger moet invoeren voordat het bestand gedownload kan worden
- Bepaal een **vervaldatum** waarna de link automatisch ongeldig wordt
- Beperk het aantal keren dat een bestand gedownload kan worden
- Ontvang notificaties wanneer je bestand is gedownload

Upload je bestanden

Klik op de uploadknop of sleep je bestanden direct naar het aangegeven gebied. Het platform ondersteunt meerdere bestandsformaten en -groottes.

Deel met ontvangers

Verstuur de link via e-mail, chatapp of elk ander communicatiekanaal. De ontvanger kan direct downloaden zonder account.

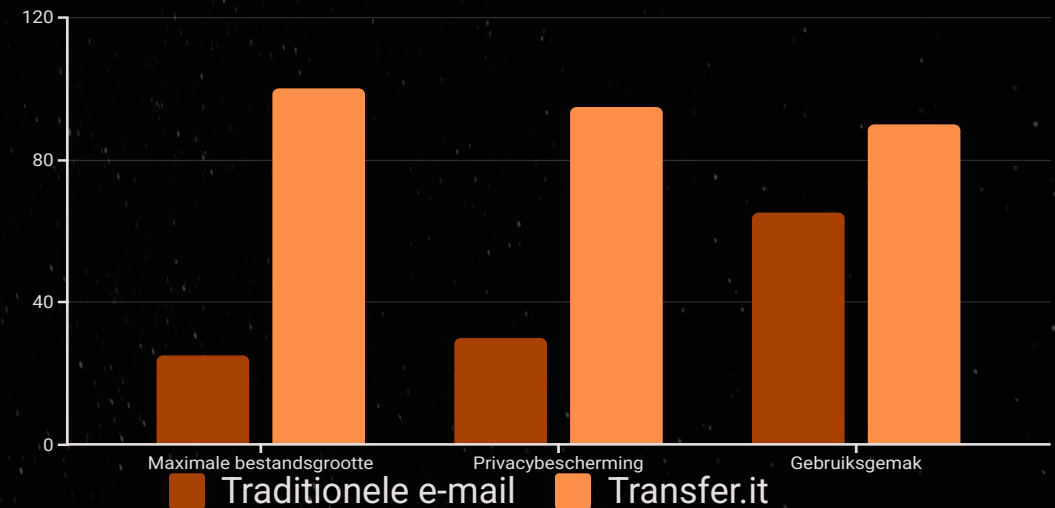


Conclusie: De slimme keuze voor gratis grote bestanden delen

Transfer.it biedt de perfecte balans tussen gebruiksgemak, functionaliteit en beveiliging, zonder enige kosten voor de gebruiker.

In een digitale wereld waar het delen van grote bestanden steeds belangrijker wordt, onderscheidt Transfer.it zich als een betrouwbare en toegankelijke oplossing. Door de integratie met MEGA's bewezen beveiligingstechnologie hoef je je geen zorgen te maken over de veiligheid van je gegevens.

Of je nu een freelancer bent die grote ontwerpbestanden deelt met klanten, een student die projecten uitwisselt met medestudenten, of gewoon iemand die vakantievideo's wil versturen naar familie - Transfer.it maakt het proces **eenvoudig, snel en veilig**.



- ✓ **Begin vandaag nog met Transfer.it** en ervaar zelf hoe eenvoudig het delen van grote bestanden kan zijn. Geen registratie, geen verborgen kosten, gewoon directe toegang tot een krachtige en veilige bestandsdeeldienst.

Bezoek Transfer.it via de website en ontdek waarom steeds meer mensen overstappen op deze innovatieve dienst van MEGA voor al hun behoeften op het gebied van bestandsoverdracht.

Gratis Office Pakketten: Welk is de Beste Vervanger voor Microsoft Office?

willem Bosgra

voor VEILIG DIGITAAL



In dit document analyseren we vijf gratis alternatieven voor Microsoft Office, waarbij we hun functies, voor- en nadelen vergelijken om te bepalen welke het beste kan dienen als vervanger voor het bekende, maar betaalde, Office-pakket van Microsoft.

Inleiding: De Behoefte aan Gratis Office Alternatieven

Microsoft Office is al jarenlang de industriestandaard voor kantoorpakketten, maar de kosten vormen voor veel gebruikers een aanzienlijke uitgave. Zowel particulieren als kleine bedrijven zoeken naar budgetvriendelijke alternatieven die dezelfde functionaliteit bieden zonder de prijskaartjes van Microsoft's oplossingen.

De markt voor gratis Office-pakketten is de afgelopen jaren sterk gegroeid, met diverse opties die elk hun eigen sterke punten hebben. In sommige gevallen kunnen deze gratis alternatieven zelfs functies bieden die in Microsoft Office ontbreken.

Waarom zoeken naar alternatieven?

- Kostenbesparing voor particulieren en bedrijven
- Voorkeur voor open-source software
- Behoefte aan specifieke functies die Microsoft niet biedt
- Platform-onafhankelijkheid (Windows, Mac, Linux)

Beoordelingscriteria

- Compatibiliteit met Microsoft Office-bestanden
- Gebruiksvriendelijkheid en interface
- Beschikbare functies en mogelijkheden
- Updates en community-ondersteuning
- Betrouwbaarheid en prestaties

In dit document vergelijken we vijf populaire gratis Office-pakketten en evalueren we welke het beste kan dienen als volwaardig alternatief voor Microsoft Office.

1. LibreOffice: De Krachtige Open-Source Optie

LibreOffice is ontstaan als afsplitsing van OpenOffice en heeft zich ontwikkeld tot één van de meest volwaardige gratis Office-alternatieven. Dit volledig open-source pakket biedt een complete suite van applicaties die vrijwel alle functies van Microsoft Office kunnen vervangen.

1

Writer

Tekstverwerker vergelijkbaar met Word, ondersteunt complexe documenten, stijlen en opmaak.

2

Calc

Spreadsheetprogramma met uitgebreide formules, draaitabellen en grafieken.

3

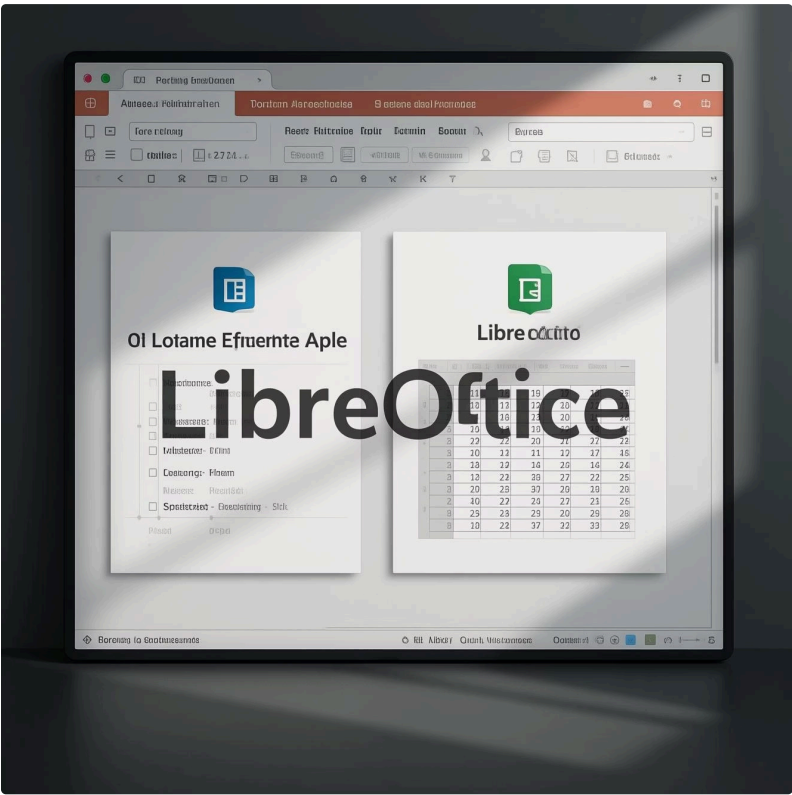
Impress

Presentatiesoftware met effecten, animaties en diverse weergavemodi.

4

Draw, Math & Base

Aanvullende programma's voor tekeningen, formules en databases.



"LibreOffice biedt de meest uitgebreide functionaliteit van alle gratis Office-alternatieven, met uitstekende compatibiliteit met Microsoft-formaten."

Voor- en Nadelen

Voordelen:

- Volledige compatibiliteit met Microsoft Office-bestanden
- Actieve ontwikkelaarsgemeenschap met regelmatige updates
- Beschikbaar voor Windows, macOS en Linux
- Uitgebreide documentatie en community-ondersteuning

Nadelen:

- Interface is minder modern dan Microsoft Office
- Geen officiële technische ondersteuning (tenzij via betaalde partners)
- Complexe documenten uit Microsoft Office kunnen soms opmaakproblemen vertonen
- Iets langere opstarttijd vergeleken met lichtere alternatieven

2. Apache OpenOffice: Een Volwaardige Vervanging

Apache OpenOffice is één van de oudste en meest gevestigde alternatieven voor Microsoft Office. Als voorloper van LibreOffice deelt het veel van dezelfde code, maar volgt een ander ontwikkelingspad met een conservatievere benadering van updates en nieuwe functies.



Writer

Tekstverwerker met uitgebreide opmaakopties, sjablonen en revisietools.



Calc

Krachtig spreadsheetprogramma met ondersteuning voor complexe berekeningen.



Impress

Presentatiesoftware met diverse sjablonen en animatie-effecten.

Waarom kiezen voor Apache OpenOffice?

