

# VEILIG DIGITAAL MAGAZINE





# 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.



# Cloud Computing en Aanvalsmethoden

Cloud computing zorgt ervoor dat dienstverlening of gegevens plaats onafhankelijk, snel en gemakkelijk beschikbaar zijn. Dit met weinig inspanning van de organisatie zelf en geringe interactie met de leverancier.

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



# Wat is Cloud Computing?



## Plaats onafhankelijk

Toegang tot gegevens en systemen vanaf elke locatie.



## Meerdere apparaten

Benaderbaar via pc, tablet en mobiele apparatuur.



## Kostenefficiënt

Verschuiving van grote investeringen naar 'huren op maat'.



## Flexibel

Eenvoudig opschalen of afbouwen van ICT-diensten.



# Risicokenmerken van de Cloud

## Minder controle

Als afnemer heeft u minder controle over waar 'de eigen gegevens' precies staan opgeslagen.

## Gekoppelde servers

Cloud-leveranciers maken vaak gebruik van verschillende gekoppelde servers om diensten te leveren.

## Gevoelige gegevens

Wanneer u met gevoelige gegevens werkt, is controle hierover van groot belang.



# Verschijningsvormen van Cloud Computing

## Publieke Cloud

Cloud-infrastructuur beschikbaar voor het algemene publiek. Beheerd door een externe dienstverlener via internet. Biedt schaalbaarheid en kostenefficiëntie, maar minder controle over gegevens.

## Private Cloud

Cloud-infrastructuur exclusief voor één organisatie. Kan intern of extern worden gehost. Biedt maximale controle over gegevens en beveiliging, maar vereist meer investeringen.

## Hybride Cloud

Combinatie van publieke en private clouds. Gevoelige gegevens blijven in de private cloud, terwijl minder kritische toepassingen in de publieke cloud draaien. Biedt flexibiliteit en kostenvoordelen met behoud van controle.

## Community Cloud

Cloud-infrastructuur gedeeld door meerdere organisaties met gemeenschappelijke belangen (zoals beveiliging, compliance of branche). Biedt kostenbesparingen ten opzichte van private clouds en meer controle dan publieke clouds.

# Mogelijke Schade bij Cloud Incidenten



## Financiële schade

Diefstal van vertrouwelijke informatie zoals creditcardgegevens

---



## Identiteitsdiefstal

Misbruik van wachtwoorden en persoonlijke gegevens

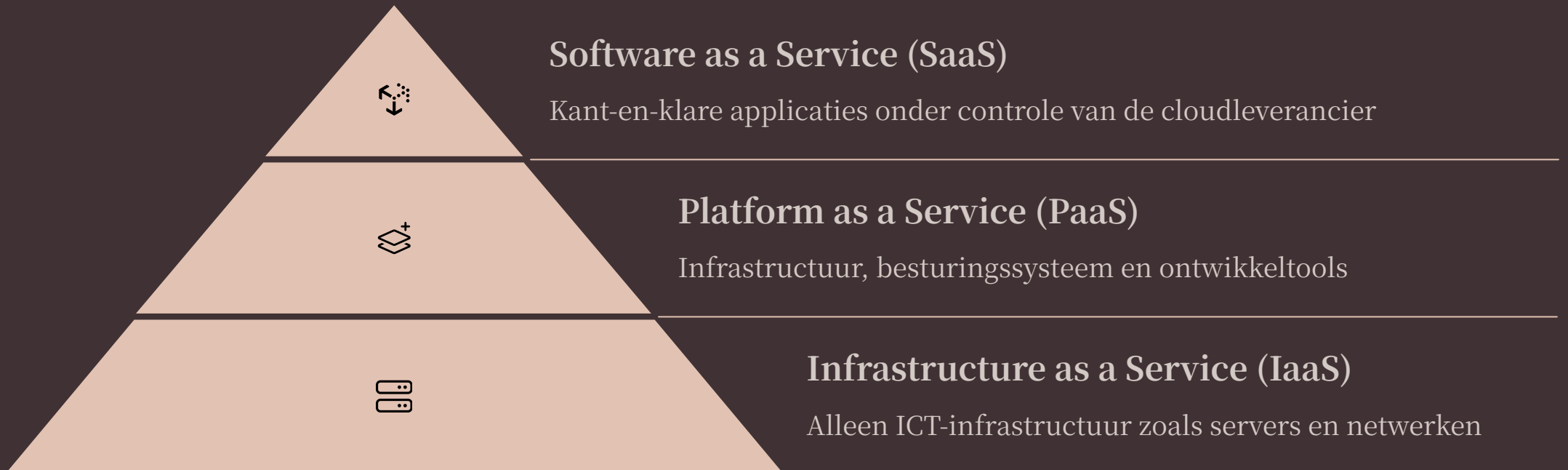
---



## Operationele schade

Productiviteitsverlies bij afhankelijkheid van clouddiensten

# Soorten Clouddiensten





### Encryptie

Noodzakelijk voor veilige, digitale communicatie

# Versleuteling van Gegevens



## Cryptografie

Beste manier om vertrouwelijkheid van data te waarborgen



## Hardwareversleuteling

Alle gegevens op de harde schijf automatisch versleuteld



## Softwareversleuteling

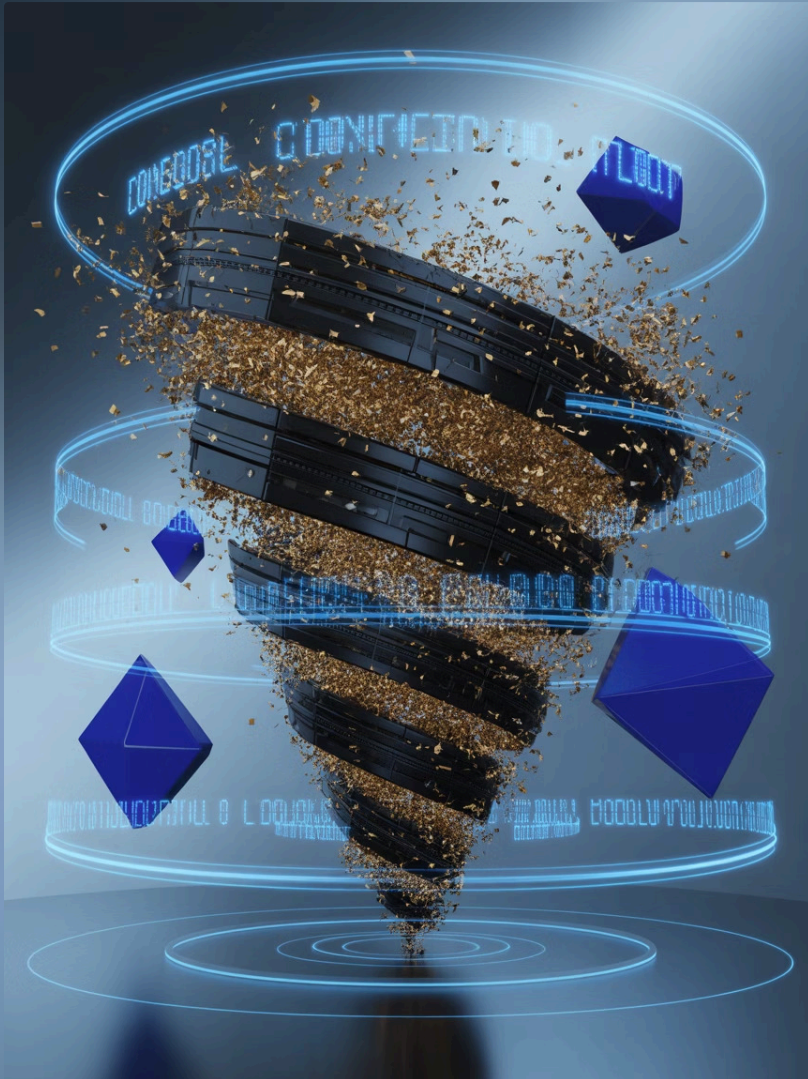
Grotere impact op performance, minder beveiliging



## Transportbeveiliging

Versleuteling tijdens transport van en naar de cloud





# Verwijderen van Gegevens



## Permanente vernietiging

Worden gegevens echt vernietigd of alleen verwijderd?



## Back-ups

Wat gebeurt er met data in back-ups?



## Eisen stellen

Bepaal vooraf welke eisen je stelt aan het verwijderen van data.

# (Distributed) Denial-of-Service Aanvallen

## Definitie

Elektronische aanvallen die een systeem, dienst of netwerk zo belasten dat ze niet meer beschikbaar zijn.

## DoS

Aanval vanaf een enkel systeem om diensten uit te schakelen of netwerk te overladen.

## DDoS

Aanval vanaf meerdere systemen tegelijkertijd voor grotere impact.



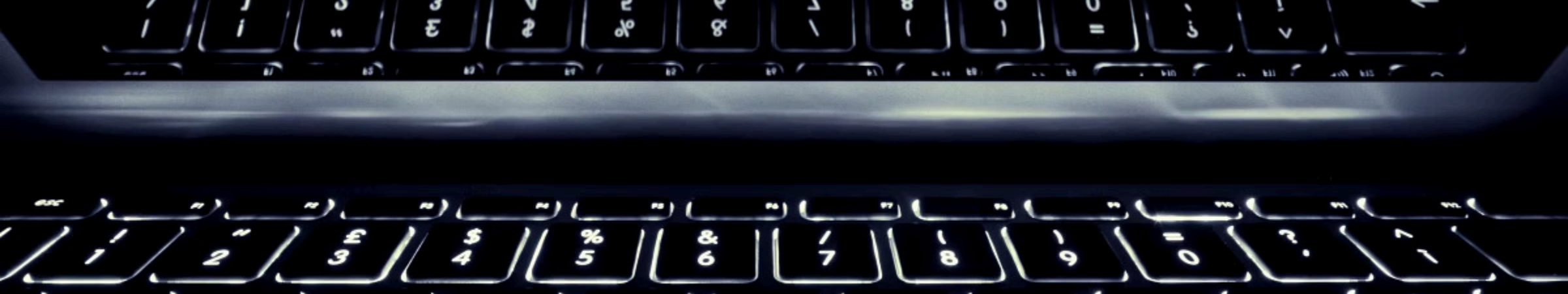
# Guest-hopping

## Wat is het?

Aanvalsmethode die kwetsbaarheden in de hypervisor gebruikt om de beveiliging tussen virtuele machines te compromitteren.

## Hoe werkt het?

De aanvaller gebruikt de zwakste virtuele machine als vertrekpunt. Van daaruit springt hij naar andere virtuele machines om toegang te krijgen tot het doelwit.



# Hyper Jacking

## Definitie

Methode waarbij een 'boosaardige' hypervisor onder de bestaande legitieme infrastructuur wordt geïnstalleerd.

## Controle

De aanvaller krijgt controle over alle acties tussen het doelwit en de hardware.

## Voorbeelden

Blue Pill en Vitriol zijn bekende voorbeelden van hyper jacking.

