

VEILIG DIGITAAL MAGAZINE





ClickFix: De Misleidende Cyberaanval

In de eerste helft van 2025 zag ClickFix een dramatische toename in populariteit als aanvalsmethode. Deze geavanceerde social engineering techniek is nu, na phishing, de meest voorkomende vorm van cyberaanval geworden.

Ontdek hoe deze misleidende methode werkt en hoe u zich kunt beschermen.



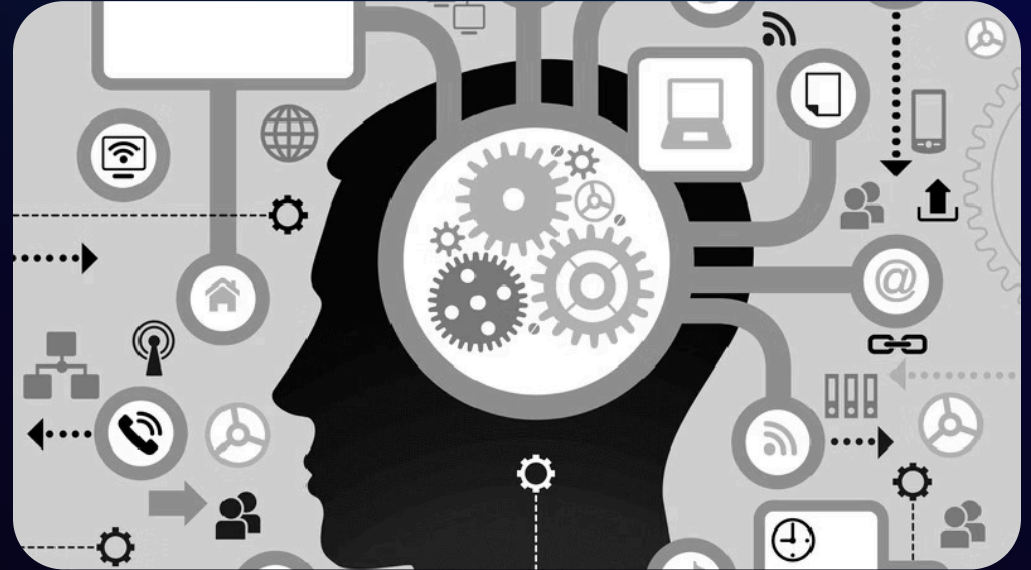
by VEILIG DIGITAAL

Wat is ClickFix?

ClickFix is een geavanceerde social engineering techniek die slachtoffers misleidt door:

- Valse systeemmeldingen en foutberichten te tonen die legitiem lijken
- Gebruikers te instrueren om zelf schadelijke opdrachten uit te voeren
- Slachtoffers te laten geloven dat ze een probleem oplossen

In tegenstelling tot traditionele malware voeren slachtoffers zelf de schadelijke commando's uit (kopiëren, plakken en uitvoeren), waardoor beveiligingssystemen worden omzeild.





Wie zit erachter?



Overheidsgesponsorde groepen

Verschillende statelijke actoren zijn geïdentificeerd achter ClickFix-aanvallen, waaronder Noord-Korea (TA457), Iran (TA450) en Rusland (TA422, UNK_RemoteRogue)



Groeiende adoptie

De grootste activiteit werd waargenomen tussen november 2024 en februari 2025, met snelle adoptie door zowel cybercriminelen als statelijke actoren



Georganiseerde verspreiding

Kennisdeling op cybercriminele fora heeft bijgedragen aan de snelle verspreiding van deze aanvalstechniek

Hoe werkt ClickFix in de praktijk?

Misleidende meldingen

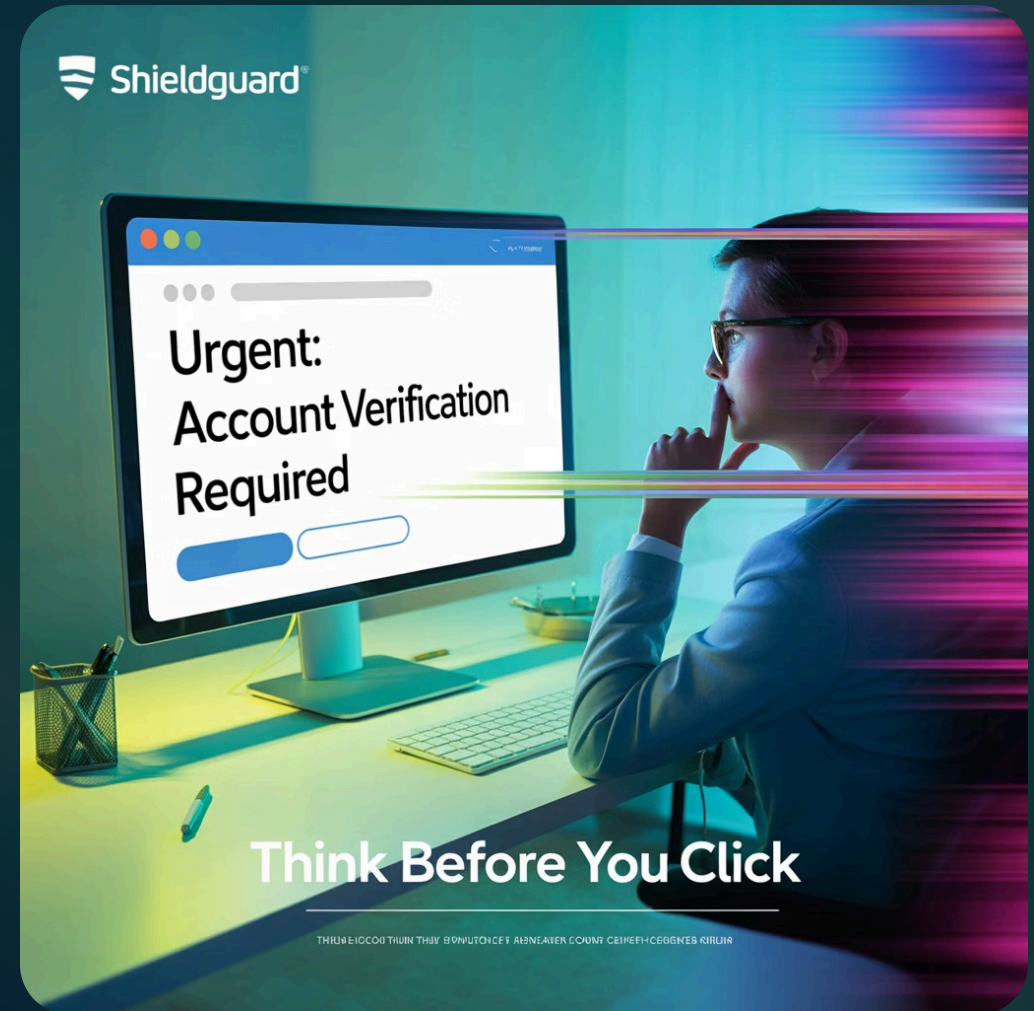
Slachtoffers ontvangen nepfouten of officieel ogende systeemwaarschuwingen

Valse oplossingen

De melding presenteert zich als oplossing, CAPTCHA-verificatie of registratieproces

Zelfuitvoering

Slachtoffers voeren zelf de schadelijke commando's uit, waardoor traditionele beveiligingsmaatregelen worden omzeild



Concrete incidenten 2024/2025

Eind 2024

Eerste ClickFix-aanvallen
gedocumenteerd op cybercriminele fora

1

Voorjaar 2025

Snelle verspreiding van de techniek na
publieke kennisdeling door
cybercriminelen

3

2

Begin 2025

Proofpoint detecteert Noord-Koreaanse
ClickFix-campagnes gericht op denktanks
en beleidsorganisaties

4

Eerste helft 2025

ClickFix groeit uit tot de tweede meest
voorkomende aanvalsmethode wereldwijd

Impact en bescherming

Uitdagingen

- Moeilijk te detecteren door legitiem ogende instructies
- Omzeilt traditionele beveiligingsmaatregelen
- Explosieve groei naar tweede plaats na phishing

Beschermingsmaatregelen

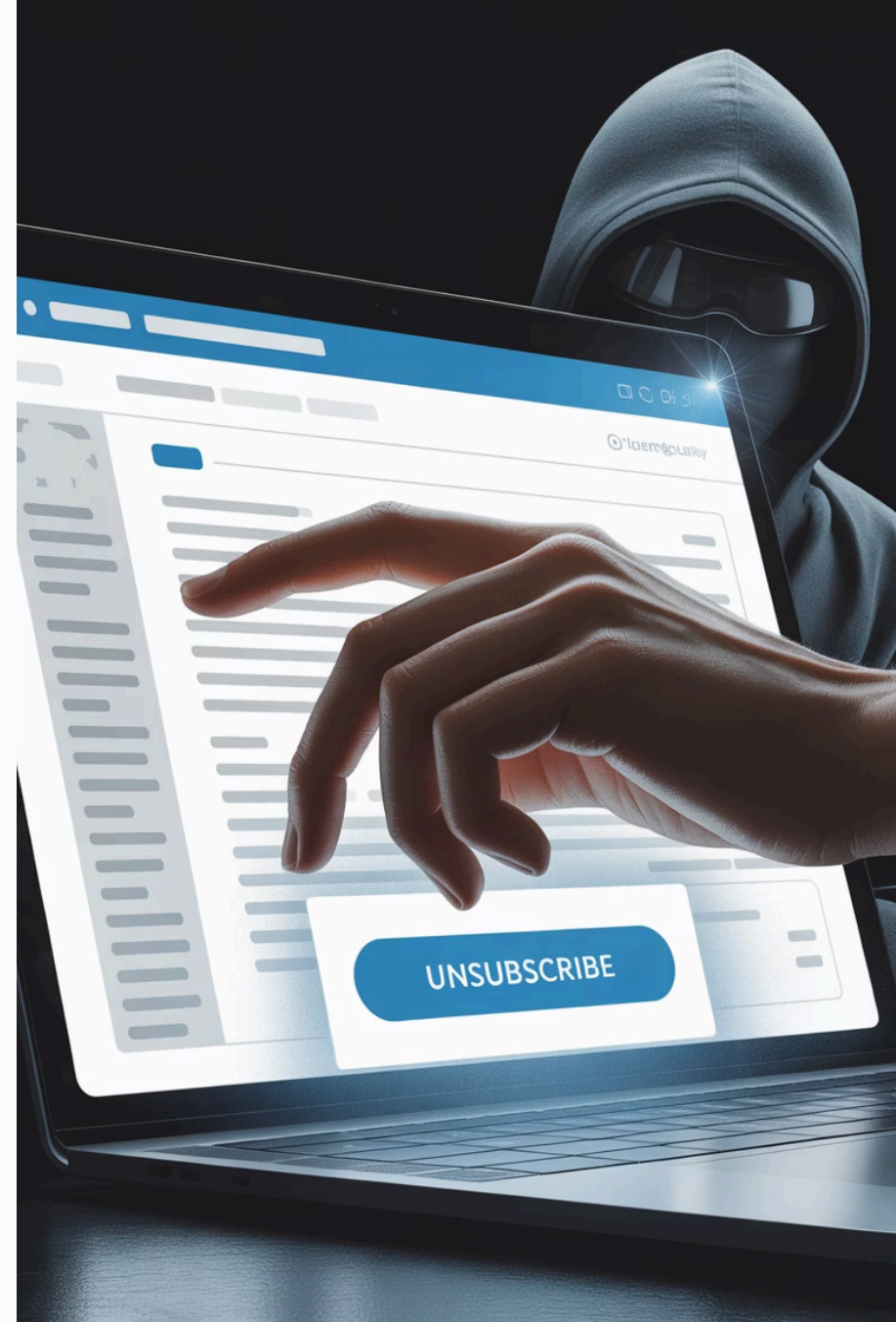
- Uitgebreide security-awareness training
- Technische restricties op opdrachtuitvoering
- Continue monitoring van verdachte activiteiten
- Zero-trust beveiligingsbeleid implementeren