Voordelen:

- Stabiele, beproefde software met minimale bugs
- Goede compatibiliteit met Microsoft Office-documenten
- Nederlandse spellingcontrole ingebouwd
- Lager geheugengebruik dan sommige alternatieven
- Beschikbaar voor Windows, macOS en Linux

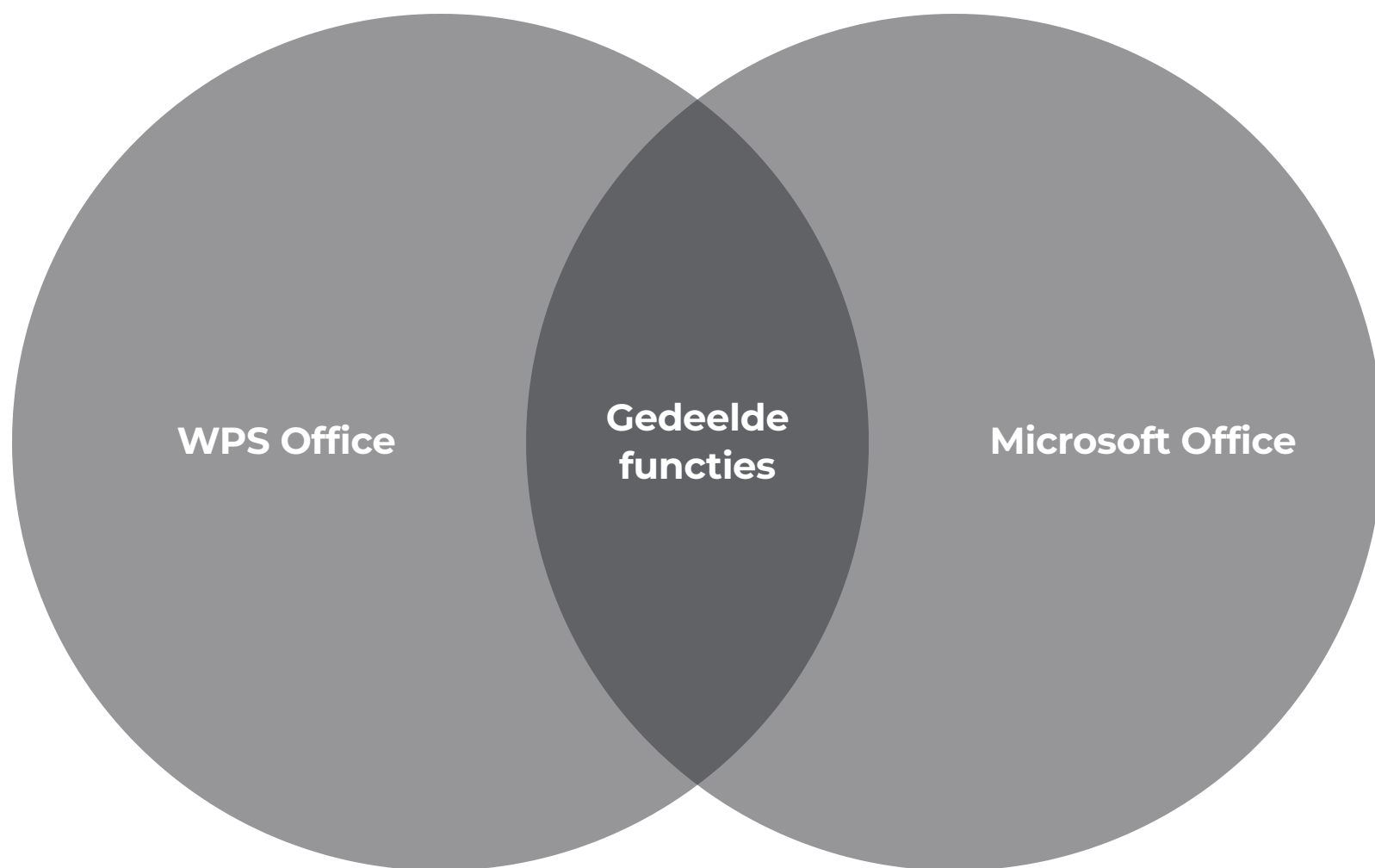
Nadelen:

- Minder frequente updates dan LibreOffice
- Kleinere ontwikkelaarsgemeenschap
- Mist enkele nieuwere functies die LibreOffice wel heeft
- Beperkte ondersteuning voor recente bestandsformaten

❏ Apache OpenOffice heeft een trouwe gebruikersbasis, maar voor wie de nieuwste functies belangrijk vindt, is LibreOffice mogelijk een betere keuze. Voor stabiele, betrouwbare prestaties blijft OpenOffice echter een solide optie.

3. WPS Office: Gebruiksvriendelijk en Compatibel

WPS Office onderscheidt zich door een moderne, aantrekkelijke interface die sterk lijkt op die van Microsoft Office. Voor gebruikers die gewend zijn aan de look-and-feel van Microsoft's producten biedt WPS Office een vertrouwde ervaring zonder de kosten.



Belangrijkste functies:

- Writer: tekstverwerking met geavanceerde opmaaktools
- Presentation: uitgebreide presentatiesoftware
- Spreadsheets: krachtige rekenbladen met formules
- PDF-bewerking en -conversie
- Cloud-opslag en synchronisatie
- Mobiele apps voor Android en iOS

Voor- en nadelen:

Voordelen:

- Zeer gebruiksvriendelijke interface
- Uitstekende compatibiliteit met Microsoft Office-formaten
- Snelle opstarttijd en prestaties
- Beschikbaar op meerdere platforms

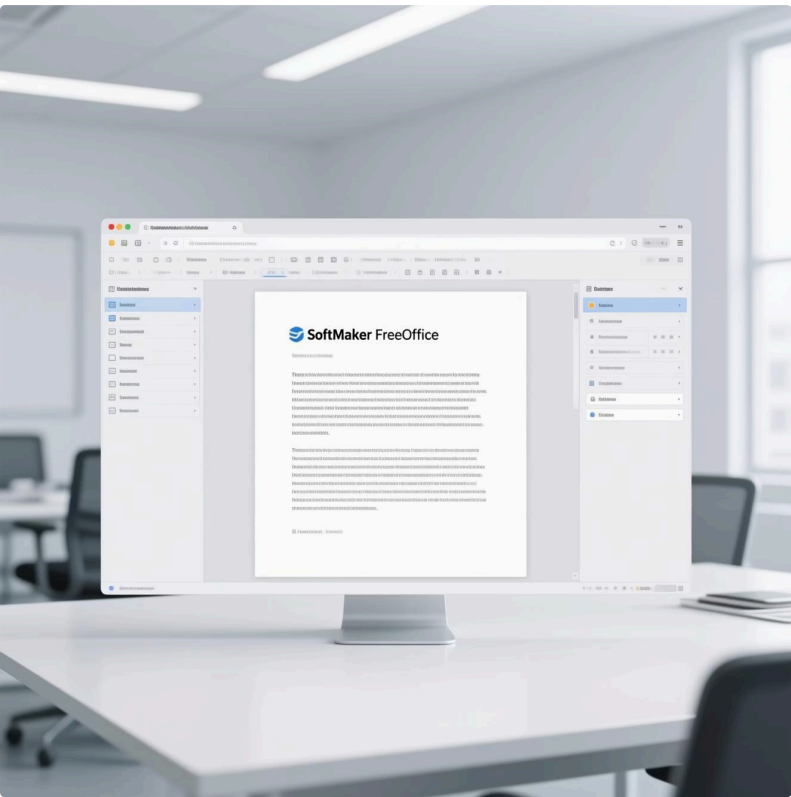
Nadelen:

- Bevat advertenties in de gratis versie
- Sommige geavanceerde functies vereisen een premium-abonnement
- Minder open source dan LibreOffice/OpenOffice

WPS Office is bijzonder geschikt voor gebruikers die een naadloze overgang zoeken van Microsoft Office, zonder concessies te doen aan gebruiksgemak of compatibiliteit.

4. SoftMaker FreeOffice: Eenvoudig en Compatibel

SoftMaker FreeOffice is een Europees alternatief dat zich richt op eenvoud en compatibiliteit. Het pakket biedt een indrukwekkende balans tussen gebruiksgemak en functionaliteit, met bijzondere aandacht voor naadloze bestandsuitwisseling met Microsoft Office.



Kerncomponenten:

1

TextMaker

Tekstverwerker compatibel met DOCX-formaat

2

PlanMaker

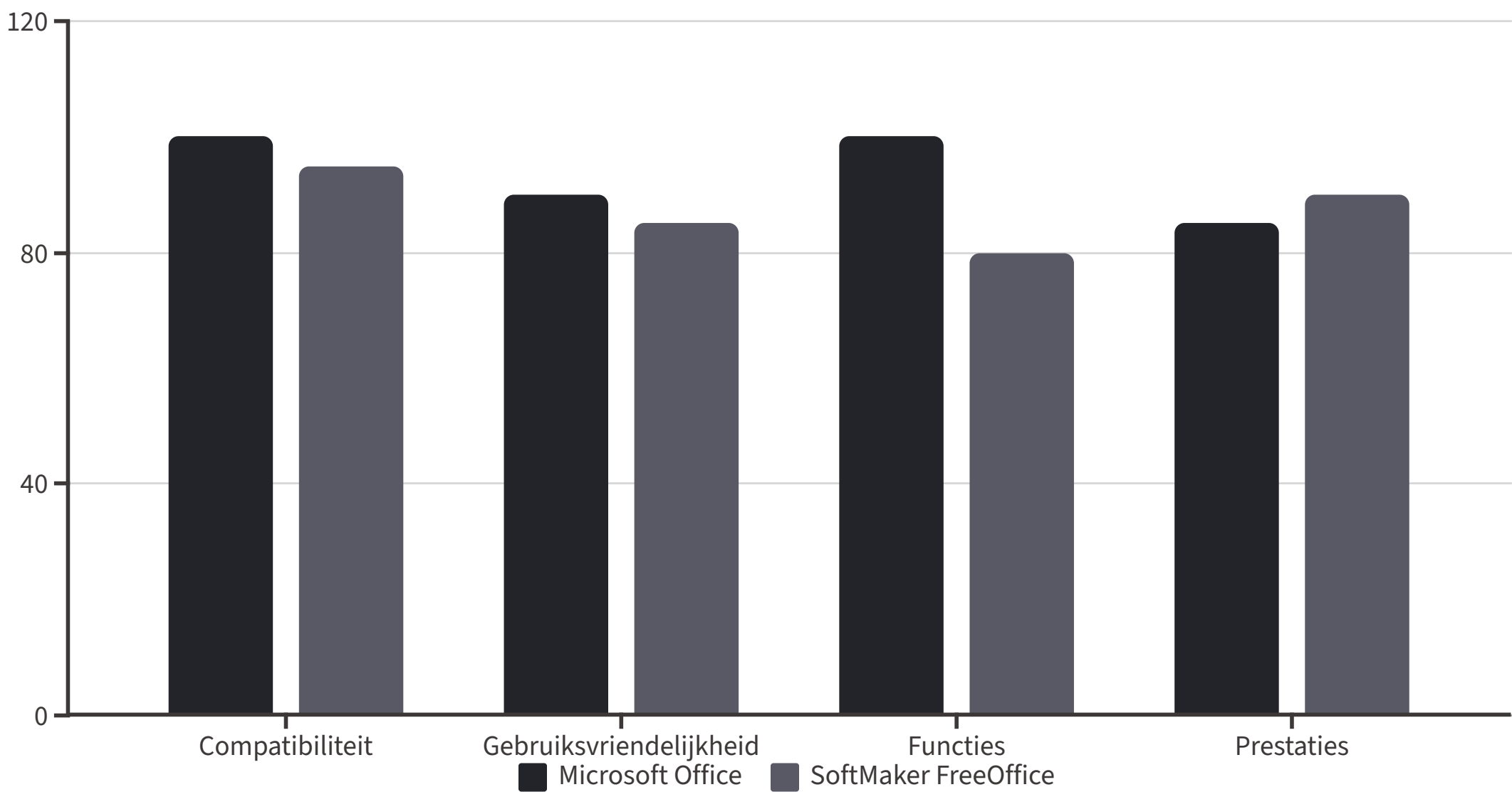
Spreadsheetprogramma met XLSX-ondersteuning

3

Presentations

Presentatiesoftware met PPTX-compatibiliteit

SoftMaker FreeOffice onderscheidt zich door de nadruk op bestandscompatibiliteit. Het kan Microsoft Office-documenten openen en opslaan zonder opmaakproblemen, wat het een ideale keuze maakt voor gebruikers die regelmatig bestanden uitwisselen met Microsoft Office-gebruikers.



