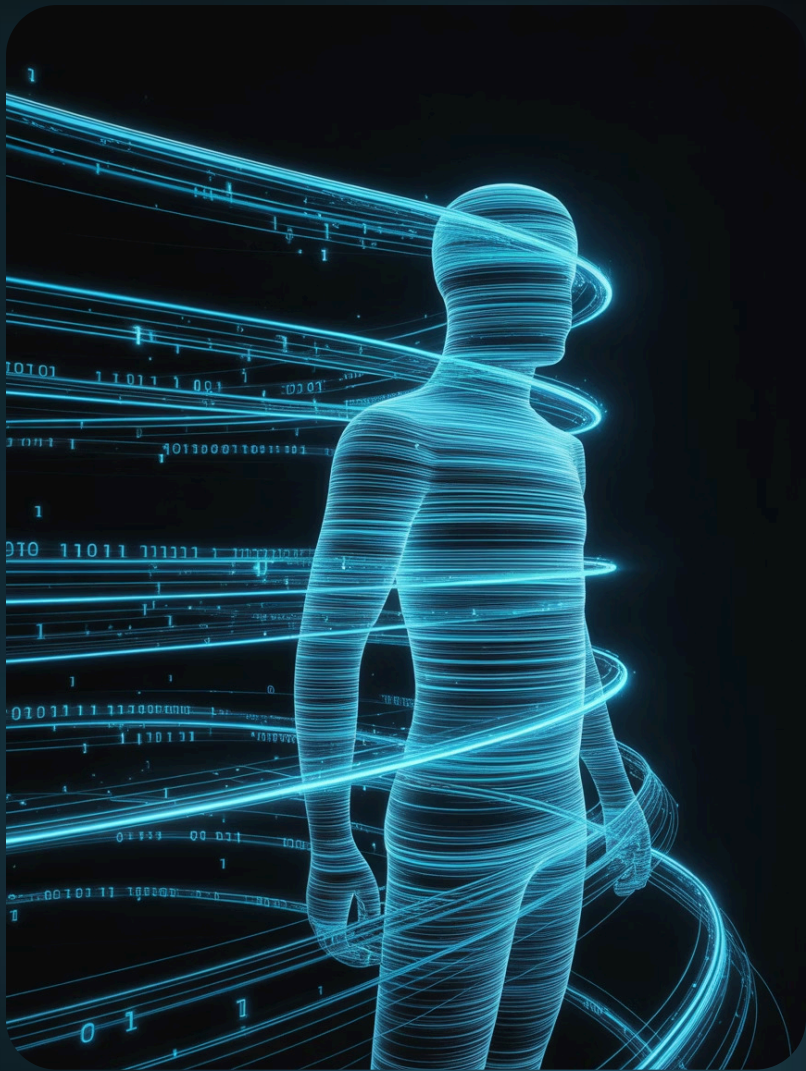


VEILIG DIGITAAL MAGAZINE





Welke Sporen Laten We Achter Op Internet?

Is het mogelijk om in alle rust op het web te surfen? Kan iemand discreet zien wat we doen en zo ja, wat kunnen de gevolgen daarvan zijn?

Privébedrijven, "data brokers", hebben toegang tot aanzienlijke volumes data. Ze kunnen een zeer precies profiel opstellen van de meeste internetgebruikers.

VEILIGDIGITAAL.COM



De Prijs Van Gratis Diensten



Persoonlijke gegevens

Data brokers verzamelen en verkopen onze gegevens zonder veel overheidscontrole.



Wereldwijde risico's

Politieke veranderingen kunnen leiden tot onverwachte problemen met verzamelde data.



Veiligheidsrisico's

Verzamelde gegevens kunnen gebruikt worden voor phishing of bedrijfsspionage.

De Misvatting Rond Het IP-adres

Wat is een IP-adres?

Een IP-adres is een reeks cijfers die computers nodig hebben om te communiceren. Bijvoorbeeld:
178.144.72.179.

Het is niet de "identiteitskaart" van je computer, zoals vaak wordt beweerd.

Privé vs. Publiek

Je toestel heeft een privé-IP-adres (bijv. 192.168.1.x). Websites zien echter het publieke IP-adres van je modem of netwerk.

Dit publieke adres wordt vaak gedeeld door meerdere gebruikers.



Wat Vertelt Je IP-adres?

Dynamisch

Je IP-adres kan regelmatig veranderen, vooral bij mobiele verbindingen of hotspots.

Gedeeld

Alle toestellen in een gezin of alle klanten in een café delen hetzelfde publieke IP-adres.

Beperkte informatie

Een website kan alleen je operator en een ruwe locatieschatting zien, vaak met een foutmarge van 100 km.

IP-adres Als Nummerplaat



Dynamische nummerplaat

Verandert regelmatig van eigenaar



Gedeeld vervoer

Soms een gezinswagen, soms een bus



Beperkte identificatie

Vertelt niet wie er achter het stuur zit

Een IP-adres geeft weinig persoonlijke informatie prijs. Alleen je internetprovider kan je identificeren, en dat alleen met een gerechtelijk bevel.

Network



IP-adres Van Bestemming



Grote diensten

Vaste, niet-gedeelde IP-adressen



Kleine websites

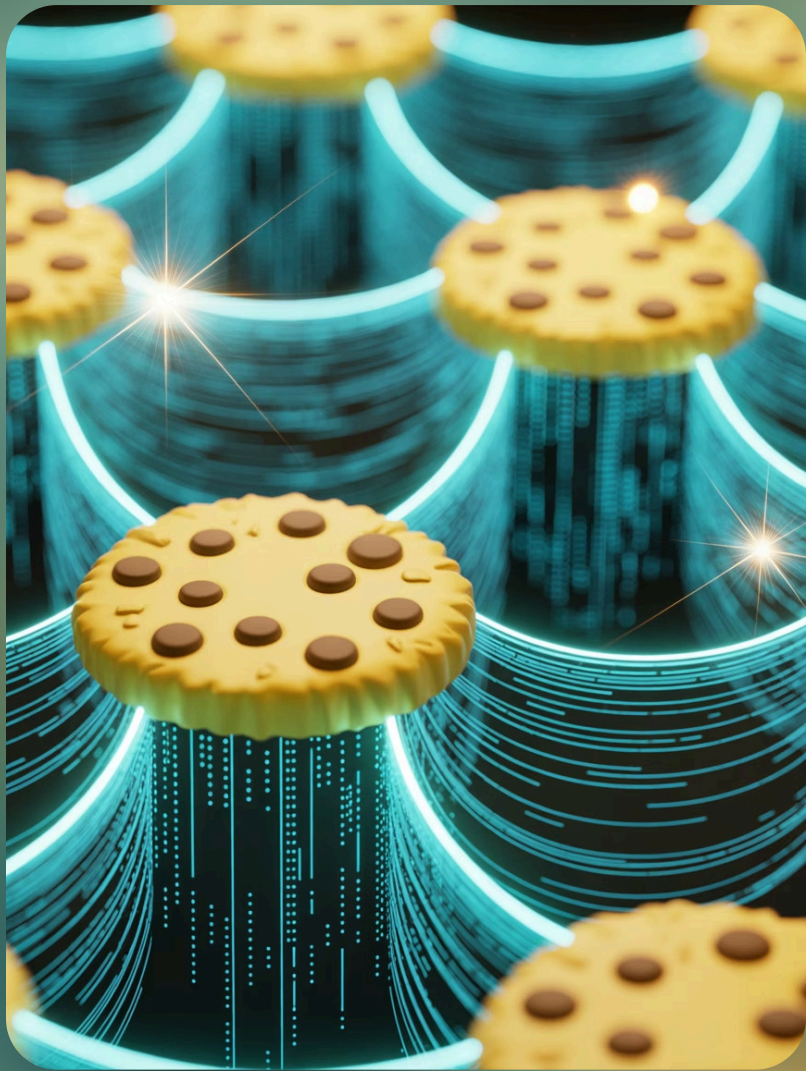
Gedeelde IP-adressen van hostingproviders



HTTPS-verbinding

Versleutelt de exacte bestemming

Bij grote diensten (Google, Facebook) kan het bestemmings-IP-adres de website onthullen. Bij kleinere sites is dit vaak onmogelijk door gedeelde hosting.



Cookies: Wat Zijn Het?



Klein bestand
Door website op je
computer
geplaatst tijdens
bezoek



Nuttig
mechanisme
Bewaart
instellingen zoals
taal of
winkelmandje



Geen spyware
Geen virus of
programma dat
informatie
verzamelt

Hoe Cookies Je Volgen



Third-Party Cookies

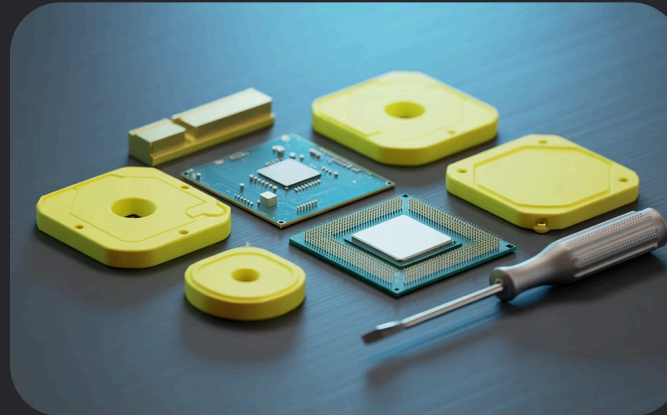


Canvas Fingerprinting



Onzichtbare afbeelding

Een complexe afbeelding wordt onzichtbaar gegenereerd om je computer te identificeren.



Hardware verschillen

Grafische kaart, drivers en processor creëren minuscule verschillen in de afbeelding.



Langdurige tracking

Je computer kan herkend worden, zelfs weken later.



Test Je Uniekheid

94.5...

Unieke
browsers

Percentage
browsers met
unieke fingerprint

100+

Datapunten

Verzameld voor
een fingerprint

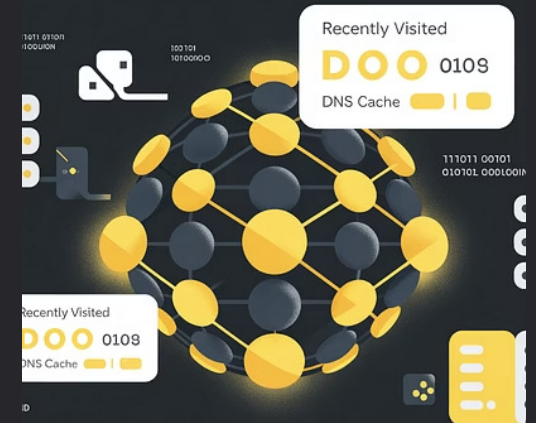
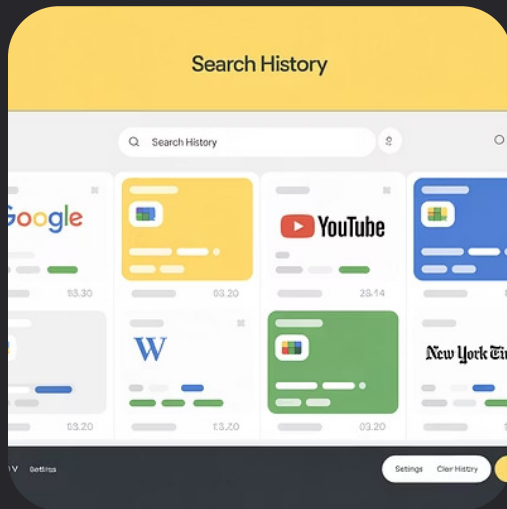
2-3

Jaren

Gemiddelde
stabiliteit van een
fingerprint

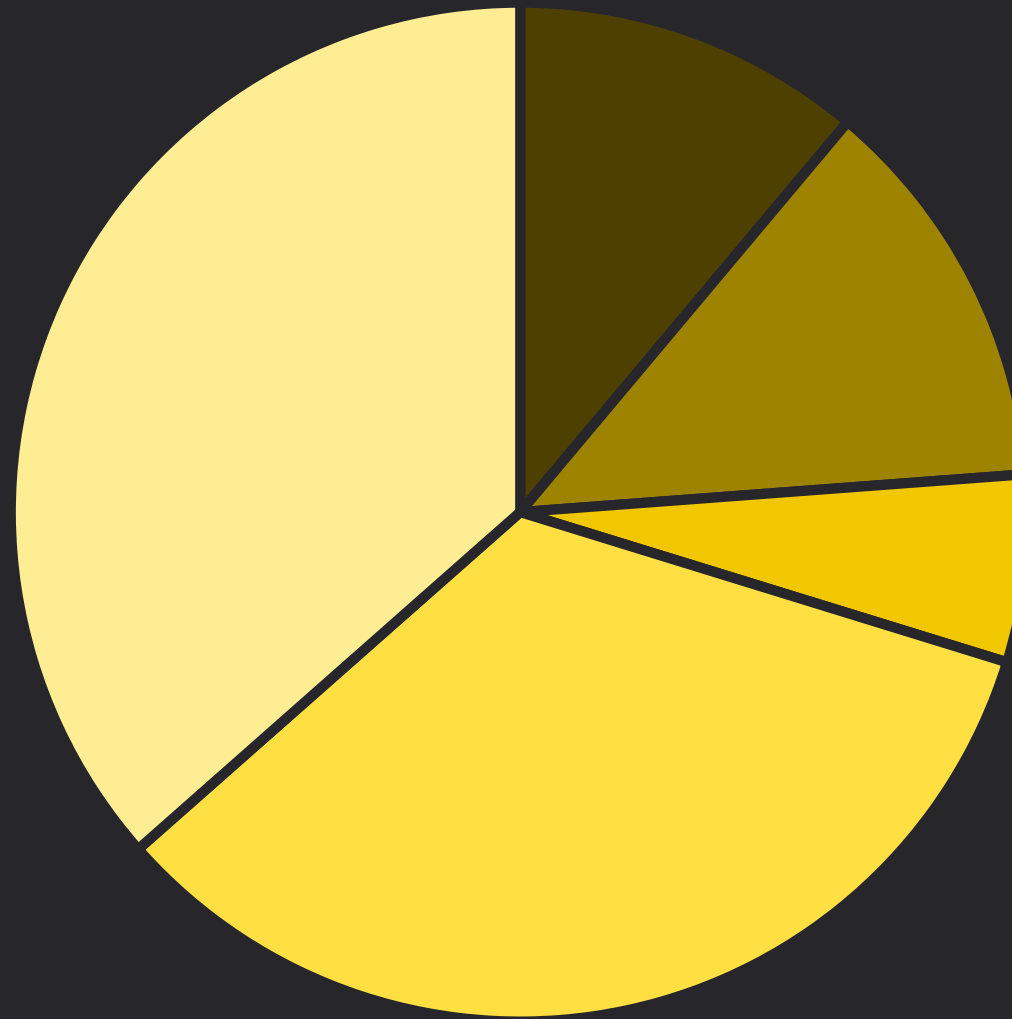
Tools zoals coveryourtracks.eff.org of amiunique.org testen hoe uniek je browser is. Hoe unieker, hoe makkelijker je te volgen bent.

Lokale Sporen Op Je Computer



Naast online tracking laat surfen ook sporen achter op je computer: browsergeschiedenis, cookies, cache, hibernatiebestand, systeemlogboeken en DNS-cache.

Waarom Bescherming Belangrijk Is



■ Identiteitsdiefstal ■ Phishing ■ Datadiefstal ■ Gerichte advertenties ■ Profilering

Bescherming op het web is niet alleen voor criminelen of houders van gevoelige geheimen. In het digitale tijdperk wordt iedereen blootgesteld aan online risico's.

Collectieve Verantwoordelijkheid



Bewustwording

Begrijp welke sporen je achterlaat op het internet.



Bescherming

Leer hoe je je privacy kunt beschermen met de juiste tools.