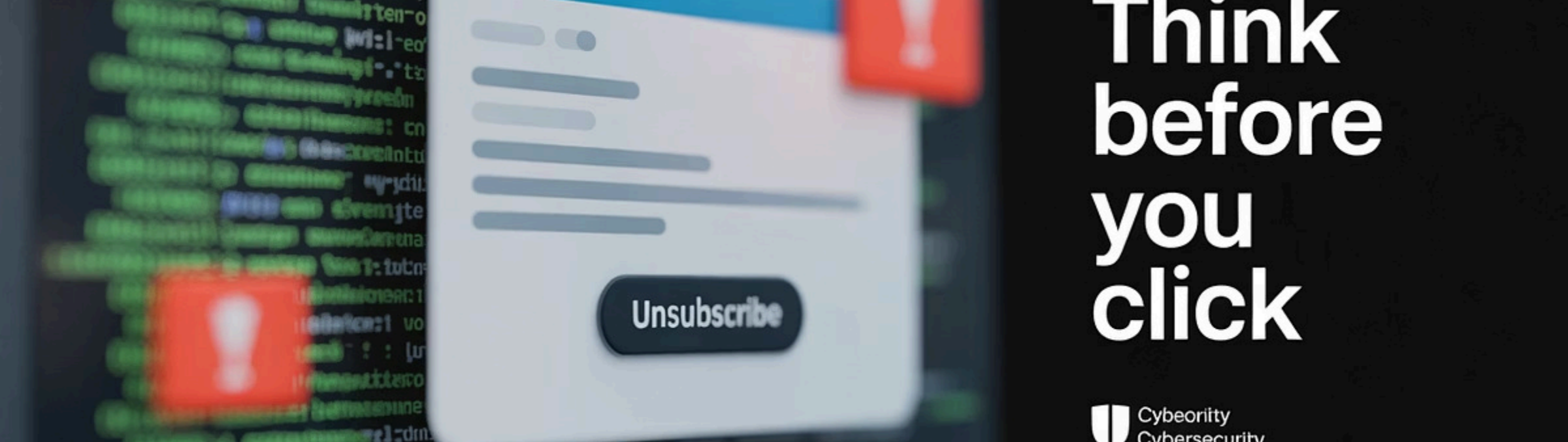
Denk na voordat u klikt: afmeldlinks als cyberrisico

Afmeldlinks in e-mails worden steeds vaker misbruikt door cybercriminelen. Veel mensen klikken automatisch op 'afmelden' bij ongewenste mails.

Experts waarschuwen dat dit klikgedrag kan leiden tot ernstige veiligheidsproblemen. Wees alert bij elke link in uw inbox.

VEILIGDIGITAAL.COM





Cybeority
Cybersecurity

Hoe worden afmeldlinks misbruikt?



Phishing

Valse afmeldlinks leiden naar nepwebsites die persoonlijke data stelen.



Gegevensdiefstal

Op nepwebsites worden inloggegevens of persoonsgegevens gevraagd.



Malware

Eén klik kan ongezien schadelijke software installeren op uw apparaat.

Be alert. Spot the phish.

Voorbeelden van recente aanvallen



Begin 2024

Hausse aan nepnieuwsbrieven met malware in Nederland.



Webwinkelfraude

Bekende webwinkels werden gekopieerd voor phishingcampagnes.



Slachtoffers

Duizenden Nederlanders deelden onbedoeld hun inloggegevens.



Wat zeggen beveiligingsexperts?

Automatisering niet voldoende

Geautomatiseerde tests kunnen niet alle risico's voorkomen. Menselijke controle blijft essentieel.

Browserrisico's

Alles wat uit de browser komt, wordt als gebruikersdata gezien. Dit kan misbruikt worden.

Handmatige verificatie

Voorzichtigheid is noodzakelijk bij e-mails met links. Controleer altijd de bron.



Veilig omgaan met afmeldlinks: praktische tips



Controleer adressen

Verifieer altijd het e-mailadres en webadres van de afmeldlink.



Gebruik officiële websites

Bij twijfel: ga direct naar de website van de afzender.



Up-to-date beveiliging

Zorg voor een spamfilter en actuele beveiligingssoftware.



Meld verdachte e-mails

Waarschuw uw IT-afdeling of het meldpunt internetfraude.



De Wereld is Gewoon Niet Veilig Genoeg voor Windows Recall

In dit artikel praten we over de veiligheidsrisico's van Microsoft's nieuwe Recall-functie. We duiken in de zorgen die beveiligingsexperts hebben over deze controversiële technologie die recent veel commotie heeft veroorzaakt.



by VEILIG DIGITAAL

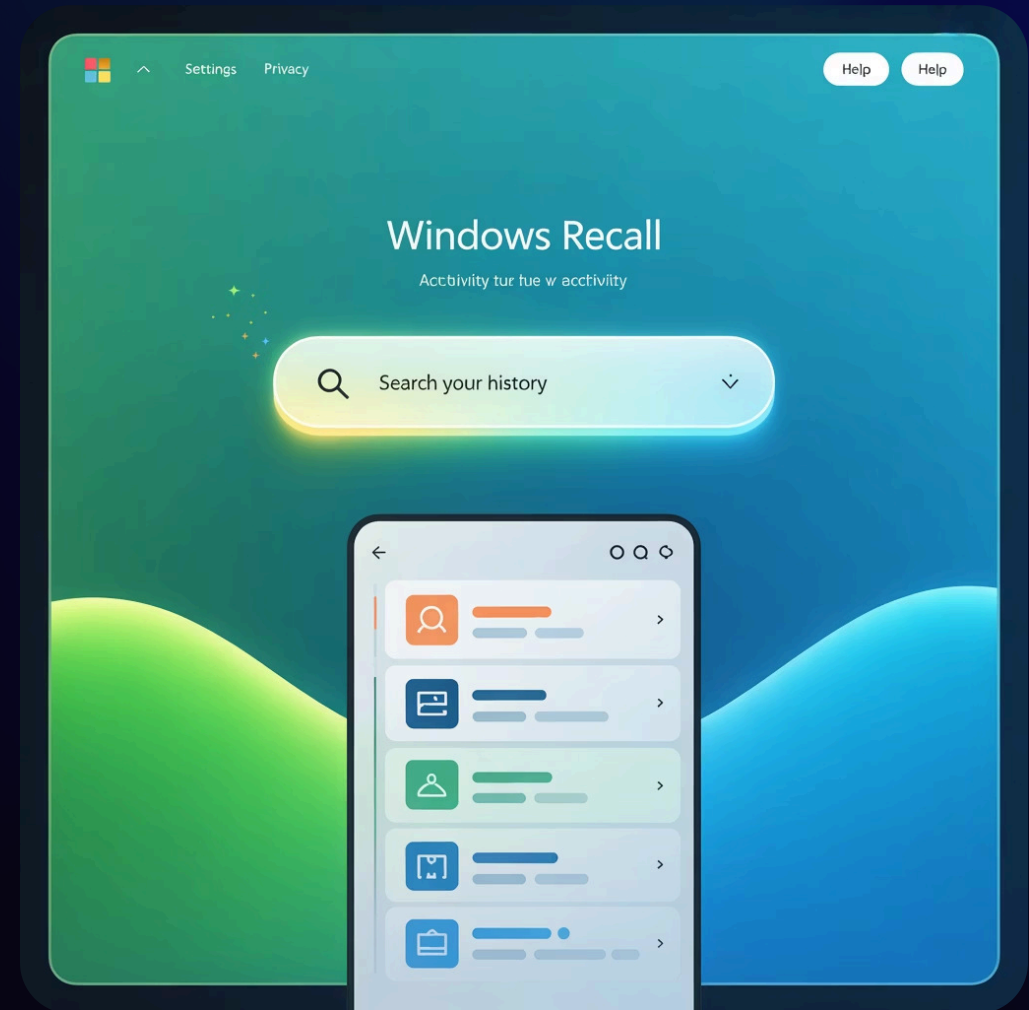
Wat is Windows Recall?

Nieuwe AI-functie

Standaard geïnstalleerd op nieuwe Copilot+ PC's

Maakt continu AI-gestuurde snapshots van gebruikersactiviteiten

Werkt als een "tijdmachine" voor je digitale activiteiten



Recall belooft een revolutionaire zoekfunctie te zijn die alles indexeert wat je ooit op je computer hebt gezien of gedaan.



Onvoldoende Beveiliging voor Gevoelige Data



Geen standaard versleuteling

Screenshots en zoekindex worden onversleuteld opgeslagen in een SQLite-database, direct toegankelijk voor kwaadwillenden



Malware-gevoeligheid

De onbeschermd database is een goudmijn voor hackers en malware die gegevens willen stelen



Fysieke kwetsbaarheid

Iedereen met fysieke toegang tot je apparaat kan potentieel je volledige digitale geschiedenis bekijken

Privacyzorgen: Een Permanente Keylogger?

Recall registreert automatisch:

- Persoonlijke berichten en chats
- Bankgegevens en wachtwoorden
- Medische en andere privé-informatie
- Werkgerelateerde vertrouwelijke documenten

Voor veel gebruikers voelt dit als een voortdurende invasie van privacy, vergelijkbaar met een keylogger die altijd actief is.



Technische Aanvallen: Prompt Injection & Extractie



Aanval op AI-model

Hackers kunnen Recall's AI-model manipuleren via prompt injection technieken



Gegevensextractie

Gevoelige informatie uit snapshots kan worden onttrokken, zoals bedrijfsgeheimen of persoonlijke gegevens



Verdere aanvallen

Gestolen informatie kan worden gebruikt voor gerichte phishing of identiteitsdiefstal



Reacties van de Security Community

"Windows Recall is een privacynachtmerrie die wacht om te gebeuren. Een goudmijn voor aanvallers en een nachtmerrie voor privacy-bewuste gebruikers."

- Bekende cybersecurity-expert

Sinds de lancering hebben talloze beveiligingsexperts hun zorgen geuit, wat Microsoft heeft gedwongen om de functie van standaard ingeschakeld naar opt-in te veranderen.



Kun je Recall Uitzetten of Verwijderen?

1

Uitschakelen mogelijk

Gebruikers kunnen Recall uitschakelen via instellingen, maar...