Voordelen: Uitstekende compatibiliteit met Microsoft Office, intuïtieve interface, snelle prestaties, klassieke menustructuur beschikbaar naast ribboninterface.

Nadelen: Sommige geavanceerde functies zijn alleen beschikbaar in de betaalde versie, minder actieve gemeenschap dan bij LibreOffice.

5. ONLYOFFICE: Samenwerkingsgerichte Cloud-oplossing

ONLYOFFICE is een moderne, op samenwerking gerichte kantooroplossing die zowel desktop- als cloudversies biedt. Het onderscheidt zich door de nadruk op real-time samenwerking en is daarmee een uitstekend alternatief voor zowel Microsoft Office als Google Workspace.

ONLYOFFICE is beschikbaar als een gratis open-source versie voor persoonlijk gebruik, en als een betaalde editie met extra functies voor bedrijven. Het combineert de voordelen van traditionele Office-pakketten met moderne cloudgebaseerde samenwerkingstools.



Document Editor

Geavanceerde tekstverwerker met uitstekende DOCX-compatibiliteit en real-time co-authoring.



Spreadsheet Editor

Krachtige rekenbladen met formules, grafieken en data-analyse tools.



Presentation Editor

Uitgebreide presentatiesoftware met overgangen en animaties.



Form Creator

Tool voor het maken en delen van online formulieren.

Waarom kiezen voor ONLYOFFICE?

Voordelen:

- Uitstekende Microsoft Office-compatibiliteit
- Real-time samenwerkingstools ingebouwd
- Moderne, schone interface
- Beschikbaar als desktop-, server- of cloudoplossing
- Open-source met actieve ontwikkeling

Nadelen:

- Desktopversie vereist meer systeembronnen dan sommige alternatieven
- Sommige geavanceerde functies alleen in betaalde versies
- Minder offline documentatie beschikbaar
- Complexere installatie voor selfhosted-versie

ONLYOFFICE is bijzonder geschikt voor teams en organisaties die op zoek zijn naar een oplossing die samenwerking centraal stelt, vergelijkbaar met Google Docs maar met betere Microsoft Office-compatibiliteit.

Conclusie: Welk Alternatief is het Beste?

Na het analyseren van de vijf gratis Office-pakketten kunnen we concluderen dat elk pakket zijn eigen sterke punten heeft, afhankelijk van de specifieke behoeften van de gebruiker.

Beste Algehele Alternatief: LibreOffice

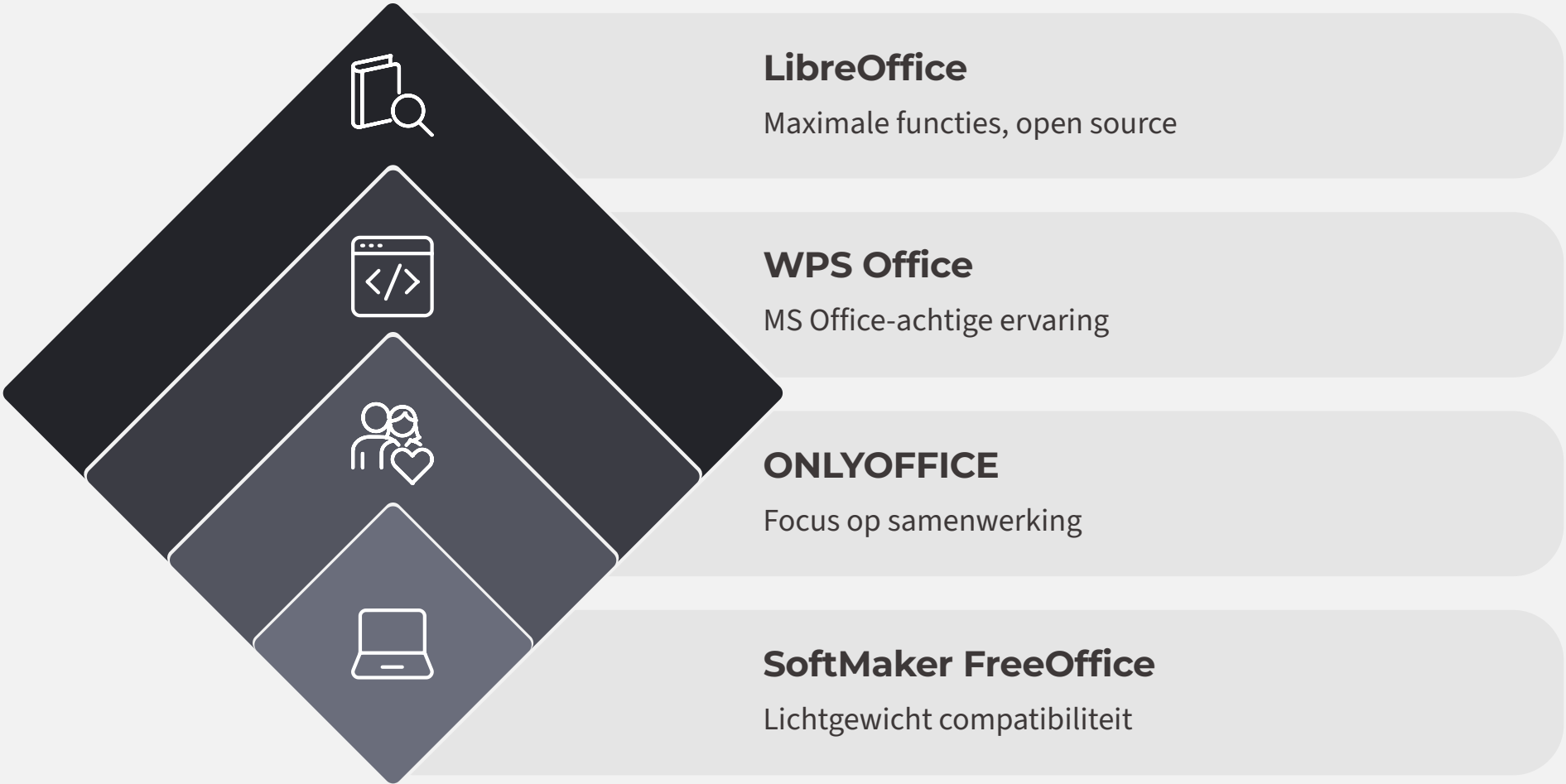
LibreOffice biedt de meest complete set functies en de beste langetermijnondersteuning. De actieve gemeenschap zorgt voor regelmatige updates en verbeteringen, wat het tot de meest duurzame keuze maakt.

Beste voor Microsoft Office-gebruikers: WPS Office

Voor gebruikers die gewend zijn aan de interface van Microsoft Office biedt WPS Office de meest naadloze overgang met een vertrouwde look-and-feel en uitstekende bestandscompatibiliteit.

Beste voor Samenwerking: ONLYOFFICE

Voor teams en organisaties die samenwerking centraal stellen, is ONLYOFFICE de beste keuze met zijn uitstekende real-time co-authoring functies.



Het is raadzaam om meerdere pakketten te proberen voordat u een definitieve keuze maakt, aangezien de persoonlijke voorkeur en specifieke gebruikspatronen een grote rol spelen bij het bepalen van de beste oplossing voor uw behoeften.

A man and a young boy are shown in a futuristic, dimly lit environment with orange and red ambient lighting. The man, on the left, is looking intently at a smartphone held by the boy on the right. A glowing white Wi-Fi symbol is superimposed over the phone. The background features architectural elements with glowing orange lines and red vertical light strips.

Is AirDrop een gevaar voor kinderen? Een gids voor ouders

Willem Bosgra

voor VEILIG DIGITAAL

AirDrop, de populaire bestandsdelingsfunctie van Apple, biedt onmiskenbare voordelen maar brengt ook risico's met zich mee voor kinderen. Deze gids helpt ouders begrijpen wat AirDrop is, waarom het een risico kan vormen, en hoe je de veiligheid van je kind kunt waarborgen bij het gebruik van deze technologie.

Wat is AirDrop en waarom gebruiken kinderen het?

AirDrop is een ingebouwde functie op Apple-apparaten die gebruikers in staat stelt om snel en draadloos bestanden uit te wisselen met andere Apple-apparaten in de buurt. Deze technologie maakt gebruik van Bluetooth en Wi-Fi om een directe verbinding tot stand te brengen tussen apparaten die zich binnen een straal van ongeveer 10 meter bevinden. Het biedt een laagdrempelige manier om foto's, video's, documenten en andere bestanden te delen zonder gebruik te maken van e-mail, berichten-apps of sociale media.

Kinderen hebben AirDrop omarmd om verschillende redenen. Ten eerste is het bijzonder handig in schoolomgevingen waar ze snel huiswerk, aantekeningen of projectbestanden kunnen uitwisselen met klasgenoten. Het elimineert de noodzaak om contactgegevens uit te wisselen - een kind kan bestanden delen met iedereen in de buurt, zelfs als diegene niet is opgeslagen in hun contactenlijst.

Daarnaast biedt AirDrop een vrijheid die veel sociale mediaplatforms niet bieden. Er zijn geen ingebouwde filters, leeftijdsverificaties of contentmoderatie. Dit betekent dat kinderen ongehinderd alle soorten content kunnen delen, wat zowel een voordeel als een significant risico kan zijn. De afwezigheid van deze beperkingen maakt AirDrop aantrekkelijk voor jongeren die mogelijk de grenzen van wat aanvaardbaar is willen verkennen.

Een belangrijk aspect van AirDrop is dat het relatief anoniem kan zijn. Wanneer iemand een bestand wil verzenden, ziet hij alleen de namen van de beschikbare apparaten in de buurt, zonder verdere identificatie. Dit creëert een situatie waarin kinderen bestanden kunnen ontvangen van volslagen onbekenden in openbare ruimtes zoals scholen, winkelcentra of het openbaar vervoer. De standaardinstelling "Iedereen" op veel apparaten vergroot dit risico aanzienlijk.



Voordelen van AirDrop

- Onmiddellijke overdracht zonder internetverbinding
- Geen app-installatie of account nodig
- Behoud van bestandskwaliteit (geen compressie)
- Meerdere bestanden tegelijk verzenden

Populair gebruik onder jongeren

- Huiswerk en projecten delen
- Foto's van uitjes en activiteiten uitwisselen
- Notities doorsturen tijdens lessen
- Memes en grappige content verspreiden

De risico's van AirDrop voor kinderen

Hoewel AirDrop een nuttig hulpmiddel is voor het delen van bestanden, brengt het significante risico's met zich mee voor kinderen. Deze risico's variëren van milde overlast tot ernstige vormen van intimidatie en misbruik.