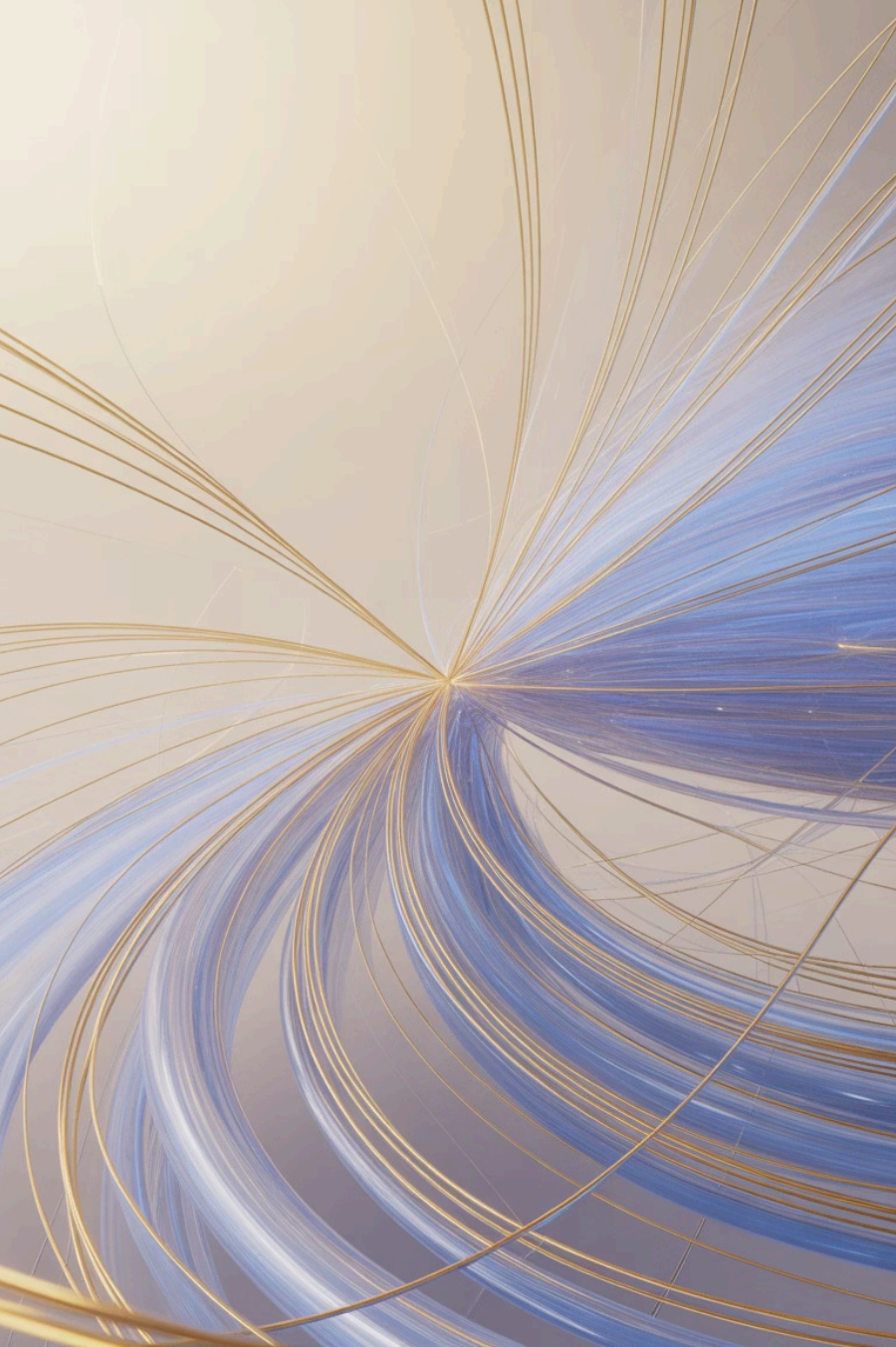
Collectieve actie

Draag bij aan een veiligere online omgeving voor iedereen.



Protecting tomorrow,
together

S SECUREFUTURE
SOLUTIONS



Wat kunnen we verwachten van het 6G-netwerk?

De volgende stap in connectiviteit belooft een revolutie. 6G zal verder gaan dan wat we kennen.

Het netwerk verbindt niet alleen apparaten maar creëert een volledig nieuw "Internet of Everything".

VEILIGDIGITAAL.COM

Wat is 6G en waarom is het belangrijk?



Nieuwe generatie

6G volgt 5G op als volgende stap in mobiele netwerken.



Ongekende prestaties

Baanbrekende snelheden en intelligentie veranderen onze digitale ervaring.

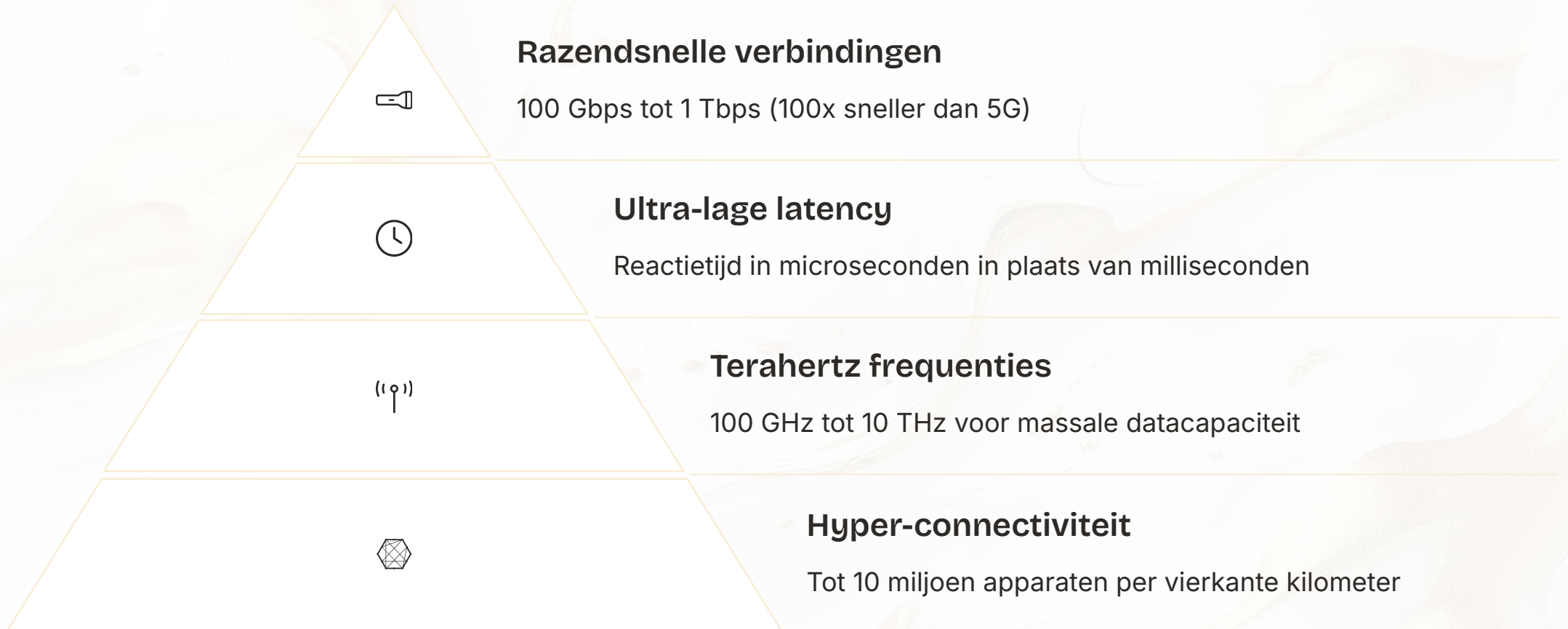


Allesomvattend

Van "Internet of Things" naar een volledig "Internet of Everything".



Technische verschuivingen in 6G



Nieuwe mogelijkheden & toepassingen



Denkende netwerken

Systemen die autonoom waarnemen en intelligent reageren.



Volledige XR-integratie

Extended reality zonder hardware-beperkingen.



Digitale tweelingen

Real-time simulaties voor complexe systemen.



AI-revolutie

Ongekende ondersteuning voor kunstmatige intelligentie.





Tijdlijn en wereldwijde impact

1

2028

Eerste testnetwerken in Azië, pioniers zijn China, Zuid-Korea en Japan.

2

2030

Commerciële uitrol begint. Digitale en fysieke wereld beginnen te vervagen.

3

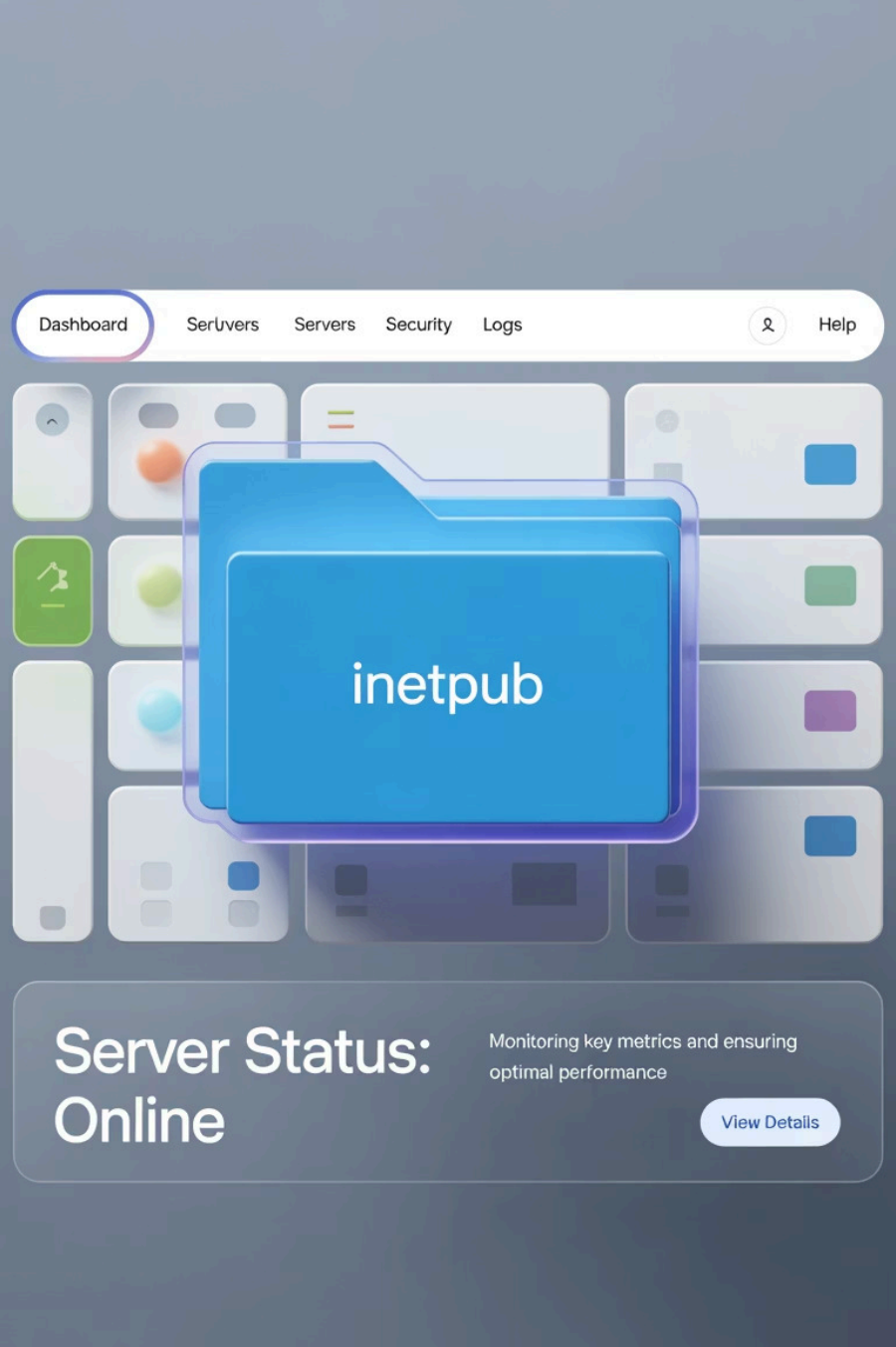
2035

Wereldwijde dekking via geïntegreerde satellieten. "Internet of Senses" wordt realiteit.

4

2040

Nieuwe economische kansen en banen. Volledig nieuwe communicatievormen ontstaan.



Wat is de inetpub-map?

De inetpub-map is een standaard Windows-map die gebruikt wordt voor webhosting via Internet Information Services (IIS), maar is nu ook onderdeel van Windows beveiliging

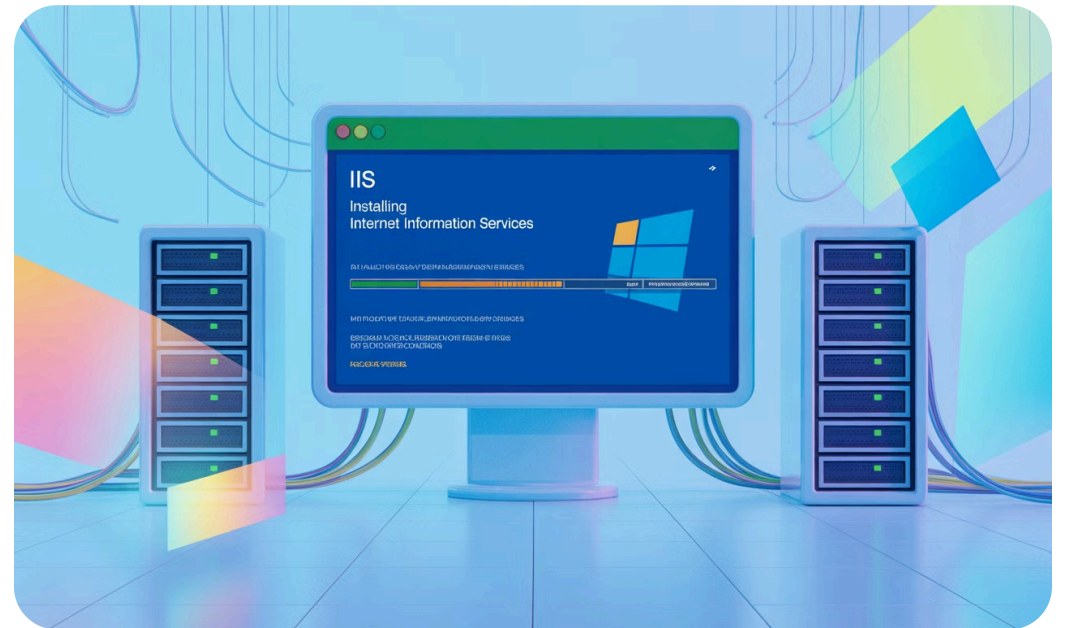
Je vindt deze map meestal in C:\inetpub. Hier worden websitebestanden en -logs opgeslagen.

VEILIGDIGITAAL.COM

Oorsprong en traditionele functie

De inetpub-map bestaat al sinds Windows XP en Server-edities. Hij is essentieel voor het draaien van websites via IIS.

Opvallend is dat deze map aanwezig kan zijn, zelfs als IIS niet actief is op je systeem.





Waarom zie je deze map tegenwoordig vaker?

Vroeger

Alleen aanwezig bij IIS-installatie

1

2

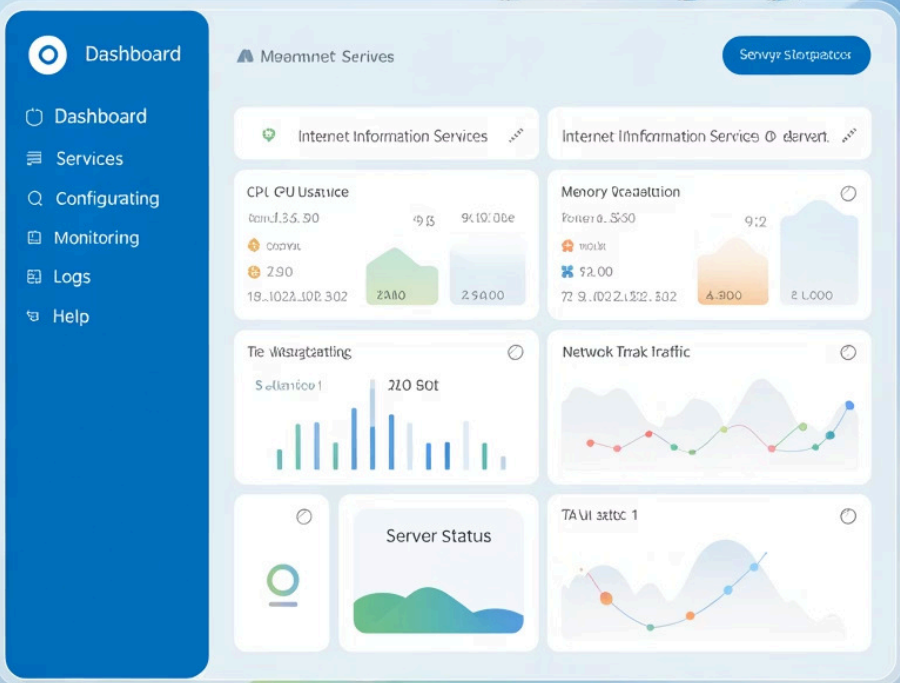
3

Resultaat

Verschijnt zelfs zonder IIS-installatie

Nu

Aangemaakt door beveiligingsupdates sinds april 2025



Wat is IIS?



Webserver-software

Internet Information Services is Microsoft's webserver-platform



Hostingdienst

Maakt het mogelijk websites te draaien op Windows-servers



Ondersteunt diverse technologieën

Werkt met ASP.NET, PHP en andere webtechnologieën

Verband met recente Windows-beveiligingsupdate



Waarom mag je de inetpub-map niet verwijderen?

Microsoft's advies

Het bedrijf raadt expliciet aan om de map NIET te verwijderen, zelfs als je IIS niet gebruikt.

