



VEILIG DIGITAAL MAGAZINE



AFM: Schade door oplichting met beleggingstrucs tien keer hoger dan gedacht

De Autoriteit Financiële Markten onthult schokkende nieuwe cijfers over de omvang van beleggingsfraude in Nederland. De werkelijke schade blijkt tienvoudig hoger dan aanvankelijk gedacht.

De Schokkende Herziening van de Schade

Recent onderzoek van de Autoriteit Financiële Markten (AFM) toont aan dat de financiële schade door beleggingstrucs en oplichting in Nederland tien keer hoger is dan eerder werd ingeschat. Waar aanvankelijk werd uitgegaan van enkele tientallen miljoenen euro's, blijkt de werkelijke schade in de **honderden miljoenen euro's** te lopen.

Deze drastische herziening onderstreept de groeiende complexiteit en schaal van fraude in de financiële markten. De AFM erkent dat de problematiek veel ernstiger is dan gedacht.



10x

Hogere schade

Dan oorspronkelijk ingeschat

100M+

Euro's verlies

Totale geschatte schade

1000+

Slachtoffers

Gedupeerde beleggers

Impact op Slachtoffers en Maatschappij

Duizenden particuliere beleggers en consumenten zijn slachtoffer geworden van misleidende en frauduleuze beleggingsaanbiedingen. Veel slachtoffers verliezen niet alleen hun spaargeld, maar kampen ook met langdurige financiële en emotionele gevolgen die hun leven ingrijpend beïnvloeden.



Boilerroompraktijken

Agressieve verkooptactieken waarbij slachtoffers onder druk worden gezet om snel te investeren in waardeloze aandelen



Ponzi-constructies

Frauduleuze beleggingsconstructies waarbij rendement wordt betaald uit inleg van nieuwe investeerders



Dubieuze platforms

Professioneel ogende maar frauduleuze beleggingsplatformen die geld ontvreemden

Maatschappelijke impact: De oplichting ondermijnt het vertrouwen in de financiële markten en het toezicht, met gevolgen voor de gehele economie.



De Rol en Acties van de AFM

De AFM intensificeert haar toezicht en handhaving op verdachte beleggingspraktijken en waarschuwt consumenten actief via haar waarschuwingspagina's. De toezichthouder neemt concrete stappen om fraude te bestrijden en slachtoffers te beschermen.

01

Intensief toezicht

Actieve monitoring van verdachte beleggingsactiviteiten en platforms

02

Waarschuwingen publiceren

Consumenten informeren over frauduleuze entiteiten zoals '24/7forextrades', 'afk capital' en 'binance center ai'

03

Klachten verzamelen

Slachtoffers aanmoedigen meldingen te doen voor gerichte onderzoeken

04

Internationale samenwerking

Partnerschappen met buitenlandse toezichthouders voor grensoverschrijdende fraude



Voorbeelden van frauduleuze entiteiten

- **24/7forextrades** - Valse forex handelsplatform
- **afk capital** - Niet-geregistreerde beleggingsonderneming
- **binance center ai** - Misleidende crypto-investering

De AFM werkt aan sancties en juridische stappen tegen deze en andere fraudeurs.

Conclusie en Aanbevelingen

De tienvoudige stijging van de geschatte schade benadrukt de urgentie voor consumenten om waakzaam te zijn en kritisch te blijven bij beleggingsaanbiedingen. De AFM blijft inzetten op transparantie, voorlichting en streng toezicht om het vertrouwen in de financiële markten te herstellen en verdere schade te voorkomen.

1

Controleer registratie

Beleg alleen via erkende en door de AFM geregistreeerde partijen. Controleer dit altijd vooraf.

2

Wees kritisch

Bij onrealistische rendementsbeloften of druk om snel te beslissen: stop en check de AFM waarschuwingslijst.

3

Neem contact op

Bij twijfel of verdachte situaties direct contact opnemen met de AFM voor advies en verificatie.

4

Meld fraude

Slachtoffers en getuigen worden aangemoedigd om fraude te melden voor effectieve handhaving.



Samen tegen fraude

Samenwerking tussen toezichthouders, financiële instellingen en consumenten is cruciaal om deze groeiende fraude effectief te bestrijden. Alleen door gezamenlijke waakzaamheid kunnen we de financiële markten veiliger maken.



**Amerikanen kunnen straks toch wel
jouw DigiD-gegevens bekijken**

De digitale beveiliging van persoonlijke gegevens staat onder toenemende druk. Recent nieuws heeft zorgen opgeroepen over de mogelijke toegang van Amerikaanse instanties tot DigiD-gegevens van Nederlandse burgers. Dit roept fundamentele vragen op over privacy, datasoevereiniteit en de veiligheid van onze meest gevoelige persoonlijke informatie in het digitale tijdperk.

Wat is DigiD en welke gegevens bevat het?

DigiD is het digitale identificatiesysteem waarmee Nederlanders veilig kunnen inloggen bij overheidsinstanties en aangesloten organisaties zoals gemeenten, zorgverzekeraars en de Belastingdienst. Het systeem vormt de digitale sleutel tot een schat aan persoonlijke informatie die de overheid over haar burgers beheert.

Via DigiD krijg je toegang tot persoonlijke gegevens zoals je naam, adres, burgerservicenummer (BSN), nationaliteit, geregistreerd inkomen, voertuiggegevens en meer, die zijn opgeslagen in de Basisregistratie Personen (BRP) en andere overheidsdatabases. Deze gegevens vormen samen een uitgebreid digitaal profiel van elke Nederlandse burger.

Je kunt deze gegevens zelf inzien en beheren via MijnOverheid.nl, waar je met DigiD kunt inloggen om bijvoorbeeld je persoonsgegevens te controleren en berichten van de overheid te ontvangen. Dit centrale toegangspunt maakt het leven gemakkelijker, maar creëert tegelijkertijd een potentieel kwetsbaar punt in de digitale infrastructuur.



Persoonlijke identificatie

Naam, adres, BSN, geboortedatum, nationaliteit en burgerlijke staat



Financiële gegevens

Inkomensgegevens, belastingaangiften en toeslagen



Zorggegevens

Zorgverzekering en medische registraties



Voertuiginformatie

Kentekens en voertuigregistraties

Hoe veilig is DigiD en wat zijn de nieuwe inlogmethodes?

DigiD gebruikt meerdere beveiligingslagen om de toegang tot gevoelige overheidsgegevens te beschermen. Het systeem combineert traditionele authenticatiemethoden zoals gebruikersnaam en wachtwoord met moderne beveiligingstechnologieën zoals sms-controle en de DigiD-app met tweefactorauthenticatie. Deze gelaagde aanpak zorgt ervoor dat zelfs als één beveiligingslaag wordt doorbroken, er nog andere barrières zijn die ongeautoriseerde toegang voorkomen.

Sinds 2021 is het ook mogelijk om in te loggen met een Nederlandse identiteitskaart die een inlogfunctie heeft, waarbij je via NFC (Near Field Communication) en een pincode extra privacygevoelige gegevens kunt benaderen. Deze methode maakt gebruik van de ingebouwde chip in moderne identiteitskaarten en biedt een extra beveiligingslaag door fysieke toegang tot de kaart te vereisen.

Deze nieuwe methode is bedoeld om maximale bescherming te bieden voor de meest gevoelige transacties en gegevenstoegang, maar is momenteel niet verplicht en alleen beschikbaar voor inwoners met een identiteitskaart die vanaf 13 maart 2021 is uitgegeven. De gefaseerde invoering geeft burgers de tijd om over te stappen op deze modernere en veiligere authenticatiemethode.



Gebruikersnaam en wachtwoord

De eerste beveiligingslaag met persoonlijke inloggegevens



SMS-controle

Eenmalige code verstuurd naar geregistreerd telefoonnummer



DigiD-app

Tweefactorauthenticatie via mobiele applicatie



ID-kaart met NFC

Hoogste beveiligingsniveau met fysieke identiteitskaart

De zorgen over Amerikaanse toegang tot DigiD-gegevens

Er is recent nieuws naar buiten gekomen dat Amerikaanse instanties of bedrijven mogelijk toch toegang kunnen krijgen tot DigiD-gegevens van Nederlandse burgers, wat fundamentele vragen oproept over privacy en dataveiligheid. Deze onthullingen hebben geleid tot bezorgdheid bij privacy-experts, juristen en burgers over de daadwerkelijke controle die Nederland heeft over de meest gevoelige persoonlijke gegevens van haar inwoners.

Dit kan te maken hebben met het gebruik van Amerikaanse cloudproviders, softwareleveranciers of dataverkeer via Amerikaanse servers, waardoor data onder Amerikaanse jurisdictie kan vallen. Bekende voorbeelden zijn Amerikaanse wetten zoals de CLOUD Act en de FISA 702, die Amerikaanse autoriteiten brede bevoegdheden geven om toegang te eisen tot data die door Amerikaanse bedrijven wordt beheerd, ongeacht waar die data fysiek wordt opgeslagen. Dit betekent dat zelfs wanneer servers zich in Nederland bevinden, de data toch toegankelijk kan zijn voor Amerikaanse inlichtingendiensten.

Hoewel de Nederlandse overheid strenge regels hanteert voor gegevensbescherming onder de Algemene Verordening Gegevensbescherming (AVG), is er bezorgdheid over mogelijke kwetsbaarheden en het risico op misbruik of ongeautoriseerde toegang vanuit het buitenland. De spanning tussen nationale soevereiniteit, internationale samenwerking op het gebied van veiligheid, en fundamentele privacyrechten van burgers wordt hiermee pijnlijk zichtbaar. Experts wijzen op de noodzaak van complete transparantie over welke diensten worden gebruikt en welke waarborgen er zijn getroffen.



Cloudproviders

Amerikaanse cloudservices die mogelijk overheidsdata hosten



Softwareleveranciers

Systemen ontwikkeld door bedrijven onder Amerikaanse jurisdictie



Dataverkeer

Gegevens die via Amerikaanse servers worden gerouteerd

📄 **Juridische context:** De CLOUD Act geeft Amerikaanse autoriteiten het recht om data op te vragen bij Amerikaanse bedrijven, zelfs wanneer deze data buiten de VS wordt opgeslagen. Dit kan conflicteren met Europese privacywetgeving.

Wat kun je doen en wat doet de overheid?

Bescherm jezelf actief

Controleer regelmatig je DigiD-gebruik en persoonlijke gegevens via MijnOverheid en meld verdachte activiteiten direct bij DigiD en de Fraudehelpdesk. Waakzaamheid is je eerste verdedigingslinie tegen misbruik van je digitale identiteit. Door actief toezicht te houden op je account kun je ongeautoriseerde toegang snel detecteren en aanpakken.



1

Monitor je account

Log regelmatig in op MijnOverheid.nl om je inloggeschiedenis te controleren. Let op onbekende inlogpogingen of toegang vanaf vreemde locaties. Bekijk welke organisaties toegang hebben gehad tot je gegevens.

2

Wees alert op phishing

Scan nooit zomaar QR-codes of klik op links die je niet vertrouwt. De overheid vraagt nooit per e-mail of sms om je DigiD-gegevens. Bij twijfel, ga altijd direct naar de officiële website.

3

Update je beveiliging

Wijzig je DigiD-wachtwoord bij twijfel en zorg voor een sterk, uniek wachtwoord. Activeer alle beschikbare beveiligingsopties, waaronder tweefactorauthenticatie via de DigiD-app.

4

Bij verlies of diefstal

Bij diefstal van je telefoon met DigiD-app kun je de app op afstand deactiveren via je DigiD-account om misbruik te voorkomen. Dit voorkomt dat criminelen toegang krijgen tot je digitale identiteit.

Overheidsmaatregelen en toekomstige stappen

De overheid werkt aan verbeterde beveiligingsmaatregelen en onderzoekt de juridische en technische mogelijkheden om buitenlandse toegang tot gevoelige data te beperken. Dit omvat evaluatie van huidige contracten met leveranciers, verkenning van Europese alternatieven voor cloudopslag en software, en versterking van encryptie en andere technische beveiligingen. Transparantie over deze inspanningen is cruciaal voor het vertrouwen van burgers in digitale overheidsdiensten.



Onderzoek

Analyse van huidige kwetsbaarheden en risico's



Versterking

Implementatie van extra beveiligingslagen



Contractbeheer

Heronderhandeling met leveranciers



Monitoring

Continue bewaking en verbetering



**AP gaat controleren hoe huisartsen
en ziekenhuizen patiëntgegevens
beveiligen**

De Autoriteit Persoonsgegevens start grootschalige controles om te waarborgen dat zorgverleners patiëntgegevens adequaat beschermen tegen cyberdreigingen en datalekken.

Achtergrond en belang van informatiebeveiliging in de zorg

Patiëntgegevens behoren tot de meest gevoelige informatie die organisaties verwerken. Huisartsen en ziekenhuizen verwerken dagelijks grote hoeveelheden medische data die essentieel zijn voor kwalitatief goede zorg en patiëntveiligheid. Deze gegevens vereisen daarom strikte bescherming tegen ongeautoriseerde toegang, diefstal en datalekken.

De Algemene Verordening Gegevensbescherming (AVG) verplicht zorgaanbieders tot het treffen van passende technische en organisatorische maatregelen om de privacy van patiënten te waarborgen. De Autoriteit Persoonsgegevens (AP) neemt haar toezichthoudende rol daarom uiterst serieus en start controles om naleving van deze beveiligingsverplichtingen actief te waarborgen.



Gevoelige data

Medische informatie vereist maximale bescherming



AVG-naleving

Wettelijke verplichting voor alle zorgaanbieders

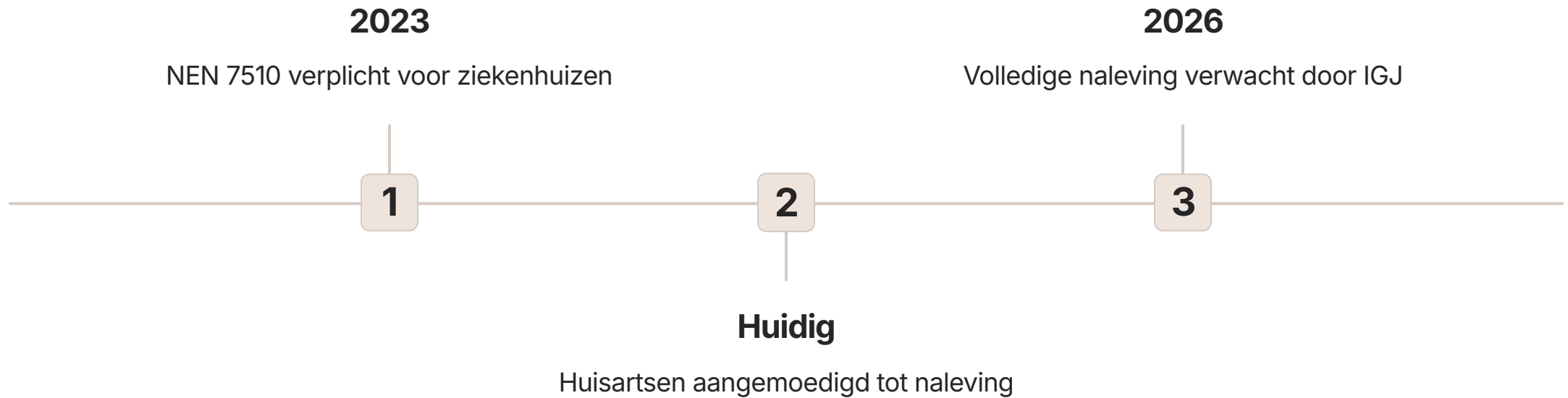


AP-toezicht

Actieve controles op beveiligingsmaatregelen

Wettelijk kader en de rol van NEN 7510

NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorgsector en richt zich op drie cruciale pijlers: beschikbaarheid, integriteit en vertrouwelijkheid van medische gegevens. Deze norm biedt zorgorganisaties een concreet framework om hun informatiebeveiliging op orde te krijgen.



Internationale aansluiting

De norm sluit naadloos aan op internationale standaarden zoals ISO 27001 en ondersteunt naleving van de aankomende Cyberbeveiligingswet en de Europese NIS2-verordening. Dit zorgt voor consistentie in beveiligingsniveaus binnen Europa.

Certificering vs. naleving

Hoewel certificering niet wettelijk verplicht is, moeten zorgorganisaties wél aantoonbaar aan de norm voldoen. Dit kan bijvoorbeeld via onafhankelijke audits die de implementatie van beveiligingsmaatregelen controleren.

Actuele tekortkomingen en toezicht door IGJ en AP

IGJ-onderzoek onthult lacunes

Recent onderzoek door de Inspectie Gezondheidszorg en Jeugd (IGJ) toonde grote tekortkomingen aan in onafhankelijke beoordelingen van informatiebeveiliging bij huisartsenspoedzorg. Deze bevindingen baren zorgen over de daadwerkelijke bescherming van patiëntdata.

Ontbrekende audits

Veel organisaties missen nog een volledige en onafhankelijke audit volgens NEN 7510. Hierdoor blijft onduidelijk of patiëntgegevens werkelijk voldoende beschermd zijn tegen cyberdreigingen en ongeautoriseerde toegang.

Verhoogde druk IGJ

De IGJ verhoogt de druk op zorgorganisaties en verwacht dat alle huisartsendiensten in 2026 aantoonbaar voldoen aan de NEN 7510-norm. Deze deadline geeft organisaties een duidelijke planning voor verbetering.

AP-controles

De Autoriteit Persoonsgegevens sluit hierop aan met eigen controles die specifiek gericht zijn op naleving van privacywetgeving en beveiligingsmaatregelen bij huisartsen en ziekenhuizen.

Praktische gevolgen en aanbevelingen voor zorgaanbieders

Zorgaanbieders moeten nu actie ondernemen om aan de strengere beveiligingseisen te voldoen. Hieronder vindt u concrete aanbevelingen en praktische stappen.

01

Risicoanalyse uitvoeren

Start met een grondige risicoanalyse en stel een beleidsplan op voor informatiebeveiliging

03

Externe expertise inschakelen

Werk samen met deskundigen en zet onafhankelijke audits in om risico's te beheersen

02

Systemen in kaart brengen

Breng alle gebruikte hard- en software, toegangsrechten en beveiligingsmaatregelen in kaart

04

Transparantie vergroten

Bied patiënten inzage en controle via platforms zoals Volgjezorg

Praktische basismaatregelen

- Vergrendel systemen bij verlaten spreekkamers
- Implementeer sterke toegangscontroles
- Train personeel regelmatig over beveiliging
- Voer regelmatige back-ups uit

Patiëntbetrokkenheid

Platforms zoals Volgjezorg stellen patiënten in staat zelf toestemming te geven voor gegevensdeling en inzage te houden in wie hun gegevens bekijkt. Dit versterkt het vertrouwen en voldoet aan transparantievereisten.

 **Belangrijke boodschap:** Zorgaanbieders moeten zich nu voorbereiden op strengere wetgeving en intensiever toezicht. Transparantie en aantoonbare beveiliging staan hierbij centraal. Wacht niet tot controles plaatsvinden, maar neem nu actie.



De Australische Federale Politie en AI: Emoji's en Jargon van Generatie Z en Alpha Ontcijferen

In een wereld waar digitale communicatie steeds complexer wordt, neemt de Australische Federale Politie (AFP) een baanbrekend initiatief. Ze ontwikkelen een geavanceerd AI-systeem dat speciaal is ontworpen om de unieke digitale taal van jonge generaties te begrijpen. Dit innovatieve project richt zich op het ontcijferen van emoji's, slang en jargon die door Generatie Z en Generatie Alpha worden gebruikt in hun online communicatie.

Waarom een AI voor jongerentaal en emoji's?

Het digitale taalprobleem

Online communicatie van Generatie Z en Alpha bestaat voor een groot deel uit emoji's, afkortingen en slang die voor buitenstaanders onbegrijpelijk zijn. Deze generaties hebben een compleet nieuwe vorm van digitale communicatie ontwikkeld, waarbij traditionele taalregels vaak niet meer van toepassing zijn.

Criminelen binnen deze generaties gebruiken deze codes slim om online misdaden te bespreken en te plannen, waardoor traditionele opsporingsmethoden volledig tekortschieten. Ze verbergen hun criminele activiteiten achter ogenschijnlijk onschuldige emoji-combinaties en afkortingen.



Detectie verbeteren

De AFP ontwikkelt een AI-systeem dat deze digitale taal kan interpreteren om criminele communicatie sneller en nauwkeuriger te detecteren.



Explosieve groei

Dit initiatief speelt in op de explosieve groei van digitale communicatie en de toenemende complexiteit van moderne misdaadbestrijding.



Digitale transformatie

De politie moet mee evolueren met de manier waarop jongeren communiceren om effectief te blijven in criminaliteitsbestrijding.

Technische uitdagingen en aanpak van de AFP

Het ontwikkelen van een AI-systeem dat de complexe digitale taal van jongeren kan begrijpen, brengt aanzienlijke technische uitdagingen met zich mee. De kern van het probleem ligt in de contextgevoeligheid van moderne online communicatie: emoji's kunnen meerdere betekenissen hebben afhankelijk van de combinatie, volgorde en situatie waarin ze worden gebruikt. Een vuurwerkje kan bijvoorbeeld vieren betekenen, maar in bepaalde contexten ook verwijzen naar illegale vuurwerkhandel of zelfs wapens.



Data verzameling

Training met datasets van echte online gesprekken, waarbij privacy en ethiek streng worden bewaakt.



Machine Learning

Geavanceerde natuurlijke taalverwerking (NLP) om patronen in slang en emoji-gebruik te herkennen.



Context analyse

Het systeem leert om betekenis af te leiden uit combinaties en situationele context.

Vergelijkbare technologieën in actie

Het AFP-project staat niet op zichzelf. Vergelijkbare technologieën worden al succesvol ingezet bij het ontcijferen van versleutelde berichten. Een opvallend voorbeeld is de hack van EncroChat in Nederland in 2020, waar AI een cruciale rol speelde bij het ontcijferen van gecodeerde criminele communicatie.

Dit resulteerde in honderden arrestaties en het oprollen van meerdere criminele netwerken. De lessen die zijn geleerd uit deze operatie vormen een waardevolle basis voor het nieuwe AFP-systeem, dat zich specifiek richt op de unieke communicatiestijl van jongere generaties.

Maatschappelijke impact en veiligheidscontext

Snellere respons

De inzet van AI helpt de politie om sneller te reageren op online misdaad, zoals drugshandel, grooming en cyberpesten, die vaak via verborgen taal plaatsvinden.

Privacy uitdagingen

Het gebruik van AI roept belangrijke vragen op over privacy, gegevensbescherming en het risico op verkeerde interpretaties van onschuldige gesprekken.

Australië voert tegelijkertijd bredere maatregelen tegen AI-misbruik, zoals het bestrijden van AI-gegenereerde kindermisbruikbeelden, wat de urgentie van verantwoord AI-gebruik onderstreept. Deze parallelle ontwikkelingen tonen aan dat de bescherming van kinderen en jongeren in de digitale wereld een absolute prioriteit heeft gekregen voor de Australische autoriteiten.

Internationale samenwerking

Digitale misdaad kent geen grenzen. Politiediensten wereldwijd delen kennis en technologie om gezamenlijk deze uitdagingen aan te pakken.

Wetgeving en regulering

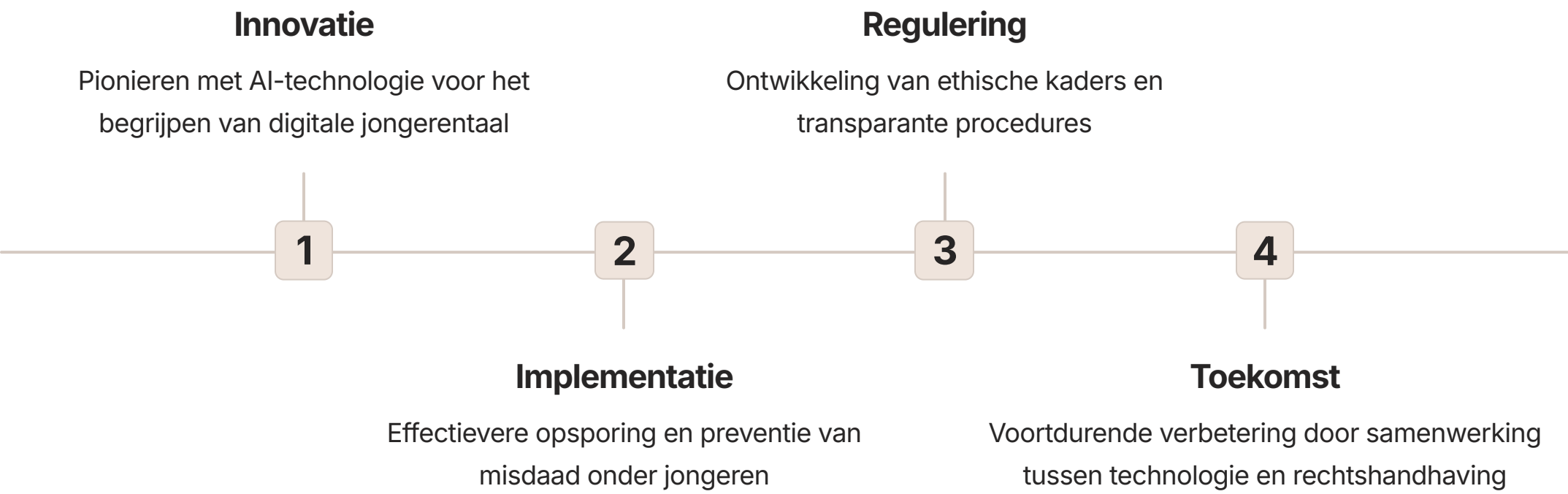
Er is dringende behoefte aan internationale wetgeving die zowel effectieve criminaliteitsbestrijding mogelijk maakt als burgerrechten beschermt.

Balans tussen veiligheid en privacy

Het vinden van de juiste balans tussen effectieve opsporing en het respecteren van privacy blijft een voortdurende uitdaging voor beleidsmakers.

Conclusie: Naar een toekomstbestendige politiezorg met AI

Het AI-project van de Australische Federale Politie vertegenwoordigt een belangrijke mijlpaal in de evolutie van moderne politiezorg. Het is een baanbrekend voorbeeld van hoe politieorganisaties zich proactief aanpassen aan de digitale samenleving en de nieuwe communicatietechnologieën die jongere generaties gebruiken. Deze aanpak erkent dat traditionele opsporingsmethoden ontoereikend zijn geworden in een wereld waar digitale communicatie steeds gelaagder en complexer wordt.



Door emoji's en jongerentaal te begrijpen, kan de politie effectiever misdaad opsporen en voorkomen, wat de veiligheid van jongeren en de bredere samenleving aanzienlijk vergroot. Dit draagt bij aan een veiligere digitale omgeving waarin criminelen minder makkelijk kunnen opereren onder de radar.

Tegelijkertijd blijft het absoluut essentieel om transparantie, ethiek en wettelijke kaders te waarborgen bij het gebruik van AI in politiewerk. Zonder deze waarborgen bestaat het risico dat de technologie wordt misbruikt of dat onschuldige burgers ten onrechte onder verdenking komen te staan.



Deze ontwikkeling illustreert de noodzaak van voortdurende innovatie en nauwe samenwerking tussen technologie, rechtshandhaving en maatschappij om digitale dreigingen effectief het hoofd te bieden, waarbij de bescherming van fundamentele rechten centraal blijft staan.

**Deze Android-privacyinstellingen
beschermen je tegen cybercrime**

Cybercriminaliteit richt zich steeds vaker op smartphones. Android-toestellen bevatten veel persoonlijke data. Denk aan je bankpas, e-mail en persoonlijke foto's. Gelukkig biedt Android zelf een aantal privacy- en beveiligingsinstellingen die je direct kunt aanpassen om het risico op misbruik, fraude en datalekken te verkleinen. Hieronder leggen we uit welke instellingen dat zijn, wat ze precies doen en hoe je zelf kunt controleren of ze goed staan ingesteld.

App-machtigingen beperken

Een van de belangrijkste stappen is het kritisch beheren van je app-machtigingen. Veel apps vragen toegang tot functies die ze niet strikt nodig hebben. Denk aan continu toegang tot je locatie, microfoon of zelfs contacten. Het is sowieso goed om deze instellingen langs te lopen en te kijken of je dit nodig hebt. Daar komt bij dat kwaadaardige apps deze rechten vaak gebruiken om gegevens te verzamelen en door te spelen aan de verkeerde personen.

In Android kun je dit controleren via **Instellingen > Beveiliging en Privacy > Privacyopties**. Hier zie je per categorie welke apps toegang hebben. Zet machtigingen die niet logisch zijn uit of kies voor "Alleen toestaan tijdens gebruik". Google adviseert expliciet om permanente locatietoegang te vermijden bij apps die dat eigenlijk niet nodig hebben, omdat dit het risico op tracking en datamisbruik vergroot. Bekijk hier ook het **Privacydashboard** af en toe. Dit geeft aan precies aan welke rechten de afgelopen 24 uur zijn gebruikt. Zo had mijn WhatsApp toegang tot mijn camera en werd mijn locatie gebruikt door een weerapp, Maps en Home.

Locatiegeschiedenis en locatie-delings uitschakelen

Over locaties gesproken, Android houdt standaard een locatiegeschiedenis bij via je Google-account. Die gegevens kunnen waardevol zijn voor gepersonaliseerde diensten, maar vormen ook een privacyrisico als ze in verkeerde handen vallen.

01

Ga naar Instellingen

Open de instellingen op je Android-toestel

02

Beveiliging en Privacy

Navigeer naar het privacy-menu

03

Privacyopties

Scroll naar Locatie om toegang te beheren

Je kunt dit aanpassen via dezelfde opties als de rechten. Locatie valt namelijk onder dezelfde noemer. Ga dus naar **Instellingen**, **Beveiliging en Privacy**, **Privacyopties** en scroll hier naar **Locatie**. Ook een stap terug, dus direct bij **Instellingen** vind je een knop met **Locatie**. Hier zag ik dat bijvoorbeeld TomTom altijd toegang heeft tot mijn locatie, maar dat natuurlijk alleen nodig is wanneer ik wil navigeren. Scroll hier eens door de lijst en vraag je af of de locatie gedeeld moet worden met die app. Wat heeft de app van mijn sportschool er bijvoorbeeld aan om altijd te weten waar ik ben?

Blokkeer standaard toegang en installaties buiten de Play Store



Microfoon en camera

Malware maakt steeds vaker misbruik van microfoon- en cameratoegang. Android biedt daarom een handige schakelaar om deze toegang volledig uit te schakelen. Ga wederom naar **Instellingen > Beveiliging en Privacy > Privacyopties**. Hier vind je een schakelaar waarmee je **Cameratoegang** en **Microfoontoegang** snel uit kunt zetten. Hierdoor krijgt geen enkele app meer toegang tot deze opties.

App-installaties blokkeren

Cybercriminelen verspreiden malware vaak via apk-bestanden buiten de Google Play Store, bijvoorbeeld via phishinglinks of nepupdates. Android laat dit alleen toe als je daar expliciet toestemming voor geeft. Gebruik je dus alleen apps vanuit de Play Store, dan heb je geen reden om hier verder iets aan te veranderen.

Deze instelling controleer je, hoe kan het ook anders, via **Instellingen > Beveiliging en Privacy** en vervolgens **Geavanceerde beveiliging**. Hier wil je dat de knop voor **Apparaatbescherming** aan staat. De functie zorgt naast bescherming van apps van buitenaf, ook voor bescherming op netwerken, websites en telefoontjes.

Google Play Protect actief houden

Google Play Protect is Androids ingebouwde beveiligingssysteem tegen schadelijke apps. Het scant regelmatig apps. Zowel bij installatie als naderhand. Daarbij controleert het de apps op verdacht gedrag.

- 📄 Je vindt deze instelling in de Google Play Store. Klik daar op je **Profielicoon**, dit kan een gekozen profielfoto zijn of je initialen. Tik vervolgens op **Play Protect**. Hier kun je zien welke apps recent zijn gescand of handmatig een scan starten.

Automatische systeem- en beveiligingsupdates inschakelen

Cyberaanvallen komen op allerlei verschillende manieren. Een daarvan is misbruik maken van bekende beveiligingslekken. Google heeft daarom heel veel baat bij het up-to-date houden en patchen van dit soort problemen. Wij schrijven regelmatig over updates die ervoor zorgen dat kwetsbaarheden worden gedicht. Zo is er recent nog een probleem gevonden en opgelost in het besturingssysteem van Google.

Controleer updates

Ga naar **Instellingen** > **Systeem** > **Software-updates**

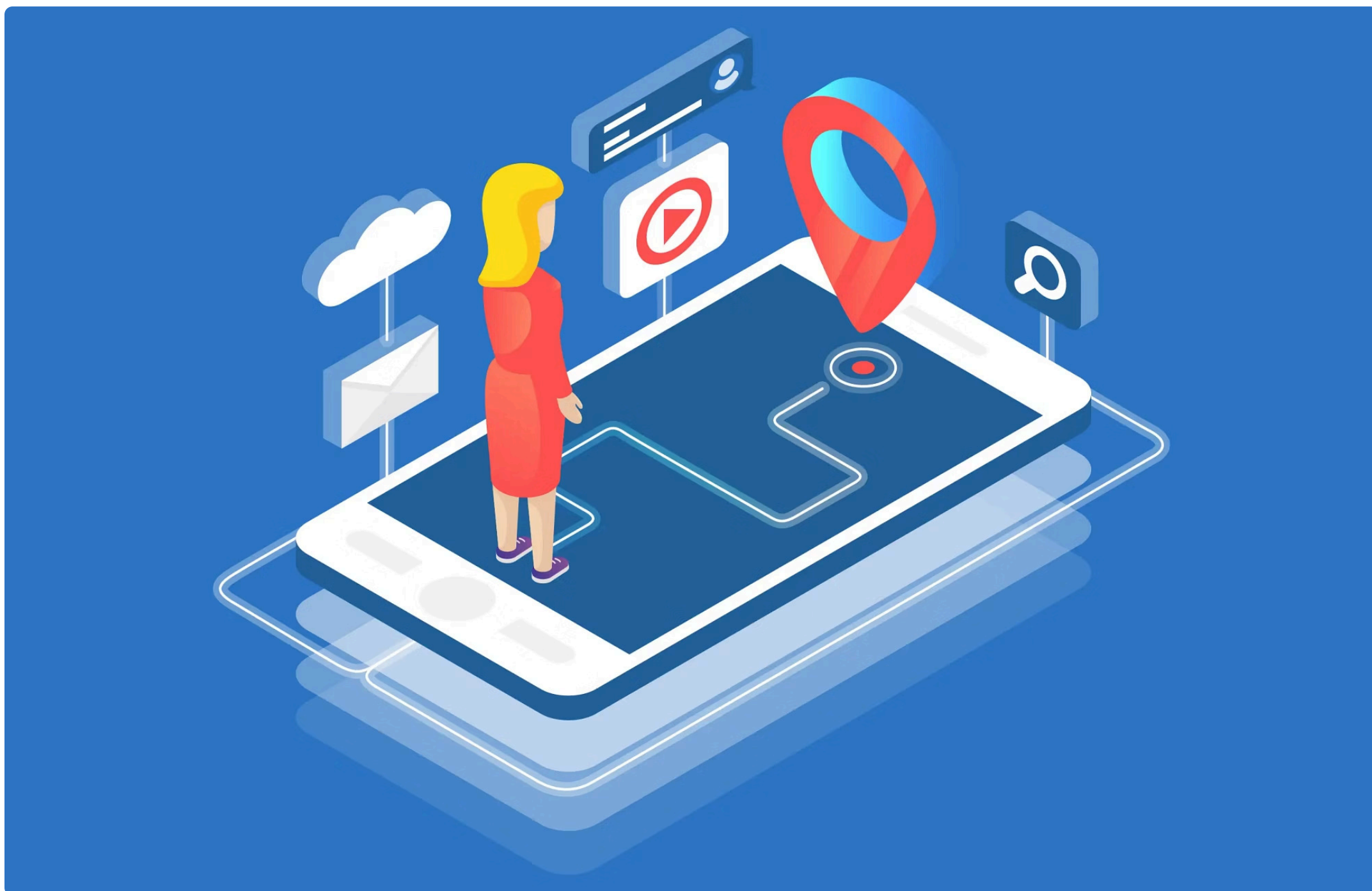
Bekijk status

Hier zie je wanneer jouw telefoon voor het laatst is voorzien van een update en welke Google Play-update er is geïnstalleerd op het toestel

Handmatig checken

Tik ook voor de zekerheid even op beide knoppen zodat de telefoon handmatig controleert of er een nieuwe update beschikbaar is. Als dat zo is, zal deze meteen installeren

App-tracking beperken en sterke schermvergrendeling gebruiken



App-tracking en advertentie-ID beperken

Android biedt opties om advertentietracking te beperken. Hoewel dit vooral voor privacy is bedoeld, verkleint het ook de hoeveelheid data die over je gedrag wordt verzameld en mogelijk misbruikt kan worden.

Je vindt deze instellingen via **Instellingen > Beveiliging en Privacy > Privacyopties**. Onder **Rechtenbeheer** zie je **Advertenties** staan. Hier kun je gepersonaliseerde advertenties uitschakelen of je advertentie-ID resetten. Volgens de [Autoriteit Persoonsgegevens](#) is dit een belangrijke stap om onnodige dataverzameling te beperken.

Sterke schermvergrendeling en biometrie gebruiken

Een eenvoudige pincode of patroon is relatief makkelijk te raden of af te kijken. Android ondersteunt daarom langere pincodes, wachtwoorden en biometrische beveiliging zoals vingerafdruk en gezichtsherkenning.

Ga daarvoor naar **Instellingen > Beveiliging en Privacy > Apparaatontgrendeling** en kies bij voorkeur een pincode van minimaal zes cijfers of een wachtwoord. Combineer dit met biometrie voor gebruiksgemak. Google en consumentenorganisaties benadrukken dat fysieke toegang tot het toestel vaak de eerste stap is bij datadiefstal. Via de vergrendeling kun je ook **Geoptimaliseerde privacy voor pincodes** instellen.