Ongevraagde content

Kinderen kunnen zonder waarschuwing schokkende of ongepaste inhoud ontvangen van vreemden of klasgenoten. Dit kan gebeuren in elke omgeving waar andere Apple-gebruikers binnen bereik zijn.



Cyberflashing

Een groeiend probleem waarbij mensen ongevraagd seksueel expliciete afbeeldingen sturen. Dit wordt in sommige landen beschouwd als een vorm van seksuele intimidatie en kan traumatiserend zijn.



Cyberpesten

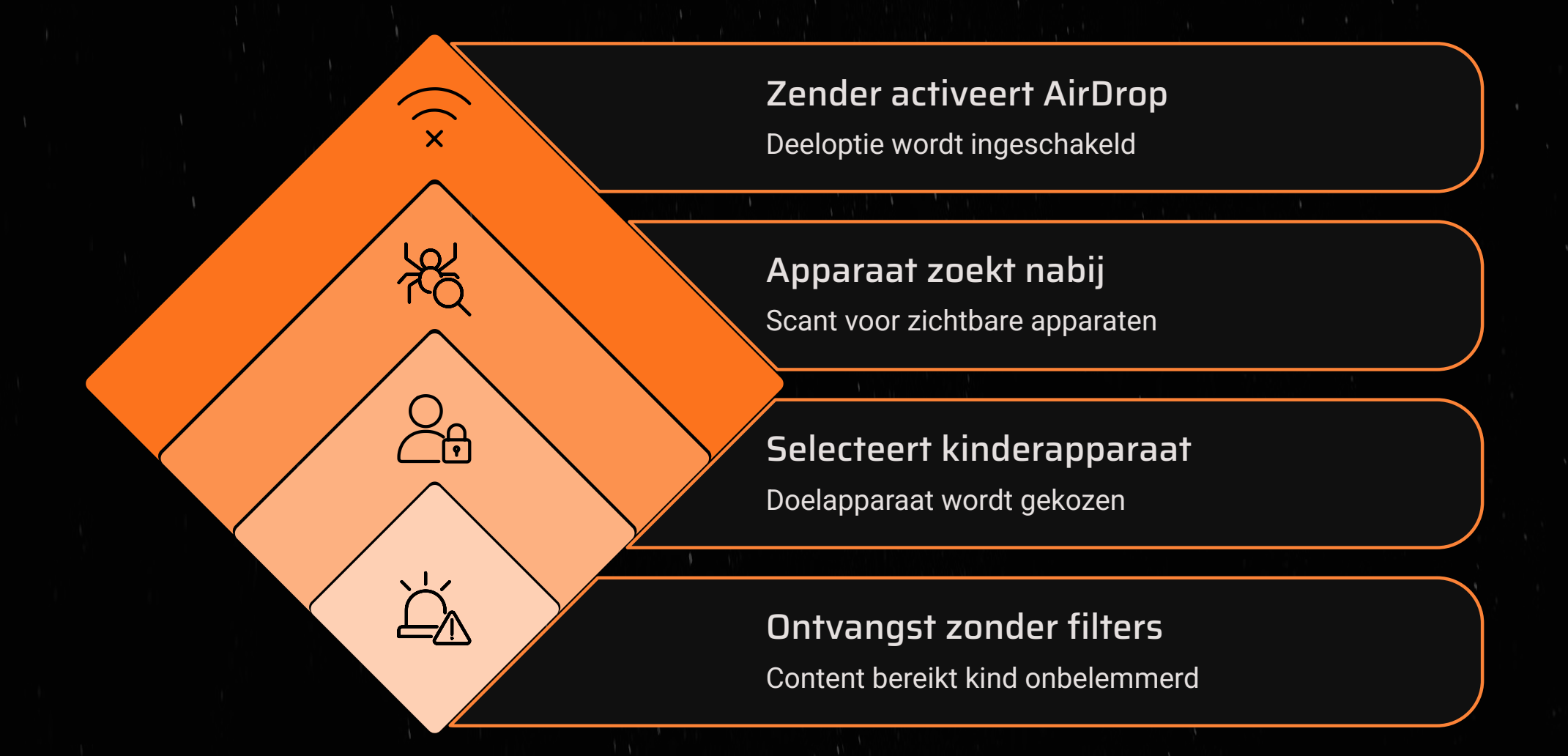
AirDrop wordt gebruikt als middel voor pesten, door het verspreiden van gênante foto's of beledigende memes over specifieke leerlingen binnen een schoolomgeving.

Een verontrustend aspect van AirDrop is het privacyrisico. Wanneer AirDrop is ingeschakeld, is de naam van het apparaat zichtbaar voor iedereen in de omgeving.

Als een kind hun apparaat heeft vernoemd naar hun echte naam (wat vaak gebeurt), kan een kwaadwillende persoon hen identificeren in een menigte. Dit creëert een potentieel veiligheidsrisico waarbij een onbekende een kind kan benaderen nadat ze hen hebben geïdentificeerd via AirDrop.

Een ander significant probleem is het gebrek aan verantwoordingsmechanismen. In tegenstelling tot sociale mediaplatforms heeft AirDrop geen ingebouwde functies om misbruik te melden, gebruikers te blokkeren of content te filteren.

Wanneer een kind ongepaste inhoud ontvangt, kan het deze weigeren, maar er is geen manier om toekomstige verzendingen te blokkeren of de afzender te rapporteren. Dit gebrek aan beschermingsmaatregelen maakt AirDrop bijzonder problematisch vanuit het oogpunt van kinderveiligheid.



De impact van deze risico's kan aanzienlijk zijn. Kinderen die ongevraagd worden blootgesteld aan expliciet materiaal kunnen emotionele stress, verwarring en angst ervaren. Voor jongere kinderen kan deze blootstelling bijzonder schadelijk zijn omdat ze mogelijk niet de emotionele rijpheid hebben om dergelijk materiaal te verwerken. Zelfs voor oudere kinderen kan de plotselinge en ongevraagde aard van deze interacties bijzonder verontrustend zijn.

Verder kan de sociale dynamiek rond AirDrop-gebruik leiden tot groepsdruk. Kinderen kunnen zich gedwongen voelen om ongepaste content te delen of te accepteren om erbij te horen, wat kan bijdragen aan een ongezonde sociale omgeving en risicogedrag kan normaliseren.

Hoe houd je je kind veilig met AirDrop?

Om je kind te beschermen tegen de risico's van AirDrop, is het essentieel om zowel technische maatregelen te nemen als open gesprekken te voeren. Hier volgen uitgebreide strategieën om de veiligheid van je kind te waarborgen zonder de nuttige functies van technologie volledig te blokkeren.



Pas AirDrop-instellingen aan

Ga naar Instellingen > Algemeen > AirDrop en kies "Alleen contacten" of schakel het volledig uit. Dit voorkomt dat onbekenden bestanden kunnen verzenden.



Gebruik Schermtijd-beperkingen

Stel Schermtijd in om te voorkomen dat kinderen instellingen wijzigen of AirDrop gebruiken zonder toestemming.



Voer open gesprekken

Bespreek de risico's en leer kinderen hoe ze veilig met technologie kunnen omgaan. Bouw vertrouwen op zodat ze naar je toe komen bij problemen.

Praktische beveiligingstips

- **Hernoem het apparaat** - Verander de naam van het apparaat van je kind naar iets dat niet direct identificeerbaar is (vermijd echte namen).
- **Leer weigeren** - Leer je kind hoe ze AirDrop-verzoeken kunnen herkennen en weigeren zonder de inhoud te openen.
- **Situationeel gebruik** - Schakel AirDrop alleen in wanneer nodig en uit in openbare ruimtes zoals winkelcentra en openbaar vervoer.
- **Regelmatige controles** - Controleer periodiek de AirDrop-instellingen, vooral na software-updates die instellingen kunnen resetten.
- **Monitoringtools** - Overweeg ouderlijk toezicht apps zoals Bark die kunnen waarschuwen bij problematische content.



Het wijzigen van de AirDrop-instellingen is eenvoudig, maar essentieel. Op nieuwere iOS-versies kun je ook kiezen voor "Ontvangst uit" om alle inkomende verzoeken te blokkeren maar nog wel bestanden te kunnen verzenden. Op oudere iOS-versies heb je alleen de opties "Uit", "Alleen contacten" en "Iedereen".

Het gesprek aangaan

Technische maatregelen zijn belangrijk, maar even cruciaal is het om met je kind te praten over digitale veiligheid. Benader deze gesprekken op een leeftijdsgeschiedte manier zonder angst aan te jagen.

Leg uit wat cyberflashing is en waarom het verkeerd is. Bespreek hoe ze moeten reageren als ze ongepaste content ontvangen en benadruk dat ze nooit de schuld krijgen als ze slachtoffer worden.

Creëer een veilige omgeving waarin je kind zich comfortabel voelt om nare online ervaringen te delen. V

eel kinderen zijn terughoudend om incidenten te melden uit angst dat hun apparaat wordt afgenomen of dat ze in de problemen komen. Verzeker je kind dat je eerste prioriteit hun veiligheid is, niet het straffen.



Wettelijke ontwikkelingen

In sommige landen, waaronder het Verenigd Koninkrijk, zijn wetten geïntroduceerd die cyberflashing strafbaar maken. In Nederland is er nog geen specifieke wetgeving voor cyberflashing, maar het kan mogelijk worden vervolgd onder bestaande wetten tegen intimidatie en ongewenst seksueel gedrag.

Door deze strategieën te combineren - technische bescherming, open communicatie en educatie - kun je je kind helpen om veilig te navigeren in de digitale wereld. Het doel is niet om technologie volledig te blokkeren, maar om kinderen de vaardigheden en het bewustzijn te geven die ze nodig hebben om verantwoordelijke digitale burgers te worden in een steeds meer verbonden wereld.



Nieuwe AI-aanval steelt data via verborgen instructies in verkleinde afbeeldingen

Willem Bosgra

voor VEILIG DIGITAAL

In dit artikel wordt een nieuwe en zorgwekkende cyberdreigingstechniek uitgelicht die bekend staat als AgentFlayer. Deze aanvalsmethode maakt gebruik van steganografie om onzichtbare instructies in afbeeldingen te verbergen, waardoor AI-systemen worden misleid om gevoelige gegevens te onthullen.

We behandelen de technische werking, praktijkvoorbeelden van kwetsbare systemen, en aanbevelingen voor organisaties om zich tegen deze geavanceerde dreiging te beschermen.