Updateproblemen

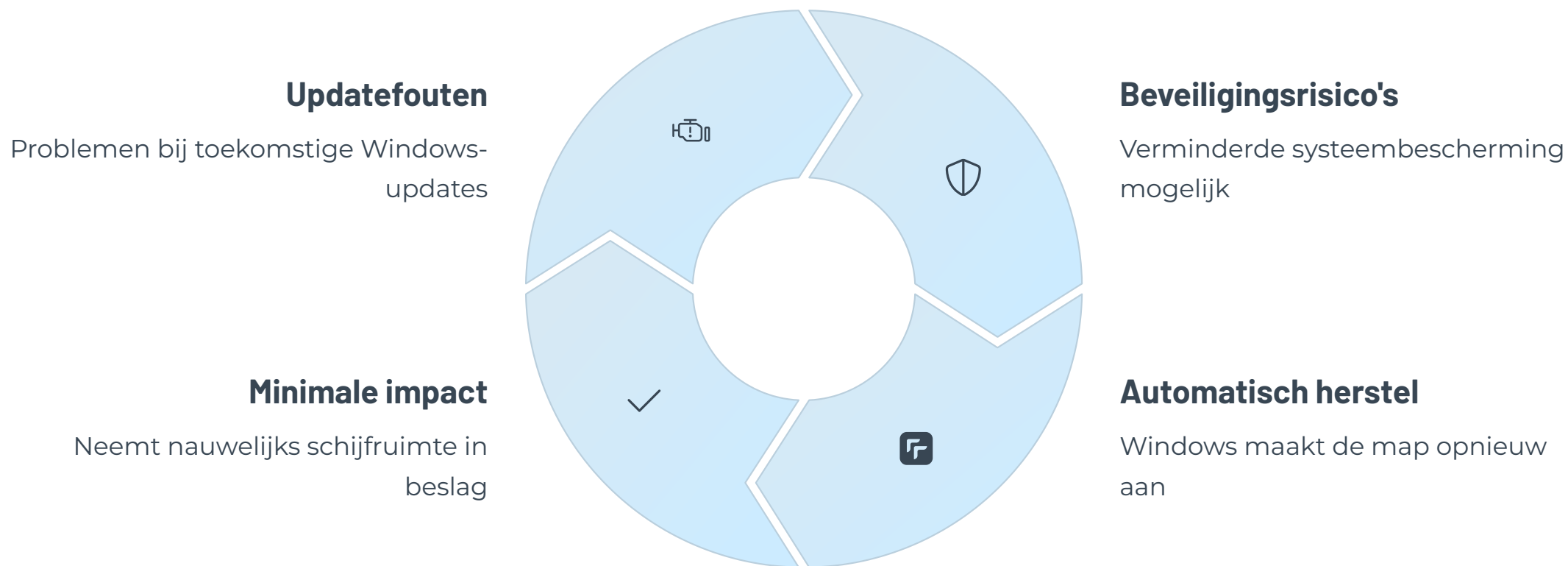
Verwijderen kan de installatie van toekomstige updates verhinderen of blokkeren.

Beveiligingsfunctie

De map is onderdeel van verhoogde systeembescherming, ook zonder actief IIS.



Mogelijke gevolgen verwijderen





Veelgestelde vragen over inetpub



Is het een virus?

Nee, het is een officieel Windows-onderdeel



Kan ik IIS verwijderen?

Ja, maar de map blijft na updates



Activeert dit IIS?

Nee, de map alleen installeert geen IIS

Samenvatting en advies

Begrijp de functie

De inetpub-map dient voor webhosting én als beveiligingsmaatregel.

Volg Microsoft's advies

Verwijder de map niet, zelfs als hij leeg is en je IIS niet gebruikt.

Voorkom problemen

Het opvolgen van deze adviezen voorkomt updateproblemen en verhoogt je beveiliging.



Waarom Zoveel Ouderen Slachtoffer Worden van Nep-agenten

De afgelopen jaren is er een zorgwekkende trend waarneembaar in Nederland: een explosieve toename van oplichting waarbij criminelen zich voordoen als politieagenten om kwetsbare ouderen te misleiden. Dit fenomeen heeft inmiddels duizenden slachtoffers gemaakt en miljoenen euro's aan schade veroorzaakt.

In dit artikel geven wij aan waarom juist ouderen zo vaak doelwit worden van deze vorm van oplichting, welke tactieken de criminelen gebruiken, en wat we kunnen doen om onze ouderen beter te beschermen tegen deze geraffineerde vorm van fraude.

VEILIGDIGITAAL.COM



Explosieve Groeicijfers



Meldingen 2023

Totaal aantal geregistreerde gevallen vorig jaar: 544 meldingen van nepagent-fraude



Meldingen 2024

Dramatische stijging naar 8329 meldingen, een toename van 1500% t.o.v. vorig jaar

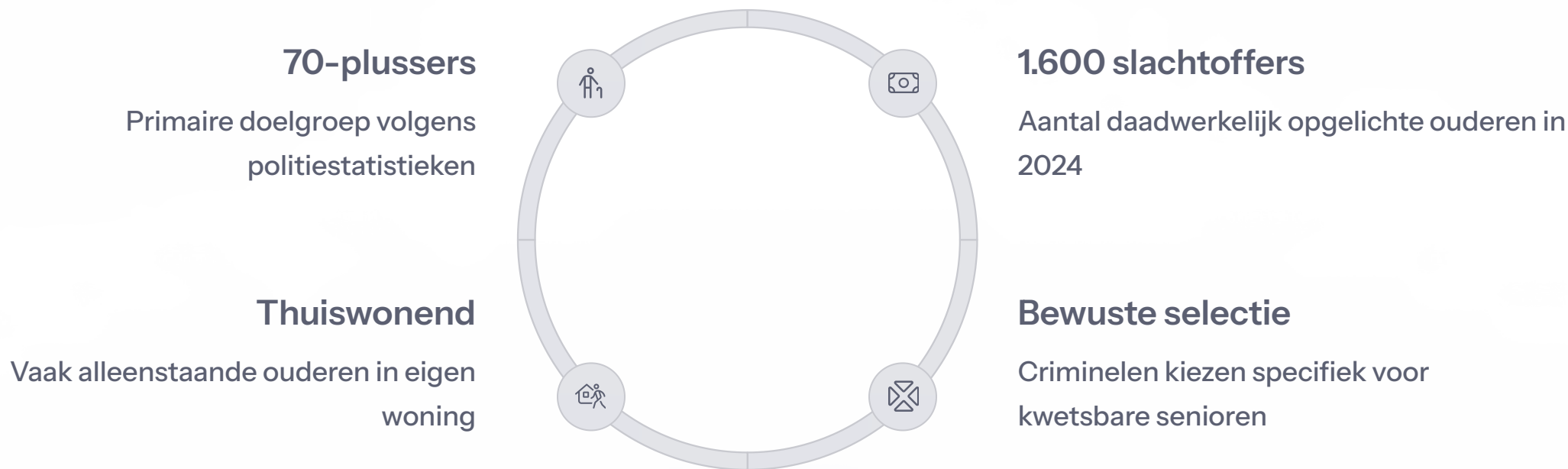


Meldingen per dag

Gemiddeld 24 meldingen per dag – bijna elk uur wordt een nieuw slachtoffer gemeld

De cijfers zijn alarmerend: waar in 2023 nog 544 meldingen binnenkwamen van ouderen die door nepagenten werden benaderd, is dit aantal in 2024 geëxplodeerd naar meer dan 8.000 incidenten. Dit betekent dat er gemiddeld bijna elk uur een nieuwe melding binnenkomt bij de politie, een trend die dringend aandacht vereist van alle betrokken instanties.

Ouderen als Specifiek Doelwit



Uit politieonderzoek blijkt dat 70-plussers specifiek worden uitgekozen door deze criminele netwerken. Van de meer dan 8.000 geregistreerde incidenten in 2024 heeft ongeveer 1.600 geleid tot daadwerkelijke oplichting met financiële schade. Deze cijfers onderstrepen dat criminelen zeer bewust kiezen voor deze kwetsbare doelgroep, wetende dat zij vaak makkelijker te overtuigen zijn.

Tactieken van Nepagenten



Telefonisch contact

Eerste contact via 'waarschuwend' telefoontje over verdachte activiteiten



Nepagent aan de deur

Vervolgens komt een zogenaamde agent aan huis om 'te helpen'



Veiligstellen waardevolle bezittingen

Overtuigen slachtoffer dat geld en sieraden 'in veiligheid' moeten worden gebracht



Overtuigende details

Gebruik van politieterminologie en namaak-identificatie

De gebruikte tactieken zijn geraffineerd en doordacht. Slachtoffers worden eerst telefonisch benaderd met een verhaal over verdachte activiteiten of een inbraak in de buurt. Vervolgens komt een nepagent langs die aanbiedt waardevolle bezittingen 'veilig te stellen'. Het misbruik van vertrouwen in de politie maakt deze vorm van oplichting bijzonder effectief en moeilijk te doorzien voor kwetsbare ouderen.



OUD

NIEUW



Waarom zijn Ouderen Kwetsbaar?



De oudere generatie is opgegroeid in een tijd waarin gezagsdragers zoals politieagenten onvoorwaardelijk werden vertrouwd. Dit diepgewortelde vertrouwen maakt hen kwetsbaarder voor deze vorm van bedrog. Daarnaast zijn veel ouderen minder digitaal vaardig, waardoor ze minder bekend zijn met moderne oplichtingsmethoden en de waarschuwingssignalen hiervan minder snel herkennen.

Sociale isolatie speelt ook een belangrijke rol: alleenwonende ouderen hebben geen partner of huisgenoot die direct kan helpen bij het herkennen van verdachte situaties of om advies te vragen wanneer ze worden benaderd door iemand die beweert van de politie te zijn.

Impact op Slachtoffers

Financiële schade

- Verlies van spaargeld
- Diefstal van sieraden en erfstukken
- Afname van bankpassen en pincodes

Emotionele impact

- Angst en onzekerheid
- Schaamtegevoelens
- Verlies van zelfvertrouwen

Langdurige gevolgen

- Wantrouwen naar autoriteiten
- Sociaal isolement
- Blijvend gevoel van onveiligheid

De gevolgen van deze vorm van oplichting reiken veel verder dan alleen het financiële verlies. Hoewel de materiële schade aanzienlijk kan zijn – met soms het verlies van levenslange spaargelden of kostbare erfstukken – is de emotionele impact vaak nog ingrijpender. Slachtoffers verliezen niet alleen hun bezittingen, maar ook hun gevoel van veiligheid en vertrouwen in de samenleving.

Veel slachtoffers kampen na de oplichting met gevoelens van schaamte en angst, waardoor ze zich terugtrekken uit sociale activiteiten. Het wantrouwen jegens de politie, die juist bescherming zou moeten bieden, is een bijzonder pijnlijk aspect van deze vorm van criminaliteit.

Oplossingen en Preventietips



Voorlichting en bewustwording

Campagnes van ANBO, politie en andere instanties om ouderen beter te informeren over de gevaren en herkenningspunten van nepagenten. Voorlichting is de belangrijkste sleutel in de strijd tegen deze vorm van oplichting.



Herkennen van waarschuwingssignalen

Echte agenten vragen nooit om waardevolle spullen af te geven of bankpassen te overhandigen. Leer verdachte telefoontjes en babbeltrucs te herkennen om niet in de val te trappen.



Direct actie ondernemen

Bij twijfel direct ophangen, de deur niet openen, en contact opnemen met de officiële politie via het algemene nummer. Informeer ook familieleden over verdachte contacten om oplichting te voorkomen.

Samenvatting en Oproep



Blijf alert

Herken de waarschuwingssignalen van nepagenten



Praat erover

Bespreek ervaringen met familie en vrienden



Meld verdachte situaties

Neem direct contact op met de politie bij twijfel

De alarmerende stijging van oplichting door nepagenten vraagt om gezamenlijke actie van alle betrokkenen. Door waakzaam te blijven, verdachte situaties te herkennen en direct te melden, kunnen we het de criminelen moeilijker maken om kwetsbare ouderen te bereiken.

Het is belangrijk dat familieleden regelmatig met hun oudere verwanten praten over dit onderwerp en hen helpen om weerbaarder te worden tegen deze vorm van oplichting. Alleen door samen te werken kunnen we deze zorgwekkende trend keren en ervoor zorgen dat ouderen zich weer veilig voelen in hun eigen huis en vertrouwen kunnen blijven houden in de echte politie.



Waarom je de Opera One browser zou moeten gebruiken

Opera One telt wereldwijd 380 miljoen actieve gebruikers. De omzet groeide met 29% in het vierde kwartaal van 2024.

Deze innovatieve browser combineert AI-integratie met Web 3.0 functionaliteiten. Opera One verandert je dagelijkse browse-ervaring.

VEILIGDIGITAAL.COM

De Browser Operator: AI voor dagelijkse taken



AI-gestuurde browsing

Eerste grote browser met intelligente "agentic browsing" technologie.



Natuurlijke taalcommando's

Voer complexe taken uit via eenvoudige gesprekken.



Privacy-georiënteerd

Gegevensverwerking gebeurt lokaal op je eigen apparaat.



Tijdbesparing

Automatisering van alledaagse browsertaken bespaart kostbare tijd.



Superieure gebruikerservaring



Sneller en efficiënter

Opera One presteert beter dan standaard browsers.



Ingebouwde VPN

Verbeterde beveiliging beschermt je online privacy.



Aanpassingsmogelijkheden

Personaliseer je browser volledig naar eigen wens.



Gebruiksvriendelijk

Intuïtieve interface voor alle gebruikersniveaus.

Web 3.0 integratie

Crypto wallets

Beheer digitaal vermogen rechtstreeks vanuit je browser. Ingebouwde wallets maken transacties eenvoudiger.

Gedecentraliseerde identiteit

Verbeterde privacy-tools geven jou controle over je gegevens. Jij bepaalt wat je deelt.

Blockchain-applicaties

Naadloze integratie met Web 3.0 toepassingen. Toegang tot de toekomst van het internet.

Privacy en veiligheid voorop



Human-in-the-loop

Jouw toestemming staat centraal bij gevoelige gegevens



Lokale gegevensverwerking

Data verlaat nooit je apparaat zonder toestemming



Sterke beveiliging

Bescherming tegen online bedreigingen en aanvallen



Duurzaamheid

Energiezuinig browsen vermindert je digitale voetafdruk

Conclusie: Een browser voor de toekomst

Innovatie voorop

Voorloper met Opera Neon en geavanceerde AI-technologie

Toekomstgericht

Klaar voor de volgende generatie internetgebruik



Krachtig alternatief

Overtuigend alternatief voor Chrome met unieke functies

Perfecte balans

Geavanceerde technologie met ongeëvenaard gebruiksgemak

Download: www.opera.com/nl/download



Waarom je DEEPSEEK AI niet zou moeten gebruiken

DeepSeek AI is momenteel een van de populairste AI-applicatie ter wereld. Overal wordt erover gesproken en gediscussieerd.

Ondanks de populariteit groeit de kritiek. Steeds meer experts in de techwereld uiten hun zorgen en waarschuwingen.

VEILIGDIGITAAL.COM



Privacyzorgen en Data-afhandeling

Chinese gegevensverwerking

DeepSeek verzendt en verwerkt alle gebruikersdata in China. Dit valt onder Chinese wetgeving en toezicht.

Uitgebreide dataverzameling

De app verzamelt gedetailleerde informatie over jouw gebruik, prompts en apparaatgegevens.

Ruime gebruiksvoorwaarden

Hun voorwaarden geven DeepSeek vergaande toegang tot jouw persoonlijke informatie.

Cybersecurity en Misinformatie

Eerdere datalekken

Cyberaanvallen hebben geleid tot het lekken van API-geheimen en gevoelige chatgeschiedenis.



Twijfelachtige beveiliging

Beveiligingsexperts plaatsen vraagtekens bij DeepSeek's beschermingsmaatregelen.

Misbruikpotentieel

Het platform kan worden gebruikt voor het genereren van misleidende informatie en deepfakes.



Ethische en Praktische Bezwaren



Desinformatie

Het model kan worden misbruikt voor beïnvloeding van de publieke opinie.



Supply-chain risico's

Open integraties vergroten de kwetsbaarheid voor aanvallen via de toeleveringsketen.



Ernstige risico's

Je data en privacy staan op het spel. Wees uiterst voorzichtig.



DeepSeek



Waarom is Thunderbird een goed alternatief voor Outlook?

Steeds meer bedrijven en particulieren zoeken naar gratis alternatieven voor hun dagelijkse e-mailbeheer.

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

Kostprijs: Vrij vs. Betaald

Thunderbird

Volledig gratis en open-source software. Geen verborgen kosten voor extra accounts.

Onbeperkt gebruik zonder licentiekosten.

Outlook

Betaalde Microsoft-dienst met terugkerende licentiekosten. Deel van Microsoft 365.

Extra kosten voor meerdere accounts mogelijk.



Gebruiksgemak & Instellingen



Eenvoudige configuratie

Minder complexe interface. Ideaal voor snelle overstap.



Veelzijdige ondersteuning

Werkt met IMAP, POP3 en andere e-mailprotocollen.



Intuïtief gebruik

Duidelijke menu's en instellingen voor alle gebruikers.

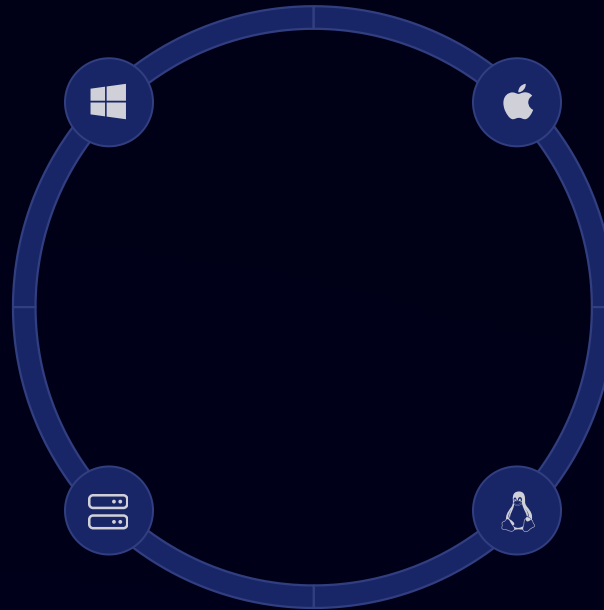
Compatibiliteit & Platformen

Windows

Volledige functionaliteit op alle Windows-versies.

Mailservers

Compatibel met vrijwel alle beschikbare e-mailservers.



Mac

Native ondersteuning voor macOS.