Door zelf deze instellingen te controleren en aan te scherpen, zorg je ervoor dat het gebruik van jouw mobiele Android-apparaat zo veilig mogelijk is.

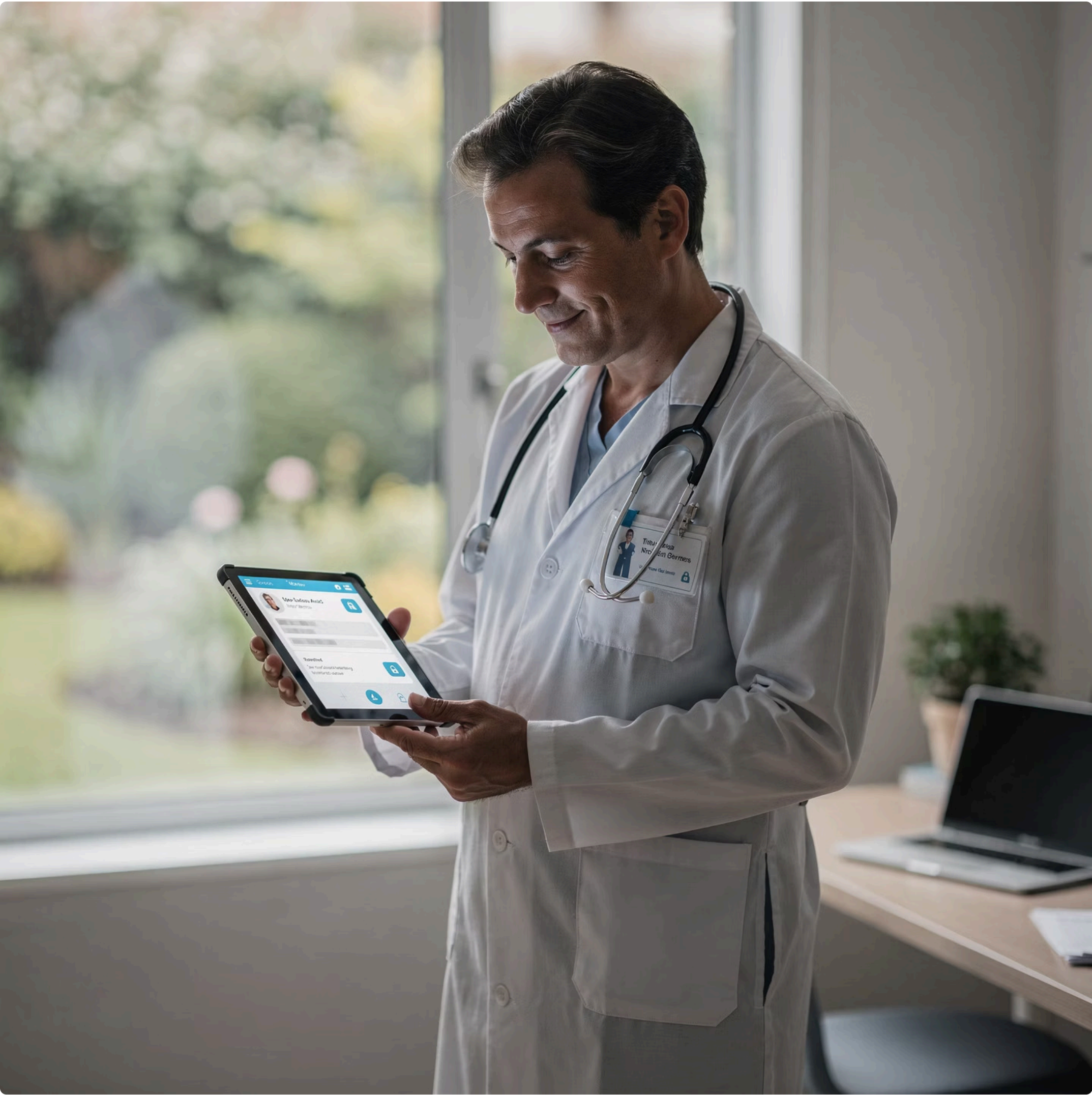


**Een nieuw landelijk systeem (Mitz)
voor het elektronisch delen van
medische gegevens: kansen en
risico's**

De Nederlandse gezondheidszorg staat aan de vooravond van een digitale revolutie. Met de invoering van Mitz, een landelijk systeem voor het elektronisch delen van medische gegevens, kunnen zorgverleners sneller en efficiënter toegang krijgen tot cruciale patiëntinformatie. Dit belooft levens te redden en de kwaliteit van zorg aanzienlijk te verhogen. Maar tegelijkertijd roept dit systeem fundamentele vragen op over privacy, toestemming en de mogelijkheid van ongewenste inzage in vertrouwelijke medische dossiers.

In dit document onderzoeken we de werking, voordelen en risico's van Mitz en het Landelijk Schakelpunt. We kijken kritisch naar de spanning tussen efficiënte zorgverlening en privacybescherming, en wat dit betekent voor de autonomie van patiënten in het digitale tijdperk.

Wat is Mitz en hoe werkt het in de praktijk?



Mitz is een revolutionair online toestemmingsvoorziening die patiënten de controle geeft over het elektronisch delen van hun medische gegevens. Het systeem fungeert als een digitale poortwachter die bepaalt welke zorgverleners toegang krijgen tot welke medische informatie. Door gebruik te maken van moderne encryptie en beveiligingstechnieken, zorgt Mitz ervoor dat alleen geautoriseerde partijen toegang kunnen krijgen tot gevoelige gezondheidsdata.

Het hart van het systeem wordt gevormd door het Landelijk Schakelpunt (LSP), dat fungeert als een beveiligde verwijzindex. Belangrijk om te benadrukken is dat het LSP zelf geen medische gegevens opslaat – het werkt puur als een intelligente routeplanner die aangeeft waar welke informatie te vinden is. Dit architectuurprincipe verhoogt de veiligheid aanzienlijk, omdat er geen centrale database bestaat met alle medische dossiers van Nederland.

01	02
Patiënt geeft toestemming	Zorgverlener vraagt toegang
Via Mitz regelt de patiënt welke zorgverleners toegang mogen krijgen tot hun medische gegevens	Bij een behandeling controleert de zorgverlener via het LSP of er toestemming is gegeven
03	04
Gegevens worden gedeeld	Alles wordt gelogd
Bij toestemming worden de benodigde medische gegevens veilig uitgewisseld tussen zorgsystemen	Elke toegang wordt vastgelegd, zodat patiënten kunnen zien wie hun dossier heeft bekeken

In de dagelijkse praktijk betekent dit dat zorgverleners bij spoedeisende situaties of waarneemzorg snel toegang kunnen krijgen tot vitale informatie zoals medicatieoverzichten, allergieën en eerdere diagnoses. Dit kan het verschil maken tussen leven en dood, vooral wanneer een patiënt bewusteloos is of niet in staat is om zelf informatie te verstrekken. Het systeem is ontworpen om de balans te vinden tussen snelle toegang tot levensreddende informatie en bescherming van de privacy van patiënten.

Wettelijke kaders en privacybescherming

De invoering van Mitz vindt niet plaats in een juridisch vacuüm. Het systeem is ingebed in een stevig kader van Nederlandse en Europese wetgeving die de rechten van patiënten beschermt en duidelijke grenzen stelt aan wie toegang mag hebben tot medische gegevens. De Wet op de geneeskundige behandelingsovereenkomst (WGBO) en de Algemene verordening gegevensbescherming (AVG) vormen samen de ruggengraat van deze bescherming.



Behandelrelatie vereist

Alleen zorgverleners die **direct betrokken** zijn bij de behandeling mogen inzage krijgen in het medische dossier



Noodzakelijkheidstoets

Toegang is alleen toegestaan als het **strikt noodzakelijk** is voor de behandeling of zorg



Transparantie door logging

Elke inzage wordt **geregistreerd** en patiënten hebben recht op inzage in deze logs

Rechten van patiënten

- Recht op inzage in wie hun dossier heeft bekeken via platforms als Volgjezorg
- Recht om toestemming te geven of te weigeren voor het delen van gegevens
- Recht om toestemming op elk moment in te trekken
- Recht op correctie van onjuiste gegevens
- Recht om bezwaar te maken tegen verwerking

Plichten van zorgverleners

- Zorgvuldig omgaan met patiëntgegevens volgens het beroepsgeheim
- Alleen toegang vragen wanneer dit noodzakelijk is
- Complete en accurate logging bijhouden van alle inzage
- Patiënten informeren over het gebruik van hun gegevens
- Technische en organisatorische beveiligingsmaatregelen treffen

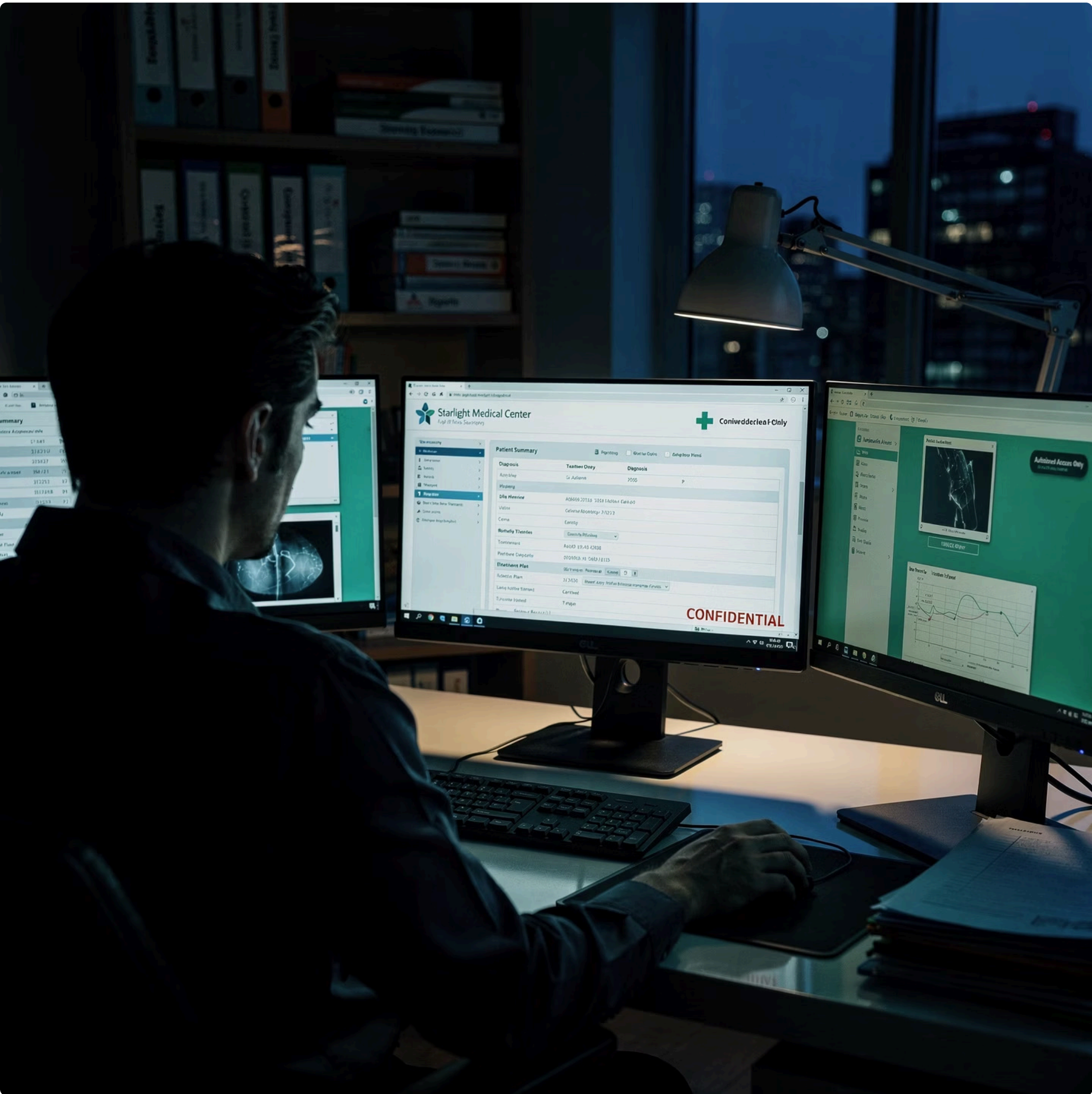
 **Let op:** Hoewel patiënten hun toestemming kunnen intrekken, kan dit in noodsituaties risico's met zich meebrengen. Zorgverleners bij de spoedeisende hulp hebben mogelijk cruciale informatie nodig om levensreddende beslissingen te nemen. Het is daarom belangrijk om zorgvuldig af te wegen wanneer en voor wie je toegang blokkeert.

De wetgeving erkent dat medische gegevens tot de meest gevoelige persoonlijke informatie behoren. Daarom gelden er strenge eisen aan de beveiliging, opslag en uitwisseling van deze data. Overtreding van deze regels kan leiden tot hoge boetes en strafrechtelijke vervolging. Toch blijft de vraag: is de wet voldoende om grootschalig misbruik te voorkomen?

De schaduwzijde: grootschalige, heimelijke inzage mogelijk?

Ondanks de ingebouwde waarborgen en wettelijke bescherming, bestaat er groeiende zorg over de mogelijkheid van grootschalige en heimelijke inzage in patiëntendossiers via Mitz en het Landelijk Schakelpunt.

Het landelijke karakter van het systeem creëert ongeken­de mogelijkheden voor datauitwisseling, maar opent ook deuren die voorheen gesloten waren. Waar voorheen medische dossiers fysiek gescheiden waren per zorginstelling, ontstaat nu een virtueel netwerk waarbij duizenden zorgverleners potentieel toegang kunnen krijgen tot dezelfde informatie.



Gerapporteerde zorgen en incidenten

Er zijn verschillende meldingen en zorgen geuit over ongewenste of heimelijke inzage in medische dossiers. Voorbeelden uit de praktijk tonen aan dat zorgverleners soms zonder directe behandelrelatie medische informatie raadplegen. Dit kan variëren van nieuwsgierige medewerkers die de dossiers van bekenden bekijken, tot structureler misbruik waarbij gegevens worden gebruikt voor doeleinden buiten de zorg.

Het probleem wordt verergerd doordat veel patiënten zich niet bewust zijn van de mogelijkheid om logging te controleren, of niet weten hoe ze dit moeten doen. Hierdoor kan ongeautoriseerde inzage lange tijd onopgemerkt blijven. Bovendien is het voor patiënten vaak moeilijk te beoordelen of een specifieke inzage terecht was of niet.

"De mogelijkheid tot grootschalige inzage is niet alleen een technisch risico, maar raakt aan het fundament van vertrouwen tussen patiënt en zorgverlener. Wanneer patiënten zich niet meer veilig voelen om hun volledige medische geschiedenis te delen, ondermijnt dit de kwaliteit van zorg."

Hoewel misbruik van medische gegevens wettelijk strafbaar is, blijkt het toezicht en de handhaving complex. De Autoriteit Persoonsgegevens (AP) en de Inspectie Gezondheidszorg en Jeugd (IGJ) hebben beperkte capaciteit om alle meldingen grondig te onderzoeken. Dit creëert een situatie waarin de theoretische bescherming sterker is dan de praktische handhaving, waardoor het systeem kwetsbaar blijft voor misbruik.

Controle en transparantie voor patiënten

In het digitale tijdperk is het essentieel dat patiënten niet alleen passieve onderwerpen zijn van dataverwerking, maar actieve beheerders van hun eigen medische informatie. Mitz en aanvullende tools zoals Volgjezorg bieden patiënten ongekekende mogelijkheden om inzicht te krijgen in wie hun gegevens bekijkt en waarom. Deze transparantie is cruciaal voor het behouden van vertrouwen in het zorgsysteem en voor het waarborgen van privacy.

Inzage in logging via Volgjezorg	Toestemming beheren in Mitz	Automatische notificaties
Patiënten kunnen precies zien welke zorgverleners hun dossier hebben geraadpleegd, op welke datum en op welk tijdstip	Via de Mitz-portal kunnen patiënten hun toestemming geven, wijzigen of intrekken voor specifieke zorgverleners of instellingen	Patiënten kunnen meldingen ontvangen wanneer iemand hun medische gegevens opvraagt, wat direct bewustzijn creëert

Praktische stappen voor patiënten om controle te behouden

	
Informeer jezelf Begrijp hoe Mitz werkt en wat je rechten zijn	Stel je voorkeuren in Configureer je toestemmingen bewust en weloverwogen
	
Controleer regelmatig Check je logging periodiek via Volgjezorg	Meld verdachte inzage Rapporteer ongeautoriseerde toegang onmiddellijk

Het is van cruciaal belang dat patiënten goed geïnformeerd worden over de werking van Mitz en hun rechten. Veel patiënten geven toestemming zonder volledig te begrijpen wat dit betekent, of zijn zich niet bewust van de mogelijkheid om deze toestemming later in te trekken of te beperken. Zorgverleners hebben daarom een belangrijke verantwoordelijkheid om patiënten actief voor te lichten en ervoor te zorgen dat toestemming op basis van volledige informatie wordt gegeven.

**Belangrijk om te weten:** Zorgverleners zijn wettelijk verplicht om logging bij te houden van alle inzage in medische dossiers. Deze logs moeten minimaal twee jaar bewaard blijven en op verzoek aan de patiënt worden verstrekt. Als je vermoedt dat iemand ongeautoriseerd je dossier heeft bekeken, heb je het recht om een kopie van de complete logging op te vragen en een klacht in te dienen.

Transparantie alleen is echter niet voldoende. Patiënten moeten ook de middelen en kennis hebben om effectief gebruik te maken van de controle-instrumenten. Dit vereist investeringen in gebruiksvriendelijke interfaces, heldere communicatie en ondersteuning voor patiënten die minder digitaal vaardig zijn. Alleen dan kan de belofte van patiëntenregie in het digitale tijdperk werkelijk worden waargemaakt.

Conclusie: balans tussen snelle zorg en privacybescherming

Mitz en het Landelijk Schakelpunt vertegenwoordigen een fundamentele verschuiving in hoe medische gegevens worden gedeeld in Nederland. De voordelen zijn onmiskenbaar: snellere toegang tot cruciale informatie, betere coördinatie tussen zorgverleners, minder medische fouten door incomplete informatie, en een efficiëntere zorgverlening. In noodsituaties kan het systeem levens redden door artsen onmiddellijk toegang te geven tot vitale medische geschiedenis.



✓ Voordelen voor de zorg

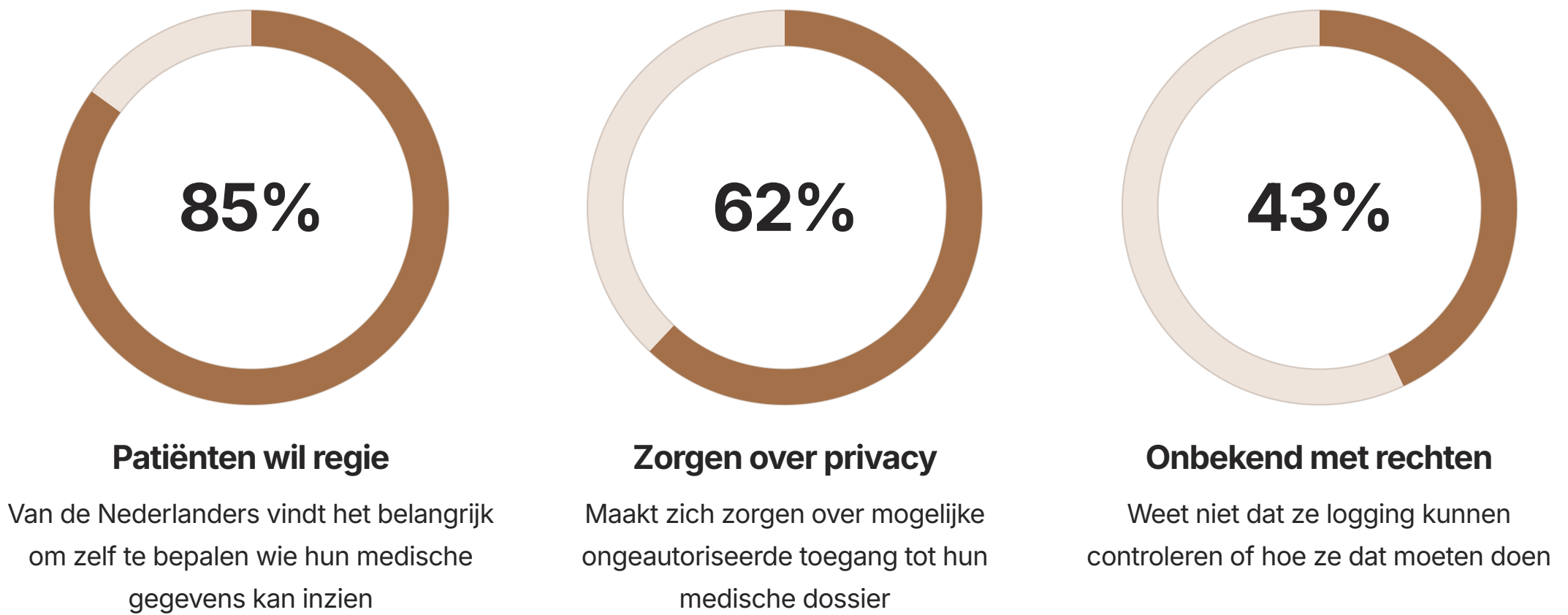
- Snellere en veiligere behandeling door directe toegang tot medische geschiedenis
- Betere continuïteit van zorg bij verwijzingen en overplaatsingen
- Vermindering van onnodige dubbele onderzoeken en tests
- Betere samenwerking tussen verschillende zorgverleners

⚠ Risico's voor privacy

- Mogelijkheid van grootschalige, heimelijke inzage in vertrouwelijke dossiers
- Onduidelijkheid over wie precies toegang heeft en wanneer
- Risico op misbruik door nieuwsgierigheid of commerciële motieven
- Beperkte capaciteit voor toezicht en handhaving van privacy-regels

De weg vooruit: vereisten voor een veilig systeem

Om de belofte van Mitz waar te maken zonder de privacy van patiënten te compromitteren, zijn strikte waarborgen noodzakelijk. Transparantie moet de norm worden, niet de uitzondering. Dit betekent dat patiënten proactief moeten worden geïnformeerd over wie hun gegevens bekijkt, en dat de drempel om logging te controleren zo laag mogelijk moet zijn. Technische maatregelen zoals realtime notificaties en geautomatiseerde anomalie-detectie kunnen helpen om verdachte toegangspatronen vroegtijdig te signaleren.



Uiteindelijk gaat het om vertrouwen. Het vertrouwen van patiënten in het zorgsysteem staat of valt met de zekerheid dat hun meest persoonlijke informatie veilig is en alleen wordt gebruikt voor legitieme zorgdoeleinden. Dit vereist niet alleen technische en juridische waarborgen, maar ook een cultuurverandering binnen de zorg waarbij privacy en patiëntenrechten net zo serieus worden genomen als medische veiligheid.

"In het nieuwe digitale tijdperk van gezondheidszorg moet de regie bij de patiënt liggen. Technologie mag nooit een excuus zijn om fundamentele rechten op privacy en zelfbeschikking te ondergraven."

De invoering van Mitz markeert het begin van een nieuw hoofdstuk in de Nederlandse gezondheidszorg. Of dit hoofdstuk wordt geschreven als een succesverhaal van innovatie en betere zorg, of als een waarschuwend verhaal over privacy-schending en verlies van vertrouwen, hangt af van de keuzes die we nu maken. Strikte naleving van wetgeving, robuuste toezichtmechanismen, transparante communicatie en actieve betrokkenheid van patiënten zijn essentieel om ervoor te zorgen dat de belofte van digitale gezondheidszorg wordt waargemaakt zonder de fundamentele waarden van privacy en autonomie op te offeren.



**EFF: Online Leeftijdsverificatie
Betekent Einde van Anonimiteit
op Internet**

De Europese richtlijnen voor online leeftijdsverificatie markeren een keerpunt in de geschiedenis van het internet. Wat begon als een digitale vrijplaats waar anonimiteit bescherming bood aan kwetsbare groepen, staat nu onder druk door nieuwe veiligheidsmaatregelen. Deze ontwikkeling roept fundamentele vragen op over de balans tussen kinderbescherming en digitale vrijheidsrechten.

Wat is Anonimiteit en Waarom is het Belangrijk?

De Oorsprong van Anonimiteit

Anonimiteit betekent dat de identiteit van een persoon onbekend blijft of niet bekend wordt gemaakt. Het woord komt van het Griekse 'anonymos', wat letterlijk 'zonder naam' betekent. Deze fundamentele vrijheid heeft door de geschiedenis heen een cruciale rol gespeeld in het beschermen van vrije meningsuiting.



Vrije Meningsuiting

Anonimiteit biedt ruimte om meningen te delen zonder angst voor repercussies of sociale druk.



Bescherming Privacy

Het waarborgt dat persoonlijke informatie en identiteit beschermd blijven tegen ongewenste inzichten.



Kwetsbare Groepen

Essentieel voor de veiligheid van minderheden, klokkenluiders en mensen in gevaar.

Internet begon als een anonieme vrijplaats, cruciaal voor democratische idealen en het beschermen van kwetsbare groepen, zoals seksuele minderheden en politieke dissidenten. De opkomst van online leeftijdsverificatie bedreigt deze anonimiteit door gebruikers te dwingen zich te identificeren, wat fundamentele vrijheden kan aantasten en de digitale veilige haven voor velen kan ondermijnen.

Europese en Nederlandse Beleidsontwikkelingen rond Leeftijdsverificatie

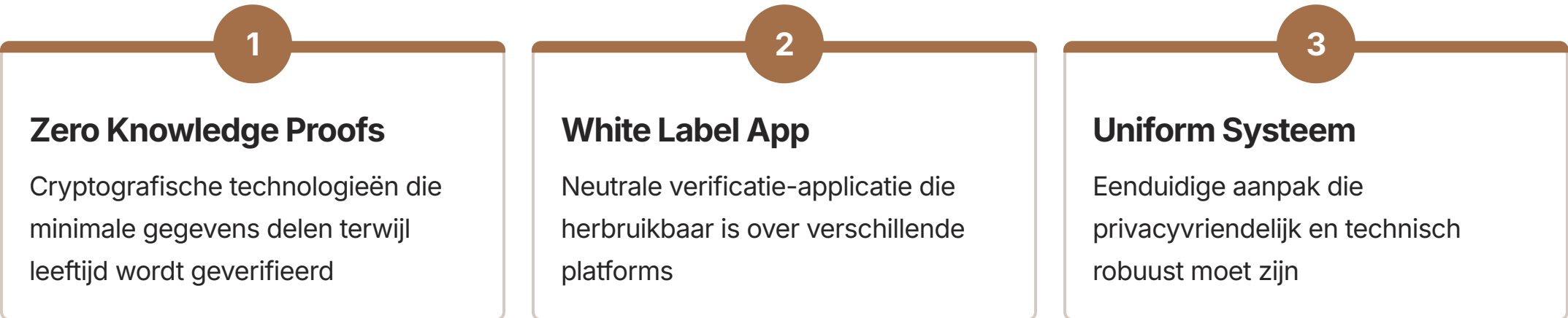
Het demissionaire Nederlandse kabinet steunt Europese richtlijnen die online leeftijdsverificatie verplichten om kinderen beter te beschermen tegen schadelijke content. Deze beleidsshift markeert een significante verandering in hoe overheden omgaan met online veiligheid en privacy.



De Uitdaging van Minister Beljaarts

Minister Beljaarts erkent openlijk dat er nog geen veilige, privacybeschermende methode bestaat voor leeftijdsverificatie. Dit is een belangrijk signaal dat de overheid zich bewust is van de complexiteit van het vraagstuk.

Grondrechten onder druk: Leeftijdsverificatie kan grote impact hebben op fundamentele rechten zoals privacy, vrijheid van meningsuiting en digitale toegankelijkheid.



Technische Uitdagingen en Praktische Voorbeelden

Online platforms zoals het Nederlandse F2F (friends2follow) implementeren leeftijdsverificatie via selfie-AI en ID-controle, wat gebruikers dwingt hun anonimiteit op te geven. Deze praktische implementaties laten de spanning zien tussen veiligheid en privacy in de dagelijkse digitale praktijk.



Selfie Upload

AI-gestuurde gezichtsherkenning analyseert gezichtskenmerken



ID-Verificatie

Document wordt gescand en gecontroleerd op authenticiteit



Leeftijd Bevestigd

Toegang verleend na succesvolle verificatie

Technische Complexiteit

- Meerdere verificatiestappen
- AI-analyse van documenten
- Biometrische vergelijking
- Backend-verificatiesystemen

Gebruikerservaring

- Extra klikken en wachttijd
- Privacy-zorgen bij gebruikers
- Drempel voor toegang
- Verlies van spontaniteit

Maatschappelijke Impact

- Uitsluiting zonder technologie
- Datamisbruik risico's
- Verlies van vertrouwen
- Digitale kloof vergroten

Digitale Uitsluiting

Mensen zonder toegang tot benodigde technologie of digitale vaardigheden worden buitengesloten van online diensten.

Datamisbruik Risico

Verzamelde persoonlijke data kan gelekt, gehackt of misbruikt worden door kwaadwillenden.

Vertrouwensverlies

Gebruikers verliezen vertrouwen in digitale diensten door verplichte identificatie en dataverzameling.

"Softwarebedrijven zoals Klippa bieden geavanceerde, AI-gestuurde leeftijdsverificatie-oplossingen die documenten scannen en authenticiteit controleren, maar dit betekent ook dat gebruikers persoonlijke data moeten delen."

Conclusie: De Botsing tussen Bescherming en Vrijheid

Online leeftijdsverificatie is een zwaar middel dat kinderen beter moet beschermen, maar het betekent ook het einde van anonieme toegang tot veel online diensten. Deze fundamentele verschuiving in het digitale landschap roept kritische vragen op over de toekomst van internet als vrije ruimte.

Privacy

Hoe beschermen we persoonlijke gegevens terwijl we leeftijd verifiëren? De spanning tussen identificatie en anonimiteit lijkt onoverkomelijk.

Vrijheid van Meningsuiting

Kan vrije meningsuiting overleven als alle gebruikers zich moeten identificeren? Anonimiteit was altijd een hoeksteen van deze vrijheid.

Digitale Inclusie

Wie wordt uitgesloten door deze nieuwe eisen? Technologische barrières kunnen tot maatschappelijke ongelijkheid leiden.

De Weg Vooruit

De uitdaging is een balans te vinden tussen effectieve bescherming van minderjarigen en het waarborgen van grondrechten. Technologische innovatie alleen is niet genoeg – we hebben ook maatschappelijke acceptatie en zorgvuldig beleid nodig.

De toekomst vraagt om transparante, privacybewuste oplossingen en een brede maatschappelijke discussie over de waarde van anonimiteit in het digitale tijdperk. Alleen door open dialoog kunnen we een evenwicht vinden dat zowel kinderen beschermt als fundamentele vrijheden waarborgt.



01

Technologische Innovatie

Ontwikkel privacybeschermende verificatiemethoden

02

Maatschappelijk Debat

Voer brede discussie over anonimiteit en veiligheid

03

Transparant Beleid

Creëer duidelijke regelgeving met waarborgen

04

Balans Vinden

Bescherm kinderen én grondrechten tegelijkertijd

 **Belangrijk om te onthouden**

De discussie over online leeftijdsverificatie gaat niet alleen over technologie, maar over de fundamentele waarden van onze samenleving. Het is een vraagstuk dat ons allemaal aangaat en waarbij we gezamenlijk moeten bepalen welke digitale toekomst we willen.



In een wereld waarin onze digitale identiteit steeds belangrijker wordt, ontstaan er nieuwe bedreigingen die ons dagelijks leven kunnen ontwrichten. SIM-swapping is een van de meest verraderlijke vormen van cybercriminaliteit, waarbij criminelen letterlijk jouw telefoonnummer kapen om toegang te krijgen tot je meest waardevolle accounts.

De opkomst van eSIM-technologie maakt deze dreiging nog urgenter, omdat de digitale aard ervan zowel kansen als risico's met zich meebrengt.

Wat is SIM-swapping en hoe werkt het?

SIM-swapping is een geavanceerde vorm van identiteitsfraude waarbij criminelen zich meester maken van jouw telefoonnummer door het over te zetten naar een SIM-kaart of eSIM die volledig onder hun controle staat. Deze aanvalsmethode is bijzonder gevaarlijk omdat het telefoonnummer in onze moderne digitale infrastructuur vaak fungeert als het sleutelstuk van onze online identiteit.



Zodra een crimineel controle heeft over jouw nummer, kunnen ze SMS-codes voor tweefactorauthenticatie (2FA) onderscheppen. Dit geeft hen direct toegang tot bankrekeningen, e-mailaccounts, cryptocurrency wallets, sociale media profielen en vrijwel elk ander account dat gebruikmaakt van SMS-verificatie. De gevolgen kunnen verwoestend zijn: van lege bankrekeningen tot volledig gekaapt sociale media-accounts.



Gegevensverzameling

Criminelen verzamelen eerst persoonlijke informatie via datalekken, phishing of social media



Provider benaderen

Met gestolen gegevens overtuigen ze de klantenservice om een nummeroverdracht uit te voeren



Nummer overzetten

Het telefoonnummer wordt overgedragen naar de SIM of eSIM van de crimineel



Accounts hacken

Met controle over het nummer onderscheppen ze 2FA-codes en krijgen toegang tot accounts

Het verraderlijke van deze aanvalsmethode is dat het proces volledig via de provider verloopt, niet via de fysieke kaart zelf. Dit betekent dat zowel traditionele SIM-kaarten als moderne eSIMs kwetsbaar zijn voor dit type fraude. De zwakste schakel is vaak de menselijke factor bij de klantenservice van providers, die door geraffineerde social engineering technieken misleid kunnen worden.

Wat is een eSIM en waarom verandert het de situatie?

Een eSIM (embedded SIM) vertegenwoordigt de volgende evolutie in mobiele connectiviteit. Het is een ingebouwde, digitale simkaart die direct in de hardware van je smartphone, tablet of smartwatch geïntegreerd is en via software geprogrammeerd kan worden. In tegenstelling tot traditionele SIM-kaarten die je fysiek moet verwisselen, werkt een eSIM volledig digitaal.



Voordelen van eSIM

- Makkelijker wisselen van provider zonder fysieke kaart
- Geen fysieke kaart die verloren of gestolen kan worden
- Minder milieubelasting door wegvallen plastic productie
- Mogelijkheid meerdere profielen op één toestel
- Ideaal voor internationale reizigers



Beveiligingsrisico's

- Over-The-Air provisioning maakt remote overzetten mogelijk
- Geen fysieke toegang nodig voor nummeroverdracht
- Criminelen kunnen proces volledig digitaal uitvoeren
- Beveiliging hangt volledig af van provider procedures
- Gebruikers merken aanval vaak pas te laat op

De digitale aard van eSIM brengt een paradox met zich mee: hoewel het de beveiliging in sommige opzichten verbetert (een fysieke dief kan je SIM niet meer stelen), maakt het tegelijkertijd SIM-swapping eenvoudiger voor cybercriminelen. Via Over-The-Air (OTA) provisioning kunnen nummers op afstand worden overgedragen zonder dat er fysieke toegang tot het toestel nodig is. Dit verlaagt de drempel voor aanvallers aanzienlijk.

Ondanks de geavanceerde technologie blijft de beveiliging grotendeels afhankelijk van de procedures en systemen van de mobiele provider. Als een provider zwakke verificatieprocessen hanteert of medewerkers onvoldoende getraind zijn om social engineering te herkennen, blijft de kwetsbaarheid voor SIM-swapping bestaan, ongeacht of je een fysieke SIM of een eSIM gebruikt.

De groeiende dreiging: recente trends en impact

SIM-swap aanvallen zijn geëvolueerd van een relatief onbekend fenomeen naar een van de snelst groeiende vormen van cybercriminaliteit wereldwijd. De cijfers zijn alarmerend en tonen een exponentiële groei die zowel individuele gebruikers als bedrijven in gevaar brengt.

De FBI rapporteerde in 2023 dat SIM-fraude Amerikaanse slachtoffers bijna \$49 miljoen kostte, maar dit cijfer vertegenwoordigt slechts een fractie van het werkelijke probleem omdat veel aanvallen ongemeld blijven. Nog verontrustender is de ontwikkeling in 2024, waarbij het aantal SIM-swap aanvallen met bijna 400% steeg ten opzichte van het voorgaande jaar.



Beroemde slachtoffers zoals Twitter CEO Jack Dorsey, wiens account werd gehackt via SIM-swapping, illustreren dat niemand immuun is voor deze dreiging. Ook gewone gebruikers en bedrijven van elke omvang worden dagelijks getroffen, met verwoestende financiële en emotionele gevolgen.

\$49M

Schade in VS (2023)

Gerapporteerde financiële verliezen door SIM-fraude volgens FBI

400%

Toename aanvallen

Stijging van SIM-swap incidenten in 2024 vergeleken met 2023

2FA

Kwetsbare methode

SMS-gebaseerde tweefactorauthenticatie is primair doelwit

❏ **Waarom is SMS-gebaseerde 2FA zo kwetsbaar?** Hoewel tweefactorauthenticatie in principe de beveiliging verhoogt, is SMS-gebaseerde 2FA fundamenteel kwetsbaar voor SIM-swapping. Zodra een crimineel controle heeft over je telefoonnummer, kunnen ze alle beveiligingscodes onderscheppen die naar dat nummer gestuurd worden. Het geeft hen effectief dezelfde toegang als de legitieme eigenaar, waardoor de "tweede factor" waardeloos wordt. Dit maakt SMS-2FA een van de zwakste schakels in moderne cybersecurity.