2

Niet volledig verwijderbaar

De functie blijft op het systeem aanwezig, zelfs na uitschakeling

3

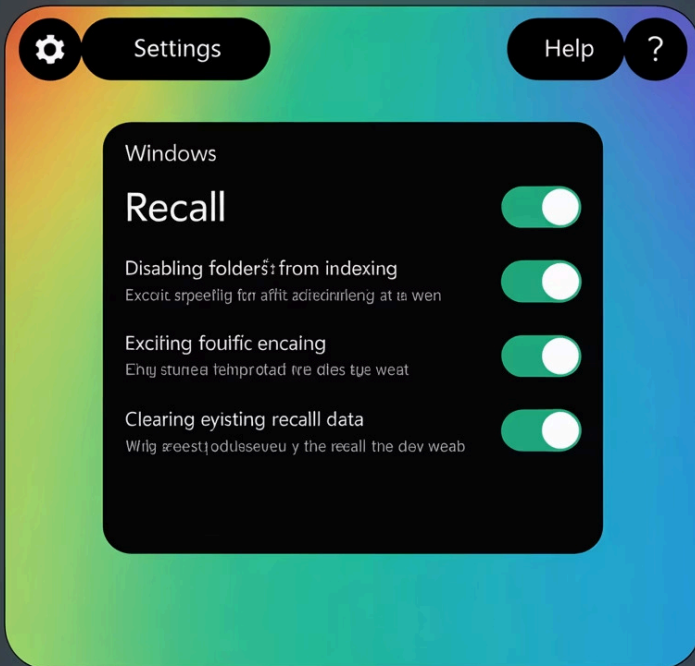
Slapende keylogger

Potentieel risico blijft bestaan, zelfs in uitgeschakelde toestand

4

Advies

Schakel Recall uit totdat Microsoft alle beveiligingsproblemen heeft opgelost



Conclusie: Recall past niet in een onveilige wereld

Risico's wegen zwaarder dan voordelen

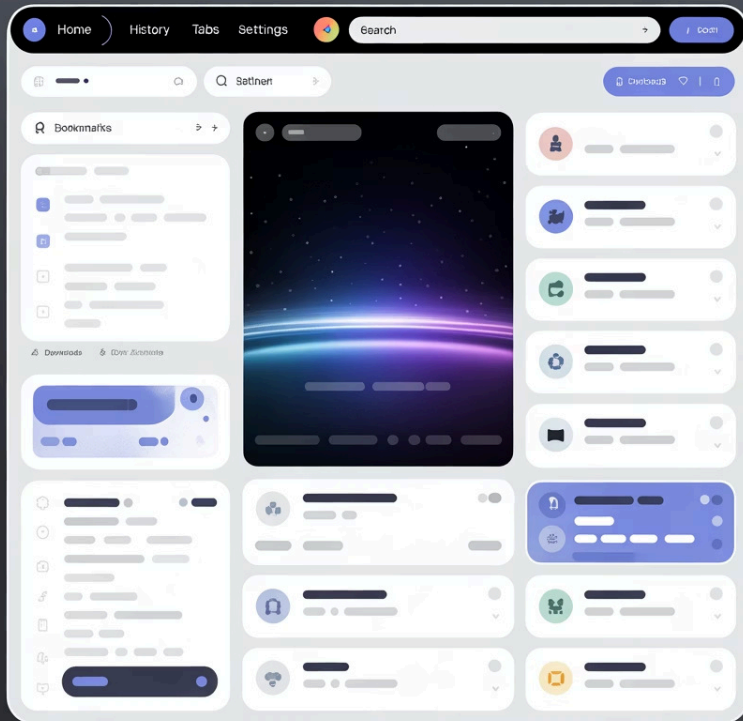
- Ernstige privacy-inbreuken
- Ontoereikende beveiliging voor gevoelige gegevens
- Wetgeving en bescherming lopen achter op technologie

Totdat Microsoft aantoonbaar veilige encryptie implementeert en privacy beter waarborgt, blijft Windows Recall een risico voor gebruikers wereldwijd.



Dacchoack

Doelgericht Webbrowser



DIA, de AI Webbrowser: Wat Maakt Het Goed?

Een innovatieve stap in het moderne internetgebruik: DIA combineert traditioneel browsen met krachtige AI-mogelijkheden om uw online ervaring te transformeren.



by VEILIG DIGITAAL

Unieke Kenmerken van DIA

Revolutionaire Browserfunctionaliteit

DIA onderscheidt zich door een naadloze integratie van AI in uw dagelijkse browsing-ervaring. Het biedt een compleet nieuwe manier om met het internet te interacteren.

1 Geïntegreerde Chat

Directe communicatie met je open browser-tabs voor snelle informatie-uitwisseling.

2 Naadloze AI-Integratie

AI-functionaliteit is direct beschikbaar binnen de browserinterface zonder externe tools.

3 Workflow-Automatisering

Automatiseert repetitieve taken en optimaliseert je internetgebruik voor maximale efficiëntie.



Voordelen voor Gebruikers



Tijdsbesparing

Door de geavanceerde AI-verwerking wordt informatie direct geanalyseerd en gepresenteerd, wat uren aan handmatig zoeken bespaart. Gebruikers rapporteren gemiddeld 40% tijdsbesparing bij onderzoekstaken.



Bronbeheer

De AI houdt meerdere bronnen bij en kan informatie combineren zonder dat je constant tussen tabs hoeft te schakelen. Ideaal voor studie, onderzoek en professioneel gebruik.



Gereduceerd Zoekwerk

DIA anticipeert op je informatiebehoeften en presenteert relevante gegevens voordat je er expliciet om vraagt, wat het aantal benodigde zoekopdrachten aanzienlijk vermindert.



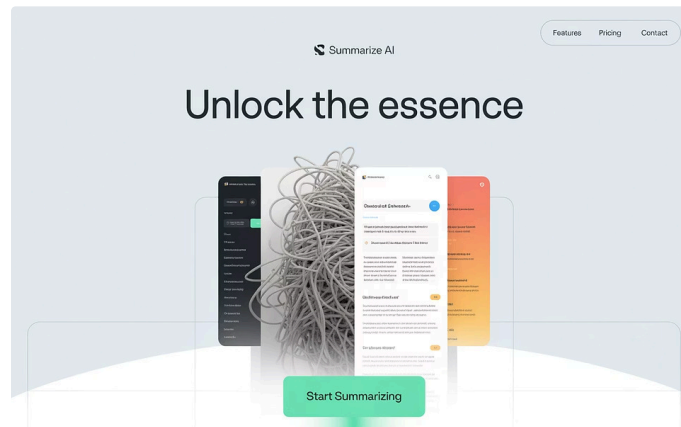
Innovaties in Kunstmatige Intelligentie

DIA implementeert geavanceerde AI-technieken die de manier waarop we online navigeren fundamenteel veranderen.



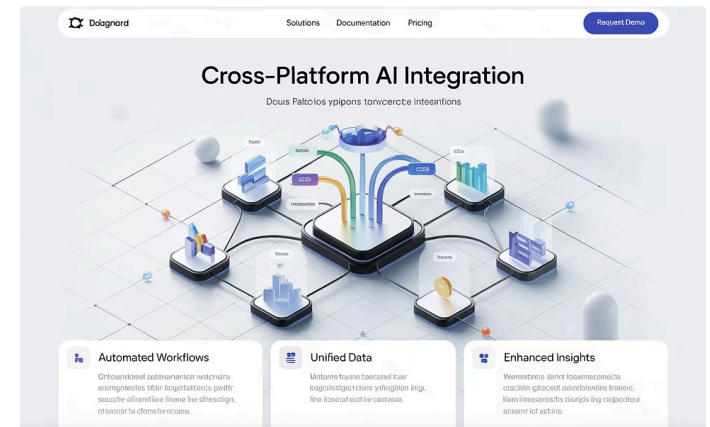
Natural Language Processing

Begrepen worden zonder technische commando's te leren - geef gewoon opdrachten in natuurlijke taal zoals "zoek het beste restaurant in de buurt".



Automatische Samenvattingen

Complexe webpagina's worden direct geanalyseerd en samengevat, waardoor je snel de essentie begrijpt zonder alles te lezen.



Cross-Platform Integratie

Naadloze verbinding met andere AI-diensten zorgt voor een uitgebreid ecosysteem van slimme hulpmiddelen.

Valkuilen en Uitdagingen



Privacy & Dataveiligheid

De AI-functionaliteit vereist toegang tot uw browsegegevens, wat potentiële risico's met zich meebrengt voor gegevensbescherming. DIA moet een balans vinden tussen functionaliteit en privacybescherming.



Contextuele Beperkingen

Ondanks geavanceerde algoritmen kan de AI soms de nuance of complexiteit van bepaalde webtaken missen, vooral bij creatieve of zeer gespecialiseerde onderwerpen.



Adoptie-Uitdagingen

Gebruikers die gewend zijn aan traditioneel browsen kunnen moeite hebben met de overstap naar een AI-gestuurde interface, wat een steile leercurve kan veroorzaken.



Protect your
digital life



Conclusie & Vooruitblik

De Toekomst van Browsen

DIA vertegenwoordigt een belangrijke evolutie in hoe we het internet ervaren en gebruiken. Met de juiste balans tussen innovatie en verantwoord gebruik kan het de standaard worden voor toekomstig webgebruik.

- Onderscheidend door naadloze AI-integratie en gebruiksgemak
- Blijf bewust van de beperkingen en privacyoverwegingen
- Enorm potentieel voor verdere ontwikkeling en verbetering

De slimme browser van vandaag vormt de basis voor het intelligente internet van morgen.

Download de DIA browser via: www.diabrowser.com



Grote Toename van SIM Swap Scams

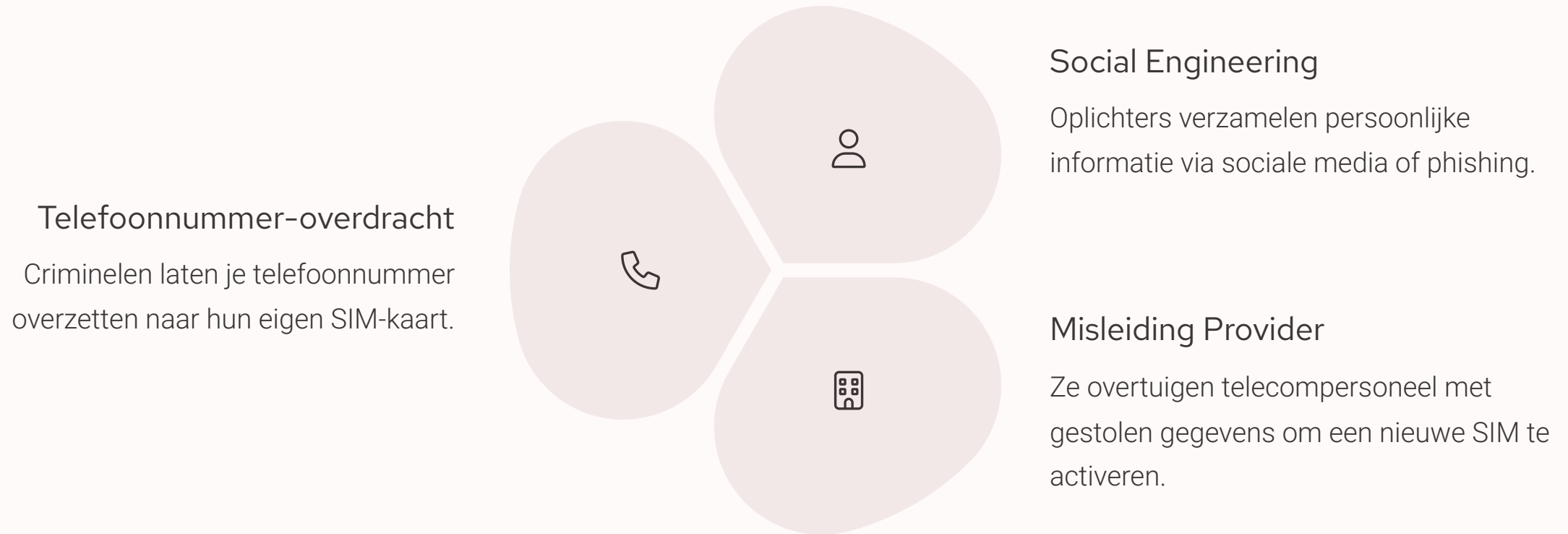
SIM swap scams vertonen een alarmerende stijging. In het VK zijn 3.000 onrechtmatige SIM-swaps gemeld in 2025.