Linux

Perfekte integratie met alle Linux-distributies.

Functionaliteiten & Uitbreidingen



Conclusie: Waarom kiezen voor Thunderbird?



Volledig gratis

Geen restricties of licenties nodig. Gebruik zoveel accounts als je wilt.



Eenvoudig en compatibel

Werkt op alle platformen. Intuïtieve interface voor elke gebruiker.



Veelzijdig en onafhankelijk

Flexibel door uitbreidingen. Geen binding aan Microsoft ecosysteem.





Sporen Veiligstellen op het Internet

Deze praktische gids helpt slachtoffers van digitale criminaliteit. We laten zien hoe je belangrijk bewijs kunt verzamelen en bewaren.

Je leert eenvoudige stappen die direct toepasbaar zijn. Zo vergroot je de kans dat daders worden opgespoord.

VEILIGDIGITAAL.COM



Waarom Sporen Veiligstellen?

18,7%

Aangifte

Percentage slachtoffers dat aangifte doet is te laag

14%

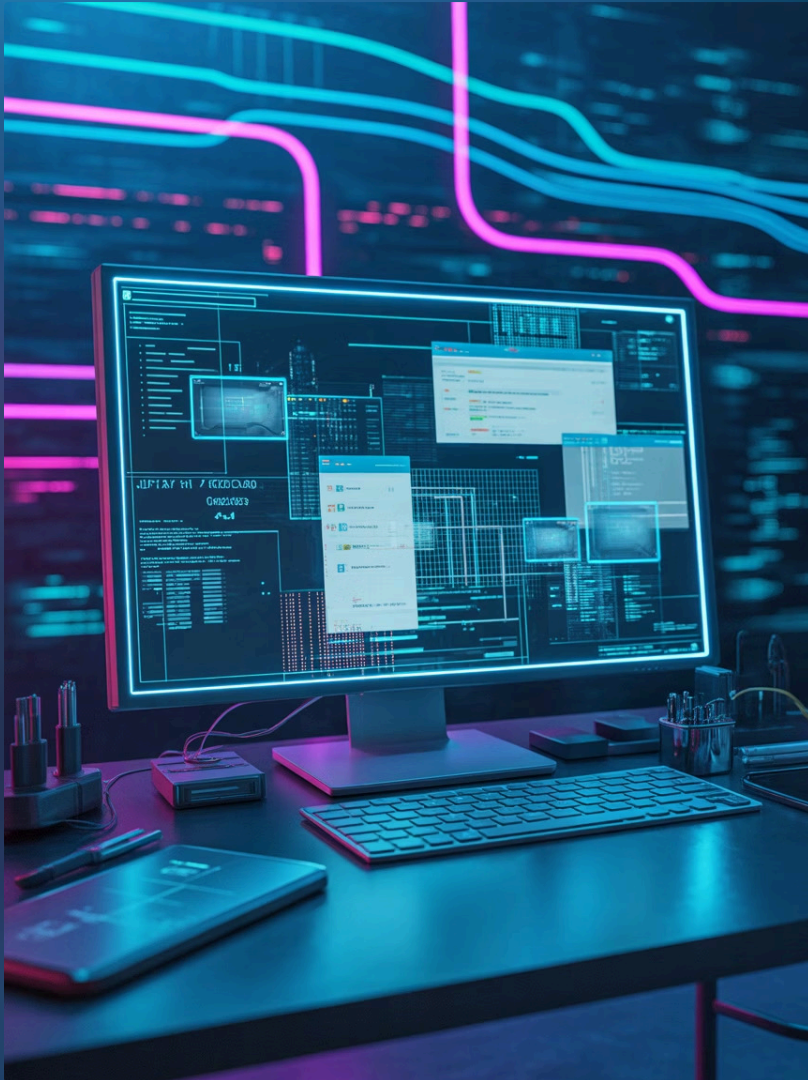
Slachtoffers

Utrechters die in 2023 slachtoffer werden van online criminaliteit

2x

Meer kans

Met goed digitaal bewijs is opsporing en vervolging waarschijnlijker



Wat Zijn Digitale Sporen?

Visuele bewijzen

Screenshots van bedreigingen, oplichting of fraude op websites en apps.

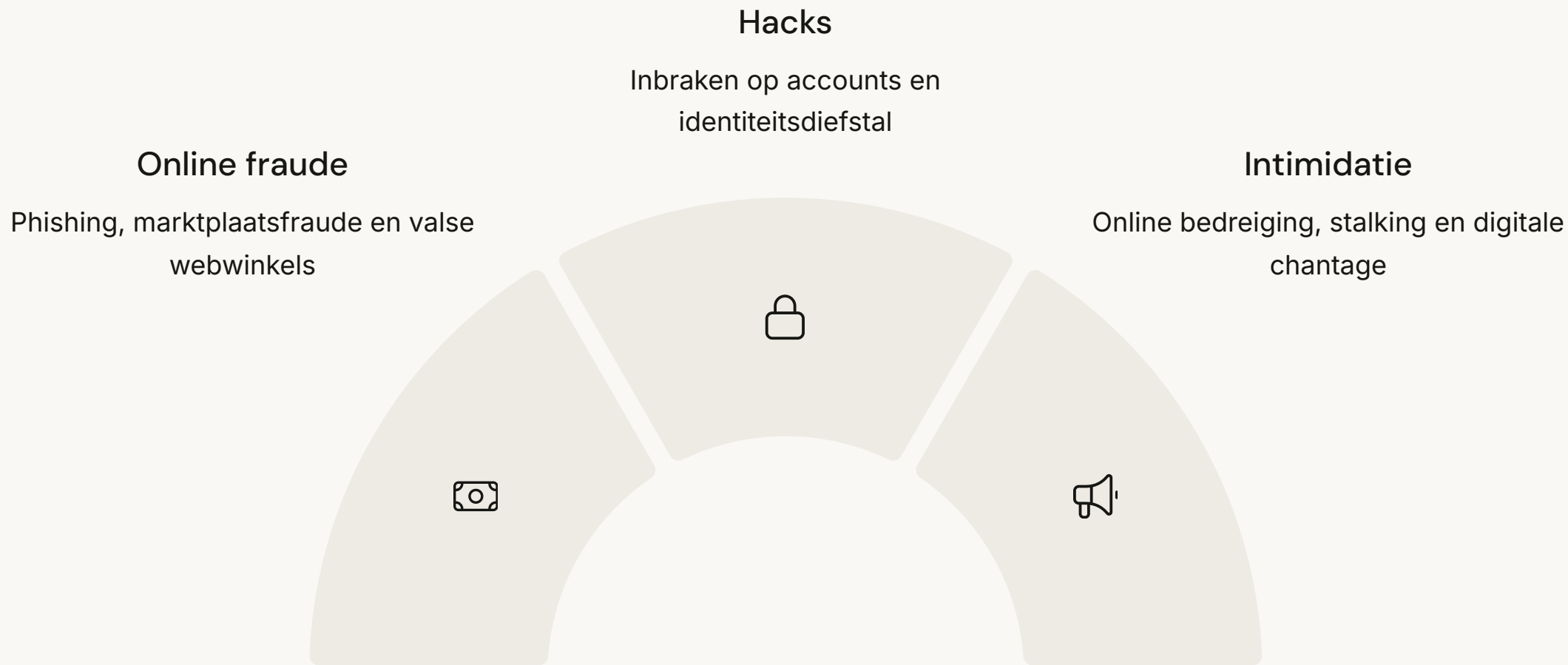
Communicatie

E-mailheaders, chatberichten en profielen van verdachten op sociale platforms.

Technische data

IP-adressen, inlogtijden en metadata die helpen bij identificatie.

Belangrijkste Soorten Internetdelicten





Eerste Reactie bij Online Delict

Blijf kalm

Reageer niet impulsief. Emotionele reacties kunnen bewijs vernietigen of de situatie verergeren.

Documenteer direct

Noteer alle feiten meteen. Schrijf op wat er precies is gebeurd.

Behoud contact

Verbreek contact niet direct als je nog bewijs moet verzamelen.



Essentiële Apparatuur en Hulpmiddelen



Opnameapparatuur

Smartphone of computer met camera voor het maken van screenshots.



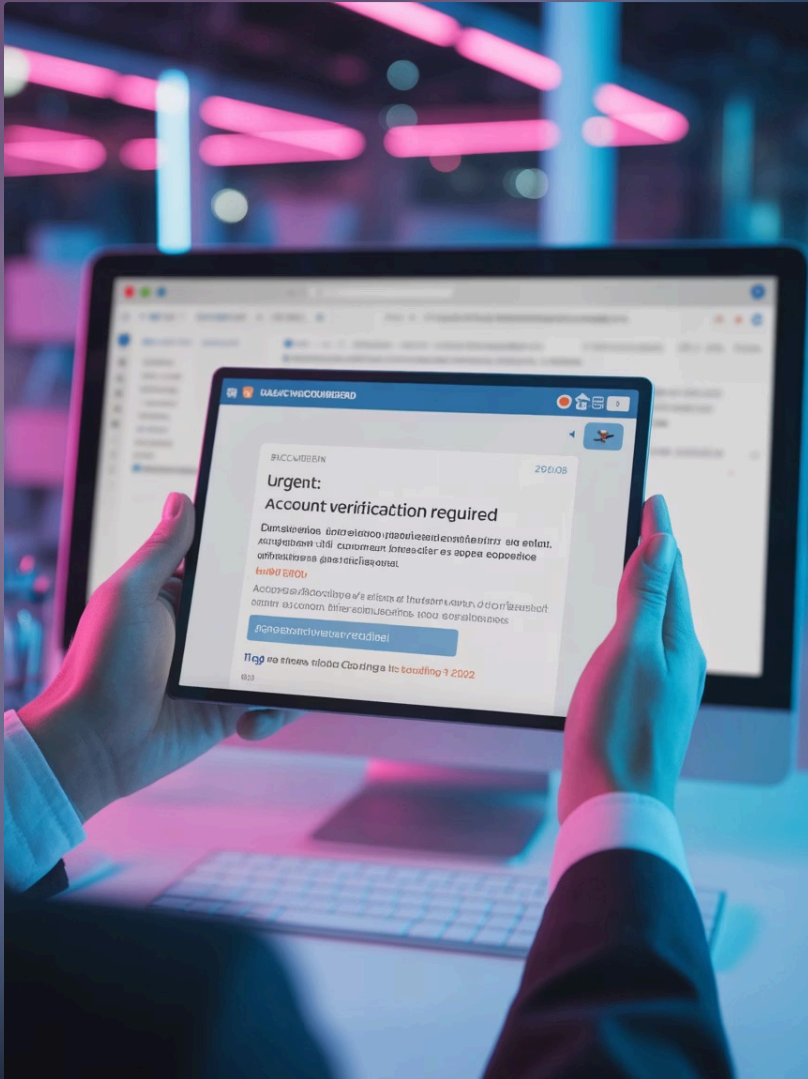
Opslagmiddelen

Cloudopslag of USB-stick voor het veilig bewaren van bewijsmateriaal.



Documentatie

Notitieboek voor het handmatig bijhouden van gebeurtenissen en tijdlijnen.



Bewaren van Digitale Berichten en Mails



Vastleggen

Maak een screenshot van het volledige scherm met alle details zichtbaar.



Documenteren

Noteer datum, tijd, afzender en volledige inhoud van het bericht.



Opslaan

Download originele e-mails inclusief headers voor technisch bewijs.

Chatgesprekken en Social Media



Screenshots

Leg volledige conversaties vast, inclusief datum- en tijdstempels.



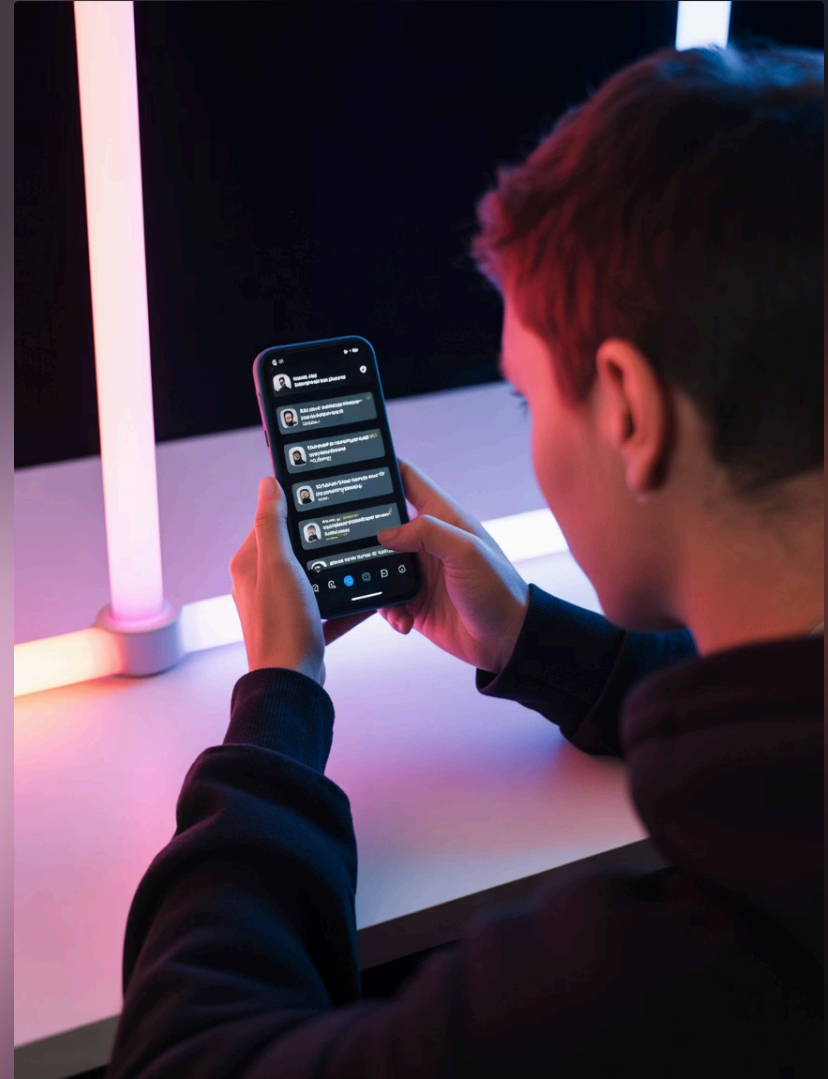
PDF-opslag

Sla belangrijke berichten op als PDF voor duurzame bewaring.



URL's bewaren

Noteer linkjes naar profielen of specifieke berichten.



Het Vastleggen van Webpagina's

1 Screenshot met context

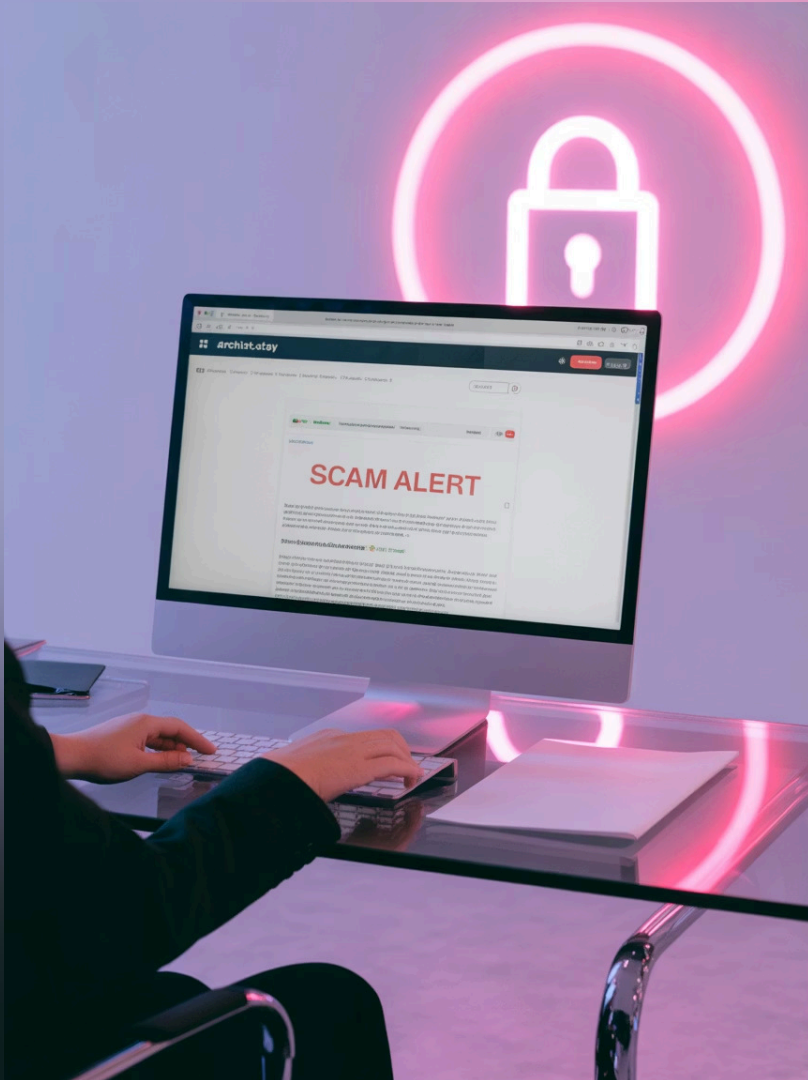
Maak een afbeelding van de hele pagina met zichtbare URL en datum.

2 PDF-export

Gebruik 'Print als PDF' voor het bewaren van complete webpagina's.

3 Archiefopslag

Gebruik diensten zoals archive.today of Wayback Machine voor onafhankelijke kopieën.