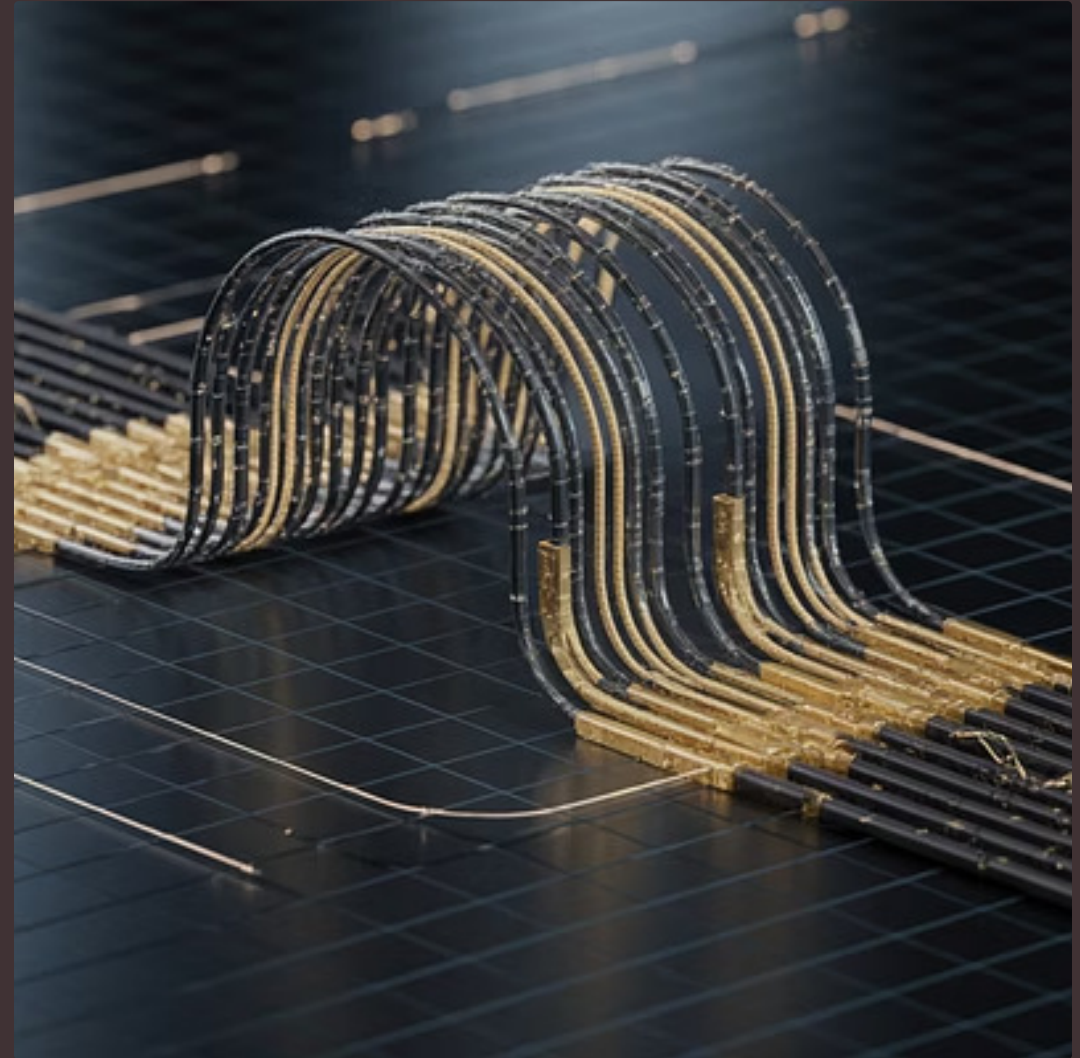


# Man-in-the-Middle en Replay Aanvallen



## Man-in-the-Middle

De aanvaller bevindt zich tussen klant en dienst, doet zich voor als beide partijen.



## Replay Aanval

Een legitieme sessie wordt opnieuw afgespeeld na het afluisteren van netwerkverkeer.

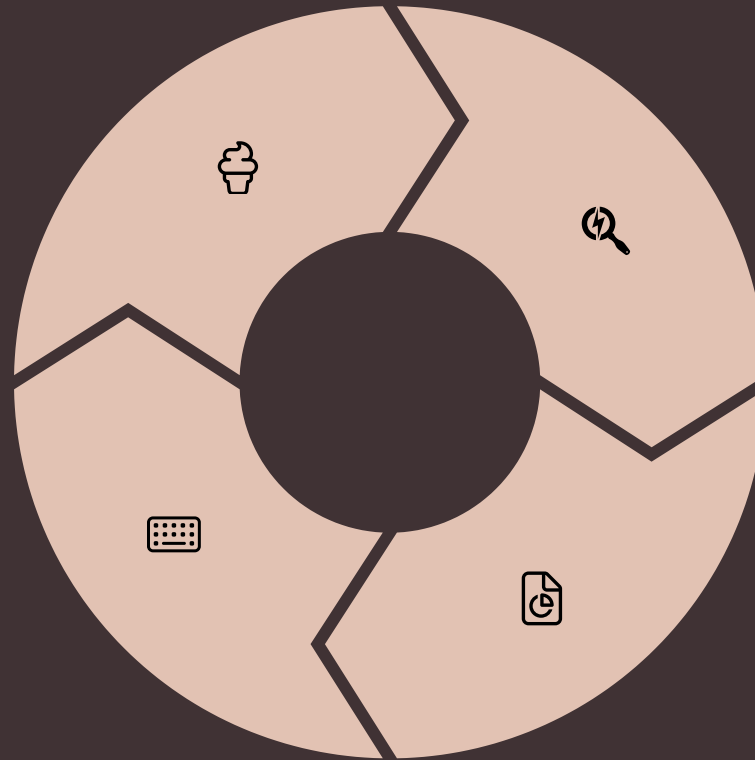
# Side Channel Aanvallen

## Installatie

Aanvallers installeren een virtuele machine via kwaadaardige software.

## Aanval

Via 'keystroke timing attacks' kunnen wachtwoorden worden achterhaald.



## Monitoring

De 'kwaadaardige' VM monitort gedeelde resources van andere virtuele machines.

## Analyse

Verzamelde gegevens worden geanalyseerd om zwakke punten te vinden.



# Overige Aanvalsmethoden



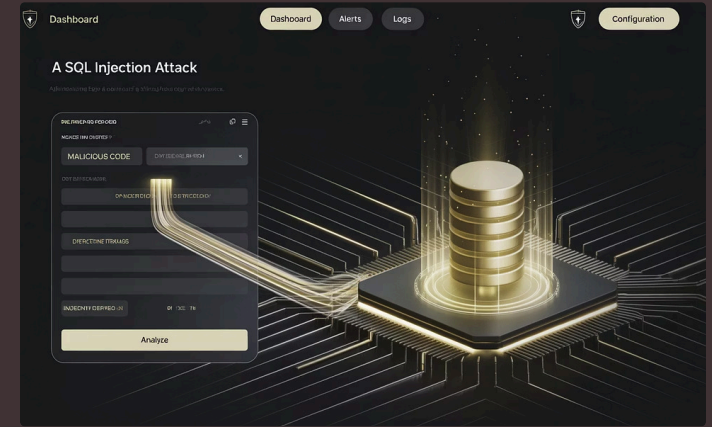
## Sniffing

Het onderscheppen en lezen van informatie, zoals e-mailberichten of gebruikersnamen en wachtwoorden.



## Spoofing

Je voordoen als een ander, bijvoorbeeld door het e-mailadres van een ander te gebruiken als afzendadres.



## SQL-injectie

Extra SQL-verzoek toevoegen waardoor de inhoud van de database wordt aangepast.



# Efficiënter batterijbeheer in Windows 11

Batterijduur is cruciaal voor mobiel werken en productiviteit. Windows 11 biedt nieuwe tools om je batterij optimaal te benutten.

De nieuwste updates bevatten slimme optimalisaties voor verschillende gebruikssituaties.

**VEILIGDIGITAAL.COM**

# Basisprincipes van batterijbeheer



## Hardware verbruik

CPU, scherm en andere componenten bepalen het basisverbruik.



## Software instellingen

Apps en systeeminstellingen beïnvloeden energieverbruik sterk.



## Prestaties vs. batterijduur

Vind de ideale balans voor jouw specifieke gebruik.

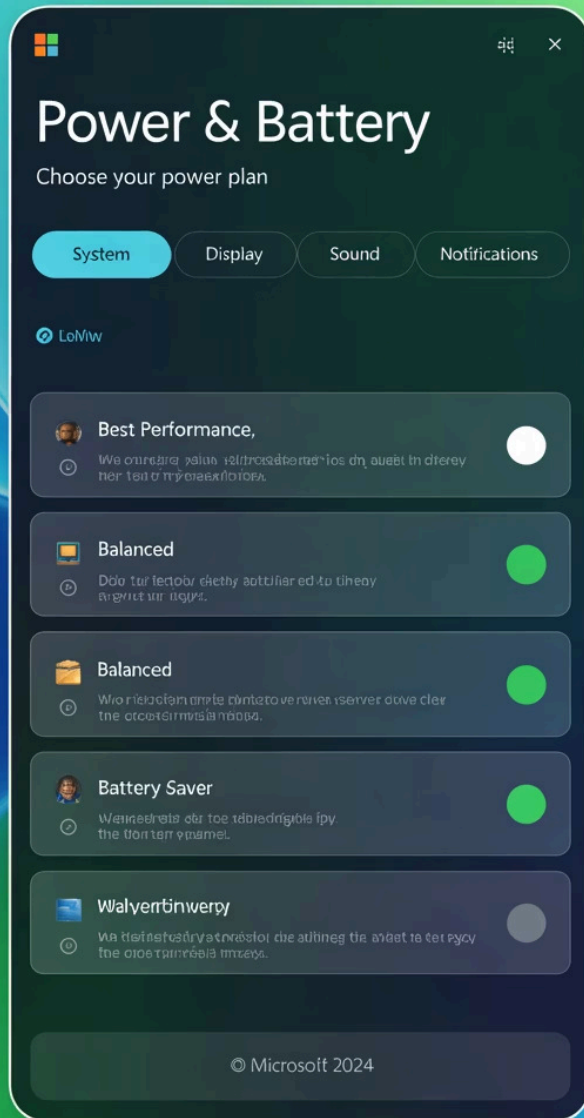


## Aanpasbare schema's

Energiebeheerschema's optimaliseren voor verschillende doeleinden.







# Energie-, slaap- en batterij-instellingen



## Toegang tot instellingen

Open Instellingen >  
Systeem > Energie &  
batterij voor alle opties.



## Energiemodi

Kies uit drie opties: Beste  
energie-efficiëntie,  
Balans, of Beste  
prestaties.



## Automatisch beheer

Laat Windows schermhelderheid en slaapstand slim regelen.

1

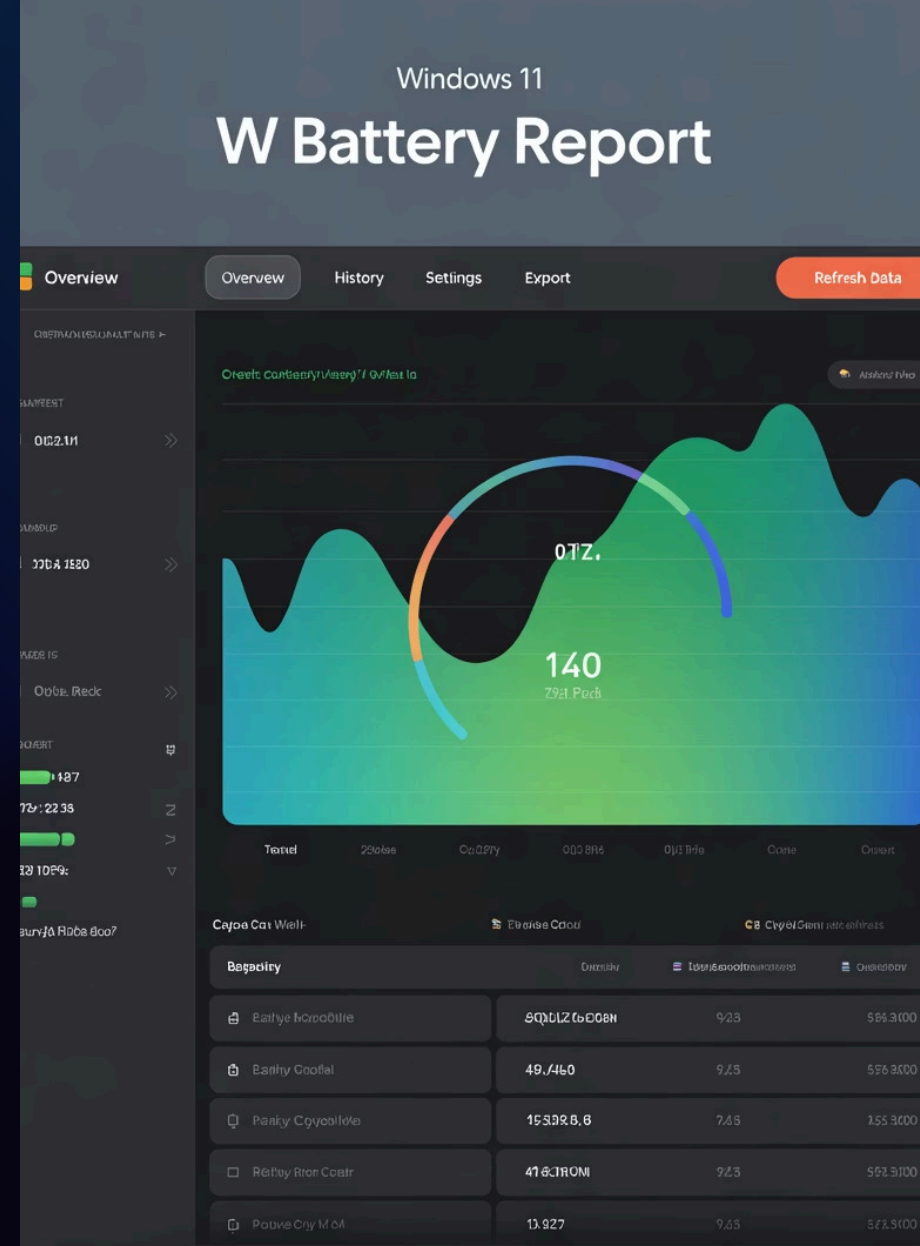
1111

## Rapport analyseren

Bekijk batterijconditie, historisch verbruik en capaciteitstrends.

