

VEILIG DIGITAAL MAGAZINE



In dit magazine zijn artikelen bijeengebracht welke onder andere in een eerder stadium zijn gepubliceerd op de website veiligdigitaal.com

Dit magazine verschijnt met onregelmatige tussenpozen meerdere keren per jaar.

Nummer 1 –2025



2FA & MFA: Beveiliging in Lagen

Extra beveiliging bij digitale toegang is essentieel. Tweefactorauthenticatie (2FA) en multifactorauthenticatie (MFA) bieden die bescherming.

In dit artikel leggen wij uit wat deze methoden inhouden. We verkennen waarom ze cruciaal zijn voor je online veiligheid.

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

Twefactorauthenticatie (2FA)



Wat is het?

Twee verschillende authenticatiefactoren zijn vereist. Je hebt beide nodig om toegang te krijgen.

Hoe werkt het?

Na je wachtwoord volgt een tweede stap. Vaak een tijdelijke code via sms of app.

Voorbeeld

Bij internetbankieren voer je je wachtwoord in. Daarna ontvang je een sms-code om de inlog te voltooien.

Multifactorauthenticatie (MFA)



Breder begrip

MFA omvat alle systemen met twee of meer beveiligingsfactoren.



Extra bescherming

Kan méér dan twee factoren combineren voor hogere veiligheid.

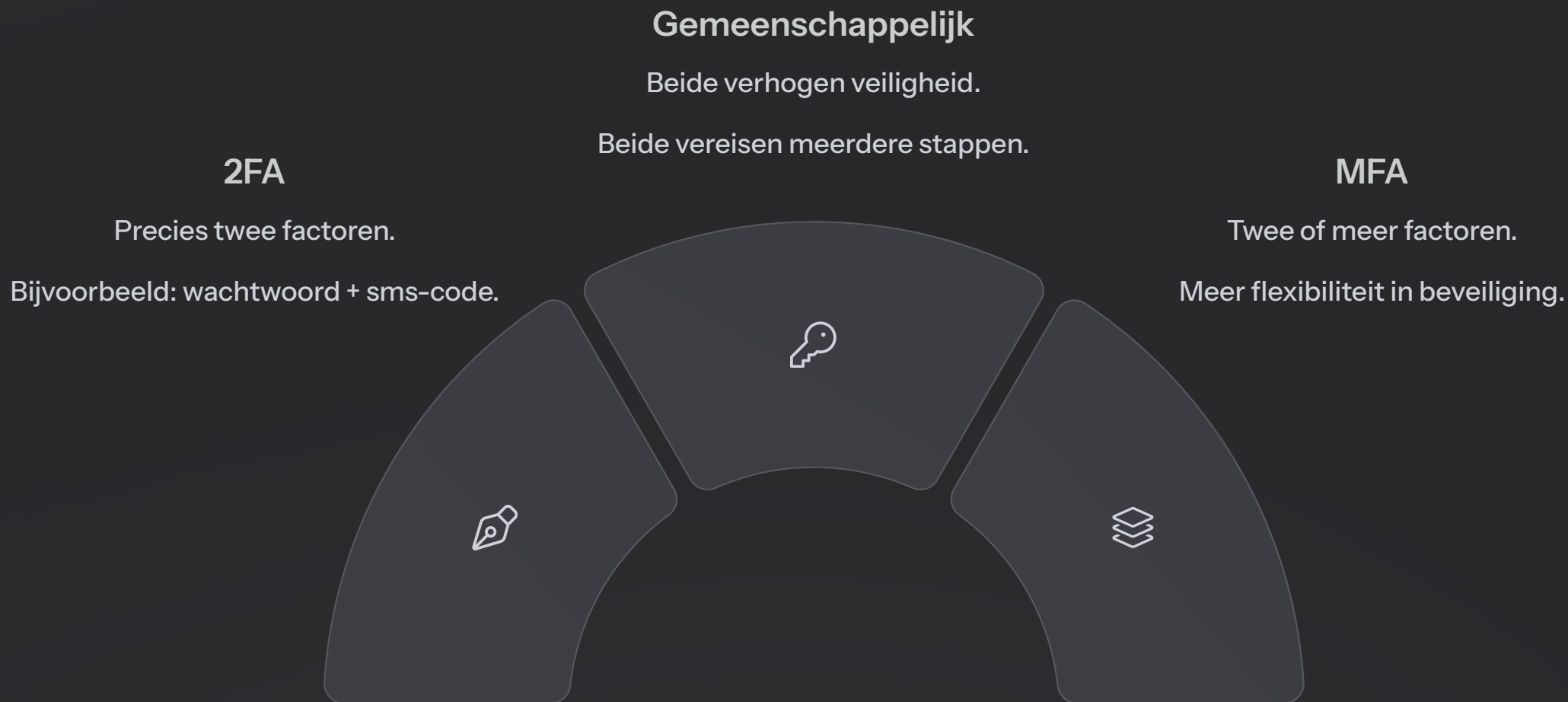


Overkoepelend

2FA is een specifieke vorm van MFA. Alle 2FA is MFA.



2FA vs. MFA: De Verschillen



Authenticatiefactoren Uitgelegd



Wat je weet

Wachtwoorden, pincodes of beveiligingsvragen. Informatie die alleen jij zou moeten kennen.



Wat je hebt

Fysieke apparaten zoals je telefoon, beveiligingstoken of bankpas. Objecten in jouw bezit.



Wat je bent

Biometrische kenmerken zoals vingerafdrukken of gezichtsherkenning. Uniek voor jou.

Populaire 2FA & MFA-methoden



Authenticator-apps

Google Authenticator of Microsoft Authenticator genereren tijdelijke codes. Deze verversen elke 30 seconden.



SMS of e-mail

Eenmalige verificatiecodes verstuurd naar je telefoon of mailbox. Eenvoudig maar effectief.



Fysieke tokens

Apparaatjes zoals YubiKey bieden hoogwaardige beveiliging. Ze werken zonder internetverbinding.



Biometrie

FacelID of vingerafdrukscans zijn gebruiksvriendelijk. Ze combineren gemak met hoge veiligheid.

Waarom 2FA/MFA Gebruiken?

99.9%

Effectiviteit

Microsoft: MFA blokkeert bijna alle account-hacks.

80%

Risicovermindering

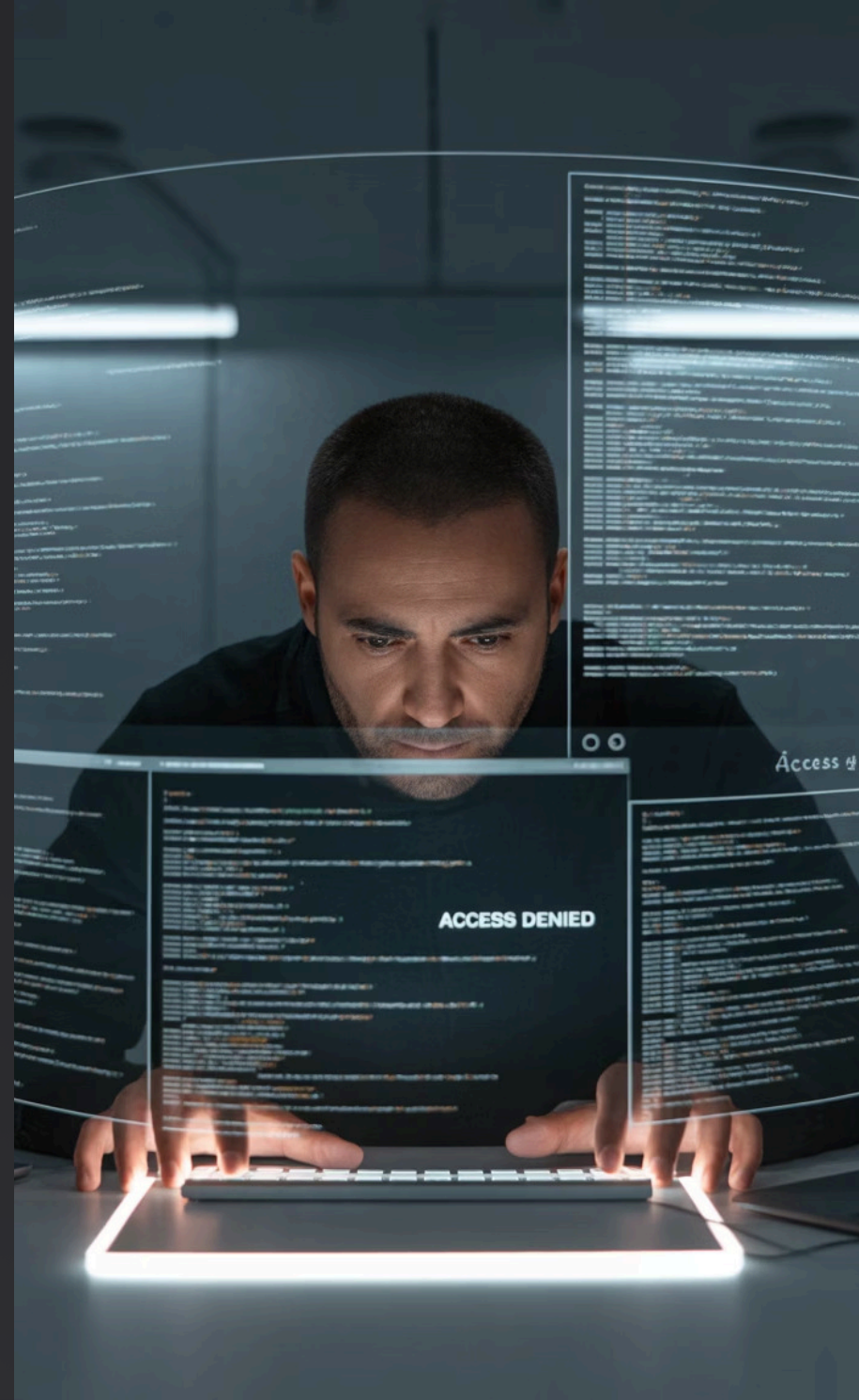
Verlaging van het risico op gegevensdiefstal.

76%

Phishing-bescherming

Percentage phishing-aanvallen dat wordt tegengehouden.

MFA is essentieel voor gevoelige gegevens. Veel banken en overheidsdiensten maken het verplicht.



Samenvatting & Advies



Begin vandaag nog met het instellen van 2FA of MFA. Het kost enkele minuten maar beschermt jarenlang.



AI-washing: Wanneer Technologie een Lege Belofte Wordt

Bedrijven die overdrijven over AI-capaciteiten

Marketingtrucs zonder substantiële technologie

De dunne lijn tussen innovatie en misleiding

VEILIGDIGITAAL.COM

Wat is AI-washing?



Overdrijven van AI-mogelijkheden

Onjuist beeld schetsen van technologische capaciteiten



Bestaande technologie hernoemen

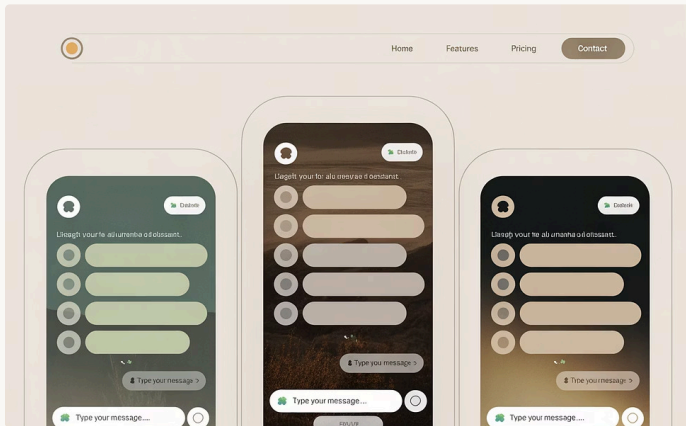
Oude automatisering presenteren als nieuwe AI



Marketing boven substantie

AI-label gebruiken puur voor verkoopvoordeel

Voorbeelden in de Praktijk



ChatGPT-klonen

Apps met nieuwe naam, identieke functionaliteit



Hergelabelde automatisering

Oude functies met nieuwe marketingtermen



"AI-verbeterde" analyses

Traditionele statistiek verkocht als geavanceerde AI

Impact en Gevolgen

Consumentenverwarring
Moeilijk onderscheid tussen echte en valse AI-claims

Innovatieremming
Echte AI-ontwikkelingen ondergesneeuwd



Dalend vertrouwen

Scepsis over alle AI-gerelateerde technologie

Regelgeving risico's

Toenemende kans op overheidsingrijpen



Desktop Snelkoppeling voor Windows Systeemherstel

Een gids voor het maken van een handige snelkoppeling naar Systeemherstel op je Windows bureaublad.

Systeemherstel is een essentiële functie die je computer kan redden in probleemsituaties.

VEILIGDIGITAAL.COM

Het Proces van Koppeling Creëren



Rechtsklik op bureaublad

Begin met een rechtermuisklik op een lege plek op je bureaublad.



Selecteer "Nieuw" en "Snelkoppeling"

Kies in het contextmenu voor "Nieuw" en daarna "Snelkoppeling".



Voer het pad in

Typ %windir%\System32\SystemPropertiesProtection.exe in het invoerveld.



Geef een naam

Noem de snelkoppeling "Systeemherstel" of een andere herkenbare naam.

Windows 11

Voordelen van Systeemherstel Koppeling



Tijdsbesparing

Direct toegang tot systeemherstel zonder door menu's te navigeren.



Proactieve beveiliging

Maak eenvoudig herstelpunten vóór riskante systeemwijzigingen.



Lichte oplossing

De snelkoppeling gebruikt vrijwel geen opslagruimte op je harde schijf.



Tips voor Probleemoplossing

Preventieve maatregelen

Maak altijd een herstelpunt aan voordat je drivers of software installeert.

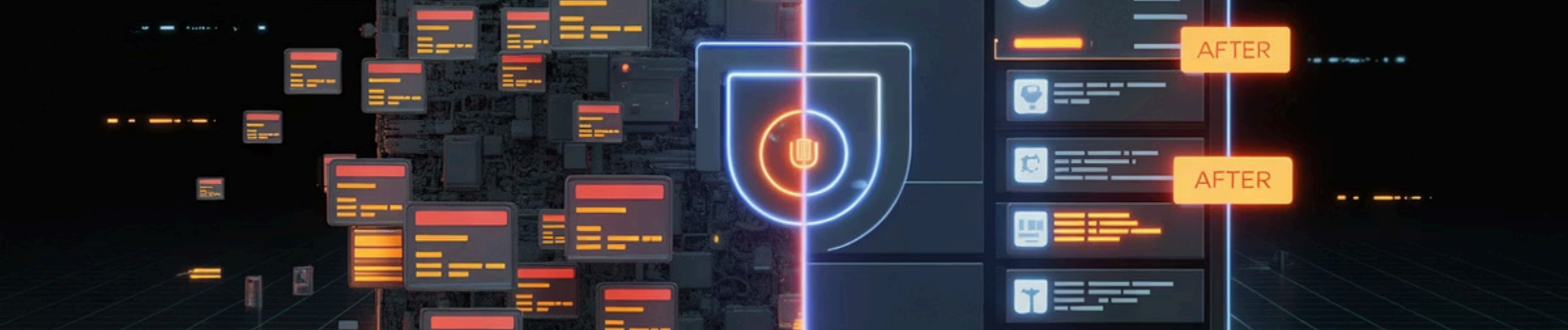
Logbestanden controleren

Bekijk systeemlogbestanden om problemen te diagnosticeren voordat je herstelt.

Updates bijhouden

Controleer regelmatig of er Windows-updates beschikbaar zijn.





Praktische Voorbeelden

1

Driver installatie

Maak een herstelpunt voordat je nieuwe hardware drivers installeert.

2

Problematische update

Gebruik systeemherstel om terug te keren na een problematische Windows update.

3

Software conflicten

Los conflicten op door terug te keren naar een werkende systeemstaat.

Veiligheid en Data Bescherming

Persoonlijke bestanden blijven veilig

Systeemherstel verandert alleen systeembestanden, niet je documenten.

Schijfruimte beheer

Windows beheert automatisch de ruimte voor herstelpunten.



Configuratie herstellen

Alleen systeeminstellingen en geïnstalleerde programma's worden aangepast.

Selectieve bescherming

Je kunt specifieke mappen uitsluiten van het herstelproces.

Best Practices voor Systeemherstelpunten





Conclusie

Veiligheidsmaatregel

Systeemherstel is je vangnet bij computerproblemen. Gebruik het proactief.

Efficiënte toegang

De desktop snelkoppeling bespaart tijd in stressvolle situaties.