Foto's, Video's en Audio



Direct opslaan

Download bestanden meteen na ontvangst



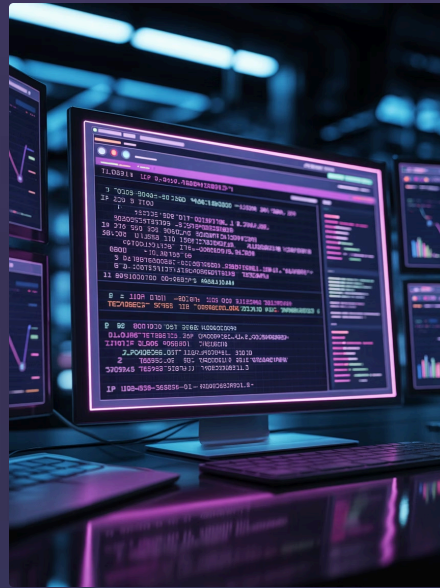
Documenteren

Noteer bij elk bestand de bron en tijd



Backup maken

Maak foto's van berichten op scherm



Logbestanden en Technische Gegevens

Type Gegevens	Hoe Vastleggen	Waarom Belangrijk
IP-adressen	Kopiëren uit e-mailheaders	Locatie en identiteit dader
Inlogtijden	Screenshots van meldingen	Tijdslijn van activiteit
Metadata	Eigenschappen van bestanden bewaren	Technisch forensisch bewijs

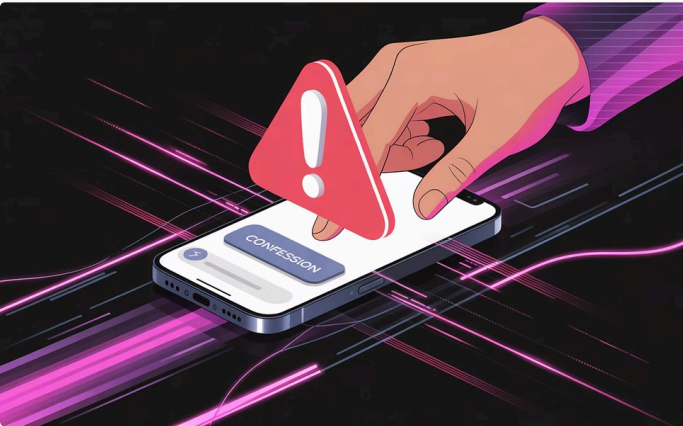
Bewijsmateriaal Veilig Bewaren



Delen met de Politie of Meldpunt

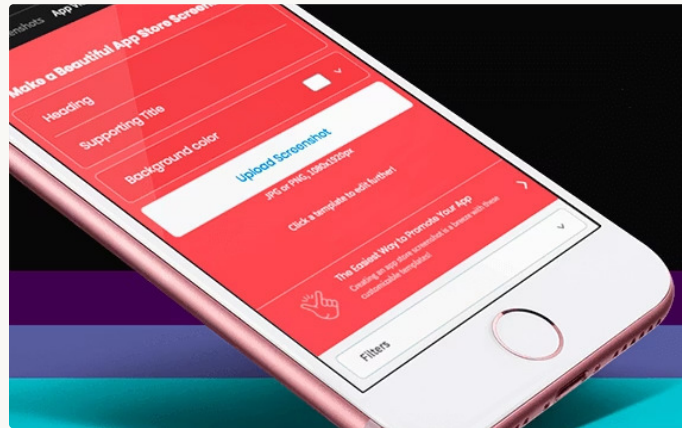


Veelgemaakte Fouten



Te snel verwijderen

Berichten wissen voordat een kopie is gemaakt voor bewijsvoering.



Onvolledige screenshots

Alleen de tekst vastleggen zonder datum, tijd of afzendergegevens.



Onjuist delen

Bewijs verspreiden onder vrienden of familie in plaats van officiële instanties.



Crimineel Misbruik van End-to-End Versleutelde Apps

Europol uit toenemende zorgen over het gebruik van versleutelde apps door criminelen. Deze encryptie belemmert opsporingsdiensten bij het verzamelen van cruciale bewijsstukken.

Dit presentatie onderzoekt de uitdagingen en mogelijke oplossingen voor dit groeiende probleem.

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

Wat is End-to-End Encryptie?

Definitie

Een beveiligingsmethode waarbij alleen de verzender en ontvanger toegang hebben tot berichten. Niemand anders kan meelezen.

Kenmerken

- Data blijft onleesbaar voor derden
- Zelfs techbedrijven kunnen niet meekijken
- Standaard in apps zoals WhatsApp en Signal





Europol's Zorgen Rond E2E (end to end) Encryptie



Onzichtbare Criminaliteit

Strafbare feiten blijven verborgen voor politie en justitie.
Bewijsmateriaal is ontoegankelijk geworden.



Geen Toegang

Techbedrijven kunnen geen gegevens meer verstrekken. Ze hebben zelf geen toegang tot de inhoud.



Ernstige Misdrijven

Kindermisbruik en terrorisme worden moeilijker op te sporen.
Criminelen genieten bescherming door technologie.

Hoe Maken Criminelen Gebruik van Encryptie?



Criminelen profiteren van geavanceerde technische mogelijkheden. Ze opereren in het donker, buiten het zicht van justitie.



Case: Het Ontmantelen van Ghost

1

Ontdekking

Ghost-platform geïdentificeerd als communicatiemiddel voor zware criminelen. Drie encryptielagen maakten het bijna ondoordringbaar.

2

Operatie

Internationale samenwerking tussen opsporingsdiensten. Complexe technische aanpak vereist om toegang te krijgen.

3

Resultaat

51 arrestaties uitgevoerd. Drugslab ontmanteld. Wapens en grote geldbedragen in beslag genomen.

Uitdagingen voor Opsporingsdiensten

Datagedreven Onderzoeken

Complexe technische analyses vereist



Specialistische Kennis

Cybercrime-experts nodig



Juridische Onzekerheid

Onduidelijkheid over toegangsrechten



Internationale Samenwerking

Grensoverschrijdende aanpak
essentieel



Oproep van Europol en Politiediensten

Geen "Veilige Zones"

Criminelen mogen geen plekken hebben waar ze buiten bereik blijven van ordehandhaving. Technologie moet geen criminele vrijhaven creëren.

Samenwerking met Techbedrijven

Technologiebedrijven moeten meewerken aan oplossingen. De huidige impasse tussen privacy en veiligheid moet doorbroken worden.

Wettelijke Waarborgen

Overheden moeten zorgen dat opsporingsdiensten toegang krijgen tot kritische informatie. Nieuwe wetgeving kan nodig zijn.

Conclusie en Vooruitblik



Balans Privacy en Veiligheid

Evenwicht vinden tussen beide waarden



Gerichte Toegang

Oplossingen voor de zwaarste misdrijven



Samenwerking

Tech, overheid en politie moeten samenwerken

De toekomst vraagt om nieuwe benaderingen. We moeten innovatieve oplossingen vinden die zowel privacy als veiligheid beschermen.

Cybercriminelen en de Zwarte Markt voor Gestolen Data

Jaarlijks vinden er wereldwijd miljoenen datalekken plaats die resulteren in een omvangrijke illegale handel in digitale informatie. Deze cybercriminele activiteiten vormen een snelgroeiende sector binnen de georganiseerde misdaad.

Gestolen gegevens worden verhandeld op goed georganiseerde ondergrondse marktplaatsen waar vraag en aanbod samenkomen. De handel in deze informatie is lucratief en heeft zich ontwikkeld tot een professioneel ecosysteem met eigen regels en structuren.

De impact van deze zwarte markten reikt ver: van individuele slachtoffers die financiële schade lijden tot bedrijven die worstelen met reputatieschade en vertrouwensverlies bij klanten.

VEILIGDIGITAAL.COM





Het Zwarte Markt Ecosysteem



Hackers

Stelen data via inbraak in systemen, malware en phishing



Datamakelaars

Faciliteren verkoop en zorgen voor betrouwbare handelsplatformen



Kopers

Gebruiken data voor fraude of verhandelen deze verder

Dit complexe netwerk functioneert als een goed geoliede machine. Hackers concentreren zich op het verkrijgen van waardevolle data, terwijl gespecialiseerde tussenpersonen zorgen voor de distributie. Kopers kunnen eindgebruikers zijn of opnieuw verkopen aan anderen binnen het netwerk.

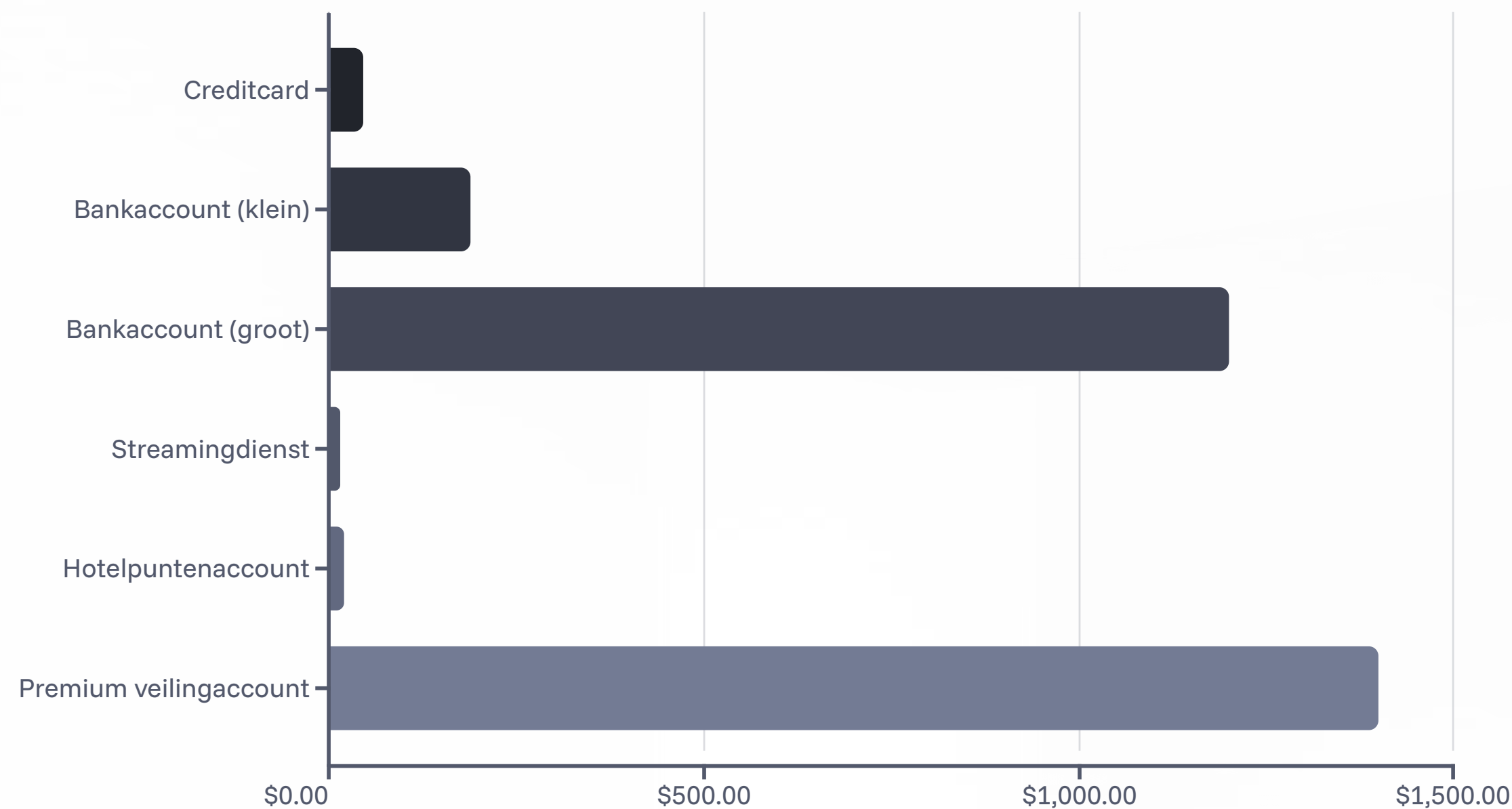
De communicatie verloopt meestal via versleutelde kanalen en betalingen worden afgehandeld met cryptocurrencies om anonimiteit te waarborgen.

Soorten Gestolen Data



De verscheidenheid aan gestolen data weerspiegelt de diverse manieren waarop criminelen waarde kunnen ontlennen aan onze digitale identiteiten en accounts.

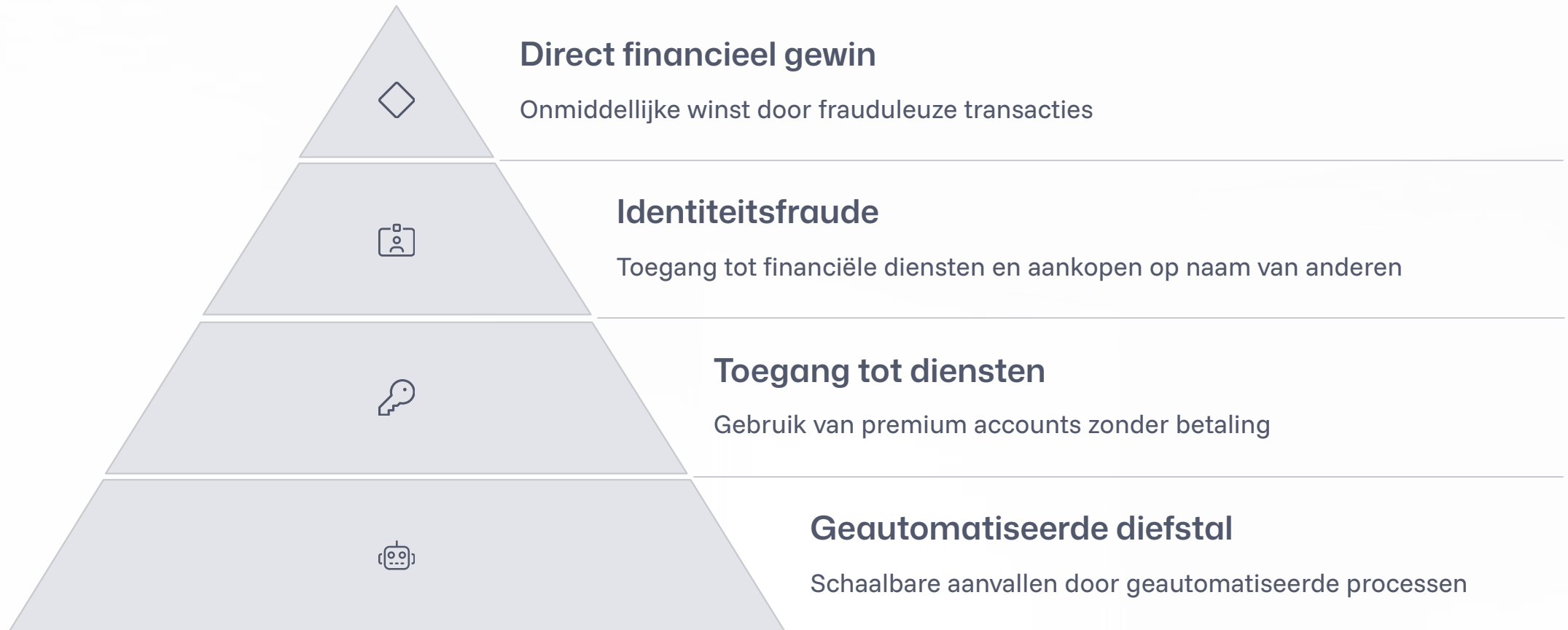
Waarde van Gegevens op de Zwarte Markt



De prijzen voor gestolen gegevens variëren sterk afhankelijk van meerdere factoren. Volledige datasets met uitgebreide informatie brengen meer op dan fragmentarische gegevens. Ook speelt de reputatie van de verkoper een belangrijke rol bij de prijsbepaling.

Interessant is dat bankrekeninggegevens met een hoger saldo aanzienlijk meer waard zijn, wat de directe relatie tussen potentiële opbrengst en marktwaarde aantoont.

Waarom is Gestolen Data Waardevol?



De waarde van gestolen data ligt vooral in de veelzijdige toepassingsmogelijkheden. Criminelen kunnen snel geld verdienen door directe fraude, maar ook door langdurige identiteitsdiefstal waarbij ze rekeningen openen of leningen afsluiten op andermans naam.

Door automatisering kunnen cybercriminelen steeds efficiënter en op grotere schaal toeslaan, wat de winstgevendheid verder verhoogt.

Voorbeeld: Nederlandse Incidenten

Zwakke Wachtwoorden

Veel Nederlandse bedrijven worden gecompromitteerd door eenvoudig te raden wachtwoorden of hergebruikte inloggegevens. Criminelen gebruiken geautomatiseerde tools om deze kwetsbaarheden op te sporen.

Phishing Aanvallen

Gerichte e-mails naar medewerkers van Nederlandse organisaties leiden tot compromittering van bedrijfssystemen. Eén succesvolle phishing aanval kan toegang geven tot duizenden klantenrecords.

Verouderde Software

Niet-bijgewerkte systemen vormen een eenvoudige toegangspoort voor hackers. Meerdere Nederlandse bedrijven hebben datalekken gemeld die te herleiden waren naar bekende, maar niet-gepatchte kwetsbaarheden.