1000

Configureer de Windows-taakbalk voor permanente batterijstatus.







# Praktische tips voor optimaal batterijgebruik

## Energiebesparingsmodus

Activeer automatisch bij lage acculading. Dit verlengt werktijd in noodsituaties.

## Scherminformatie

Verlaag helderheid en gebruik donkere modus. Dit bespaart aanzienlijk op energieverbruik.

## App-beheer

Sluit onnodige achtergrondapps. Vermijd zware programma's bij batterijgebruik.

## Aangepaste schema's

Maak profielen voor verschillende scenario's zoals presentaties of reizen.

# Samenvatting & aanbevelingen

## Regelmatige controle

Controleer batterij-instellingen maandelijks voor optimale prestaties.

## Onderhoudscyclus

Plan periodieke volledige laad- en ontlaadcycli voor kalibratie.



## Batterijrapporten

Gebruik diagnostische rapporten om batterijgezondheid te monitoren.

## Energiezuinige gewoonten

Ontwikkel routines die batterijlevensduur maximaliseren.

# Fixyfier: Alles-in-één Windows Reparatietool

Fixyfier is een gratis software voor Windows-gebruikers, beschikbaar via de Microsoft Store.

Gelanceerd in maart 2025, maakt deze tool Windows-reparatie eenvoudig voor zowel beginners als IT-professionals.

VEILIGDIGITAAL.COM





# Belangrijkste Functionaliteiten



## Systeembestandscontrole

Automatische detectie en reparatie van corrupte systeembestanden.



## Netwerkd Diagnose

Oplossen van verbindingproblemen met één klik.



## AI-analyse

Slimme probleemoplossing op basis van systeemgegevens.



## Schijfoptimalisatie

Verwijdert overbodige bestanden voor betere prestaties.

# Praktische Toepassingen

## Systeemherstel

Herstel Windows zonder volledige herinstallatie.  
Fixyfier bewaart je bestanden en instellingen.

## Netwerkbeheer

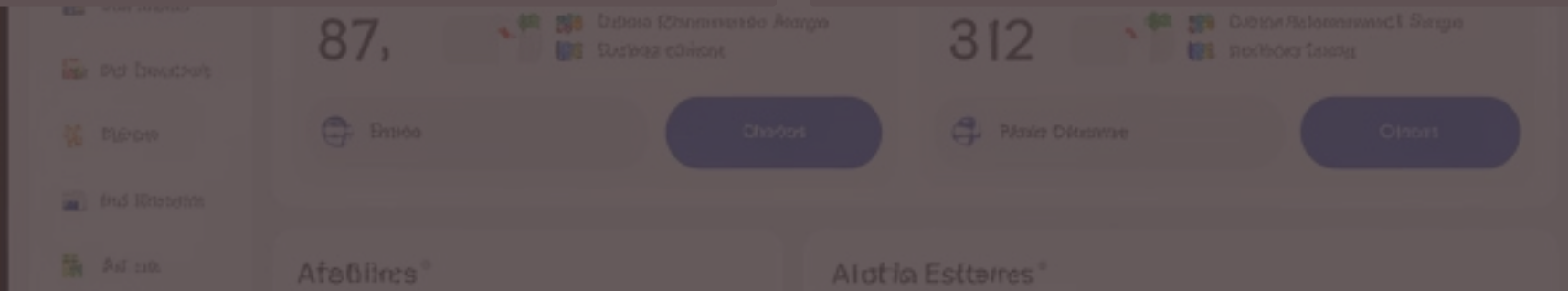
Los verbindingsproblemen op. Vernieuw IP-adressen met één druk op de knop.

## Bestandsbeheer

Verwijder tijdelijke bestanden en caches die je systeem vertragen.

## Updates

Beheer drivers en Windows-updates vanuit één overzichtelijke interface.





# Veiligheid en Privacy Opties

## Windows Firewall

Centraal beheer van firewall-instellingen en netwerkbescherming.



## Systeemherstelpunten

Creëer en beheer herstelpunten voor noodgevallen.



## BitLocker-encryptie

Stel schijfversleuteling in via een eenvoudige interface.



## Smart App Control

Beheer welke apps toegang hebben tot je systeem.



# Voordelen en Toepasbaarheid



**DOWNLOAD HET IN DE WINDOWS STORE**

# Het gebruik van een MESH systeem: Hoe veilig is dat?

MESH systemen bieden betere wifi-verbinding voor grotere ruimtes. Ze vormen een oplossing voor dekking in het hele huis.

We bekijken de veiligheidsrisico's en voordelen van deze draadloze netwerken.

VEILIGDIGITAAL.COM





# Wat zijn MESH systemen?



## Optimaal wifi-bereik

Ontworpen voor volledige dekking door het hele huis.



## Verbonden knooppunten

Systeem van meerdere samenwerkende routers.



## Grote ruimtes

Speciaal ontwikkeld voor naadloze dekking in grotere woningen.

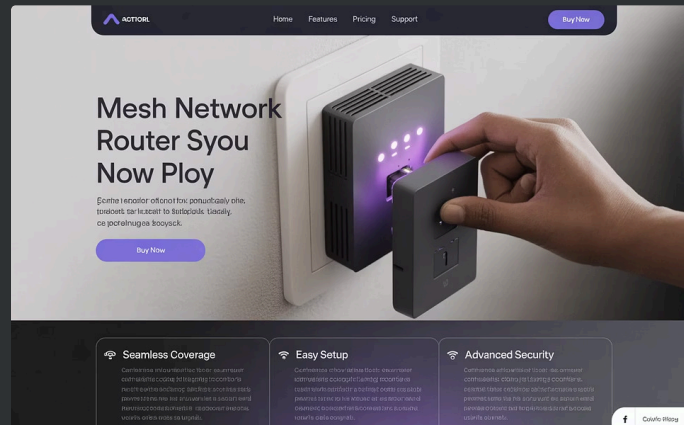


# Voordelen van MESH-netwerken



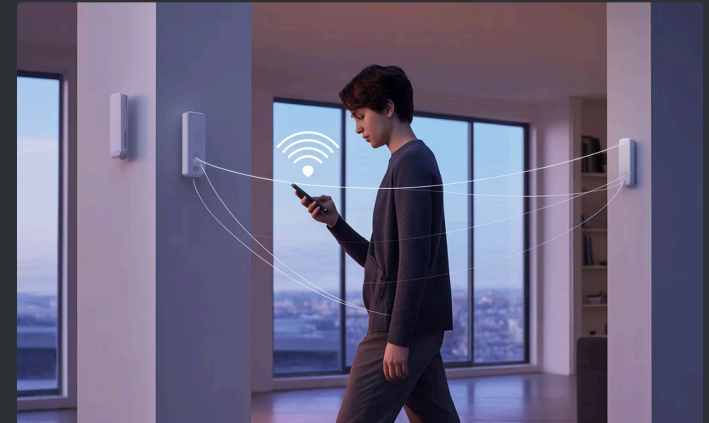
## Verbeterd bereik

Aanzienlijk groter bereik dan met traditionele routers. Geen dode zones meer in uw woning.



## Eenvoudige uitbreiding

Het netwerk is gemakkelijk uit te breiden met extra knooppunten. Perfect voor groeiende behoeften.



## Naadloze verbinding

Geen verbroken wifi-sigitaal meer wanneer u door het huis beweegt. Apparaten schakelen automatisch.

# Veiligheidsrisico's



# Praktische veiligheidsuitdagingen



## Ingewikkelde installatie

Complexer onderhoud dan bij traditionele routers.



## Snelheidsuitdagingen

Veel verkeer op knooppunten kan tot vertraging leiden.



## Probleemidentificatie

Veiligheidsproblemen zijn moeilijker te lokaliseren.



## Beveiligingscomplexiteit

Alle toegangspunten moeten afzonderlijk beveiligd worden.

# Beschermingsmaatregelen

## VPN-installatie

Installeer VPN op uw router. Dit beschermt al uw internetverkeer. Het versleutelt gegevens van alle verbonden apparaten.

## Firmware-updates

Update regelmatig de firmware van alle mesh-apparaten. Dit dicht bekende beveiligingslekken. Stel automatische updates in.

## Sterke wachtwoorden

Gebruik unieke, complexe wachtwoorden. Verander deze regelmatig. Overweeg een wachtwoordmanager.

## Gast-netwerk

Maak een apart netwerk voor bezoekers. Isoleer slimme apparaten hierop. Dit beschermt uw hoofdnetwerk.





# Aandachtspunten bij aanschaf

## Tweedehands systemen

Wees voorzichtig met tweedehands mesh-systemen. Controleer of ze gereset kunnen worden.



## Update-ondersteuning

Verifieer of oudere modellen nog updates ontvangen. Dit is cruciaal voor veiligheid.



## Gespecialiseerde knooppunten

Kies voor speciaal ontwikkelde mesh-knooppunten. Deze bieden betere veiligheid.



## Recente testresultaten

Raadpleeg de meest recente tests uit 2025. Deze tonen de nieuwste veiligheidsfeatures.



## Conclusie:

# Is een MESH systeem veilig?

**Afweging voordelen en risico's**  
MESH biedt uitstekende dekking maar vereist extra veiligheidsmaatregelen. De technologie evolueert snel.

### Juiste implementatie

Voordelen wegen meestal op tegen risico's bij correcte installatie. Volg best practices voor netwerkveiligheid.

### Balans vinden

Met goede beveiliging is mesh een veilige oplossing. Zoek evenwicht tussen gebruiksgemak, bereik en veiligheid.



# IMEI-nummer kwijt? Zo vind je die terug!

Elk toestel heeft een uniek 15-cijferig IMEI-nummer. Het is essentieel bij verlies, diefstal of defecten.

Ook zonder je smartphone kun je dit belangrijke nummer terugvinden. We leggen uit hoe.

VEILIGDIGITAAL.COM

# Wat is het IMEI-nummer?

## Identificatie

IMEI staat voor "International Mobile Equipment Identity". Het is een wereldwijd unieke code voor elk toestel.

## Samenstelling

Het bestaat uit precies 15 cijfers. Deze code is onvervangbaar en uniek.

## Toepassing

Je hebt het nodig bij aangifte van diefstal. Ook voor garantie of blokkeren is het essentieel.

# Waarom is het IMEI-nummer belangrijk?

## Eigendomsbewijs

Het dient als bewijs dat het toestel van jou is. Handig bij diefstal of verlies.