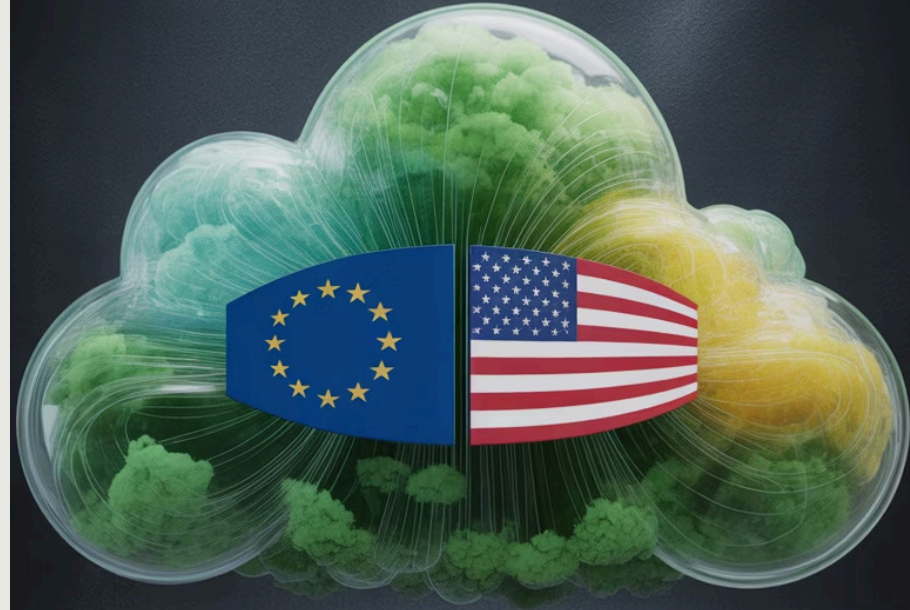
Complete beveiliging

Combineer systeemherstel met regelmatige back-ups voor maximale veiligheid.

ALTERNATIEVEN OM JE DATA UIT DE AMERIKAANSE CLOUD TE HOUDEN

Europese bedrijven zoeken steeds vaker naar alternatieven voor Amerikaanse cloudopslag. Data-soevereiniteit en compliance worden belangrijker in het huidige digitale landschap.

VEILIGDIGITAAL.COM





DE DOMINANTIE VAN AMERIKAANSE CLOUDPROVIDERS

70%+

MARKTAANDEEL

AWS, Microsoft en Google beheersen samen meer dan 70% van de cloudmarkt.

85%

OVERHEIDSDATA

Percentage Nederlandse overheidsdata opgeslagen in Amerikaanse cloudsysteem.

92%

ZAKELIJKE SECTOR

Europese bedrijven die afhankelijk zijn van minstens één Amerikaanse cloudprovider.

RISICO'S VAN AMERIKAANSE CLOUDDIENSTEN



CLOUD ACT IMPACT

Amerikaanse overheid kan gegevens opeisen.



GEOPOLITIEKE KWETSBAARHEID

Risico op sancties of blokkades bij internationale spanningen.



GDPR-BOETES

Miljoenenboetes bij compliance-schendingen.

EUROPESE ZORGEN EN OVERHEIDSBELEID

1

NATIONALE VEILIGHEIDSRISICO'S

Rapporten waarschuwen voor toenemende afhankelijkheid van buitenlandse technologie.

2

OVERHEIDSINITIATIEVEN

Stimuleringsmaatregelen voor Europese cloudaanbieders door verschillende lidstaten.

3

REKENKAMER WAARSCHUWT

Kritische dienstverlening staat op het spel bij te grote afhankelijkheid.

DATA SOVEREIGNTY

EUROPESE ALTERNATIEVEN: HUIDIGE STAND VAN ZAKEN



EUROPESE PROVIDERS

OVHcloud (Frankrijk), Deutsche Telekom (Duitsland) en Scaleway (Frankrijk) bieden Europese alternatieven voor cloudopslag en -diensten.



GAIA-X INITIATIEF

Europees samenwerkingsverband voor open en transparante cloudinfrastructuur. Standaardisatie en interoperabiliteit staan centraal.



UITDAGINGEN

Europese oplossingen hebben nog niet dezelfde schaal en functionaliteit als Amerikaanse tegenhangers, wat adoptie belemmert.

'EUROPESE' CLOUDOPLOSSINGEN VAN AMERIKAANSE AANBIEDERS



SOVEREIGN CLOUD OPLOSSINGEN

AWS, Google en Microsoft bieden specifieke diensten voor Europese data-opslag.



ONZEKERE BESCHERMING

Juridische onduidelijkheid over daadwerkelijke onafhankelijkheid van Amerikaanse wetgeving.



LOKALE DATACENTERS

Fysieke opslag in Europa, maar software en beheer vaak nog Amerikaans.

PRAKTISCHE ALTERNATIEVEN EN STRATEGIEËN

MULTI-CLOUD STRATEGIE

Combineer meerdere aanbieders voor risicospreiding.

OPEN SOURCE OPLOSSINGEN

Nextcloud en ownCloud bieden controle over je eigen data.



ENCRYPTIE

Versleutel data lokaal voordat deze naar de cloud gaat.

RISICOANALYSE

Bepaal welke data kritisch is en specifieke bescherming vereist.



SAMENVATTING & AANPAK VOOR DE TOEKOMST

BEWUSTE KEUZES MAKEN

Analyseer risico's en compliancevereisten voor je specifieke situatie. Niet alle data vereist dezelfde bescherming.

GEFASEERDE OVERGANG

Stap voor stap migreren naar veiliger alternatieven. Begin met de meest gevoelige data.

BLIJF OP DE HOOGTE

Europese cloudmarkt evolueert snel door nieuwe regelgeving. Verwacht meer lokale opties.

CLOUD ALTERNATIEVEN

Alternatieven voor Amerikaanse clouddiensten: aanbevelingen

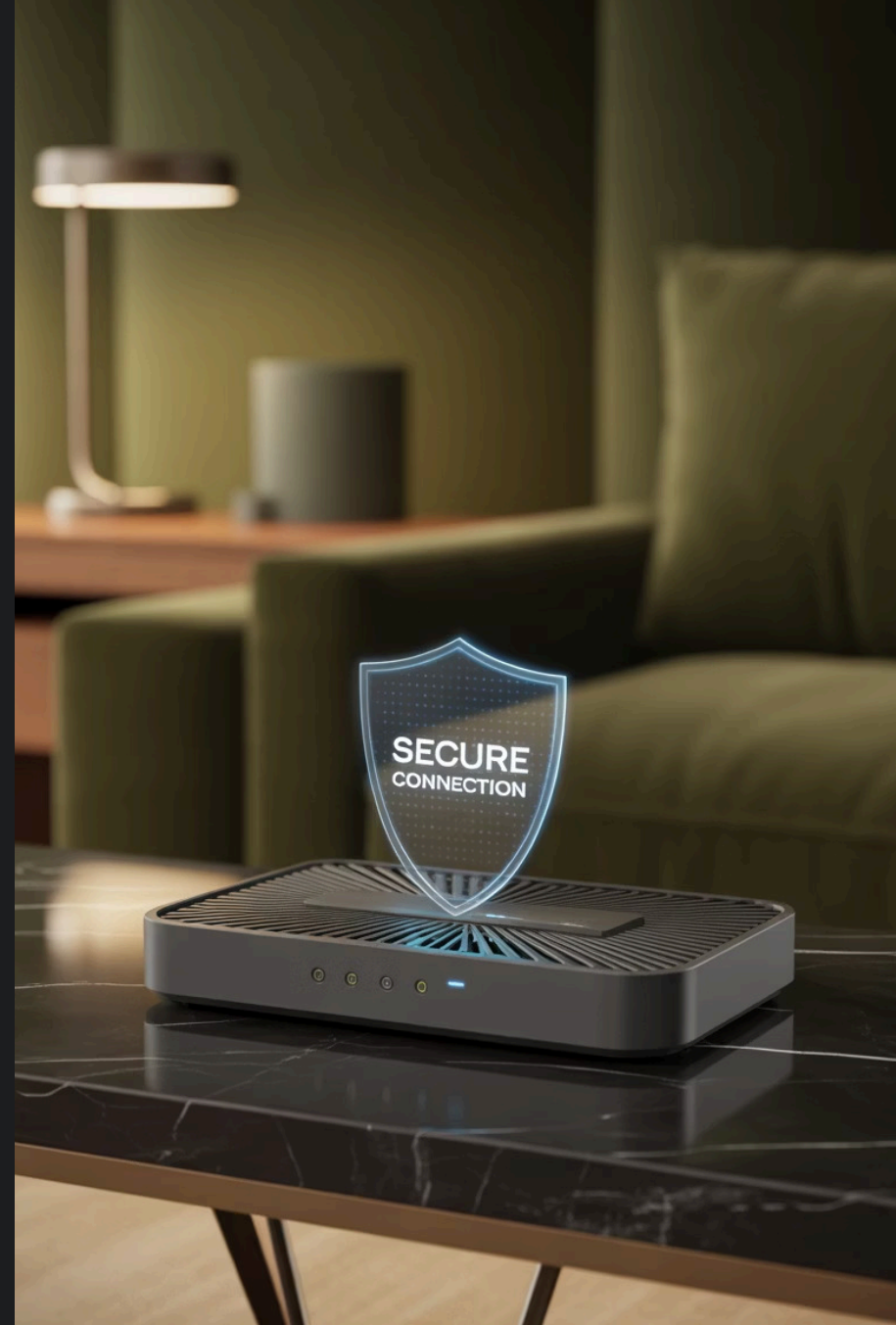
Toepassing	Amerikaanse dienst	Alternatief	Opmerking
Adresboek	Google, iCloud	Nextcloud, div. mailhosters (zie e-mail)	
Agenda	Google Calendar, iCloud	Nextcloud, div. mailhosters (zie e-mail)	
AI	ChatGPT, Claude	Mistral	diverse hosters bieden non VS-AI als service
Bestanden synchroniseren	Dropbox, Google Drive, OneDrive , iCloud	Nextcloud, Strato HiDrive, div. mailhosters (zie e-mail)	ook zelf te hosten, bijvoorbeeld software als Syncthing
Chatserver	Slack	Nextcloud, Mattermost, Matrix	
E-mail	Outlook, Google Mail, Yahoo ...	Posteo, mailbox.org, ProtonMail, Tuta, div. hosters	soms met extra opties als agenda, adresboek, bestandssync en het delen en bewerken van officedocumenten
Foto-opslag	Google Photo, iCloud	Immich	andere oplossing: bestandssynchronisatie
Groupware	Exchange	Grommunio, Kopano Cloud, Open-Xchange	bevatten niet de volledige Exchange-functieomvang
Hyperscaler	AWS, Azure, Google Cloud	StackIT, div. hosters	alternatieven vaak gebaseerd op Kubernetes of OpenStack
Kaartdienst	Google Maps, Bing Maps	Here, OpenStreetMap, OsmAnd Maps	
Messenger	WhatsApp	Threema, Element (Matrix), XMPP (Jabber)	
Muziekstreaming	Apple Music	Spotify, Deezer, Qobuz, SoundCloud	Spotify: oprichter doneerde aan Trump-campagne
Notities	OneNote	Joplin, Obsidian	
Office online	M365	Nextcloud	Nextcloud gebruikt OnlyOffice of Collabora Online; div. mailhosters bieden vergelijkbare functies
Smarthome	Apple Home, Google Home	Home Assistant, HomeBridge, OpenHab, ioBroker, Domoticz	allemaal zelf te hosten en geschikt om bestaande componenten te integreren
Socialemedia	X, Facebook, Instagram, Reddit, LinkedIn, YouTube	Mastodon, Pixelfed, Lemmy, Quodari, Xing, PeerTube	
Versiebeheer	GitHub	Codeberg, Radicle, Forgejo	
Videogames	Steam	gog.com	DRM-vrij
Videoconferenties	Teams, Zoom, Google Talk	Nextcloud, Jitsi Meet, BigBlueButton, OpenTalk	meestal mindere integratie van e-mail, office e.d.
Videostreaming	Netflix, Amazon Prime, Disney, Paramount+, Apple-TV+	Filmfriend, Sooner, Mubi, Joyn	
Zoekmachine	Google, Bing	Ecosia, Good Search, SearXNG, Qwant, metaGer	

Essentiële Router-instellingen voor Optimale Veiligheid

Een nieuwe wifi-router in huis betekent niet automatisch veilig internet. Door enkele cruciale instellingen aan te passen, kun je je netwerk aanzienlijk beter beschermen tegen ongewenste toegang en cyberaanvallen.

In dit artikel bespreken we vijf essentiële aanpassingen die je direct moet doorvoeren na de installatie van je nieuwe router. Deze eenvoudige stappen vormen samen een solide basis voor een veilige thuisnetwerkomgeving.

VEILIGDIGITAAL.COM



Verander het Standaardwachtwoord

Standaard Combinaties

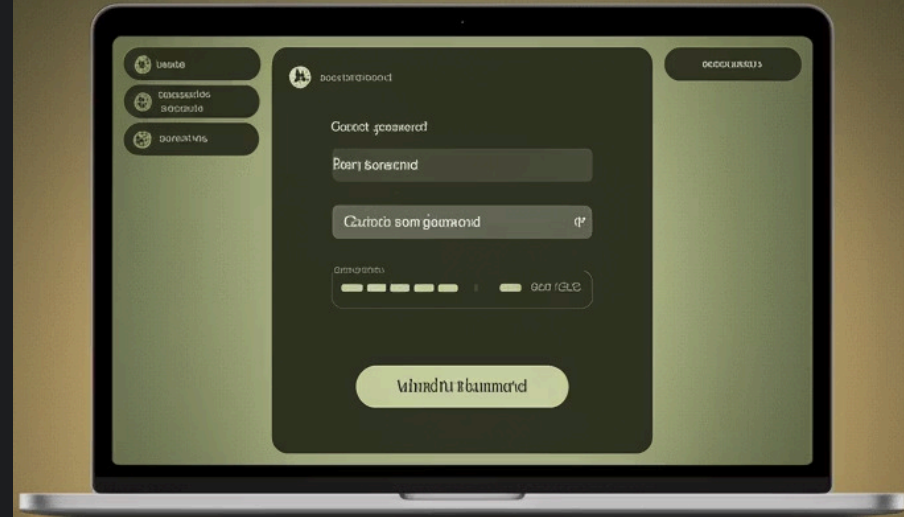
Routers komen vaak met voorspelbare combinaties zoals "admin/admin" of "admin/1234", die hackers op grote schaal proberen.

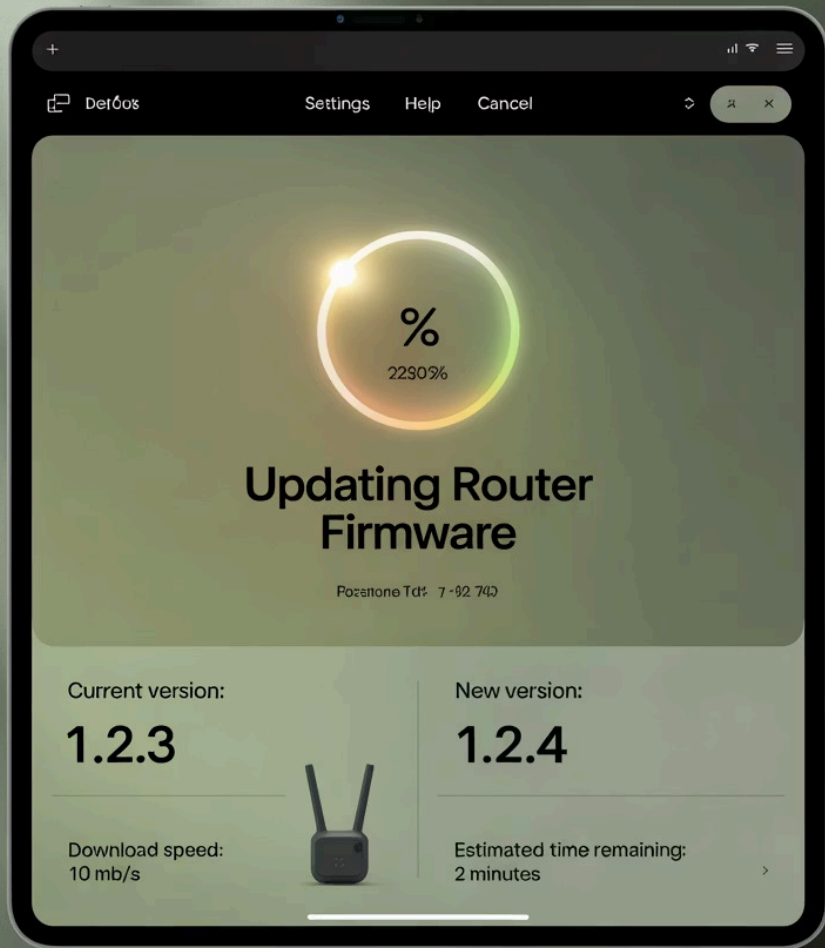
Beheerderswachtwoord

Dit is niet je wifi-wachtwoord, maar geeft toegang tot de router-instellingen. Een zwak wachtwoord hier maakt je hele netwerk kwetsbaar.