Deze Nederlandse voorbeelden tonen aan dat zelfs in een technologisch geavanceerd land, basisbeveiliging vaak tekortschiet. De gestolen gegevens van Nederlandse burgers en bedrijven verschijnen regelmatig op internationale zwarte markten.



Gevolgen Voor Bedrijven en Consumenten

1 Financiële Schade

Directe verliezen door frauduleuze transacties en kosten voor herstel van beveiligingssystemen. Gemiddelde schade per incident voor een Nederlands MKB-bedrijf: €50.000-€150.000.

2 Identiteitsdiefstal

Slachtoffers worden geconfronteerd met langdurige processen om hun identiteit te herstellen. Soms duurt het jaren voordat alle valse accounts en schulden zijn opgeruimd.

3 Wereldwijde Verspreiding

Eenmaal gestolen gegevens worden meermaals doorverkocht op verschillende platformen, waardoor de impact blijft groeien en de oorsprong moeilijk te traceren is.

4 Vertrouwensverlies

Consumenten verliezen vertrouwen in bedrijven na datalekken, wat leidt tot klantverlies en mogelijke juridische gevolgen onder de AVG-wetgeving.

De langetermijngevolgen van datalekken strekken zich uit ver voorbij het initiële incident, met blijvende impact op zowel consumenten als bedrijven.



Conclusie: Oplossingen en Preventie



Versterkte Beveiliging

Implementeer meervoudige authenticatie en encryptie voor gevoelige gegevens. Regelmatige beveiligingsaudits helpen om zwakke plekken te identificeren voordat criminelen dit doen.



Bewustwording

Train medewerkers en consumenten om phishing te herkennen en veilig online gedrag te vertonen. Bewustzijn is de eerste verdedigingslinie tegen cybercriminaliteit.



Actuele Systemen

Houd software en systemen up-to-date en implementeer een streng wachtwoordbeleid. Automatische updates zorgen ervoor dat bekende kwetsbaarheden snel worden gedicht.



Samenwerking

Internationale samenwerking tussen overheden, bedrijven en cybersecurityexperts is essentieel om de zwarte markten effectief aan te pakken.

De strijd tegen cybercriminelen vereist een gezamenlijke inspanning van alle betrokkenen. Door preventieve maatregelen te combineren met snelle respons bij incidenten, kunnen we de winstgevendheid van gestolen data verminderen en het ecosysteem verstoren.



De "Going Dark" Initiatief: High-Level Group van de EU

De Europese Commissie richtte in juni 2023 deze speciale groep op.

De officiële naam is "High-Level Group on Access to Data for Effective Law Enforcement".

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

Samenstelling en Structuur van de HLG



Doelstellingen van de Groep



Toegang tot Data

Vergroten van mogelijkheden voor politiediensten om digitale gegevens te verkrijgen.



Encryptie Omzeilen

Ontwikkelen van methoden om versleutelde communicatie toegankelijk te maken.



Security by Design

Invoeren van nieuwe concepten voor technologie-ontwikkeling met ingebouwde toegangspoorten.



Wetgevende Voorbereiding

Opstellen van blauwdrukken voor nieuwe surveillancewetgeving in de EU.



Controverses en Kritiek



Gesloten Vergaderingen

Alle bijeenkomsten vinden plaats achter gesloten deuren zonder publieke toegang.



Uitsluiting

Maatschappelijke organisaties mogen niet deelnemen aan de discussies.



Onduidelijkheid

Weinig transparantie over de exacte deelnemers en besproken onderwerpen.



Privacy-zorgen

Vrees voor onevenredige inbreuken op digitale rechten van EU-burgers.



Reacties van Maatschappelijke Organisaties

Open Brief

EDRi en 20 andere organisaties hebben een gezamenlijke brief gestuurd.

Ze eisen meer openheid over de activiteiten van de groep.

Afgewezen Verzoeken

Verzoeken om als experts deel te nemen werden afgewezen.

Dit versterkt zorgen over eenzijdige belangenbehartiging.

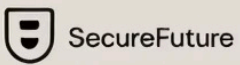
Misleidende Terminologie

"Security by design" wordt bekritiseerd als misleidende term.

In werkelijkheid betekent het verzwakking van beveiliging voor burgers.

Toekomstperspectief en Implicaties





SecureFuture

**Digitale
Beveiliging**

Digitale Beveiliging verandert

Onderzoek uit 2025 toont aan dat moderne authenticatiemethoden zoals biometrische verificatie en token-gebaseerde toegang steeds meer de norm worden.

Effectieve digitale beveiliging vereist een combinatie van geavanceerde technologie en bewust gebruikersgedrag om cyberdreigingen tegen te gaan.

VEILIGDIGITAAL.COM

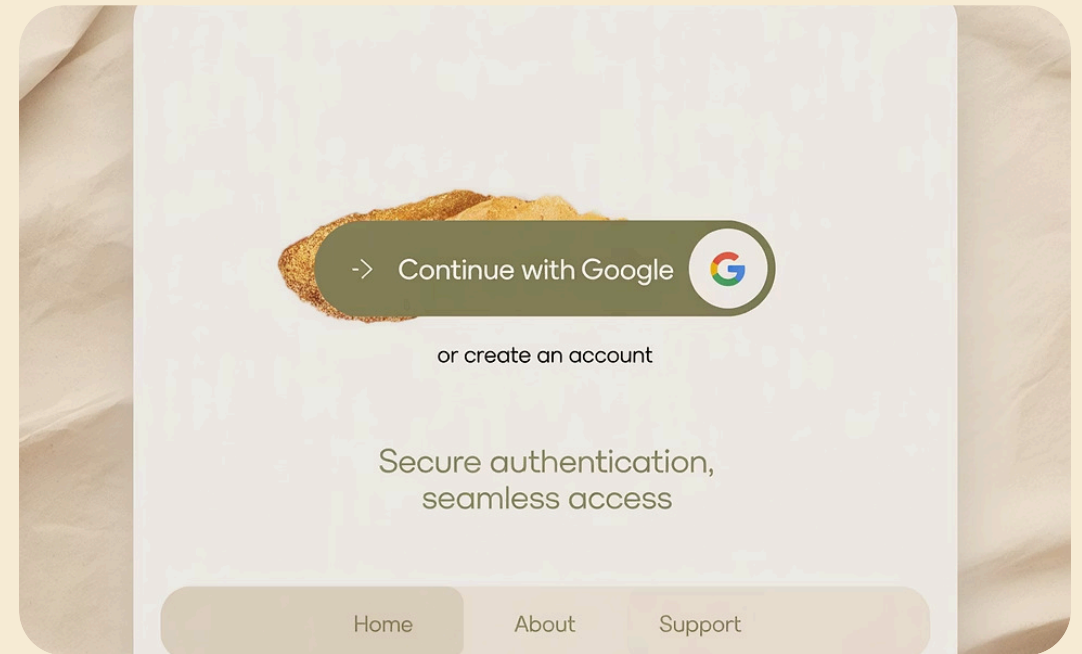
Authenticatiemethoden bij Oudere Generaties

Gen X- en babyboomers houden vast aan vertrouwde inlogmethoden, ondanks bekendheid met moderne alternatieven.



Traditionele Wachtwoorden

Meer dan 60% van de Gen X- en babyboomers gebruikt wachtwoorden als hun primaire inlogmethode.



Sociale Aanmeldingen

Ondanks bekendheid met nieuwere methoden zoals 'Inloggen met Google', gebruikt slechts ongeveer 30% deze dagelijks.

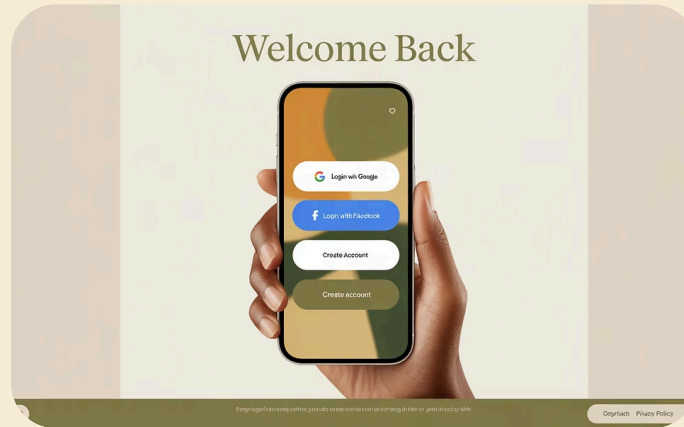
Authenticatievoorkeuren van Gen Z en Millennials

Digitaal native generaties kiezen voor moderne beveiligingsmethoden boven traditionele wachtwoorden.



Biometrische Authenticatie

Gen Z-gebruikers omzeilen traditionele wachtwoorden ten gunste van vingerafdruk- en gezichtsherkenning.



Sociale Aanmeldingen

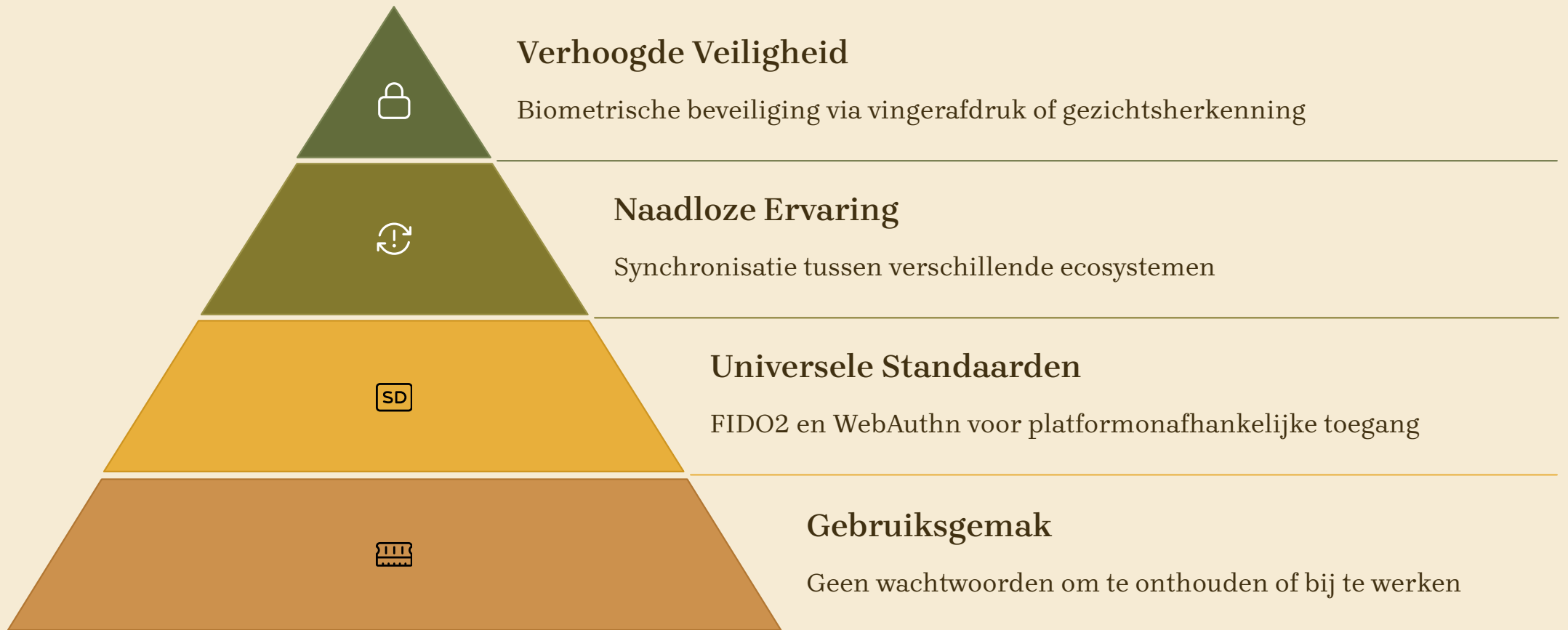
Millennials en Gen Z zijn merkbaar meer afhankelijk van 'Inloggen met Google' en andere sociale aanmeldopties.



Passkeys

Geavanceerde authenticatietools zoals passkeys worden de voorkeur voor digitaal native gebruikers.

Voordelen van Moderne Authenticatie



De Toekomst van Digitale Authenticatie



HaveIBeenPwned: Wat is er veranderd?

Een overzicht van de grote update van mei 2025 voor de bekende website die je helpt controleren of je gegevens zijn gelekt.

Troy Hunt's platform ondergaat zijn eerste grote redesign sinds 2021.

VEILIGDIGITAAL.COM

***Have I Been
Pwned***

Check if your email address is in a data breach

***Have I Been
Pwned***

Check if your email address is in a data breach

Voorgeschiedenis en Achtergrond

1

2013

Oprichting door Troy Hunt als persoonlijk project.

2

2019

Samenwerkingen met FBI en NCA voor "Pwned Passwords".

3

2021

Vorige grote redesign van het platform.

4

2025

Huidige grote vernieuwing van de website.

Wat controleer je met HavelBeenPwnd?

HavelBeenPwned biedt verschillende controlemogelijkheden voor je persoonlijke gegevens:

Emailadressen

Controleer of je e-mail voorkomt in bekende datalekken.

Wachtwoorden

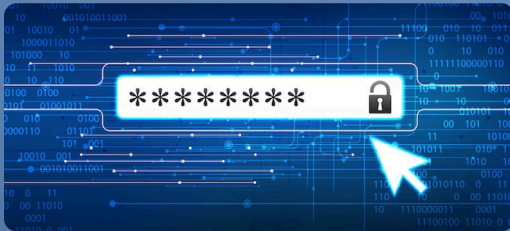
Kijk of je wachtwoord gelekt is zonder het te delen.

Domeinen

Bedrijven kunnen hun hele domein monitoren.

Telefoonnummers

Nieuw: controleer of je telefoonnummer gelekt is.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Vernieuwde Website & UI

Moderne Look

Grootste redesign in jaren met een frissere uitstraling. De interface is intuïtiever geworden.

Schoner dashboard met betere visualisatie van data.

Snellere Zoekfunctie

Geoptimaliseerde backend voor snellere resultaten. Zoekgeschiedenis is nu beter georganiseerd.

API-toegang is verbeterd voor ontwikkelaars.

Confetti bij "No Breach"

Leuke nieuwe feature: confetti-animatie wanneer geen datalekken gevonden zijn.

Positieve gebruikerservaring bij goede resultaten.

Nieuwe Functionaliteiten



Dedicated breach-pagina's

Gedetailleerde informatie per datalek nu beschikbaar.



Monitoring-dashboard

Eenvoudiger accounts en domeinen in de gaten houden.



Passkey-ondersteuning

Toekomstige implementatie van passwordless authenticatie.



Familie-accounts

Beheer meerdere accounts van gezinsleden.

Impact en Voordelen voor Gebruikers

Individuen

- Snellere controle van persoonlijke gegevens
- Betere visualisatie van risico's
- Eenvoudiger te begrijpen resultaten

Bedrijven

- Geavanceerde domeinmonitoring
- Gedelegeerd beheer voor teams
- Uitgebreidere rapportages

Ontwikkelaars

- Verbeterde API-integratie
- Betere documentatie
- Snellere responstijden



Conclusie



Modernier platform

HavelBeenPwned heeft een volledig vernieuwde interface gekregen.



Uitgebreidere functionaliteit

Nieuwe tools maken het controleren van datalekken efficiënter.



Toekomstgericht

De basis is gelegd voor innovatieve functies in het komende jaar.



Blijvend essentieel

Dé plek om snel en eenvoudig je datalek-risico te checken.





Sporen Veiligstellen op het Internet

Deze praktische gids helpt slachtoffers van digitale criminaliteit. We laten zien hoe je belangrijk bewijs kunt verzamelen en bewaren.

Je leert eenvoudige stappen die direct toepasbaar zijn. Zo vergroot je de kans dat daders worden opgespoord.

VEILIGDIGITAAL.COM



Waarom Sporen Veiligstellen?

18,7%

Aangifte

Percentage slachtoffers dat aangifte doet is te laag

14%

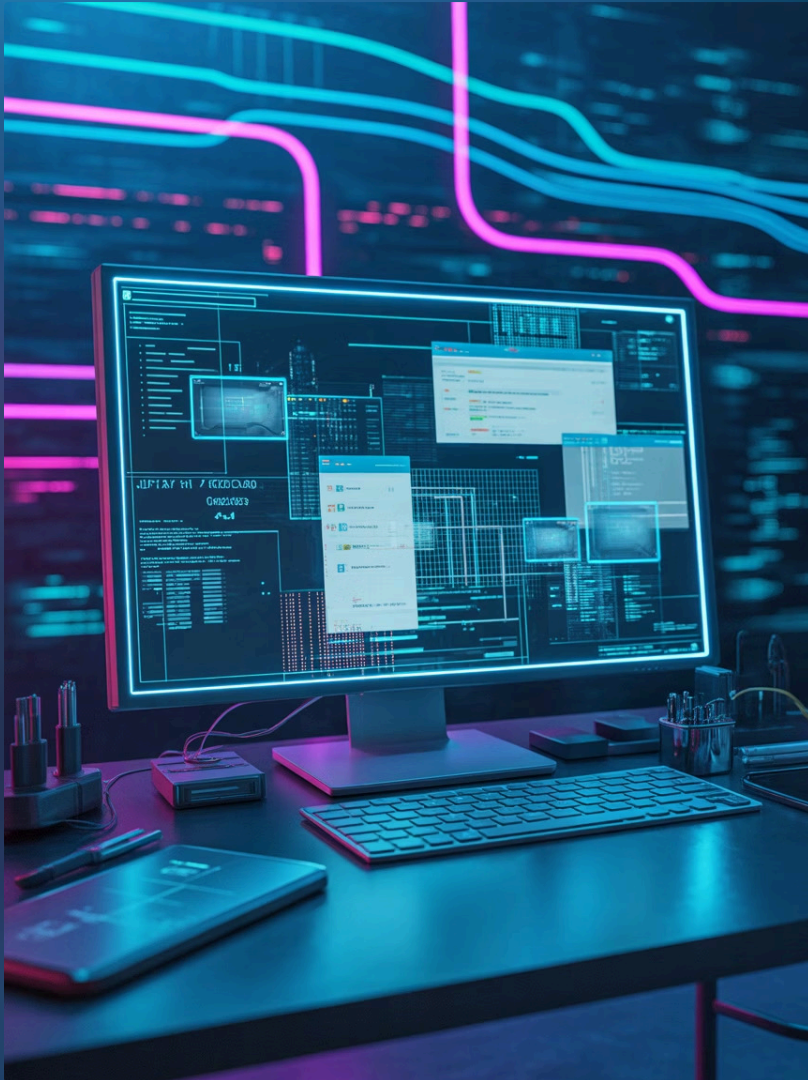
Slachtoffers

Utrechters die in 2023 slachtoffer werden van online criminaliteit

2x

Meer kans

Met goed digitaal bewijs is opsporing en vervolging waarschijnlijker



Wat Zijn Digitale Sporen?