Dit vertegenwoordigt een schrikbarende 1.055% toename sinds vorig jaar. De dreiging heeft nu wereldwijde proporties aangenomen. Nederland blijft niet achter.

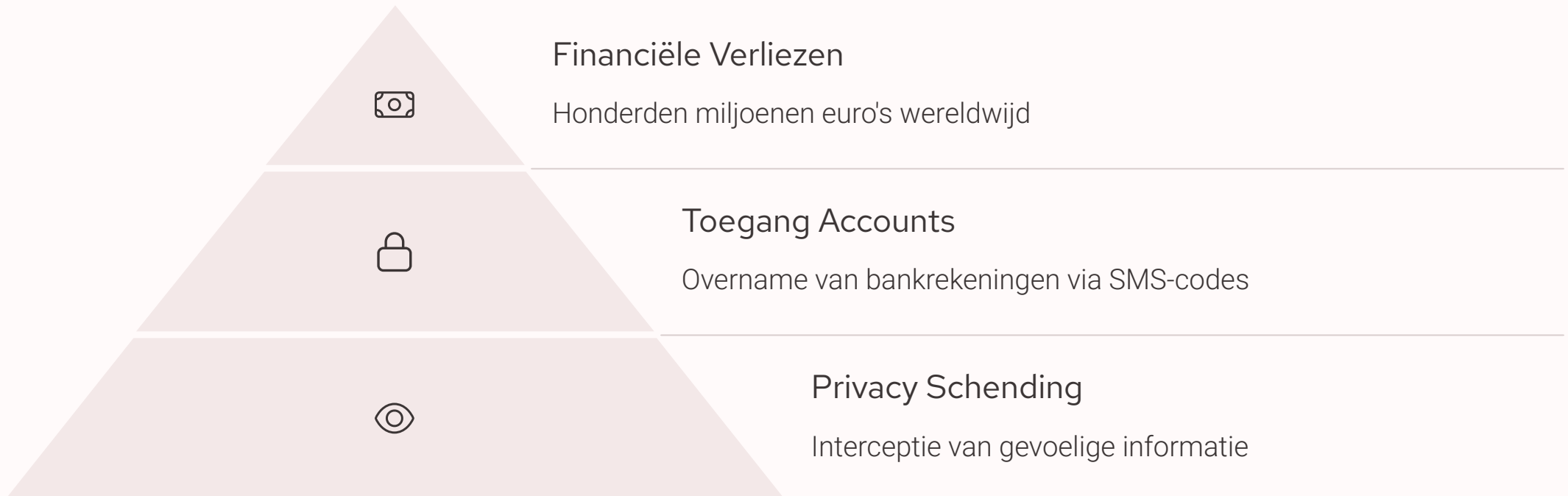
VEILIGDIGITAAL.COM



Hoe Werkt SIM Swapping in de Praktijk?



Risico's en Gevolgen van SIM Swap Fraud



SIM Swap Scams in Nederland

Lokale Trends

Nederland ziet vergelijkbare stijging in SIM swap fraude als andere Europese landen.

Betrokken Instanties

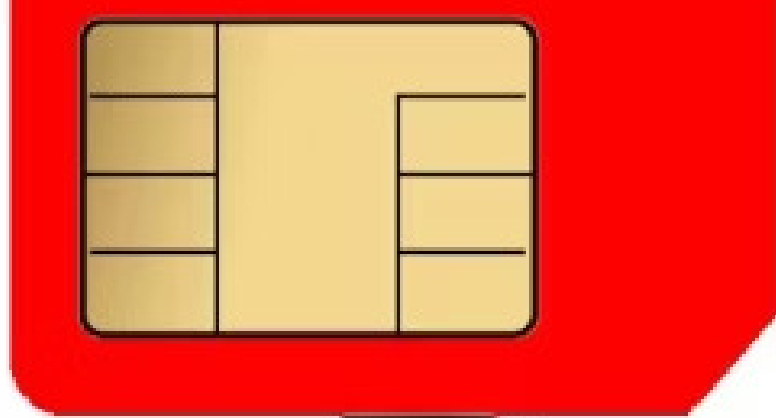
De Autoriteit Consument & Markt en politie werken samen aan preventie.

Nederlandse Aanpak

Telecombedrijven versterken identificatieprocedures bij SIM-kaartvervanging.

Meldpunt

Slachtoffers kunnen aangifte doen bij de politie en Fraudehelpdesk.



SIM card Swapping



Hoe Bescherm Je Jezelf Tegen SIM Swap Scams?

Authenticatie-apps Gebruiken

Vervang SMS-codes door apps zoals Google Authenticator of Microsoft Authenticator.

SIM-PIN Activeren

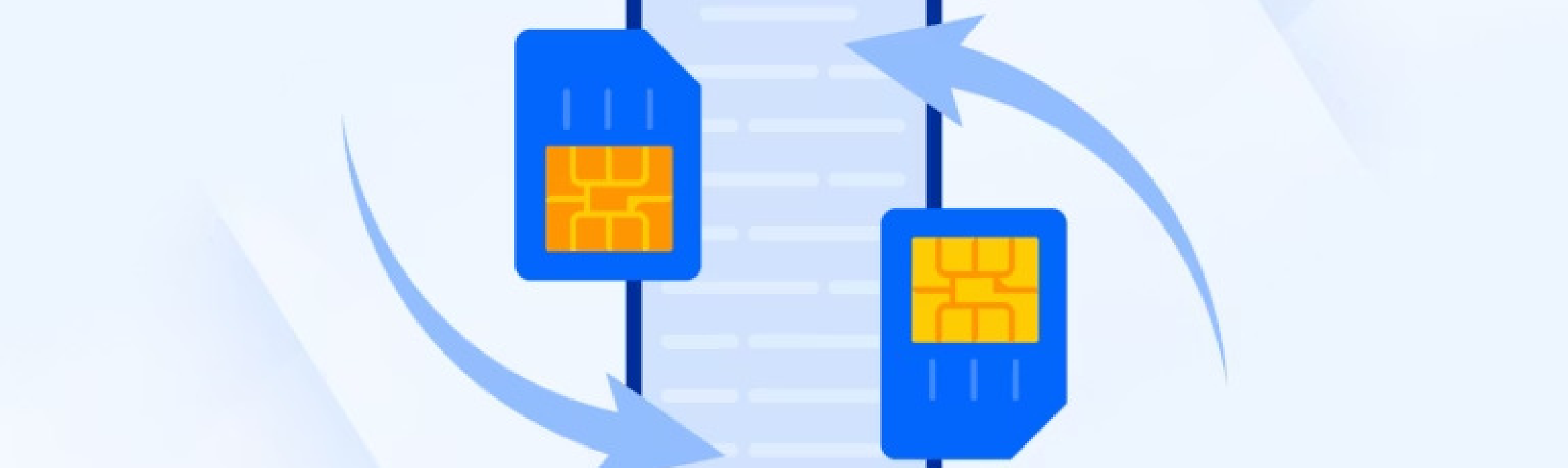
Stel een unieke SIM-PIN in bij je provider. Wijzig deze regelmatig.

Persoonlijke Gegevens Beschermen

Deel minimale informatie online. Controleer privacy-instellingen op sociale media.

Monitor Telefoonsignaal

Let op plotseling verlies van verbinding. Meld verdachte activiteiten direct.



Samenvatting en Slotwoord



Groeiende Dreiging

SIM swap scams nemen wereldwijd toe in frequentie en impact.



Preventieve Maatregelen

Proactieve bescherming is essentieel voor individuen en organisaties.



Bewustwording Creëren

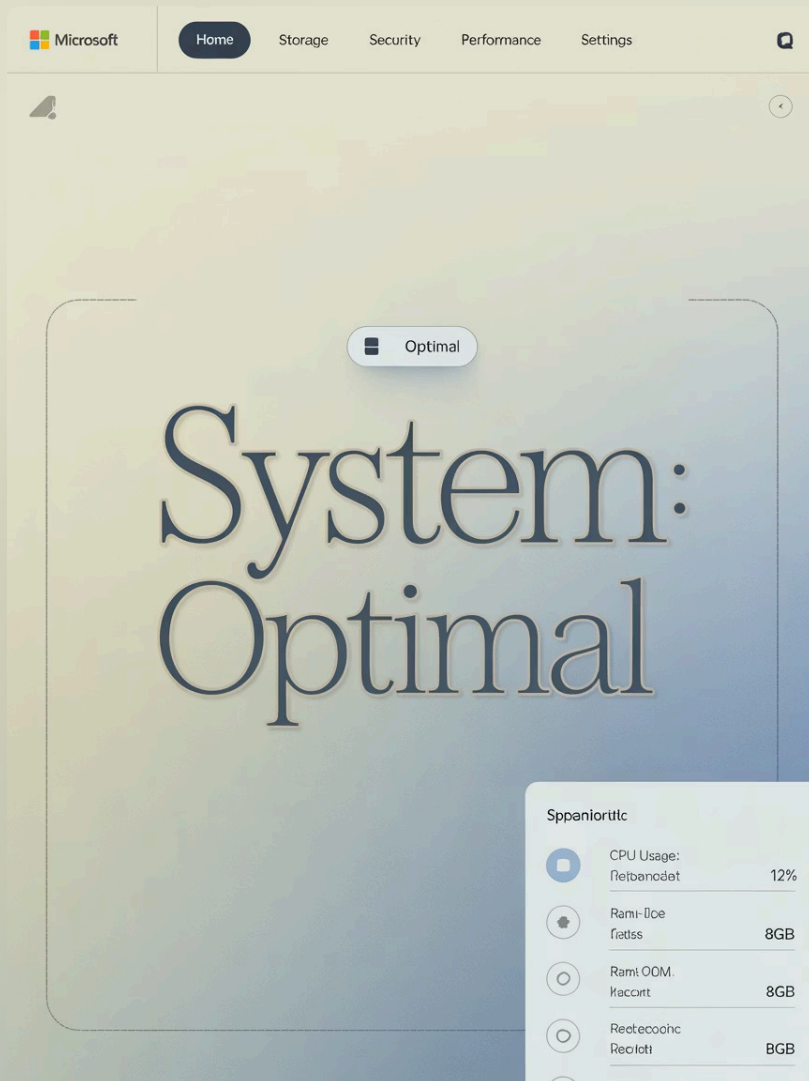
Informeer anderen over de risico's en beschermingsmethoden.

Is Microsoft PC Health Check veilig en betrouwbaar?

Microsoft PC Health Check. We onderzoeken deze handige diagnostische tool voor Windows-apparaten.

VEILIGDIGITAAL.COM





Wat is PC Health Check?

Gratis Microsoft Tool

Ontwikkeld voor Windows 10 en nieuwere versies. Volledig kosteloos te gebruiken.

Systeemdiagnostiek

Analyseert de gezondheid van je pc. Controleert hardware en softwarestatus.

Windows 11 Check

Beoordeelt of je apparaat klaar is voor Windows 11. Identificeert eventuele knelpunten.

Belangrijkste functies van PC Health Check



Compatibiliteitscheck

Controleert of je hardware voldoet aan Windows 11-eisen.