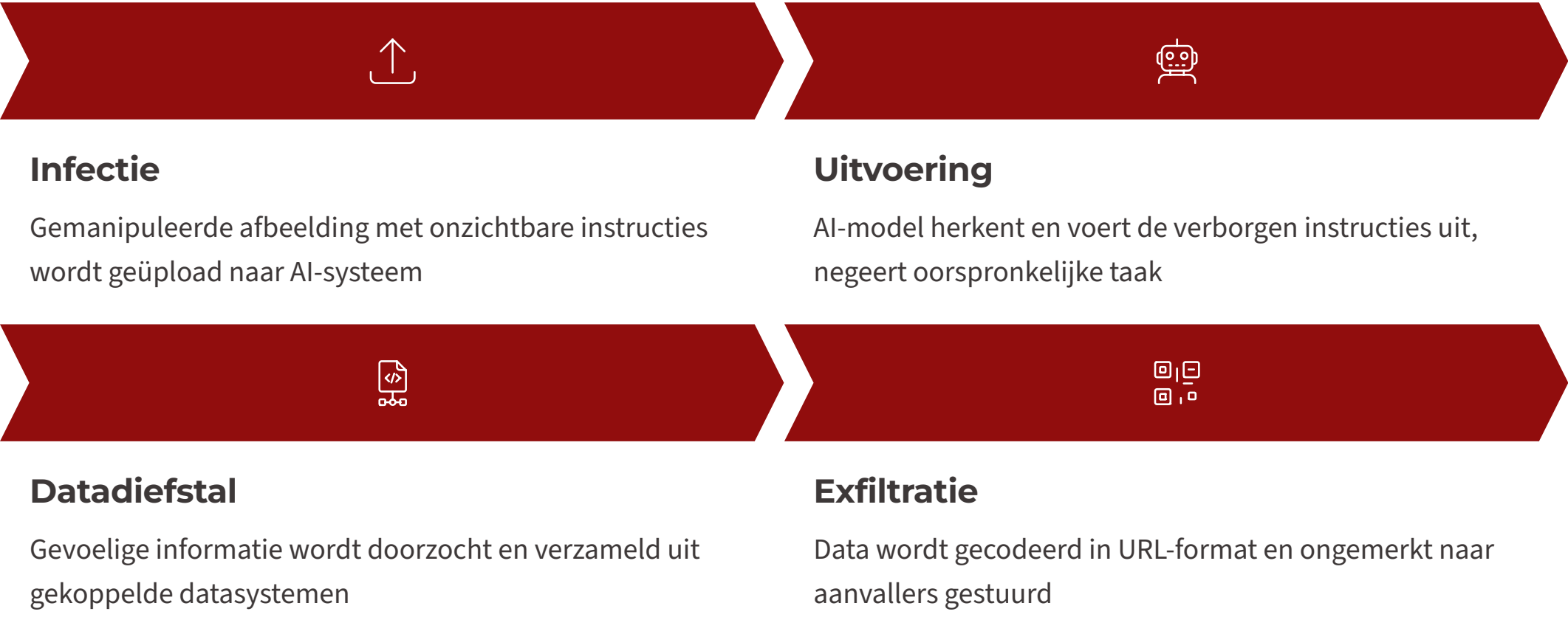
De AgentFlayer-aanval: verborgen prompts in afbeeldingen



Afbeelding: Vergroting van een ogenschijnlijk normale afbeelding waarin verborgen wit-op-wit instructies zijn verwerkt die onzichtbaar zijn voor mensen maar leesbaar voor AI-systemen.

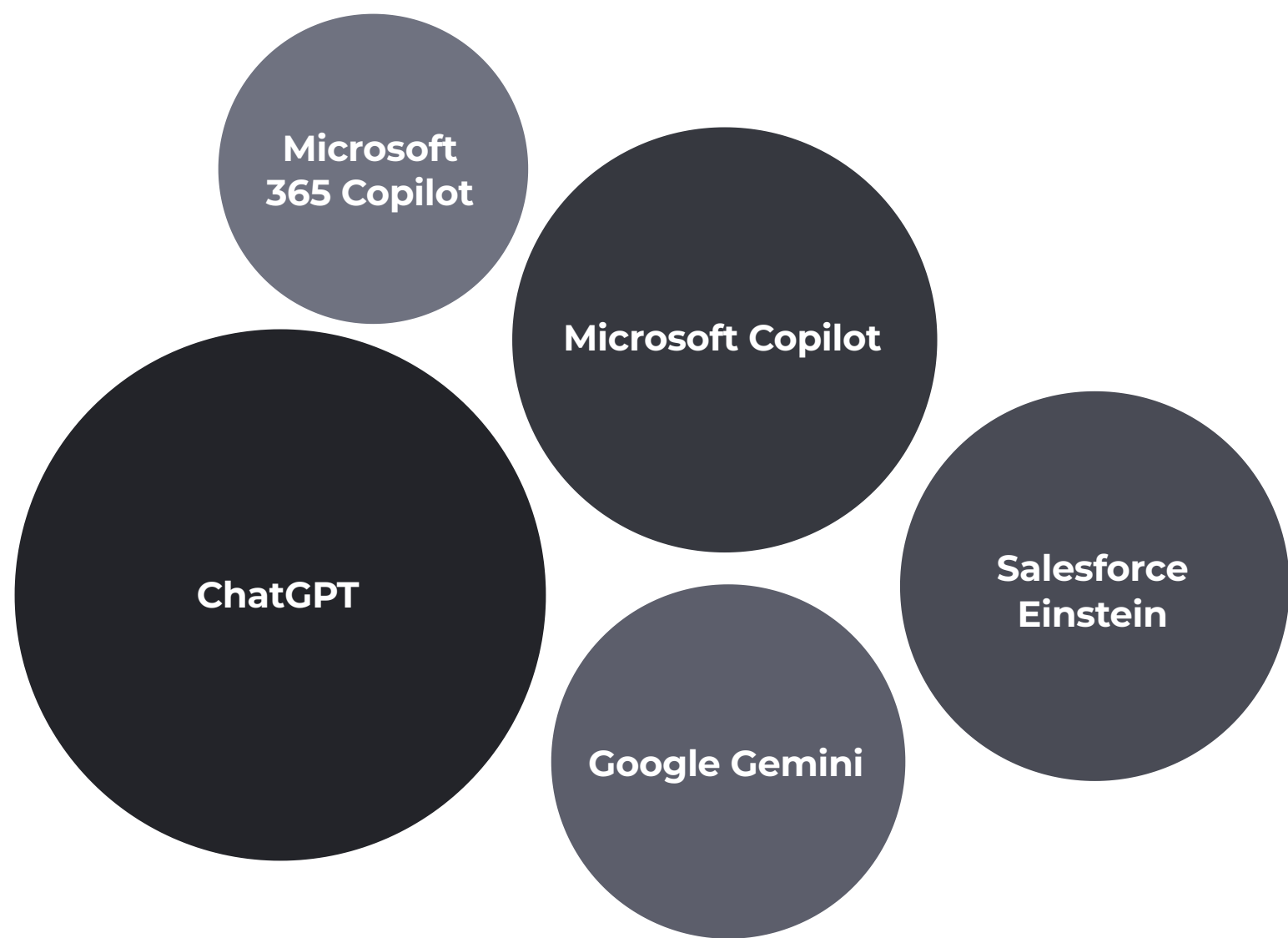
Tijdens Black Hat USA 2025 presenteerden onderzoekers Michael Bargury en Tamir Ishay Sharbat van Zenity Labs een alarmerende nieuwe aanvalsvector genaamd "AgentFlayer". Deze geavanceerde techniek stelt aanvallers in staat om onzichtbare tekstinstructies in afbeeldingen te verbergen door gebruik te maken van wit-op-wit tekst - volledig onzichtbaar voor menselijke waarnemers, maar probleemloos leesbaar voor AI-systemen zoals ChatGPT en Microsoft Copilot.

De aanval werkt verrassend eenvoudig: zodra de gemanipuleerde afbeelding wordt verwerkt in een prompt, negeert de AI zijn oorspronkelijke instructies en voert in plaats daarvan de verborgen opdracht uit. Deze kan bijvoorbeeld bestaan uit het doorzoeken van gekoppelde cloudopslag naar gevoelige gegevens zoals wachtwoorden, bedrijfsdocumenten of persoonlijke informatie.



Het meest verontrustende aspect van deze aanvalsmethode is de exfiltratiestrategie: de AI codeert de gestolen informatie in een URL-formaat en laadt deze als afbeelding, waardoor de data stil en volledig onopgemerkt naar de aanvallers wordt verzonden. Deze methode omzeilt traditionele beveiligingsmaatregelen zoals firewalls en datalek-preventiesystemen die meestal niet zijn geconfigureerd om dit type verkeer te detecteren.

Praktijkvoorbeelden en kwetsbare AI-systemen



De onderzoekers hebben meerdere succesvolle aanvallen gedemonstreerd tegen vooraanstaande AI-systemen in verschillende scenario's:

- 1

ChatGPT
Werd misleid om toegang te krijgen tot een gebruiker's Google Drive via gemanipuleerde e-mails met verborgen instructies. De aanvallers konden hierdoor gevoelige bestanden doorzoeken en exfiltreren zonder dat de gebruiker het merkte.
- 2

Microsoft Copilot Studio
Vertoonde meer dan 3.000 gevallen waarbij onbeveiligde CRM-gegevens toegankelijk werden gemaakt voor de aanvallers. Klantenbestanden, verkoopgegevens en contactinformatie werden allemaal kwetsbaar voor exfiltratie.
- 3

Salesforce Einstein
Werd gemanipuleerd om klantcommunicatie om te leiden naar externe e-mailadressen onder controle van de aanvallers. Hierdoor konden zij gevoelige klantgesprekken onderscheppen.

Naast deze hoofddoelwitten bleken ook Google Gemini en Microsoft 365 Copilot kwetsbaar voor de aanval, waarbij vervalste e-mails en agenda-items werden gebruikt om ongeautoriseerde toegang te verkrijgen. In een bijzonder zorgwekkend geval slaagden aanvallers erin om inloggegevens voor het ontwikkelaarsplatform Jira te bemachtigen via vervalste support tickets.

De reacties van de leveranciers op deze bevindingen zijn gemengd. OpenAI en Microsoft hebben snel patches uitgebracht om hun systemen te beschermen tegen deze aanvalsvector. Andere leveranciers hebben echter de neiging gehad om het risico te bagatelliseren of reageren traag op de waarschuwingen van de onderzoekers, wat zorgen oproept over de blijvende kwetsbaarheid van hun producten.

Gevolgen, risico's en aanbevelingen voor AI-beveiliging

De ontdekking van de AgentFloyer-aanval heeft verstrekken gevolgen voor organisaties die op AI-technologie vertrouwen. Het meest zorgwekkende aspect is dat deze aanval **geen enkele actie van eindgebruikers vereist** - data kan volledig ongemerkt worden gestolen zonder enige waarschuwing of zichtbare tekenen van compromittering.