Visuele bewijzen

Screenshots van bedreigingen, oplichting of fraude op websites en apps.

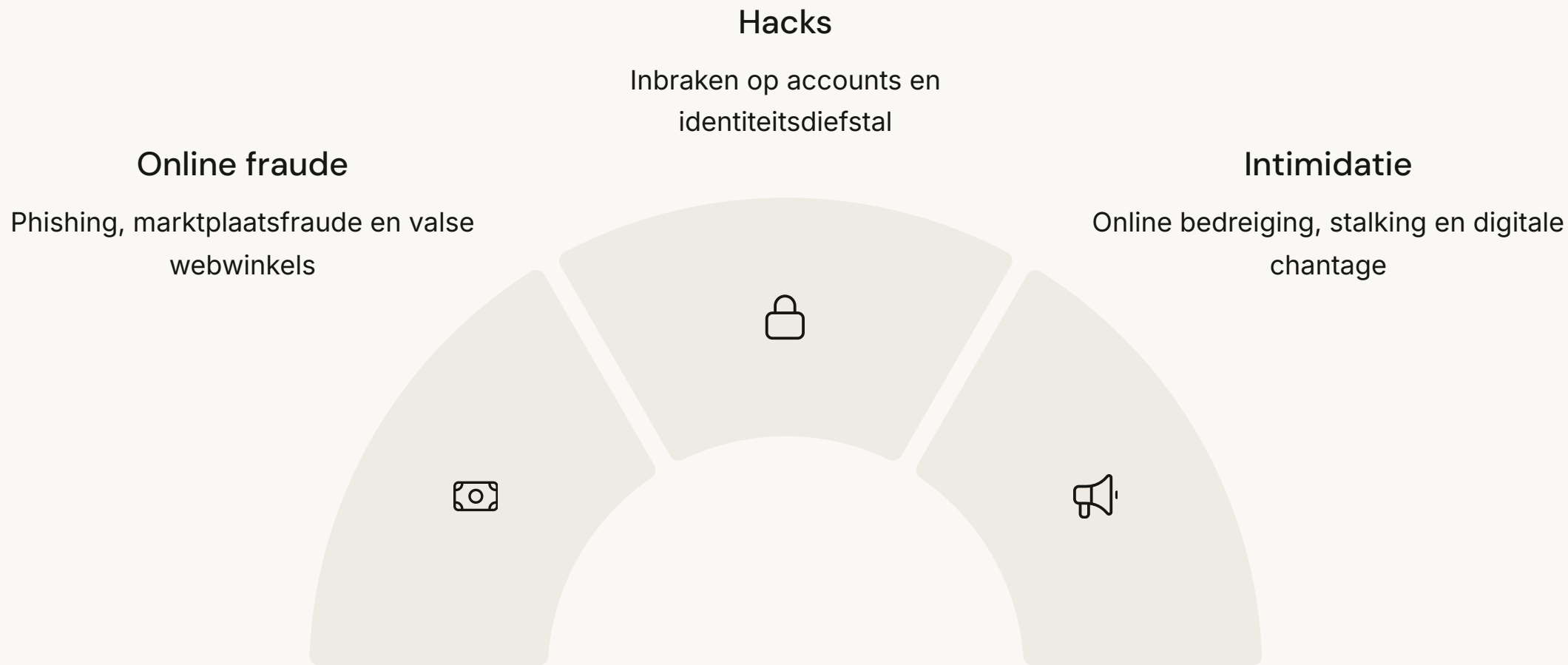
Communicatie

E-mailheaders, chatberichten en profielen van verdachten op sociale platforms.

Technische data

IP-adressen, inlogtijden en metadata die helpen bij identificatie.

Belangrijkste Soorten Internetdelicten





Eerste Reactie bij Online Delict

Blijf kalm

Reageer niet impulsief. Emotionele reacties kunnen bewijs vernietigen of de situatie verergeren.

Documenteer direct

Noteer alle feiten meteen. Schrijf op wat er precies is gebeurd.

Behoud contact

Verbreek contact niet direct als je nog bewijs moet verzamelen.



Essentiële Apparatuur en Hulpmiddelen



Opnameapparatuur

Smartphone of computer met camera voor het maken van screenshots.



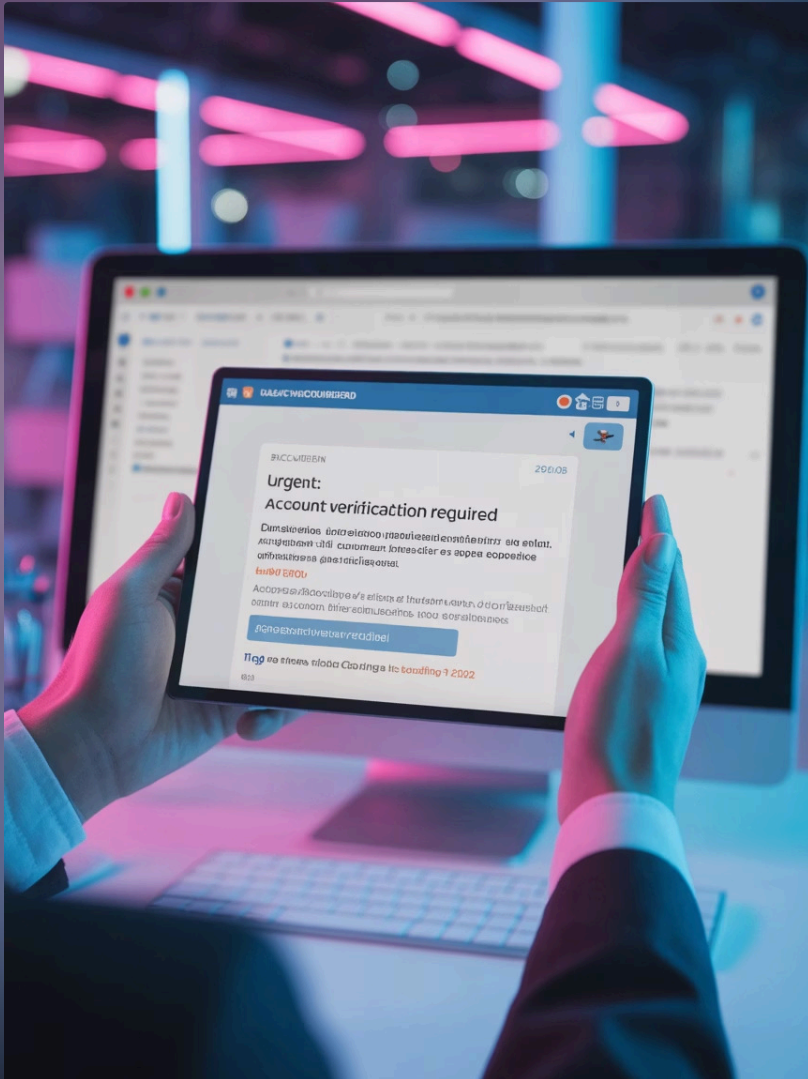
Opslagmiddelen

Cloudopslag of USB-stick voor het veilig bewaren van bewijsmateriaal.



Documentatie

Notitieboek voor het handmatig bijhouden van gebeurtenissen en tijdlijnen.



Bewaren van Digitale Berichten en Mails



Vastleggen

Maak een screenshot van het volledige scherm met alle details zichtbaar.



Documenteren

Noteer datum, tijd, afzender en volledige inhoud van het bericht.



Opslaan

Download originele e-mails inclusief headers voor technisch bewijs.

Chatgesprekken en Social Media



Screenshots

Leg volledige conversaties vast, inclusief datum- en tijdstempels.



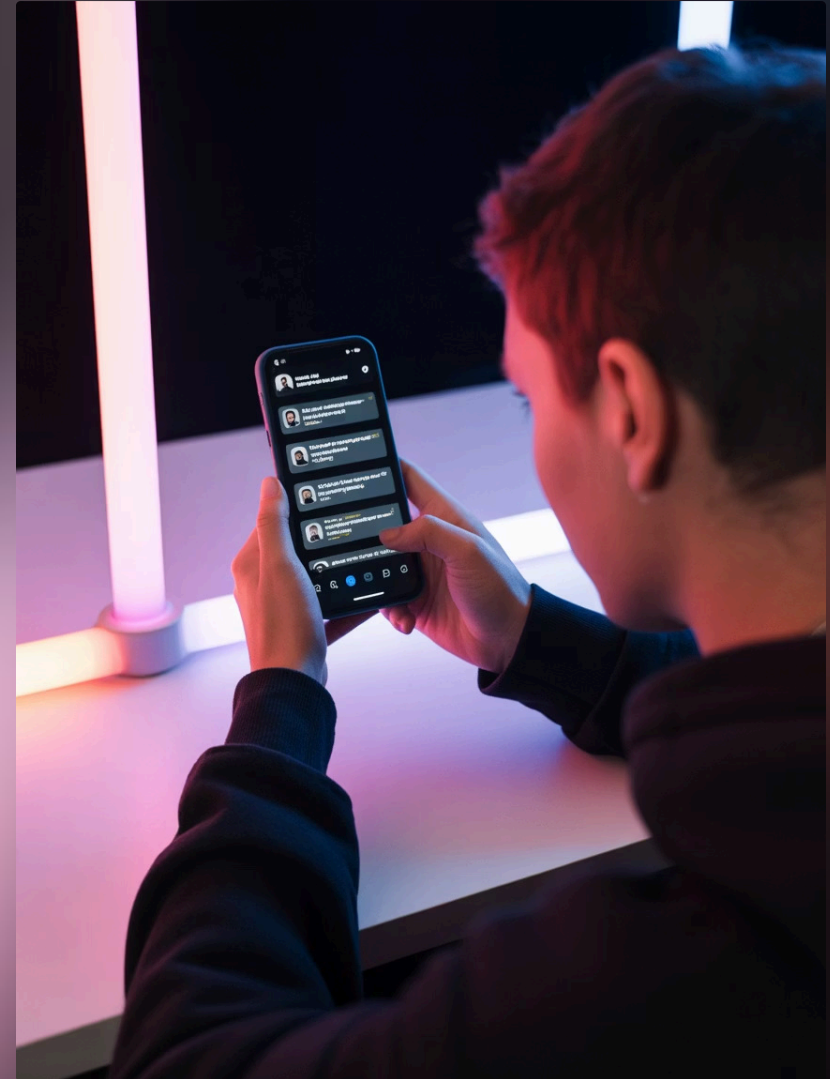
PDF-opslag

Sla belangrijke berichten op als PDF voor duurzame bewaring.



URL's bewaren

Noteer linkjes naar profielen of specifieke berichten.



Het Vastleggen van Webpagina's

1 Screenshot met context

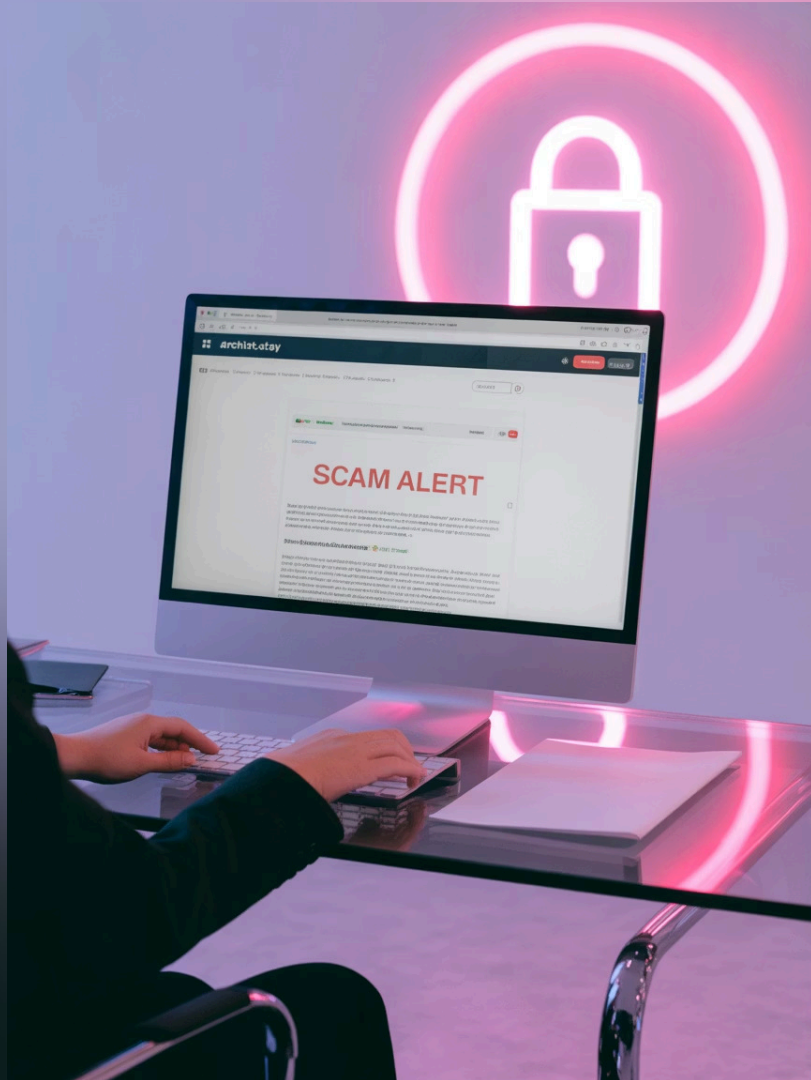
Maak een afbeelding van de hele pagina met zichtbare URL en datum.

2 PDF-export

Gebruik 'Print als PDF' voor het bewaren van complete webpagina's.

3 Archiefopslag

Gebruik diensten zoals archive.today of Wayback Machine voor onafhankelijke kopieën.



Foto's, Video's en Audio



Direct opslaan

Download bestanden meteen na ontvangst



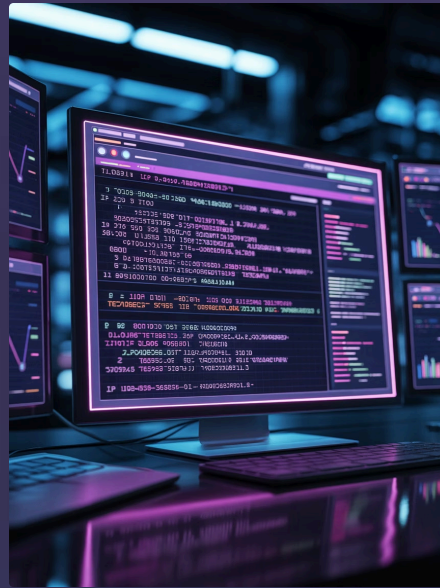
Documenteren

Noteer bij elk bestand de bron en tijd



Backup maken

Maak foto's van berichten op scherm



Logbestanden en Technische Gegevens

Type Gegevens	Hoe Vastleggen	Waarom Belangrijk
IP-adressen	Kopiëren uit e-mailheaders	Locatie en identiteit dader
Inlogtijden	Screenshots van meldingen	Tijdslijn van activiteit
Metadata	Eigenschappen van bestanden bewaren	Technisch forensisch bewijs

Bewijsmateriaal Veilig Bewaren



Delen met de Politie of Meldpunt

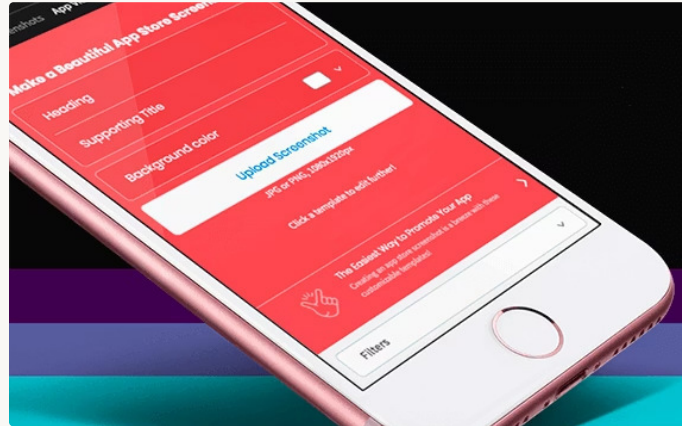


Veelgemaakte Fouten



Te snel verwijderen

Berichten wissen voordat een kopie is gemaakt voor bewijsvoering.