Sterke Alternatieven

Kies een uniek, complex wachtwoord en bewaar het op een veilige plaats voor toekomstig gebruik.





Houd Firmware Up-to-date



Controleer Updates

Verifieer of je router de nieuwste firmware heeft, vooral als het apparaat al even op de plank lag.



Beveiligingsvoordelen

Updates dichten beveiligingslekken en maken het hackers moeilijker om toegang te krijgen tot je netwerk.



Extra Functionaliteit

Naast verbeterde beveiliging krijg je vaak nieuwe functies bij firmware-updates.

Personaliseer je Netwerdnaam



Standaard SSID Risico's

Namen als "D-Link_3F9A" of "KPN1234" verraden je routertype, wat gerichte aanvallen vergemakkelijkt.



Kies een Unieke Naam

Verander je netwerdnaam naar iets dat geen informatie over je router prijsgeeft, zoals "HomeInternet7" of "WifiVanHuis8".



Sterk Wifi-wachtwoord

Gebruik een lang, uniek wachtwoord met een combinatie van woorden die niet voor de hand ligt. De lengte is belangrijker dan complexiteit.



Optimale Versleuteling Kiezen

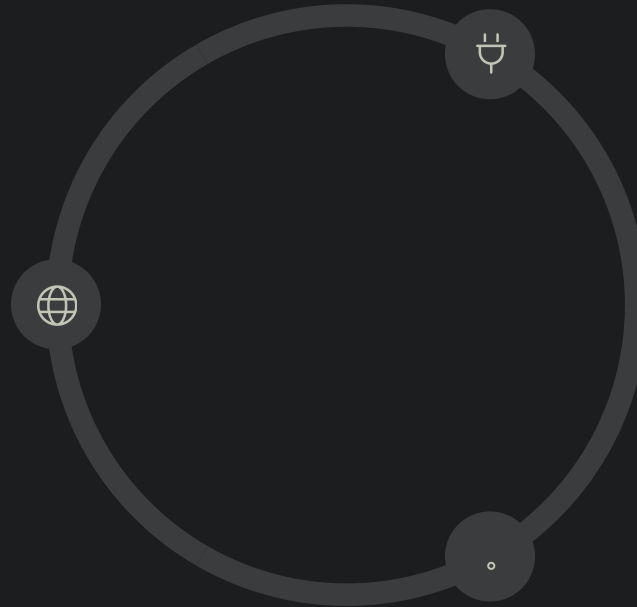


Controleer in je router-instellingen welke versleutelingsmethode actief is. Kies bij voorkeur voor WPA3, de meest geavanceerde en veilige optie. Als je oudere apparaten hebt die problemen hebben met WPA3, kun je vaak een gemengde modus (WPA3 + WPA2) activeren voor maximale compatibiliteit zonder te veel in te leveren op veiligheid.

Schakel Risicovolle Functies Uit

Extern Beheer via WAN

Maakt beheer van buitenaf mogelijk, maar creëert onnodige toegangspunten voor hackers.



UPnP

Laat apparaten automatisch poorten openen, wat tot beveiligingsproblemen kan leiden.

WPS

Maakt snelle verbinding via pincode mogelijk, maar is relatief eenvoudig te kraken.

Veel routers bevatten functies die bedoeld zijn voor gebruiksgemak, maar in de praktijk vooral beveiligingsrisico's vormen. Controleer je instellingen en schakel deze opties uit voor een veiliger netwerk.



Voordelen van Goede Router-beveiliging

99%

Bescherming

Percentage aanvallen dat wordt afgeweerd met juiste instellingen

24/7

Bewaking

Continue beveiliging van je thuisnetwerk

100+

Apparaten

Gemiddeld aantal verbonden apparaten in moderne huishoudens tegen 2025

Een goed beveiligde router vormt de eerste verdedigingslinie tegen cyberaanvallen op je thuisnetwerk. Met het toenemende aantal slimme apparaten in onze woningen wordt deze beveiliging steeds belangrijker. Door de juiste maatregelen te nemen, bescherm je niet alleen je gegevens, maar ook je privacy en die van je gezin.

Samenvatting: Essentiële Router-beveiligingsstappen

Verander Standaardwachtwoord en

Zowel het beheerderswachtwoord als het wifi-wachtwoord moeten uniek en sterk zijn.

Update Firmware Regelmatig

Controleer op updates en installeer deze om beveiligingslekken te dichten.

Personaliseer Netwerkinstellingen

Kies een unieke netwerknaam en gebruik WPA3-versleuteling waar mogelijk.

Schakel Risicovolle Functies Uit

Deactiveer UPnP, WPS en extern beheer voor optimale veiligheid.

Door deze eenvoudige maar effectieve stappen te volgen, creëer je een aanzienlijk veiliger thuisnetwerk. Neem de tijd om je router correct in te stellen - het is een kleine investering die grote problemen kan voorkomen.

Blackbox aanval op geldautomaten: een analyse

In de digitale wereld van vandaag zijn geldautomaten (ATM's) een integraal onderdeel van onze financiële systemen. Ze bieden gebruikers de mogelijkheid om toegang te krijgen tot hun geld, transacties uit te voeren en verschillende bankdiensten te gebruiken.

Echter, zoals bij elke technologie, zijn geldautomaten niet immuun voor misbruik en fraude. Een van de meest verontrustende vormen van aanvallen op deze machines is de zogenaamde "blackbox aanval". In dit artikel bespreken we wat een blackbox aanval is, hoe deze wordt uitgevoerd, de gevolgen ervan en de maatregelen die genomen kunnen worden om dergelijke aanvallen te voorkomen.

VEILIGDIGITAAL.COM



Wat is een Blackbox Aanval?



Definitie

Een blackbox aanval is een techniek waarbij criminelen gebruikmaken van een extern apparaat (de "blackbox") om toegang te krijgen tot de interne systemen van een geldautomaat. Het doel van deze aanvallen is meestal om contant geld of gevoelige informatie van de geldautomaat te stelen.



Betekenis van de term

De term "blackbox" verwijst naar het feit dat de aanvaller geen directe toegang heeft tot de interne componenten van de geldautomaat; in plaats daarvan gebruiken ze een externe interface om de functionaliteit van de machine te manipuleren.



Doel van de aanval

Met deze techniek kunnen aanvallers de transactieprocessen omzeilen zonder diepgaande technische kennis van de machine zelf. Het uiteindelijke doel is om de geldautomaat te manipuleren zodat deze geld uitgeeft zonder geautoriseerde transacties.

Hoe Wordt een Blackbox Aanval Uitgevoerd?



Onderzoek en Planning

De aanvaller begint met het onderzoeken van geldautomaten. Dit kan inhouden dat ze de omgeving scannen op beveiligingscamera's, personeel en andere mogelijke getuigen. De aanvaller probeert ook te bepalen welk type geldautomaat is betrokken en welke beveiligingsmaatregelen zijn getroffen.



Creëren van de Blackbox

De criminelen bouwen een apparaat, vaak een laptop of een speciaal ontworpen software-hardware combinatie, die in staat is om te communiceren met de geldautomaat. Dit apparaat kan verschillende functies hebben, zoals het nabootsen van de software van de geldautomaat, het manipuleren van signalen of het interfacing met de interne software.



Fysieke Toegang

Bij sommige blackbox aanvallen is het nodig om fysiek toegang te krijgen tot de geldautomaat. De aanvaller kan de machine openen of toegang verkrijgen tot de interne poorten die de communicatie tussen het apparaat en de geldautomatensystemen mogelijk maken.



Manipulatie van de Transactie

Zodra de blackbox is verbonden met de geldautomaat, kan de aanvaller commando's geven die de machine doen denken dat legitieme transacties worden uitgevoerd. Dit kan leiden tot het onterecht uitgeven van contant geld.



Diefstal en Ontsnapping

Na de misdaad is gepleegd, kan de aanvaller snel ontsnappen, vaak met een aanzienlijke hoeveelheid geld, voordat het ongebruikelijke gedrag van de geldautomaat opgemerkt kan worden.

Voorbeeldscenario

1 Doelwitselectie

Stel je voor dat een criminelen-team een geldautomaat in een afgelegen restaurant heeft uitgekozen. Na zorgvuldig onderzoek ontdekken ze dat het personeel 's nachts weinig in de buurt is.

2 Voorbereiding

Ze ontwikkelen een apparaat dat de communicatie met de geldautomaat kan onderscheppen en manipuleren.

3 Uitvoering

's Nachts, wanneer het restaurant gesloten is, gebruiken ze hun blackbox om de geldautomaat te openen.

4 Manipulatie

Ze sluiten hun apparaat aan op de interne poorten van de machine en geven valse commando's door.

5 Resultaat

De geldautomaat begint geld uit te geven zonder dat er daadwerkelijke banktransacties plaatsvinden.

Dit scenario illustreert de effectiviteit van de blackbox-aanval en hoe relatief eenvoudig het kan zijn voor goed voorbereide criminelen.

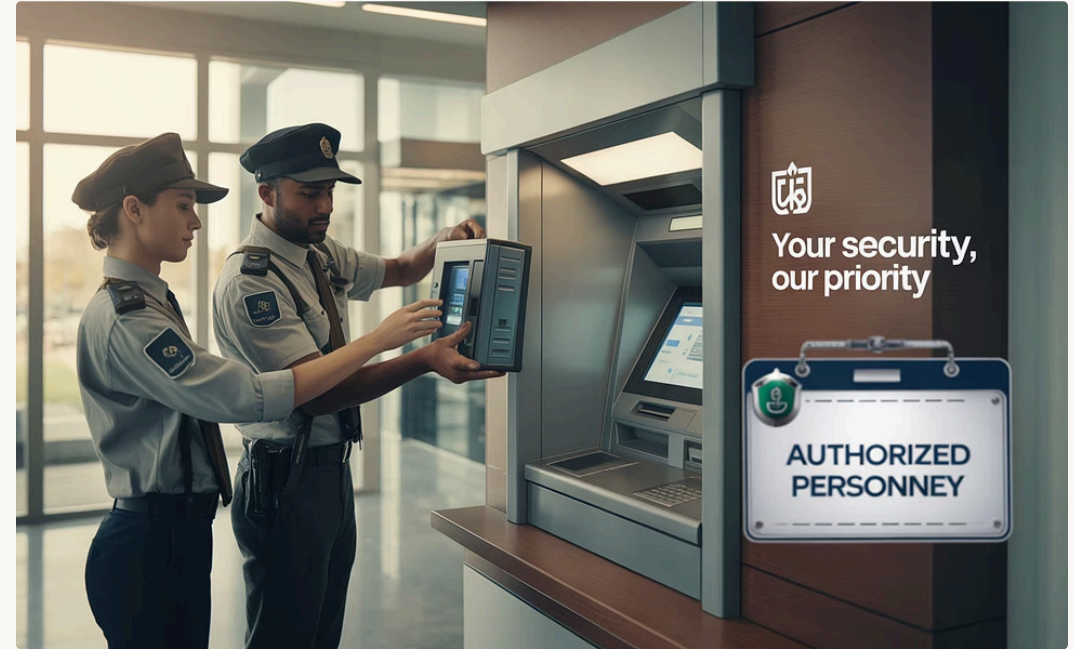
Gevolgen van een Blackbox Aanval: Financiële Impact



Financiële Verliezen

Banken kunnen aanzienlijke verliezen lijden door de diefstal van contant geld. Dit kan ook leiden tot hogere kosten voor het herstellen van de schade en het verbeteren van de beveiliging.

De financiële gevolgen van blackbox aanvallen strekken zich uit van directe verliezen tot langetermijninvesteringen in beveiliging.



Verhoogde Beveiligingsmaatregelen

Banken moeten mogelijk aanzienlijke investeringen doen in beveiligingssystemen en anti-fraudetechnologieën om toekomstige aanvallen te voorkomen.

Preventieve Maatregelen



Fysieke Beveiliging

Geldautomaten moeten worden uitgerust met sterke fysieke beveiliging zoals camera's, alarmsystemen en stevige behuizingen die moeilijker toegankelijk zijn voor onbevoegden.



Software-updates en Patches

Banken moeten regelmatig de software van geldautomaten bijwerken met de nieuwste beveiligingspatches om bekende kwetsbaarheden te verhelpen en de algehele beveiliging van de systemen te verbeteren.



Bewustwording en Training

Werknemers van de bank en het onderhoudspersoneel moeten goed opgeleid worden in het herkennen van mogelijke signalen van een blackbox aanval en andere vormen van fraude.



Regelmatige Onderhoud en Inspectie

Regelmatige inspecties en onderhoud van geldautomaten kunnen helpen om verdachte apparatuur of mogelijke kwetsbaarheden te detecteren en aan te pakken voordat ze kunnen worden uitgebuit.



Beveiligde Communicatie

Geldautomaten moeten gebruik maken van beveiligde communicatieprotocollen om data-inbreuken en manipulaties vanuit externe apparaten te voorkomen.



Gebruik van Biometrische Technologie

Het implementeren van biometrische identificatietechnologieën, zoals vingerafdruk- of gezichtsherkenning, kan de toegang tot geldautomaten verder beveiligen.



Technische Beveiligingsmaatregelen



Encryptie

Versleuteling van alle communicatie tussen de geldautomaat en de bank.



Monitoring

Real-time bewaking van ongebruikelijke activiteiten.



Biometrie

Identificatie via vingerafdruk of gezichtsherkenning.



Fysieke Beveiliging

Verbeterde sloten en toegangscontrole.

Het implementeren van deze technische beveiligingsmaatregelen kan de kwetsbaarheid van geldautomaten voor blackbox aanvallen aanzienlijk verminderen. Door meerdere lagen van beveiliging te combineren, wordt het voor criminelen steeds moeilijker om succesvol een aanval uit te voeren.

Bewustwording voor Consumenten



Let op verdachte apparaten

Controleer de geldautomaat op ongebruikelijke onderdelen of bevestigingen



Bescherm je pincode

Houd je hand over het toetsenbord tijdens het invoeren



Meld onregelmatigheden

Informeer de bank direct bij verdachte transacties

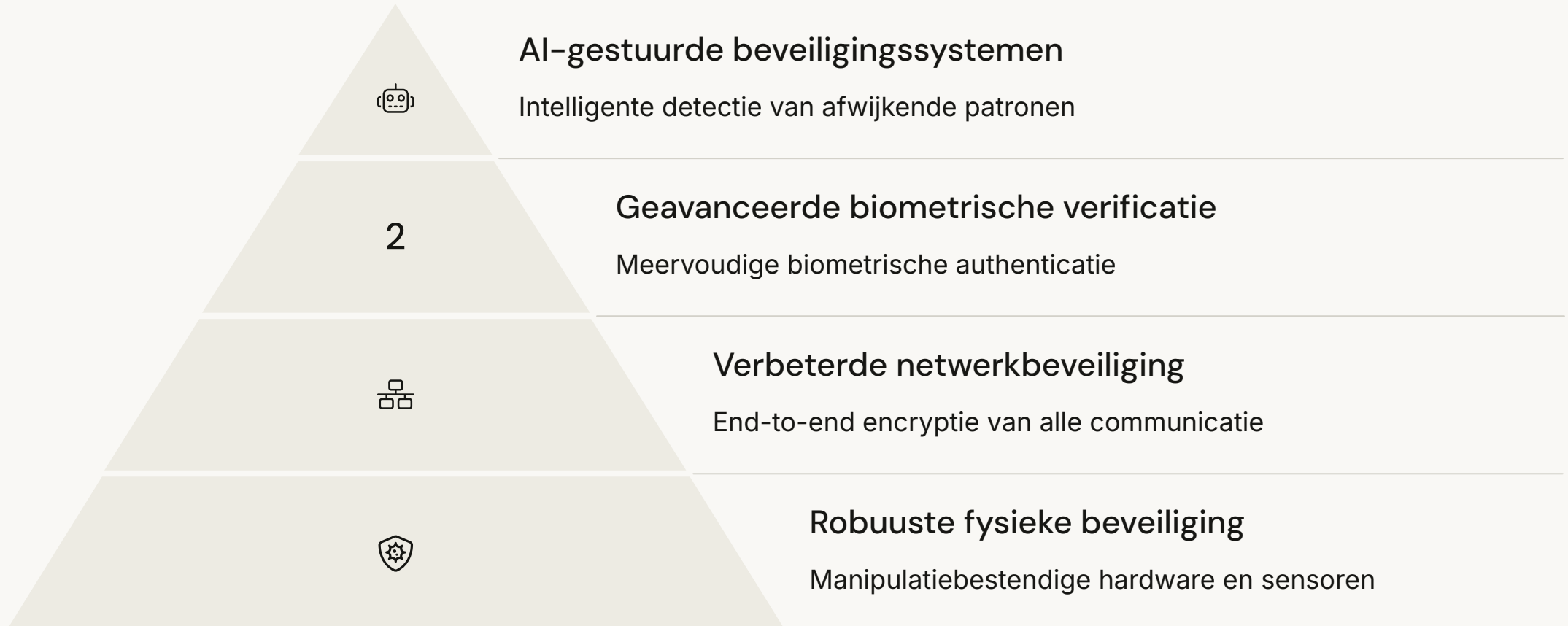


Gebruik bankapp voor monitoring

Controleer regelmatig je rekening op ongeautoriseerde transacties

Het waarborgen van de integriteit van geldautomaten is niet alleen een verantwoordelijkheid van banken; ook consumenten moeten zich bewust zijn van de risico's en hun eigen maatregelen nemen om hun financiële gegevens te beschermen.