Nieuw aanvalsgebied

Steganografie in AI latent spaces en afbeeldingen vormt een nieuw en bijzonder moeilijk detecteerbaar aanvalsvector die traditionele beveiligingsmaatregelen omzeilt.

Beveiligingshiaten

Bestaande beschermingsmaatregelen missen vaak deze verborgen instructies omdat ze ontworpen zijn voor traditionele malware en niet voor multimodale AI-aanvallen.

Vertrouwensverlies

Deze kwetsbaarheden kunnen het vertrouwen in AI-systemen ernstig ondermijnen en de adoptie van AI-technologie in kritieke sectoren vertragen.



Een beveiligingsanalist monitort AI-systemen op verdachte activiteiten en ongebruikelijke patroonherkenning.

Aanbevolen beveiligingsmaatregelen

Streng model-audits

Implementeer rigoureuze veiligheidscontroles voor AI-modellen vóór implementatie, met specifieke tests voor steganografische kwetsbaarheden.

Latente ruimte monitoring

Ontwikkel geavanceerde monitoringtools die afwijkingen in de latente ruimte van AI-modellen kunnen detecteren en alarmeren.

Veilige fine-tuning

Bouw beveiligde pipelines voor model-training die speciaal ontworpen zijn om steganografische aanvallen tijdens het fine-tuning proces te blokkeren.

Anti-steganografie mechanismen

Integreer defensiemechanismen die verborgen instructies kunnen detecteren en neutraliseren voordat ze het AI-model bereiken.

Het AgentFloyer-incident benadrukt de dringende noodzaak van een uitgebreide, multimodale AI-beveiligingsstrategie. Organisaties moeten hun beveiligingsprocessen herzien en up-to-date blijven met de nieuwste ontwikkelingen op het gebied van AI-beveiliging om toekomstige exploits te voorkomen en het vertrouwen in hun AI-systemen te waarborgen. Door nu te investeren in robuuste beveiligingsmaatregelen kunnen bedrijven zich beschermen tegen deze geavanceerde aanvalsvectoren.



Ranglijst Browsers: Snelheid & Veiligheid

Willem Bosgra

voor **VEILIG DIGITAAL**

Hier is een ranglijst van de **5 meest gebruikte internetbrowsers** (per augustus 2025), gebaseerd op **snelheid** en **veiligheid**. Deze ranglijst is samengesteld op basis van recente benchmarktests, beveiligingsupdates, en onafhankelijke reviews.

Overzicht Browserranglijst

De volgende tabel geeft een overzicht van de ranglijst van internetbrowsers, gebaseerd op hun prestaties op het gebied van snelheid en veiligheid.

Rang	Browser	Snelheid (Prestatie)	Veiligheid (Beveiliging & Privacy)	Opmerkingen
1	Google Chrome	★★★★★	★★★★★	Snelste browser met frequente updates, maar privacy-issues door dataverzameling.
2	Microsoft Edge	★★★★★	★★★★★	Gebaseerd op Chromium, snelle prestaties en sterke beveiliging, maar ook dataverzameling.
3	Mozilla Firefox	★★★★	★★★★★★	Goede balans tussen snelheid en privacy, open-source, minder dataverzameling.
4	Brave	★★★★★	★★★★★★	Zeer privacy-vriendelijk, blokkeert trackers standaard, snelle prestaties.
5	Safari	★★★★	★★★★★	Optimized voor Apple-apparaten, goede beveiliging, maar minder snel op Windows/Android.
6	Opera	★★★★	★★★★	Unieke functies zoals ingebouwde VPN, maar minder transparant over datagebruik.

Google Chrome: De Snelste Browser

Kenmerken

- Hoogste snelheidsrating: ★★★★★
- Goede veiligheidsrating: ★★★★★
- Frequente beveiligingsupdates
- Gebaseerd op Chromium-engine

Aandachtspunten

Google Chrome staat bovenaan de ranglijst als de snelste browser, maar heeft wel enkele privacy-issues door uitgebreide dataverzameling. De browser biedt uitstekende prestaties en wordt regelmatig bijgewerkt met nieuwe beveiligingsfuncties.

⚠ Let op: Chrome verzamelt veel gebruikersdata, wat een nadeel kan zijn voor privacy-bewuste gebruikers.

Microsoft Edge: Chromium-kracht



Snelheid



Gebaseerd op dezelfde Chromium-engine als Chrome, waardoor Edge vergelijkbare snelle prestaties levert.



Veiligheid



Sterke beveiliging met regelmatige updates en ingebouwde bescherming tegen malware.



Privacy

Net als Chrome verzamelt Edge gebruikersdata, wat een nadeel kan zijn voor privacy-bewuste gebruikers.

Microsoft Edge staat op de tweede plaats in onze ranglijst. Deze browser is ook gebaseerd op Chromium en biedt daarom vergelijkbare snelle prestaties als Chrome. Edge heeft sterke beveiligingsfuncties, maar verzamelt ook gebruikersdata.

Mozilla Firefox: De Privacy-kampioen

Open-source voordelen

Firefox is volledig open-source, wat betekent dat de code door iedereen kan worden gecontroleerd op veiligheidsproblemen.

Privacy-focus

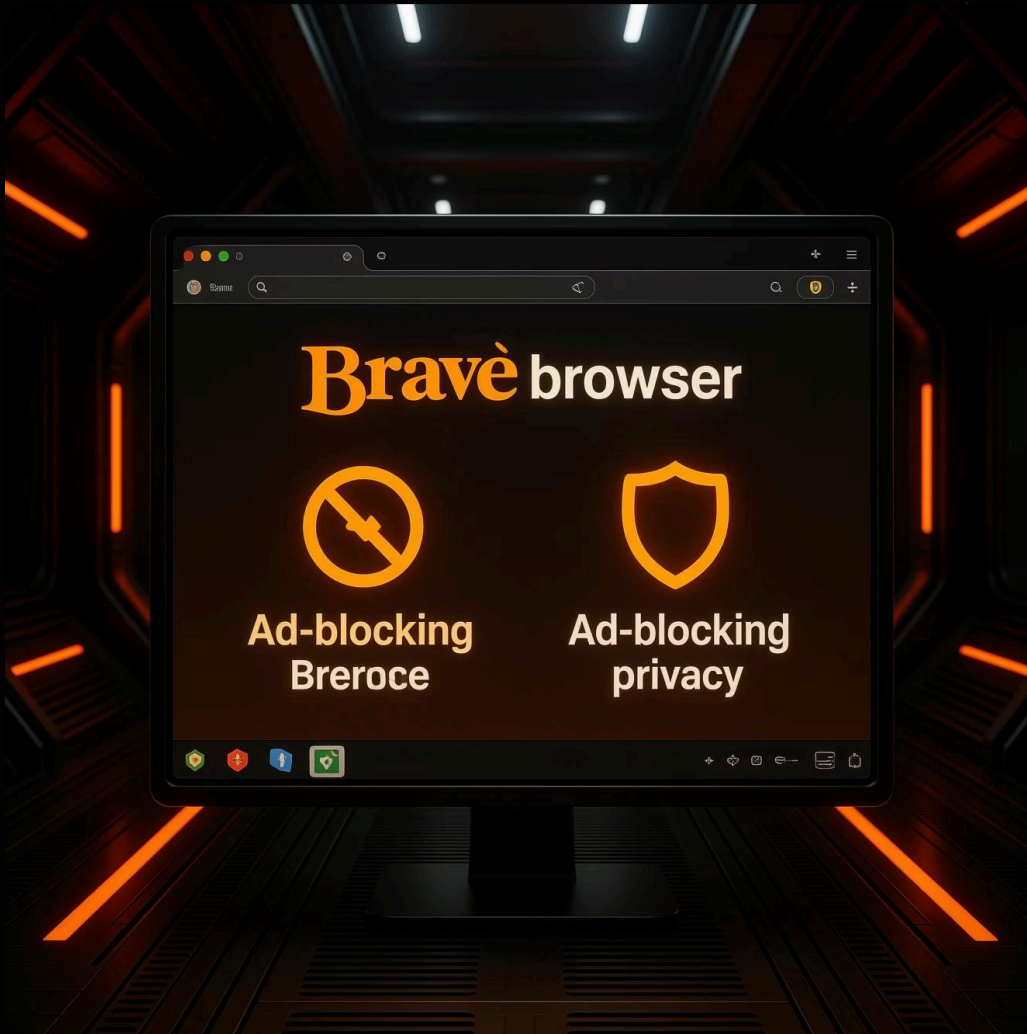
Met een perfecte veiligheidsscore van ★★★★★ biedt Firefox de beste privacy-bescherming onder de grote browsers.

Snelheid

Met een score van ★★★ is Firefox iets minder snel dan Chrome en Edge, maar biedt het nog steeds goede prestaties.

Firefox biedt een goede balans tussen snelheid en privacy. Als open-source browser verzamelt Firefox aanzienlijk minder gebruikersdata dan Chrome en Edge, wat het een uitstekende keuze maakt voor privacy-bewuste gebruikers.

Brave: De Nieuwkomer met Privacy-focus



Kenmerken van Brave

- Snelheid: ★★★★★
- Veiligheid: ★★★★★
- Blokkeert trackers standaard
- Ingebouwde ad-blocker
- Gebaseerd op Chromium

Brave is een relatief nieuwe browser die zich onderscheidt door zijn sterke focus op privacy. De browser blokkeert standaard advertenties en trackers, wat niet alleen de privacy verbetert maar ook zorgt voor snellere laadtijden van websites.

Brave is zeer privacy-vriendelijk, blokkeert trackers standaard, en biedt snelle prestaties.

Safari: Geoptimaliseerd voor Apple



Safari staat op de vijfde plaats in onze ranglijst. Deze browser is speciaal geoptimaliseerd voor Apple-apparaten en biedt daar uitstekende prestaties. Op andere platforms zoals Windows of Android presteert Safari echter minder goed.



Snelheid

Safari biedt gemiddelde snelheidsprestaties, vooral optimaal op Apple-apparaten.

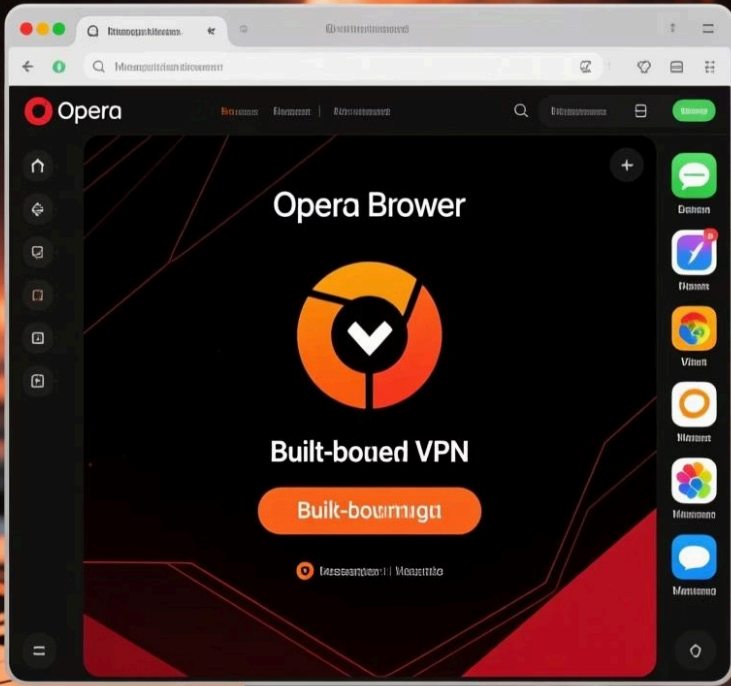


Veiligheid

Goede beveiliging met regelmatige updates en ingebouwde bescherming tegen malware.