Onvolledige screenshots

Alleen de tekst vastleggen zonder datum, tijd of afzendergegevens.



Onjuist delen

Bewijs verspreiden onder vrienden of familie in plaats van officiële instanties.

Polymorfe Malware: Een Evoluerend Gevaar

In het huidige digitale landschap vormt polymorfe malware een van de meest geavanceerde cyberdreigingen. Deze geavanceerde vorm van kwaadaardige software heeft het unieke vermogen om zijn code of uiterlijk te wijzigen met als primair doel het ontwijken van detectie door beveiligingssoftware.

Door constant te veranderen en zich aan te passen, blijft polymorfe malware een stap voor op traditionele beveiligingsmechanismen. Dit artikel belicht de werking, kenmerken en gevaren van deze evolerende dreiging, evenals strategieën om uw digitale omgeving te beschermen.



Hoe Werkt Polymorfe Malware?

Mutatie-engine

Polymorfe malware gebruikt een geïntegreerde mutatie-engine die de broncode systematisch wijzigt bij elke nieuwe infectie of replicatie. Dit zorgt ervoor dat elke nieuwe versie van de malware een unieke digitale handtekening heeft.

Zelfversleuteling

De malware versleutelt zichzelf met verschillende algoritmes en wijzigt voortdurend de decodeerroutines die nodig zijn om zichzelf uit te voeren. Dit maakt patroonherkenning vrijwel onmogelijk voor beveiligingssoftware.

Consistente Functionaliteit

Ondanks alle veranderingen in uiterlijk en bestandskenmerken blijft de onderliggende functionaliteit van de malware gelijk. De dreiging verandert niet, alleen de manier waarop deze zich presenteert.

Belangrijkste Kenmerken



Door deze combinatie van eigenschappen vormt polymorfe malware een bijzonder uitdagende bedreiging voor cybersecurity-professionals. Terwijl conventionele malware relatief eenvoudig te identificeren is door zijn constante kenmerken, blijft polymorfe malware een bewegend doelwit dat voortdurend nieuwe detectiemethoden vereist.



Bedreigingen & Impact



Systeemprestaties

Kan computersystemen ernstig vertragen door overmatig gebruik van systeembronnen en voortdurende achtergrondactiviteit



Datacorruptie

Risico op permanente beschadiging of verlies van belangrijke gegevens door schadelijke activiteiten



Persistente Infectie

Ontwikkeld om langdurig in systemen te verblijven, zelfs na herhaaldelijke pogingen tot verwijdering



Alarmerende Statistieken

Volgens Webroot gebruikt maar liefst 97% van alle moderne malware een vorm van polymorfisme

Detectie-uitdagingen

Handtekening-ontwikijing

Ontwikt systematisch traditionele detectiemethoden gebaseerd op vaste handtekeningen

Gedragsmonitoring

Effectieve bescherming moet zich richten op abnormaal gedrag in plaats van bekende signatures



Antivirus-ineffectiviteit

Typische antivirusoplossingen schieten tekort door focus op bekende patronen

Heuristische analyse

Moderne detectie vereist geavanceerde heuristiek die verdacht gedrag kan herkennen

De evolutionaire aard van polymorfe malware vereist een fundamenteel andere benadering van cybersecurity. Waar traditionele methoden vaak reactief zijn, moet moderne bescherming proactief en adaptief zijn om deze dynamische bedreigingen het hoofd te bieden.

Preventie & Best Practices



AI-gebaseerde Bescherming

Implementeer beveiligingsoplossingen die gebruik maken van kunstmatige intelligentie en machine learning om abnormaal gedrag te detecteren dat kenmerkend is voor polymorfe malware, zelfs wanneer de code zelf voortdurend verandert.



Regelmatige Updates

Houd alle software, besturingssystemen en beveiligingstools up-to-date met de nieuwste patches en definities om bekende kwetsbaarheden te dichten die door malware kunnen worden uitgebuit.



Bewustzijnstraining

Investeer in uitgebreide cybersecurity-training voor alle medewerkers, met specifieke aandacht voor het herkennen van phishing-pogingen en verdachte links die polymorfe malware kunnen verspreiden.



Endpoint Protection

Implementeer robuuste endpoint protection platforms die gedragsgebaseerde detectie combineren met traditionele beveiligingsmethoden voor een gelaagde verdedigingsstrategie.

Conclusie

Evoluerend Risico

Polymorfe malware blijft zich ontwikkelen en vormt een steeds groeiend risico voor zowel individuen als organisaties. De technologieën achter deze dreigingen worden geavanceerder, waardoor ze moeilijker te detecteren en te bestrijden zijn.

Moderne Bescherming

Effectieve detectie vereist de inzet van geavanceerde beveiligingstechnologieën die verder gaan dan traditionele handtekeninggebaseerde methoden. AI-gestuurde oplossingen en gedragsanalyse zijn essentieel geworden in de strijd tegen polymorfe bedreigingen.

Voortdurende Waakzaamheid

Het belangrijkste wapen tegen polymorfe malware blijft de combinatie van geavanceerde technologie en menselijke waakzaamheid. Proactieve beschermingsmaatregelen, gecombineerd met doorlopende bewustwording en training, vormen de beste verdediging tegen deze veranderende dreigingen.



MICROSOFT'S EUROPESE SECURITY PROGRAM (ESP)

**DIT GRATIS BEVEILIGINGSPROGRAMMA
WERD GELANCEERD OP 4 JUNI 2025. HET
RICHT ZICH OP DE VERSTERKING VAN
CYBERVEILIGHEID IN EUROPA.**

**HET ESP IS BESCHIKBAAR VOOR ALLE 27
EU-LIDSTATEN, KANDIDAAT-LIDSTATEN,
EVA-LANDEN, HET VK, MONACO EN
VATICAANSTAD.**

VEILIGDIGITAAL.COM



ACHTERGROND EN CONTEXT



VOORTZETTING VAN GSP

Het ESP bouwt voort op het bestaande Microsoft Government Security Program.



LANCERING IN BERLIJN

Brad Smith, Microsoft's President, introduceerde het programma in Berlijn.



STRATEGISCHE RESPONS

Het is een reactie op toenemende cyberdreigingen in Europa.

DRIE KERNONDERDELEN VAN ESP



Het programma is volledig kosteloos voor alle deelnemende landen.

Fortress AI:
Proactive Cybersecurity.



Detected threats	Resolved incidents	Vulnerability score
2023-10-01 10:00:00	2023-10-01 10:00:00	2023-10-01 10:00:00
76.6	76.6	76.6
Time: 200.000	Time: 200.000	Time: 200.000
29.02	10.0	1.00
Vulnerability: 0.000	Vulnerability: 0.000	Vulnerability: 0.000
6.00	4.00	9.50

DREIGINGSINFORMATIE EN AI-TECHNOLOGIE



INZICHTEN UIT DREIGINGSINFORMATIE

Rapporten over cybercriminaliteit en staatshackers



AI-ANALYSE

Geavanceerde analyse van cyberdreigingsactiviteiten



REALTIME BESCHERMING

Directe inzichten voor verdediging van regeringen



MICROSOFT'S EXPERTISE

Kennis van Digital Crimes Unit en Threat Analysis Center

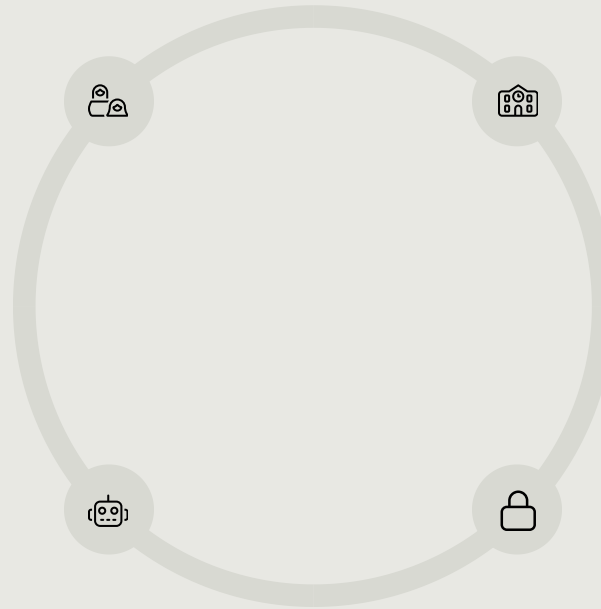
HUIDIGE CYBERDREIGINGEN IN EUROPA

STAATSDREIGINGEN

Aanhoudende dreigingen van landen zoals
Rusland en China

AI-MISBRUIK

Misbruik voor verkenning en social engineering



ACADEMISCHE AANVALLEN

Toenemende aanvallen op onderwijsinstellingen

RANSOMWARE

Groeiende dreiging van Ransomware-as-a-Service
(RaaS)



BREDERE CONTEXT EN TOEKOMST

DATACENTERGROEI

Strategie voor 40% datacentergroei in Europa

BEVEILIGINGSNIVEAU

Focus op verbetering van algemene veiligheid

PARTNERSCHAP

Schouder aan schouder met Europese overheden

LANGETERMIJNVERBINTENIS

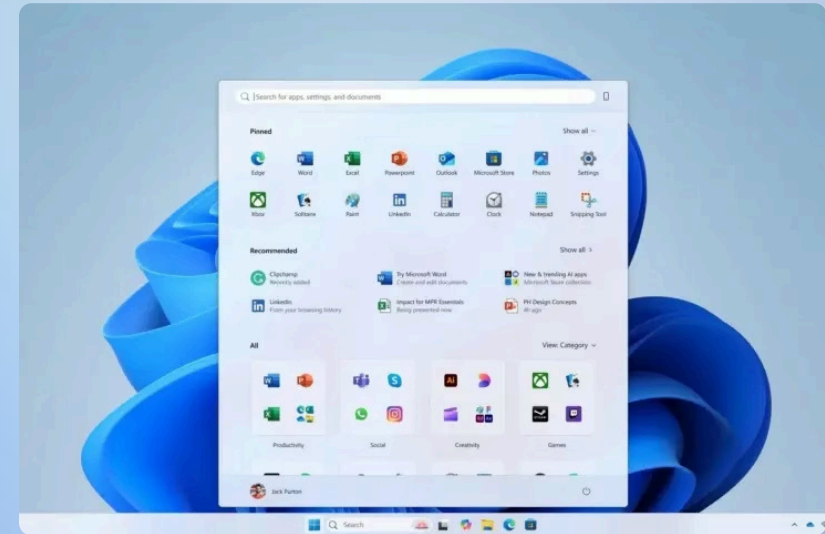
Verdediging van Europa's digitale ecosysteem

Microsoft onthult nieuwe Startmenu-layout in Windows 11

Microsoft heeft een vernieuwde Startmenu-layout voor Windows 11 onthuld. De officiële lancering staat gepland voor later dit jaar.

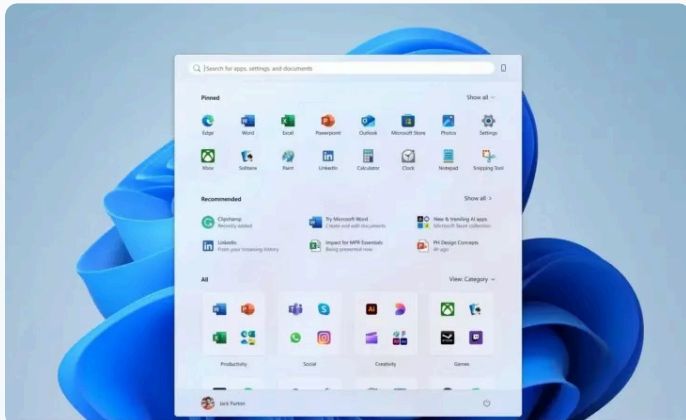
Deze update brengt een samenvoeging van de apps-lijst en vastgemaakte apps. Het vormt een belangrijke stap naar meer personalisatie en eenvoud.

VEILIGDIGITAAL.COM



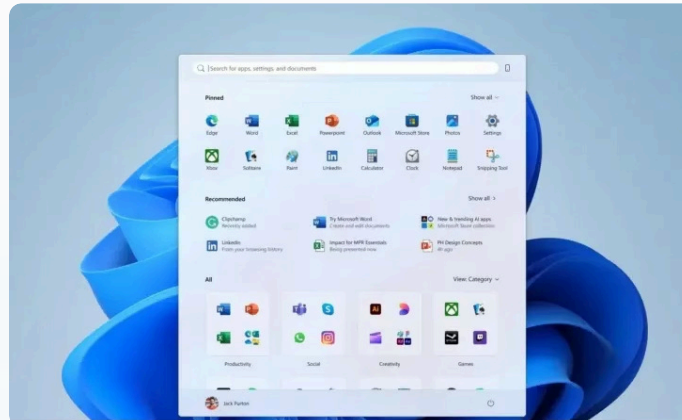
Nieuwe visuele indeling en functies

Het nieuwe Windows 11 startmenu biedt meer ruimte en flexibiliteit met verschillende weergave-opties.



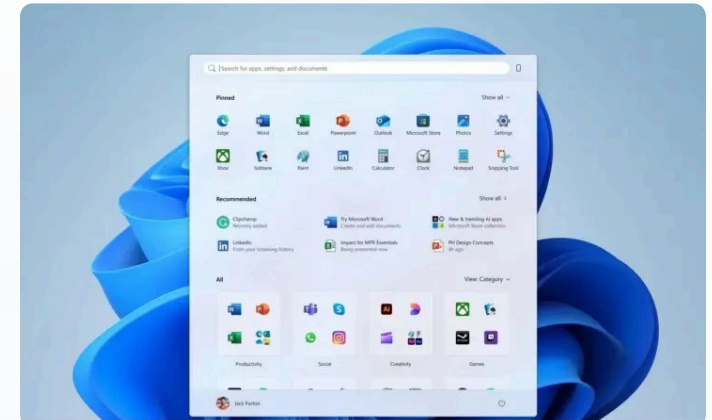
Lijstweergave

De klassieke lijstweergave met "Alle apps"-lijst onderaan en vastgemaakte apps direct zichtbaar bovenaan.



Rasterweergave

Een bredere lay-out met meer ruimte voor vastgemaakte apps in een overzichtelijk raster.



Categorieweergave

Apps georganiseerd per categorie voor snellere navigatie en een gepersonaliseerde ervaring.

Grotere personalisatie en integratie



Uitschakelbaar aanbevolen-gebied

Het "Recommended"-gebied kan nu volledig worden uitgeschakeld. Hierdoor ontstaat ruimte voor meer persoonlijke content.



Automatisch gegroepeerde app- mappen

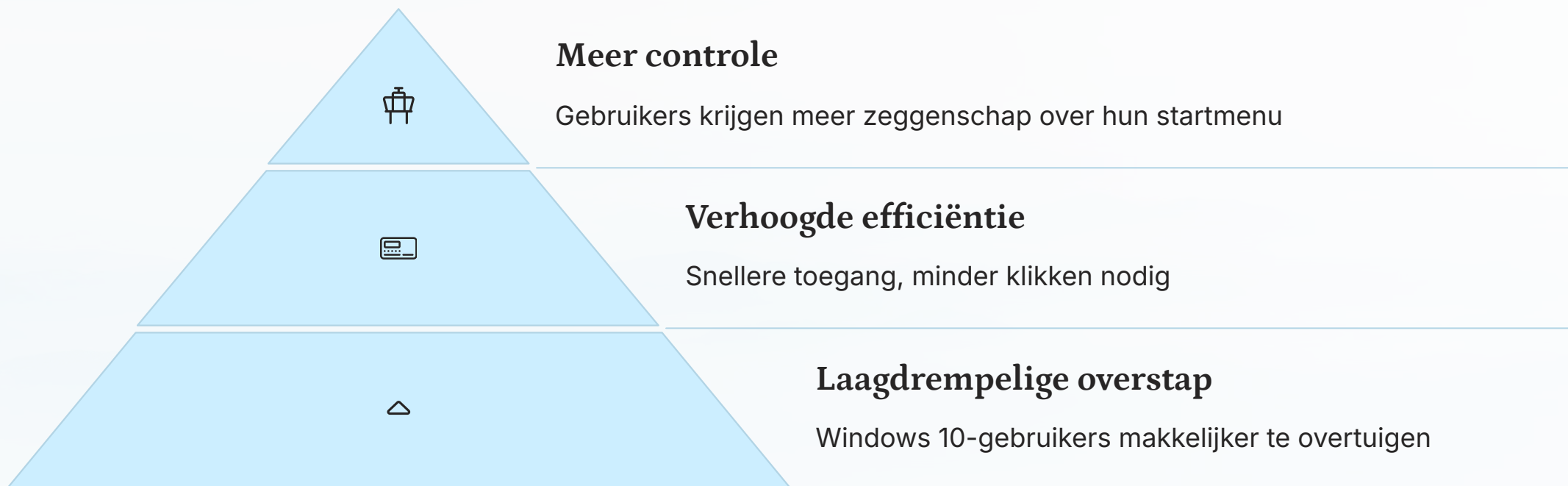
Apps worden automatisch gegroepeerd in mappen. Dit werkt vergelijkbaar met iOS en iPadOS.



Phone Link-companion

De nieuwe companion toont je gekoppelde smartphone. Ook berichten en foto's zijn direct zichtbaar.

Toekomst en impact voor gebruikers



Deze vernieuwing is het begin van bredere veranderingen in de Windows 11-ervaring. Microsoft richt zich op personalisatie en gebruiksgemak.