De impact reikt verder dan alleen financieel verlies. Slachtoffers ervaren vaak ernstige emotionele stress, verlies van vertrouwen in digitale diensten, en kunnen maanden bezig zijn met het herstellen van hun digitale identiteit. Sommige verliezen zijn onherstelbaar, zoals cryptocurrency die naar onbekende wallets is overgemaakt of privéfoto's die publiekelijk zijn gedeeld.

Hoe herken je een SIM-swap aanval?

Vroege detectie van een SIM-swap aanval kan het verschil maken tussen beperkte schade en een complete ramp. Helaas realiseren veel slachtoffers zich pas dat ze aangevallen zijn wanneer de schade al is aangericht. Daarom is het cruciaal om de waarschuwingssignalen te kennen en onmiddellijk te handelen wanneer je deze opmerkt.



Plotseling verlies van mobiele verbinding

Je telefoon verliest onverwacht alle mobiele signalen en kan geen gesprekken ontvangen of plaatsen, terwijl anderen om je heen wel normaal bereik hebben. Dit is vaak het eerste teken dat je nummer is overgedragen naar een andere SIM.



Onverwachte meldingen van je provider

Je ontvangt berichten of e-mails over de activatie van een nieuwe SIM-kaart of eSIM, terwijl je zelf geen wijzigingen hebt aangevraagd. Dit kan wijzen op een poging om je nummer over te zetten.



Problemen met inloggen op accounts

Je kunt plotseling niet meer inloggen op bankaccounts, e-mail of sociale media. Dit kan betekenen dat een aanvaller je wachtwoorden al heeft veranderd nadat ze via SIM-swap toegang hebben gekregen.



Ongebruikelijke activiteiten

Je ontdekt vreemde transacties op je bankrekening, onbekende berichten die vanaf je accounts zijn verstuurd, of vrienden die rare berichten van je hebben ontvangen die je niet hebt verzonden.



Geen ontvangst van 2FA-codes

Je probeert in te loggen op een account en vraagt een SMS-verificatiecode aan, maar deze komt nooit aan. Dit kan erop wijzen dat je nummer wordt onderschept en de codes naar de crimineel gaan.

"Het moment dat ik merkte dat mijn telefoon geen bereik meer had, dacht ik eerst aan een storing. Tien minuten later zag ik dat €15.000 van mijn rekening was verdwenen. Dat was het moment dat ik besepte wat er aan de hand was."

— Anoniem SIM-swap slachtoffer

Als je een of meerdere van deze signalen opmerkt, handel dan onmiddellijk. Neem via een alternatieve methode (bijvoorbeeld wifi of een andere telefoon) contact op met je provider en financiële instellingen. Hoe sneller je reageert, hoe kleiner de kans op ernstige schade. Tijd is essentieel bij een SIM-swap aanval.

Bescherming tegen SIM-swapping: praktische tips

Hoewel SIM-swapping een serieuze dreiging vormt, zijn er effectieve maatregelen die je kunt nemen om jezelf te beschermen. Een gelaagde beveiligingsaanpak die zowel technische als sociale aspecten omvat, biedt de beste verdediging tegen deze vorm van cybercriminaliteit.



Activeer SIM-bescherming

Vraag je provider om SIM-bescherming of een extra PIN-code in te stellen. Hierdoor kunnen wijzigingen aan je SIM alleen plaatsvinden met jouw expliciete toestemming en verificatie. Sommige providers bieden ook biometrische verificatie aan.



Gebruik app-gebaseerde 2FA

Schakel over van SMS-gebaseerde tweefactorauthenticatie naar authenticator-apps zoals Google Authenticator, Microsoft Authenticator of Authy. Deze genereren codes lokaal op je toestel en zijn niet afhankelijk van je telefoonnummer.



Sterke, unieke wachtwoorden

Gebruik voor elk account een uniek, complex wachtwoord van minimaal 12 karakters. Gebruik een password manager om deze veilig op te slaan. Hergebruik nooit wachtwoorden tussen verschillende accounts.



Beperk online info

Deel zo min mogelijk persoonlijke gegevens op sociale media. Informatie zoals geboortedatum, telefoonnummer en adres kunnen criminelen gebruiken om providers te misleiden.



Herken phishing

Wees alert op verdachte e-mails, berichten of telefoontjes die om persoonlijke informatie vragen. Legitieme bedrijven vragen nooit via deze kanalen om wachtwoorden of verificatiecodes.



Monitor je accounts

Controleer regelmatig je bankrekeningen en belangrijke accounts op ongebruikelijke activiteit. Schakel notificaties in voor transacties en inlogpogingen.

Actieplan bij vermoeden van aanval

1. **Contacteer onmiddellijk je provider** via een alternatieve verbinding en laat je SIM blokkeren
2. **Waarschuw je bank** en andere financiële instellingen om accounts tijdelijk te bevriezen
3. **Verander wachtwoorden** van alle belangrijke accounts vanaf een veilig toestel
4. **Schakel 2FA uit en opnieuw in** met een nieuwe methode (bij voorkeur authenticator-app)
5. **Doe aangifte** bij de politie en rapporteer het incident bij relevante instanties
6. **Informeer contacten** dat je account mogelijk gecompromitteerd is



**Extra tip voor cryptocurrency-gebruikers:** Als je cryptocurrency bezit, zijn de risico's van SIM-swapping nog groter. Overweeg het gebruik van hardware wallets die je crypto offline bewaren en niet afhankelijk zijn van telefoonverificatie. Schakel ook alle SMS-gebaseerde recovery opties uit voor je crypto-accounts en gebruik alleen authenticator-apps of hardware security keys.

Conclusie: bewustzijn en actie zijn cruciaal



De digitale revolutie heeft ons leven verrijkt met ongekende mogelijkheden, maar brengt ook nieuwe kwetsbaarheden met zich mee. De opkomst van eSIM-technologie illustreert deze paradox perfect: enerzijds biedt het gemak en flexibiliteit, anderzijds creëert het nieuwe aangrijpingspunten voor cybercriminelen.

SIM-swapping is geen abstract gevaar dat alleen anderen overkomt. Het is een groeiend probleem dat iedereen kan treffen, van doorsnee gebruikers tot CEO's van technologiebedrijven. De gevolgen kunnen verstrekkend zijn: van financieel verlies tot identiteitsdiefstal, van gekaapt sociale media tot verloren cryptocurrency. De emotionele impact van zo'n aanval kan maanden of zelfs jaren aanhouden.

Proactieve beveiliging

Wacht niet tot je slachtoffer wordt. Implementeer nu de beschermingsmaatregelen: activeer SIM-bescherming, schakel over op app-gebaseerde 2FA, en gebruik sterke, unieke wachtwoorden voor al je accounts.

Waakzaamheid

Blijf alert op waarschuwingssignalen en ongebruikelijke activiteiten. Vroege detectie kan het verschil maken tussen beperkte overlast en een complete ramp. Vertrouw op je intuïtie bij verdachte situaties.

Blijf geïnformeerd

Cyberdreigingen evolueren constant. Blijf op de hoogte van nieuwe aanvalsmethoden en beveiligingstechnieken. Volg betrouwbare cybersecurity bronnen en deel kennis met familie en vrienden.

Samenwerking

Werk samen met je provider, bank en andere dienstverleners om je digitale identiteit te beschermen. Vraag naar hun beveiligingsopties en eisen ze dat ze sterke verificatieprocedures hanteren.

Jouw digitale identiteit is waardevol — bescherm het alsof je leven ervan afhangt

In onze hyperverbonden wereld is je telefoonnummer meer dan alleen een communicatiemiddel: het is de sleutel tot je digitale leven. Behandel het met de zorg die het verdient.

De strijd tegen cybercriminaliteit is een gedeelde verantwoordelijkheid. Providers moeten hun verificatieprocessen versterken, overheden moeten wetgeving aanscherpen, en wijzelf moeten bewust en proactief omgaan met onze digitale beveiliging. Door deze drieslag kunnen we de risico's van SIM-swapping minimaliseren en veilig genieten van de voordelen die moderne technologie ons biedt.

De vraag is niet óf je maatregelen moet nemen, maar wanneer. En het antwoord is: nu. Elke dag dat je wacht, ben je kwetsbaar. Investeer vandaag nog in je digitale veiligheid — je toekomstige zelf zal je dankbaar zijn.



**Europol wil end-to-end encryptie
na gerechtelijk bevel kunnen
doorbreken**

In het digitale tijdperk staat Europa voor een complexe uitdaging: hoe beschermen we de privacy van burgers terwijl we tegelijkertijd effectief optreden tegen georganiseerde misdaad? Europol, de Europese politiedienst, pleit voor de mogelijkheid om versleutelde communicatie te doorbreken wanneer een rechter dit toestaat. Deze ontwikkeling markeert een keerpunt in de discussie over digitale veiligheid en rechtshandhaving.

Dit document verkent de spanning tussen encryptie en opsporing, analyseert recente doorbraken zoals EncroChat en Sky ECC, en bespreekt de juridische en ethische vraagstukken die hiermee gepaard gaan. We onderzoeken hoe Europa probeert een balans te vinden tussen fundamentele rechten en effectieve criminaliteitsbestrijding.

Het encryptiedilemma: veiligheid versus privacy



Waarom encryptie essentieel is

Encryptie vormt de ruggengraat van onze digitale samenleving. Het beschermt fundamentele rechten zoals privacy en vrije meningsuiting, beveilgt financiële transacties en zakelijke communicatie, en waarborgt de veiligheid van burgers en bedrijven in een steeds meer gedigitaliseerde wereld.

Zonder sterke encryptie zouden bankgegevens, medische dossiers en persoonlijke gesprekken kwetsbaar zijn voor hackers, criminelen en ongeautoriseerde surveillance. Voor journalisten, activisten en klokkenluiders is encryptie vaak levensnoodzakelijk.

De uitdaging voor rechtshandhaving

Tegelijkertijd bemoeilijkt sterke end-to-end encryptie het werk van opsporingsdiensten aanzienlijk. Criminele organisaties gebruiken versleutelde communicatieplatforms om drugshandel, mensenhandel en geweldsmisdrijven te coördineren, waarbij zij buiten het bereik van traditionele opsporingsmethoden blijven.

De Europese Raad erkende dit dilemma in december 2020 met een resolutie die benadrukt dat encryptie essentieel blijft, maar dat rechtshandavingsinstanties hun wettelijke bevoegdheden moeten behouden om in uitzonderlijke gevallen encryptie te kunnen doorbreken.

- ❏ **Nederlandse positie:** De minister van Justitie ondersteunt deze balans actief en laat onderzoek doen naar de specifieke rol van encryptie in moderne opsporing, met als doel effectieve maar rechtmatige methoden te ontwikkelen.

Europol en Eurojust: succesvolle hacks en juridische uitdagingen



2020: De EncroChat-doorbraak

Een gezamenlijke Frans-Nederlandse hackoperatie kraakte EncroChat, een cryptotelefoonnetwerk populair in de onderwereld. Circa 80 miljoen berichten van 60.000 gebruikers wereldwijd werden onderschept. Nederlandse politie speelde een cruciale rol door software in te zetten om live mee te lezen.

Internationale spanning

Een vertrouwenscrisis ontstond met Britse autoriteiten over de openbaarmaking van technische details van de hack. Dit kan vergaande gevolgen hebben voor de acceptatie van bewijsmateriaal in lopende strafzaken.

1

2

Juridische controverse

Nederlandse rechters weigeren de rechtmatigheid van de hack te toetsen, omdat Franse rechters dit al deden. Advocaten betwisten dit vanwege de nauwe Nederlandse betrokkenheid bij de operatie.

3

"De EncroChat-operatie toonde aan dat geen enkel cryptosysteem volledig onkraakbaar is wanneer internationale opsporingsdiensten samenwerken en innovatieve technieken inzetten."

Operationele doorbraken: Sky ECC en Anom

Sky ECC (2021)

Na het vallen van EncroChat migreerden criminelen massaal naar Sky ECC, beschouwd als een onkraakbaar alternatief. Europol en Eurojust slaagden er opnieuw in de encryptie te doorbreken.

- Honderden miljoenen berichten ontsleuteld
- Honderden strafzaken wereldwijd
- Levensbedreigende situaties voorkomen

Operatie Trojan Shield (2021)

De FBI lanceerde samen met internationale partners een geniale undercoveroperatie met de Anom-app, een zogenaamd veilige communicatie-app die in werkelijkheid door politiediensten werd gecontroleerd.

- Meer dan 27 miljoen berichten onderschept
- 800 verdachten wereldwijd gearresteerd
- 49 arrestaties in Nederland alleen
- Grote drugslocaties ontmanteld
- Meerdere huurmoorden voorkomen

80M

Berichten onderschept

Bij EncroChat-operatie

800

Arrestaties wereldwijd

Dankzij Anom-operatie

60K

Gebruikers wereldwijd

Van cryptotelefoons

Deze operaties illustreren hoe innovatieve opsporingsmethoden en internationale samenwerking criminele netwerken kunnen ontwrichten. Tegelijkertijd roepen ze fundamentele vragen op over de grenzen van rechtmatige opsporing en de bescherming van burgerrechten in het digitale tijdperk.

Juridische en ethische dilemma's rond het doorbreken van encryptie

Privacybezwaren

Opsporingsmethoden zoals hacken en het live meekijken met communicatie roepen fundamentele vragen op over privacy, de onschuldpresumptie en de rechtmatigheid van massale dataverzameling. Advocaten betogen dat het verzamelen van data zonder concrete verdenking neerkomt op een digitaal sleepnet.



Schending van grondrechten?

Het onderscheppen van communicatie van tienduizenden gebruikers, waarvan velen mogelijk geen misdrijven hebben gepleegd, roept vragen op over proportionaliteit en subsidiariteit. Is dit een gerechtvaardigde inbreuk op artikel 8 EVRM (recht op privacy)?

Rechtvaardiging door resultaten

Nederlandse rechtbanken oordelen dat het voorkomen van ernstige misdrijven zoals moord, grootschalige drugshandel en mensenhandel deze methoden rechtvaardigt. Het verkrijgen van cruciaal bewijs weegt zwaarder dan de privacy-inbreuk.

Internationale complexiteit

Verschillen in nationale wetgeving compliceren internationale samenwerking. Wat in Frankrijk rechtmatig is, kan in Nederland of het VK tot juridische problemen leiden. Er is behoefte aan geharmoniseerde juridische kaders.

Transparantie en controle

De geheimhouding rond hackoperaties bemoeilijkt effectieve rechterlijke controle. Verdediging en rechters hebben vaak onvoldoende inzicht in de technische details om de rechtmatigheid grondig te beoordelen.

"De vraag is niet óf we encryptie kunnen doorbreken, maar wanneer en onder welke strikte voorwaarden dit gerechtvaardigd is in een democratische rechtsstaat."

Conclusie: de toekomst van encryptie en opsporing in Europa

Europa bevindt zich op een kruispunt waar technologische innovatie, georganiseerde misdaad en fundamentele rechten samenkomen. Europol en Eurojust benadrukken dat internationale samenwerking en continue innovatie essentieel zijn om criminele organisaties die versleutelde communicatie misbruiken effectief te bestrijden.



01

Bewezen effectiviteit

Doorbraken bij EncroChat, Sky ECC en Anom tonen aan dat technische en juridische uitdagingen overwonnen kunnen worden, met concrete resultaten: honderden arrestaties en het voorkomen van ernstige misdrijven.

02

Juridische kaders ontwikkelen

Het doorbreken van end-to-end encryptie na gerechtelijk bevel wordt gezien als noodzakelijk, maar vereist heldere wettelijke kaders die fundamentele rechten beschermen en rechterlijke controle waarborgen.

03

Blijvende balans

De spanning tussen privacybescherming en veiligheid blijft dynamisch. Technologie evolueert, criminele tactieken veranderen, en juridische normen ontwikkelen zich. Continue dialoog tussen wetgevers, rechters, opsporingsdiensten en privacyexperts is cruciaal.

📌 **Vooruitblik:** De komende jaren zullen bepalend zijn voor hoe Europa de balans vindt tussen digitale privacy en effectieve criminaliteitsbestrijding. De uitdaging is een model te creëren dat zowel rechten beschermt als veiligheid waarborgt – een blauwdruk die mogelijk wereldwijd navolging kan vinden.



**Fors meer
wachtwoorddiefstal,
spyware en backdoors in
2025**

In 2025 detecteerden de beveiligingssystemen van Kaspersky dagelijks gemiddeld 500.000 kwaadaardige bestanden, een stijging van 7% ten opzichte van het voorgaande jaar. Met name de detectie van wachtwoordendieven steeg met 59%, spyware met 51% en backdoors met 6% in vergelijking met 2024.

Cyberdreigingen in 2025: Een explosieve toename

De cybersecurity-landschap van 2025 toont een ongeken­de escalatie van digitale bedreigingen. Kaspersky's geavanceerde detectiesystemen registreerden een alarmerende toename in kwaadaardige activiteiten, waarbij dagelijks een half miljoen gevaarlijke bestanden werden geïdentificeerd.

Deze stijging van 7% ten opzichte van 2024 is meer dan een statistiek—het vertegenwoordigt een fundamentele verschuiving in de aard en schaal van cyberaanvallen. De meest verontrustende trend is de explosieve groei in gerichte aanvallen op persoonlijke en zakelijke gegevens.

500K

Dagelijkse detecties

Kwaadaardige bestanden per dag

7%

Totale stijging

Ten opzichte van 2024

Wachtwoordendieven

+59% stijging

Criminelen richten zich massaal op inloggegevens

Spyware

+51% stijging

Verborgene surveillance neemt drastisch toe

Backdoors

+6% stijging

Blijvende toegang tot systemen

Deze cijfers weerspiegelen de groeiende complexiteit en agressiviteit van cyberaanvallen wereldwijd. Cybercriminelen worden steeds professioneler en hun aanvalsmethoden steeds geavanceerder.

Wachtwoorddiefstal: De stille crisis

Wachtwoorddiefstal is uitgegroeid tot een van de meest kritieke cybersecurity-uitdagingen van 2025. De explosieve stijging van 59% in wachtwoordendieven toont aan dat cybercriminelen hun focus hebben verlegd naar de zwakste schakel in digitale beveiliging: menselijke authenticatie.



Zwakke wachtwoorden

Gebruikers kiezen voorspelbare combinaties



Hergebruik

Hetzelfde wachtwoord voor meerdere accounts



Lek

Één compromis geeft toegang tot alles



Fraude

Identiteitsdiefstal en financiële schade

De gevolgen zijn verwoestend

- Accountovernames leiden tot identiteitsfraude en reputatieschade
- Financiële verliezen door ongeautoriseerde transacties
- Grootschalige datalekken bij organisaties
- Verlies van vertrouwelijke bedrijfsinformatie

Bescherming is beschikbaar

Multifactor-authenticatie (MFA) en wachtwoordmanagers zijn cruciaal, maar worden nog onvoldoende toegepast. Slechts een minderheid van gebruikers maakt gebruik van deze essentiële beveiligingslagen.

📌 **2025 Trend:** Het aantal phishing-aanvallen gericht op wachtwoordroof nam sterk toe, mede door AI-gegenereerde, overtuigende nepberichten die bijna niet van echte communicatie te onderscheiden zijn.

Spyware en backdoors: Onzichtbare bedreigingen

Spyware: +51% groei

Onzichtbare surveillancesoftware verzamelt langdurig gevoelige informatie zonder detectie. Deze kwaadaardige programma's leggen toetsaanslagen vast, maken screenshots en stelen persoonlijke gegevens.

Backdoors: +6% groei

Verborgen toegangspoorten bieden hackers blijvende controle over systemen. Deze achterdeurtjes worden vaak geïnstalleerd via gecompromitteerde softwareleveranciers.

Supply chain attacks: De nieuwe realiteit

Een van de meest verontrustende ontwikkelingen van 2025 is de sterke toename van supply chain attacks. Aanvallers infiltreren niet langer direct bij hun doelwit, maar via vertrouwde derde partijen en softwareleveranciers. Deze tactiek maakt het mogelijk om in één klap duizenden organisaties te compromitteren.

01

Infiltratie softwareleverancier

Hackers compromitteren een vertrouwde leverancier

02

Backdoor in update

Kwaadaardige code wordt toegevoegd aan legitieme software-updates

03

Massale distributie

Duizenden klanten installeren automatisch de gecompromitteerde update

04

Stille toegang

Aanvallers verkrijgen onopgemerkt toegang tot systemen wereldwijd

"In 2025 werden meerdere grote bedrijven getroffen door backdoors in populaire software, wat leidde tot grootschalige datalekken. De impact was ongekend: miljoenen gebruikersgegevens werden gecompromitteerd en het herstel kostte organisaties maanden."

Nieuwe tactieken en technologieën van aanvallers

De digitale onderwereld evolueert in razend tempo. Cybercriminelen in 2025 zijn niet langer opportunistische amateurs, maar hoogopgeleide professionals die cutting-edge technologie inzetten om hun doelen te bereiken. De convergentie van kunstmatige intelligentie, machine learning en social engineering heeft geleid tot een nieuwe generatie aanvallen die moeilijker te detecteren en te stoppen zijn.



AI & Machine Learning

Cybercriminelen gebruiken geavanceerde AI om aanvallen te automatiseren, patronen in verdediging te analyseren en kwetsbaarheden sneller te identificeren dan ooit tevoren. Machine learning-algoritmes perfectioneren aanvalstechnieken met elke poging.



Deepfake & Social Engineering

Deepfake-technologieën creëren overtuigende video's en audio-opnames van executives en vertrouwde contacten. Deze worden gebruikt in geavanceerde phishingcampagnes die zelfs ervaren professionals misleiden.



Dubbele afpersing

Ransomware evolueert naar dubbele en driedubbele afpersing: gegevens worden versleuteld, gestolen én bedreigd met publicatie. Aanvallers eisen losgeld van meerdere partijen, inclusief de slachtoffers van het datalek.



Nation-state actors

Door staten gesponsorde hackers en georganiseerde misdaadgroepen intensiveren hun activiteiten, gericht op kritieke infrastructuur, financiële sector en strategische industrieën. Hun middelen en expertise zijn ongeëvenaard.

Geautomatiseerd

AI voert duizenden aanvallen tegelijk uit

Gepersonaliseerd

Berichten zijn maatwerk voor elk slachtoffer

Onstopbaar

24/7 operaties zonder menselijke tussenkomst

Conclusie: Versterk uw digitale verdediging nu

De dramatische stijging van wachtwoorddiefstal, spyware en backdoors in 2025 is een duidelijk waarschuwingssignaal. De cybersecurity-landschap is fundamenteel veranderd, en passieve verdediging is niet langer voldoende. Organisaties en individuen moeten overgaan op een proactieve, gelaagde beveiligingsstrategie.

1 Sterke authenticatie Implementeer complexe, unieke wachtwoorden voor elk account Activeer multifactor-authenticatie (MFA) overal waar mogelijk Gebruik wachtwoordmanagers om credentials veilig te beheren	2 Software hygiene Installeer regelmatig beveiligingsupdates en patches Scan systemen periodiek op kwetsbaarheden Gebruik alleen software van geverifieerde bronnen
3 Bewustwording Train medewerkers in herkenning van phishing en social engineering Creëer een cultuur van security awareness Simuleer regelmatig aanvallen om paraatheid te testen	4 Samenwerking Deel threat intelligence tussen organisaties Werk samen met beveiligingsbedrijven en overheden Meld incidenten en draag bij aan collectieve verdediging

De urgentie is reëel

Met de toenemende sophistication van cyberaanvallen is er geen ruimte meer voor complaisance. Elke dag wachten betekent een groter risico op compromittering. De dreigingen van 2025 vereisen onmiddellijke actie en blijvende waakzaamheid.

Investeren in cybersecurity is geen kostenpost—het is een existentiële noodzaak in de digitale economie. De vraag is niet of u geconfronteerd wordt met een cyberaanval, maar wanneer.



Uw actieplan voor 2025

- Voer een security audit uit binnen 30 dagen
- Implementeer MFA voor alle kritieke systemen
- Start een maandelijks bewustwordingsprogramma
- Ontwikkel een incident response plan
- Test uw backups en herstelprocessen

Alleen met een gelaagde en adaptieve beveiligingsstrategie kunnen we de digitale veiligheid waarborgen in een steeds gevaarlijker wordend landschap.



**Half miljoen malware-bedreigingen
per dag: Cyberdreigingen in 2025**

Cyberdreigingen in 2025: Een Nieuwe Realiteit

Kaspersky zag in 2025 dagelijks vijfhonderdduizend malware-bestanden, zeven procent meer dan in 2024. Vooral password stealers en spyware namen sterk toe. Deze explosieve groei markeert een nieuw tijdperk in het digitale dreigingslandschap, waarin cybercriminelen steeds geavanceerder en georganiseerder te werk gaan.

Explosieve groei van malware in 2025

500.000 nieuwe bedreigingen

Kaspersky registreerde dagelijks een half miljoen nieuwe malware-bestanden, een stijging van 7% ten opzichte van 2024.

Password stealers dominant

Password stealers en spyware namen het sterkst toe, wat wijst op een focus op datadiefstal en spionage.

Malware-as-a-Service

MaaS blijft groeien, waardoor cybercriminelen met weinig technische kennis toch geavanceerde tools kunnen inzetten.

Nieuwe malware-toolkits geschreven in moderne programmeertalen als Rust en Go maken aanvallen veelzijdiger en aanzienlijk moeilijker te detecteren.

Password stealers en spyware: de stille datadieven

IBM X-Force meldde een alarmerende toename van 84% in phishing e-mails die infostealers verspreiden. Spyware wordt strategisch ingezet om langdurig toegang te krijgen tot gevoelige informatie.

Meest getroffen sectoren:

- Gezondheidszorg: Patiëntgegevens en medische dossiers
- Technologie: Intellectueel eigendom en ontwikkelingscode
- Financiën: Bankinformatie en transactiegegevens

Impact op sectoren en kosten

93%

Zorgincidenten

van Amerikaanse zorgorganisaties rapporteerde minstens één cyberincident in 2024, met gemiddelde kosten van \$10,3 miljoen per incident.

47%

Financiële aanvallen

stijging in aanvallen binnen de financiële sector.

50%

Technologie-inbreuken

van derdepartij-inbreuken troffen de technologiesector.

Nieuwe aanvalstechnieken



AI-aanvallen

Cybercriminelen gebruiken AI en automatisering om hun aanvallen te verfijnen.



Phishing dominant

1 op de 4 e-mails bevat malafide inhoud, wat phishing een continue dreiging maakt.



Verdedigingsgaten

25% van incidenten is te wijten aan het falen van patches en identiteitsbescherming.

Conclusie: De noodzaak van proactieve cyberweerbaarheid

De stijging naar een half miljoen malware-bedreigingen per dag onderstreept de urgentie van geavanceerde beveiligingsstrategieën.

Actiestappen:

01

Investeer in educatie

Train medewerkers om bedreigingen te herkennen.

02

Implementeer geavanceerde technologie

Zet moderne beveiligingstools in met AI-ondersteuning.

03

Bevorder samenwerking

Deel dreigingsinformatie met andere organisaties.

04

Blijf continu valideren

Test regelmatig de weerbaarheid van systemen.

Alleen met een geïntegreerde aanpak van preventie, detectie en respons kan de groeiende dreiging effectief worden bestreden.

A person with glasses is sitting at a desk in a dimly lit room, looking at multiple computer monitors. The monitors display code and data. Overlaid on the scene is a complex, glowing digital network of nodes and lines, with a bright central point of convergence, suggesting a cyber attack or data breach. The overall tone is dark and technological.

**Het gevaar van Pharming:
Onzichtbare
cyberaanvallen die je
identiteit stelen**

Een nieuwe generatie cybercriminelen voert stille aanvallen uit die zelfs de meest oplettende internetgebruikers kunnen misleiden. Pharming vertegenwoordigt een evolutie in digitale fraude waarbij technische manipulatie de plaats inneemt van menselijke zwakheden.

Wat is Pharming? Een onzichtbare valstrik op het internet

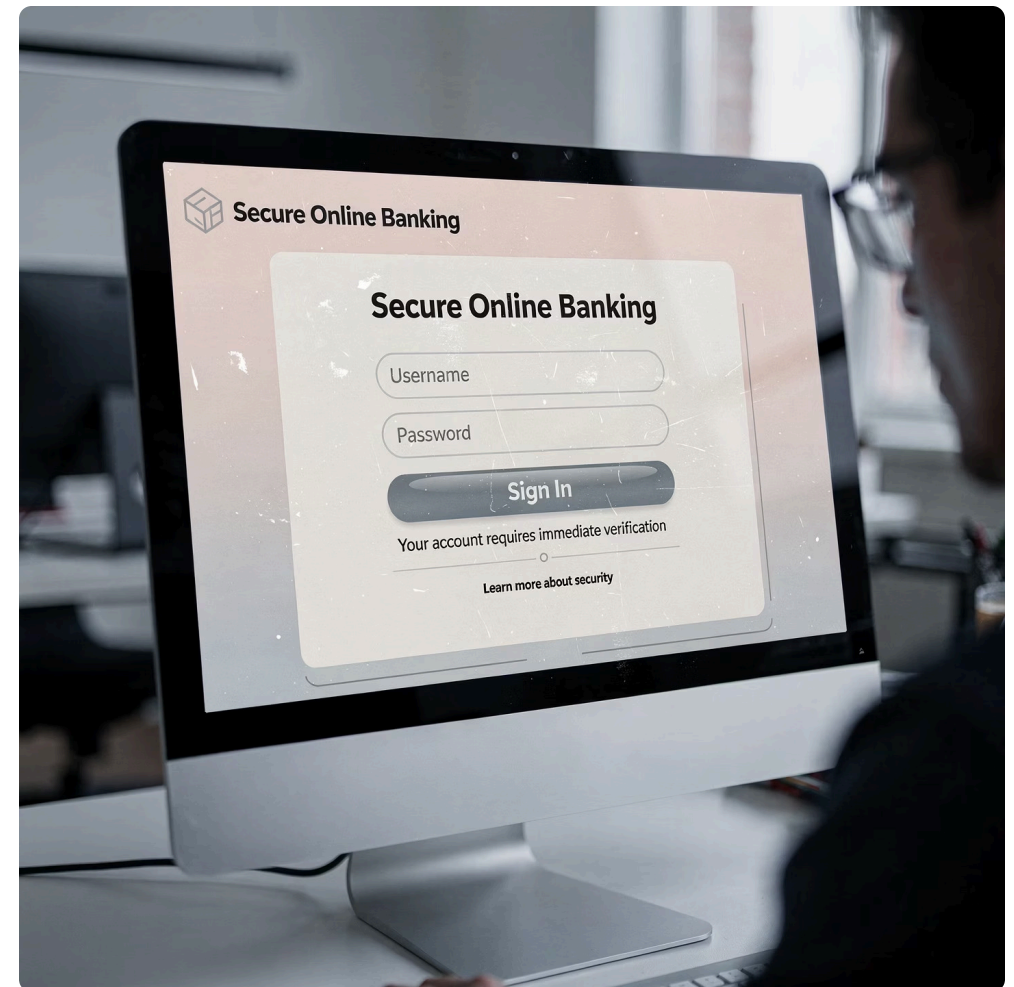
Pharming is een geavanceerde vorm van cyberfraude waarbij internetgebruikers zonder het te merken worden omgeleid naar nepwebsites. Deze techniek heeft zijn naam te danken aan een combinatie van "phishing" en "farming", wat verwijst naar de systematische manier waarop cybercriminelen slachtoffers oogsten.

Het verraderlijke van pharming is dat gebruikers zelfs naar frauduleuze websites worden geleid wanneer ze de correcte URL handmatig intypen in hun browser.

De nepwebsites die bij pharming worden gebruikt, zijn met uiterste precisie nagemaakt om exact op de echte websites te lijken. Van het logo en de kleurenschema's tot de exacte plaatsing van knoppen en formulieren - alles wordt gekopieerd om een perfecte illusie te creëren.

Hierdoor geven nietsvermoedende gebruikers hun meest gevoelige persoonlijke gegevens prijs, waaronder wachtwoorden, bankrekeningnummers, creditcardgegevens en andere vertrouwelijke informatie.

In tegenstelling tot traditionele phishing, waarbij het slachtoffer actief moet klikken op een verdachte link, gebeurt pharming volledig automatisch en onzichtbaar op de achtergrond. Dit maakt het een van de gevaarlijkste vormen van online fraude die momenteel bestaat.



Hoe werkt Pharming? De techniek achter de misleiding

Om pharming te begrijpen, moeten we eerst kijken naar het Domain Name System (DNS), het onzichtbare systeem dat het internet laat functioneren. Het DNS werkt als een gigantisch telefoonboek voor het internet: wanneer u een webadres zoals "www.bank.nl" intypt, vertaalt het DNS dit naar een numeriek IP-adres zoals 192.168.1.1, dat computers kunnen begrijpen. Cybercriminelen exploiteren dit fundamentele systeem op slinkse wijze.



Hosts-bestand manipulatie

Bij deze methode installeert malware, zoals Trojans of virussen, zich op de computer van het slachtoffer. Deze kwaadaardige software wijzigt vervolgens het lokale hosts-bestand, een klein configuratiebestand dat prioriteit krijgt boven DNS-servers.

Hierdoor worden vertrouwde webadressen automatisch omgeleid naar kwaadaardige IP-adressen zonder dat de gebruiker enige indicatie krijgt dat er iets mis is.



DNS-serververgiftiging

Dit is een nog gevaarlijker vorm waarbij hackers de DNS-cache van internetproviders of bedrijfsservers aanvallen en vervalsen. Door deze centrale servers te compromitteren, kunnen cybercriminelen duizenden of zelfs miljoenen gebruikers tegelijk naar nepwebsites omleiden.

Het verraderlijke is dat gebruikers helemaal niets hoeven te doen - zelfs het correct intypen van een webadres leidt naar de frauduleuze site.

Deze technische manipulatie maakt pharming aanzienlijk gevaarlijker dan traditionele phishing-aanvallen. Waar phishing-slachtoffers tenminste nog een verdachte e-mail of link moeten openen, gebeurt pharming volledig automatisch en is vrijwel ondetecteerbaar voor de gemiddelde gebruiker.

Pharming versus Phishing: Het subtiele verschil

Hoewel pharming en phishing beide tot doel hebben om gevoelige informatie te stelen, verschillen hun werkwijzen fundamenteel. Deze verschillen begrijpen is essentieel voor effectieve bescherming tegen beide bedreigingen.



Phishing

Phishing is gebaseerd op social engineering en menselijke psychologie. Aanvallers versturen misleidende e-mails, sms-berichten of sociale media-berichten die urgentie of nieuwsgierigheid wekken. Deze berichten bevatten links naar nepwebsites die op het eerste gezicht legitiem lijken.

Het slachtoffer moet actief handelen door op de link te klikken en vervolgens gegevens in te voeren.



Pharming

Pharming daarentegen werkt volledig achter de schermen door technische infrastructuur te manipuleren. Er is geen verdachte e-mail of link nodig - de gebruiker wordt automatisch omgeleid, zelfs wanneer deze de correcte URL rechtstreeks intypt.

Deze aanval is passief voor het slachtoffer maar actief op systeemniveau, waardoor detectie extreem moeilijk is.

📌 **Pharming wordt ook wel "phishing zonder lokaas" genoemd** - een toepasselijke benaming die de essentie van deze dreiging perfect samenvat. Terwijl phishing afhankelijk is van menselijke fouten en oplettenheid, kan pharming zelfs de meest waakzame gebruikers misleiden.

Het belangrijkste onderscheid ligt in de mate van betrokkenheid van het slachtoffer. Bij phishing heeft de gebruiker nog een kans om de aanval te herkennen aan verdachte e-mails, spelfouten of vreemde links. Bij pharming ontbreekt deze waarschuwing volledig - de technologie zelf is gecompromitteerd, wat betekent dat zelfs de meest voorzichtige gebruiker kan worden misleid zonder enig vermoeden.

Grote pharming-aanvallen: Schokkende voorbeelden uit de praktijk

De theoretische dreiging van pharming wordt concreet wanneer we kijken naar werkelijke aanvallen die wereldwijd hebben plaatsgevonden. Deze incidenten tonen aan hoe verwoestend pharming kan zijn en hoeveel schade het kan aanrichten aan zowel individuen als grote organisaties.



Deze voorbeelden illustreren de ernst en omvang van pharming-aanvallen. Het zijn geen geïsoleerde incidenten, maar deel van een groeiende trend waarbij cybercriminelen steeds geavanceerdere technieken ontwikkelen om onze digitale infrastructuur te misbruiken.

Hoe bescherm je jezelf tegen Pharming? Praktische tips en maatregelen

Hoewel pharming een geavanceerde technische dreiging is, zijn er effectieve maatregelen die zowel individuele gebruikers als organisaties kunnen nemen om het risico aanzienlijk te verkleinen. Bescherming begint met bewustwording en wordt versterkt door concrete technische oplossingen.



Kies een betrouwbare internetprovider

Uw ISP is uw eerste verdedigingslinie tegen pharming. Selecteer een provider die investeert in geavanceerde beveiligingsmaatregelen en actief kwaadaardige omleidingen blokkeert.

Vraag naar hun DNS-beveiligingsprotocollen en of ze DNSSEC (Domain Name System Security Extensions) ondersteunen.



Controleer URL's zorgvuldig

Neem de tijd om website-adressen kritisch te bekijken voordat u gevoelige informatie invoert. Let op kleine afwijkingen zoals extra letters, cijfers die letters vervangen (bijvoorbeeld een '0' in plaats van een 'O'), of ongebruikelijke domeinnamen.

Cybercriminelen gebruiken vaak subtiele variaties die op het eerste gezicht legitiem lijken.



Gebruik alleen HTTPS-websites

Websites met HTTPS (te herkennen aan het slotje in de adresbalk) gebruiken versleutelde verbindingen die veel veiliger zijn.

Voer nooit wachtwoorden of financiële gegevens in op websites zonder HTTPS. Let echter op: cybercriminelen kunnen ook SSL-certificaten verkrijgen, dus HTTPS alleen is geen garantie.