Toekomstige Ontwikkelingen in ATM-beveiliging



In een wereld waar digitale en fysieke veiligheid steeds meer met elkaar verweven zijn, is aandacht voor beveiliging essentieel om een vertrouwde financiële omgeving te behouden.

Conclusie



Voortdurende Waakzaamheid

Blackbox aanvallen op geldautomaten vormen een ernstige bedreiging voor de financiële sector. Deze aanvallen zijn relatief eenvoudig uit te voeren voor goed voorbereide criminelen, wat hen in staat stelt om aanzienlijke financiële schade aan te richten.

Het is cruciaal voor zowel banken als consumenten om bewust te zijn van deze risico's en effectieve maatregelen te implementeren om de beveiliging te verbeteren.



Samenwerking en Innovatie

Door samen te werken aan beveiligingsstrategieën en voortdurend te investeren in technologie en training, kunnen we de kans op blackbox aanvallen verkleinen en de veiligheid van financiële transacties waarborgen.

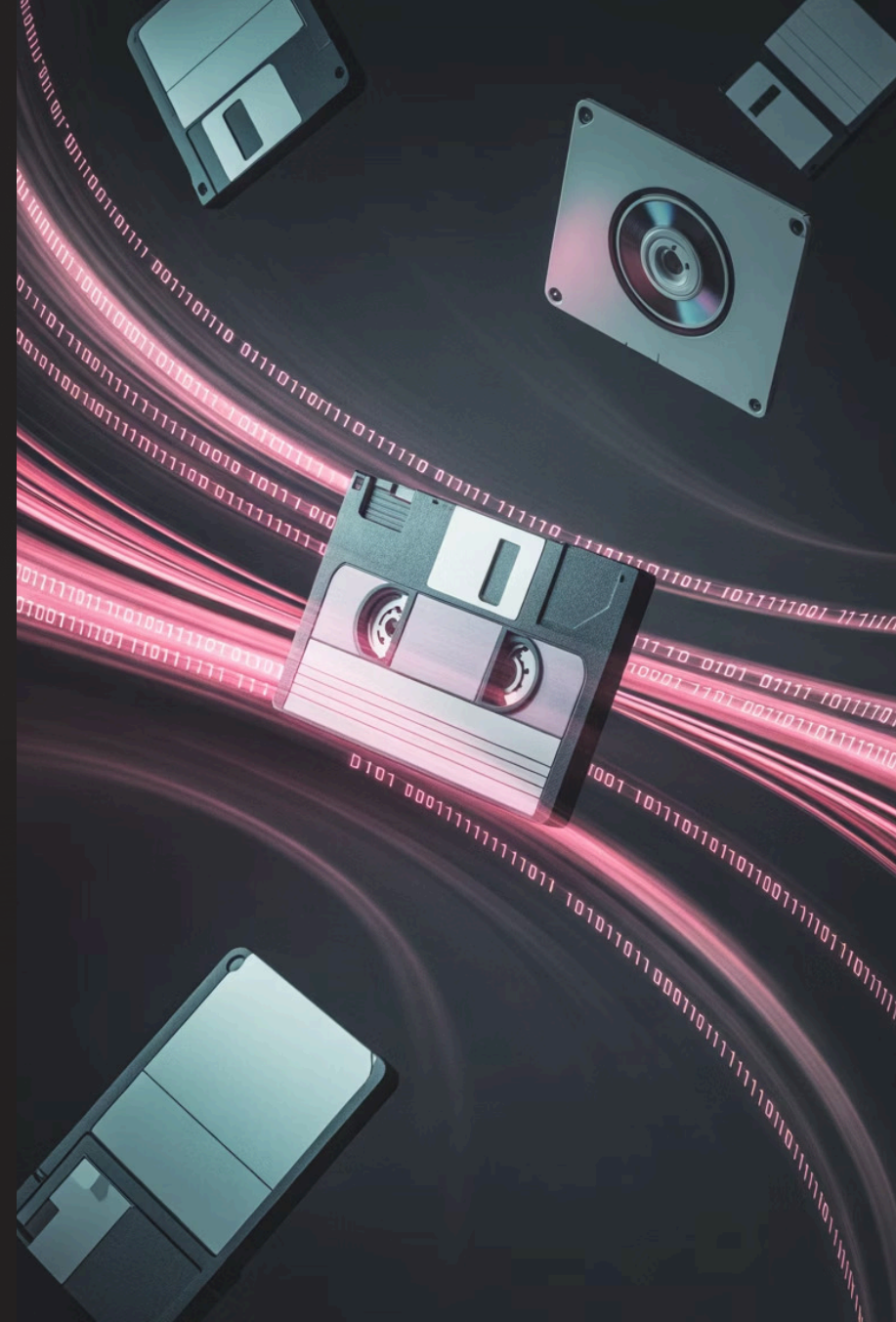
Het waarborgen van de integriteit van geldautomaten is niet alleen een verantwoordelijkheid van banken; ook consumenten moeten zich bewust zijn van de risico's en hun eigen maatregelen nemen om hun financiële gegevens te beschermen.

Digitale Erfenis in Gevaar: Bestandsformaten op de Rand van Uitsterven

Digitale bestandsformaten vormen de ruggengraat van onze informatiemaatschappij. Toch verdwijnen sommige formaten langzaam uit beeld.

We onderzoeken welke formaten binnenkort mogelijk verloren gaan. Van tekstbestanden tot video en specialistische formaten.

VEILIGDIGITAAL.COM



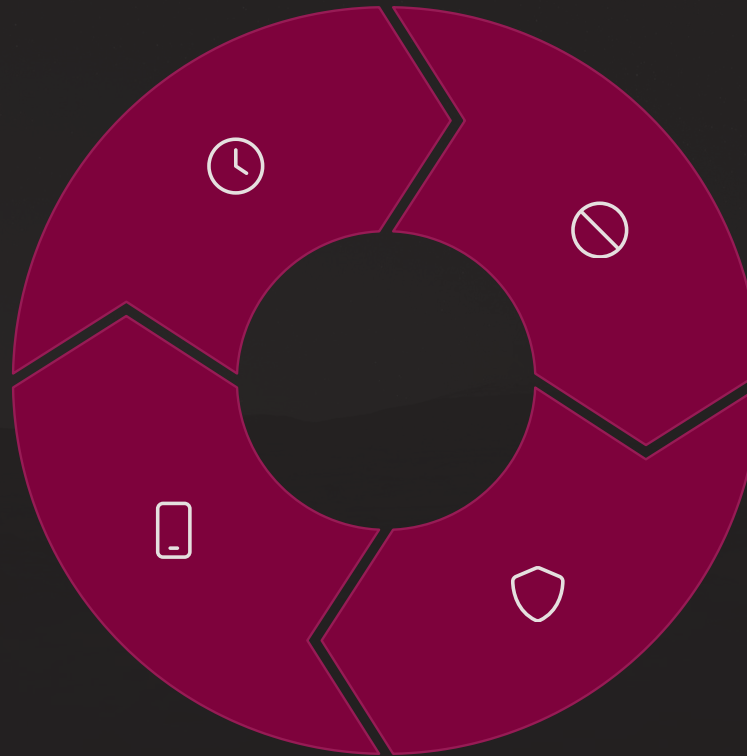
Waarom Verdwijnen Bestandsformaten?

Technologische Veroudering

Nieuwe standaarden vervangen verouderde technologieën. Dit gebeurt steeds sneller.

Veranderende Behoeften

Mobiele apparaten vereisen andere formaten. Efficiëntie wordt belangrijker.



Einde Ondersteuning

Softwareleveranciers stoppen met updates. Belangrijke reden voor het verdwijnen.

Veiligheidsrisico's

Oude formaten bevatten vaak beveiligingslekken. Deze blijven ongepatcht.



Tekstbestanden in Gevaar



RTF (Rich Text Format)

Verouderd en steeds minder ondersteund. Bevat vaak beveiligingsproblemen.



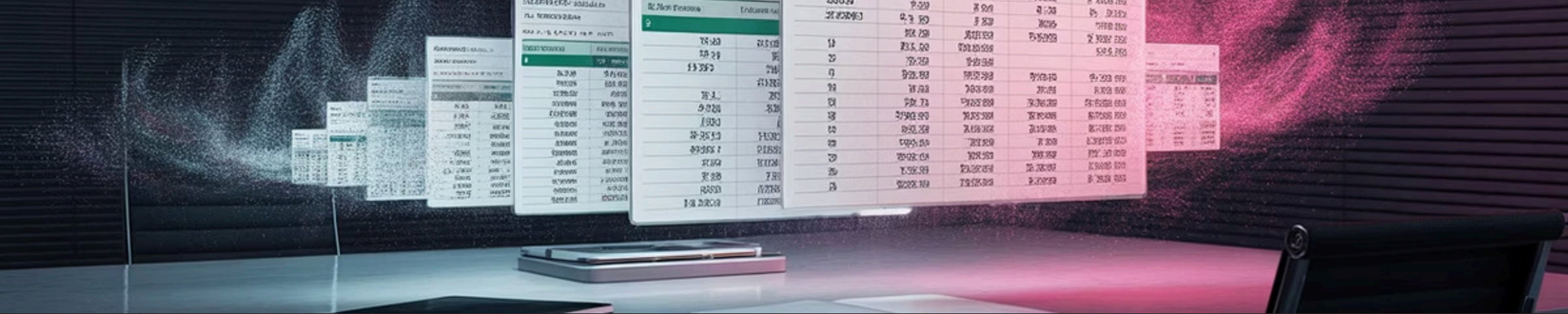
Oude DOC-bestanden

Pre-2007 formaat verliest snel ondersteuning. Microsoft raadt migratie aan.



Office 2016/2019 EOL

Ondersteuning stopt per 14 oktober 2025. Grote impact op bedrijven.



Spreadsheets Onder Druk



XLS-formaat

Pre-2007 Excel-bestanden worden zelden nog ondersteund. Groot migratieprobleem.



Compatibiliteitsrisico's

Complexe macro's en formules werken niet meer. Data-integriteit in gevaar.



Deadline 2025

Excel 2016/2019 niet meer ondersteund na oktober 2025. Plan nu migratie.

Beeldformaten op Retour

BMP

Windows Bitmap-formaat is inefficiënt. Gebruikt veel opslagruimte zonder voordelen.

- Geen compressie
- Geen transparantie
- Beperkte metadata

GIF

Animatie-format uit jaren '90. Verdrongen door modernere alternatieven.

- Beperkt kleurenpalet
- Matige beeldkwaliteit
- Vervangen door WebP/MP4

TIFF

Professioneel maar complex formaat. Buiten specialistische toepassingen steeds zeldzamer.

- Grote bestanden
- Beperkte webondersteuning
- Complexe structuur





Videoformaten in Transitie



Windows Media Video (WMV)

Propriëtair formaat van Microsoft. Verliest terrein aan MP4 en WebM.



Audio Video Interleave (AVI)

Uit de jaren '90. Nauwelijks nog ondersteund op mobiele apparaten.



MPEG-1

Sterk verouderde compressie. Kwaliteitsverlies vergeleken met moderne alternatieven.



Overstap naar H.264/H.265

Betere compressie en kwaliteit. Formaten die deze codecs gebruiken winnen terrein.

Sectorspecifieke Formaten

MT940 Bankformaat

Standaard voor elektronische rekeningafschriften. Wordt in 2025 definitief uitgefaseerd.

Vervangen door XML-gebaseerde CAMT.053 standaard. Banken stoppen ondersteuning.

Microsoft Exchange

Exchange Server 2016/2019 verdwijnt na 2025. Organisaties moeten migreren.

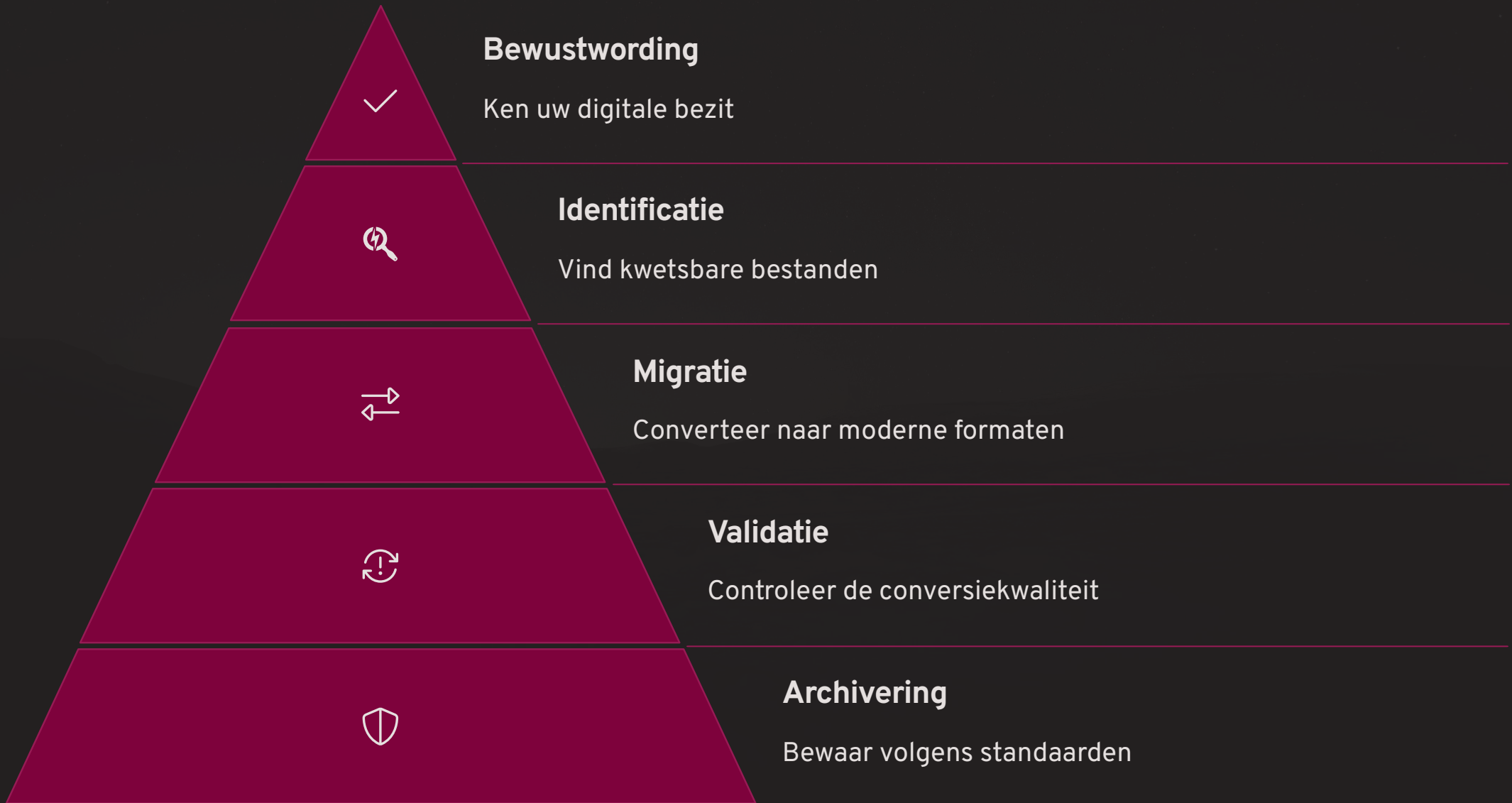
E-mailformaten en archieven veranderen. Oudere archieven worden mogelijk onleesbaar.

Branchespecifieke Formaten

Elk vakgebied heeft eigen bedreigde formaten. Van CAD tot medische beeldvorming.

Software-updates dwingen migratie af. Specialistische kennis vaak noodzakelijk.