## Blokkeren

Met het IMEI-nummer kan je provider een gestolen toestel blokkeren.

## Controle

Bij tweedehands aankoop kun je controleren of het toestel niet gestolen is.





# Terugvinden zonder je smartphone



## Verpakking

Controleer de originele doos. Het IMEI staat vaak op de zijkant.



## Aankoopbewijs

Kijk op je factuur. Veel winkels vermelden het IMEI-nummer hierop.



## Online account

Check je Google Dashboard of Apple ID. Daar staat je IMEI vaak geregistreerd.



## Provider

Je provider kan het IMEI-nummer opvragen. Neem wel je legitimatie mee.

# Samenvatting & tips



## Preventie

Noteer je IMEI-nummer voordat er problemen zijn. Het scheelt veel stress.



## Bewaren

Houd verpakking en aankoopbewijs bij. Ze bevatten vaak het IMEI-nummer.



## Administratie

Sla het IMEI op in je digitale administratie. Zo heb je het altijd bij de hand.



## Veiligheid

Bij diefstal helpt het IMEI-nummer bij politieaangifte en verzekeringsclaims.





# Pas op voor malware bij online bestandsconverters

De FBI waarschuwt voor een nieuwste cyberdreiging: frauduleuze online bestandsconverters. Deze malafide diensten zijn actief sinds maart 2025.

VEILIGDIGITAAL.COM

# Waarom gebruiken mensen online converters?

## Gemak

Snel bestanden omzetten zonder gedoe. Bijvoorbeeld een Word-document naar PDF converteren.

## Kosteloos

Gratis te gebruiken zonder dure software te kopen.

## Direct beschikbaar

Geen installatie nodig. Populair bij studenten en bedrijven.





# Hoe werkt de malware-truc precies?



## Namaakwebsites

Criminelen bouwen echte conversiesites perfect na.



## Werkende service

De converter doet wat beloofd wordt.



## Verborgен gevaar

Het gedownloade bestand bevat verborgen malware.



# Mogelijke gevolgen voor je veiligheid



## Ransomware

Bestanden worden versleuteld en ontoegankelijk gemaakt.



## Diefstal

Persoonlijke gegevens, wachtwoorden en bankinfo verdwijnen.



## Account hacks

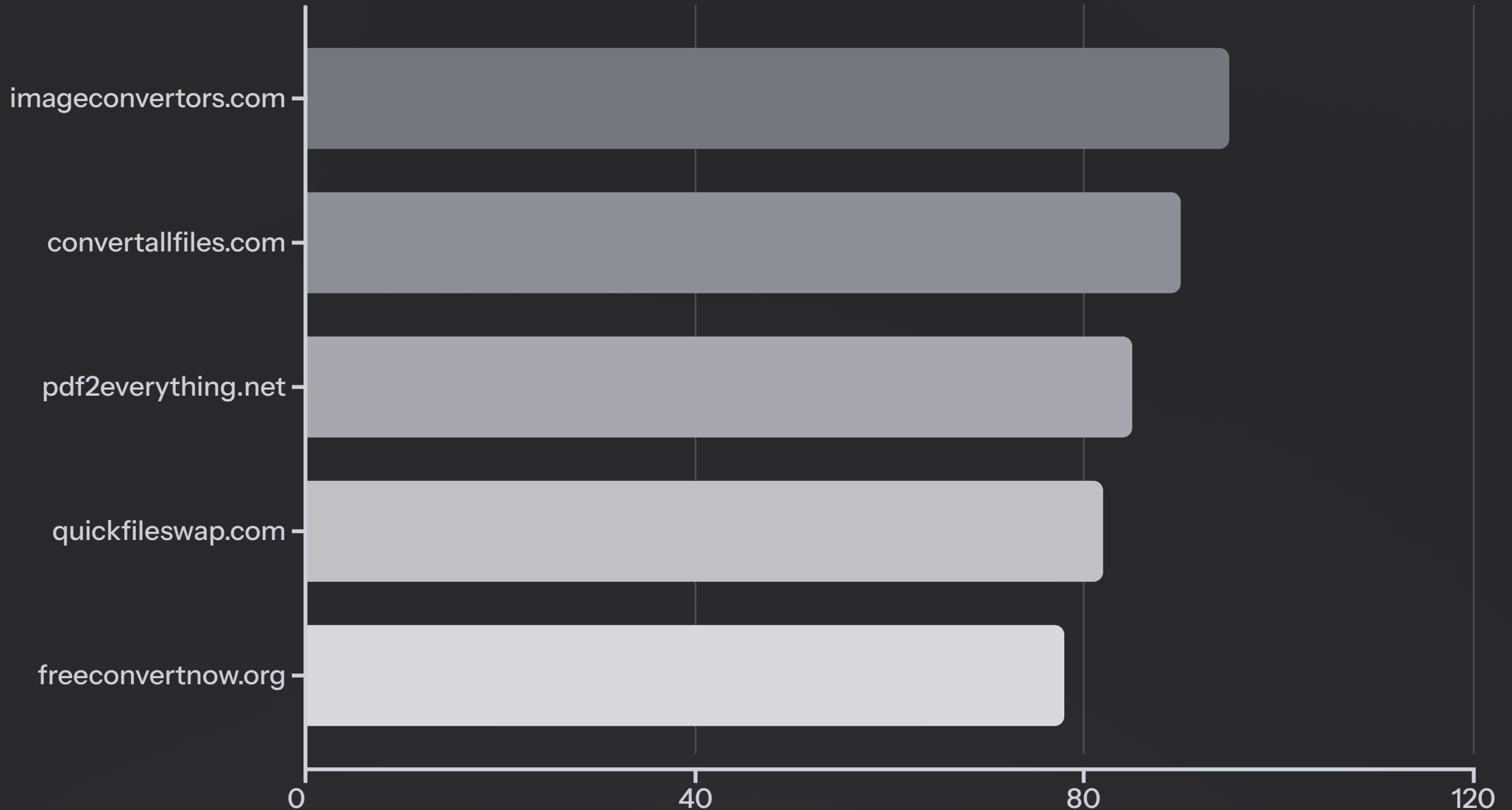
Gehackte accounts en gestolen crypto-wallets.



## Phishing

Jouw contacten ontvangen verdachte berichten.

# Voorbeelden van gevaarlijke sites



Sommige sites infecteren je systeem al bij het bezoeken. De lijst met risicodomeinen groeit dagelijks.

# Wat kun je merken na besmetting?



## Systeemproblemen

Je computer wordt trager. Vreemde pop-ups verschijnen onverwacht.



## Onbevoegde toegang

Inlogactiviteit op je accounts zonder jouw toestemming.



## Verdachte berichten

Contacten melden vreemde e-mails of berichten van jou.



## Onbekende transacties

Vreemde afschrijvingen of activiteit op je rekeningen.

# Hoe voorkom je de valkuilen?



Controleer altijd de URL en zoek naar reviews van de dienst voordat je deze gebruikt. Let op waarschuwingssignalen zoals slechte grammatica of overdreven beloftes.

# Wat te doen bij verdachte activiteit?

## Wachtwoorden wijzigen

Gebruik een schoon apparaat om direct alle belangrijke wachtwoorden te veranderen.

## Volledige scan

Draai een uitgebreide malware scan met betrouwbare software.

## Fraudemelding

Meld het incident bij de Fraudehelpdesk, politie of zelfs FBI indien nodig.





**Je moet wel gek zijn om nog steeds Windows 7 te gebruiken**

**Windows 7 werd gelanceerd in 2009. Het besturingssysteem is nu zwaar verouderd.**

**Ooit gebruikten miljoenen mensen wereldwijd Windows 7. Die tijd is voorbij.**

VEILIGDIGITAAL.COM



# Definitieve einde van ondersteuning



**14 januari 2020**

Officiële Microsoft-ondersteuning volledig beëindigd



**Heden**

Zeer beperkte ondersteuning alleen voor zakelijke klanten



**31 december 2025**

Absoluut geen enkele update meer beschikbaar



# Grote beveiligingsrisico's



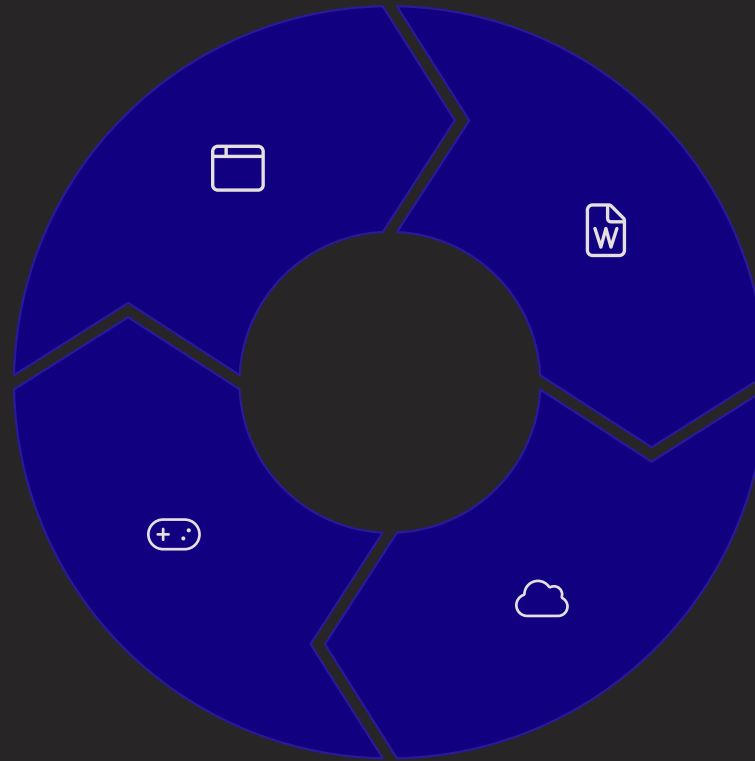
# Software werkt niet meer

## Browsers

Chrome en Firefox stoppen Windows 7-ondersteuning

## Games

Nieuwe games vereisen Windows 10 of 11



## Office

Moderne Office-versies werken niet meer

## Online diensten

Banken en webshops blokkeren verouderde systemen

# Voorbeelden van recente incidenten

1

## Ransomware-golf 2023

Wereldwijde toename in aanvallen op verouderde Windows-systemen

2

## Dataverlies bij bedrijven

MKB-bedrijven met Windows 7 vaker slachtoffer van hacks

3

## Banken blokkeren toegang

Meerdere banken weigeren Windows 7-gebruikers toegang tot internetbankieren







# Waarom mensen tóch Windows 7 blijven gebruiken

## Legacy software

Oude programma's draaien uitsluitend op Windows 7

Geen moderne alternatieven beschikbaar

## Verouderde hardware

Computer te traag voor Windows 10 of 11

Budget ontbreekt voor nieuwe apparatuur

## Onwetendheid

Geen kennis over de grote risico's

Uitstelgedrag vanwege angst voor verandering



# Zijn er überhaupt nog veilige oplossingen?



## Offline gebruik

Alleen veilig zonder internetverbinding.  
Uitsluitend voor specifieke toepassingen.



## Virtuele machine

Windows 7 draaien binnen een moderne beveiligde omgeving. Technisch complex.



## Alternatief besturingssysteem

Overstappen naar Linux geeft oude hardware nieuw leven. Vereist leercurve.

# Conclusie: Geen excuus meer!



## Groot risico

Verouderde software bedreigt jou en je data



## Tijdig overstappen

Voorkomt problemen, verlies en kosten



## Update vandaag nog

Blijf niet achter in het digitale tijdperk

Om duidelijk te zijn.....

dat geldt straks natuurlijk ook voor Windows 10





# De gevaarlijkste plekken op internet

**Cyberveiligheidsrisico's in kaart gebracht op basis van de meest recente cyberdreigingen van 2025. Ontdek de digitale gevaren die op de loer liggen.**

**In dit atikel delen we praktische tips om jezelf te beschermen tegen deze groeiende bedreigingen.**

VEILIGDIGITAAL.COM



# Desinformatie platforms



## Broedplaatsen

Sociale media en nepnieuwswebsites fungeren als broedplaatsen voor misleidende informatie.