Installeer betrouwbare antivirussoftware

Hoogwaardige antivirussoftware kan malware detecteren en blokkeren die het hosts-bestand probeert te wijzigen. Update uw software regelmatig en voer wekelijks volledige systeemscans uit.

Veel moderne beveiligingspakketten bevatten ook anti-pharming functies die verdachte DNS-omleidingen kunnen herkennen.



Vermijd onbeveiligde openbare wifi

Openbare wifi-netwerken in cafés, hotels of luchthavens zijn notoir onveilig en kwetsbaar voor DNS-aanvallen. Gebruik altijd een VPN (Virtual Private Network) wanneer u op openbare netwerken bent.

Een VPN versleutelt al uw internetverkeer en beschermt tegen verschillende vormen van cyberaanvallen, inclusief pharming.



Beveilig DNS-servers (voor organisaties)

Bedrijven en organisaties moeten hun DNS-infrastructuur beschermen met DNSSEC en andere moderne beveiligingsprotocollen.

Implementeer regelmatige beveiligingsaudits, monitor DNS-verkeer op anomalieën, en train IT-personeel om pharming-aanvallen te herkennen en te neutraliseren.

 **Twefactorauthenticatie (2FA) toevoegen** aan uw belangrijke accounts biedt een extra beveiligingslaag. Zelfs als cybercriminelen uw wachtwoord stelen via pharming, kunnen ze zonder de tweede verificatiefactor geen toegang krijgen tot uw account.

Bescherming tegen pharming vereist een combinatie van technische oplossingen, gezond wantrouwen en voortdurende waakzaamheid. Door deze maatregelen te implementeren, verkleint u het risico aanzienlijk en creëert u een veel veiliger digitale omgeving voor uzelf en uw organisatie.

Conclusie: Bewustwording en preventie zijn je beste wapens tegen pharming

Pharming vertegenwoordigt een van de meest geavanceerde en verraderlijke cyberdreigingen van onze tijd. Het is een sluipende techniek die miljoenen internetgebruikers wereldwijd kan treffen zonder dat ze het merken, en die zelfs de meest technisch onderlegde gebruikers kan misleiden.

De onzichtbare manipulatie van fundamentele internetinfrastructuur maakt pharming tot een formidabele vijand in het digitale landschap.

Door het begrijpen van hoe pharming werkt en het cruciale verschil met traditionele phishing-aanvallen, kunnen zowel individuele gebruikers als organisaties gerichte en effectieve maatregelen nemen.

Bewustwording is de eerste en belangrijkste stap in de verdediging tegen deze dreiging. Wanneer u weet waarnaar u moet uitkijken en hoe cybercriminelen opereren, bent u al veel beter beschermd.



Blijf waakzaam

Controleer websites altijd kritisch voordat u persoonlijke informatie invoert. Een moment van oplettendheid kan u voor veel ellende behoeden.

Investeer in beveiliging

Goede antivirussoftware, een betrouwbare VPN en regelmatige updates zijn geen luxe maar noodzaak in het moderne digitale tijdperk.

Educatie is essentieel

Deel uw kennis over pharming met familie, vrienden en collega's. Collectieve bewustwording creëert een veiliger internet voor iedereen.

De strijd tegen pharming is een voortdurende inspanning die constante waakzaamheid vereist. Cybercriminelen ontwikkelen voortdurend nieuwe technieken en methoden om beveiligingsmaatregelen te omzeilen. Echter, door de principes en praktische tips uit dit document toe te passen, creëert u een robuuste verdediging tegen deze onzichtbare valstrik.

Wees alert, blijf geïnformeerd over nieuwe dreigingen, en neem uw digitale veiligheid serieus - want in de digitale wereld is preventie altijd beter dan de gevolgen van een succesvolle aanval.

A man and a young child are sitting on a wooden bench outdoors. The man, wearing a blue denim jacket, is holding a smartphone and looking at the screen. The child, also wearing a denim jacket, is looking at the phone with interest. The background shows a park-like setting with green trees and a clear sky. The text is overlaid on the bottom left of the image.

**Hoe timmer je de privacy-instellingen
van TikTok en Roblox dicht?**

In het digitale tijdperk zijn TikTok en Roblox niet meer weg te denken uit het leven van jongeren. Deze platforms bieden eindeloos entertainment, maar brengen ook belangrijke privacy-uitdagingen met zich mee. Deze gids helpt je stap voor stap om de privacy-instellingen van beide platforms vakkundig in te stellen en je gezin te beschermen tegen digitale risico's.

Waarom privacy-instellingen belangrijk zijn op TikTok en Roblox

TikTok en Roblox behoren tot de meest populaire sociale platforms ter wereld, met miljoenen jonge gebruikers die dagelijks uren doorbrengen met het maken van content, gamen en communiceren. Deze platforms zijn ontworpen om verslavend te zijn en verzamelen daarbij enorme hoeveelheden persoonlijke gegevens. Van locatiegegevens tot browsegedrag, van contactlijsten tot video-interacties – alles wordt bijgehouden en geanalyseerd.

Het gevaar schuilt niet alleen in dataverzameling door de platforms zelf, maar ook in wie er toegang heeft tot de profielen en content van je kind. Onvoldoende beveiligde accounts kunnen leiden tot ongewenste contacten met vreemden, cyberpesten, online grooming, of blootstelling aan ongepaste inhoud. Kinderen zijn zich vaak niet bewust van de risico's en delen vrijelijk persoonlijke informatie.

Goed geconfigureerde privacy-instellingen vormen een essentiële verdedigingslinie. Ze bepalen wie je kind kan contacteren, wat anderen kunnen zien, en hoeveel informatie er wordt gedeeld. Door deze instellingen correct te configureren, creëer je een veiliger digitale omgeving waarin je kind kan genieten van deze platforms zonder onnodige risico's te lopen.



Databescherming

Voorkom ongewenste dataverzameling



Privacy

Bepaal wie je content kan zien



Veiligheid

Bescherm tegen ongewenste contacten

TikTok: Je account volledig privé maken

01

Open je profiel

Tik rechtsboven in de TikTok-app op de drie horizontale lijnen om het menu te openen

03

Kies privacy

Tik op de optie "Privacy" om alle privacy-gerelateerde instellingen te bekijken

Wat betekent een privé account?

Wanneer je account op privé staat, krijgen alleen mensen die je expliciet goedkeurt toegang tot je video's en profiel. Bestaande volgers behouden hun toegang automatisch, maar nieuwe volgers moeten eerst een verzoek indienen dat je handmatig moet accepteren of afwijzen.

Dit is bijzonder effectief voor kinderen, omdat het onbekenden verhindert om zomaar je content te bekijken of te interacteren. Let wel op: video's die je hebt geplaatst voordat je het account privé maakte, kunnen nog steeds zichtbaar zijn geweest voor het publiek.

02

Ga naar instellingen

Selecteer "Instellingen en privacy" onderaan het menu

04

Activeer privé account

Zet de schakelaar bij "Privé account" aan om je profiel af te schermen



Belangrijk om te weten

Een privé account voorkomt niet dat je video's worden gedownload door bestaande volgers. Wees daarom altijd voorzichtig met wat je deelt, zelfs op een privé account.

TikTok: Beperk wie je kan vinden en volgen

Naast het privé maken van je account zijn er nog meer instellingen die bepalen hoe vindbaar je bent op TikTok. Het platform probeert actief om gebruikers met elkaar te verbinden en stelt daarom automatisch je profiel voor aan anderen. Dit kan ongewenst zijn, vooral voor kinderen.

Schakel aanbevelingen uit

Ga naar Privacy > "Beveel je account aan anderen aan" en schakel deze optie uit. Dit voorkomt dat TikTok jouw profiel suggereert aan mensen die je niet kent, gebaseerd op gedeelde interesses, contacten of andere factoren.

Verwijder contactsynchronisatie

TikTok kan je contactenlijst synchroniseren om vrienden te vinden. Ga naar Privacy > "Suggestie door contacten synchroniseren" en schakel dit uit. Verwijder ook eerder gesynchroniseerde contacten om te voorkomen dat mensen uit je telefoonboek je automatisch kunnen vinden op TikTok.

Maak volglijsten privé

Standaard kunnen anderen zien wie jij volgt en wie jou volgt. Ga naar Privacy > "Volglijst" en stel in op "Alleen ik". Doe hetzelfde voor "Gelikte video's" via Privacy > "Gelikte video's" > "Alleen ik". Dit voorkomt dat anderen kunnen zien met wie je interacteert.

Waarom is vindbaarheid beperken belangrijk?

Hoe minder vindbaar een account is, hoe kleiner de kans dat onbekenden je kind kunnen vinden en benaderen. Kinderen onderschatten vaak het risico van onbekende contacten en accepteren snel volgverzoeken van mensen die ze niet kennen.

Extra tip

Gebruik geen herkenbare profielfoto en geen echte naam als gebruikersnaam. Dit maakt het moeilijker voor onbekenden om je kind te identificeren of terug te vinden op andere platforms.

TikTok: Controleer reacties, tags en directe berichten

Interactie is een kernonderdeel van TikTok, maar niet alle interacties zijn gewenst. TikTok biedt gelukkig uitgebreide mogelijkheden om te bepalen wie kan reageren op je video's, wie je kan taggen, en wie je directe berichten kan sturen. Deze instellingen zijn cruciaal voor het voorkomen van cyberpesten en ongewenste aandacht.

Reacties beperken

Ga naar Privacy > "Reacties" en kies uit verschillende opties:

- **Iedereen:** Alle TikTok-gebruikers kunnen reageren (niet aanbevolen)
- **Vrienden:** Alleen mensen die jij volgt én die jou volgen
- **Niemand:** Schakel alle reacties uit

Voor kinderen raden we aan om te kiezen voor "Vrienden" of "Niemand".

Filter ongepaste reacties

Activeer de optie "Filter alle reacties" om automatisch spam en potentieel schadelijke reacties te blokkeren. Je kunt ook specifieke trefwoorden toevoegen die je wilt filteren.

Ga naar Privacy > "Reacties" > "Filter trefwoorden" en voeg woorden toe die je wilt blokkeren in reacties op je video's.

Tags en vermeldingen

Bepaal wie je kan taggen in hun video's of je kan noemen in reacties. Ga naar Privacy > "Tags en vermeldingen" en selecteer "Vrienden" of "Niemand".

Dit voorkomt dat onbekenden je account linken aan hun content zonder jouw toestemming.

Directe berichten

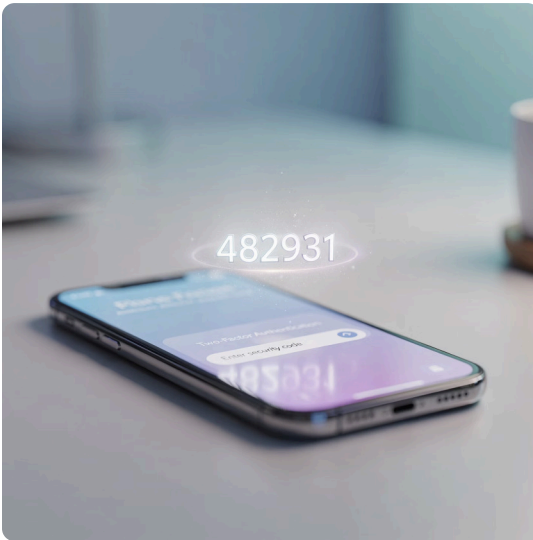
Ga naar Privacy > "Directe berichten" en stel in wie je mag sturen:

- **Vrienden:** Alleen wederzijdse volgers
- **Niemand:** Alle DM's uitschakelen (veiligste optie)

Dit voorkomt dat vreemden je kind kunnen benaderen via privéberichten.

Let op: Bespreek met je kind dat ze nooit persoonlijke informatie moeten delen in reacties of berichten, zelfs niet met mensen die ze online kennen. Vertrouwen moet online altijd eerst worden opgebouwd voordat er persoonlijke informatie wordt gedeeld.

TikTok: Extra beveiliging met tweestapsverificatie



Tweestapsverificatie (ook wel 2FA genoemd) is een essentiële beveiligingslaag die voorkomt dat hackers toegang krijgen tot je account, zelfs als ze je wachtwoord weten. Bij het inloggen moet je naast je wachtwoord ook een unieke code invoeren die naar je telefoon of e-mail wordt gestuurd.

Dit betekent dat een aanvaller niet alleen je wachtwoord nodig heeft, maar ook fysieke toegang tot je telefoon of e-mailaccount. Dit maakt het hacken van accounts aanzienlijk moeilijker en beschermt tegen de meest voorkomende aanvalsmethoden.

Open beveiligingsinstellingen

Ga naar Instellingen en privacy >
Beveiliging en inloggen

Selecteer verificatiemethode

Tik op "2-stapsverificatie" en kies
tussen SMS, e-mail of authenticator-
app

Voltooi activering

Voer de verificatiecode in die je
ontvangt om 2FA te activeren

Welke methode moet je kiezen?

SMS: Gemakkelijk maar minder veilig (kwetsbaar voor SIM-swap aanvallen)

E-mail: Betere optie, zorg wel dat je e-mailaccount zelf goed beveiligd is

Authenticator-app: Meest veilige optie (bijv. Google Authenticator of Microsoft Authenticator)

Naast tweestapsverificatie is het belangrijk om een sterk, uniek wachtwoord te gebruiken voor TikTok. Gebruik minimaal 12 tekens met een combinatie van hoofdletters, kleine letters, cijfers en symbolen. Gebruik dit wachtwoord nergens anders en overweeg het gebruik van een wachtwoordmanager om al je wachtwoorden veilig op te slaan.

Roblox: Accountbeperkingen inschakelen voor kinderen

Roblox is een enorm populair gaming-platform waar miljoenen kinderen dagelijks spelen, creëren en communiceren. Het platform biedt vrijwel onbeperkte mogelijkheden, maar niet alle content is geschikt voor kinderen. Gelukkig heeft Roblox uitgebreide ouderlijke controles ingebouwd, waarbij accountbeperkingen de meest effectieve eerste verdedigingslinie vormen.



Stap 1: Open instellingen

Log in op het Roblox-account van je kind en klik op het tandwiel-icoon rechtsboven in het scherm om naar de instellingen te gaan.



Stap 2: Activeer beperkingen

Klik op het tabblad "Privacy" en scroll naar beneden tot je "Accountbeperkingen" ziet. Zet deze schakelaar aan om strenge filters te activeren.



Stap 3: Verifieer instellingen

Controleer dat alleen door Roblox goedgekeurde games zichtbaar zijn en dat chat-functionaliteit is uitgeschakeld of zeer beperkt.

Wat doet accountbeperkingen precies?

Wanneer accountbeperkingen zijn ingeschakeld, past Roblox automatisch meerdere beveiligingslagen toe. Ten eerste worden alleen games weergegeven die door Roblox zijn geverifieerd als geschikt voor alle leeftijden. Games met gewelddadige, enge of anderszins ongepaste content worden automatisch uitgefilterd.

Ten tweede wordt alle chat-functionaliteit sterk beperkt of volledig uitgeschakeld. Je kind kan niet chatten met andere spelers of alleen met vooraf goedgekeurde berichten. Dit voorkomt dat vreemden je kind kunnen benaderen of dat je kind persoonlijke informatie deelt.

Tot slot worden andere interacties zoals friend requests en groepsuitnodigingen ook beperkt, waardoor een veel veiligere speelomgeving ontstaat die specifiek is ontworpen voor jongere kinderen.



Let op

Accountbeperkingen zijn vooral geschikt voor jonge kinderen (onder de 13 jaar). Voor oudere tieners kunnen deze beperkingen te restrictief zijn, en kun je beter werken met aangepaste privacy-instellingen en open communicatie.



Roblox: Communicatie en toegangsinstellingen aanpassen

Voor kinderen die accountbeperkingen te beperkend vinden of voor oudere tieners biedt Roblox gedetailleerde communicatie- en toegangsinstellingen. Hiermee kun je precies bepalen met wie je kind kan communiceren, wie hen kan uitnodigen voor games, en welke ervaringen ze kunnen spelen.

1	Chat en berichten aanpassen Ga naar Instellingen > Privacy en scroll naar "Wie kan met mij chatten?" Kies uit: • Niemand: Alle chat uitschakelen (veiligst) • Vrienden: Alleen chatten met toegevoegde vrienden • Vrienden en volgers: Chat met vrienden en mensen die je volgen • Iedereen: Onbeperkt chatten (niet aanbevolen voor kinderen) Stel ook in wie je privéberichten kan sturen onder "Wie kan mij een bericht sturen?" Voor de meeste kinderen is "Vrienden" of "Niemand" de beste keuze.
2	Game-toegang beperken Bepaal wie je kind kan uitnodigen voor games en wie je kind kan volgen naar andere games. Ga naar Privacy > "Wie kan mij uitnodigen voor VIP-servers?" en "Wie kan mij naar games volgen?" Stel beide in op "Vrienden" of "Niemand" om te voorkomen dat onbekenden je kind kunnen benaderen tijdens het gamen.
3	Leeftijdscategorieën instellen Roblox categoriseert games op basis van geschiktheid voor verschillende leeftijden. Ga naar Instellingen > Ouderlijk toezicht > Toegestane ervaringen en kies een geschikt niveau: • Alle leeftijden: Content geschikt voor alle leeftijden • 9+: Mild geweld of licht angstaanjagende content • 13+: Meer realistisch geweld en mature thema's • 17+: Content met volwassen thema's (alleen beschikbaar na leeftijdsverificatie) Kies een niveau dat past bij de leeftijd en maturiteit van je kind. Je kunt dit altijd aanpassen naarmate ze ouder worden.

"Het belangrijkste is om regelmatig te praten met je kind over wat ze spelen en wie ze ontmoeten in games. Privacy-instellingen zijn een hulpmiddel, maar open communicatie is de beste bescherming."

Roblox: Ouderlijk toezicht en schermtijd beheren



Roblox biedt een geavanceerd ouderlijk toezicht-systeem waarmee je als ouder direct betrokken kunt blijven bij de gaming-ervaring van je kind. Door een ouderaccount te koppelen aan het account van je kind, krijg je toegang tot uitgebreide controles en inzichten in hun activiteiten.

- 1

Maak een ouderaccount
Ga naar roblox.com en maak een apart account aan met je eigen e-mailadres. Dit wordt je ouderlijk toezicht-account.
- 2

Koppel accounts
Log in op je ouderaccount, ga naar Instellingen > Ouderlijk toezicht > Beheer kinderen en voer de gebruikersnaam van je kind in. Je kind moet de koppeling goedkeuren via hun account.
- 3

Configureer toezichtinstellingen
Eenmaal gekoppeld kun je vanuit je ouderaccount alle privacy- en veiligheidsinstellingen van je kind beheren, inclusief chat, vriendschappen en toegestane ervaringen.
- 4

Stel schermtijdlimieten in
Ga naar Ouderlijk toezicht > Schermtijdlimiet en stel dagelijkse limieten in voor hoeveel tijd je kind op Roblox mag besteden. Je kunt verschillende limieten instellen voor weekdays en weekends.
- 5

Beveilig met pincode
Stel een 4-cijferige pincode in onder Ouderlijk toezicht > Beveiliging. Deze pincode is vereist om instellingen te wijzigen, zodat je kind deze niet zelf kan aanpassen.

Nadat je ouderlijk toezicht hebt ingesteld, ontvang je regelmatig meldingen en samenvattingen over de activiteiten van je kind op Roblox. Je ziet welke games ze hebben gespeeld, met wie ze hebben gecommuniceerd, en hoeveel tijd ze hebben besteed. Dit geeft je waardevolle inzichten en gespreksstarters om met je kind te praten over hun online ervaringen.

2	15	1x
Uur per dag	Minuten	Per week
Aanbevolen maximale schermtijd voor kinderen volgens experts	Pauze tussen gaming-sessies voorkomt verslaving en bevordert gezonde gewoonten	Frequentie waarmee je privacy-instellingen moet controleren

Samenvatting en tips voor blijvende privacybescherming

Privacy op sociale media en gaming-platforms is geen eenmalige taak, maar een voortdurend proces. Platforms zoals TikTok en Roblox updaten regelmatig hun functies, instellingen en privacybeleid. Wat vandaag veilig is ingesteld, kan morgen aangepast moeten worden door een nieuwe feature of beleidswijziging. Daarom is het essentieel om waakzaam te blijven en periodiek de instellingen te controleren.



Regelmatige controle

Plan maandelijks een moment in om de privacy-instellingen van TikTok en Roblox door te nemen. Platforms voegen regelmatig nieuwe functies toe die standaard minder veilig zijn ingesteld. Een snelle check van 10 minuten kan voorkomen dat er nieuwe privacylekken ontstaan.



Open communicatie

Praat regelmatig met je kinderen over wat ze online doen, wie ze ontmoeten en welke content ze zien of delen. Leg uit waarom privacy belangrijk is en help ze begrijpen welke informatie veilig is om te delen en wat niet. Maak het bespreekbaar zonder veroordelend te zijn, zodat ze naar je toe komen wanneer er iets vervelends gebeurt.



Actief ouderlijk toezicht

Gebruik de ouderlijke controlemogelijkheden die platforms bieden. Maak gebruik van schermtijdlimieten, content-filters en activiteitenrapporten. Maar vergeet niet dat technologie slechts een hulpmiddel is – vertrouwen en communicatie zijn de basis van online veiligheid.



Tweestapsverificatie overal

Activeer 2FA niet alleen op TikTok en Roblox, maar op alle accounts die je kind gebruikt: e-mail, schoolaccounts, andere sociale media. Dit is de meest effectieve manier om accounts te beschermen tegen hacking en identiteitsdiefstal.



Blijf op de hoogte

Volg nieuwsbronnen over digitale veiligheid en privacy. Platforms kondigen grote wijzigingen vaak aan via hun blogs of nieuwssecties. Blijf alert op nieuwe functies die invloed kunnen hebben op de privacy van je kind en pas instellingen dienovereenkomstig aan.



Educatie is de sleutel

Leer je kinderen kritisch te denken over wat ze online delen. Help ze begrijpen dat alles wat online wordt geplaatst permanent kan zijn, zelfs als het later wordt verwijderd. Teach them about digital footprints en de lange-termijn consequenties van online gedrag.

Belangrijkste actiepunten

1. Maak TikTok-accounts privé en beperk wie kan communiceren
2. Schakel accountbeperkingen in op Roblox voor jonge kinderen
3. Activeer tweestapsverificatie op beide platforms
4. Stel ouderlijk toezicht en schermtijdlimieten in
5. Controleer instellingen maandelijks en praat wekelijks met je kind

Onthoud: Privacy-instellingen zijn krachtige tools, maar de meest effectieve bescherming komt van educatie, open communicatie en betrokkenheid. Blijf in gesprek met je kinderen over hun digitale leven en maak online veiligheid een natuurlijk onderdeel van jullie dagelijkse interacties.



Internetgebruikers kiezen voor gratis
diensten met trackingvrije
advertenties

Het 'Pay or Okay'-model staat centraal in het debat over online privacy en verdienmodellen. Privacyorganisatie noyb onderzoekt hoe gebruikers denken over de keuze tussen betalen voor diensten of gratis toegang met trackingvrije advertenties.

Het 'Pay or Okay'-model: keuzevrijheid tussen betalen of trackingvrije advertenties



Privacy eerst

Gebruikers willen controle over hun gegevens zonder financiële drempels



Gratis toegang

Meerderheid prefereert gratis diensten met trackingvrije advertenties



Derde optie

Een alternatief naast gratis-met-tracking of betaald-zonder-tracking

Privacyorganisatie noyb onderzocht de voorkeuren van internetgebruikers voor online diensten. Het onderzoek toont een duidelijke voorkeur: gebruikers willen gratis toegang tot online diensten, maar dan wel zonder invasieve tracking. Dit model biedt een innovatieve middenweg die gebruikers meer autonomie geeft over hun privacy.

Traditioneel model

- Gratis met uitgebreide tracking
- Betaald zonder tracking
- Beperkte keuzevrijheid

Pay or Okay-model

- Gratis met trackingvrije advertenties
- Betaald voor ad-free ervaring
- Meer controle voor gebruikers

Het idee achter dit model is simpel maar krachtig: gebruikers hoeven niet te kiezen tussen hun portemonnee en hun privacy. Door trackingvrije advertenties als derde optie aan te bieden, krijgen zij de mogelijkheid om diensten gratis te gebruiken terwijl hun privacyrechten gerespecteerd worden.

Praktijkervaringen: waarom trackingvrije advertenties niet altijd werken

De theorie van trackingvrije advertenties klinkt aantrekkelijk, maar de praktijk blijkt weerbarstiger. Tweakers, een Nederlandse technieuwssite, stapte in 2022 moedig over op advertenties zonder third-party tracking. Hun ervaring illustreert de economische uitdagingen van dit model.



Na anderhalf jaar bleek dat adverteerders minder budgetten inzetten vanwege gebrek aan meetmogelijkheden en afwijkende workflows. Het aantal adverteerders daalde sterk, wat leidde tot een forse daling van advertentie-inkomsten.

De ervaring van Tweakers toont de spanning tussen privacyvriendelijke advertentiemodellen en de economische realiteit van online uitgevers. Adverteerders zijn gewend aan gedetailleerde tracking en targeting, en zonder deze tools zijn ze minder bereid om te investeren. Dit illustreert een fundamenteel probleem: het hele advertentie-ecosysteem is gebouwd op tracking, en een eenzijdige verandering door uitgevers is moeilijk vol te houden zonder bredere marktverandering.

Europese regelgeving en de impact op advertentiemodellen

Europa loopt voorop in het beschermen van online privacy door middel van wetgeving. De Digital Services Act (DSA) en de GDPR hebben het landschap van online advertenties fundamenteel veranderd en dwingen platforms tot meer transparantie en keuzevrijheid.

1

GDPR-vereisten

Toestemming voor tracking moet 'vrij' gegeven worden, met een echt gelijkwaardig alternatief zonder tracking beschikbaar

2

DSA-regelgeving

Versterkt privacyrechten verder en stelt strengere eisen aan transparantie van advertentiesystemen

3

Platform-respons

Meta en andere grote platforms bieden sinds 2023 betaalde abonnementen aan als trackingvrij alternatief

Juridische ontwikkelingen

Europese privacytoezichthouders handhaven streng: toestemming moet echt vrijwillig zijn. Dit betekent dat het gratis alternatief even bruikbaar moet zijn als de betaalde variant. Het 'Pay or Okay'-principe wordt hiermee juridisch bevestigd, maar roept tegelijk discussie op over de betaalbaarheid van privacy.



Adblock Plus

Initiatieven zoals Adblock Plus bevorderen 'acceptabele advertenties' zonder tracking die gebruikers respecteren én websites inkomsten bieden.

Grote platforms zoals Meta hebben gereageerd met abonnementsmodellen: gebruikers kunnen betalen voor een trackingvrije ervaring, of gratis blijven met tracking. Dit model past binnen de regelgeving, maar critici vragen zich af of privacy zo niet een luxegoed wordt dat alleen voor betalende gebruikers beschikbaar is.

Conclusie: de toekomst van online diensten en privacyvriendelijke advertenties



Gebruikerswensen

Internetgebruikers willen gratis toegang zonder privacy in te leveren - het 'Pay or Okay'-model speelt hierop in



Europese wetgeving

Regelgeving dwingt tot transparantie en keuzevrijheid, maar de markt zoekt nog naar optimale oplossingen



Uitdaging uitgevers

Uitgevers worstelen met duurzame verdienmodellen die trackingvrije advertenties combineren met voldoende inkomsten



Technologische innovatie

First-party-data en privacyvriendelijke advertentietechnieken bieden hoop op betere balans

De komende jaren worden cruciaal voor de toekomst van online diensten. De spanning tussen gebruikersprivacy, advertentie-inkomsten en vrije toegang tot content moet opgelost worden. Innovaties in privacyvriendelijke advertentietechnieken, zoals contextual advertising en first-party data, kunnen een uitweg bieden.

Het succes van het 'Pay or Okay'-model hangt af van een gezamenlijke inspanning: wetgevers moeten eerlijke regelgeving handhaven, platforms moeten investeren in alternatieve advertentietechnologie, en adverteerders moeten accepteren dat effectieve reclame mogelijk is zonder invasive tracking.

Uiteindelijk gaat het om het vinden van een nieuw evenwicht in het internet-ecosysteem. Een evenwicht waarbij gebruikers niet hoeven te kiezen tussen hun privacy en toegang tot informatie, waarbij uitgevers kunnen blijven bestaan, en waarbij adverteerders hun doelen kunnen bereiken op een respectvolle manier. De antwoorden zijn nog niet volledig duidelijk, maar de richting is gezet: naar een internet dat privacy respecteert zonder toegankelijkheid op te offeren.

De kern van de uitdaging

Hoe houden we online diensten betaalbaar én privacybewust voor iedereen, zonder dat uitgevers hun verdienmodel verliezen?



**Je gebruikersnaam of wachtwoord
wordt niet geaccepteerd: wat nu?**

Wie kent het niet? Je probeert in te loggen op je belangrijke Microsoft- of Google-account, maar je krijgt steeds de melding dat je gebruikersnaam of wachtwoord niet wordt geaccepteerd. Een frustrerende situatie, maar gelukkig is er bijna altijd een oplossing. Of je nu een simpele typfout hebt gemaakt, je wachtwoord bent vergeten, of te maken hebt met een geblokkeerd account - er zijn meer dan genoeg manieren om weer toegang te krijgen.

In dit document nemen we je stap voor stap mee door de verschillende oplossingen voor inlogproblemen bij Microsoft en Google. We beginnen met de meest voorkomende oorzaken, behandelen vervolgens de concrete herstelstappen voor beide platforms, en geven je praktische tips om toekomstige problemen te voorkomen. Aan het einde van dit document kun je zelfstandig de meeste inlogproblemen oplossen en weet je precies waar je terecht kunt als je er echt niet uitkomt.

Waarom werkt mijn gebruikersnaam of wachtwoord niet?

Voordat je in paniek raakt en allerlei herstelprocessen start, is het goed om te begrijpen waarom je inlogpoging mislukt. In veel gevallen ligt de oplossing dichterbij dan je denkt. De meest voorkomende oorzaken zijn vaak simpel te verhelpen, terwijl andere wat meer uitleg en actie vereisen.



Typfouten en verkeerde invoer

Dit is veruit de meest voorkomende oorzaak van inlogproblemen. Een enkele verkeerde letter, een omgedraaid cijfer, of het gebruik van het verkeerde e-maildomein kan al genoeg zijn. Denk aan @outlook.com in plaats van @hotmail.com, of .co.uk in plaats van .com. Ook de Caps Lock-toets die per ongeluk aan staat kan roet in het eten gooien.



Verouderde software

Oude apps of browsers kunnen compatibiliteitsproblemen veroorzaken, vooral bij Google-diensten. Technologie ontwikkelt zich razendsnel, en providers updaten regelmatig hun beveiligingsprotocollen. Een app of browser die een paar jaar oud is, voldoet mogelijk niet meer aan de huidige veiligheidseisen en wordt daarom geblokkeerd bij inlogpogingen.



Beveiligingsmaatregelen

Zowel Microsoft als Google nemen beveiliging zeer serieus. Als hun systemen verdachte inlogactiviteit detecteren - bijvoorbeeld meerdere mislukte pogingen, inloggen vanaf een onbekende locatie, of gebruik van een onveilige verbinding - kan je account tijdelijk worden geblokkeerd. Dit is een beschermingsmaatregel om te voorkomen dat hackers toegang krijgen tot jouw persoonlijke gegevens.



Verlopen of geblokkeerd account

Sommige accounts worden automatisch vergrendeld na een periode van inactiviteit, of als je wachtwoord volgens het beveiligingsbeleid te oud is. Ook kan het zijn dat je account door het bedrijf zelf is opgeschort vanwege schending van gebruiksvoorwaarden, of dat er betalingsproblemen zijn bij betaalde diensten.

Nu je weet wat er mogelijk mis kan zijn, kunnen we aan de slag met de oplossingen. In de volgende secties behandelen we de specifieke herstelstappen voor zowel Microsoft- als Google-accounts, zodat je snel weer toegang hebt tot je belangrijke gegevens en diensten.

Microsoft-account: account herstellen in 5 stappen

Als je niet meer kunt inloggen op je Microsoft-account, hoef je niet direct in paniek te raken. Microsoft heeft een duidelijk en gebruiksvriendelijk herstelproces ontwikkeld waarmee je in de meeste gevallen binnen enkele minuten weer toegang hebt. Het is belangrijk dat je deze stappen zorgvuldig volgt en de juiste informatie bij de hand hebt.

01

Ga naar de herstelpagina

Open je webbrowser en navigeer naar de officiële Microsoft-pagina 'Uw account herstellen'. Je vindt deze door te zoeken op 'Microsoft account recovery' of via account.live.com/acsrr. Zorg ervoor dat je op de officiële Microsoft-website bent en niet op een phishing-site.

03

Kies je verificatiemethode

Microsoft vraagt je nu waar je de beveiligingscode wilt ontvangen. Je kunt kiezen tussen een sms naar je geregistreerde telefoonnummer of een e-mail naar je alternatieve e-mailadres. Kies de methode waarbij je direct toegang hebt tot het ontvangstmedium.

05

Stel een nieuw wachtwoord in

Nu je je identiteit hebt bevestigd, mag je een nieuw wachtwoord instellen. Kies een sterk wachtwoord van minimaal 8 tekens met een mix van hoofdletters, kleine letters, cijfers en speciale tekens. Vermijd voor de hand liggende keuzes zoals '123456' of 'wachtwoord'.

Wat als deze stappen niet werken?

Als je na het doorlopen van deze stappen nog steeds geen toegang hebt, kan dat verschillende oorzaken hebben. Mogelijk heb je geen toegang meer tot je registreerde telefoonnummer of e-mailadres, of is je account zwaarder beveiligd door tweestapsverificatie. In dat geval kun je contact opnemen met de Microsoft-ondersteuning via hun officiële supportkanalen.

Houd zo veel mogelijk informatie bij de hand over je account, zoals recent gebruikte wachtwoorden, de datum waarop je het account hebt aangemaakt, en namen van mappen of contacten in je account.

02

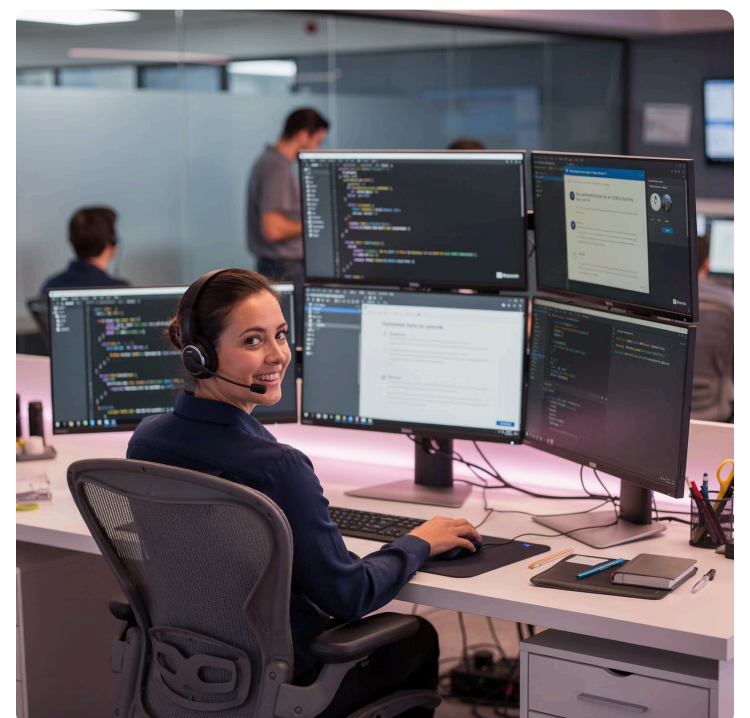
Vul je accountgegevens in

Voer het e-mailadres, telefoonnummer of de Skype-naam in die aan je Microsoft-account is gekoppeld. Als je meerdere adressen hebt gebruikt in het verleden, probeer dan alle varianten. Wees extra alert op typefouten of verkeerde domeinen zoals eerder besproken.

04

Voer de beveiligingscode in

Check je telefoon of e-mail voor de code die Microsoft je heeft gestuurd. Deze code is meestal enkele minuten geldig, dus wees er snel bij. Voer de code exact in zoals je deze hebt ontvangen, inclusief eventuele streepjes of spaties.



Microsoft-tips om inlogproblemen te voorkomen

Voorkomen is beter dan genezen - dit geldt zeker voor inlogproblemen. Door enkele simpele voorzorgsmaatregelen te nemen, kun je veel frustratie in de toekomst voorkomen. Microsoft biedt verschillende mogelijkheden om je account toegankelijk en veilig te houden, en het is verstandig om daar gebruik van te maken.

Controleer altijd het e-maildomein

Een van de meest gemaakte fouten is het gebruik van een verkeerd e-maildomein. Microsoft heeft verschillende domeinen in gebruik: @outlook.com, @hotmail.com, @live.com, en voor zakelijke accounts vaak een bedrijfsdomein. Zorg dat je precies weet welk adres bij jouw account hoort. Tip: bewaar je inloggegevens in een notitie of wachtwoordmanager, zodat je altijd de juiste variant gebruikt. Let ook op landspecifieke varianten zoals @hotmail.co.uk of @outlook.de - een klein verschil met grote gevolgen.

Gebruik alternatieve inlogmethoden

Microsoft staat toe dat je meerdere aliassen aan je account koppelt. Dit zijn alternatieve e-mailadressen of telefoonnummers waarmee je ook kunt inloggen. Het is verstandig om ten minste één alternatief toe te voegen in je accountinstellingen. Als je primaire e-mailadres niet werkt - bijvoorbeeld omdat je er geen toegang meer toe hebt of omdat je een typfout blijft maken - kun je je alias gebruiken. Ook een telefoonnummer toevoegen is handig: je kunt dan inloggen met je nummer en een sms-code ontvangen voor verificatie.