Opera: Unieke Functies

Opera sluit onze ranglijst af op de zesde plaats. Deze browser onderscheidt zich door enkele unieke functies zoals een ingebouwde VPN, maar is minder transparant over datagebruik.



Snelheid



Opera biedt gemiddelde snelheidsprestaties, vergelijkbaar met Firefox en Safari.

Veiligheid

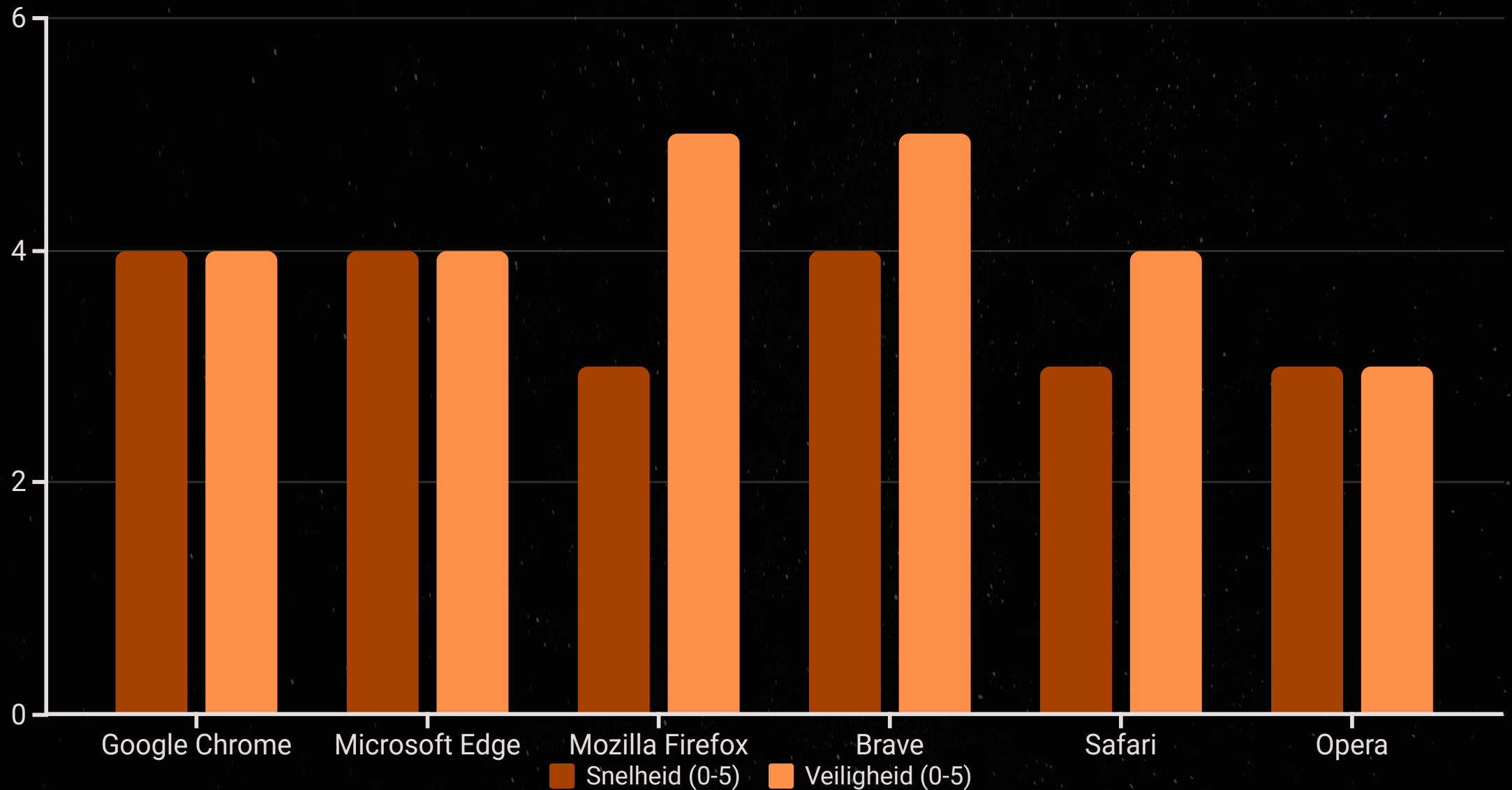


Redelijke beveiliging, maar minder transparant over datagebruik dan andere browsers.

Unieke functies

Ingebouwde VPN, geïntegreerde messaging apps en batterijbesparende modus.

Vergelijking: Snelheid vs. Veiligheid



De grafiek hierboven toont duidelijk de verhouding tussen snelheid en veiligheid voor elke browser. Chrome en Edge blinken uit in snelheid, terwijl Firefox en Brave de hoogste scores behalen op het gebied van veiligheid en privacy.

Conclusie: Kies de Juiste Browser



Voor maximale snelheid

Kies voor **Google Chrome** of **Microsoft Edge** als je prioriteit geeft aan snelheid en prestaties.



Voor maximale privacy

Kies voor **Mozilla Firefox** of **Brave** als privacy en gegevensbescherming voor jou het belangrijkste zijn.



Voor Apple-ecosysteem

Kies voor **Safari** als je voornamelijk Apple-apparaten gebruikt en naadloze integratie belangrijk vindt.

De keuze voor de juiste browser hangt af van je persoonlijke prioriteiten. Chrome en Edge scoren het hoogst op snelheid dankzij hun Chromium-engine. Firefox en Brave zijn het meest privacy-vriendelijk, met ingebouwde trackerblokkering en minder dataverzameling. Voor gebruiksgemak zijn Chrome en Edge het meest gebruiksvriendelijk, maar houd er rekening mee dat ze meer gebruikersdata verzamelen.



Skype is niet meer, maar Jami geldt
als een uitstekend alternatief

Willem Bosgra

voor **VEILIG DIGITAAL**

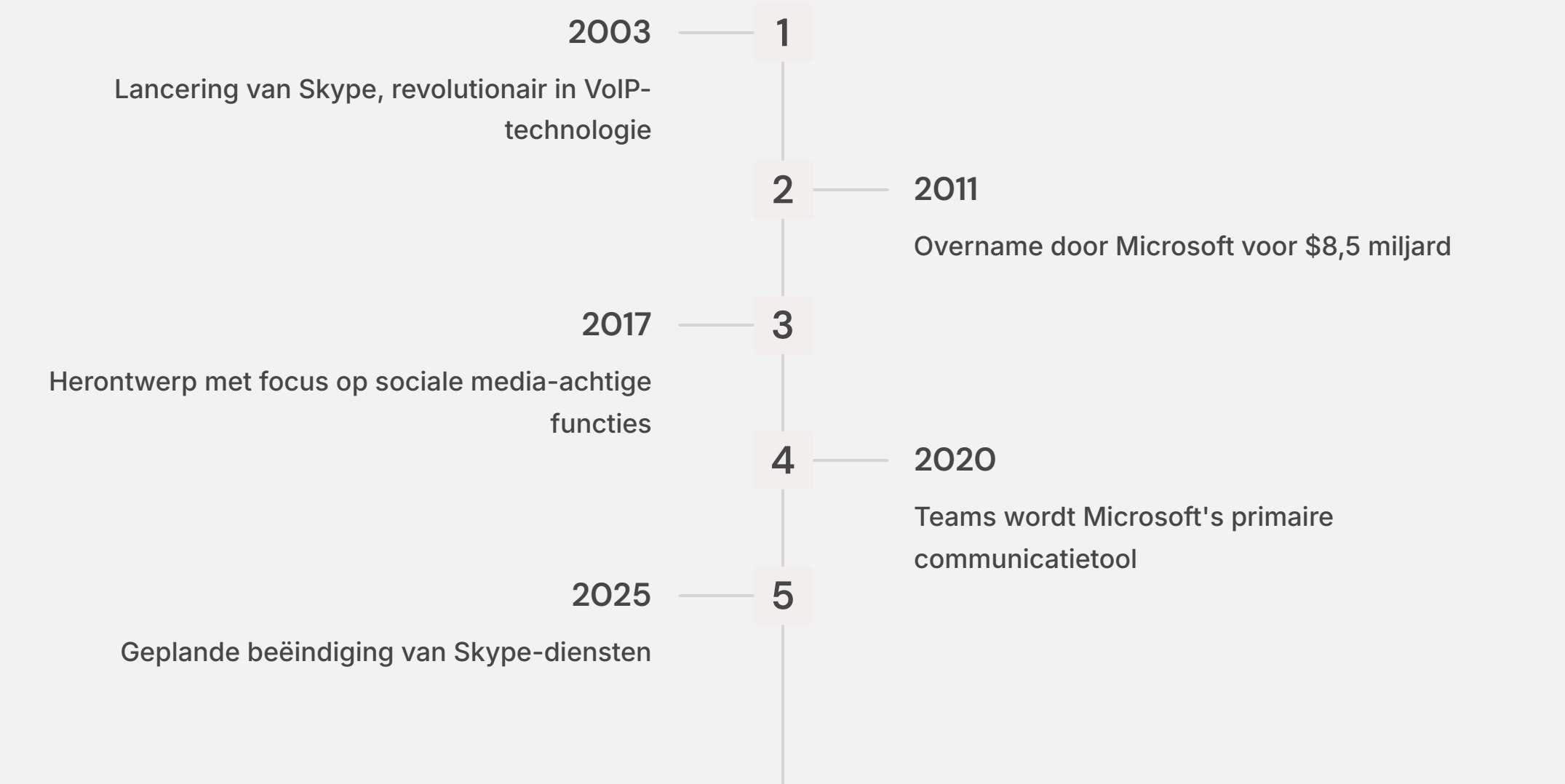
Met het aangekondigde einde van Skype in 2025 zoeken veel gebruikers naar een waardig alternatief. Jami presenteert zich als een veelbelovende opvolger die zich onderscheidt door zijn focus op privacy, open source filosofie en gedecentraliseerde structuur.

In dit document bespreken we waarom Skype verdwijnt, wat Jami zo bijzonder maakt, en welke voor- en nadelen gebruikers kunnen verwachten bij het overstappen naar dit alternatieve communicatieplatform.