## Snelle verspreiding

Gemanipuleerde content verspreidt zich zes keer sneller dan waarheidsgetrouwe informatie.



## Maatschappelijke impact

Desinformatie beïnvloedt verkiezingen, gezondheidsgedrag en openbare veiligheid.



# Deepfakes en AI-oplichting

## Geavanceerde technologie

AI-tools maken het mogelijk om uiterst realistische vervalsingen te maken. Deze zijn met het blote oog nauwelijks te herkennen.

## Frauduleuze gesprekken

Oplichters gebruiken deepfake-technologie om telefoongesprekken en video's van "bekenden" na te bootsen. Zo winnen ze vertrouwen.

## Familieleden nabootsen

De stemmen van familieleden worden realistisch nagebootst. Dit maakt emotionele manipulatie bijzonder effectief.

# Lookalike URL's



## Nabootsing

Websites worden ontworpen om legitieme diensten perfect na te bootsen.



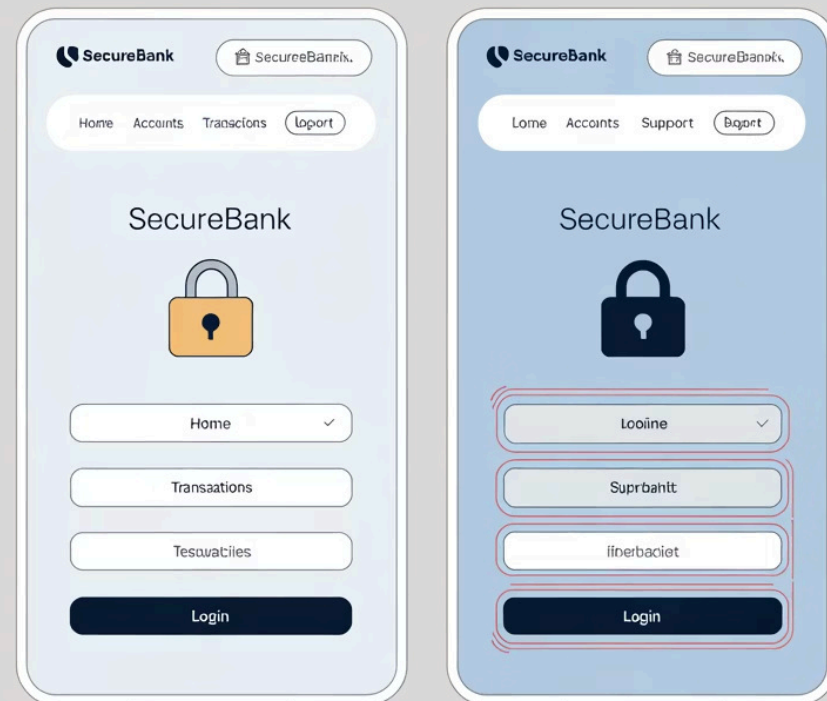
## Subtiele verschillen

Kleine wijzigingen in URL's zijn moeilijk te detecteren voor het ongetrainde oog.



## Phishing aanvallen

Vooral banken en webwinkels worden nagebootst om inloggegevens te stelen.



Legitimate mobile app interface to deposit and withdraw funds.

Phishing mobile app interface to steal login credentials.

Legitimate mobile app interface to deposit and withdraw funds.

Phishing mobile app interface to steal login credentials.



# QR-code oplichting

**150%**

## Toename fraude

QR-code gerelateerde fraude is sinds 2023 explosief toegenomen.

**68%**

## Onbewust scannen

Percentage Nederlanders dat QR-codes scant zonder de bestemming te controleren.

**43%**

## Openbare locaties

Percentage fraudegevallen dat plaatsvindt via QR-codes op openbare plekken.

# Malvertising



## Kwaadaardige advertenties

Malafide advertenties verschijnen op legitieme websites. Ze lijken betrouwbaar maar bevatten schadelijke code.



## Onzichtbare code

Zonder dat je het merkt, wordt malware gedownload. Dit gebeurt vaak zonder dat je ergens op klikt.



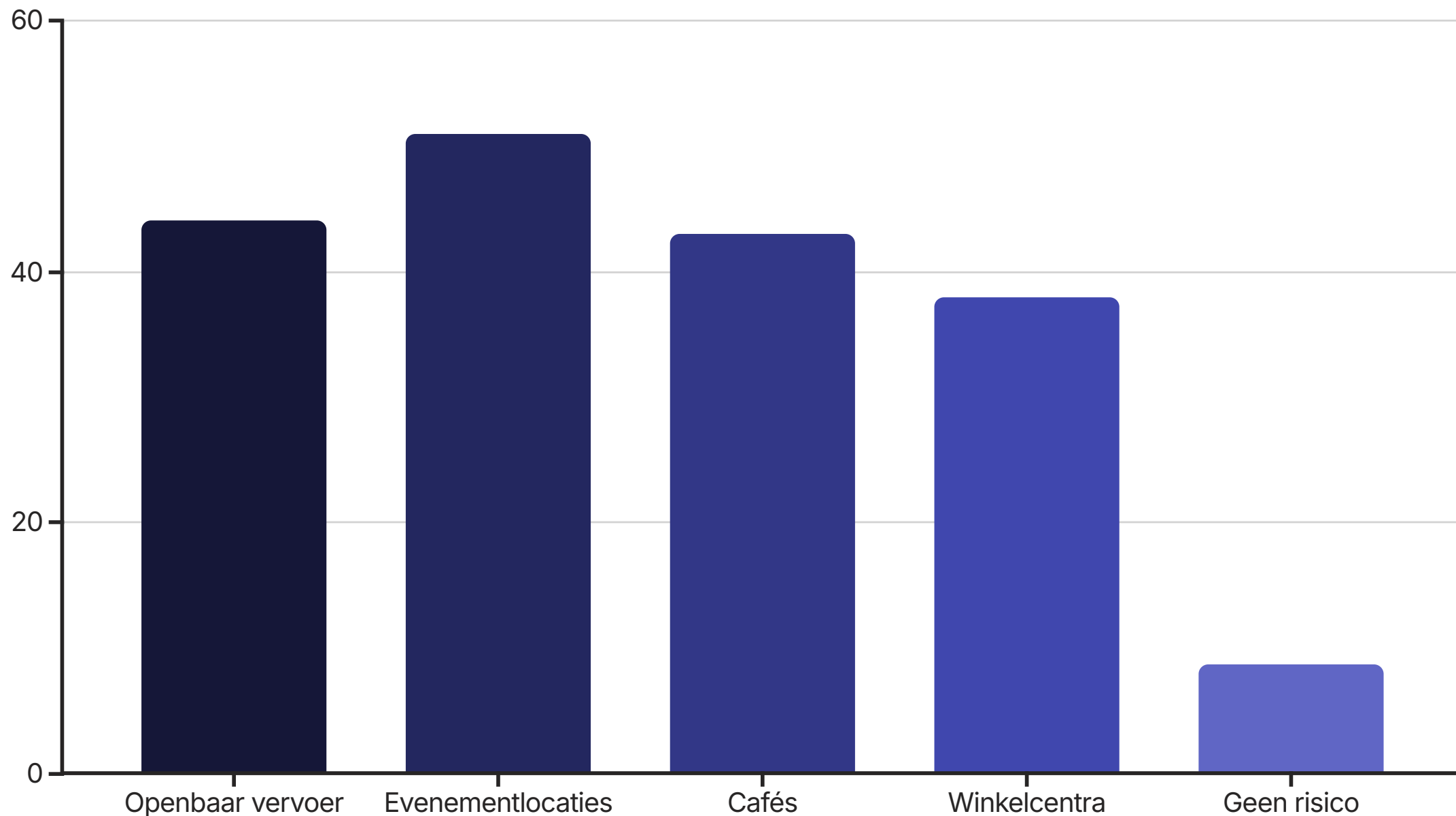
## Vertrouwde bronnen

Zelfs betrouwbare nieuwssites kunnen onbedoeld besmette advertenties tonen. Niemand is immuun.

Protect your  
digital footprint



# Openbare wifi-netwerken



Nederlanders zijn zich steeds meer bewust van de risico's van openbare wifi. Toch neemt slechts een klein percentage beschermende maatregelen.

# Gemeentelijke wifi-hotspots

## Onveilige netwerken

75% van Nederlandse gemeenten biedt onveilige wifi-gastnetwerken aan.

## Beveiligde gemeenten

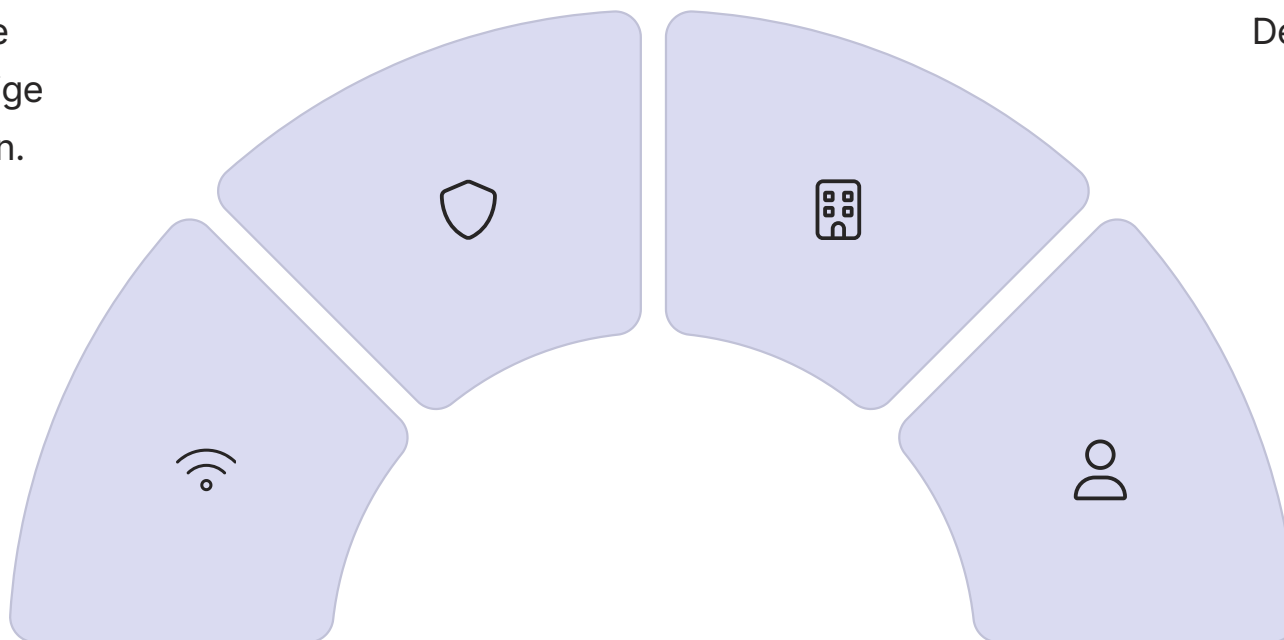
Slechts 15 gemeenten hebben voldoende beveiligde netwerken geïmplementeerd.

## Publieke diensten

Risico's bij verbinding met publieke diensten via deze netwerken zijn aanzienlijk.

## Gebruikersgedrag

De meeste burgers zijn zich niet bewust van deze kwetsbaarheden.



Free 'WIFI' - Enjoy!



# Winkelcentra en horecagelegenheden

## Bezorgde Nederlanders

43% van Nederlanders is bezorgd over wifi-veiligheid in cafés en restaurants. Toch maken velen er gebruik van.

## Nepnetwerken

Hackers zetten nepnetwerken op die legitiem lijken. Namen als "Café\_Free\_Wifi" wekken vertrouwen.