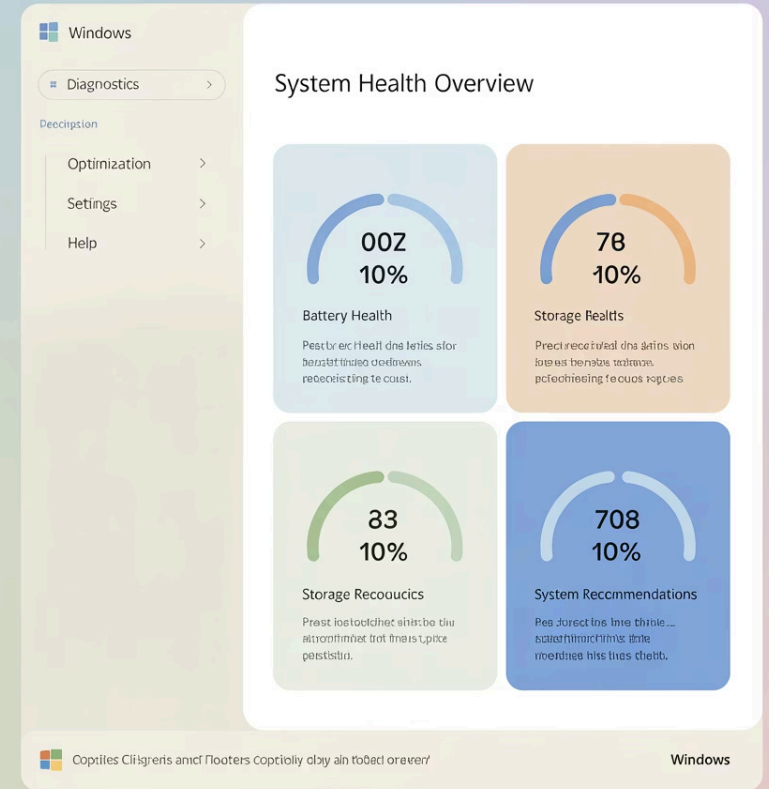
Statusoverzicht

Toont accu- en opslagstatus. Analyseert opstarttijden.



Aanbevelingen

Geeft tips over updates en back-ups. Biedt OneDrive-integratie.





Door wie wordt het ontwikkeld?



Officiële Microsoft-applicatie

Ontwikkeld door Microsoft zelf. Geen derde partijen betrokken.



Veilige distributie

Alleen beschikbaar via de Microsoft Support website.

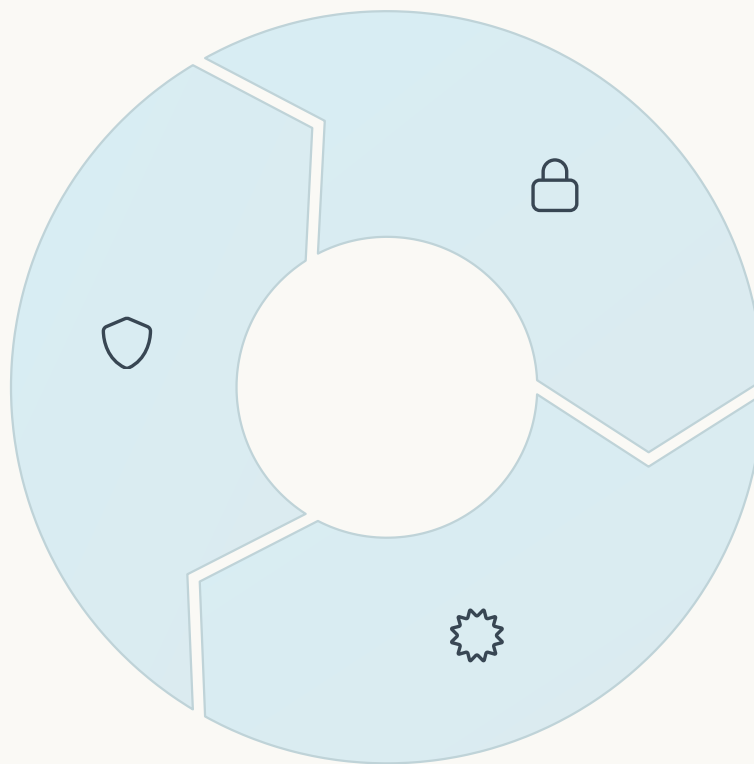


Regelmatige updates

Microsoft verzorgt automatische updates. Beveiligingspatches inbegrepen.

Veiligheid: Is PC Health Check veilig?

Betrouwbare code
Geen malware of adware.
Geverifieerde Microsoft-applicatie.



Privacybescherming

Werkt binnen Windows-omgeving. Volgt Microsoft-privacyrichtlijnen.

Officiële bron

Download alleen via Microsoft Support.
Vermijd onofficiële bronnen.

Mogelijke risico's en aandachtspunten



Misleidende downloads

Neplinks en phishing zijn gevaarlijk. Ze bootsen Microsoft-websites na.



Controleer de bron

Gebruik alleen microsoft.com URLs. Let op https-beveiliging.



Automatische updates

Updates kunnen niet worden uitgeschakeld. Dit beperkt gebruikerscontrole.

Betrouwbaarheid en gebruikerservaringen

1000+

Positieve reviews

Duizenden gebruikers bevestigen de betrouwbaarheid.

99%

Nauwkeurigheid

Hoge precisie bij Windows 11-compatibiliteitscheck.

<5%

Probleemgevallen

Beperkt tot niet-ondersteunde systemen.



Your PC.
Your peace of mind.



Conclusie



KeyScrambler vs. Ghostpress: Anti-Keylogger Software Vergelijking

Bescherming tegen keyloggers is essentieel voor computergebruikers vandaag de dag.

We vergelijken twee populaire oplossingen: KeyScrambler en Ghostpress.

Ontdek hoe u veilig kunt typen in een steeds onveiliger digitale wereld.

VEILIGDIGITAAL.COM



Wat zijn Keyloggers?



Kwaadaardige Software

Registreert elke toetsaanslag die u maakt op uw computer.



Gegevensdiefstal

Steelt wachtwoorden, creditcardgegevens en persoonlijke informatie.



Verspreiding

Via phishing, geïnfecteerde downloads en malware-aanvallen.



KeyScrambler



KeyScrambler: Overzicht



Encryptietechnologie

Versleutelt toetsaanslagen op laag niveau in het systeem.



Prestatie-impact

Kleine vertraging in toetsenbordrespons soms merkbaar.



Licenties

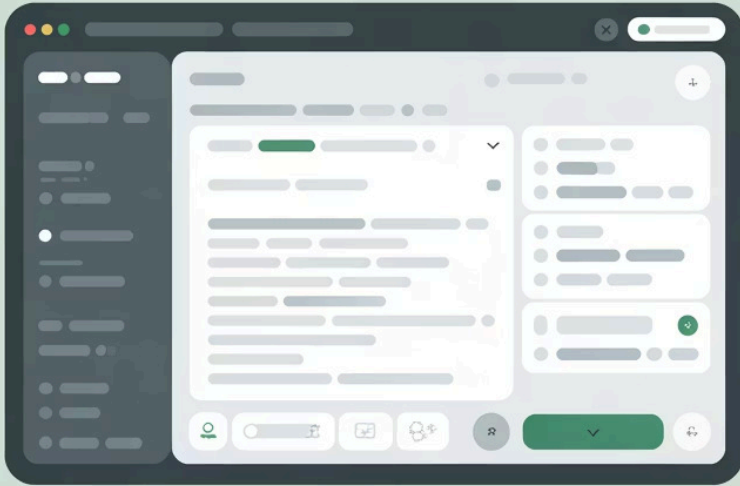
Betalende software met verschillende prijsniveaus beschikbaar.

GhostPress

File Edit View Insert Help

Security status:

Search documents



Document saved

Ghostpress: Overzicht

Gratis Bescherming

Kosteloos voor niet-commercieel gebruik, met robuuste beveiliging.

Gebruiksvriendelijk

Eenvoudige installatie en intuïtieve interface voor alle gebruikers.

Effectieve Beveiliging

Voorkomt het vastleggen van toetsaanslagen door schadelijke software.

Funcatievergelijking

Funcatie	KeyScrambler	Ghostpress
Low-level bescherming	Ja	Ja
Winlogon-bescherming	Beperkt	Volledig
Screenshot-bescherming	Nee	Ja (Pro)
Responsiviteit	Vertraging gemeld	Minimale impact

Ghostpress Licentiemodellen



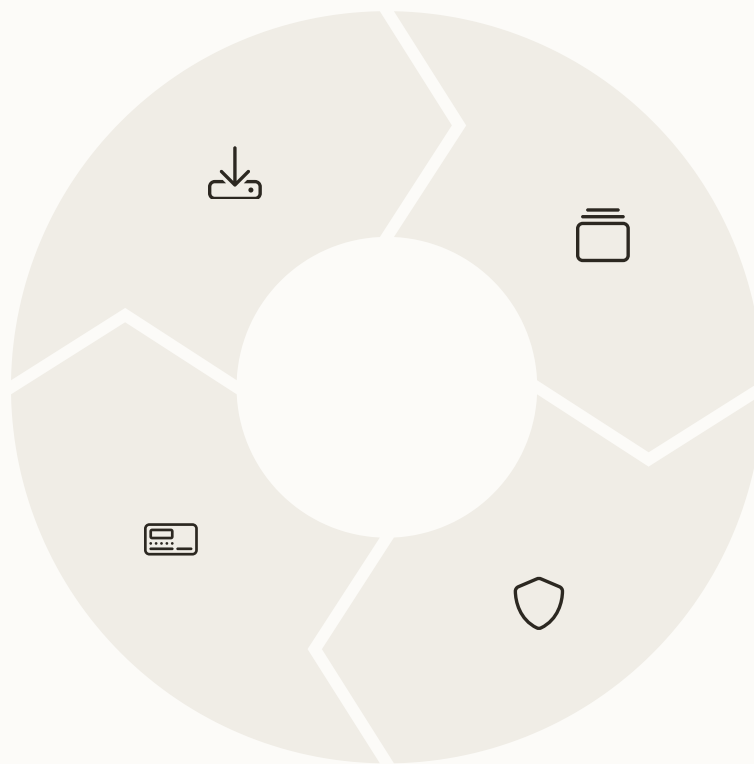
Praktische Overwegingen

Installatie

Ghostpress biedt eenvoudige installatie voor alle gebruikers.

Systeemprestaties

Minimale impact op computerprestaties bij beide oplossingen.



Betrouwbaarheid

KeyScrambler heeft een langere marktgeschiedenis.

Beschermingsniveau

Beide breken effectief de hooks die keyloggers gebruiken.

Conclusie en Aanbevelingen



Persoonlijk gebruik

Ghostpress (gratis) is een uitstekende keuze.



Zakelijk gebruik

Vergelijk KeyScrambler met Ghostpress Pro/Business.



Complete beveiliging

Combineer met andere beveiligingsmaatregelen voor optimale bescherming.

Microsoft Edge Scareware-blokker: Bescherming tegen digitale oplichterij

Een nieuwe beveiligingsfunctie in Microsoft Edge beschermt u sinds 2024 tegen digitale oplichterij. De Scareware-blokker herkent en stopt bedreigende waarschuwingen.

Deze functie is speciaal ontwikkeld als integraal onderdeel van de Microsoft Edge browser.

VEILIGDIGITAAL.COM



Wat is Scareware en waarom is het gevaarlijk?