Houd je software up-to-date

Verouderde browsers en apps zijn niet alleen een beveiligingsrisico, ze kunnen ook compatibiliteitsproblemen veroorzaken bij het inloggen. Microsoft ondersteunt niet meer alle oude versies van Internet Explorer en oudere versies van Edge. Ook apps van derden, zoals e-mailclients of synchronisatietools, kunnen problemen geven als ze niet regelmatig worden geüpdatet. Controleer daarom periodiek of er updates beschikbaar zijn voor je browser, besturingssysteem en apps die verbinding maken met je Microsoft-account. Moderne browsers zoals de nieuwste versies van Edge, Chrome, Firefox en Safari zijn altijd een veilige keuze.

Door deze preventieve maatregelen toe te passen, verklein je de kans op inlogproblemen aanzienlijk. Het kost wat tijd om alles goed in te stellen, maar dat weegt niet op tegen de frustratie van een geblokkeerd account wanneer je dringend toegang nodig hebt tot belangrijke documenten of e-mails.

Google-account: wat te doen bij foutmelding 'Onjuist wachtwoord'?

Google-accounts zijn misschien nog wel belangrijker dan Microsoft-accounts, omdat ze toegang geven tot een enorm ecosysteem van diensten: Gmail, Google Drive, YouTube, Google Photos, en meer. Wanneer je de melding 'Onjuist wachtwoord' krijgt, kan dat verschillende oorzaken hebben die specifiek zijn voor hoe Google met beveiliging omgaat.



Controleer je wachtwoord zorgvuldig

Dit klinkt voor de hand liggend, maar is cruciaal. Google-wachtwoorden zijn hoofdlettergevoelig, wat betekent dat 'Wachtwoord123' iets heel anders is dan 'wachtwoord123'. Ook speciale tekens zoals @, #, ! en \$ moeten exact overeenkomen. Probeer je wachtwoord in een notitieblok te typen waar je het kunt zien, en kopieer het dan naar het inlogveld - zo voorkom je typefouten. Let ook op of je misschien per ongeluk een spatie aan het begin of einde hebt toegevoegd.



Update je apps en besturingssysteem

Als je probeert in te loggen via een app van een derde partij - bijvoorbeeld Apple Mail op je iPhone, Thunderbird op je computer, of een andere e-mailclient - kan het zijn dat deze app een verouderd beveiligingsprotocol gebruikt. Google heeft in de afgelopen jaren de beveiligingseisen aangescherpt en ondersteunt oude authenticatiemethoden niet meer. De oplossing is simpel: update je app naar de nieuwste versie, of beter nog, schakel over op de officiële Gmail-app die altijd de modernste beveiligingsstandaarden gebruikt.



Gebruik veiligere authenticatie

Google blokkeert actief apps die als 'minder veilig' worden beschouwd. Als je zo'n app gebruikt, krijg je de melding dat inloggen is geblokkeerd. Google stuurt je dan een e-mail met een waarschuwing en de optie om 'minder veilige apps' toe te staan - maar dit wordt afgeraden! Beter is om over te stappen op apps die moderne OAuth-authenticatie ondersteunen, of om gebruik te maken van app-specifieke wachtwoorden (hier komen we later op terug).



Maak gebruik van app-wachtwoorden

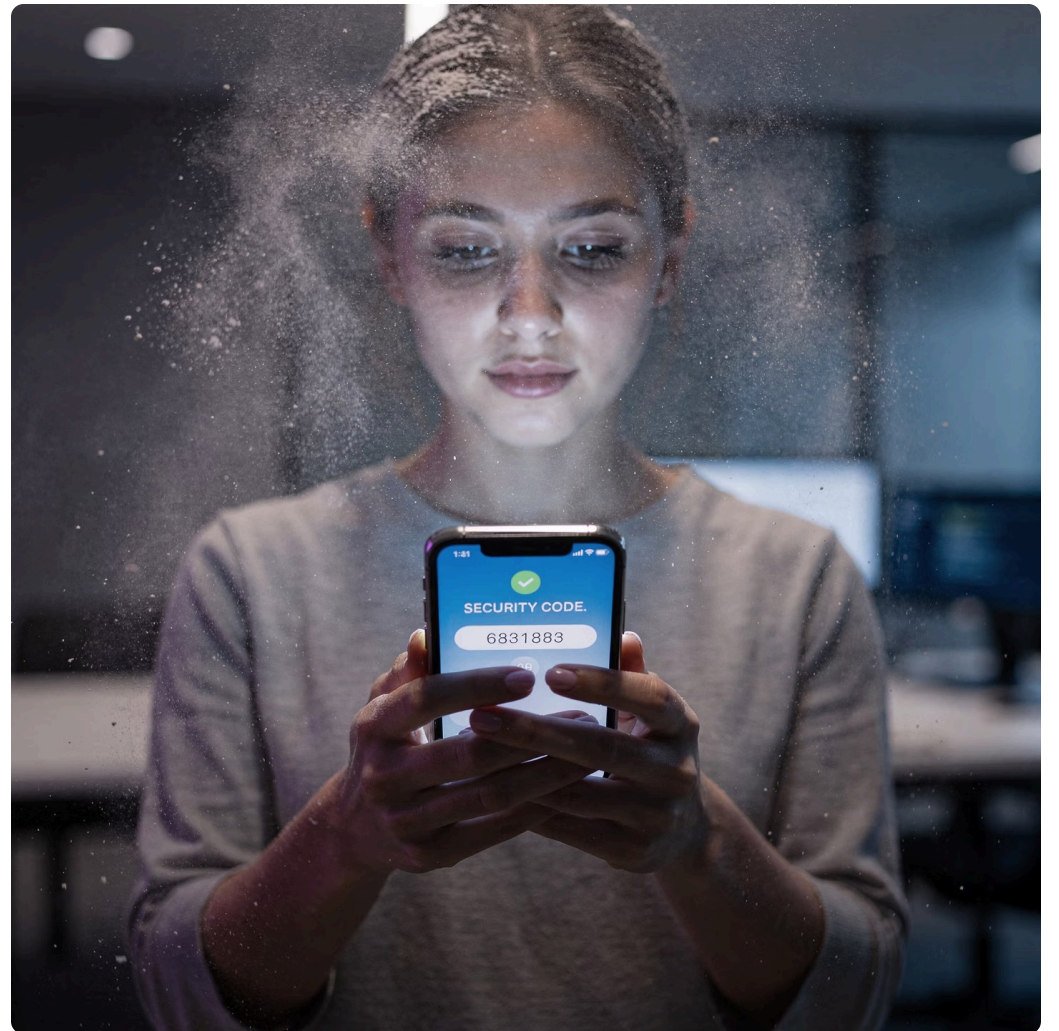
Voor apps die geen standaard Google-login ondersteunen, biedt Google een elegante oplossing: app-wachtwoorden. Dit zijn unieke, automatisch gegenereerde wachtwoorden van 16 tekens die je eenmalig invoert in je app. Je vindt deze functie in je Google-accountinstellingen onder 'Beveiliging' en dan 'App-wachtwoorden'. Let op: deze functie is alleen beschikbaar als je tweestapsverificatie hebt ingeschakeld. Het gebruik van app-wachtwoorden is veel veiliger dan je hoofdwachtwoord delen met apps van derden.

Google-account herstellen en beveiligen

Als je echt je Google-wachtwoord bent vergeten of om een andere reden geen toegang hebt tot je account, heeft Google een uitgebreid herstelproces. Daarnaast is het verstandig om je account proactief te beveiligen om toekomstige problemen te voorkomen. Google neemt beveiliging zeer serieus en biedt verschillende tools om je account te beschermen.

Het herstelproces stap voor stap

1. Ga naar accounts.google.com en klik op 'Wachtwoord vergeten'
2. Voer je Gmail-adres of telefoonnummer in dat aan je account is gekoppeld
3. Google vraagt je het laatste wachtwoord in te voeren dat je nog weet - probeer je best, maar klik anders op 'Probeer op een andere manier'
4. Kies hoe je een verificatiecode wilt ontvangen: via sms naar je geregistreerde telefoonnummer of via e-mail naar je herstel-e-mailadres
5. Voer de ontvangen code in (deze is 10 minuten geldig)
6. Maak een nieuw, sterk wachtwoord aan van minimaal 8 tekens



Controleer je accountactiviteit

Google houdt gedetailleerd bij waar en wanneer je account wordt gebruikt. Ga naar 'Mijn account' en klik op 'Beveiligingscontrole' om recente inlogactiviteiten te bekijken. Zie je verdachte activiteit - zoals inlogpogingen vanaf onbekende locaties of apparaten - dan kun je deze sessies onmiddellijk beëindigen en je wachtwoord wijzigen.

Wijzig wachtwoord regelmatig

Hoewel je niet elke maand je wachtwoord hoeft te veranderen (dit kan juist leiden tot zwakkere wachtwoorden), is het wel verstandig om dit jaarlijks of na een beveiligingsincident te doen. Gebruik nooit hetzelfde wachtwoord voor meerdere accounts, en overweeg een wachtwoordmanager om sterke, unieke wachtwoorden bij te houden.

Activeer tweestapsverificatie

Dit is verreweg de belangrijkste beveiligingsmaatregel die je kunt nemen. Bij tweestapsverificatie heb je naast je wachtwoord een tweede vorm van identificatie nodig - meestal een code van je telefoon. Zelfs als iemand je wachtwoord zou stelen, kunnen ze zonder toegang tot je telefoon niet inloggen. Ga naar je Google-accountinstellingen en schakel dit vandaag nog in!

Gebruikersnaam kwijt? Zo vind je hem terug

Soms is het probleem niet je wachtwoord, maar weet je simpelweg niet meer welke gebruikersnaam of welk e-mailadres je hebt gebruikt bij het aanmaken van je account. Dit komt vaker voor dan je denkt, vooral als je meerdere e-mailadressen gebruikt of als je account al jaren geleden hebt aangemaakt. Gelukkig zijn er verschillende manieren om je gebruikersnaam terug te vinden.

1

Zoek in je e-mail inbox

Wanneer je een account aanmaakt bij Microsoft of Google, ontvang je altijd een welkomst- of bevestigingsmail. Deze e-mail bevat je volledige gebruikersnaam of e-mailadres. Zoek in al je e-mail accounts naar termen als 'welkom', 'bevestig je account', 'account aangemaakt', 'Microsoft', 'Google', of 'verificatie'.

Check niet alleen je inbox, maar ook je spam- of prullenbak. Deze mails kunnen jaren oud zijn, dus scrollaar ver terug of gebruik de zoekfunctie van je e-mailprogramma. Als je gebruik maakt van meerdere e-mailaccounts, doorzoek ze allemaal - je weet nooit waar die bevestigingsmail terecht is gekomen.

2

Probeer in te loggen met alternatieven

Zowel Microsoft als Google staan toe dat je inlogt met verschillende typen gebruikersnamen. Bij Microsoft kun je vaak inloggen met je e-mailadres, telefoonnummer of Skype-naam. Bij Google kun je proberen in te loggen met je volledige Gmail-adres (inclusief @gmail.com), maar ook met alleen je gebruikersnaam zonder het domein.

Probeer ook varianten van je naam die je mogelijk hebt gebruikt: voornaam.achternaam, voornaam_achternaam, voornaamachternaam, enzovoort. Als je je telefoonnummer hebt gekoppeld aan je account, probeer dan ook daarmee in te loggen.

3

Gebruik de 'gebruikersnaam vergeten' functie

Beide diensten hebben een speciale hersteloptie voor verloren gebruikersnamen. Bij Microsoft ga je naar account.live.com en klik je op 'Gebruikersnaam vergeten' of 'Account zoeken'.

Bij Google ga je naar accounts.google.com/signin/recovery en klik je op 'E-mailadres vergeten'. Je wordt dan gevraagd om alternatieve informatie in te voeren die gekoppeld is aan je account, zoals een herstel-e-mailadres of telefoonnummer. Als je deze hebt ingesteld, kan de dienst je helpen je gebruikersnaam te achterhalen.

4

Vul gevraagde verificatiegegevens in

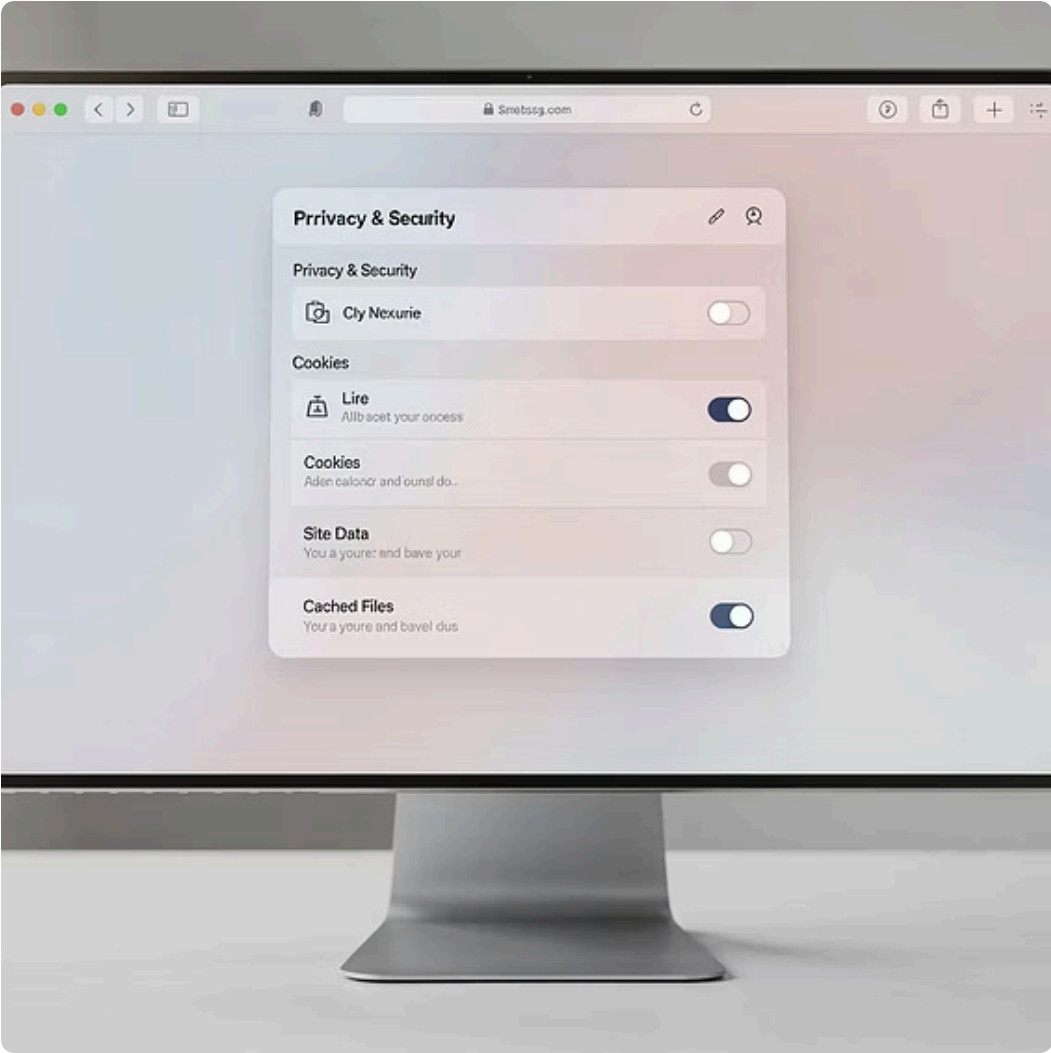
Tijdens het herstelproces vragen Microsoft en Google vaak om aanvullende informatie om je identiteit te verifiëren. Dit kunnen vragen zijn over je geboortedatum, de maand en het jaar waarin je het account hebt aangemaakt, namen van mappen in je account, recente contacten, of zelfs onderwerpen van recente e-mails die je hebt verstuurd.

Hoe meer vragen je correct beantwoordt, hoe groter de kans dat je toegang krijgt tot je accountinformatie. Neem de tijd om na te denken over deze vragen - sommige informatie ligt misschien opgeslagen in oude notities of kan worden nagevraagd bij mensen met wie je regelmatig correspondeert.

Als geen van deze methoden werkt, is het helaas mogelijk dat je permanent de toegang tot je account bent kwijtgeraakt. In dat geval rest weinig anders dan contact opnemen met klantenservice of een nieuw account aanmaken. Probeer wel eerst alle bovenstaande stappen grondig voordat je deze conclusie trekt.

Algemene tips bij inlogproblemen

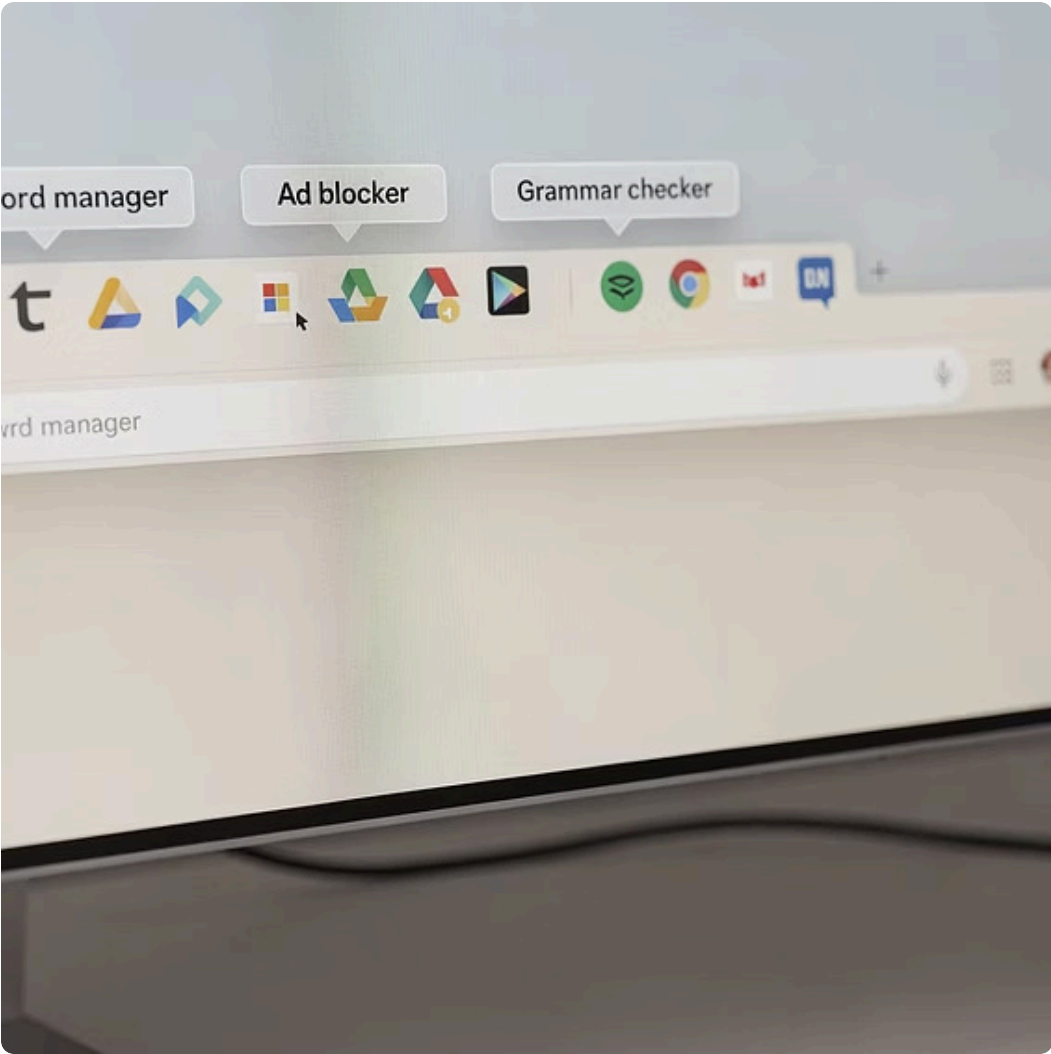
Naast de specifieke oplossingen voor Microsoft en Google zijn er ook algemene technische tips die bij vrijwel elk inlogprobleem kunnen helpen. Deze tips richten zich op je browser en apparaat, en kunnen vaak wonderbaarlijk goed werken wanneer andere methoden falen. Ze zijn bovendien simpel toe te passen en vereisen geen technische kennis.



Wis cookies en cache

Je browser slaat tijdelijke bestanden op die inlogprocessen kunnen verstoren. Oude sessies of corrupte bestanden kunnen ervoor zorgen dat de website denkt dat je al bent ingelogd, of juist dat je login-informatie niet wordt geaccepteerd. Ga naar de instellingen van je browser en zoek naar 'Privacy en beveiliging' of 'Browsegegevens wissen'.

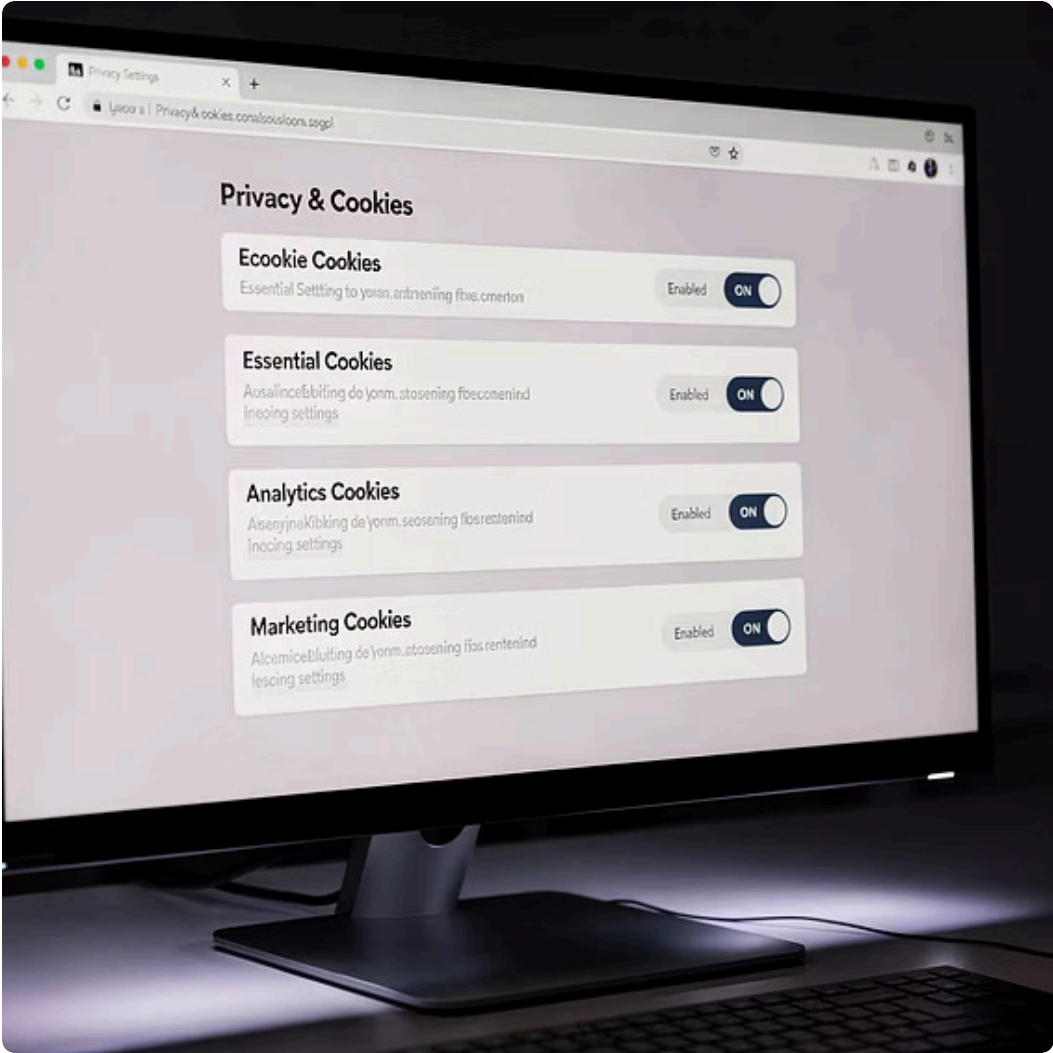
Selecteer 'Cookies en andere sitegegevens' en 'Afbeeldingen en bestanden in cache', en kies ervoor om gegevens te wissen van 'de afgelopen tijd' of 'alles'. Let op: dit logt je uit bij alle websites, dus zorg dat je je wachtwoorden elders hebt opgeslagen.



Schakel extensies tijdelijk uit

Browserextensies zoals adblockers, privacy-tools of beveiligingssoftware kunnen soms te agressief zijn en legitieme inlogprocessen blokkeren. Ad-blockers kunnen bijvoorbeeld inlogformulieren per ongeluk verbergen of het versturen van login-gegevens tegenhouden. Privacy-extensies kunnen cookies blokkeren die nodig zijn voor authenticatie.

Test dit door al je extensies tijdelijk uit te schakelen: in Chrome, Edge en Firefox kun je dit doen via het extensiemenu (puzzelstukje-icoon rechtsboven). Probeer daarna opnieuw in te loggen. Als het nu wel werkt, schakel je extensies één voor één weer in om te ontdekken welke de boosdoener is.



Schakel cookies in

Sommige mensen schakelen cookies uit voor privacyredenen, maar dit kan inloggen onmogelijk maken. Websites zoals Microsoft en Google hebben cookies nodig om je sessie bij te houden en om te verifiëren dat je bent ingelogd. Ga naar je browserinstellingen en zoek naar 'Cookies'.

Zorg dat de optie 'Cookies toestaan' is ingeschakeld, of voeg ten minste microsoft.com en google.com toe aan je lijst met uitzonderingen. Na het inschakelen moet je de pagina verversen en opnieuw proberen in te loggen.



Probeer een andere browser

Soms ligt het probleem simpelweg bij je specifieke browser of browserversie. Probeer in te loggen met een alternatieve browser: als je normaal Chrome gebruikt, test dan Firefox, Edge of Safari. Dit helpt je te bepalen of het probleem browser-specifiek is.

Je kunt ook de 'privémodus' of 'incognito-modus' van je huidige browser proberen - deze modus start zonder extensies en met lege cookies, waardoor je kunt testen of het probleem ligt aan je browserinstellingen. Als inloggen in een andere browser of privémodus wel lukt, weet je dat het probleem te maken heeft met je hoofdbrowser en kun je daar gericht naar een oplossing zoeken.

Wat te doen als niets werkt?

Je hebt alle stappen geprobeerd, alle tips gevolgd, maar je krijgt nog steeds geen toegang tot je account. Frustrerend, maar niet hopeloos. Er zijn nog enkele laatste opties die je kunt proberen voordat je het opgeeft. Deze opties vereisen meer tijd of externe hulp, maar kunnen wel het verschil maken.



Neem contact op met klantenservice

Zowel Microsoft als Google hebben uitgebreide klantenservicekanalen, hoewel deze niet altijd even gemakkelijk te vinden zijn. Voor Microsoft kun je terecht op support.microsoft.com waar je kunt chatten met een medewerker of een callback kunt aanvragen. Voor Google is de hulp wat beperkter, maar via support.google.com kun je formulieren invullen voor accountherstel. Wees voorbereid: je moet waarschijnlijk veel vragen beantwoorden om je identiteit te bewijzen. Houd informatie bij de hand zoals:

- De datum waarop je het account hebt aangemaakt
- Recent gebruikte wachtwoorden
- Namen van mappen, labels of contacten in je account
- Onderwerpen van recente e-mails
- Apparaten waarmee je normaal inlogt

Gebruik eID of digitale identificatie

In sommige landen bieden Microsoft en Google de mogelijkheid om in te loggen met officiële identificatiemethoden zoals eID (elektronische identiteitskaart) of andere door de overheid erkende digitale identiteiten. Dit is vooral nuttig voor zakelijke of overheidsaccounts.

Als deze optie beschikbaar is in je land en je deze eerder hebt gekoppeld, kan dit een snelle manier zijn om weer toegang te krijgen, ook als je je wachtwoord niet meer weet. Check in de instellingen van de inlogpagina of er een optie is voor 'Inloggen met eID' of 'Alternatieve aanmelding'.

Maak een nieuw account aan

Als laatste redmiddel, wanneer alle andere opties zijn uitgeput en klantenservice je niet kan helpen, rest er weinig anders dan een nieuw account aanmaken. Dit is natuurlijk niet ideaal - je verliest toegang tot al je oude e-mails, bestanden en contacten. Maar soms is het onvermijdelijk.

Voordat je deze stap neemt, probeer dan echt grondig alle herstelopties die we in dit document hebben besproken. Maak van de gelegenheid gebruik om ditmaal je account beter te beveiligen: stel herstel-e-mailadressen en telefoonnummers in, activeer tweestapsverificatie, en bewaar je inloggegevens op een veilige plek.

 **Belangrijke waarschuwing:** Wees altijd alert op oplichters die beweren je te kunnen helpen met accountherstel tegen betaling. Zowel Microsoft als Google bieden gratis hersteldiensten aan. Vertrouw nooit mensen die via e-mail, telefoon of social media contact met je opnemen en beweren van Microsoft of Google te zijn - deze bedrijven nemen nooit ongevraagd contact op over accountproblemen. Gebruik alleen de officiële websites en supportkanalen.

Samenvatting: altijd toegang tot je account herstellen

Na het doorlopen van alle informatie in dit document heb je nu een compleet overzicht van hoe je inlogproblemen bij Microsoft en Google kunt oplossen. Laten we de belangrijkste punten nog eens samenvatten, zodat je precies weet wat je moet doen wanneer je de volgende keer een inlogprobleem tegenkomt.

Controleer altijd de basics eerst

Voor je diep in herstelprocessen duikt, verifieer eerst de simpele zaken: typfouten in je gebruikersnaam of wachtwoord, Caps Lock die aan staat, het verkeerde e-maildomein (@outlook.com vs @hotmail.com), of een spatie die per ongeluk is toegevoegd. Deze kleine details zijn verantwoordelijk voor het merendeel van alle inlogproblemen. Neem de tijd om je invoer zorgvuldig te controleren - het kan je veel tijd en frustratie besparen.

Gebruik officiële herstelpagina's

Zowel Microsoft als Google hebben goed functionerende accountherstelsystemen. Voor Microsoft ga je naar account.live.com/acsrr en voor Google naar accounts.google.com/signin/recovery. Gebruik alleen deze officiële websites - nooit links uit e-mails van onbekende afzenders of websites die beweren je sneller te kunnen helpen. Volg de stappen systematisch en geef eerlijke antwoorden op verificatievragen.

Houd software en apps actueel

Verouderde browsers, besturingssystemen en apps kunnen compatibiliteitsproblemen veroorzaken die inloggen onmogelijk maken. Dit geldt vooral voor oudere versies van Internet Explorer, verouderde e-mailclients zoals Outlook 2010 of eerder, en apps van derden die niet meer worden ondersteund. Zorg dat je altijd de nieuwste versies gebruikt van je browser en apps die verbinding maken met je accounts. Schakel automatische updates in waar mogelijk.

Beveilig je account proactief

Tweestapsverificatie is de beste bescherming die je kunt hebben. Het voorkomt dat anderen toegang krijgen tot je account, zelfs als ze je wachtwoord weten. Daarnaast is het verstandig om herstel-e-mailadressen en telefoonnummers toe te voegen, zodat je altijd een manier hebt om je account te herstellen. Gebruik sterke, unieke wachtwoorden voor elk account, en overweeg een wachtwoordmanager om deze bij te houden. Voor apps die geen moderne authenticatie ondersteunen, gebruik app-specifieke wachtwoorden in plaats van je hoofdwachtwoord.

Blijf kalm en systematisch

Inlogproblemen kunnen stressvol zijn, vooral wanneer je dringend toegang nodig hebt tot belangrijke informatie. Maar paniek helpt niet - het leidt vaak juist tot meer fouten. Neem de tijd om elke stap zorgvuldig te doorlopen, maak notities van wat je hebt geprobeerd, en wees geduldig. In de meeste gevallen is er een oplossing, en met de informatie uit dit document ben je goed uitgerust om die te vinden. Als je er echt niet uitkomt, is professionele hulp beschikbaar via de officiële supportkanalen.

Met deze kennis en tips ben je goed voorbereid om nagenoeg elk inlogprobleem aan te pakken. Bewaar dit document voor toekomstig gebruik, en deel het gerust met anderen die mogelijk soortgelijke problemen ervaren. Succes met het herstellen van je account!

A modern computer monitor sits on a wooden desk. The screen displays a macOS desktop environment. On the left side of the screen, a grid of folders is visible, including 'Desktop', 'Documents', 'Downloads', 'Music', 'Pictures', 'Public', 'Videos', and 'Work'. At the bottom of the screen, a dock contains various application icons such as Finder, Safari, Mail, Photos, App Store, Messages, Maps, Notes, Reminders, Calendar, and System Preferences. The desk also holds a small potted plant, a keyboard, a mouse, and a closed notebook. The background is a dark, textured wall.

**Mappen vastmaken aan de taakbalk:
Eén klik naar je favoriete map**

Ontdek hoe je met een eenvoudige truc je meest gebruikte mappen direct toegankelijk maakt vanaf je Windows-taakbalk. Deze gids leidt je stap voor stap door het proces om je workflow te optimaliseren en kostbare tijd te besparen.

Voor je begint:

Windows 11 tip

In Windows 11 is het proces vaak nog eenvoudiger geworden. Je kunt sommige mappen direct naar de taakbalk slepen zonder de aanpassing van het doelpad. Probeer eerst de directe methode – als deze werkt, scheelt het je een paar stappen!

Waarom mappen vastmaken aan de taakbalk?



In de moderne digitale werkruimte is snelheid essentieel. Het vastmaken van mappen aan je taakbalk is meer dan alleen een handige shortcut – het is een fundamentele verandering in hoe je met je bestanden omgaat. Door directe toegang tot vaak gebruikte mappen creëer je een efficiëntere werkstroom die je dagelijkse productiviteit aanzienlijk verhoogt.

Denk eens na over hoeveel tijd je dagelijks besteedt aan het navigeren door mappenstructuren. Elke keer dat je Verkenner opent, door verschillende lagen klikt, en zoekt naar die ene specifieke map, verlies je waardevolle seconden. Deze seconden stapelen zich op tot minuten, en minuten tot uren over de loop van een week.



Directe toegang

Geen gedoe meer met zoeken via Verkenner of het bureaublad. Met één enkele klik open je precies de map die je nodig hebt, wanneer je hem nodig hebt.



Verhoogde productiviteit

Bespaar kostbare tijd door veelgebruikte locaties altijd binnen handbereik te hebben. Elke seconde telt in een drukke werkdag.



Gepersonaliseerd startpunt

Je taakbalk wordt een persoonlijke werkruimte die perfect is afgestemd op jouw specifieke behoeften en werkstijl.

De taakbalk transformeert van een simpele app-launcher naar een krachtig commando centrum voor je hele digitale workflow. Door je belangrijkste mappen hier te verzamelen, creëer je een intuïtieve en ergonomische werkplek die naadloos aansluit bij jouw manier van werken.

Stap 1: Maak een snelkoppeling van de map

De eerste stap in het proces is verrassend eenvoudig, maar wel cruciaal voor het eindresultaat. Je begint met het creëren van een snelkoppeling die later als brug zal dienen tussen je map en de taakbalk. Deze methode werkt voor vrijwel elke map op je computer, of het nu gaat om lokale documenten, netwerklocaties of cloudopslag.

01

Open Windows Verkenner

Start Verkenner door op het mappictogram in je taakbalk te klikken, of gebruik de sneltoets Windows-toets + E voor directe toegang.

03

Klik met de rechtermuisknop

Zodra je de juiste map hebt gevonden, klik je met de rechtermuisknop op de map om het contextmenu te openen. Hier vind je allerlei opties voor interactie met de map.

Na het voltooien van deze stappen verschijnt er een nieuwe snelkoppeling op je bureaublad. Dit pictogram ziet er uit als het originele mappictogram, maar heeft een kleine pijl in de hoek om aan te geven dat het een snelkoppeling is. Deze snelkoppeling is momenteel nog een standaard link naar je map, maar in de volgende stap gaan we deze aanpassen om hem geschikt te maken voor de taakbalk.

02

Navigeer naar je gewenste map

Browse door je bestandssysteem en zoek de map op die je frequent gebruikt en graag direct toegankelijk wilt maken. Dit kan een projectmap zijn, je downloadlocatie, of een map met belangrijke documenten.

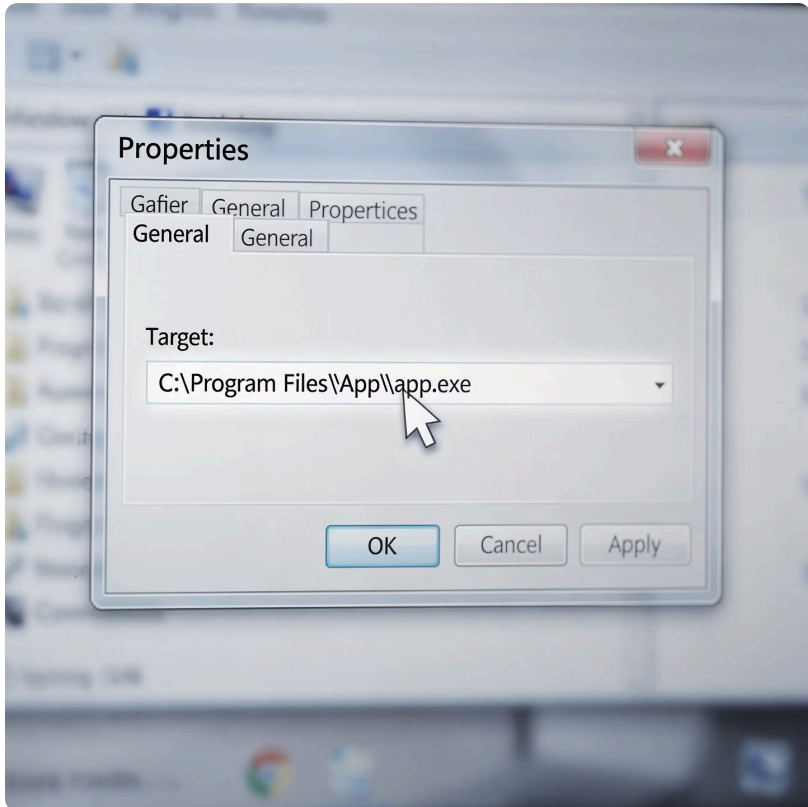
04

Selecteer 'Kopiëren naar'

In het contextmenu, zoek je de optie 'Kopiëren naar' of 'Verzenden naar' (afhankelijk van je Windows-versie) en selecteer vervolgens 'Bureaublad (snelkoppeling maken)'.