## Online winkelen

Datadiefstal bij online winkelen via openbare netwerken komt vaak voor. Bankgegevens zijn het doelwit.

# Datingapps en -websites



## Identiteitsfraude

Valse profielen worden gebruikt om persoonlijke informatie te verzamelen. Dit leidt tot identiteitsdiefstal.



## Romance scams

Oplichters bouwen emotionele banden op. Ze vragen uiteindelijk om financiële hulp.



## Persoonlijke informatie

Foto's en persoonlijke details worden gebruikt voor afpersing. Dit heet "sextortion".



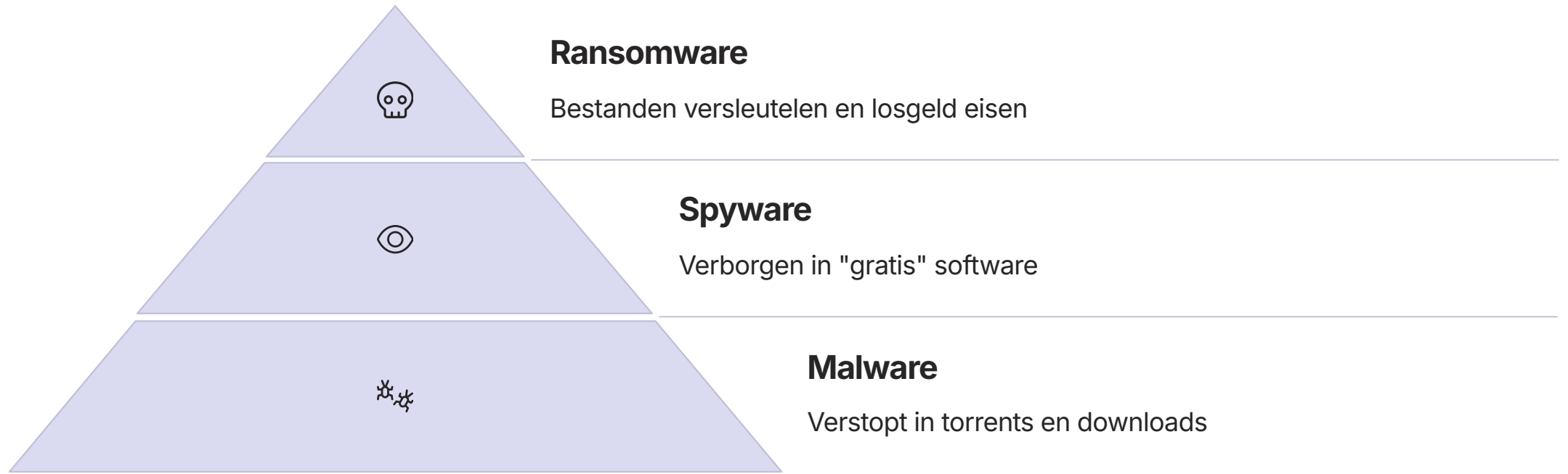
## Financiële schade

Gemiddelde schade per slachtoffer bedraagt €9.400.  
Emotionele schade is onberekenbaar.

Is it real?



# Illegale downloadplatforms



Illegale downloadplatforms lijken gratis entertainment te bieden. De werkelijke prijs is echter hoog. Je betaalt met je privacy en computerbeveiliging.

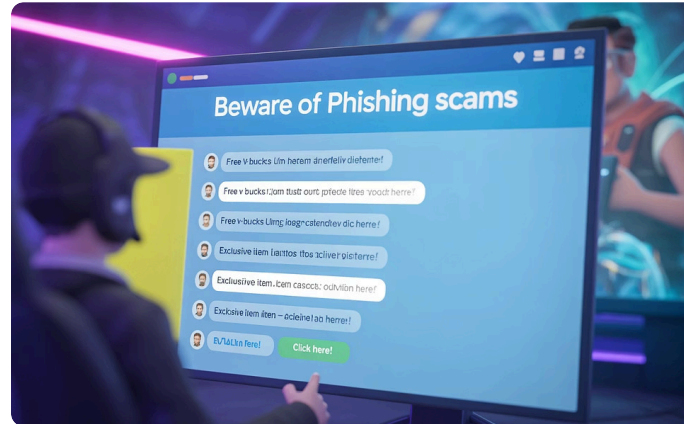
# Online gaming platforms



## In-game oplichting

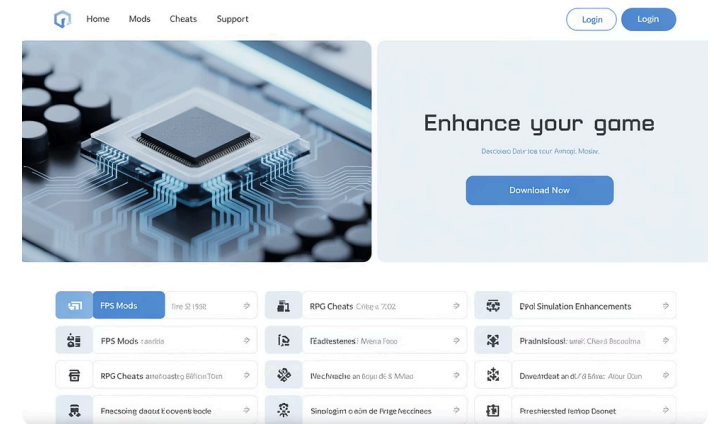
Frauduleuze in-game aankopen en valse items

Gamers zijn kwetsbaar omdat vertrouwen snel ontstaat in teamverband. Oplichters misbruiken deze gemeenschapszin om toegang te krijgen tot accounts en financiële gegevens.



## Chat-phishing

Phishing via gaming chats en privéberichten



## Malware verspreiding

Schadelijke software via game mods en cheats

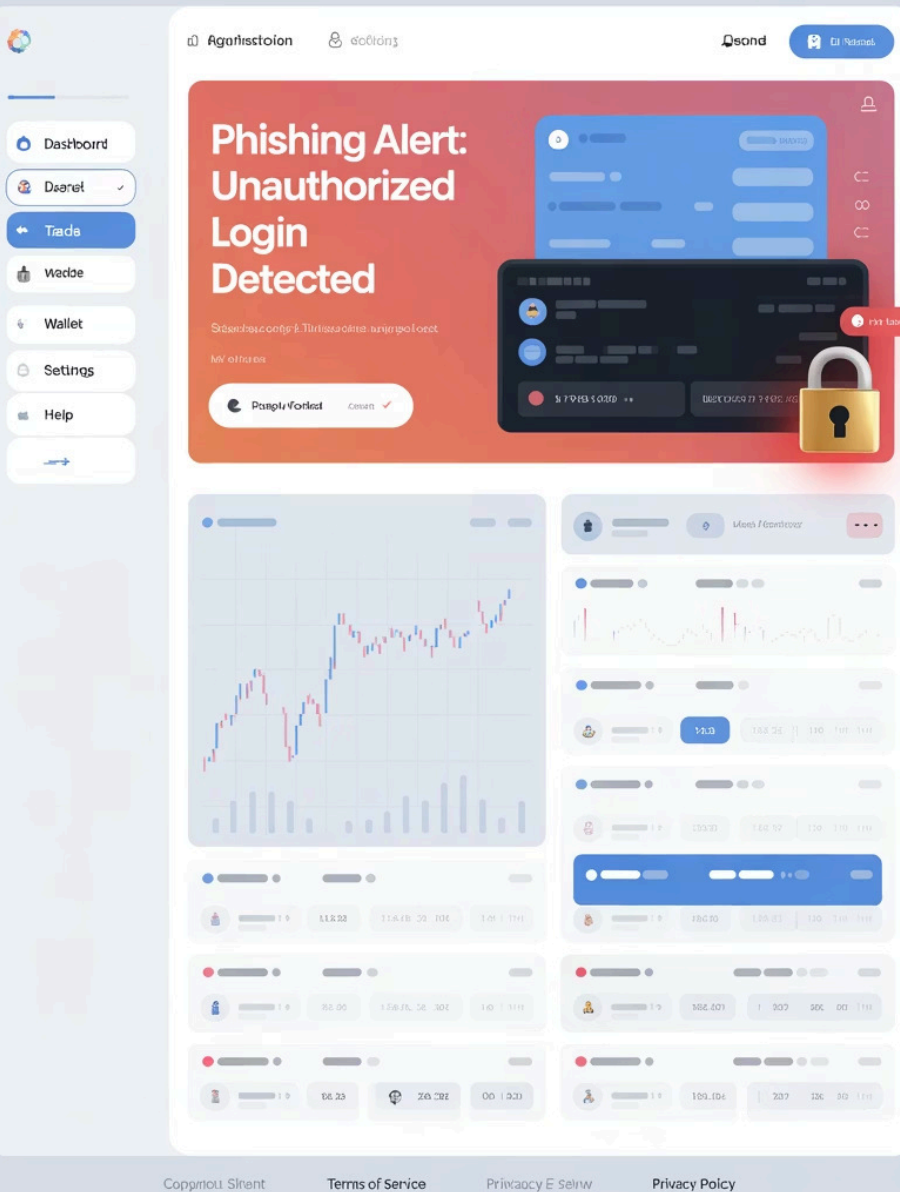
# Slecht beveiligde IoT-apparaten



Peace of mind, digitally protected



Slimme apparaten maken ons leven gemakkelijker. Ze creëren echter ook toegangspoorten voor cybercriminelen. Standaardwachtwoorden worden zelden gewijzigd.



# Cryptocurrency exchanges

## Ongereguleerde platforms

Veel crypto-exchanges opereren zonder toezicht. Ze hanteren minimale beveiligingsmaatregelen voor gebruikers.

## Wallet-aanvallen

Phishing-aanvallen richten zich specifiek op digitale wallets. Slachtoffers verliezen hun volledige crypto-bezit.

## Financiële verliezen

Cryptofraude veroorzaakte vorig jaar €12,5 miljard schade wereldwijd. Dit blijft toenemen.



# Beschermingsmaatregelen

## VPN gebruiken

Beveilig je verbinding op openbare wifi-netwerken met een betrouwbare VPN-dienst

## Tweefactorauthenticatie

Activeer 2FA voor alle belangrijke accounts om je beveiliging te versterken



## URL's controleren

Controleer webadressen zorgvuldig voor het inloggen op gevoelige diensten

## Updates installeren

Houd software en apparaten up-to-date met de nieuwste beveiligingspatches



# Onchain-phishing

Stel je voor dat je een digitale portemonnee hebt, een plek waar je jouw digitale munten bewaart. Criminelen proberen soms deze portemonnee leeg te halen zonder dat je het doorhebt. Dit doen ze met iets dat 'onchain phishing' wordt genoemd.

VEILIGDIGITAAL.COM

# Wat is een zero-value transfer?

Een zero-value transfer is een nieuwe vorm van onchain-phishing waarbij de aanvaller een transactie van nul tokens verstuurt naar de wallet van het slachtoffer. Omdat er geen waarde wordt overgemaakt, is geen handtekening vereist en wordt de transactie automatisch geaccepteerd.

Toch verschijnt deze lege transactie in de transactiegeschiedenis van de gebruiker. Daardoor lijkt het verzendadres legitiem, wat later tot verwarring leidt.