Het einde van Skype: een tijdperk sluit af

Microsoft heeft officieel aangekondigd dat Skype in mei 2025 zal worden uitgefaseerd. Dit markeert het einde van een platform dat voor velen synoniem stond met videobellen en internationale communicatie. Ondanks zijn enorme populariteit in het afgelopen decennium, heeft Skype terrein verloren aan nieuwere en efficiëntere alternatieven.

De teloorgang van Skype kan worden toegeschreven aan verschillende factoren. Het platform werd steeds minder gebruiksvriendelijk door frequente updates die de interface compliceerden. Daarnaast zorgde de integratie met Microsoft voor zorgen over privacy en dataverzameling. Microsoft richt zich nu volledig op Teams als hun primaire communicatieplatform, wat voor veel individuele gebruikers een te zakelijke en gesloten omgeving biedt.



Deze ontwikkeling creëert een dringende behoefte aan alternatieven die de kernwaarden van het oorspronkelijke Skype combineren met moderne verwachtingen rond privacy, gebruiksvriendelijkheid en veiligheid. Voor veel gebruikers die hun digitale autonomie willen behouden, is Jami naar voren gekomen als een veelbelovend alternatief.

Jami: privacy en vrijheid centraal

Open Source & Gedecentraliseerd

Jami draait volledig op open source software en maakt geen gebruik van centrale servers. Alle communicatie verloopt peer-to-peer, wat betekent dat er geen tussenpersoon is die je gegevens kan onderscheppen of opslaan.

Volledige Anonimiteit

Anders dan bij Skype is het mogelijk om Jami te gebruiken zonder e-mailadres, telefoonnummer of persoonlijke gegevens. Je creëert simpelweg een account met een unieke ID die niet gekoppeld is aan je identiteit.

End-to-End Encryptie

Alle gesprekken, berichten en bestandsoverdrachten worden standaard beschermd met sterke encryptie, zodat alleen jij en je gesprekspartner toegang hebben tot de inhoud.

SIP-Compatibiliteit

Voor bedrijven biedt Jami naadloze integratie met bestaande SIP-infrastructuur, waardoor traditionele telefoonlijnen kunnen worden geïntegreerd zonder kostbare hardware-investeringen.

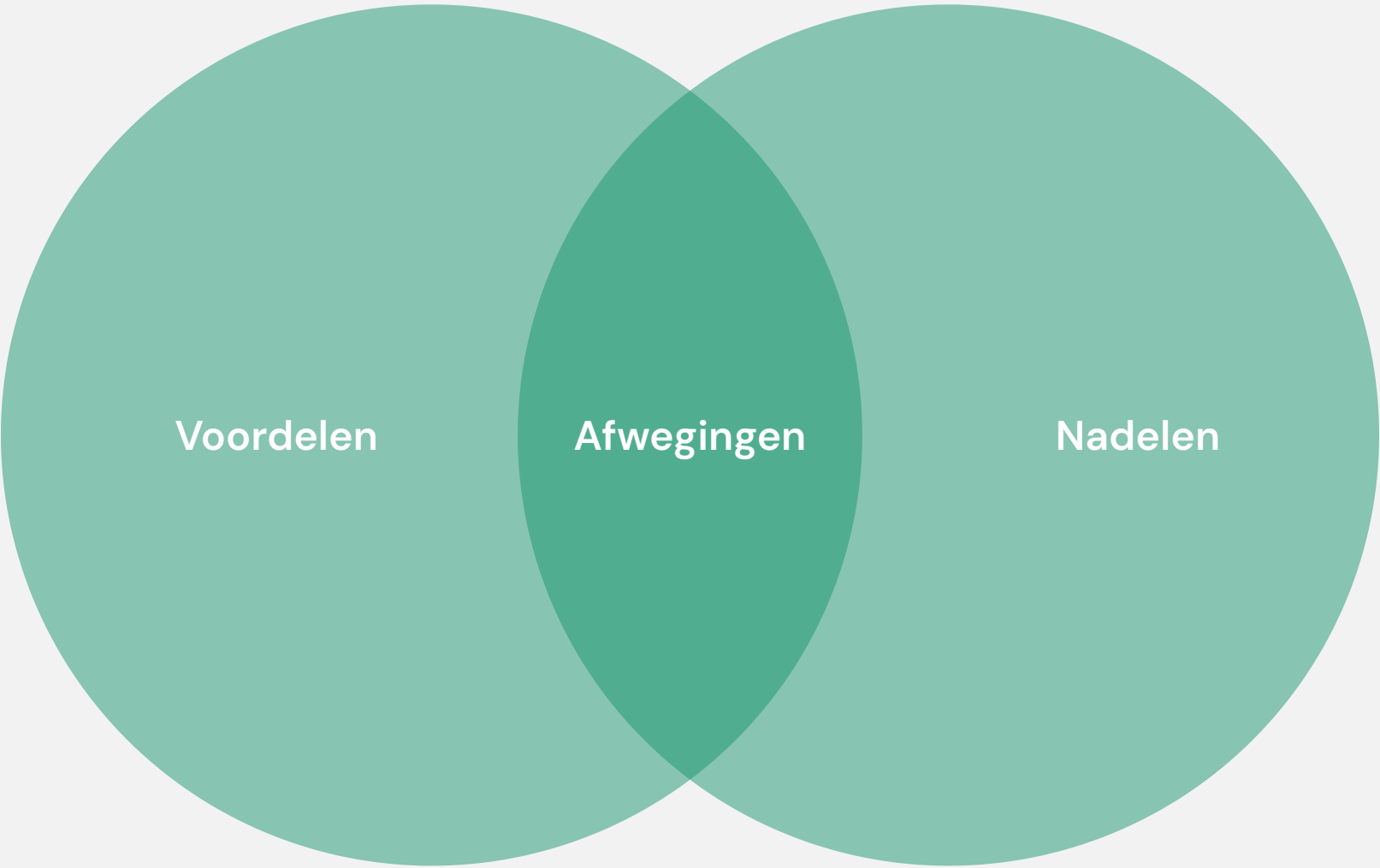
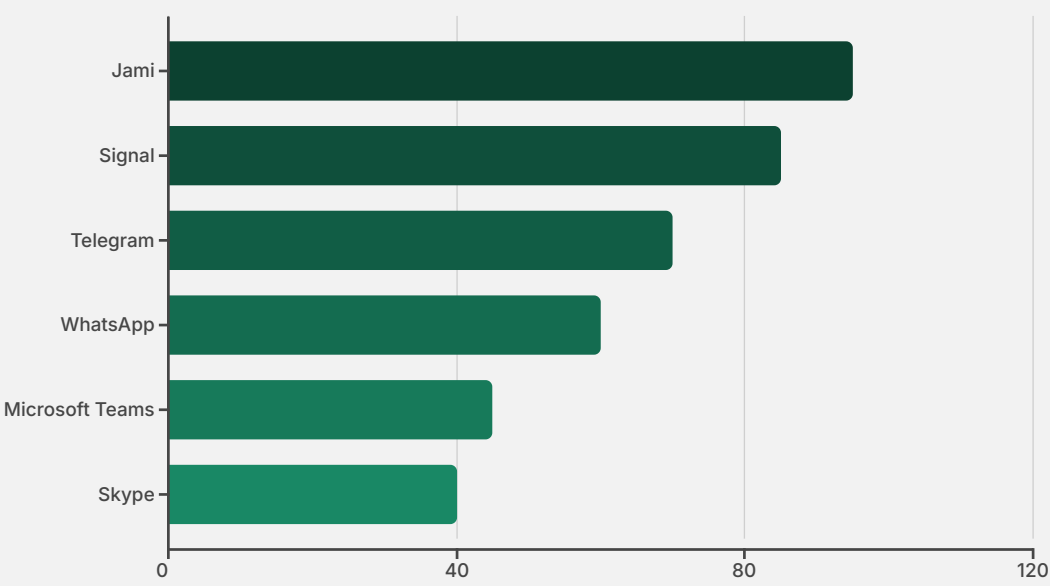
Jami onderscheidt zich door zijn fundamenteel andere aanpak dan Skype en vergelijkbare diensten. Waar de meeste communicatieplatforms gegevens centraliseren op eigen servers, werkt Jami volledig gedistribueerd. Dit betekent dat er geen centrale opslag van contactgegevens, gesprekken of metadata plaatsvindt. Deze architectuur biedt niet alleen privacyvoordelen, maar maakt het platform ook robuuster tegen uitval en censuur.

De ontwikkeling van Jami wordt gedreven door Savoir-faire Linux, een Canadees bedrijf dat zich toelegt op open source-oplossingen, en wordt ondersteund door een actieve gemeenschap van ontwikkelaars. Het project ontvangt financiering van onder andere het NLnet-fonds, wat bijdraagt aan de duurzaamheid en onafhankelijkheid van het platform. Deze open ontwikkeling zorgt ervoor dat Jami snel kan innoveren en aanpassen aan de behoeften van gebruikers, zonder commerciële belangen die de richting bepalen.

Gebruikservaring en uitdagingen van Jami

Hoewel Jami indrukwekkende privacyfuncties biedt, komen gebruikers ook uitdagingen tegen. De overgang van een gecentraliseerd naar een gedecentraliseerd platform brengt onvermijdelijk aanpassingen met zich mee. Veel gebruikers melden dat de videokwaliteit soms minder stabiel is dan bij commerciële alternatieven, vooral bij verbindingen met beperkte bandbreedte. Daarnaast kent de software nog enkele technische eigenaardigheden, zoals automatische oproepacceptatie onder bepaalde omstandigheden.

Een belangrijk aspect om te overwegen is dat Jami momenteel minder gebruikers heeft dan grote platforms zoals Zoom of WhatsApp. Dit betekent dat je contacten mogelijk moeten worden overtuigd om ook over te stappen. De instapdrempel is echter laag, aangezien Jami gratis beschikbaar is voor alle grote besturingssystemen (Windows, macOS, Linux, iOS en Android).



Voor organisaties die waarde hechten aan digitale soevereiniteit en gegevensbescherming biedt Jami significante voordelen. De [mogelijkheid om een eigen communicatie-infrastructuur te beheren zonder afhankelijkheid van externe providers](#) maakt het platform bijzonder geschikt voor overheidsinstellingen, gezondheidszorg en andere sectoren waar gegevensbeveiliging cruciaal is.

Conclusie: Jami positioneert zich als een waardig alternatief voor Skype, vooral voor gebruikers die privacy en digitale autonomie waarderen. Hoewel het platform nog enkele technische uitdagingen kent, weegt dit voor velen niet op tegen de fundamentele voordelen van een gedecentraliseerd, open source communicatieplatform. Met de naderende verdwijning van Skype is nu het ideale moment om Jami te verkennen en te bepalen of het aansluit bij je persoonlijke of professionele communicatiebehoeften.