Actieplan: Bescherm Uw Digitale Gegevens

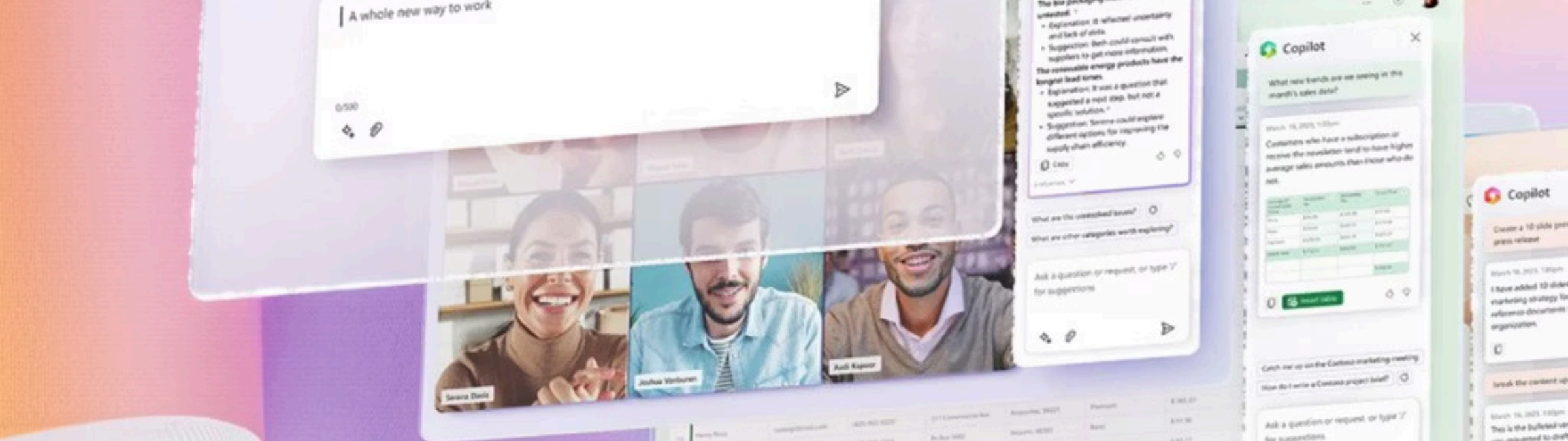


Copilot Vision: De AI die met je meekijkt – kansen en risico's

Copilot Vision is een innovatieve functie van Microsoft die kunstmatige intelligentie combineert met visuele context om gebruikers te ondersteunen tijdens hun digitale activiteiten. Deze technologie stelt Copilot in staat om te 'zien' wat er op je scherm gebeurt en biedt contextuele hulp op basis van de inhoud die je bekijkt.

Of je nu een webpagina leest, een document bewerkt of een applicatie gebruikt, Copilot Vision kan relevante informatie en suggesties bieden om je productiviteit te verhogen. Maar naast de voordelen zijn er ook potentiële cyberdreigingen waar gebruikers zich bewust van moeten zijn.





Hoe werkt Copilot Vision?



Activering

Gebruikers moeten Copilot Vision handmatig inschakelen. In Edge gebeurt dit via de Copilot-zijbalk door op het microfoonpictogram te klikken. In Windows 11 is er een 'bril'-icoon in de Copilot-app.



Contextuele Analyse

Zodra geactiveerd, analyseert Copilot Vision de inhoud van het actieve venster of de geselecteerde applicatie. Het gebruikt AI-modellen, waaronder GPT-4, om de context te begrijpen.



Interactie

Gebruikers kunnen vragen stellen of opdrachten geven via spraak of tekst. Copilot Vision reageert met suggesties, uitleg of begeleiding, afhankelijk van de context.

4

Beëindiging

De sessie eindigt wanneer de gebruiker Copilot Vision uitschakelt of de applicatie sluit. Alle tijdelijke gegevens worden dan verwijderd.

Webnavigatie en Productiviteit

Webnavigatie

Tijdens het browsen kan Copilot Vision aanvullende informatie bieden over de inhoud van een webpagina, zoals samenvattingen of definities van termen. Dit verrijkt de online ervaring en helpt gebruikers informatie sneller te verwerken.

Door deze contextuele ondersteuning kunnen gebruikers sneller werken en complexe taken eenvoudiger uitvoeren zonder constant tussen verschillende informatiebronnen te hoeven schakelen. De AI fungeert als een digitale assistent die altijd klaarstaat om te helpen.

Productiviteit

Bij het werken met documenten of spreadsheets kan Copilot Vision suggesties doen voor verbeteringen of uitleg geven over complexe functies. Dit verhoogt de efficiëntie en helpt gebruikers het maximale uit hun software te halen.



Educatie en Softwaregebruik

Educatie

Studenten kunnen Copilot Vision gebruiken om uitleg te krijgen over studiemateriaal of begeleiding bij het oplossen van problemen. De AI kan complexe concepten verduidelijken en aanvullende bronnen suggereren, wat het leerproces versnelt.

Softwaregebruik

Voor complexe softwaretoepassingen kan Copilot Vision stapsgewijze instructies geven, waardoor de leercurve wordt verkort. Gebruikers hoeven niet langer uitgebreide handleidingen door te nemen of tutorials te volgen.

Mobiele toepassingen

Op mobiele apparaten kan Copilot Vision via de camera visuele input analyseren, wat handig is voor taken zoals het identificeren van objecten of het vertalen van tekst in de echte wereld.

Privacy en Gegevensbeveiliging

Opt-in-systeem

Copilot Vision is standaard uitgeschakeld en vereist expliciete toestemming van de gebruiker om te worden geactiveerd. Dit geeft gebruikers volledige controle over wanneer de AI toegang heeft tot hun scherminhoud.

Gegevensverwerking

Tijdens een sessie verwerkt Copilot Vision de inhoud van het actieve venster om contextuele assistentie te bieden. Deze gegevens worden echter niet opgeslagen of gebruikt voor trainingsdoeleinden.

Sessiebeheer

Na het beëindigen van een sessie worden alle tijdelijke gegevens verwijderd. Alleen de reacties van Copilot worden gelogd om de veiligheidssystemen te verbeteren.

Beperkte toegang

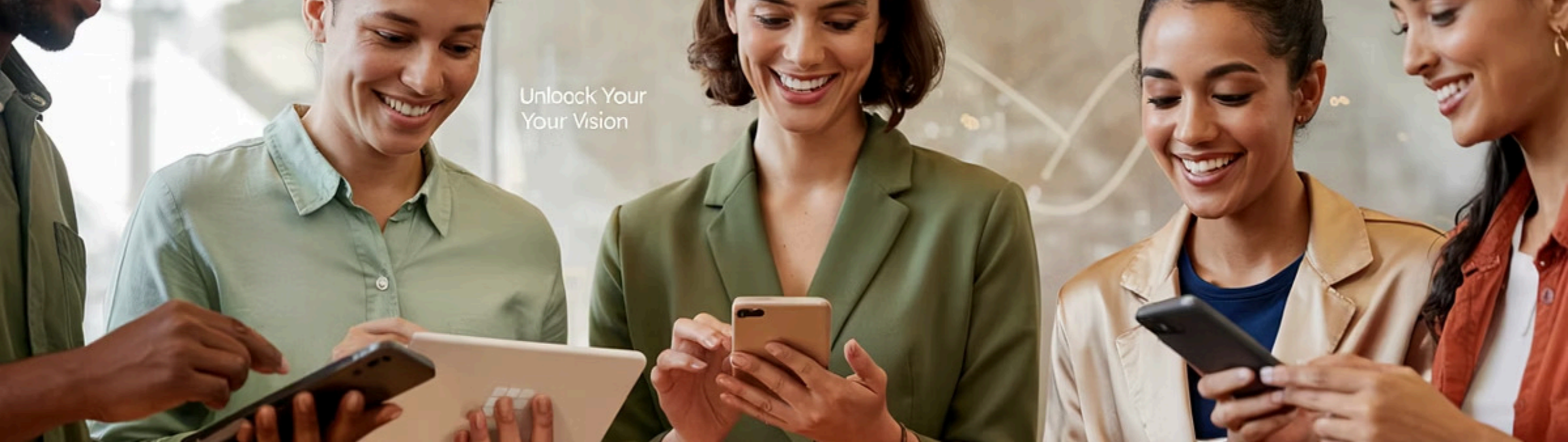
Copilot Vision heeft alleen toegang tot de inhoud van het venster waarvoor het is geactiveerd en kan geen acties uitvoeren zonder toestemming van de gebruiker.



Potentiële Cyberdreigingen



Hoewel Copilot Vision ontworpen is met privacy en veiligheid in gedachten, zijn deze risico's belangrijk om te overwegen. Gebruikers moeten zich bewust zijn van de context waarin ze de functie activeren en alert blijven op mogelijke beveiligingsproblemen.



Unlock Your
Your Vision

Voordelen voor Verschillende Gebruikers



Zakelijke professionals

Snellere verwerking van documenten, efficiëntere vergaderingen en verbeterde presentaties door contextuele ondersteuning.



Studenten

Verbeterd begrip van studiemateriaal, hulp bij onderzoek en ondersteuning bij het schrijven van papers.



Ontwikkelaars

Codeassistentie, foutopsporing en suggesties voor optimalisatie tijdens het programmeren.



Creatieven

Inspiratie, ontwerpfeedback en hulp bij het gebruik van complexe creatieve software.



Verantwoord Gebruik van Copilot Vision

Ken de privacy-instellingen

Zorg dat je bekend bent met alle privacy-instellingen en weet hoe je Copilot Vision kunt in- en uitschakelen. Controleer regelmatig of deze instellingen nog steeds aan je voorkeuren voldoen.

Wees bewust van de context

Activeer Copilot Vision alleen in vensters zonder gevoelige informatie. Wees extra voorzichtig bij het werken met persoonlijke of bedrijfsgevoelige gegevens en schakel de functie uit wanneer deze niet nodig is.

Blijf alert op verdachte activiteiten

Let op ongebruikelijke verzoeken of gedrag van Copilot Vision. Als iets verdacht lijkt, schakel de functie dan onmiddellijk uit en controleer je systeem op mogelijke beveiligingsproblemen.

Toekomstige Ontwikkelingen

Verbeterde AI-modellen

Toekomstige versies zullen waarschijnlijk geavanceerdere AI-modellen gebruiken, wat leidt tot nauwkeurigere context-interpretatie en betere suggesties.

Uitgebreide realiteit

Integratie met AR/VR-technologieën zou Copilot Vision kunnen transformeren tot een nog krachtigere assistent in gemengde realiteitsomgevingen.



Verbeterde beveiliging

Verwacht meer geavanceerde beveiligingsmaatregelen om de privacy van gebruikers te beschermen en potentiële dreigingen te minimaliseren.

Bredere integratie

Copilot Vision zal waarschijnlijk worden geïntegreerd in meer Microsoft-producten en mogelijk ook beschikbaar komen voor externe applicaties.

Conclusie: Balanceren van Innovatie en Veiligheid



Innovatieve mogelijkheden

Copilot Vision biedt ongekennde mogelijkheden voor productiviteit en ondersteuning



Bewuste afwegingen

Gebruikers moeten voordelen en risico's zorgvuldig afwegen



Verantwoord gebruik

Privacy-bewustzijn en veiligheidsmaatregelen zijn essentieel

Copilot Vision vertegenwoordigt een belangrijke stap voorwaarts in de evolutie van AI-assistenten. Door de juiste balans te vinden tussen het benutten van de innovatieve mogelijkheden en het handhaven van sterke beveiligingspraktijken, kunnen gebruikers optimaal profiteren van deze technologie terwijl ze hun digitale veiligheid waarborgen.

De Wereld van AI-Agents: Slimme Zelfredzame Systemen

In dit artikel duiken we in de fascinerende wereld van deze zelfdenkende systemen die verder gaan dan gewone chatbots.

VEILIGDIGITAAL.COM

Cognito AI

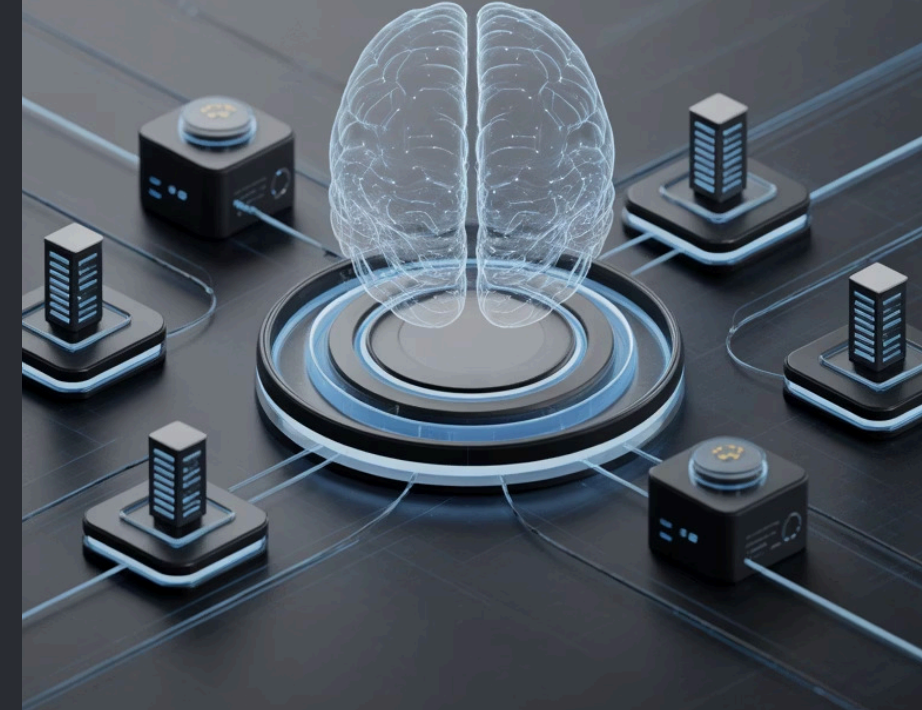
Solutions

Features

Pricing

Pricing

Request demo



Unlock the power of adaptive intelligence

Derparctis eunt et ptiw orits care. lts al eturdielliengrutienei: vneepes oi ans atptioiy
paeneine aingluisy me ollucline e: pnateautn gorivulij atgjiom calrugianes
ecaungau teperetibes er bauatvestmicheaeaejratice.

Learn more

Wat zijn AI-agents precies?



Zelfstandige systemen

AI-agents kunnen zelfstandig taken uitvoeren zonder voortdurende menselijke begeleiding.



Zelfredzaam

Ze kunnen leren van eigen acties en fouten corrigeren wanneer nodig.

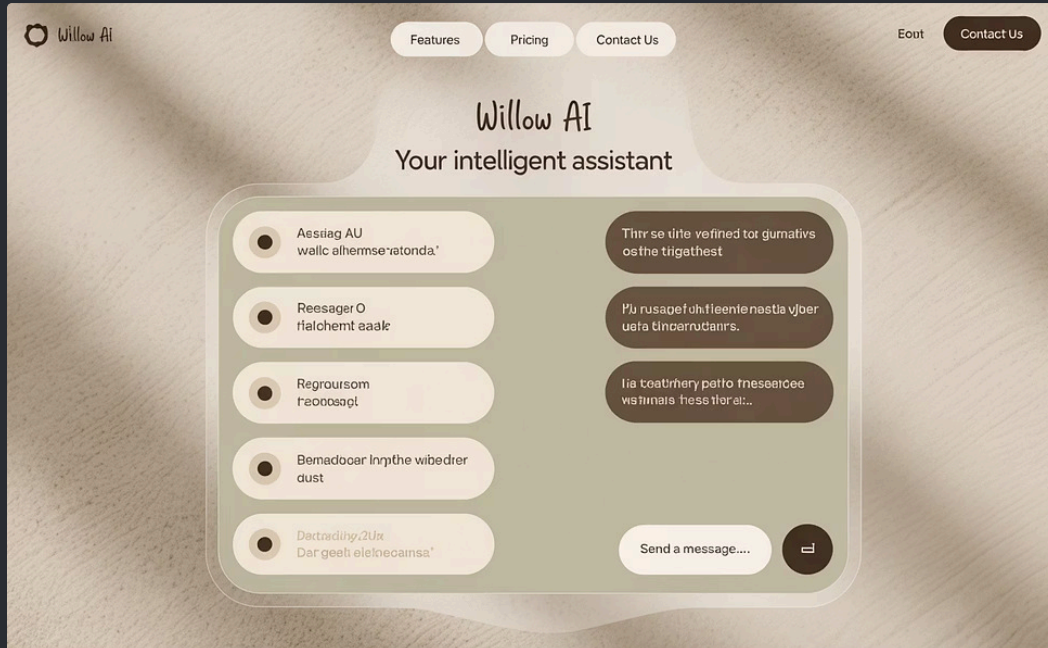


Proactief

In tegenstelling tot chatbots wachten ze niet alleen op input maar handelen ze zelf.