 **Let op:** Als de optie 'Aan taakbalk vastmaken' niet direct beschikbaar is voor mappen, geen zorgen – dat is normaal. Windows behandelt mappen anders dan programma's, maar met de volgende stappen omzeilen we deze beperking elegant.

Stap 2: Snelkoppeling aanpassen voor taakbalkvastmaak



Nu komt het slimme deel van de truc. Windows staat normaal gesproken niet toe dat je mappen direct aan de taakbalk vastmaakt – de taakbalk is ontworpen voor programma's en applicaties. Maar met een kleine aanpassing aan het doelpad kunnen we Windows 'overtuigen' dat onze map eigenlijk een uitvoerbaar item is.

Deze technische aanpassing is volkomen veilig en wijzigt niets aan de daadwerkelijke map of de inhoud ervan. Het is simpelweg een manier om de beperkingen van Windows te omzeilen en de functionaliteit te krijgen die je nodig hebt.

Open Eigenschappen

- 1 Klik met de rechtermuisknop op de snelkoppeling die je zojuist op het bureaublad hebt gemaakt. Selecteer 'Eigenschappen' onderaan het contextmenu. Er opent zich nu een nieuw venster met verschillende tabbladen.

Zoek het veld 'Doel'

- 2 In het eigenschapsvenster zie je onder het tabblad 'Snelkoppeling' een veld genaamd 'Doel'. Dit bevat het volledige pad naar je map, bijvoorbeeld: `C:\Gebruikers\JouwNaam\Documenten\MijnMap`

Voeg de magische toevoeging toe

- 3 Plaats je cursor helemaal aan het einde van het pad in het doelveld. Voeg nu een backslash en een punt toe, zodat het pad er zo uitziet: `C:\Gebruikers\JouwNaam\Documenten\MijnMap\.` Deze simpele toevoeging is de sleutel tot succes.

Bevestig de wijziging

- 4 Klik op 'Toepassen' en vervolgens op 'OK' om de eigenschappen op te slaan. Als Windows vraagt om bevestiging, klik dan op 'Doorgaan'. Je snelkoppeling is nu getransformeerd.

"De backslash-punt combinatie (\.) is een elegante oplossing die Windows doet denken dat de map een uitvoerbaar bestand is, waardoor de taakbalk hem accepteert als een geldig item om vast te maken."

Deze aanpassing is het geheim achter de hele methode. Door het pad op deze manier te wijzigen, gedraagt de snelkoppeling zich technisch gezien als een programma in de ogen van Windows, maar opent nog steeds gewoon je map wanneer je erop klikt. Het is een perfecte balans tussen functionaliteit en gebruiksvriendelijkheid.

Stap 3: Vastmaken aan de taakbalk

Je bent nu aangekomen bij de finale en meest bevredigende stap van het proces. Na alle voorbereidende werk is het tijd om je aangepaste snelkoppeling daadwerkelijk aan de taakbalk toe te voegen. Dit moment markeert de transformatie van een gewone map naar een altijd-beschikbare werkruimte-shortcut.



Methode 1: Slepen

Klik en houd de aangepaste snelkoppeling vast op je bureaublad. Sleep het pictogram naar een lege plek op je taakbalk. Je ziet een label verschijnen dat aangeeft waar het pictogram wordt geplaatst.



Methode 2: Contextmenu

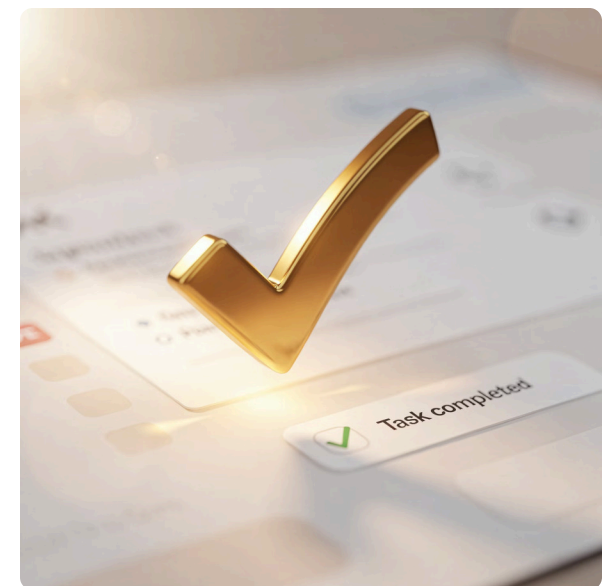
Klik met de rechtermuisknop op de aangepaste snelkoppeling. In het menu dat verschijnt, selecteer je 'Aan taakbalk vastmaken'. Het pictogram verschijnt direct op je taakbalk.

Zodra de map succesvol is vastgemaakt, zie je een nieuw pictogram verschijnen op je taakbalk. Dit pictogram gedraagt zich nu net als elk ander taakbalkitem – je kunt er met één klik op klikken om direct toegang te krijgen tot de map. De map opent zich in Windows Verkenner, precies zoals je zou verwachten, maar zonder al het navigeren.

Wat nu?

Test je nieuwe snelkoppeling meteen uit door erop te klikken. De map zou direct moeten openen in een nieuw Verkenner-venster. Als alles correct is uitgevoerd, heb je nu een volledig functionele map-snelkoppeling op je taakbalk.

Je kunt de snelkoppeling op je bureaublad nu verwijderen als je wilt – de taakbalkversie werkt onafhankelijk en heeft de bureaubladsnelkoppeling niet meer nodig.



- 📌 **Probleemoplossing:** Als het pictogram niet wil vastmaken, controleer dan of je de backslash en punt correct hebt toegevoegd aan het doelpad in stap 2. Dit is de meest voorkomende oorzaak van problemen. Herhaal indien nodig stap 2 en zorg ervoor dat de syntax exact klopt.

Gefeliciteerd! Je hebt zojuist je eerste map succesvol aan de taakbalk vastgemaakt. Dit is echter pas het begin – je kunt dit proces herhalen voor alle mappen die je regelmatig gebruikt, en zo een volledig gepersonaliseerd commando centrum creëren op je taakbalk.

Extra tips voor efficiënt gebruik

Nu je de basistechniek onder de knie hebt, is het tijd om je taakbalk-setup naar het volgende niveau te tillen. Met een aantal slimme strategieën en aanvullende tips kun je een werkelijk krachtig systeem bouwen dat perfect aansluit bij jouw persoonlijke workflow. De kunst zit hem in het vinden van de juiste balans tussen toegankelijkheid en overzicht.



Maak meerdere mappen vast

Beperk jezelf niet tot één map. Je kunt dezelfde methode gebruiken voor al je belangrijke locaties: je werkprojecten, downloadmap, documentenarchief, of zelfs specifieke klantmappen. Bouw een complete toolkit van snelkoppelingen.



Gebruik visuele distinctie

Overweeg om aangepaste pictogrammen toe te wijzen aan verschillende mappen om ze gemakkelijker herkenbaar te maken. Klik hiervoor op 'Pictogram wijzigen' in de eigenschappen van de snelkoppeling voordat je deze vastmaakt.



Organiseer strategisch

Sleep pictogrammen op de taakbalk naar links of rechts om ze te herschikken. Plaats je meest gebruikte mappen aan de linkerkant voor snelle toegang, en minder frequente mappen verder naar rechts. Creëer een logische volgorde die jouw werkproces weerspiegelt.



Houd het overzichtelijk

Wees selectief met wat je vastmaakt. Te veel pictogrammen kunnen de taakbalk onoverzichtelijk maken en het voordeel tenietdoen. Kies alleen voor mappen die je echt dagelijks gebruikt.

Verwijderen en onderhoud

Je workflow verandert in de loop van de tijd, en dat is volkomen normaal. Wanneer je merkt dat een bepaalde map niet langer relevant is of je hem minder vaak gebruikt, kun je deze eenvoudig van de taakbalk verwijderen. Klik met de rechtermuisknop op het pictogram en selecteer 'Van taakbalk losmaken' of 'Losmaken van taakbalk', afhankelijk van je Windows-versie. Het pictogram verdwijnt direct, zonder dat de originele map wordt beïnvloed.

Keyboard shortcuts

Wist je dat je taakbalkitems kunt activeren met toetsencombinaties? Windows-toets + cijfer (1-9) opent het corresponderende item van links naar rechts. Positioneer je belangrijkste map op positie 1 voor ultieme snelheid.

Een pro-tip voor gevorderden: creëer een speciaal mapje op je computer genaamd 'Snelle Toegang' of 'Werkruimte', en verzamel hier snelkoppelingen naar al je belangrijkste locaties, documenten en tools. Maak vervolgens deze hoofdmap vast aan de taakbalk. Met één klik heb je toegang tot je hele gepersonaliseerde toolkit – een hub die naar al je belangrijke plekken verwijst.

Conclusie: Werk slimmer met mappen op de taakbalk

Je hebt nu een krachtige vaardigheid geleerd die je dagelijkse computergebruik fundamenteel kan veranderen. Het vastmaken van mappen aan de taakbalk lijkt misschien een klein dingetje, maar de cumulatieve tijdsbesparing en verhoogde efficiëntie maken een echt verschil in je productiviteit.

Door je favoriete bestanden en projectmappen altijd binnen handbereik te hebben, elimineer je onnodige klikken, verminder je frustratie, en creëer je een werkruimte die perfect is afgestemd op jouw behoeften. Je computer wordt een verlengstuk van je werkproces, in plaats van een obstakel ertussen.



30+

Seconden bespaard

Per keer dat je een map opent via de taakbalk in plaats van te navigeren

15+

Minuten per dag

Gemiddelde tijdsbesparing bij regelmatig gebruik van taakbalk-mappen

100+

Uren per jaar

Die je kunt investeren in écht productief werk in plaats van navigeren

Neem actie vandaag nog

Kennis zonder actie is zinloos. Zet wat je vandaag hebt geleerd direct in praktijk. Identificeer nu meteen drie mappen die je het vaakst gebruikt – misschien je werkprojecten, je downloadmap, en een belangrijke documentenlocatie – en maak ze vast aan je taakbalk. Het kost je slechts vijf minuten, maar de voordelen pluk je elke dag.

"De beste investeringen zijn die welke je tijd vrijmaken om je te focussen op wat echt belangrijk is. Een efficiënte digitale werkruimte is zo'n investering."

Deze eenvoudige aanpassing transformeert je werkproces van reactief naar proactief. In plaats van tijd te verspillen aan het zoeken naar bestanden, besteed je die tijd aan het daadwerkelijk werken met die bestanden. Je computer wordt een tool die voor je werkt, niet een barrière die je moet overwinnen.

Deel deze tip met collega's en vrienden die ook worstelen met bestandsnavigatie. Kleine verbeteringen in werkstroomefficiëntie hebben een domino-effect – wanneer je team productiever werkt, profiteren projecten, deadlines worden makkelijker gehaald, en stress neemt af. Begin vandaag nog met het optimaliseren van je digitale werkruimte, en ervaar zelf het verschil dat één klik kan maken!

A group of seven people are gathered on a bridge at night. Three people are standing in the background, each looking at a smartphone. Four people are sitting on the bridge's edge in the foreground, focused on their devices: two are using laptops, and two are using smartphones. They are dressed in casual evening wear. The background features a row of historic Dutch buildings with illuminated windows, and several bicycles are parked along the bridge railing. The scene is dimly lit, with light from the buildings and street lamps providing the main illumination.

**Meer Nederlanders twifelen aan
online-informatie, ouderen twifelen
het minst**

In het digitale tijdperk worstelen steeds meer Nederlanders met de betrouwbaarheid van online informatie. Terwijl het internet een onuitputtelijke bron van kennis lijkt, groeit tegelijkertijd de twijfel over wat waar is en wat niet. Opmerkelijk genoeg zijn het vooral de jongere generaties die kritisch zijn, terwijl ouderen juist meer vertrouwen tonen in wat ze online tegenkomen. Deze paradox werpt interessante vragen op over digitale geletterdheid, mediagebruik en de manier waarop verschillende leeftijdsgroepen omgaan met de informatiestroom.

Toenemend Wantrouwen in Online Informatie

Het landschap van online informatie verandert snel, en daarmee ook het vertrouwen van Nederlanders. Cijfers uit 2023 laten een duidelijke trend zien: een groeiend deel van de bevolking stelt vraagtekens bij wat ze online tegenkomen. Deze ontwikkeling is niet uniek voor Nederland, maar de intensiteit ervan is opmerkelijk.

Vooraf jonge Nederlanders navigeren door een complexe digitale wereld waarin desinformatie en nepnieuws steeds vaker voorkomen. Hun verhoogde blootstelling aan diverse online bronnen, van sociale media tot nieuwsapps, maakt hen zowel kritischer als kwetsbaarder voor misleidende informatie.



67%

Nederlanders twijfelen

Percentage dat in 2023 twijfelde aan online informatie, gestegen van 63% in 2021

71%

EU-koploper

Nederland heeft het hoogste percentage twijfelaars in de EU, ver boven het gemiddelde van 49%

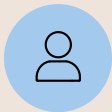
2.5x

Generatiekloof

Jongeren (18-35) ervaren tweeënhalf keer vaker twijfel dan 75-plussers

Ouderen Twijfelen het Minst en Controleren Minder

De cijfers onthullen een fascinerende paradox in het Nederlandse medialandschap: terwijl jongeren het meest twijfelen aan online informatie, zijn het juist de ouderen die minder kritisch lijken te zijn. Deze bevinding roept belangrijke vragen op over digitale vaardigheden en mediawijsheid over verschillende leeftijdsgroepen.



Bepaalde Blootstelling

Ouderen (65+) gebruiken sociale media en online nieuwsplatforms minder intensief, waardoor ze minder vaak misleidende informatie tegenkomen



Opleidingsverschillen

76% van hoger opgeleiden (hbo/universitair) ziet twijfelachtige informatie, tegenover 57% met een vmbo-diploma



Actieve Verificatie

Van wie twijfelt, controleert 66% de informatie via andere nieuwswebsites of Wikipedia; 20% controleert niet omdat ze de informatie al onwaar achten

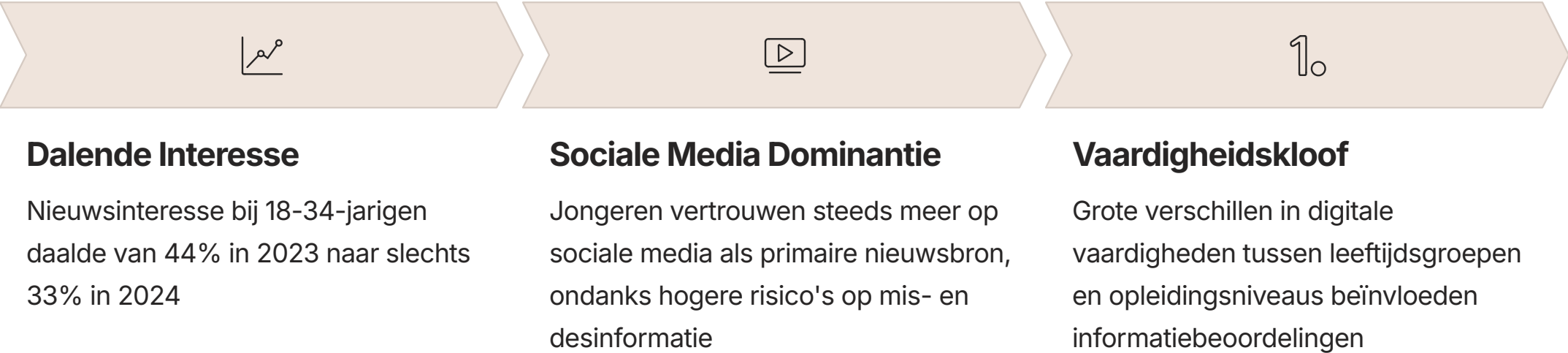
Controlegedrag

Hoger opgeleiden tonen een actievere houding in het verifiëren van twijfelachtige informatie. Ze beschikken over betere digitale vaardigheden en weten waar ze betrouwbare bronnen kunnen vinden.



Impact op Nieuwsgebruik en Digitale Vaardigheden

De verschuivende dynamiek in nieuwsconsumptie heeft verstrekkende gevolgen voor hoe Nederlanders geïnformeerd blijven. De combinatie van dalende nieuwsinteresse en toenemende afhankelijkheid van sociale media creëert een kwetsbare situatie, vooral voor jongere generaties.



Kwetsbare Groepen

Ouderen en lager opgeleiden hebben volgens onderzoek van de Universiteit van Amsterdam in 2024 minder vertrouwen en vaardigheden om online informatie kritisch te beoordelen. Dit maakt hen kwetsbaarder voor misleidende content.

Platformverschuiving

De migratie naar sociale media als nieuwsbron brengt unieke uitdagingen met zich mee. Algoritmes bepalen wat gebruikers zien, waardoor filterbubbels ontstaan en desinformatie zich sneller verspreidt.

Conclusie: Kritisch Blijven en Digitale Vaardigheden Versterken

Het groeiende wantrouwen in online informatie onder Nederlanders, met name onder jongeren, onderstreept de urgentie van sterke digitale geletterdheid. Terwijl jongeren het meest twijfelen, zijn ouderen juist het minst kritisch maar beschikken zij ook over minder digitale vaardigheden. Deze paradox vraagt om een genuanceerde aanpak die alle leeftijdsgroepen bereikt.

Versterking Mediawijsheid

Investeren in digitale geletterdheid en mediavaardigheden voor alle leeftijdsgroepen is essentieel om burgers weerbaar te maken tegen misinformatie en desinformatie

Actieve Verificatie

Stimuleren van kritisch denken en het controleren van bronnen moet centraal staan in educatie. Betrouwbare nieuwsbronnen en fact-checking platforms spelen hierbij een cruciale rol

Inclusieve Digitale Educatie

Speciale aandacht voor ouderen en lager opgeleiden die minder digitale vaardigheden bezitten, met gerichte programma's die aansluiten bij hun behoeften en mogelijkheden

Gezamenlijke Verantwoordelijkheid

Samenwerking tussen overheid, onderwijs en media is noodzakelijk om vertrouwen te herstellen en een informatieecosysteem te creëren waarin betrouwbaarheid voorop staat



"Een goed geïnformeerde burger is de basis van een gezonde democratie. Investeren in digitale vaardigheden is investeren in onze toekomst."

De weg vooruit vereist een collectieve inspanning om alle Nederlanders, ongeacht leeftijd of achtergrond, uit te rusten met de tools om betrouwbare informatie van misleidende content te onderscheiden.

A young person with dark hair, wearing a dark hoodie and large black headphones, is shown in profile, looking intently at a computer monitor. Their hands are positioned on a black keyboard. The room is dimly lit, with the primary light source being the blue glow from the monitor. In the background, a poster is visible on the wall, and a grey jacket hangs on a chair. The overall atmosphere is focused and somewhat somber due to the low lighting.

**Nederlandse studie toont aan dat
cybercriminaliteit onder tieners
vooral slechts een fase is**

Een verrassende ontdekking uit recent Nederlands onderzoek toont aan dat cybercriminaliteit onder jongeren niet het begin is van een criminele carrière, maar eerder een tijdelijke ontwikkelingsfase. Deze inzichten bieden nieuwe perspectieven voor preventie en begeleiding van digitaal vaardige jongeren.

Inleiding: Cybercriminaliteit onder jongeren in Nederland

Het digitale landschap van Nederland kent een opvallende en zorgwekkende trend: ongeveer de helft van alle jongeren tussen 15 en 25 jaar met een ICT-opleiding heeft wel eens een online-delict gepleegd. Van hacking tot phishing, van DDoS-aanvallen tot identiteitsdiefstal – de variëteit aan digitale overtredingen is veelzijdig en complex.

Deze jongeren zijn opgegroeid in een volledig gedigitaliseerde wereld. Ze zijn digitaal native, technisch vaardig en verkennen online grenzen met een gemak dat voor oudere generaties ondenkbaar was. Smartphones, tablets en computers zijn voor hen geen hulpmiddelen, maar natuurlijke extensies van hun sociale en intellectuele leven.



Wat deze statistieken echter niet direct laten zien, is de context achter dit gedrag. Veel jongeren zijn zich simpelweg niet bewust van de juridische consequenties van hun online acties. Een 'onschuldige' hack, bedoeld als technische uitdaging of grap onder vrienden, kan juridisch gezien een ernstig misdrijf zijn met verstrekkende gevolgen.



50% betrokkenheid
Ongeveer de helft van ICT-studenten heeft ervaring met online-delicten



Tijdelijke fase
Cybercriminaliteit wordt gezien als onderdeel van persoonlijke ontwikkeling



Onbewuste overtredingen
Jongeren realiseren zich vaak niet de juridische impact

De belangrijkste verschuiving in het denken over dit fenomeen is de erkenning dat cybercriminaliteit onder tieners steeds vaker wordt beschouwd als een tijdelijke fase in hun ontwikkeling. Het is niet automatisch het begin van een blijvende criminele carrière, maar eerder vergelijkbaar met andere risicovolle gedragingen die adolescenten vertonen tijdens hun zoektocht naar identiteit en grenzen. Deze nieuwe kijk biedt hoopvolle perspectieven voor preventie en interventie, en vraagt om een genuanceerde benadering die onderscheid maakt tussen experimenteel gedrag en werkelijke criminele intenties.

Motieven en sociale context van tieners in cybercriminaliteit

De drijfveren achter cybercrimineel gedrag onder jongeren zijn verrassend divers en vaak fundamenteel anders dan bij volwassen cybercriminelen. Waar volwassenen doorgaans gedreven worden door financieel gewin of kwaadwillende intenties, ontstaat het gedrag van jongeren uit een complexe mix van psychologische en sociale factoren die kenmerkend zijn voor de adolescentie.

- 1

Nieuwsgierigheid en exploratie

Jongeren zijn van nature nieuwsgierig en willen begrijpen hoe systemen werken. Het kraken van een beveiligingssysteem wordt gezien als een intellectuele puzzel, niet als een criminele daad. Deze nieuwsgierigheid is een natuurlijk onderdeel van cognitieve ontwikkeling.
- 2

Behoefte aan erkenning

In online communities en hackfora kunnen jongeren status verwerven door hun technische vaardigheden te demonstreren. Deze sociale erkenning is bijzonder belangrijk in de adolescentie, wanneer identiteitsvorming centraal staat.
- 3

Bewijs van technische competentie

Voor veel jongeren is het succesvol uitvoeren van een hack een manier om hun technische bekwaamheid te bewijzen, zowel aan zichzelf als aan peers. Het gaat om het gevoel van eigenwaarde en meesterschap.

De rol van online leeromgevingen

Online games en hackfora fungeren als informele maar krachtige leeromgevingen waar jongeren spelenderwijs kennis opdoen over hackingtechnieken. Forums leren hen over DDoS-aanvallen, phishing-methoden en kwetsbaarheden in systemen. Deze kennis wordt gedeeld in een context die het experimenteren normaliseert en zelfs aanmoedigt.



De sociale omgeving speelt een cruciale rol in het gedrag van jongeren. Onderzoek toont aan dat adolescenten hun gedrag sterk aanpassen op basis van wat zij denken dat hun vrienden doen – zelfs als deze perceptie niet accuraat is. Dit fenomeen, bekend als 'pluralistic ignorance', betekent dat jongeren cybercrimineel gedrag kunnen vertonen omdat ze denken dat het normaal is binnen hun peergroup, terwijl dit in werkelijkheid niet het geval is.

Belangrijke observatie: Cybercriminaliteit gebeurt vaak volledig onopgemerkt door ouders en scholen. De digitale wereld van jongeren is grotendeels onzichtbaar voor volwassenen, waardoor problematisch gedrag zich kan ontwikkelen en escaleren voordat er interventie plaatsvindt. Dit gebrek aan toezicht en bewustzijn bij volwassenen maakt vroege detectie en preventie bijzonder uitdagend.

Cybercriminaliteit als fase: bewijs uit Nederlandse studies

Nederlands wetenschappelijk onderzoek heeft cruciale inzichten opgeleverd die de perceptie van jeugdcybercriminaliteit fundamenteel veranderen. Studies uitgevoerd door de Vrije Universiteit Amsterdam in samenwerking met het Nederlands Studiecentrum Criminaliteit en Rechtshandaving (NSCR) tonen aan dat cybercrimineel gedrag onder jongeren een veel genuanceerder beeld vertoont dan voorheen werd aangenomen.



Het meest opvallende resultaat van deze onderzoeken is de ontdekking dat veel jongeren die betrokken zijn bij cyberdelicten tegelijkertijd ook constructief en positief ICT-gedrag vertonen. Ze ontwikkelen software, helpen vrienden met computerproblemen, of dragen bij aan open-source projecten. Dit duidt op een experimentele fase waarin jongeren zowel de donkere als de lichte kant van hun technische vaardigheden verkennen, zonder een duidelijke keuze voor een criminele richting.

Monitor Jeugdcriminaliteit 2024

De Monitor Jeugdcriminaliteit 2024 bevestigt dat cybercriminaliteit onder jongeren in Nederland toeneemt. Echter, en dit is cruciaal, deze toename leidt vaak niet tot langdurige criminele betrokkenheid. De meeste jongeren stoppen met cybercrimineel gedrag wanneer ze ouder worden, verantwoordelijkheden krijgen en de consequenties beter begrijpen.

Stopt na adolescentie
Van jongeren die cyberdelicten plegen

Toont positief gedrag
Tegelijkertijd met risicovol gedrag

Nederlandse preventieprogramma's in actie

Op basis van deze wetenschappelijke inzichten zijn verschillende innovatieve preventieprogramma's ontwikkeld die specifiek gericht zijn op Nederlandse jongeren. Deze programma's erkennen dat repressie alleen niet werkt, en dat educatie en begeleiding effectievere instrumenten zijn.

HackShield

Een educatief programma dat jongeren bewust maakt van de risico's van cybercriminaliteit en tegelijkertijd hun interesse in ethisch hacken stimuleert

Mijn Cyberrijbewijs

Een initiatief dat jongeren leert over digitale veiligheid, privacy en verantwoord online gedrag, vergelijkbaar met een rijbewijs voor de digitale wereld

re_BOOTCMP

Een intensief programma voor jongeren met IT-talent die de grenzen hebben opgezocht, gericht op het behouden van talent en het voorkomen van verder daderschap

Deze interventies zijn gebaseerd op het principe dat jongeren met technisch talent niet verloren moeten gaan voor de samenleving, maar juist moeten worden begeleid richting constructieve toepassingen van hun vaardigheden. Het re_BOOTCMP programma is bijzonder innovatief omdat het specifiek werkt met jongeren die al een eerste overtreding hebben begaan, en hen helpt om hun pad te corrigeren voordat er een patroon ontstaat. Door deze jongeren uit te dagen met ethische hackprojecten en hen in contact te brengen met professionals uit de cybersecuritysector, wordt hun talent erkend en wordt een positieve carrière richting mogelijk gemaakt.

Conclusies en aanbevelingen voor beleid en preventie

De Nederlandse studies naar cybercriminaliteit onder tieners leiden tot belangrijke conclusies die de basis vormen voor effectief beleid en gerichte preventiestrategieën. Het fundamentele inzicht dat cybercrimineel gedrag onder adolescenten vaak een experimentele, tijdelijke fase is, vereist een benadering die onderscheid maakt tussen interventie en criminalisering.



Vergroten van cyberweerbaarheid en risicobewustzijn

Het vergroten van cyberweerbaarheid en risicobewustzijn bij jongeren is niet alleen cruciaal voor het voorkomen van eerste overtredingen, maar ook om herhaling en escalatie te voorkomen bij jongeren die al experimenteel gedrag hebben vertoond. Dit vereist een geïntegreerde aanpak die zowel de technische als de ethische dimensies van digitaal burgerschap adresseert. Jongeren moeten leren dat hun acties online reële consequenties hebben voor andere mensen, organisaties en voor henzelf.

Essentiële samenwerking

- Scholen moeten digitaal burgerschap structureel opnemen in het curriculum
- Ouders hebben toegankelijke informatie nodig over de digitale leefwereld van hun kinderen
- Politie en justitie moeten maatwerk bieden bij first offenders
- Gemeenten coördineren lokale preventie en zorgen voor laagdrempelige hulp
- ICT-sector biedt alternatieve carrièrepaden voor technisch talent



Samenwerking tussen scholen, ouders, politie en gemeenten is essentieel om vroegtijdig signalen op te vangen en passende interventies te bieden. Deze ketensamenwerking moet gebaseerd zijn op vertrouwen en informatie-uitwisseling, waarbij de privacy van jongeren gerespecteerd wordt maar signalen van risicovol gedrag snel kunnen worden opgepakt. Scholen hebben hierin een sleutelpositie omdat zij dagelijks contact hebben met jongeren en een natuurlijke setting bieden voor preventie-educatie.

Investeren in positieve ICT-vaardigheden		Bieden van constructieve alternatieven		Erkennen en belonen van talent
---	---	---	---	---------------------------------------

Investeren in positieve ICT-vaardigheden en het bieden van alternatieven voor crimineel gedrag kan jongeren helpen hun talenten constructief in te zetten. Dit betekent concreet: hackathons organiseren, stages aanbieden bij cybersecuritybedrijven, certificeringen mogelijk maken voor ethical hacking, en jonge talenten in contact brengen met positieve rolmodellen uit de ICT-sector. Wanneer jongeren zien dat hun vaardigheden gewaardeerd worden en tot interessante carrières kunnen leiden, vermindert de aantrekkingskracht van cybercriminele activiteiten aanzienlijk.

**Cruciale aanbeveling:** Ouders en professionals moeten beter geïnformeerd worden over de digitale leefwereld van jongeren om adequaat te kunnen ondersteunen. Dit vereist toegankelijke informatiebronnen, trainingen voor ouders en docenten, en een cultuuromslag waarbij digitale opvoeding net zo belangrijk wordt geacht als traditionele opvoedingsthema's.

De weg vooruit vereist een paradigmaverschuiving: van het criminaliseren van experimenterende adolescenten naar het begeleiden van digitaal talent. Nederland heeft met zijn sterke infrastructuur, innovatieve onderwijsstelsel en progressieve jeugdzorg alle middelen om hierin internationaal voorop te lopen. Door cybercriminaliteit onder tieners te erkennen als wat het vaak is – een fase van ontwikkeling en exploratie – kunnen we effectievere strategieën ontwikkelen die niet alleen criminaliteit voorkomen, maar ook bijdragen aan het ontwikkelen van de cybersecurityprofessionals die onze digitale samenleving zo hard nodig heeft.



One-click-fraude: hoe één tik op een link al foute boel kan zijn

In het digitale tijdperk kan één onschuldige klik op een link verstreckende gevolgen hebben. One-click-fraude is een van de snelst groeiende vormen van cybercriminaliteit, waarbij criminelen misbruik maken van onze natuurlijke neiging om snel op links te klikken zonder na te denken. Deze gids biedt inzicht in de gevaren en beschermt u tegen deze digitale dreiging.

Wat is one-click-fraude en waarom is het zo gevaarlijk?

One-click-fraude is een geraffineerde vorm van cybercriminaliteit waarbij een enkele klik op een link al kan leiden tot ernstige schade. Dit kan variëren van malware-infecties en identiteitsdiefstal tot directe financiële fraude. Het gevaar schuilt in de schijnbare onschuld van de handeling: een simpele klik lijkt harmlos, maar kan catastrofale gevolgen hebben.

Cybercriminelen zijn meesters in het camoufleren van hun aanvallen. Ze verstoppen schadelijke software of valse websites achter links die er op het eerste gezicht volkomen legitiem uitzien. Deze frauduleuze links duiken op in phishingmails die lijken te komen van je bank, in sms'jes (ook wel smishing genoemd) die urgent lijken, of in social media berichten van schijnbaar betrouwbare contacten.



Het meest verontrustende aspect van one-click-fraude is dat zelfs een snelle klik zonder verdere actie al toegang kan geven tot je apparaat of persoonlijke gegevens. Je merkt het vaak niet direct, waardoor de schade ongemerkt kan doorlopen. Een veelvoorkomend scenario is dat je wordt doorgeleid naar een nep-inlogpagina die er identiek uitziet aan de echte website van je bank of sociale media platform. Zonder het te beseffen geef je je wachtwoord rechtstreeks aan criminelen.



Phishing via e-mail

Vervalste berichten van banken, overheidsinstanties of bekende bedrijven met urgente oproepen



Smishing via SMS

Tekstberichten met links naar nepwebsites of malware, vaak met pakketbezorging als smoesje



Social media

Frauduleuze posts of directe berichten die je doorsturen naar gevaarlijke websites

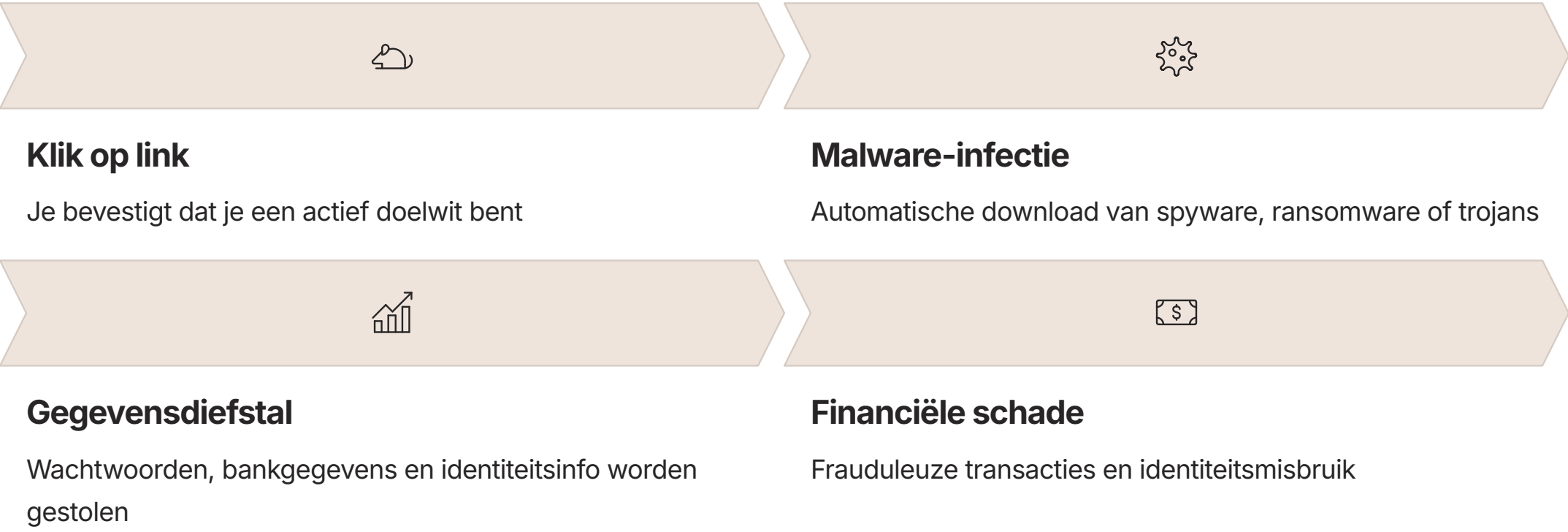
De directe gevolgen van klikken op een frauduleuze link

De gevolgen van het klikken op een frauduleuze link kunnen verstrekkend en langdurig zijn. Het moment dat je klikt, zet je een keten van gebeurtenissen in gang die je digitale leven ernstig kunnen ontwrichten. Het eerste dat gebeurt, is dat je jezelf identificeert als een actief en vatbaar doelwit. Cybercriminelen houden bij wie op hun links klikt en markeren deze personen voor toekomstige, vaak nog gerichtere aanvallen.

Maar de directe technische gevolgen zijn nog verontrustender. Malware kan automatisch worden gedownload zonder dat je het doorhebt. Dit kan verschillende vormen aannemen: spyware die elke toetsaanslag registreert en je wachtwoorden steelt, ransomware die al je bestanden versleutelt en losgeld eist, of trojans die volledige controle over je apparaat overnemen. Deze schadelijke software werkt vaak onzichtbaar op de achtergrond en verzamelt gedurende weken of maanden je gevoelige informatie.

De meest directe financiële schade ontstaat wanneer persoonlijke gegevens worden gestolen. Inloggegevens voor je bankrekening, creditcardinformatie, burgerservicenummers en andere identiteitsgegevens kunnen binnen enkele minuten in handen van criminelen vallen. Deze gegevens worden vervolgens misbruikt voor financiële fraude of doorverkocht op het dark web aan andere criminelen.

**Waarschuwing:** Een recent voorbeeld toont aan hoe gevaarlijk dit kan zijn. Na het klikken op een schijnbaar onschuldige phishinglink ontdekte een slachtoffer plotseling dure online aankopen op haar naam, werden er leningen afgesloten onder haar identiteit, en was haar bankrekening volledig geplunderd. De totale schade bedroeg meer dan €15.000 en het kostte maanden om haar digitale identiteit te herstellen.



Hoe herken je verdachte links en voorkom je one-click-fraude?

Preventie is de beste verdediging tegen one-click-fraude. Door alert te blijven en enkele eenvoudige maar effectieve controles uit te voeren, kun je jezelf beschermen tegen de meeste aanvallen. Het goed nieuws is dat cybercriminelen, hoe slim ze ook zijn, altijd kleine foutjes maken die verdachte links verraden aan de oplettende gebruiker.