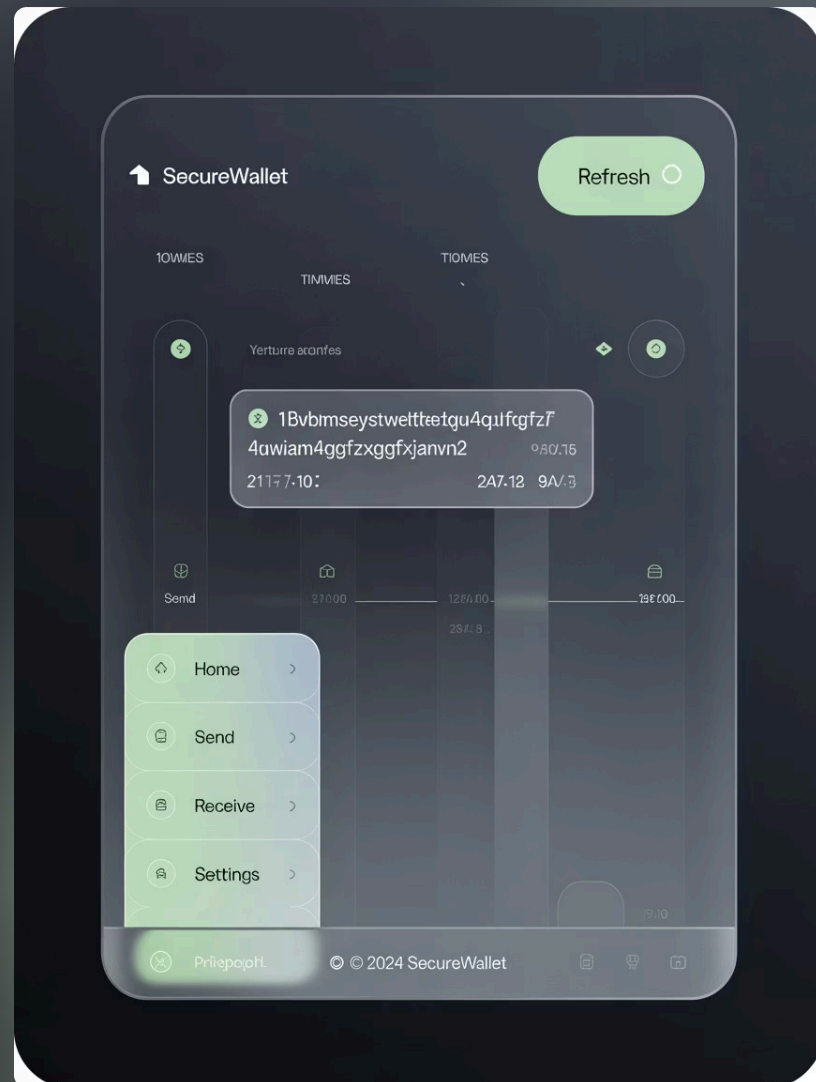
Aanvaller verstuurt nul tokens

Geen handtekening vereist, transactie automatisch geaccepteerd.



Verschijnt in transactiegeschiedenis

Verzendadres lijkt legitiem, leidt tot verwarring.



# Waarom is dit zo gevaarlijk?

Doordat het frauduleuze adres al in de transactiegeschiedenis voorkomt, herkennen gebruikers het niet als verdacht. Bij een volgende overboeking sturen ze wél daadwerkelijk geld naar het nepadres, in de veronderstelling dat het vertrouwd is. Het geld komt dan direct bij de aanvaller terecht.

Deze methode is een verfijning van zogeheten adresvergiftiging, waarbij opzettelijk kleine bedragen worden verzonden vanuit adressen die sterk lijken op legitieme wallets.

## Adresvergiftiging

Opzettelijk kleine bedragen verzonden vanuit adressen die sterk lijken op legitieme wallets.

## Zero-value transfer

Frauduleus adres al in transactiegeschiedenis, gebruikers herkennen het niet als verdacht.

# Meer Voorbeelden van Onchain Phishing

- **Token-approvals:** Aanvallers vragen toegang tot alle tokens in je wallet via slimme contracten. Eenmaal goedgekeurd kunnen ze alles leegroven.
- **Airdrop-fraude:** Nepluchtdroppingen lokken slachtoffers naar malafide websites waar ze verbinding maken met hun wallet.
- **Fake NFT minting:** Frauduleuze NFT-projecten die je wallet leegroven zodra je probeert te minten.
- **Replica-dApps:** Exacte kopieën van legitieme gedecentraliseerde apps met verborgen malafide functies.
- **Slimme-contract exploits:** Kwaadaardige code die kwetsbaarheden in slimme contracten misbruikt om fondsen te stelen.

## Hoe vaak gebeurt dit?

Uit een onderzoek van januari 2025 blijkt dat tussen 1 juli 2022 en 30 juni 2024 ruim 270 miljoen pogingen tot adresvergiftiging zijn gedaan op de netwerken van BNB Chain en Ethereum. Daarvan waren ongeveer 6.000 pogingen succesvol, met een totale schade van meer dan \$83 miljoen.



# Hoe blijf je veilig tegen onchain phishing

Bescherm jezelf tegen deze geavanceerde aanvallen met deze essentiële veiligheidsmaatregelen.

## Controleer adressen zorgvuldig

Verifieer altijd het volledige wallet-adres. Vertrouw nooit op eerder gebruikte adressen zonder dubbelcheck.

## Gebruik hardware wallets

Bewaar grote bedragen offline. Hardware wallets bieden extra bescherming tegen phishing-aanvallen.

## Controleer smart contracts

Lees permissies zorgvuldig. Gebruik tools als Etherscan om contractcode te verifiëren.

## Blijf geïnformeerd

Volg beveiligingsnieuws in de cryptowereld. Nieuwe aanvalsmethoden ontstaan voortdurend.

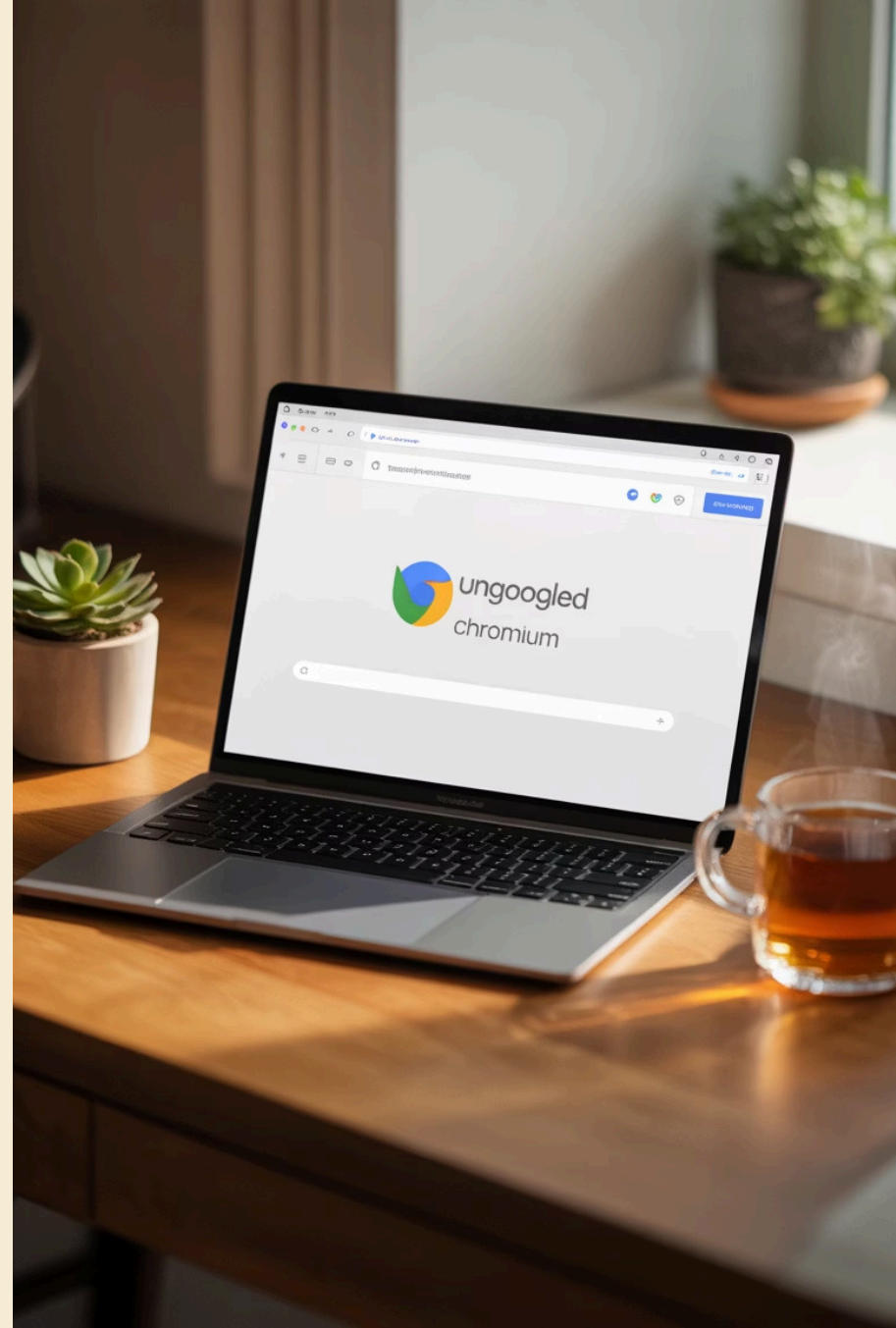


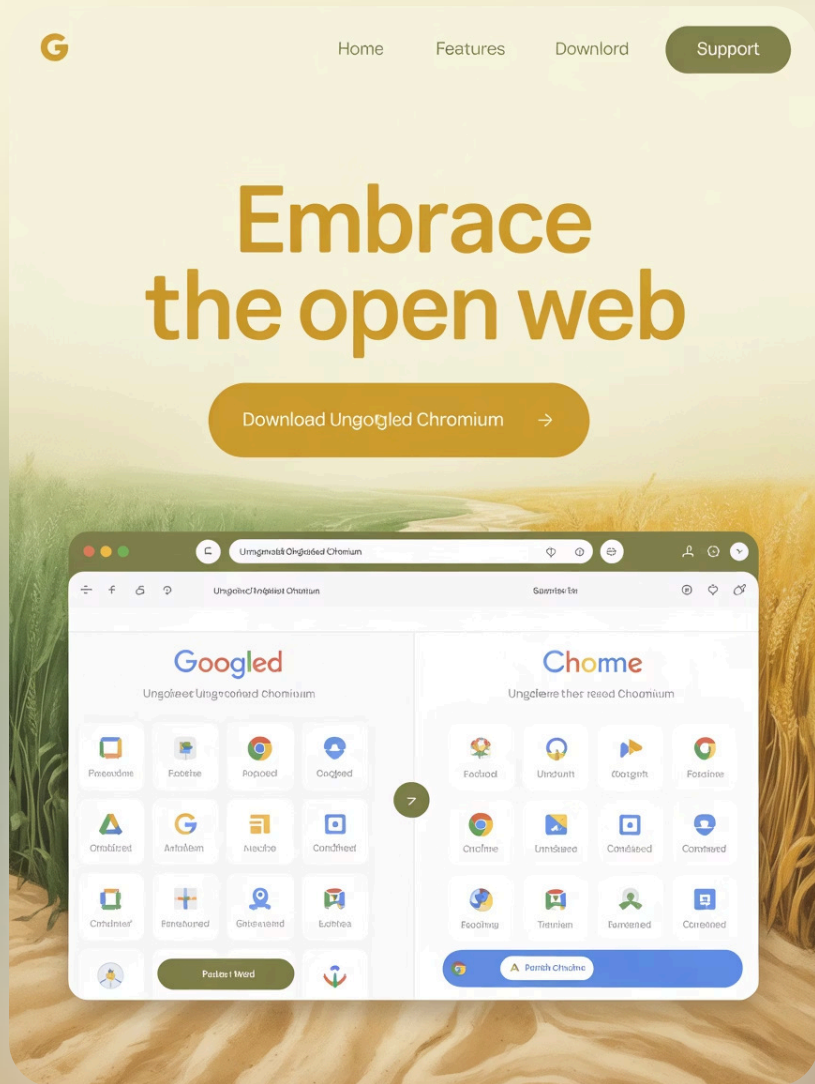
# Ungoogled Chromium: de webbrowser die je wilt?

Ungoogled Chromium is een open-source variant van de Google Chromium browser. Het project werd in 2015 opgericht door ontwikkelaar "Eloston".

De browser verwijdert alle Google-services en tracking voor maximale privacy.