Verskil met traditionele AI-modellen



Traditionele Chatbots

- Reageren alleen op directe vragen
- Beperkte contextverwerking
- Geen zelfstandige acties

AI-Agents

- Nemen zelf initiatief
- Leren van eerdere acties
- Voeren complexe taken uit

Toepassingen van AI-agents

E-mailbeheer
Sorteren en prioriteren van berichten in uw inbox.

Online interactie
Zoeken en verwerken van informatie op het internet.



Software schrijven
Genereren en debuggen van code voor ontwikkelaars.

Workflowbeheer
Automatiseren van complexe bedrijfsprocessen.

De toekomst van AI-agents



AI-agents zullen steeds belangrijker worden in ons dagelijks leven en werk. Ze bieden ongekennde mogelijkheden voor automatisering en innovatie.



De donkere kant van emoji's

Emojis zijn een onmiskenbaar onderdeel van onze digitale communicatie. Ze brengen emotie over in tekst en verrijken gesprekken met levendigheid. Op platforms zoals TikTok vormen ze zelfs een essentieel aspect van de digitale cultuur. Toch schuilt er achter deze schijnbaar onschuldige symbolen een minder bekende realiteit: cybercriminelen maken strategisch gebruik van emojis voor kwaadaardige doeleinden.

In dit artikel analyseren we de manieren waarop specifieke TikTok-emojis worden ingezet binnen cybercriminaliteit en benadrukken we het belang van verhoogde alertheid bij gebruikers.

Verborgen TikTok-emoji's



Verborgen codes

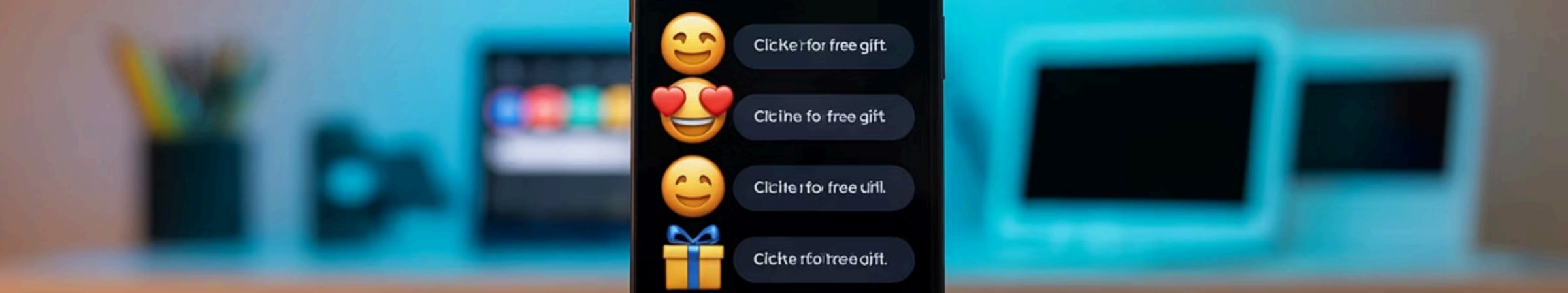
TikTok beschikt over een reeks verborgen emoji's die gebruikers kunnen activeren door specifieke codes tussen vierkante haken in te voeren, bijvoorbeeld `\[smile\]` of `\[cry\]`.

Unieke eigenschappen

Deze unieke emoji's zijn niet beschikbaar op reguliere toetsenborden en zijn bedoeld om de gebruikerservaring te optimaliseren.

Potentiële risico's

De verborgen aard ervan brengt echter ook het risico met zich mee dat ze voor ongepaste doeleinden worden gebruikt.



Phishing en Malware Verspreiding



Verbergen van schadelijke links

Cybercriminelen maken gebruik van emoji's om schadelijke links op een subtiele wijze te verbergen.



Combinatie met verkorte URL's

Door een combinatie van emoji's te integreren met verkorte URL's, slagen zij erin gebruikers te misleiden.



Verleiden tot klikken

Gebruikers worden verleid om te klikken op links die toegang bieden tot phishingwebsites of het downloaden van malware initiëren.



Verminderde alertheid

De visuele aantrekkingskracht van emoji's verhoogt aanzienlijk de kans dat gebruikers hun alertheid verliezen.

Omzeilen van Moderatie door 'Algospeak'

Gecodeerde taal

'Algospeak' verwijst naar het gebruik van gecodeerde taal met als doel automatische moderatiesystemen te omzeilen.

Verspreiding van inhoud

Deze strategie stelt gebruikers in staat om potentieel schadelijke of ongepaste inhoud te verspreiden, terwijl zij onopgemerkt blijven door moderatie-algoritmen.



Emoji substitutie

Op TikTok wordt regelmatig gebruikgemaakt van emoji's om gevoelige of verboden onderwerpen op een discrete wijze te bespreken.

Ontwijken van algoritmes

Een veelvoorkomend voorbeeld hiervan is het gebruik van de 🌽-emoji als substituuut voor het woord "porn".

Verbergen van Illegale Activiteiten



Verhullen van illegale communicatie

Emoticons worden eveneens aangewend om illegale activiteiten te verhullen.



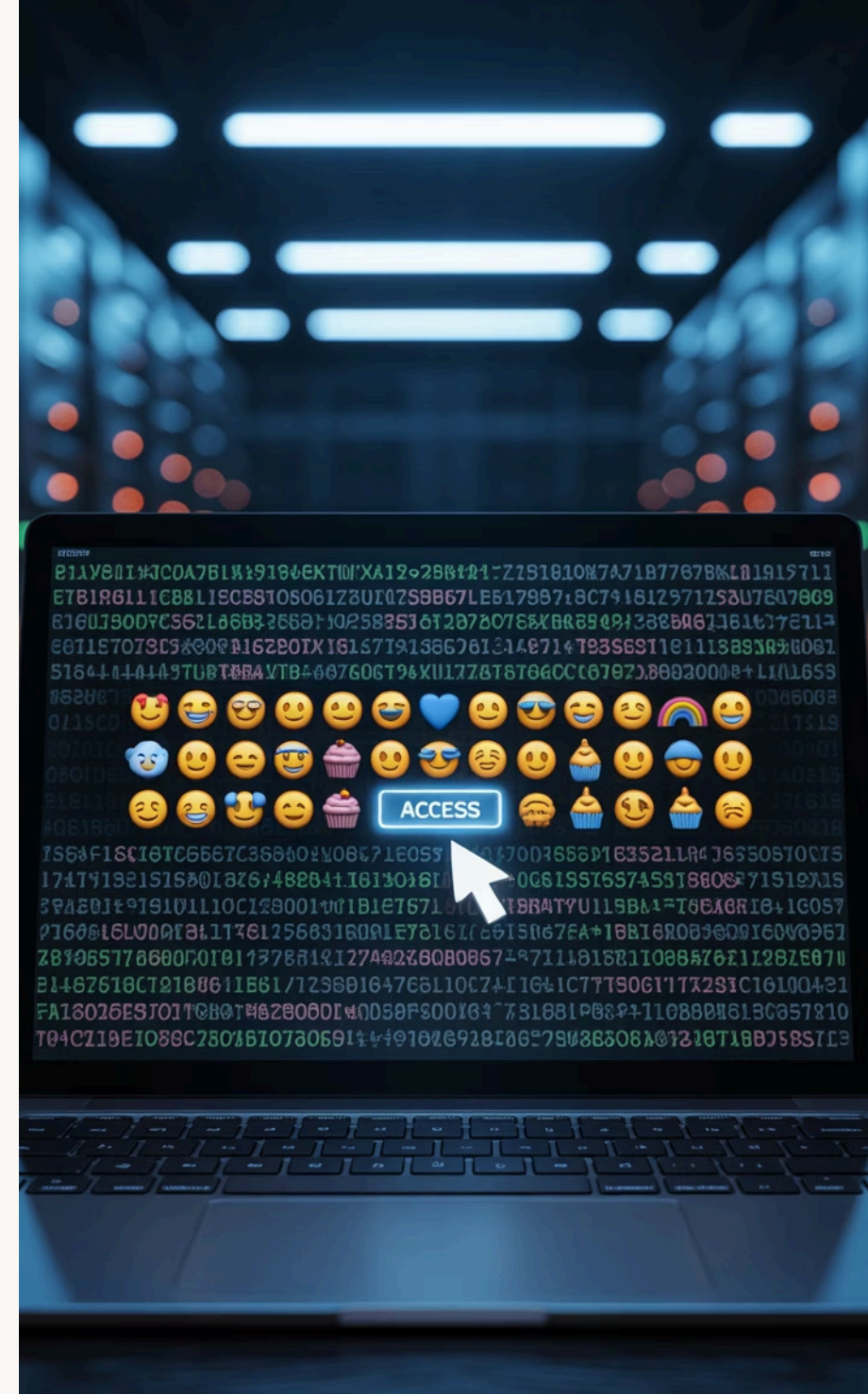
Specifieke emoji-combinaties

Door middel van een specifieke combinatie van emoticons kunnen gebruikers met elkaar communiceren over drugs, wapens of andere verboden onderwerpen, zonder expliciet taalgebruik toe te passen.



Uitdagingen voor autoriteiten

Hierdoor wordt het voor autoriteiten aanzienlijk complexer om dergelijke communicatie te identificeren en hierop effectief te acteren.



De Impact op Gebruikers en Samenleving



Verhoogd Risico op Slachtofferschap

Gebruikers kunnen onbewust slachtoffer worden van phishing-aanvallen of malware-infecties.



Verspreiding van Schadelijke Inhoud

Door het omzeilen van moderatie kunnen schadelijke of ongepaste inhoud zich sneller verspreiden.



Verlies van Vertrouwen

Als gebruikers zich niet veilig voelen op platforms zoals TikTok, kan dit leiden tot een afname van gebruikersvertrouwen en betrokkenheid.

Bescherming tegen Emoji-gebaseerde Cyberdreigingen

Wees Kritisch op Links

Klik niet zomaar op links, zelfs als ze worden gepresenteerd met aantrekkelijke emojis.

Herken 'Algospeak'

Leer de betekenissen achter bepaalde emoji-combinaties om gecodeerde communicatie te herkennen.

Gebruik Beveiligingssoftware

Installeer betrouwbare antivirus- en anti-malwareprogramma's om je apparaten te beschermen.

Rapporteer Verdachte Inhoud

Meld verdachte of ongepaste inhoud aan platformmoderatoren om de gemeenschap veilig te houden.



Conclusie

Expressieve communicatie

Hoewel emojis een leuke en expressieve manier van communiceren bieden, is het essentieel om bewust te zijn van hun potentieel misbruik in de wereld van cybercriminaliteit.

Waakzaamheid blijft belangrijk

Door geïnformeerd en waakzaam te blijven, kunnen gebruikers zichzelf en anderen beschermen tegen de verborgen gevaren die schuilgaan achter deze kleurrijke symbolen.

De actuele geïntegreerde graphics van AMD, Intel en Apple

VEILIGDIGITAAL.COM



AMD Geïntegreerde Graphics



Radeon Graphics

AMD's geïntegreerde graphics zijn bekend onder de naam Radeon Graphics en worden geleverd in hun APU's (Accelerated Processing Units).



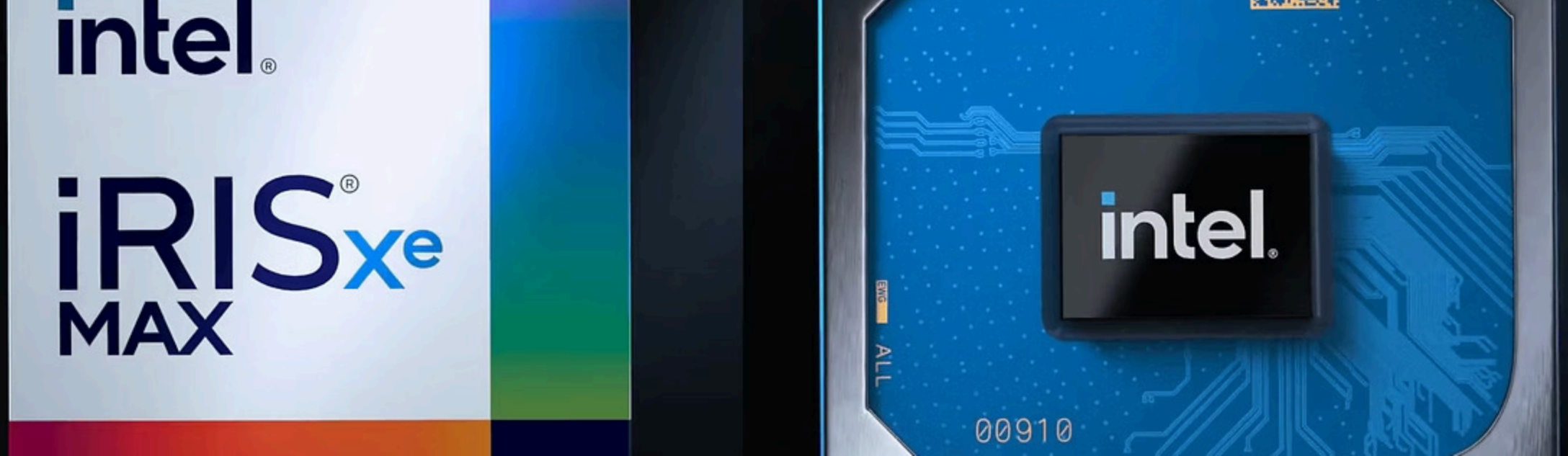
RDNA Architectuur

De nieuwste generatie maakt gebruik van de RDNA architectuur, die betere prestaties en energie-efficiëntie biedt.



Gaming Prestaties

AMD's geïntegreerde graphics staan bekend om hun relatief sterke gaming prestaties in vergelijking met concurrenten.



Intel Geïntegreerde Graphics



Intel Iris Xe Graphics

De nieuwste geïntegreerde graphics van Intel dragen de naam Iris Xe en bieden een significante verbetering ten opzichte van eerdere UHD Graphics.



Gen12 Architectuur

Gebaseerd op de Gen12 architectuur met verbeterde prestaties voor zowel productiviteit als lichte gaming.



Display Ondersteuning

Biedt ondersteuning voor meerdere 4K-displays en verbeterde media-encoding en -decoding.



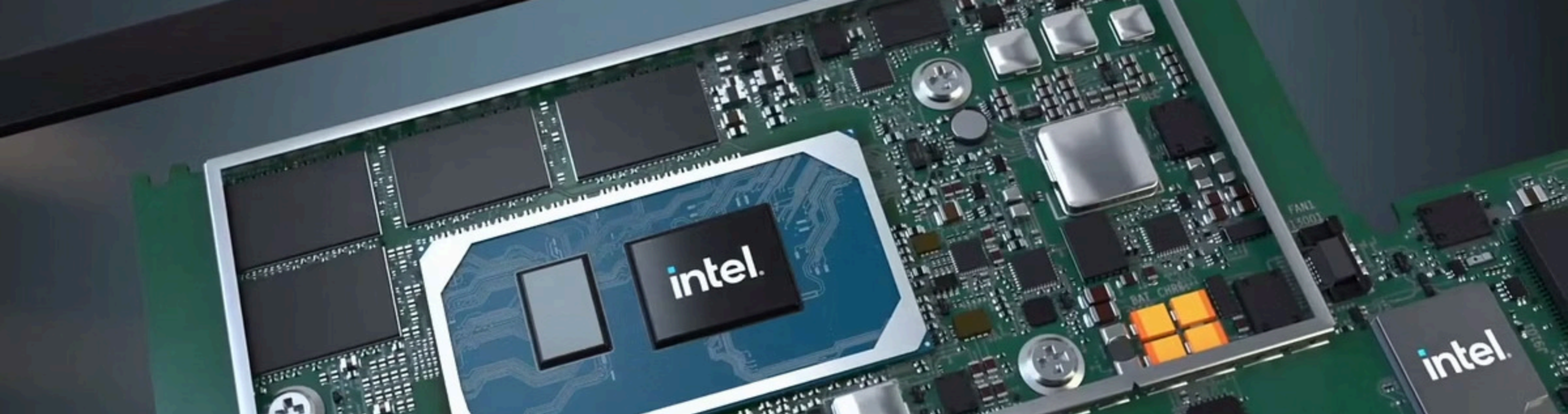
AI Versnelling

Bevat speciale hardware voor AI-versnelling en machine learning toepassingen.

Apple Geïntegreerde Graphics



Apple's geïntegreerde graphics in de M-serie chips hebben de industrie verrast met hun uitzonderlijke prestaties, terwijl ze zeer energie-efficiënt blijven. Deze GPU's zijn volledig door Apple zelf ontworpen en geoptimaliseerd voor hun eigen ecosysteem.