01

Controleer de URL zorgvuldig

Beweeg met je muis over de link (hoveren) zonder te klikken om te zien waar deze werkelijk naartoe leidt. Verdachte links bevatten vaak vreemde domeinnamen zoals "ama2on.com" in plaats van "amazon.com", onnodige cijfers, of bizarre toevoegingen zoals extra punten of streepjes. Let vooral op subtiele spelfouten die je makkelijk over het hoofd ziet.

02

Wees op je hoede bij verkorte links

Diensten zoals bit.ly, tinyurl of andere URL-verkorters verbergen de echte bestemming van een link. Hoewel deze diensten legitiem gebruikt kunnen worden, zijn ze ook favoriet bij cybercriminelen omdat ze de werkelijke, vaak verdachte URL maskeren. Gebruik indien mogelijk een URL-expander om de echte bestemming te controleren voordat je klikt.

03

Verifieer onverwachte berichten

Zelfs als een bericht lijkt te komen van je bank, een vriend of een bekende organisatie, klik dan nooit op links in onverwachte berichten. Neem contact op met de afzender via een ander, bekend en betrouwbaar kanaal om te verifiëren of het bericht echt is. Banken en overheidsinstanties vragen nooit via e-mail of sms om op links te klikken voor gevoelige informatie.

04

Gebruik beveiligingssoftware

Installeer betrouwbare beveiligingssoftware die phishing en malware kan detecteren en blokkeren voordat de schade is aangericht. Zorg ervoor dat je besturingssysteem, browser en alle applicaties altijd up-to-date zijn met de laatste beveiligingspatches. Veel succesvolle aanvallen maken gebruik van bekende kwetsbaarheden in verouderde software.



Rode vlaggen bij verdachte links

- Urgentie en dreigementen ("uw account wordt geblokkeerd!")
- Te mooi om waar te zijn aanbiedingen
- Spelfouten en grammaticale fouten in de tekst
- Verzoeken om persoonlijke of financiële informatie
- Afzenders met vreemde e-mailadressen
- Onpersoonlijke aanhef zoals "Beste klant"

Wat te doen als je per ongeluk op een frauduleuze link hebt geklikt?

Zelfs de meest voorzichtige persoon kan een keer een fout maken. Misschien was je afgeleid, moe, of was de phishingpoging bijzonder overtuigend. Het belangrijkste is om niet in paniek te raken, maar snel en doordacht te handelen. Elke seconde telt, want hoe sneller je reageert, hoe meer schade je kunt beperken.

Direct (0-5 minuten)

1

Verbreek onmiddellijk de internetverbinding van je apparaat door WiFi en mobiele data uit te schakelen. Dit voorkomt dat malware verdere communicatie kan opzetten met servers van aanvallers of dat er meer gegevens kunnen worden gestolen. Schakel Bluetooth ook uit voor de zekerheid.

2

Eerste uur

Start een volledige malware-scan met betrouwbare, up-to-date antivirussoftware. Als je deze niet hebt, download deze dan op een ander apparaat en installeer via USB. Verander ondertussen al je wachtwoorden vanaf een ander, veilig apparaat, te beginnen met je meest kritische accounts zoals e-mail en bankzaken.

3

Eerste 24 uur

Neem contact op met je bank en creditcardmaatschappijen om hen te informeren over mogelijk fraude. Vraag om extra monitoring van je rekeningen. Controleer je bankafschriften op verdachte transacties. Als je login-gegevens hebt ingevoerd, blokkeer dan die accounts tijdelijk of zet tweefactorauthenticatie aan voor extra beveiliging.

4

Eerste week

Monitor je accounts dagelijks op ongebruikelijke activiteit. Overweeg een fabrieksreset van je apparaat als de malware-scan iets heeft gevonden of als je apparaat zich vreemd gedraagt. Let op: herstel geen back-ups die mogelijk besmet zijn, gebruik alleen back-ups van vóór de infectie.

5

Langetermijn

Blijf extra alert in de komende maanden. Criminelen kunnen je gegevens langere tijd bewaren voordat ze deze gebruiken. Controleer regelmatig je kredietrapport op ongeautoriseerde leningen of kredietaanvragen. Leer van deze ervaring en train jezelf om toekomstige aanvallen beter te herkennen.

 **Belangrijk:** Doe aangifte bij de politie via politie.nl als je financiële schade hebt geleden of als je identiteitsgegevens zijn gestolen. Dit is niet alleen belangrijk voor eventuele juridische stappen en verzekeringsclaims, maar helpt ook de autoriteiten bij het bestrijden van cybercriminaliteit. Meld het incident ook bij het Digital Trust Center via fraudehelpdesk.nl.

Preventie is beter dan genezen

Gebruik deze ervaring om je digitale weerbaarheid te versterken. Volg cybersecurity-trainingen, blijf op de hoogte van nieuwe dreigingen, en deel je kennis met familie en vrienden om ook hen te beschermen.

Blijf waakzaam

Cybercriminelen evolueren continu en ontwikkelen steeds geavanceerdere methoden. Wat vandaag werkt als bescherming, kan morgen onvoldoende zijn. Blijf kritisch, update regelmatig je kennis, en vertrouw op je intuïtie als iets niet klopt.

A man in a dark suit and light blue shirt is sitting in a black office chair, looking intently at a large computer monitor. The monitor displays a ransomware warning in a web browser window. The warning text reads "RANSOMWARE DETECTED" in large, bold, black letters, followed by "YOUR FILES HAVE BEEN ENCRYPTED" in smaller black letters, and a timer "00:106:13:00". Below the text are three red icons: an information icon (i), and two warning triangles. The background is a dimly lit office with a filing cabinet and stacks of papers on the desk. The overall tone is serious and urgent.

Online politieaangifte ransomware vertraagd door technische uitdagingen

In het huidige digitale tijdperk vormt ransomware een groeiende bedreiging voor zowel bedrijven als zelfstandigen. Hoewel de Nederlandse politie de mogelijkheid biedt om online aangifte te doen van cybercriminaliteit, worstelen slachtoffers met aanhoudende technische problemen die het aangifteproces ernstig vertragen. Deze uitdagingen komen op een moment dat snelheid juist cruciaal is bij het bestrijden van cybercriminelen en het beschermen van gevoelige bedrijfsgegevens.

Het belang van aangifte bij ransomware-aanvallen

Ransomware is een gevaarlijke vorm van malware die computersystemen en bestanden gijzelt door middel van versleuteling. Criminelen eisen vervolgens losgeld om de toegang te herstellen, vaak in cryptocurrency om hun sporen uit te wissen. De gevolgen voor getroffen organisaties zijn verstrekkend: bedrijfsprocessen komen stil te liggen, klantgegevens zijn ontoegankelijk, en de reputatieschade kan aanzienlijk zijn.

Deskundigen en autoriteiten zijn unaniem in hun advies: betaal nooit het gevraagde losgeld. Betaling biedt geen garantie dat u uw bestanden terugkrijgt en draagt bij aan het verdienmodel van criminele organisaties. Sterker nog, bedrijven die betalen worden vaak gezien als makkelijke doelwitten en lopen een verhoogd risico op herhaalde aanvallen.



Opsporing mogelijk maken

Aangifte bij de politie stelt opsporingsdiensten in staat om patronen te herkennen en criminele netwerken te identificeren



Ontsleuteling faciliteren

Verzamelde informatie kan leiden tot ontwikkeling van decryptietools waarmee bestanden zonder losgeld kunnen worden hersteld



Toekomstige aanvallen voorkomen

Inzicht in criminele methodes helpt bij het ontwikkelen van effectievere beveiligingsmaatregelen en waarschuwingssystemen

Het aangifteproces verschilt voor verschillende soorten organisaties. Zelfstandigen kunnen relatief eenvoudig online aangifte doen via de politiewebsite met hun DigiD-inloggegevens. Voor bedrijven ligt dit complexer: zij moeten telefonisch contact opnemen via 0900-8844 om een afspraak te maken met gespecialiseerde digitale rechercheurs. Hierbij is het essentieel om relevante logbestanden, forensische rapportages en communicatie met de aanvallers mee te nemen. Deze gedetailleerde informatie vormt de basis voor effectief politieonderzoek en verhoogt de kans op succesvolle opsporing.

De waarde van aangifte reikt verder dan individuele gevallen. Elke melding draagt bij aan een breder begrip van het cybercriminaliteitslandschap in Nederland. Door gegevens te delen met internationale partners zoals Europol, kunnen grootschalige criminele operaties worden ontmanteld en kunnen tools worden ontwikkeld die slachtoffers wereldwijd helpen hun gegevens te herstellen zonder losgeld te betalen.

Technische uitdagingen bij online aangifte

Hoewel de Nederlandse politie aanzienlijk heeft geïnvesteerd in digitale dienstverlening, blijkt de praktijk weerbarstig. Veel slachtoffers van ransomware-aanvallen stuiten op technische barrières wanneer zij online aangifte willen doen. Formulieren die niet laden, inlogsystemen die vastlopen en foutmeldingen zonder duidelijke uitleg vormen een frustrerende realiteit voor organisaties die juist in een crisissituatie snel actie moeten ondernemen.



Inlogproblemen

DigiD-authenticatie faalt regelmatig of vraagt om herhaalde verificatie, wat het proces vertraagt



Ontoegankelijke formulieren

Aangifteformulieren laden niet correct of tonen foutmeldingen bij het invullen van verplichte velden



Beperkte ondersteuning

Telefonische hulp is beschikbaar maar leidt tot vertragingen voor bedrijven die directe actie nodig hebben

Voor bedrijven die niet online kunnen melden, biedt de politie ondersteuning via het landelijke meldnummer 0900-8844. Hoewel digitale rechercheurs bereid zijn om afspraken te maken en ter plaatse onderzoek uit te voeren, kost dit aanzienlijk meer tijd dan een directe online melding. In de cruciale eerste uren na een aanval, wanneer bewijs nog vers is en systemen mogelijk nog deels toegankelijk zijn, kan elke vertraging de kans op succesvolle opsporing verkleinen.

Technische oorzaken

- Verouderde IT-infrastructuur bij politiesystemen
- Onvoldoende capaciteit tijdens piekperiodes
- Compatibiliteitsproblemen met moderne browsers
- Gebrekkige integratie tussen verschillende systemen
- Ontoereikende gebruikerstests voorafgaand aan implementatie

Gevolgen voor slachtoffers

- Vertraging in het starten van officieel onderzoek
- Verlies van kostbare tijd in crisissituaties
- Extra frustratie bovenop de stressvolle aanvalservaring
- Verhoogd risico op verlies van digitaal bewijs
- Verminderd vertrouwen in digitale overheidsdiensten

Voor gebruikers die technische problemen ervaren met de aangiftesite, bestaat er een helpdesk via helpdesk@poolz.nl. Helaas is dit contactadres niet breed bekend en blijkt de responstijd vaak ontoereikend voor de urgentie van ransomware-situaties. De combinatie van technische storingen en beperkte ondersteuningskanalen creëert een ongewenste drempel voor slachtoffers die juist zo snel mogelijk hun plicht tot melding willen vervullen.

Gevolgen van vertragingen en technische tekortkomingen

De impact van vertragingen in het aangifteproces reikt veel verder dan alleen administratieve ongemakken. Wanneer cruciale uren verstrijken tussen een ransomware-aanval en de officiële melding bij autoriteiten, verdwijnt waardevol digitaal bewijs. Logbestanden worden overschreven, tijdelijke bestanden worden automatisch verwijderd en aanvallers krijgen meer tijd om hun sporen uit te wissen. Dit verzwakt niet alleen individuele onderzoeken, maar ondermijnt ook de bredere strijd tegen cybercriminaliteit.



De technische uitdagingen rond aangifte worden nog gecompliceerder door de wettelijke verplichtingen die organisaties hebben. Ransomware-aanvallen worden in de meeste gevallen ook beschouwd als datalekken, aangezien er ongeautoriseerde toegang tot persoonsgegevens heeft plaatsgevonden. Dit betekent dat organisaties niet alleen aangifte moeten doen bij de politie, maar ook binnen 72 uur melding moeten maken bij de Autoriteit Persoonsgegevens. Deze dubbele druk vereist een soepel werkend aangiftesysteem dat momenteel ontbreekt.



Recente voorbeelden uit 2025 illustreren de harde realiteit waarmee organisaties worden geconfronteerd. Meerdere bedrijven ontvingen boetes wegens onvoldoende IT-beveiligingsmaatregelen, ondanks dat zij aanvallen relatief snel hadden ontdekt en gemeld. De onderliggende problematiek was vaak het niet tijdig installeren van kritieke beveiligingsupdates of het ontbreken van adequate back-upsystemen. Deze gevallen onderstrepen dat zowel preventie als snelle reactie essentieel zijn.

De paradox is pijnlijk: terwijl organisaties worden geacht proactief te zijn in cybersecurity en snel te handelen bij incidenten, worden zij gehinderd door technische systemen die juist die snelle actie belemmeren. Dit creëert een situatie waarin de intentie om correct te handelen wordt gefrustreerd door de middelen die daarvoor beschikbaar zijn gesteld.

Bewijsverlies

Cruciale digitale sporen verdwijnen door vertraging, waardoor opsporing bemoeilijkt wordt en daders langer vrijuit gaan

Juridische consequenties

Organisaties riskeren boetes voor te late melding van datalekken, ook als technische problemen de oorzaak waren

Reputatieschade

Vertraagde respons kan leiden tot negatieve publiciteit en verminderd vertrouwen van klanten en partners

Financiële impact

Langere downtime en herstelprocessen resulteren in hogere kosten en omzetverlies voor getroffen bedrijven

Aanbevelingen en toekomstperspectief

De weg vooruit vereist een gecoördineerde inspanning van meerdere partijen. De Nederlandse politie moet prioriteit geven aan het moderniseren van haar digitale aangifteplatform. Dit betekent investeren in robuuste IT-infrastructuur, uitgebreide gebruikerstests met echte slachtoffers, en het implementeren van duidelijke foutmeldingen met concrete oplossingsrichtingen. Gebruiksvriendelijkheid moet centraal staan, met speciale aandacht voor stressvolle situaties waarin slachtoffers verkeren.

01

Platformmodernisering

Investeer in stabiele, gebruiksvriendelijke systemen met meertalige ondersteuning en 24/7 beschikbaarheid

02

Proactieve voorbereiding

Bedrijven moeten vooraf machtigingen, contactpersonen en documentatie gereed hebben voor snelle aangifte

03

Preventieve maatregelen

Regelmatige back-ups, tijdige updates en beveiligingstrainingen blijven de beste verdediging tegen ransomware

04

Publiek-private samenwerking

Versterk partnerschappen tussen politie, IT-sector en bedrijfsleven voor effectievere cybercrime-bestrijding

Praktische voorbereidingstips voor organisaties

- Zorg voor actuele contactgegevens van relevante bevoegde personen binnen uw organisatie
- Documenteer IT-infrastructuur en bewaar deze veilig offline
- Maak afspraken met forensisch IT-specialisten voordat een incident plaatsvindt
- Test regelmatig back-up- en herstelprocessen onder realistische condities
- Installeer beveiligingsupdates binnen 48 uur na publicatie
- Train personeel in het herkennen van phishing en andere aanvalsvectoren



De toekomst van cybersecurity-aangifte ligt in naadloze integratie tussen preventie, detectie en respons. Geautomatiseerde systemen zouden verdachte activiteiten moeten kunnen signaleren en voorbereidende stappen voor aangifte automatisch kunnen uitvoeren. Dit vergt niet alleen technologische innovatie, maar ook wetgeving die stap houdt met de digitale werkelijkheid. De Autoriteit Persoonsgegevens, politie en IT-sector moeten gezamenlijk protocollen ontwikkelen die zowel juridisch robuust als praktisch uitvoerbaar zijn.

Samenwerking versterken

Publieke en private sector moeten kennis en middelen delen om cybercriminelen voor te blijven

Infrastructuur verbeteren

Investeer in betrouwbare systemen die schaalbaar zijn en onder druk blijven functioneren

Bewustzijn creëren

Doorlopende training en voorlichting maken organisaties weerbaarder tegen aanvallen

Uiteindelijk is het doel een situatie waarin technische barrières geen obstakel meer vormen voor snelle en effectieve melding van cybercriminaliteit. Slachtoffers van ransomware bevinden zich al in een crisissituatie; het aangiftesysteem moet hen ondersteunen in plaats van extra frustratie te veroorzaken. Door te investeren in moderne, gebruiksvriendelijke systemen en door organisaties te helpen zich beter voor te bereiden, kunnen we gezamenlijk de strijd tegen cybercriminaliteit effectiever voeren. De uitdaging is groot, maar met gecoördineerde inspanning en doorlopende verbetering is een veiligere digitale toekomst binnen bereik.



Openbare wifi-routers kunnen je identificeren, zelfs zonder telefoon

Een nieuwe technologie toont aan hoe kwetsbaar onze privacy is in een steeds meer verbonden wereld. Zelfs zonder apparaat bij je te dragen, kunnen wifi-routers je herkennen en volgen.

Hoe wifi-routers mensen herkennen zonder apparaat

Onderzoekers van het Karlsruhe Institute of Technology (KIT) hebben een baanbrekende en verontrustende ontdekking gedaan: commerciële wifi-routers kunnen mensen identificeren via subtiele veranderingen in wifi-signalen. Deze technologie werkt op een manier die voor de meeste gebruikers volledig onzichtbaar blijft.

Het mechanisme achter deze identificatiemethode is gebaseerd op onversleutelde feedbacksignalen, bekend als Beamforming Feedback Information (BFI), die verbonden apparaten automatisch naar de router sturen. Deze signalen brengen de verspreiding van radiogolven in een ruimte nauwkeurig in kaart en creëren als het ware een onzichtbaar beeld van de omgeving.



Signaalverstoringen

Wanneer een persoon door een ruimte beweegt, veroorzaakt dit meetbare verstoringen in de wifi-signalen die door kunstmatige intelligentie kunnen worden geanalyseerd.

Individuele herkenning

AI-algoritmes kunnen deze verstoringen bijna foutloos aan specifieke individuen koppelen, waarbij elke persoon een unieke "signaalvingerafdruk" creëert.

Geen eigen apparaat nodig

Het meest verontrustende aspect is dat dit werkt zelfs als je geen eigen wifi-apparaat bij je hebt of alle apparaten hebt uitgeschakeld, zolang er andere actieve apparaten in de buurt zijn.

Deze technologie maakt gebruik van het feit dat het menselijk lichaam radiogolven absorbeert en reflecteert op een karakteristieke manier. Elke beweging, van lopen tot handgebaren, creëert een uniek patroon in de wifi-signalen dat door geavanceerde machine learning-algoritmes kan worden herkend. De precisie van deze methode is opmerkelijk: zelfs subtiele verschillen in lichaamshouding en bewegingspatronen kunnen worden gedetecteerd en gebruikt voor identificatie.

De privacy- en veiligheidsrisico's van wifi-signaalimaging

KIT-onderzoeker Julian Todt waarschuwt voor de verstreckende gevolgen van deze technologie: elke wifi-router wordt een potentieel surveillance-instrument. Overheden, bedrijven of cybercriminelen kunnen deze techniek gebruiken om mensen onopgemerkt te volgen, zonder dat de betrokkenen daar ook maar enig vermoeden van hebben. De alomtegenwoordigheid van wifi-netwerken maakt dit risico des te groter.



Openbare ruimtes

In cafés, bibliotheken en winkelcentra kunnen bezoekers geïdentificeerd en gevolgd worden via de wifi-infrastructuur, zelfs als ze geen gebruik maken van het netwerk.



Privéomgevingen

Ook thuis of op kantoor kan deze techniek worden misbruikt, waarbij burens of andere partijen mogelijk inzicht krijgen in bewegingspatronen.



Autoritaire regimes

In landen met repressieve overheden kan wifi-tracking leiden tot onderdrukking van demonstranten en dissidenten die via signalen worden opgespoord.

De mogelijkheden voor misbruik zijn legio. In commerciële contexten kunnen bedrijven deze technologie inzetten voor gedetailleerde klantprofilering zonder toestemming.

Retail-omgevingen zouden kunnen bijhouden hoe lang klanten voor bepaalde producten blijven staan, welke routes ze door de winkel nemen, en deze informatie gebruiken voor gerichte marketing of prijsdiscriminatie.

Nog zorgwekkender is het potentieel voor overheidstoezicht. In combinatie met andere surveillance-technologieën zoals gezichtsherkenning en nummerplaatherkenning, zou wifi-signaalimaging een ongekend nauwkeurig beeld kunnen geven van iemands bewegingen en sociale contacten.

De onderzoekers pleiten daarom voor strengere beveiligingsstandaarden, zoals encryptie van feedbacksignalen in toekomstige wifi-protocollen zoals IEEE 802.11bf.

Praktische voorbeelden en impact op gebruikers

197

Proefpersonen

Aantal deelnemers in de KIT-studie die betrouwbaar konden worden geïdentificeerd

99%

Nauwkeurigheid

Identificatiesucces ongeacht loopstijl, perspectief of meegedragen objecten

0

Apparaten nodig

Je hoeft geen eigen apparaat bij je te hebben om geïdentificeerd te worden

De resultaten van de KIT-studie zijn zowel indrukwekkend als verontrustend. Met 197 proefpersonen demonstreerden de onderzoekers dat mensen betrouwbaar herkend kunnen worden ongeacht variabelen die je zou verwachten van invloed te zijn. Of iemand met bagage loopt, een jas draagt, of vanuit verschillende hoeken wordt "waargenomen" door het wifi-netwerk - de identificatie blijft consistent accuraat.



Dit betekent dat openbare wifi-netwerken, die overal aanwezig zijn in winkels, restaurants, luchthavens en stadscentra, onbedoeld een bijna universeel identificatienetwerk vormen. Elke locatie met wifi wordt een potentieel trackingpunt. Voor gewone gebruikers heeft dit verstrekken gevolgen: zelfs het uitschakelen van je telefoon of het bewust niet bij je dragen van elektronische apparaten biedt geen garantie meer tegen identificatie en tracking.

De technologie werkt namelijk indirect: zolang er andere mensen in de ruimte zijn met actieve wifi-apparaten, kunnen de routers jouw bewegingen detecteren en analyseren. Je bent als het ware een "schaduw" in het wifi-signaal van anderen.

"Het uitschakelen van je telefoon beschermt je niet meer tegen identificatie via wifi-signalen. Je bent zichtbaar in de digitale schaduwen van andermans apparaten."

Dit roept urgente vragen op over de huidige staat van wifi-beveiliging en het bewustzijn van privacy bij het gebruik van openbare netwerken. De meeste mensen nemen aan dat ze anoniem zijn als ze geen gebruik maken van een wifi-netwerk of hun apparaten hebben uitgeschakeld. Deze veronderstelling blijkt fundamenteel onjuist te zijn. De passieve aard van deze tracking maakt het extra problematisch: er is geen manier om te weten wanneer je wordt geobserveerd, en er zijn momenteel geen effectieve tegenmaatregelen voor individuele gebruikers.

Conclusie en aanbevelingen voor bescherming

De ontdekking van wifi-signaalimaging is een wake-up call voor iedereen die waarde hecht aan privacy. Onze draadloze netwerken, die we dagelijks gebruiken voor gemak en connectiviteit, blijken veel meer informatie prijs te geven dan we ooit hadden gedacht. Deze technologie heeft verstreckende gevolgen voor zowel persoonlijke privacy als maatschappelijke veiligheid, en vereist dringende actie van meerdere partijen.

01	02
Industrie-actie Fabrikanten en standaardisatie-instellingen moeten encryptie en privacybescherming integreren in wifi-protocollen om misbruik structureel te voorkomen.	Regelgeving Overheden moeten wetgeving ontwikkelen die het ongeautoriseerd gebruik van wifi-tracking expliciet verbiedt en handhaafbaar maakt.
03	04
Bewustwording Publieke voorlichting over deze risico's is essentieel zodat gebruikers geïnformeerde beslissingen kunnen nemen over hun connectiviteit.	Persoonlijke maatregelen Wees voorzichtig met openbare wifi, gebruik VPN's waar mogelijk, en blijf kritisch over de netwerken waarmee je verbindt.

Wat je nu kunt doen

- Beperk het gebruik van openbare wifi-netwerken waar mogelijk
- Gebruik een betrouwbare VPN-dienst voor extra bescherming
- Schakel wifi uit wanneer je het niet actief gebruikt
- Blijf op de hoogte van ontwikkelingen in wifi-beveiliging
- Ondersteun organisaties die pleiten voor betere privacy-wetgeving

Toekomstperspectief

De komende jaren zullen cruciaal zijn voor het bepalen hoe we als samenleving omgaan met deze technologie. Zal wifi-tracking genormaliseerd worden als "de prijs van gemak", of zullen we succesvolle technische en juridische barrières opwerpen?

De keuzes die we nu maken, bepalen of wifi-routers blijven wat ze bedoeld waren - tools voor connectiviteit - of veranderen in onzichtbare surveillancetools die onze fundamentele anonimiteit ondermijnen.

**Belangrijke boodschap:** Deze technologie is niet toekomstig of theoretisch - het werkt nu al met commerciële hardware. Bewustwording en actie zijn niet alleen wenselijk, maar noodzakelijk om onze privacy te beschermen in een steeds meer verbonden wereld.



Overheid lanceert 'Phishkraam' als onderdeel van campagne over phishing

De Nederlandse overheid neemt een nieuwe stap in de strijd tegen online criminaliteit met de lancering van een innovatieve bewustwordingscampagne. In een tijdperk waarin digitale dreigingen steeds verfijnder worden, komt de overheid met concrete hulpmiddelen om burgers te beschermen tegen phishing.

Wat is phishing en waarom is het zo gevaarlijk?



Phishing is internetfraude waarbij criminelen via valse berichten proberen persoonlijke gegevens zoals wachtwoorden en bankgegevens te stelen. Deze vorm van cybercriminaliteit heeft zich ontwikkeld tot een van de meest voorkomende digitale dreigingen in Nederland, met verstrekende gevolgen voor zowel particulieren als bedrijven.

De cijfers liegen er niet om: in 2024 werd in Nederland ruim 39 miljoen euro buitgemaakt via phishing. Nog zorgwekkender is de stijging van het aantal phishingaanvallen van meer dan 40% op bekende Nederlandse merken. Criminelen worden steeds slimmer in het nabootsen van vertrouwde bedrijven en instanties, waardoor zelfs kritische gebruikers voor de gek kunnen worden gehouden.



E-mail phishing
Valse e-mails die lijken van banken of overheidsinstanties te komen



SMS en WhatsApp
Berichten met verdachte links naar nep-websites



QR-codes
Malafide codes die leiden naar phishing-websites

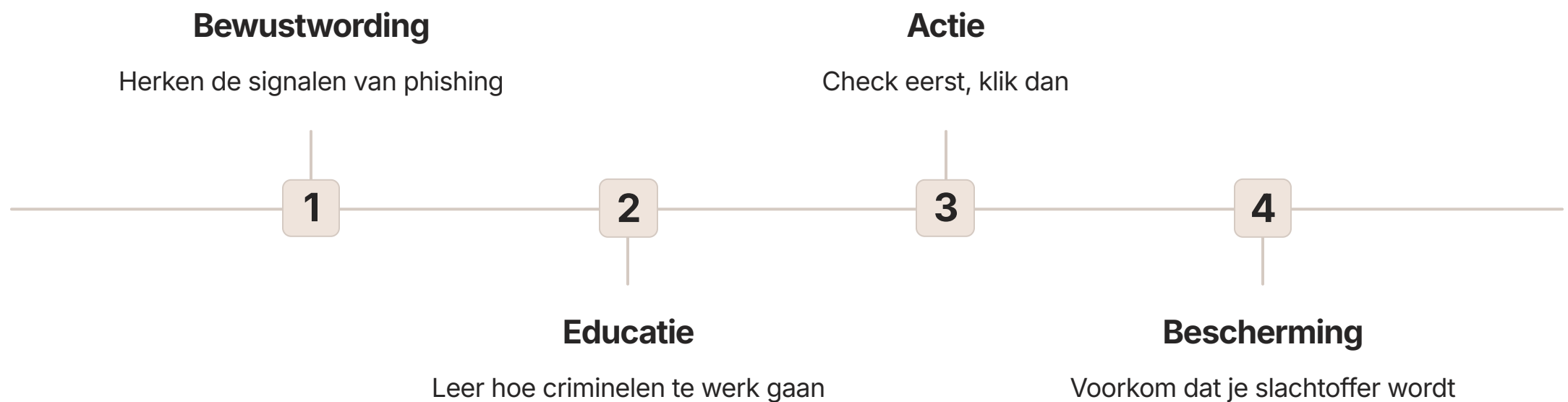


Social media
Vervalste accounts en advertenties op sociale platforms

Phishing gebeurt niet alleen via traditionele e-mail, maar heeft zich uitgebreid naar vrijwel elk digitaal communicatiekanaal. Van sms-berichten en WhatsApp tot QR-codes en social media - criminelen maken gebruik van alle beschikbare middelen om hun slachtoffers te bereiken. Deze veelzijdige aanpak maakt dat niemand immuun is voor deze dreiging, ongeacht leeftijd, technische kennis of voorzichtigheid. De realiteit is dat iedereen kwetsbaar is en dat constante waakzaamheid noodzakelijk is in ons digitale tijdperk.

De nieuwe campagne: 'Phishkraam' en 'Eerst checken, dan klikken'

De Nederlandse overheid heeft de handschoen opgepakt met de lancering van de innovatieve 'Phishkraam'-campagne. Deze grootschalige bewustwordingsactie is specifiek ontworpen om burgers te wapenen tegen de groeiende dreiging van phishing. De campagne combineert educatie met praktische hulpmiddelen en heeft als doel om het herkennen van verdachte berichten een tweede natuur te maken voor alle Nederlanders.



"Eerst checken, dan klikken"

De kernboodschap van de campagne benadrukt het belang van waakzaamheid: controleer altijd eerst de afzender en de link voordat je klikt, om te voorkomen dat je slachtoffer wordt van cybercriminelen.

De campagne wordt breed verspreid via multiple kanalen om maximale impact te bereiken. Televisiereclames, social media-campagnes en strategische samenwerkingen met bedrijven en brancheorganisaties zorgen ervoor dat de boodschap alle lagen van de samenleving bereikt. Door deze geïntegreerde aanpak wordt 'Eerst checken, dan klikken' niet alleen een slogan, maar een gedeelde norm in onze digitale cultuur. Bedrijven spelen een cruciale rol door de campagne intern te delen en hun werknemers bewust te maken van de risico's, terwijl brancheorganisaties zorgen voor verspreiding binnen hun netwerken.

Wat is de 'Phishkraam' en hoe helpt het?



De 'Phishkraam' is het concrete hulpmiddel dat voortkomt uit de overheidscampagne - een geavanceerde online tool en browserextensie die als digitale bodyguard functioneert. Deze innovatieve oplossing helpt gebruikers in real-time phishingwebsites te herkennen door het vertrouwen van bezochte domeinen te beoordelen aan de hand van verschillende veiligheidscriteria.

De technologie achter de 'Phishkraam' analyseert websites op verdachte kenmerken en vergelijkt deze met databases van bekende phishingsites. Wanneer een gebruiker een potentieel gevaarlijke website bezoekt, verschijnt er direct een waarschuwing. Dit voorkomt dat gebruikers onbedoeld persoonlijke gegevens zoals wachtwoorden, bankrekeningnummers of andere gevoelige informatie invoeren op nepwebsites die zich voordoen als legitieme diensten.



Installeer de extensie

Download de Phishkraam-tool gratis voor je browser



Automatische controle

De tool scant elke website die je bezoekt



Ontvang waarschuwingen

Direct melding bij verdachte websites



Surf veilig

Bescherming tegen phishing en datadiefstal

Dit hulpmiddel is geen op zichzelf staand initiatief, maar maakt deel uit van het bredere Safeonweb-platform. Dit platform heeft al jarenlang een bewezen staat van dienst in het geven van betrouwbare tips en actuele waarschuwingen over internetveiligheid. Door de integratie van de 'Phishkraam' in dit ecosysteem krijgen gebruikers toegang tot een complete suite van beveiligingstools en educatief materiaal. Het platform biedt daarnaast up-to-date informatie over nieuwe phishingtrends, waardoor gebruikers altijd op de hoogte blijven van de nieuwste dreigingen en hoe ze zich hiertegen kunnen beschermen.

Praktische tips om phishing te herkennen en te voorkomen

Het herkennen van phishing vereist een scherp oog voor detail en een gezonde dosis scepsis. De volgende praktische tips helpen je om verdachte berichten te identificeren en jezelf te beschermen tegen digitale oplichters.

1

Controleer de afzender

Bekijk het e-mailadres nauwkeurig op spelfouten en afwijkingen. Officiële instanties en banken hebben altijd professionele e-mailadressen. Let op subtiele verschillen zoals extra letters of cijfers in het domein.

- Officiële banken vragen nooit om wachtwoorden via e-mail
- Overheidsinstanties sturen geen sms'jes met betaalverzoeken
- Bedrijven vragen niet om pincode of volledige kaartnummer

2

Herken urgentie

Wees extra alert op berichten die je onder druk zetten om snel te handelen. Zinnen als "binnen 24 uur", "account geblokkeerd" of "onmiddellijke actie vereist" zijn klassieke phishing-tactieken.

- Echte organisaties geven je altijd voldoende tijd
- Dreigingen met accountsluiting zijn vaak vals
- Bij twijfel: bel de organisatie via hun officiële nummer

3

Verifieer links

Klik nooit direct op links in verdachte berichten. Zweef met je muis over een link om het echte webadres te zien voordat je klikt. Bij twijfel zoek je de website zelf op via een zoekmachine.

- Controleer of de URL begint met https://
- Let op spelfouten in de domeinnaam
- Verkorte links kunnen het echte adres verbergen

4

Gebruik extra bescherming

Installeer beveiligingssoftware en maak gebruik van de 'Phishkraam'-extensie. Deze tools bieden een extra laag bescherming en waarschuwen je automatisch voor bekende phishingsites.

- Houd je antivirus software up-to-date
- Activeer tweefactorauthenticatie waar mogelijk
- Gebruik verschillende wachtwoorden per account



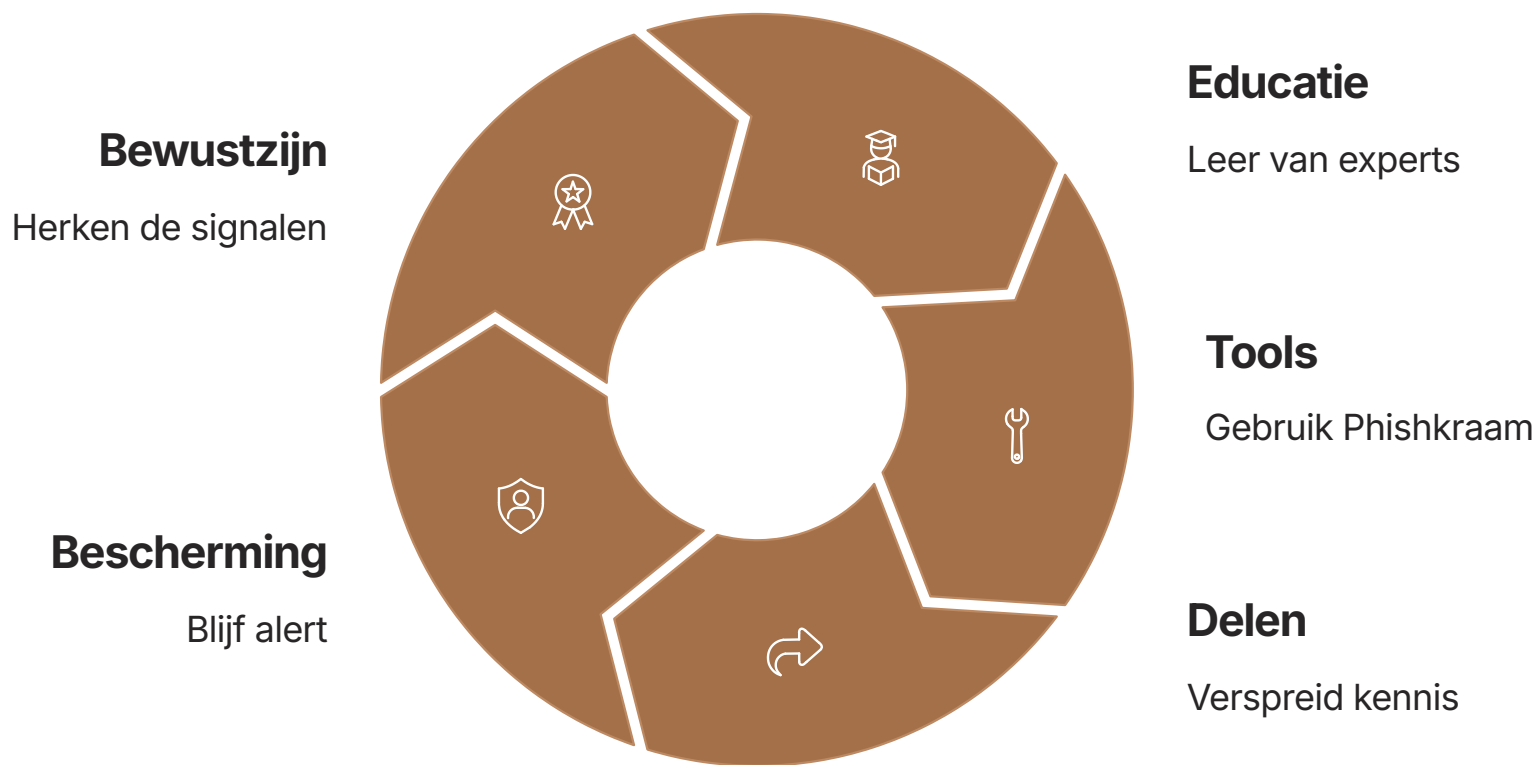
Wat te doen als je toch op een phishing-link hebt geklikt?