Angstaanjagende tactieken

Scareware gebruikt valse waarschuwingen over virussen. Het zet gebruikers onder druk om "support" te bellen.

Ernstige gevolgen

Oplichters krijgen zo toegang tot uw computer. Ze gebruiken fullscreen-modus om ontsnappen moeilijk te maken.

Hoe werkt de Scareware-blokker in Edge?



AI-detectie



Machine learning op uw apparaat herkent verdachte pagina's.

Automatische bescherming



Breekt fullscreen-modus af bij vermoedens van een aanval.

Waarschuwing



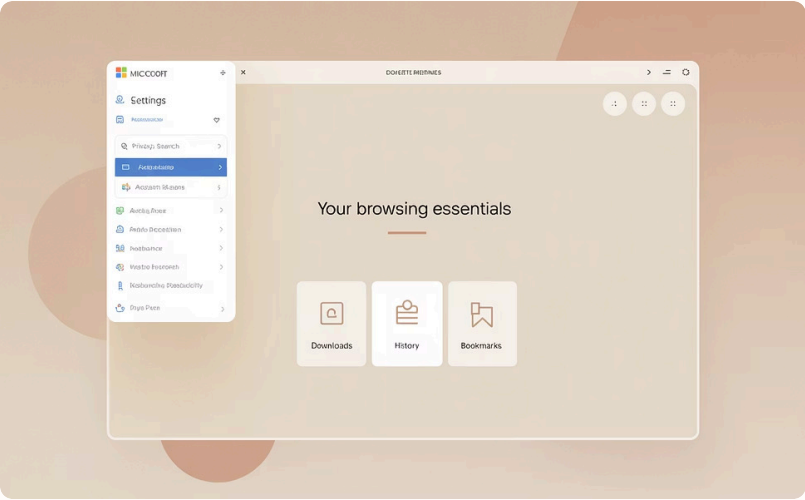
U kiest: doorgaan of de pagina sluiten.

Rapportage



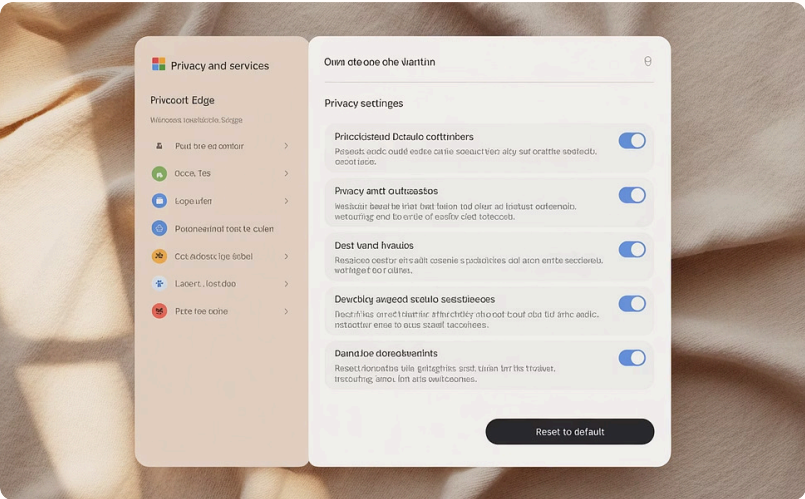
Meld scareware of fout-positieven aan Microsoft.

Hoe stel je de Scareware-blokker in?



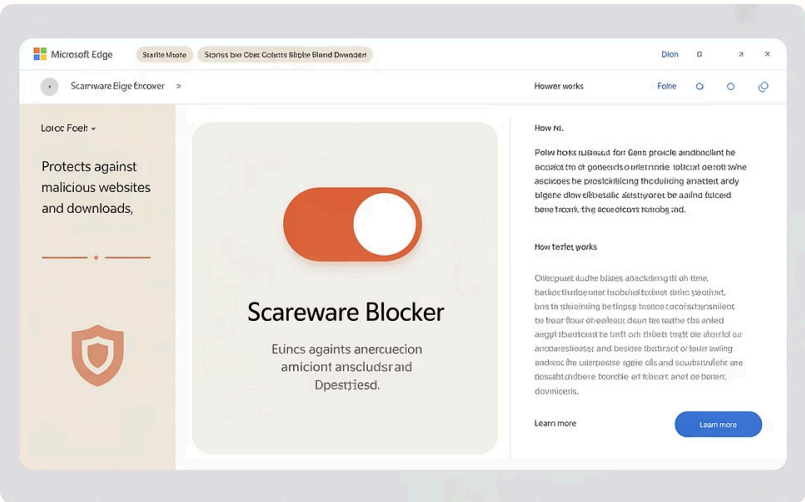
Open instellingen

Klik op de drie puntjes rechtsboven in Edge. Selecteer 'Instellingen'.



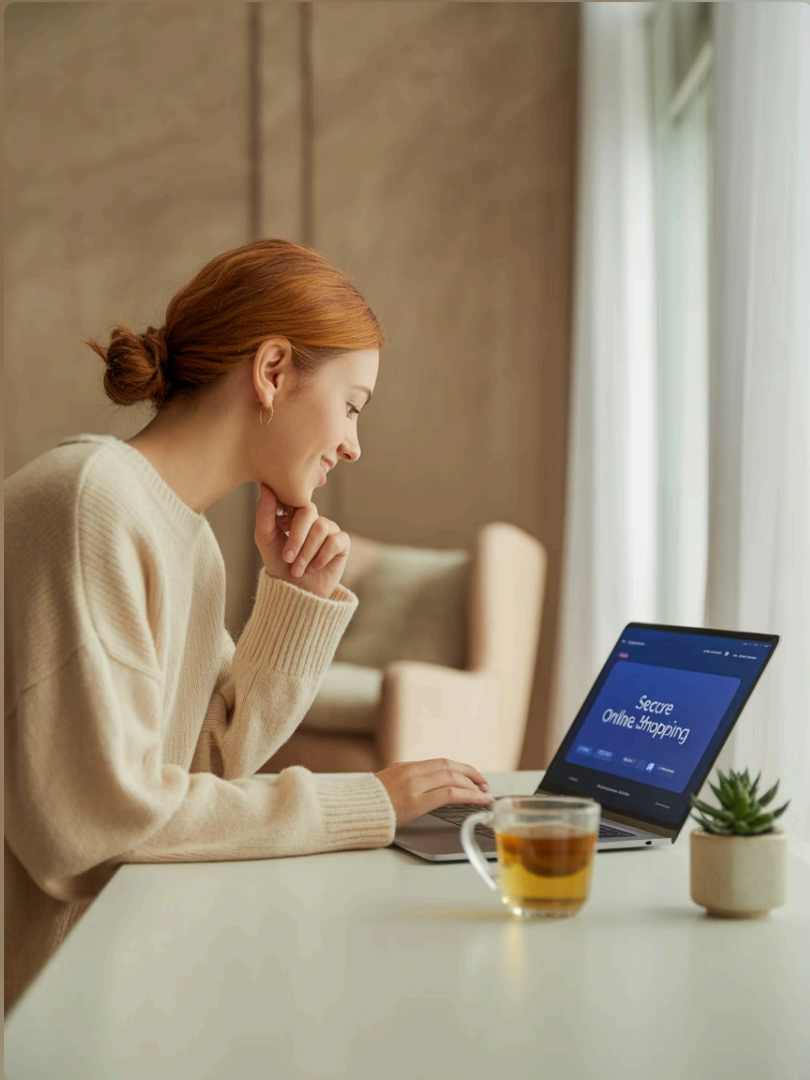
Privacy en beveiliging

Klik op 'Privacy, zoeken en services' in het linkermenu.



Scareware-bescherming

Scrol naar 'Beveiliging'. Zet de schakelaar bij 'Scareware-blokker' aan.



Samenvatting en tips voor veilig browsen



Extra beveiligingslaag

Edge Scareware-blokker beschermt tegen digitale oplichting.



Klik verstandig

Reageer nooit op verdachte waarschuwingen of onbekende telefoonnummers.



Escape-toets

Houd ESC ingedrukt om fullscreen-modus te verlaten.



Updates

Houd Edge en beveiligingsfuncties altijd up-to-date.



Meldingen op je telefoon: een risico voor hackers?

Jaarlijks worden tienduizenden Nederlanders
slachtoffer van hack-pogingen via hun telefoon.

Maar liefst 98% van alle Nederlanders ontvangt
dagelijks notificaties op hun smartphone.

Deze ogenschijnlijk onschuldige meldingen kunnen
een toegangspoort vormen voor cybercriminelen.

VEILIGDIGITAAL.COM

Hoe hackers meldingen kunnen misbruiken



Vervalste meldingen

Lokken naar valse websites voor phishing-aanvallen.



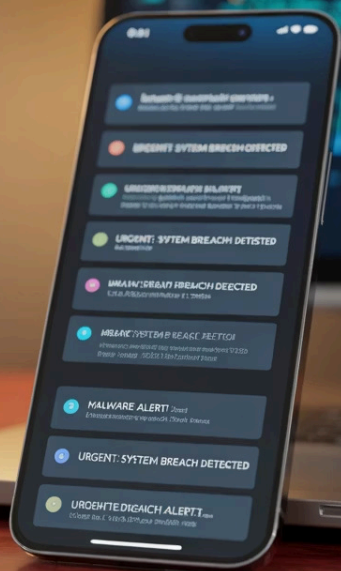
Kwaadaardige pushmeldingen

Moedigen installatie van malware aan.



Nep-beveiligingswaarschuwingen

Ontworpen om gevoelige gegevens te stelen.



Phishing via notificaties

Geloofwaardige meldingen

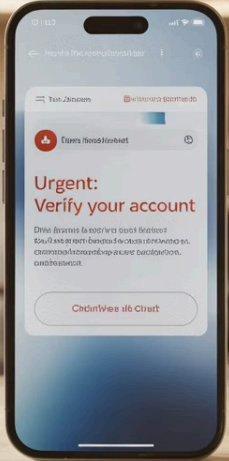
Hackers sturen notificaties die lijken te komen van banken of populaire apps.

Valse links

De link in de melding leidt naar een nauwkeurig nagemaakte loginpagina.

Gegevensdiefstal

Het doel is om je accountgegevens of bankgegevens te stelen.



Stay protected
PUESCOUIN SECURITY

Gevaar van Unicode-manipulatie

Unicode-kwetsbaarheid

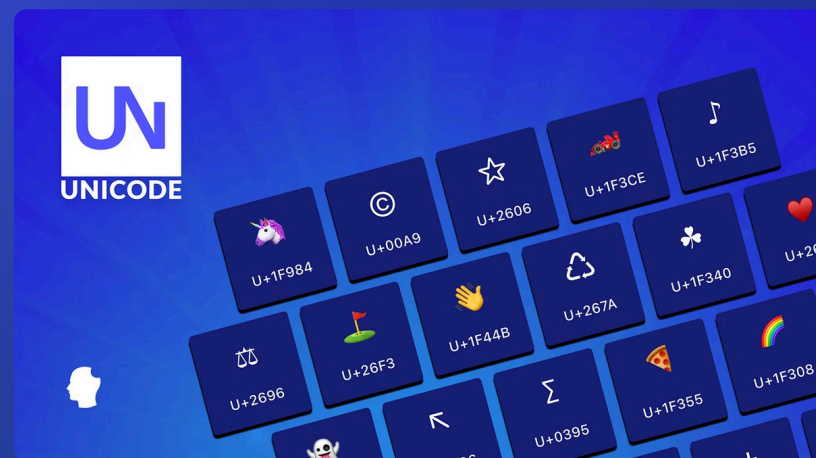
Android kan bepaalde Unicode-teken niet goed verwerken in meldingen.