Vergelijking van Geïntegreerde Graphics

Fabrikant	Huidige Generatie	Sterke Punten	Zwakke Punten
AMD	Radeon Graphics (RDNA)	Sterke gaming prestaties, goede prijs-kwaliteitverhouding	Hoger stroomverbruik dan Apple
Intel	Iris Xe Graphics	Verbeterde prestaties, goede media-verwerking	Minder krachtig in gaming dan AMD
Apple	M-serie geïntegreerde GPU	Uitzonderlijke energie-efficiëntie, hoge prestaties	Alleen beschikbaar in Apple-apparaten

Prestatievergelijking: AMD Radeon vs Intel Iris Xe

AMD Radeon Graphics

Gebaseerd op de nieuwste RDNA architectuur voor betere prestaties per watt.

- Superieure gaming prestaties in de meeste tests
- Betere 3D-rendering capaciteiten
- Meer Compute Units dan Intel concurrenten

Intel Iris Xe Graphics

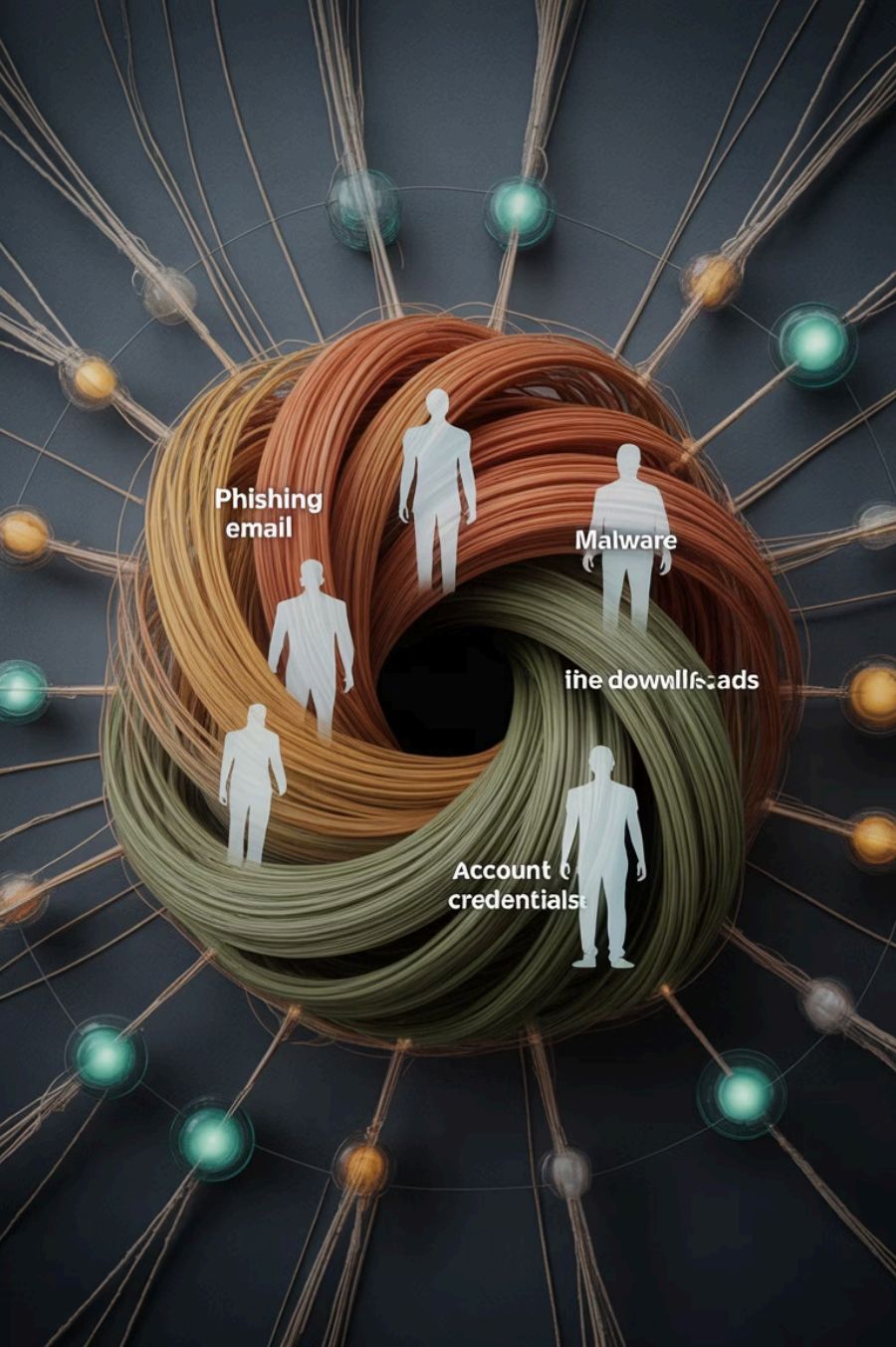
Aanzienlijke vooruitgang ten opzichte van oudere Intel UHD Graphics.

- Excelleert in mediabewerkingstaken
- Betere hardware-versnelde videocodering
- Meer energie-efficiënt in lichte werklasten

Prestatieverhouding

AMD leidt in pure grafische kracht, Intel in veelzijdigheid.

- AMD tot 20% sneller in games
- Intel presteert beter in AI-werklasten
- AMD biedt meer waar voor je geld



De vele varianten van de ClickFix social engineering-tactiek

Omdat er vrijwel maandelijks nieuwe malwarecampagnes worden ontdekt die gebruikmaken van de social engineering-tactiek ClickFix, is het interessant om te zien hoe de verschillende aanvallers proberen de twee belangrijkste elementen te verfijnen: het lokaas en de 'instructiepagina'.

VEILIGDIGITAAL.COM

De ClickFix/FakeCaptcha-aanpak

ClickFix is een tactiek die malware verspreidt zonder dat hiervoor een webbrowser nodig is en zonder dat gebruikers handmatig een bestand hoeven uit te voeren. Hiermee voorkomen aanvallers dat ze worden gedetecteerd door e-mail- en endpoint-beveiligingsoplossingen.

Identify all traffic lights



Warning:
Unusual activity
detected.

Enter the sequence

Verify



Vermijdt detectie

Aanvallers omzeilen e-mailbeveiliging



Verspreidt malware

Zonder handmatige uitvoering van bestanden



Browseronafhankelijk

Werkt zonder webbrowser als tussenpersoon



Typische ClickFix-aanval: Stap 1

Misleiding van de gebruiker

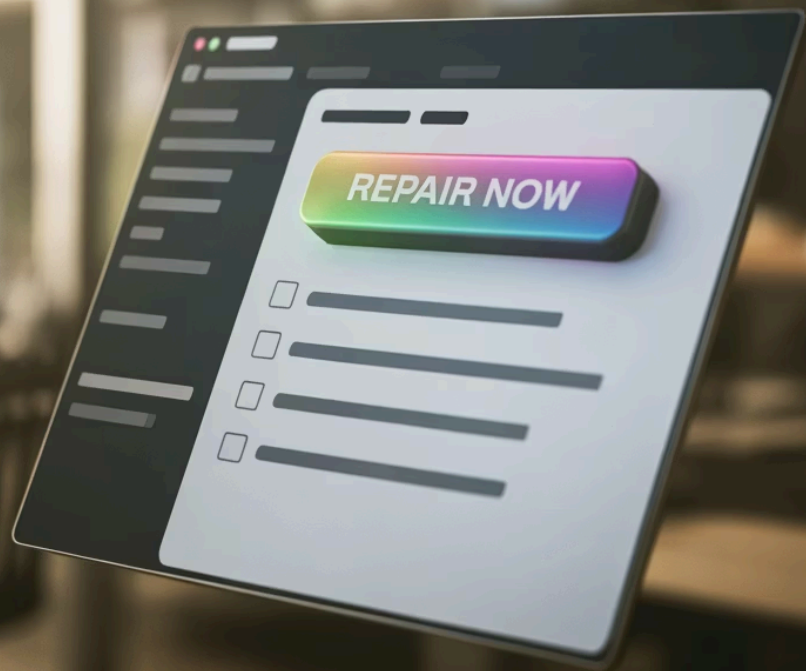
De gebruiker wordt misleid om een pagina te bezoeken die een nep-waarschuwing of een nep-CAPTCHA-test zal tonen.

Valse meldingen

De pagina toont alarmerend ogende waarschuwingen of een ogenschijnlijk onschuldige CAPTCHA-verificatie.

Creëren van urgentie

De gebruiker wordt onder druk gezet om snel te handelen zonder na te denken over de gevolgen.



Are you protected?

Typische ClickFix-aanval: Stap 2



Instructies volgen

De pagina vertelt de gebruiker om op de knop 'Repareer het' te drukken of het vakje 'Ik ben geen robot' aan te vinken.



Reeks acties

De gebruiker wordt gevraagd een reeks acties uit te voeren (de 'instructies').



Schijnbare oplossing

De gebruiker denkt een probleem op te lossen of een verificatie te voltooien.

Typische ClickFix-aanval: Stap 3

Kwaadaardige uitvoering

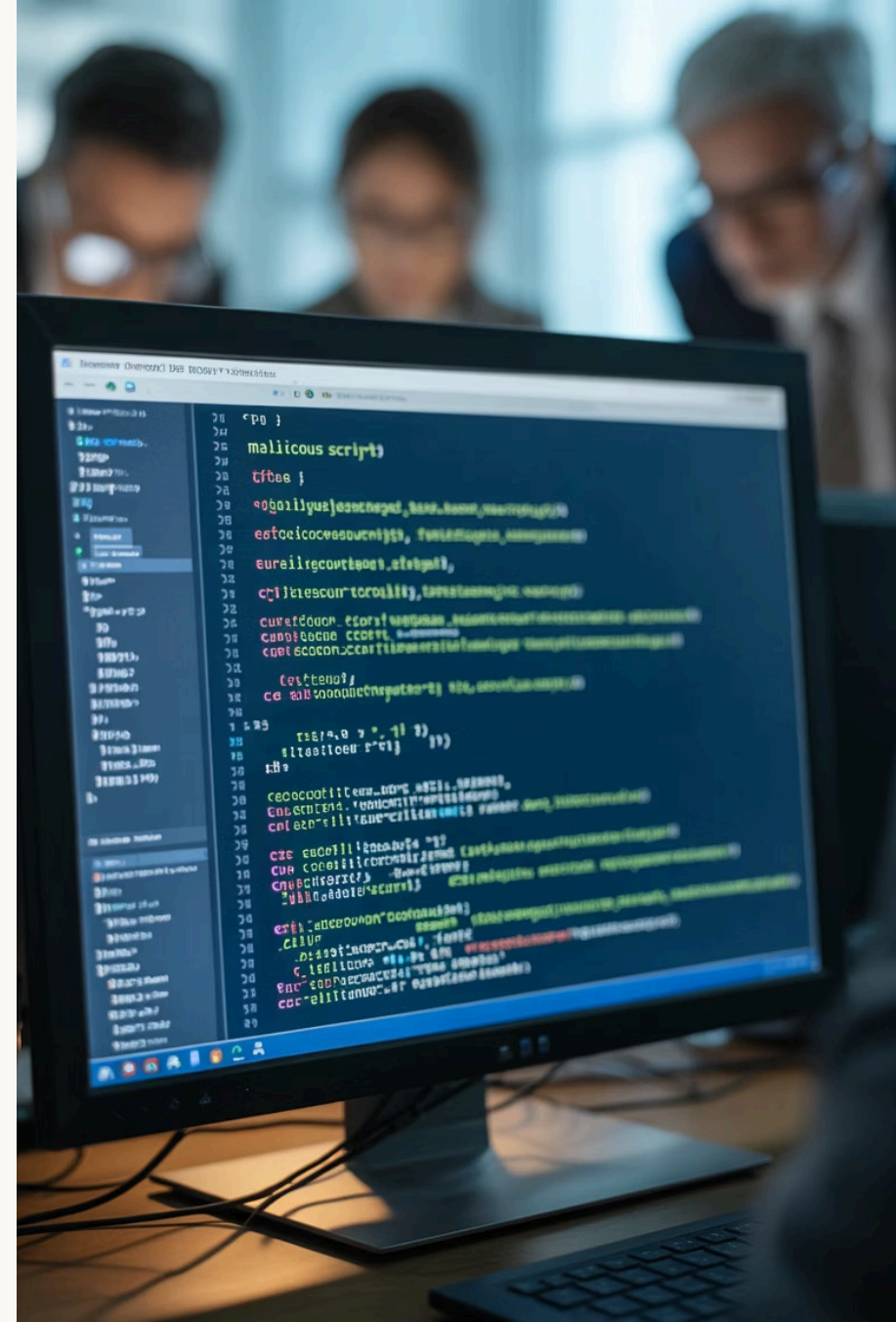
Een kwaadaardige PowerShell-opdracht wordt gedownload en uitgevoerd.

Onzichtbare infectie

De malware installeert zich zonder dat de gebruiker dit merkt of toestemming geeft.

Systeem compromitteren

Het systeem wordt geïnfecteerd en kan worden gebruikt voor verdere aanvallen of gegevensdiefstal.



Het lokaas verfijnen

Overtuigende waarschuwingen

Aanvallers besteden veel aandacht aan het ontwerpen van realistische waarschuwingsschermen die gebruikers doen geloven dat er een echt probleem is met hun computer of account.

Bekende merken imiteren

Door het nabootsen van bekende bedrijven zoals Microsoft, Google of beveiligingsbedrijven, wekken aanvallers vertrouwen bij de gebruiker en verlagen ze de drempel om de instructies te volgen.

Angst en urgentie

Het lokaas speelt vaak in op angst door te suggereren dat de computer geïnfecteerd is of dat de toegang tot belangrijke diensten wordt geblokkeerd als er niet snel wordt gehandeld.

De instructiepagina optimaliseren

Duidelijke stappen

Eenvoudige, stapsgewijze instructies die zelfs door technisch onervaren gebruikers kunnen worden gevolgd

Tijdsdruk

Suggesties dat snelle actie noodzakelijk is om problemen te voorkomen



Visuele hulpmiddelen

Pijlen, markeringen en screenshots om de gebruiker precies te tonen wat te doen

Veilig ogende taal

Gebruik van beveiligingsterminologie om de indruk te wekken dat de acties het systeem beschermen



Maandelijkse evolutie van ClickFix-campagnes

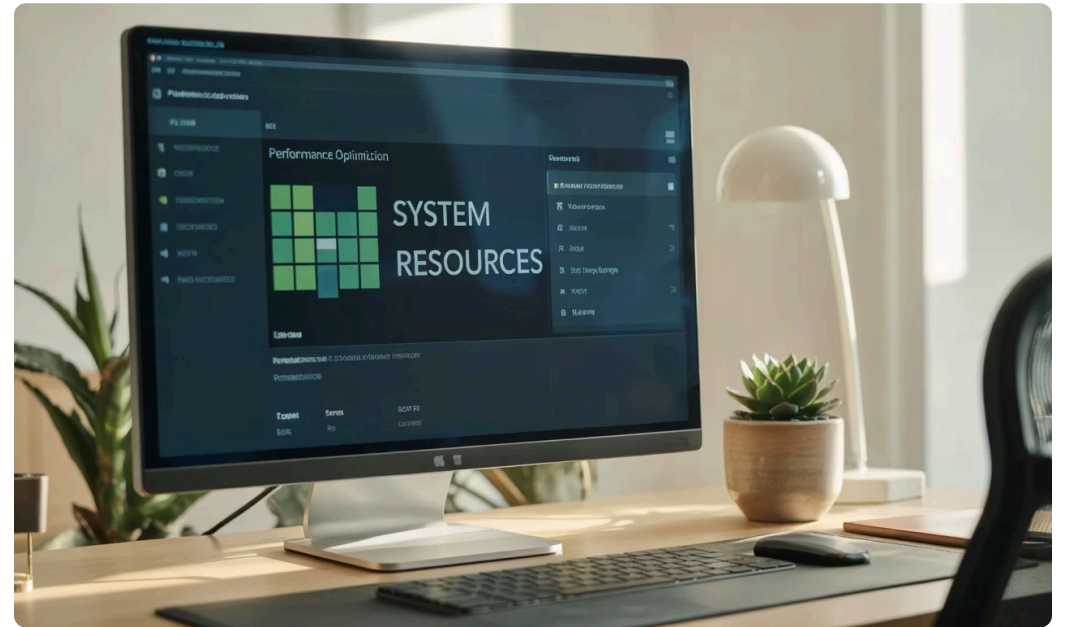
- 1 — Eerste varianten**
Eenvoudige nep-CAPTCHA's met basale instructies en beperkte vermomming van de kwaadaardige code.
- 2 — Verbeterde misleiding**
Toevoeging van realistische bedrijfslogo's en professionelere lay-outs om legitimiteit te suggereren.
- 3 — Geavanceerde technieken**
Implementatie van complexere PowerShell-scripts die moeilijker te detecteren zijn door beveiligingssoftware.
- 4 — Huidige campagnes**
Vrijwel maandelijks worden nieuwe malwarecampagnes ontdekt die gebruikmaken van steeds verfijndere ClickFix social engineering-tactieken.