Verander onmiddellijk je wachtwoorden, neem contact op met je bank als je bankgegevens hebt ingevuld, en doe aangifte bij de politie. Scan je computer op malware en monitor je rekeningen nauwlettend op ongebruikelijke activiteiten.

Door deze tips te integreren in je dagelijkse digitale routine, bouw je een effectieve verdediging op tegen phishing. Onthoud dat cybercriminelen constant hun tactieken aanpassen, dus blijf je kennis bijwerken en deel deze informatie met familie en vrienden. Samen kunnen we de impact van phishing aanzienlijk verminderen.

Conclusie: Samen sterk tegen phishing

Phishing blijft een groeiende en evoluerende bedreiging die iedereen kan treffen, ongeacht achtergrond, technische kennis of voorzichtigheid. Van particulieren die hun spaargeld verliezen tot bedrijven die geconfronteerd worden met datalekken en reputatieschade - de impact van phishing kent vele gezichten. De cijfers spreken voor zich: met 39 miljoen euro aan schade in 2024 en een stijging van 40% in het aantal aanvallen, is duidelijk dat we te maken hebben met een serieuze en urgente digitale dreiging.



De 'Phishkraam'-campagne en bijbehorende tools zoals de browserextensie zijn cruciale initiatieven om Nederlanders bewuster en weerbaarder te maken tegen deze digitale dreiging. Door de combinatie van educatie, praktische hulpmiddelen en brede verspreiding via verschillende kanalen, creëert de overheid een solide fundament voor een veiliger digitaal Nederland. De browserextensie biedt real-time bescherming, terwijl de campagneboodschap 'Eerst checken, dan klikken' een nieuwe standaard zet voor online gedrag.

Digitale veiligheid is een gedeelde verantwoordelijkheid. Alleen door samen alert te blijven, kennis te delen en gebruik te maken van beschikbare tools, kunnen we de strijd tegen phishing effectief voeren.

De boodschap is helder: blijf alert, leer verdachte signalen herkennen en deel je kennis actief met anderen. Of het nu gaat om het waarschuwen van een ouder familielid voor een verdachte e-mail, het informeren van collega's over nieuwe phishing-tactieken, of simpelweg het installeren van de Phishkraam-extensie - elke actie telt. Door collectief onze digitale weerbaarheid te versterken, kunnen we de impact van phishing significant beperken en bouwen we aan een veiliger digitaal ecosysteem voor iedereen. De tools zijn beschikbaar, de kennis wordt gedeeld - nu is het aan ons om deze te gebruiken en te blijven investeren in onze digitale veiligheid.



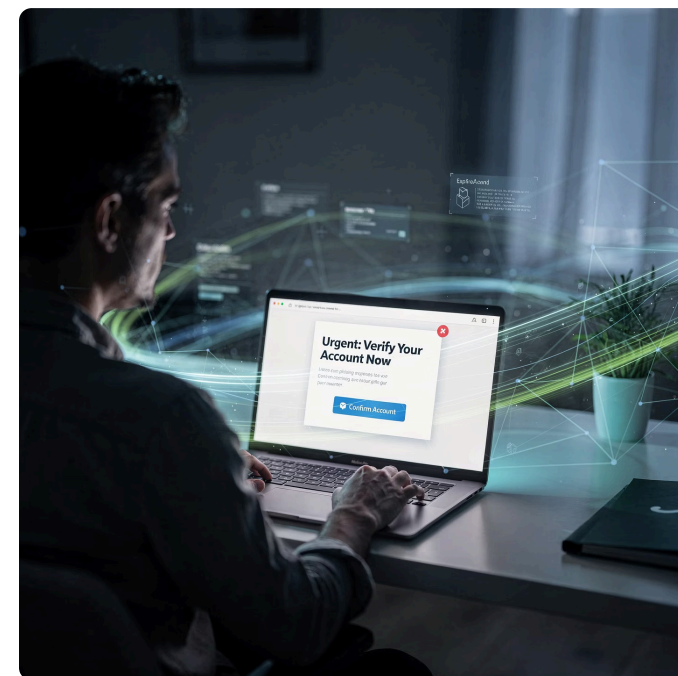
**Phishing en verouderde
software vormen (nog
altijd) grootste risico**

In het digitale tijdperk van 2025 blijven cyberrisico's een constante bedreiging voor organisaties van elke omvang. Twee gevaren steken hierbij prominent uit: phishing-aanvallen die misbruik maken van menselijk vertrouwen, en verouderde software die technische zwaktes blootlegt. Deze dreigingen werken niet geïsoleerd, maar versterken elkaar in een gevaarlijke synergie die bedrijven en individuen kwetsbaar maakt voor dataverlies, financiële schade en reputatieschade.

De onverminderde dreiging van phishing in 2025

Phishing blijft de meest voorkomende vorm van cybercriminaliteit, waarbij aanvallers steeds verfijnder te werk gaan. Geavanceerde technieken zoals **spear phishing** en **whaling** richten zich specifiek op individuen binnen organisaties, waarbij cybercriminelen grondig onderzoek doen naar hun doelwitten om vertrouwen te wekken.

Het probleem wordt verergerd door een gebrek aan bewustzijn. In België is **9% van de bevolking** nog onbekend met phishing, terwijl bij Generatie Z dit percentage oploopt tot alarmerend **30%**. Deze kenniskloof maakt vooral jongere medewerkers kwetsbaar voor misleidende e-mails, sms'jes en telefoontjes.



E-mail phishing

Nabootsen van vertrouwde merken en collega's om inloggegevens te stelen



SMS phishing (Smishing)

Urgente berichten die gebruikers naar valse websites leiden



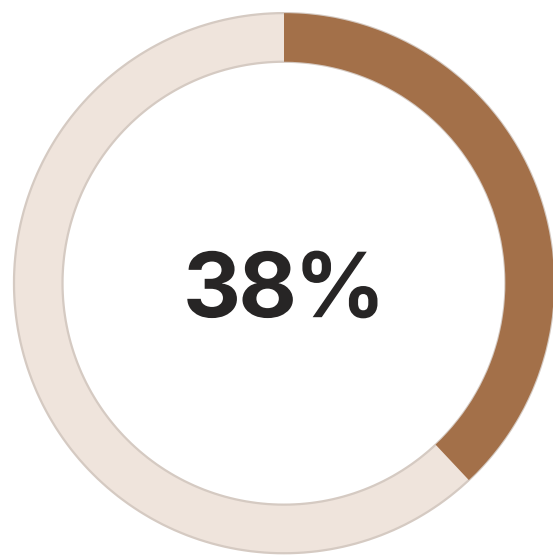
Voice phishing (Vishing)

Telefoonoplichtingen die zich voordoen als legitieme organisaties

 **Extra kwetsbaar:** Accountants en kmo's zijn bijzonder populaire doelwitten vanwege hun toegang tot financiële data en relatief beperkte IT-beveiliging, waardoor ze aantrekkelijke prooien vormen voor cybercriminelen.

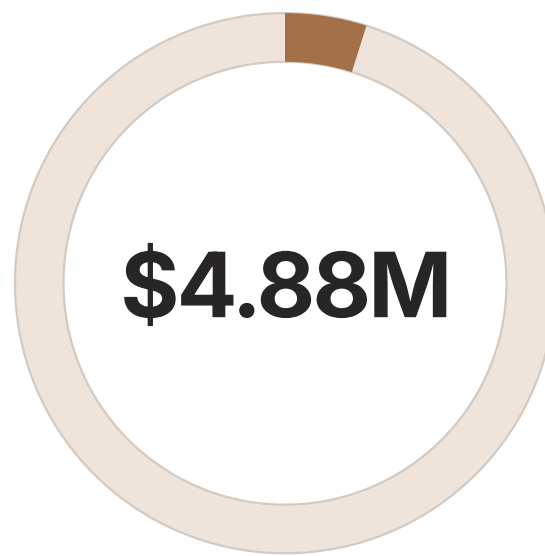
Verouderde software: een sluipend gevaar met grote gevolgen

Terwijl phishing de menselijke factor exploiteert, vormt verouderde software een technische achilleshiel. In 2025 werden maar liefst **21.500 nieuwe kwetsbaarheden (CVE's)** ontdekt, waarvan 38% als hoog of kritiek werd beoordeeld. Deze cijfers onderstrepen de constante evolutie van digitale dreigingen.



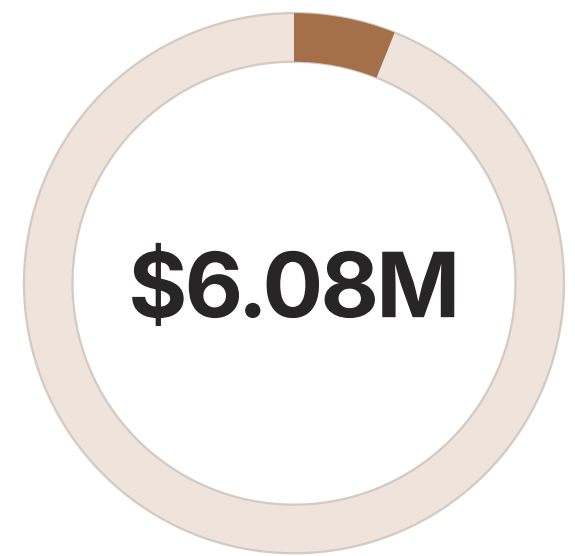
Kritieke kwetsbaarheden

Van alle ontdekte CVE's in 2025



Gemiddelde kosten datalek

Volgens IBM Security Research



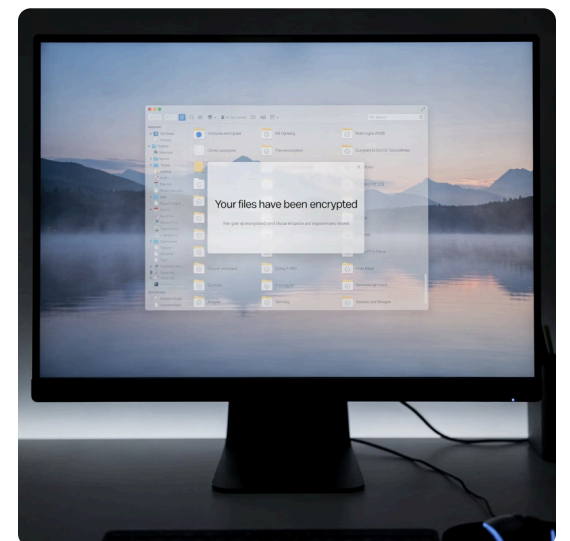
In gereguleerde sectoren

Waar compliance extra kosten meebrengt

Het probleem met legacy systemen

Legacy systemen ontvangen vaak geen beveiligingsupdates meer, waardoor bekende lekken open blijven staan. Cybercriminelen scannen actief naar verouderde Windows-versies, ongepatched servers en end-of-life software.

Deze kwetsbaarheden worden misbruikt voor **ransomware**, **datadiefstal** en **Remote Code Execution-aanvallen**, waarbij aanvallers volledige controle over systemen kunnen verkrijgen.



Hoe phishing en verouderde software elkaar versterken

De werkelijke gevaarlijkheid ontstaat wanneer deze twee dreigingen samenkomen in een gecoördineerde aanval. Phishing fungeert vaak als de initiële toegangspoort, waarna malware de technische zwaktes in verouderde software uitbuit.



Phishing-e-mail

Medewerker ontvangt een overtuigende nep-e-mail



Klikken op link

Gebruiker opent bijlage of bezoekt valse website



Malware-infectie

Schadelijke code wordt geïnstalleerd op het systeem



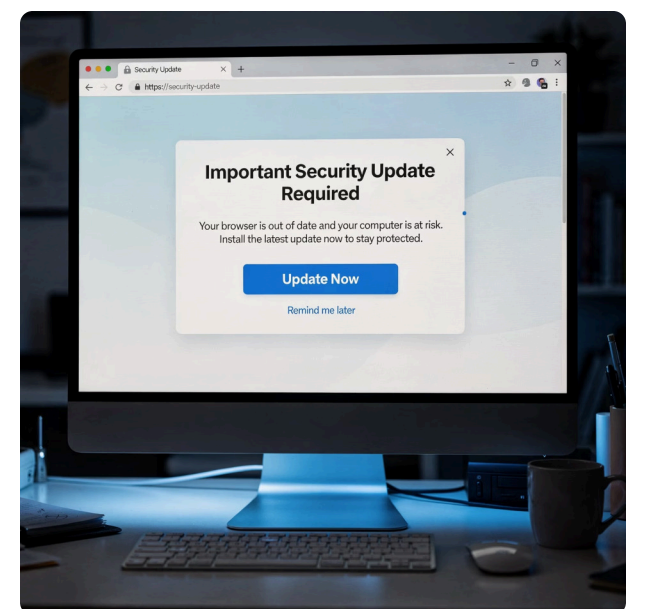
Exploit kwetsbaarheid

Malware misbruikt verouderde software voor verdere toegang

Fake browser updates: een groeiende tactiek

Een bijzonder verraderlijke methode zijn **fake browser updates**. Gebruikers worden misleid via gecompromitteerde legitieme websites die aangeven dat hun browser verouderd is. Bij het installeren van de "update" wordt in werkelijkheid schadelijke software geïnstalleerd – vaak zonder dat antivirus-software alarm slaat.

Deze drive-by-downloads gebeuren soms volledig automatisch, waarbij kwetsbaarheden in verouderde browsers worden misbruikt zonder dat de gebruiker iets merkt.



"Organisaties die verouderde software gebruiken, missen vaak moderne detectie- en verdedigingsmiddelen, waardoor phishing-aanvallen aanzienlijk effectiever zijn. De combinatie van menselijke fouten en technische zwaktes creëert een perfect storm voor cyberaanvallen."

Praktische aanbevelingen voor mitigatie en bewustwording

Effectieve cyberbeveiliging vereist een gelaagde aanpak die zowel technische als menselijke factoren adresseert. Hieronder vindt u concrete stappen om uw organisatie beter te beschermen tegen de gecombineerde dreiging van phishing en verouderde software.

1

Strikt update- en patchmanagement

Implementeer een gestructureerd proces om alle softwarecomponenten actueel te houden, inclusief besturingssystemen, applicaties en firmware. Automatiseer waar mogelijk en stel duidelijke verantwoordelijkheden vast.

2

Geavanceerde e-mailbeveiliging

Investeer in technologieën die phishing-pogingen detecteren en blokkeren voordat ze de inbox bereiken. Dit omvat DMARC, SPF, DKIM-verificatie en AI-gedreven anomaliedetectie.

3

Continue medewerkerstraining

Train personeel regelmatig in het herkennen van phishing en social engineering-tactieken. Gebruik gesimuleerde aanvallen om bewustzijn te testen en te vergroten, met focus op urgentie-trucs en verdachte linktekst.

4

Periodieke IT-infrastructuuraudits

Voer regelmatig audits uit om legacy systemen te identificeren. Ontwikkel een migratieplan om verouderde systemen te vervangen, of isoleer ze in gesegmenteerde netwerken indien vervanging niet onmiddellijk mogelijk is.

5

Open incidentcommunicatie

Stimuleer een cultuur waarin medewerkers zich veilig voelen om verdachte berichten en beveiligingsincidenten te melden zonder angst voor verwijten. Dit vergroot het collectieve bewustzijn en verbetert de responstijd.

📌 **Expertadvies:** Zoals aanbevolen door cybersecurity-specialisten in het notariaat en andere professionele dienstverlening: succesvol beveiligingsbeleid combineert technische maatregelen met een sterke veiligheidscultuur waarin transparantie en continu leren centraal staan.

A hand is shown holding a tablet, with the index finger pointing at the screen. The background is a dark blue gradient with several white shopping cart icons of varying sizes, some enclosed in rounded squares. The overall theme is online shopping and digital commerce.

Praktische Tips om te Checken of een Webshop Betrouwbaar Is

Online winkelen is tegenwoordig gemakkelijker dan ooit, maar helaas zijn er ook steeds meer onbetrouwbare webshops actief. Of je nu op zoek bent naar een koopje of gewoon je boodschappen online doet, het is essentieel om te weten of je te maken hebt met een serieus bedrijf of een oplichter. In deze gids nemen we je mee langs tien praktische stappen om de betrouwbaarheid van een webshop te controleren voordat je je gegevens en geld overhandigt.

Check de Contactgegevens Grondig

Een website is niet door robots bedacht, er zit altijd iemand achter. Check goed wie dat is. Staat er op de website een adres, telefoonnummer en e-mailadres? Het kan ook de moeite waard zijn om even een chatgesprek aan te gaan en te kijken of er wordt gereageerd en of je wordt begrepen.



Even bellen kan ook helpen om te ontdekken of je met een echt bedrijf te maken hebt of een oplichter. En nu je toch bezig bent: check meteen het KvK-nummer op de site van de Kamer van Koophandel. Een legitiem Nederlands bedrijf staat altijd ingeschreven bij de KvK.

Adresgegevens Controleer of er een volledig fysiek adres vermeld staat, niet alleen een postbus	Telefoonnummer Test of het nummer werkt door even te bellen tijdens openingstijden	KvK-nummer Verifieer het nummer via kvk.nl om zekerheid te krijgen
---	--	---

Controleer het Webadres en HTTPS-Beveiliging

In je adresbalk zie je het adres van de webwinkel staan, maar je ziet tegenwoordig niet meer of het dan http of https is. Je wil alleen winkelen op websites die die 's' wel hebben. Deze 's' staat voor 'secure' en betekent dat de verbinding tussen jouw computer en de website versleuteld is.

Klik dus even op het adres in de adresbalk en typ daar zelf: https:// voor. Als de site dan ineens niet meer werkt, dan kun je dit koopje beter links laten liggen, zeker omdat je betaalgegevens moet overleggen en http niet veilig genoeg is. Een hangslotje in de adresbalk is tegenwoordig het minimale veiligheidsniveau dat je mag verwachten.



HTTPS Verplicht

Zonder de 's' is je verbinding niet versleuteld en kunnen je gegevens onderschept worden



Hangslotje Check

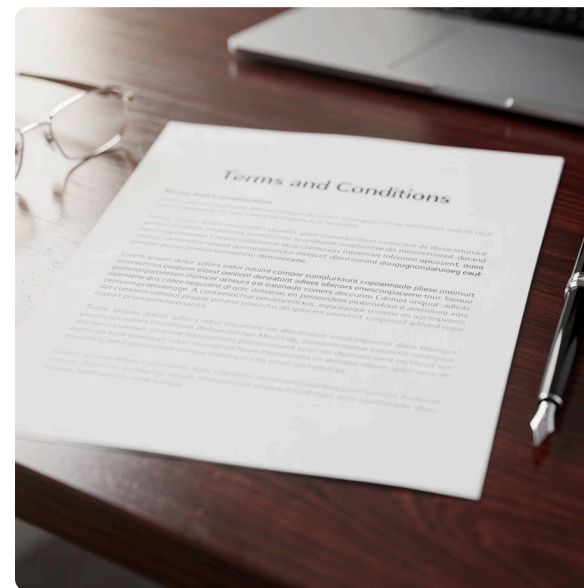
Het hangslotje in de adresbalk geeft aan dat de website een geldig beveiligingscertificaat heeft

Lees de Algemene Voorwaarden Zorgvuldig

Als je de algemene voorwaarden van de winkel niet kunt vinden, dan is er waarschijnlijk al iets niet aan de haak. Maar zelfs als ze er wel zijn, is het verstandig om ze grondig door te lezen. Als je ziet dat retourneren bijvoorbeeld duurder is dan het product zelf, dan is dat ook een moment om je even achter de oren te krabbelen.

Check goed wat de garantie is, het retourbeleid en bijvoorbeeld het privacybeleid, voordat je zomaar je gegevens overlegt. Betrouwbare webshops zijn transparant over hun voorwaarden en maken deze gemakkelijk vindbaar. Let vooral op:

- De retourperiode en eventuele kosten
- Garantievoorwaarden op producten
- Hoe je persoonsgegevens worden gebruikt
- Levertijden en verzendkosten
- Procedure bij klachten of geschillen



Speur naar Reviews op Trustpilot en Google

Als je naar een restaurant gaat, zit het er dik in dat je even de recensies leest. Doe dat ook als je iets gaat kopen. Ook als je allang weet dat dit het product is dat je graag wil, is het vooral verstandig om in de reviews te lezen hoe de webwinkel de koop van anderen heeft afgehandeld.

Trustpilot heeft een strikt beleid tegen betaalde of neppe reviews en hoewel ze er echt af en toe wel tussenzitten, kun je meestal redelijk van TrustPilot op aan. Let niet alleen op het aantal sterren, maar lees ook wat mensen daadwerkelijk schrijven. Zijn er klachten over niet-geleverde producten, slechte klantenservice of misleidende advertenties? Dan weet je genoeg.



Algemene Score

Kijk naar het gemiddelde aantal sterren en het totaal aantal reviews



Recente Reviews

Focus vooral op de meest recente ervaringen van andere klanten



Rode Vlaggen

Let op patronen in negatieve reviews over niet-leveren of oplichting

Gebruik Google en Zoek naar Ervaringen

Op Google vind je vaak reviews, maar als je ook nog googelt naar [naam webwinkel] oplichting of [naam winkel] ervaringen, dan kun je al snel vinden of een winkel zich doorgaans goed gedraagt. Ook zijn er misschien artikelen in de media verschenen over de webshop: of schrijven er juist opvallend weinig mensen over deze winkel?



Je hoeft natuurlijk niet alles te gaan lezen, maar als een winkel er ook maar de schijn van heeft dat het klanten niet altijd koning maakt, dan kun je daaruit voorzichtig concluderen dat jij daar wellicht dan ook liever geen klant wordt. Zoek ook naar de naam van het bedrijf in combinatie met woorden als 'oplichting', 'scam', 'fraude' of 'niet ontvangen'.

01	02	03
Zoek op "[winkelnaam] ervaringen"	Probeer "[winkelnaam] oplichting"	Lees nieuwsartikelen
Ontdek wat andere klanten over hun aankopen zeggen	Check of er waarschuwingen of klachten te vinden zijn	Bekijk of er berichtgeving over de webshop is verschenen

Bekijk de Website Grondig op Kwaliteit

Zijn er keurmerken aanwezig, zien de afbeeldingen en de teksten er goed uit? Staan er geen gekke vertalingen of spelfouten op? Eerlijk is eerlijk, dit was vooral vroeger een teken aan de wand dat je met een beurzensnijder te maken had, want tegenwoordig kunnen websites vrijwel identiek worden nagemaakt en haalt AI alle spelfouten er wel uit.

Toch zijn er nog steeds oplichters die minder slim te werk gaan, dus zorg dat jij ze op jouw beurt te slim af bent door dit te spotten. Let ook op de algemene uitstraling van de website: ziet alles er professioneel uit of lijkt het op een haastig in elkaar geflanste pagina?



Keurmerken

Controleer of WebwinkelKeur, Thuiswinkel Waarborg of andere certificaten aanwezig zijn



Beeldkwaliteit

Professionele foto's en consistente styling wijzen op een serieus bedrijf



Tekstkwaliteit

Goede grammatica en spelling zonder rare vertalingen zijn essentieel

Vraag Hulp aan AI-Tools zoals Gemini



Je kunt natuurlijk ook wat hulp van buitenaf inschakelen om je te helpen bedenken of een webshop betrouwbaar is. Je kunt bijvoorbeeld Gemini of ChatGPT vragen: 'Kun je beoordelen of deze website betrouwbaar is?' En dan de link plaatsen naar de winkel.

Vaak checkt een AI-chatbot verschillende dingen die ook in dit artikel voorbijkomen, zoals de reviews, de contactgegevens en de https-verbinding. Het is een snelle manier om een eerste indruk te krijgen, maar verlaat je er niet volledig op. Gebruik het als een extra laag van controle naast je eigen onderzoek.

 **Tip:** AI-tools kunnen snel veel informatie verzamelen, maar blijf kritisch. Combineer altijd meerdere controlemethoden voor de beste zekerheid.

Controleer Actualiteit en Sociale Media

Staat er nog steeds iets over de lente van 2023, dan is deze website waarschijnlijk al lang niet geüpdatet en dus niet de prioriteit van de maker. Er hoeft niet een blog aanwezig te zijn dat recent is geüpdatet, maar als je het gevoel hebt dat er al een tijdje niks aan de website gedaan is, dan is dat waarschijnlijk ook zo en dan kan er zomaar een boef achter zitten die meer van dit soort webshops runt.

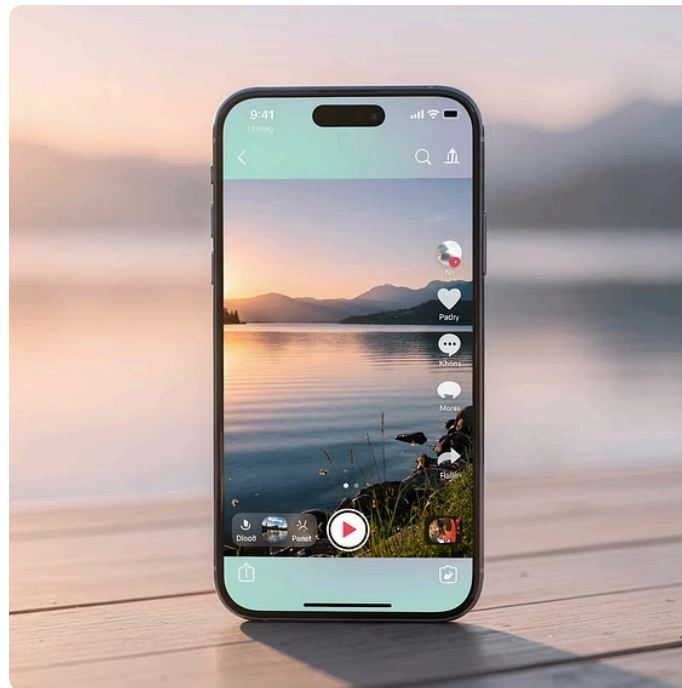
Als jij anno 2025 een bedrijf hebt, dan zorg je dat mensen het onder andere leren kennen door ze er op social media op te wijzen, toch? Als een webwinkel niet op social media te vinden is, dan is dat meestal een teken dat je met boeven te maken hebt. Als webwinkel ben je toch trots op je waar en wil je dat aan potentiële klanten laten zien, toch?

Check dus onder andere Instagram en TikTok om te zien of een bedrijf daar te vinden is. Plus, misschien kom je nog reviews van mensen tegen over die webwinkel. Let op de frequentie van posts, de interactie met volgers en of de accounts authentiek lijken. Duizenden volgers zonder interactie kan wijzen op gekochte volgers.



Instagram

Zoek naar actieve posts en echte klantfoto's



TikTok

Controleer of er video's zijn en hoe mensen reageren



Facebook

Bekijk reviews en de bedrijfspagina voor extra verificatie

Betaal Veilig met Extra Bescherming

Op betalingen met PayPal of een creditcard zitten vaak extra beveiligingslagen, waardoor je meer kans hebt om je geld terug te krijgen als het toch om een charlatan gaat. Vaak mist iDEAL extra aankoopbeveiliging en bij PayPal kun je aankloppen als je product niet aankomt of hevig beschadigd is.

Oke, dit is geen manier om te checken of een webshop te vertrouwen is, maar het is wel een manier om in ieder geval te zorgen dat je je geld niet kwijt bent. PayPal en creditcards bieden koopbescherming die het mogelijk maakt om een geschil te openen en je geld terug te vorderen bij problemen.

PayPal Koopbescherming

Biedt bescherming als je bestelling niet aankomt of significant afwijkt van de beschrijving

Creditcard Chargeback

Mogelijkheid om transacties te betwisten via je creditcardmaatschappij

iDEAL Beperkt

Direct overboeking zonder mogelijkheid tot terugdraaien - gebruik met extra voorzichtigheid

Door deze stappen te volgen, vergroot je de kans aanzienlijk dat je alleen zaken doet met betrouwbare webshops. Blijf altijd alert en vertrouw op je intuïtie: als iets te mooi lijkt om waar te zijn, is het dat waarschijnlijk ook. Veilig online shoppen begint met een gezonde dosis voorzichtigheid en de bereidheid om even wat extra tijd te investeren in verificatie.

**Smart App Control: De Cruciale
Windows 11 Beveiligingsfunctie
Nu Voor Alle Pc's**

Een cruciale beveiligingsfunctie van Windows 11 die Microsoft eerder alleen voor nieuwe Windows-installaties beschikbaar stelde, komt nu alsnog naar alle pc's. Deze doorbraak in digitale beveiliging markeert een belangrijke mijlpaal in de strijd tegen malware en onveilige software.

Wat is Smart App Control?

Smart App Control (SAC) is een geavanceerde beveiligingsfunctie die Microsoft in 2022 introduceerde voor Windows 11 Home en Pro. Deze innovatieve technologie vertegenwoordigt een fundamentele verschuiving in hoe Windows-gebruikers worden beschermd tegen digitale dreigingen.

De functie beschermt gebruikers door alleen veilige apps toe te staan via een AI-gestuurde cloudbeoordeling die in realtime draait. Dit betekent dat elke applicatie die u probeert te installeren of uit te voeren, eerst wordt gecontroleerd tegen een enorme database van bekende veilige en onveilige software. Het systeem blokkeert automatisch malware, potentieel ongewenste apps en ongetekende software voordat deze schade kan aanrichten.



Wat Smart App Control bijzonder effectief maakt, is dat het naadloos samenwerkt met bestaande antivirussoftware. In plaats van uw huidige beveiligingsoplossingen te vervangen, versterkt SAC deze door een extra beschermingslaag toe te voegen. Dit zorgt voor een meervoudige verdedigingsstrategie die zelfs de nieuwste en meest geavanceerde bedreigingen kan tegenhouden.



Geïntroduceerd in 2022

Voor Windows 11 Home en Pro



AI-gestuurde bescherming

Cloudbeoordeling in realtime



Automatische blokkering

Malware en onveilige apps



Extra beveiligingslaag

Versterkt antivirus

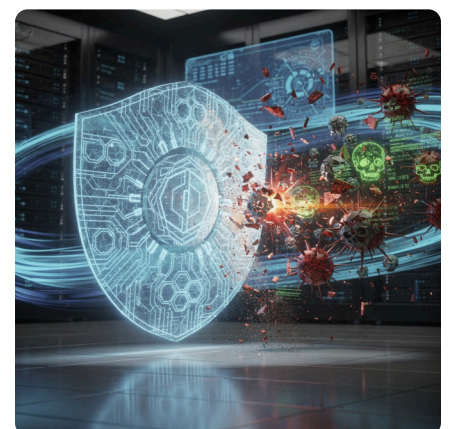
Waarom Alleen Voor Nieuwe Installaties?



De beperking tot nieuwe installaties is geen willekeurige keuze van Microsoft, maar een weloverwogen beveiligingsstrategie. Smart App Control vereist namelijk een volledig schone installatie van Windows 11, specifiek vanaf versie 22572. Deze vereiste is cruciaal om te garanderen dat er geen onbetrouwbare of potentieel gevaarlijke apps al op het systeem aanwezig zijn op het moment dat SAC wordt geactiveerd.

De uitdaging met bestaande systemen

Bij bestaande Windows-installaties kan Smart App Control niet zomaar worden ingeschakeld zonder Windows volledig opnieuw te installeren of het systeem te resetten naar fabrieksinstellingen. Dit lijkt misschien streng, maar het heeft een belangrijke reden: als SAC zou worden geactiveerd op een systeem waar mogelijk al malware of onveilige software op staat, zou deze software kunnen blijven draaien en zou de beveiligingsfunctie zijn doel voorbijschieten.



Microsoft wil hiermee absoluut voorkomen dat onveilige software ongemerkt blijft draaien en zich kan verschuilen tussen legitieme programma's. Door te eisen dat het systeem volledig schoon is bij activering, creëert Smart App Control een betrouwbare uitgangssituatie waarop alle toekomstige app-installaties kunnen worden beoordeeld. Dit "schone lei" principe is vergelijkbaar met hoe beveiligingssystemen op smartphones werken, waar apps vanaf het begin worden gecontroleerd.



Schone installatie vereist

Windows 11 versie 22572 of nieuwer moet vanaf nul worden geïnstalleerd



Geen vooraf geïnstalleerde apps

Garandeert dat er geen onbetrouwbare software aanwezig is bij activering



Reset noodzakelijk

Bestaande systemen moeten volledig opnieuw worden opgezet voor activering

Hoe Werkt Smart App Control Technisch?

De technische werking van Smart App Control is een indrukwekkend staaltje moderne beveiligingstechnologie. Het systeem controleert apps via Microsoft's intelligente cloudservice die dagelijks miljarden datapoints verwerkt. Deze cloud-infrastructuur analyseert continu nieuwe apps, software-updates en potentiële bedreigingen uit de hele wereld.



Apps met een geldige digitale handtekening van een vertrouwde certificaatautoriteit worden automatisch toegestaan. Deze digitale handtekeningen werken als een legitimatiebewijs voor software, waarbij de uitgever zijn identiteit bevestigt en garandeert dat de code niet is gemanipuleerd sinds het ondertekenen.

Ongetekende of verdachte apps worden direct geblokkeerd, zelfs als traditionele antivirusprogramma's ze niet als gevaarlijk detecteren. Dit is een cruciaal voordeel: veel nieuw ontwikkelde malware wordt niet herkend door antivirussoftware omdat de virusdefinities nog niet zijn bijgewerkt. Smart App Control kan deze zero-day bedreigingen wel tegenhouden dankzij zijn AI-gestuurde beoordelingssysteem.

Een uniek aspect van SAC is de evaluatiemodus. Wanneer Smart App Control voor het eerst wordt geactiveerd, draait het een tijdje in deze modus om te bepalen of het geschikt is voor uw gebruikspatroon. Als u regelmatig ongetekende of zelfgemaakte software gebruikt (bijvoorbeeld als ontwikkelaar), kan het systeem concluderen dat het te vaak zou interfereren met uw werk en schakelt het zichzelf automatisch uit. Dit voorkomt frustratie bij power users terwijl gewone gebruikers maximaal worden beschermd.



Impact en Beperkingen voor Gebruikers

1

Verhoogde Veiligheid

Smart App Control biedt aanzienlijk verhoogde bescherming tegen onbekende en nieuwe malwarebedreigingen. Voor de gemiddelde gebruiker betekent dit een dramatische vermindering van het risico op infecties door ransomware, trojans en andere kwaadaardige software die traditionele antivirusprogramma's mogelijk missen.

2

Compatibiliteitsproblemen

Ontwikkelaars en zakelijke gebruikers kunnen compatibiliteitsproblemen ervaren, vooral bij het gebruik van eigen software, interne bedrijfstoets of gespecialiseerde programma's die geen officiële digitale handtekening hebben. Dit kan leiden tot workflow-onderbrekingen en productiviteitsverlies.

3

Beperkte Flexibiliteit

Er is geen mogelijkheid om individuele apps te omzeilen of uitzonderingen toe te voegen. Gebruikers kunnen Smart App Control alleen volledig in- of uitschakelen via de systeeminstellingen, of door Windows opnieuw te installeren. Deze alles-of-niets benadering kan frustrerend zijn voor gebruikers die meer controle willen.

4

Beperkte Beschikbaarheid

SAC is nog niet standaard geactiveerd op alle nieuwe pc's. Microsoft breidt de beschikbaarheid geleidelijk uit, maar veel gebruikers moeten de functie handmatig inschakelen bij een schone installatie om ervan te profiteren. Dit betekent dat veel systemen nog steeds onbeschermd zijn.

Voor wie is SAC ideaal?

- Thuisgebruikers die maximale bescherming willen
- Families met kinderen die online zijn
- Senioren en minder technisch onderlegde gebruikers
- Organisaties met standaard softwarepakketten

Minder geschikt voor:

- Softwareontwikkelaars en programmeurs
- IT-professionals die testomgevingen nodig hebben
- Gamers die mods en patches installeren
- Bedrijven met custom legacy software

Conclusie: Een Stap Vooruit in Windows-beveiliging

Smart App Control vertegenwoordigt een significante evolutie in Windows-beveiliging en brengt het besturingssysteem dichterbij het veilige app-model dat we kennen van iOS en macOS. Het grote verschil is dat Microsoft dit doet zonder de gebruikersvrijheid volledig te beperken – gebruikers behouden de optie om SAC uit te schakelen als het niet past bij hun workflow.

Door nu ook oudere pc's via herinstallatie toegang te geven tot deze functie, verbetert Microsoft de beveiliging voor potentieel miljoenen gebruikers wereldwijd. Dit is geen kleine prestatie: elk systeem dat wordt beschermd door Smart App Control is een systeem dat minder waarschijnlijk onderdeel wordt van een botnet, slachtoffer wordt van ransomware, of gebruikt wordt om anderen aan te vallen.

Verbeterde Bescherming

AI-gestuurde beveiliging tegen moderne dreigingen

Wereldwijde Impact

Miljoenen gebruikers krijgen toegang tot betere beveiliging

Balans Gevonden

Veiligheid zonder vrijheid volledig op te offeren

Gebruikers wordt ten zeerste aangeraden om Smart App Control te activeren bij een schone installatie voor optimale bescherming. Hoewel de herinstallatie tijdrovend kan zijn en enige voorbereiding vereist, wegen de beveiligingsvoordelen ruimschoots op tegen de ongemakken. Voor gezinnen, thuisgebruikers en organisaties die voornamelijk standaardsoftware gebruiken, is dit een no-brainer.

Microsoft zet met deze uitbreiding een belangrijke stap in het veiliger maken van het Windows-ecosysteem tegen moderne dreigingen. In een tijd waarin cybercriminelen steeds geavanceerder worden en aanvallen steeds frequenter, zijn proactieve beveiligingsmaatregelen zoals Smart App Control niet langer een luxe maar een noodzaak. Het is een investering in digitale veiligheid die zich duizendvoudig kan terugbetalen door het voorkomen van één enkele succesvolle aanval.

"Smart App Control is een cruciale stap vooruit in Windows-beveiliging die gebruikers beschermt tegen de bedreigingen van morgen, niet alleen van vandaag."