Afgebroken links

Linktekst wordt in twee delen gesplitst door niet-werkende tekens.

Misleidende URLs

Een link lijkt naar Amazon.com te gaan, maar leidt eigenlijk naar DE malafide site zon.com



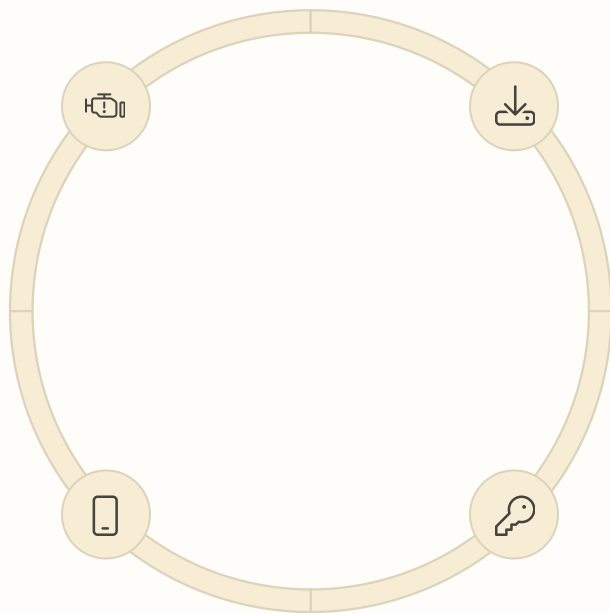
Schadelijke apps en meldingen

Verdachte pushmeldingen

Apps sturen meldingen met kwaadaardige links.

Apparaatcontrole

Hackers kunnen je telefoon overnemen.



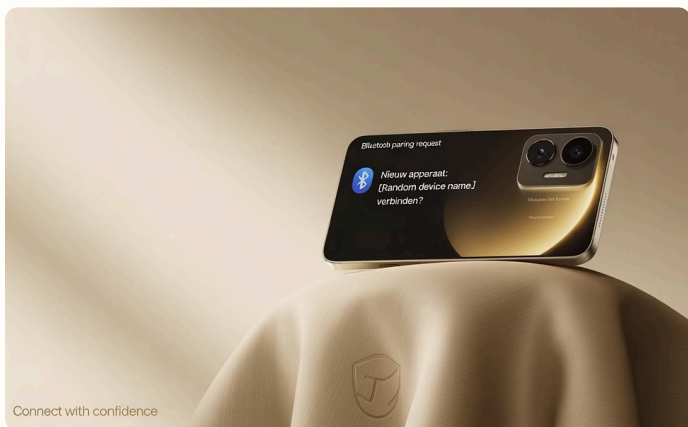
Malware-installatie

Eén klik kan schadelijke software installeren.

Gegevensdiefstal

Wachtwoorden en persoonlijke informatie worden gestolen.

Bluetooth- en Wifi-meldingen als aanvalskanaal



Valse verbindingsmeldingen

Hackers creëren meldingen over "nieuwe apparaten" of "verbinding maken". Deze lijken afkomstig van je besturingssysteem maar zijn nep.



Gegevens onderschepping

Via open WiFi/Bluetooth kan een hacker verbinding maken met je toestel. Gevoelige gegevens worden onderschept zonder dat je het doorhebt.



Risicolocaties

Drukke openbare plekken zoals stations en winkelcentra zijn favoriet. Hier kunnen hackers onopgemerkt toeslaan.

Tekenen van een gehackte telefoon



Ongewone meldingen

Notificaties van apps die je niet herkent zijn een waarschuwingssignaal.



Batterijproblemen

Snelle batterij-leegloop kan duiden op malware die actief is.



Onbekende apps

Apps die je niet zelf hebt geïnstalleerd wijzen op een hack.



Vreemde pop-ups

Onverwachte advertenties of meldingen zijn een slecht teken.



Bescherm je tegen notificatie-hacks



Samenvatting en advies

60%

Notificatiegebruikers

Checkt meldingen zonder na te denken

35%

Hack-risico

Kans op gegevensdiefstal via meldingen

90%

Preventie

Beschermingsgraad met juiste maatregelen

Meldingen kunnen een toegangspoort voor hackers zijn. Blijf kritisch op elke notificatie.

Voorkom schade door je systeem bij te werken. Wees alert op verdachte meldingen.

Bescherm je toestel met goede beveiligingssoftware en gezond verstand.

MU: Het nieuwe generatieve AI-systeem van Microsoft

MU is de codenaam voor Microsoft's meest geavanceerde AI-platform tot nu toe. Dit baanbrekende systeem is ontwikkeld binnen de Microsoft Cloud en Azure AI Foundry, met als belangrijkste speerpunten: verhoogde autonomie, diepgaande personalisatie en naadloze integratie in dagelijkse werkprocessen.

MU vertegenwoordigt een nieuwe generatie kunstmatige intelligentie die verder gaat dan wat we tot nu toe hebben gezien.

 by VEILIG DIGITAAL





MU AI



Autonome AI-agents

MU introduceert een volgende generatie AI-agents met ongekeende zelfstandigheid, waardoor complexe taken kunnen worden uitgevoerd met minimale menselijke supervisie.



Copilot Evolutie

GitHub Copilot evolueert van een eenvoudige assistent naar een volwaardige agentic partner die proactief meedenkt tijdens ontwikkelprocessen.



Nieuwe Tools

Microsoft heeft innovatieve tools zoals Copilot Studio en Windows AI Foundry gelanceerd om maximaal gebruik te maken van de mogelijkheden die MU biedt.

AI op Maat: Customisatie & Autonomie

Copilot Tuning

MU maakt het mogelijk om eigen AI-agents te creëren die specifiek zijn afgestemd op uw bedrijfsdata en -processen. Deze gepersonaliseerde agents leren continu van interacties en worden steeds effectiever naarmate ze meer worden gebruikt.

- 1 Geen programmeerkennis vereist - iedereen binnen de organisatie kan AI-agents aanpassen
- 2 Direct inzetbaar in bestaande bedrijfsprocessen zonder complexe integratie
- 3 Multi-Agent Orchestration laat meerdere gespecialiseerde agents samenwerken aan complexe taken

Praktische toepassingen van MU AI



MU wordt naadloos geïntegreerd in het hele Microsoft-ecosysteem, waaronder Microsoft 365, Power BI, Edge en Windows 11. Dit zorgt voor een consistente AI-ervaring over alle platforms.

INTRODUCING
MU



Juridische Toepassingen

Advocatenkantoren kunnen automatisch juridische argumenten genereren op basis van interne kennisbanken en precedenten, wat de efficiëntie drastisch verhoogt.



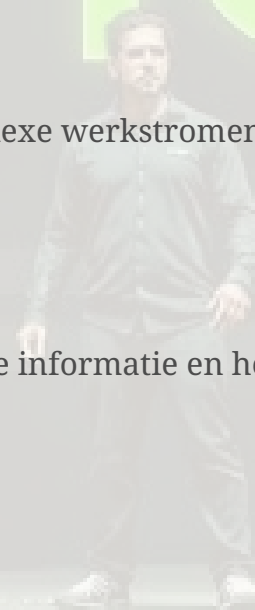
Workflow Optimalisatie

AI-agents stroomlijnen bedrijfsprocessen door routinetaken over te nemen en complexe werkstromen te coördineren zonder menselijke tussenkomst.



Klantgerichte Oplossingen

Gepersonaliseerde agents kunnen klantinteracties beheren met toegang tot relevante informatie en het vermogen om direct oplossingen aan te bieden.

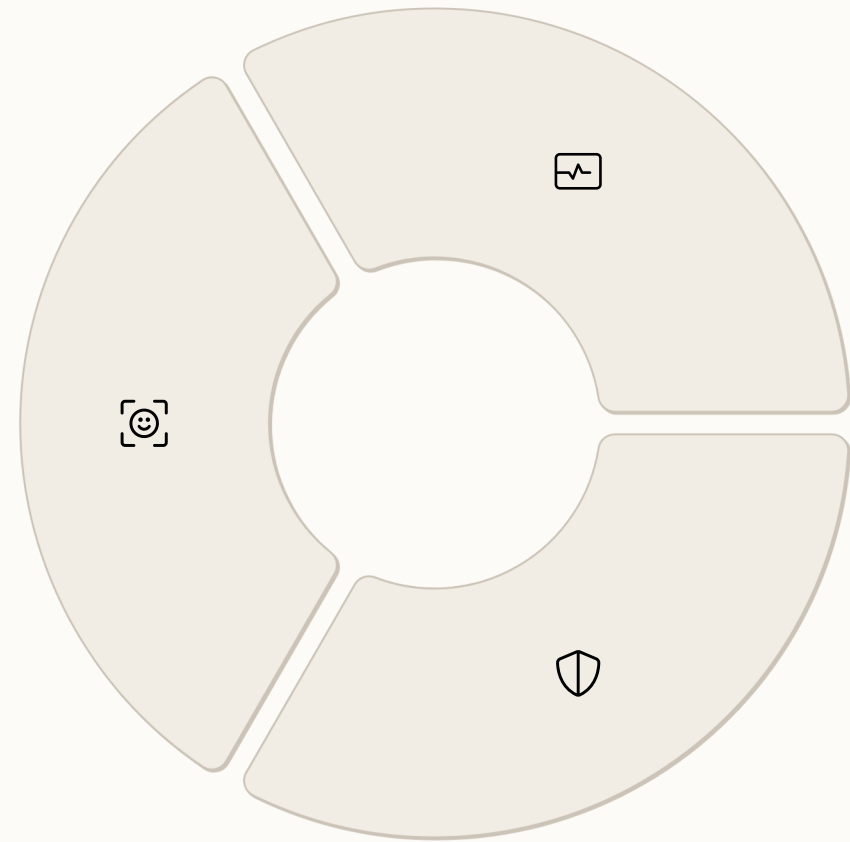


Veiligheid, Toezicht en Beheer

Enterprise-grade Beveiliging

Microsoft heeft veiligheid en privacy als topprioriteit gesteld bij de ontwikkeling van MU. Het nieuwe Entra Agent ID-systeem biedt gedetailleerd beheer over alle AI-agents binnen een organisatie.

Bedrijven krijgen toegang tot gecentraliseerd toezicht op hun AI-systemen, waardoor ze volledige controle behouden over hoe, waar en wanneer AI wordt ingezet.



Entra Agent ID

Beveiligde identiteiten voor elke AI-agent met gedetailleerde toegangscontrole



Monitoring

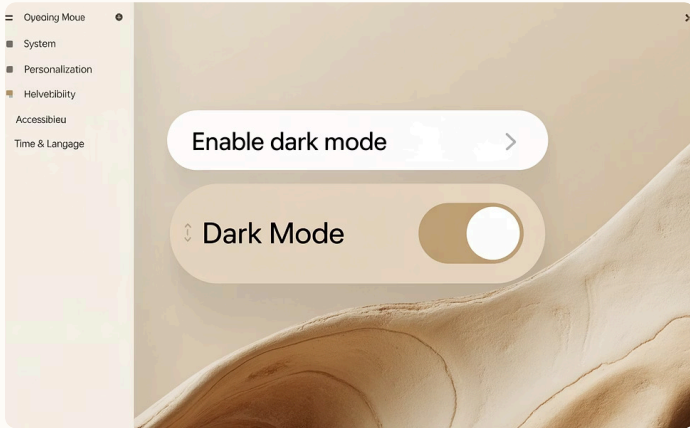
Realtime toezicht op alle AI-activiteiten binnen de organisatie



Privacy

Geavanceerde dataprotectie bij het tunen en inzetten van AI-agents

MU nog niet voor iedereen



Natuurlijke taalbesturing

Met Mu kunnen mensen hun computer bedienen met behulp van gewone taal. Je kunt bijvoorbeeld typen of zeggen: "zet de donkere modus aan" of "maak mijn muisaanwijzer groter", en de computer voert deze taken automatisch uit. Mu verschijnt eerst in de Windows 11-instellingen-app.