De 5 Essentiële Stappen voor PC-Optimalisatie

Uw computer werkt traag? Met deze simpele stappen verbetert u de prestaties aanzienlijk. Verwijder eerst ongebruikte programma's via het configuratiescherm.

Schakel daarna onnodige opstartprogramma's uit. Dit verkort uw opstarttijd. Voer regelmatig een schijfopruiming uit voor meer vrije ruimte.

Defragmenteer uw harde schijf maandelijks. Overweeg tenslotte een upgrade naar een SSD voor spectaculaire snelheidswinst.





Europol: ouders moeten alert zijn als kind versleutelde chatapps gebruikt

Ouders moeten alert zijn als hun kind opeens gebruikmaakt van versleutelde chatapps en vragen wat ze te verbergen hebben, zo adviseert Europol aan ouders. Volgens de Europese opsporingsdienst maken versleutelde communicatie en aan te passen privacyinstellingen het mogelijk om anonieme groepen en kanalen op social media aan te maken, waar criminelen vaak gebruik van maken voor het plannen van illegale activiteiten. Cijfers of andere onderbouwing geeft de Europese opsporingsdienst niet.



Taskforce tegen 'violence-as-a-service'



Internationale samenwerking

Europol laat weten dat het samen met verschillende landen, waaronder Nederland, een taskforce heeft opgericht om 'violence-as-a-service' aan te pakken.



Rekrutering van jongeren

Het gaat dan om criminelen die jongeren rekruteren voor het plegen van aanslagen en andere gewelddadige misdrijven.



Intelligence Notification

Eind vorig jaar kwam Europol met een 'Intelligence Notification' over criminelen die online jongeren voor illegale activiteit rekruteren.

Risico's van versleutelde communicatie

Anonieme groepen

Versleutelde communicatiediensten van social media en aan te passen privacyinstellingen maken het mogelijk om anonieme groepen en kanalen aan te maken.

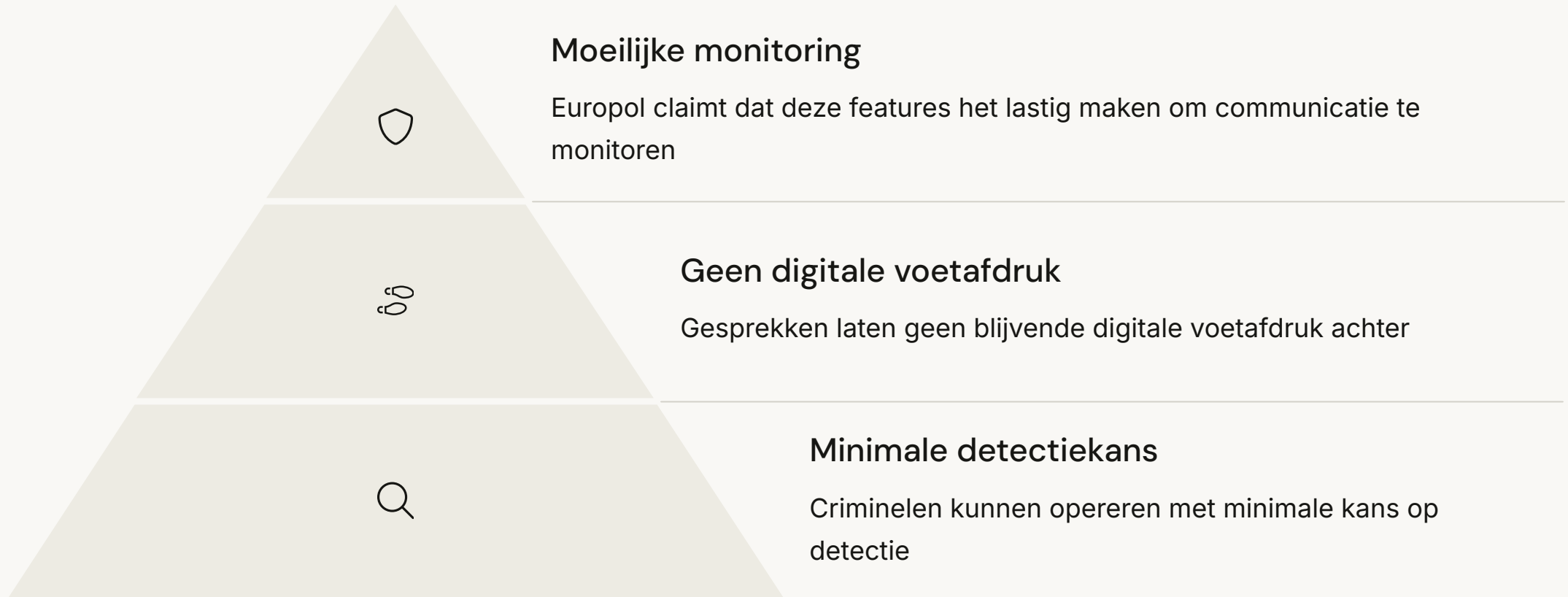
Illegale activiteiten

Die worden vaak gebruikt voor het organiseren van illegale activiteiten, met minimale kans op detectie.

Privacyfuncties

Criminelen kunnen instellen dat berichten zichzelf vernietigen, gespreksgeschiedenissen verwijderen en groepstoegang tot geverifieerde leden beperken.

Uitdagingen voor opsporing



Advies aan ouders



Georganiseerde misdaad begint thuis

Niet met geweld, maar met subtiele veranderingen



Let op waarschuwingssignalen

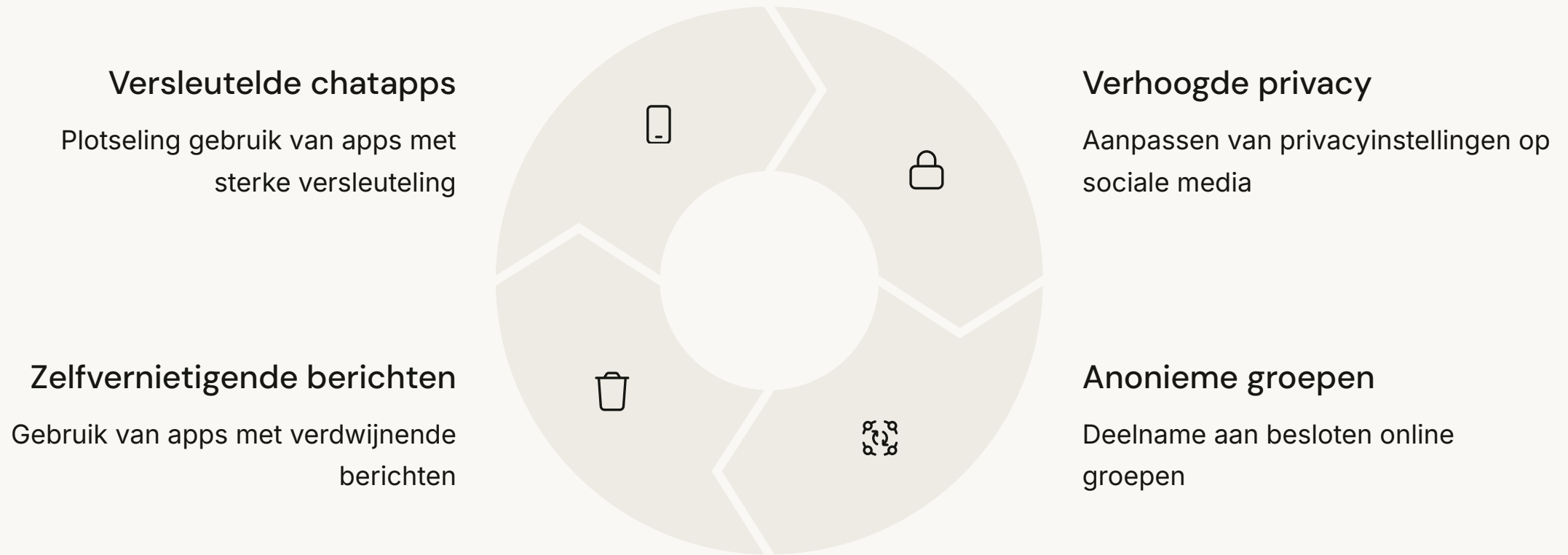
Ouders moeten alert zijn op veranderend gedrag



Vraag naar versleutelde apps

Vraag waarom. Wat hebben ze te verbergen?

Herkennen van risicosignalen





Europol's preventieve aanpak



Bewustwording

Informeren van ouders over digitale risico's



Educatie

Voorlichting over rekruteringsacties



Samenwerking

Internationale taskforce tegen criminele netwerken



Interventie

Vroegtijdig ingrijpen bij risicogedrag

Advies voor ouders

Naast de Intelligence Notification is Europol ook gekomen met advies aan ouders. Georganiseerde misdaad begint in huis - niet met geweld, maar met subtiele veranderingen. Op deze zaken moet worden gelet, zo begint het advies.

Hoe kun je jouw Facebookaccount definitief verwijderen?

Permanent verwijderen betekent dat je al je data verliest. Het is een definitieve keuze.

Als alternatief kun je je account tijdelijk deactiveren of de snooze-functie gebruiken.

VEILIGDIGITAAL.COM



Verschil: Deactiveren vs. Verwijderen

Deactiveren

Je profiel blijft bewaard, maar is tijdelijk onzichtbaar voor anderen.

Je kunt altijd weer terugkeren door in te loggen.

Verwijderen

Al je gegevens worden na 30 dagen definitief gewist.

Binnen die periode kun je de verwijdering nog annuleren.



Maak een back-up van je gegevens

Foto's & Video's

Download al je persoonlijke media voordat deze verloren gaan.

Berichten & Contacten

Bewaar belangrijke gesprekken en contactgegevens van vrienden.

Persoonlijke Informatie

Sla je tijdlijnposts, gebeurtenissen en andere persoonlijke content op.

Stap-voor-stap: Je account verwijderen



Inloggen

Log in op je Facebook-account.



Verwijderpagina bezoeken

Ga naar www.facebook.com/help/delete_account



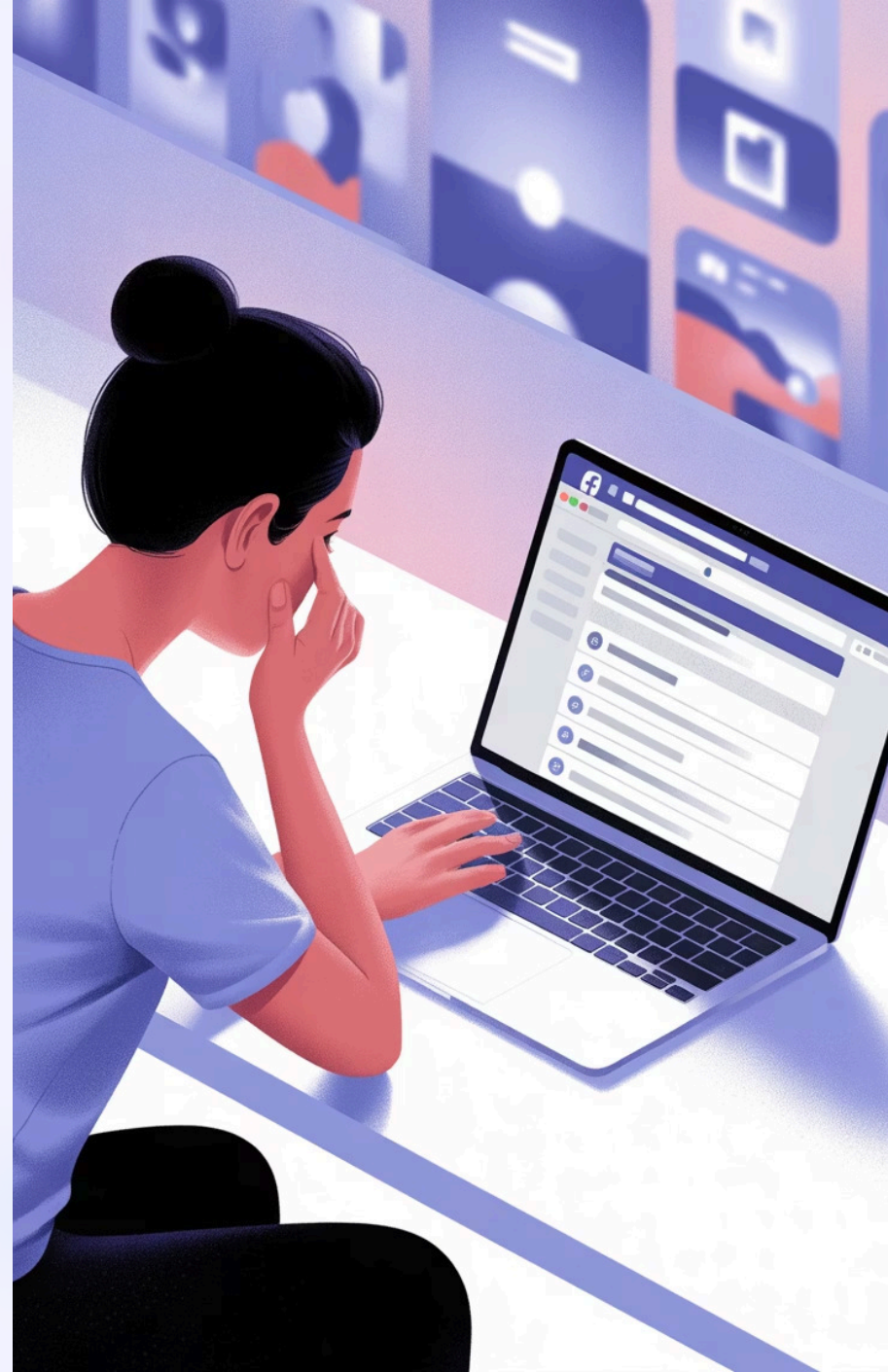
Account verwijderen

Klik op 'Account verwijderen' en volg de instructies.



Bevestigen

Voer je wachtwoord in en klik op 'Doorgaan'.





Wat gebeurt er na verwijdering?

1

Direct

Je account is niet meer zichtbaar voor anderen.

Je kunt niet meer inloggen met je gegevens.

2

30 dagen

Bedenktijd waarin je de verwijdering nog kunt annuleren.

Je krijgt een bevestigingsmail van je verzoek.

3

Na 30 dagen

Al je gegevens worden definitief verwijderd.

Er is geen mogelijkheid meer om terug te keren.



Tips & Slot



Overweeg goed

Je verliest toegang tot berichten, foto's en vrienden.



Liever een pauze?

Deactiveer tijdelijk of gebruik alleen Messenger.



Hulp nodig?

Vraag ondersteuning bij twijfel of problemen.



IDfier: Veilig je identiteit verifiëren, persoon tot persoon

De IDfier is wereldwijd gelanceerd. Een systeem dat identiteitsverificatie van mens tot mens mogelijk maakt.

Eenvoudig én veilig controleren met wie je in contact komt. Zonder gedoe, zonder zorgen.

Hoe werkt IDfier?



Document scannen

Scan je paspoort, rijbewijs of identiteitskaart met je telefoon.



NFC-verificatie

Bij documenten met NFC scant IDfier ook de chip voor extra beveiliging.



Levensechtheidstest

Maak een korte hoofdbeweging om te bewijzen dat je echt bent.





Waarom IDfier kiezen?

Gebruiksvriendelijk

Het verificatieproces is eenvoudig en snel. Binnen enkele minuten ben je geverifieerd.

Maximale beveiliging

De combinatie van documentscans, NFC-technologie en levensechtheidstests maakt fraude vrijwel onmogelijk.

Direct controleren

Verifieer ter plekke iemands identiteit. Ideaal voor online afspraken of transacties.

Bescherming tegen fraude



Geen foto's of video's

De hoofdbeweging voorkomt verificatie met stilstaande beelden of opgenomen video's.



Deepfake-detectie

Geavanceerde technologie herkent kunstmatig gegenereerde beelden.



Documentvalidatie

Het systeem controleert echtheidskenmerken van officiële identiteitsdocumenten.



End-to-end versleuteling

Jouw gegevens blijven altijd veilig en privé.



Begin vandaag nog met IDfier

Download de app

Beschikbaar voor iOS en Android. Gratis te downloaden uit de app stores.

Maak je profiel aan

Volg de stappen voor verificatie. Het duurt slechts enkele minuten.

Start met verifiëren

Gebruik IDfier om anderen te controleren of laat jezelf verifiëren.