VEILIGDIGITAAL.COM





# Wat is Ungogled Chromium?



## Drop-in vervanging

Een naadloze vervanging voor de reguliere Chromium browser.



## Google-vrij

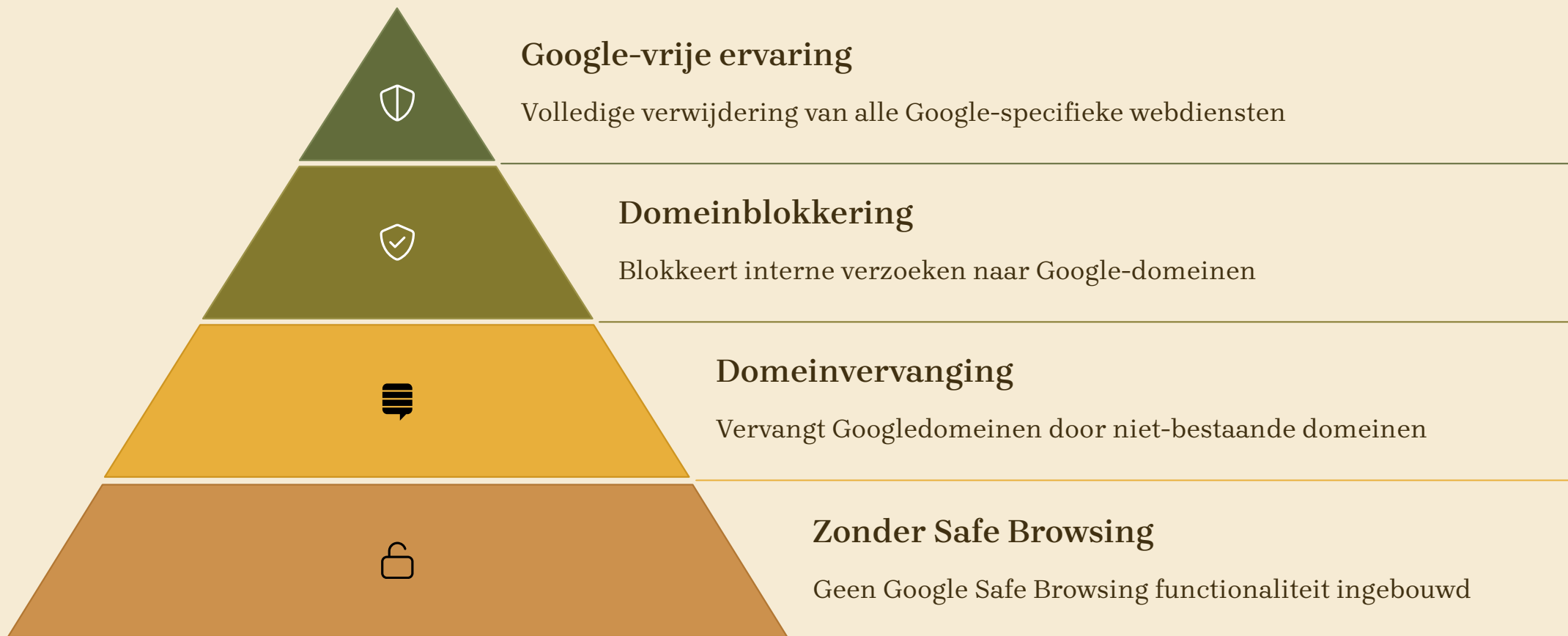
Behoud van Chromium-ervaring zonder Google-diensten.



## Open-source

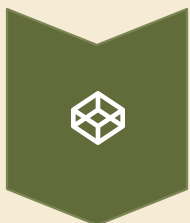
Vrije software onder BSD-licentie, nu beheerd door de "ungogled-software" community.

# Belangrijkste Kenmerken





# Privacy Verbeteringen



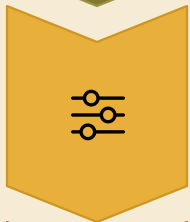
## Blob verwijdering

Verwijdering van binaire blobs in de Chromium-code



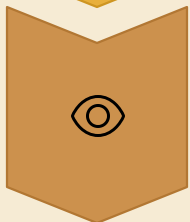
## Alternatieven

Vervanging door aangepaste privacyvriendelijke alternatieven



## Configuratie

Toevoeging van tientallen privacy-configuratie-opties



## Transparantie

Transparantere werking van de browser voor de gebruiker





# Vergelijking met Andere Browsers

| Browser           | Engine | Privacy | Google Diensten |
|-------------------|--------|---------|-----------------|
| Chromium          | Blink  | Matig   | Volledig        |
| Ungogled Chromium | Blink  | Hoog    | Geen            |
| Firefox           | Gecko  | Hoog    | Beperkt         |
| Brave             | Blink  | Hoog    | Beperkt         |

# Voor- en Nadelen

## Voordelen

- Betere privacy bescherming
- Veel minder tracking
- Meer controle over browsergedrag
- Snellere laadtijden

## Nadelen

- Moeilijker installeren van extensies
- Updates niet automatisch
- Speciale extensie nodig voor Chrome Web Store
- Meer technische kennis vereist



# Installatie en Gebruik

## Download kiezen

Kies de juiste build voor jouw besturingssysteem (Windows, macOS of Linux).

## Installeren

Volg de installatierichtlijnen specifiek voor jouw platform.

## Configureren

Pas de privacy-instellingen aan voor optimale bescherming.

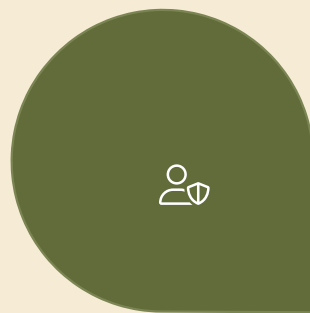
## Extensies toevoegen

Installeer chromium-web-store extensie voor toegang tot Chrome Web Store.

# Conclusie: Is Het De Browser Voor Jou?

## Privacybewust

Ideaal voor gebruikers die privacy prioriteit geven.

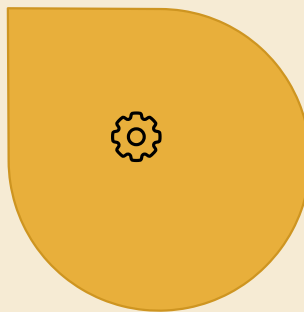
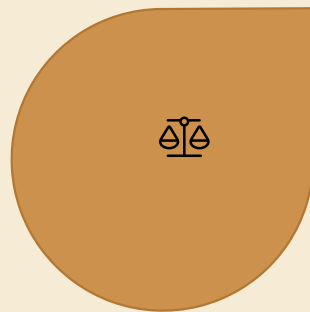


## Google-vrij

Perfect als je Google-services wilt vermijden.

## Perfekte balans

Evenwicht tussen functionaliteit en privacy.



## Technische kennis

Vereist meer technische kennis dan standaard browsers.

# Wat is Poort 443?

Poort 443 is een virtuele, veilige poort voor dataverkeer op internet. Het is de standaardpoort voor HTTPS-verkeer.

Deze poort is één van de 65.535 genummerde netwerkpoorten die beschikbaar zijn voor internetcommunicatie.

VEILIGDIGITAAL.COM





# Poort 443 vs. Poort 80 (HTTP)

## Poort 80

Verwerkt onversleuteld HTTP-verkeer. Dit is zichtbaar aan 'http:/' in het webadres.

Biedt geen databeveiliging tijdens verzending.

## Poort 443

Verwerkt versleuteld HTTPS-verkeer. Dit is zichtbaar aan 'https:/' in het webadres.

Zorgt voor veilige gegevensoverdracht.



# Waarom is Poort 443 belangrijk?



## Veilige communicatie

Maakt beveiligde communicatie via HTTPS mogelijk.



## Gegevensbescherming

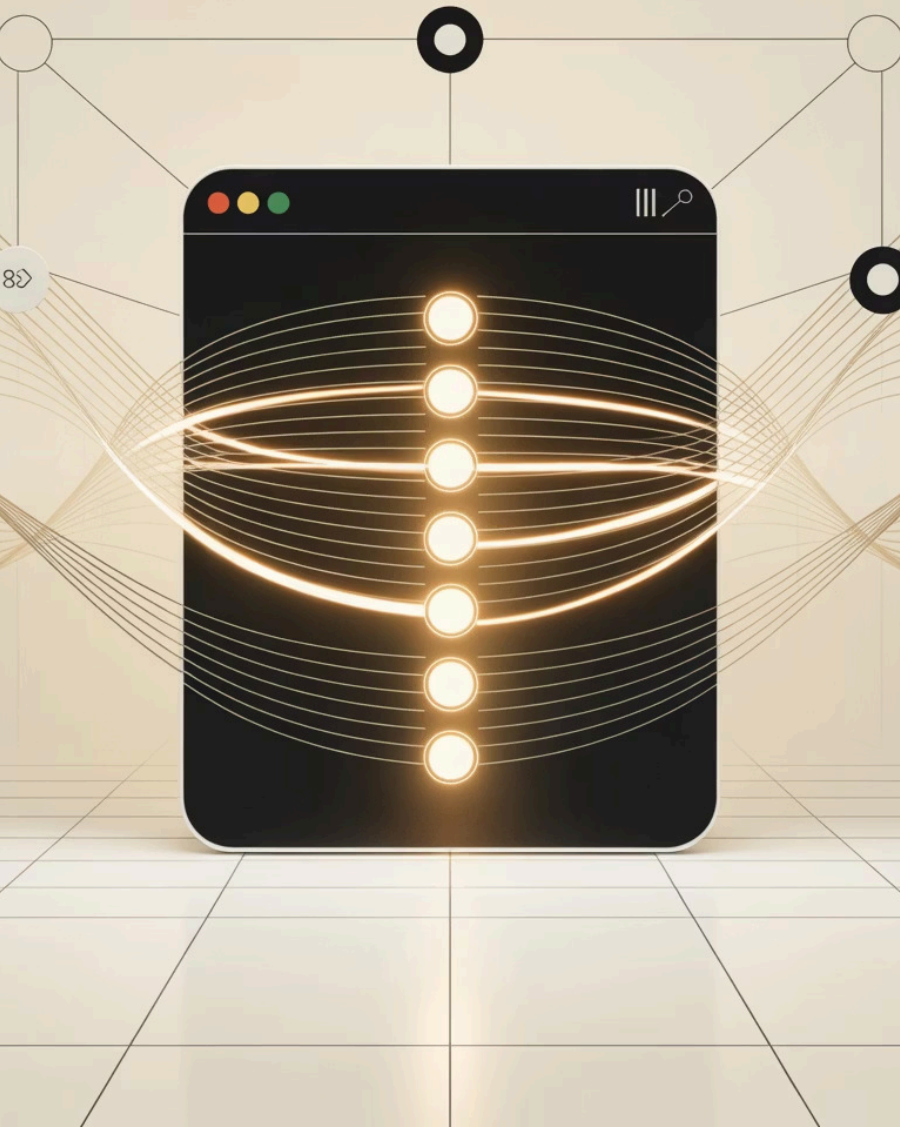
Beschermt gevoelige informatie zoals wachtwoorden en betaalgegevens.



## Cyberbeveiliging

Helpt bij het voorkomen van datalekken en cyberaanvallen.

## SSL/TLS Handshake Process



# Hoe werkt Poort 443 met SSL/TLS?



## Certificaatverificatie

SSL/TLS-certificaten verifiëren identiteit.



## TLS-handshake

Browser en server wisselen veilig encryptiesleutels uit.



## Versleutelde verbinding

Data blijft vertrouwelijk tijdens verzending.

# Praktijkvoorbeelden & Conclusie



## Online Bankieren

Gebruikt standaard poort 443 voor veilige transacties.



## Webshops

Beschermen klantgegevens via beveiligde verbindingen.



## E-maildiensten

Beveiligen communicatie via geëncrypteerde verbindingen.

**Poort 443 is dé standaard voor veilig en vertrouwelijk internetverkeer.**