Lokaal draaiend taalmodel

Mu is een **klein taalmodel** (SLM) met een relatief schamele 330 miljoen parameters. Het is geen chatbot gebaseerd op een LLM die in de cloud draait, maar een SLM die volledig op de pc werkt, zelfs zonder internetverbinding.



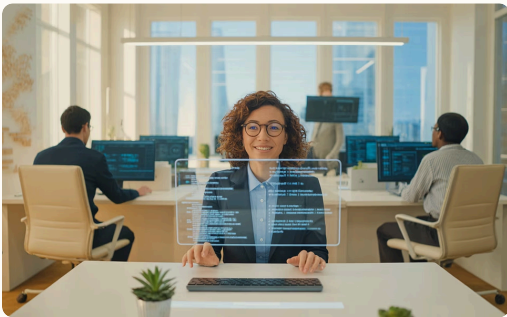
Copilot+ pc's met NPU

Mu is gebouwd om te draaien op een gespecialiseerde AI-chip, een zogenaamde **neural processing unit** (NPU). Deze chip is alleen te vinden in de nieuwste Copilot+ pc's van Microsoft, Dell, HP, Lenovo, Samsung en Acer, die sinds juni 2024 leverbaar zijn.

Samenvatting & Toekomstperspectief

Microsoft's MU-platform is ontworpen om generatieve AI de nieuwe standaard te maken in zowel zakelijke omgevingen als thuisgebruik. De snelle ontwikkeling van autonome, veilige agents zal de manier waarop we werken fundamenteel veranderen.

"MU vertegenwoordigt een nieuwe fase in onze AI-strategie, waarbij we streven naar systemen die niet alleen reageren, maar anticiperen en samenwerken."



Blijvende Innovatie

Microsoft blijft innoveren met een sterke focus op praktische bruikbaarheid in dagelijkse toepassingen



Veiligheid & Privacy

Veiligheid en privacy blijven fundamentele pijlers van de MU-ontwikkeling en implementatie



Naadloze Integratie

Naadloze integratie met bestaande systemen zorgt voor snelle adoptie in diverse werkomgevingen



Toekomstige Ontwikkelingen

Verwacht nog meer baanbrekende ontwikkelingen in de nabije toekomst van Microsoft's AI-initiatieven

Nederlands DNS-gebaseerd Anti Phishing Shield: Een Innovatieve Samenwerking

Het Nationaal Cyber Security Centrum (NCSC) en KPN slaan de handen ineen om deze zomer een baanbrekend project te lanceren: het DNS-gebaseerde Anti Phishing Shield.

Dit innovatieve systeem heeft als doel Nederlandse internetgebruikers te beschermen tegen de groeiende dreiging van phishing-aanvallen door verdachte websites te blokkeren voordat gebruikers er schade van ondervinden.

 by VEILIG DIGITAAL



KPN Solutions Services Threat Intelligence Partners [Contact Us](#)

Protecting Dutch Digital Infrastructure

Advanced cybersecurity solutions tailored for businesses and government entities

[Learn more](#)



Potential security threat detected

Go to **safe website**

Wat is een Anti Phishing Shield (APS)?

Waarschuwingssysteem

Een Anti Phishing Shield (APS) is een geavanceerd beveiligingssysteem dat internetgebruikers automatisch naar een waarschuwingspagina doorstuurt wanneer zij proberen een malafide website te bezoeken. Hiermee wordt voorkomen dat gebruikers slachtoffer worden van phishing-aanvallen.

DNS-filtering

Het systeem maakt gebruik van DNS-filters om phishing-websites te identificeren en te blokkeren. Deze aanpak werkt op netwerkniveau, waardoor er geen software op de apparaten van gebruikers geïnstalleerd hoeft te worden.

Gebruikersbescherming

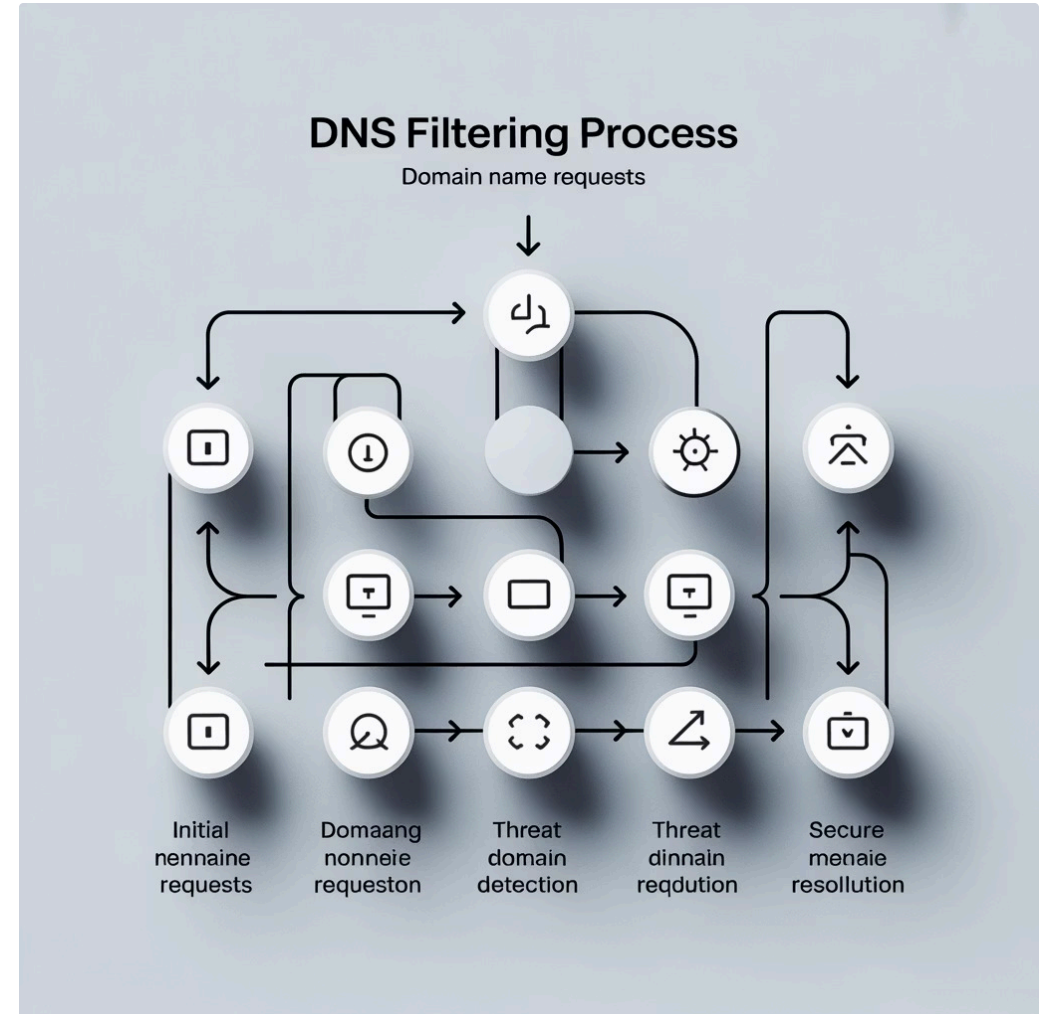
In plaats van toegang te krijgen tot een kwaadaardige website, ziet de gebruiker een duidelijke waarschuwingspagina die uitlegt waarom de toegang is geblokkeerd en welke risico's er verbonden zijn aan het bezoeken van de website.

De rol van DNS in APS

Het Domain Name System (DNS) vormt de ruggengraat van het internet en vertaalt domeinnamen naar IP-adressen. Door deze fundamentele functie te benutten, kan het Anti Phishing Shield fungeren als een krachtige eerste verdedigingslinie tegen phishing-aanvallen.

Bij het APS-systeem wordt elke DNS-aanvraag gecontroleerd tegen een regelmatig bijgewerkte database van bekende malafide domeinen. Wanneer een match wordt gevonden, wordt de verbinding geblokkeerd voordat de gebruiker zelfs maar de kans krijgt om met de schadelijke website te interacteren.

Een belangrijk voordeel van deze aanpak is dat er minimale vertraging optreedt voor de eindgebruiker en er geen extra software op apparaten geïnstalleerd hoeft te worden, wat de gebruiksvriendelijkheid ten goede komt.





Opzet van de pilot in Nederland

1

Zomertest 2025

Het NCSC en KPN starten in de zomer van 2025 met een uitgebreide testfase van het Anti Phishing Shield. Gedurende deze periode worden de effectiviteit en gebruikerservaring nauwkeurig gemonitord en geëvalueerd.

2

Selectie van deelnemers

Een zorgvuldig geselecteerde groep Nederlandse internetgebruikers en bedrijven wordt uitgenodigd om deel te nemen aan de pilot. Deze groep vertegenwoordigt verschillende typen gebruikers om een representatief beeld te krijgen van de werking van het systeem.

3

Real-time analyse

Tijdens de testfase wordt het DNS-verkeer in real-time geanalyseerd om phishingrisico's te identificeren. Dit stelt het team in staat om de effectiviteit van het systeem direct te beoordelen en waar nodig aanpassingen door te voeren.

Betrokken partijen en samenwerking



NCSC

Het Nationaal Cyber Security Centrum levert essentiële coördinatie en expertise op het gebied van cyberdreigingen. Hun kennis van actuele phishing-technieken en aanvalsvectoren is cruciaal voor het succes van het project.



KPN

Als grote Nederlandse telecomprovider zorgt KPN voor de technische uitvoering en netwerktoegang. Hun infrastructuur maakt het mogelijk om het APS op grote schaal te implementeren en te testen.

Het hoofddoel van deze samenwerking is om de landelijke schaalbaarheid van het Anti Phishing Shield te onderzoeken en te bepalen of een nationale uitrol haalbaar en effectief zou zijn in de Nederlandse context.

Protecting
your digital future



Verwachte impact en vervolg



Verhoogde digitale veiligheid

Met de implementatie van het APS wordt verwacht dat de digitale veiligheid voor Nederlandse internetgebruikers significant zal verbeteren. Phishing-aanvallen vormen momenteel een van de grootste cyberdreigingen voor burgers en bedrijven.



Snelle detectie en blokkade

Door de real-time monitoring kunnen nieuwe phishingcampagnes snel worden gedetecteerd en geblokkeerd, vaak nog voordat ze op grote schaal slachtoffers kunnen maken. Dit vermindert de effectiviteit van cybercriminelen aanzienlijk.



Evaluatie en implementatie

Na afloop van de zomertest volgt een grondige evaluatie van de resultaten. Bij positieve uitkomsten kan vanaf 2026 een bredere implementatie worden overwogen, mogelijk zelfs op nationale schaal.