compu links

uw link naar de digitale wereld

hcc! seniorenacademie

Helpt bij het gebruik van tablet, smartphone en computer

Jaargang 31

2026 2

Inhoud

- **Telefonische helpdesk voor HCC SeniorenAcademie**
  Deze service is gratis beschikbaar voor leden van HCC SeniorenAcademie ig. Houdt uw HCC-lidmaatschappas bij de hand.
  Het lidmaatschapsnummer kan worden gevraagd.

- **Landstede College, Harderwijk**
  tel: 088-850 78 35 (normaal tarief)
  Op werkdagen 09.00-12.00 uur en 13.00-16.00 uur
  Dinsdag- en vrijdagmiddag gesloten

- **ROC A12 / TECHNOVA, Ede**
  tel: 0318- 45 52 31 (normaal tarief)
  Op werkdagen 09.00-12.00 uur
  Indien u de centrale krijgt, vraag dan naar de *studentenhelpdesk* nummer 5231

- *Bij de colleges kunt u, na **telefonische afspraak vooraf** een bezoek brengen aan de ICT-balie.*
- ***Tijdens schoolvakanties gesloten***

- **Vrijwilliger(s) HCC!SeniorenAcademie**
  Van maandag t/m vrijdag onder nummers **085-0441808**
  Raadpleeg de Helpdeskpagina op de website van **HCC!SeniorenAcademie**
  https://seniorenacademie.hcc.nl/helpdesk

compu links ...uw link naar de computer is een uitgave van de HCC!SeniorenAcademie ig
www.seniorenacademie.hcc.nl

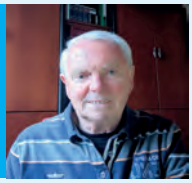
31e jaargang nr 2, zomer 2026
Oplage 4000 exemplaren
Verschijnt vier maal per jaar

Redactie: Euryzakade 405
3331 MM Zwijndrecht
e-mail: redactie@seniorenacademie.hcc.nl of c.vd.vlies@hccnet.nl

Vormgeving: ImageSoft, Krimpen aan den IJssel
e-mail: imagesoft@planet.nl

Druk: Senefelder Misset, Doetinchem

Van de Voorzitter



Het jaar 2026 is inmiddels alweer een tijdje onderweg en binnen de HCC!Seniorenacademie is dat goed te merken. Onze vrijwilligers zijn in het hele land actief met het organiseren van bijeenkomsten, workshops en presentaties. Ook online blijven we volop in beweging. In de afgelopen periode kon u deelnemen aan een reeks webinars, waarin actuele en herkenbare onderwerpen centraal stonden. De grote belangstelling hiervoor laat zien dat de behoefte aan begrijpelijke digitale kennis onverminderd groot is.

Eind maart hebben we onze Algemene Leden Vergadering weer gehouden. Deze keer online, omdat er dit voorjaar geen Kennisdag werd georganiseerd. Dit jaar was het de beurt aan Colette Keuten en Rob van Geuns om periodiek af te treden. Gelukkig stelden beiden zich herkiesbaar. Ook u vond ze onmisbaar binnen ons bestuur, want er werden geen tegenkandidaten ingediend. Daarom kon ik de vergadering met heel veel plezier voorstellen beiden bij acclamatie te herkiezen, hetgeen geschiedde.
Waar we ook aandacht voor hebben gevraagd is de vergrijzing van ons vrijwilligerskorps, veelal bestaande uit 70ers en 80ers. Het wordt steeds lastiger om voldoende vrijwilligers te vinden. Er is nauwelijks aanwas van nieuwe vrijwilligers. En juist zij zijn onmisbaar voor alles wat we doen. Van het geven van presentaties en het begeleiden van bijeenkomsten tot het schrijven van artikelen en het ondersteunen van leden: het werk van onze vrijwilligers vormt het fundament van de Seniorenacademie.

Daarom wil ik hier graag een oproep doen. Heeft u affiniteit met digitale onderwerpen? Vindt u het leuk om kennis te delen, mensen te helpen of betrokken te zijn bij onze activiteiten? Dan nodigen wij u van harte uit om eens na te denken over een rol als vrijwilliger. Er zijn veel manieren om bij te dragen, groot of klein, en ervaring leert dat het niet alleen waardevol is voor anderen, maar ook bijzonder leuk en leerzaam voor uzelf. Samen zorgen we ervoor dat we kunnen blijven groeien en onze kennis kunnen blijven delen.

Een van de meest in het oog springende ontwikkelingen is de opkomst van kunstmatige intelligentie in het dagelijks leven. AI is inmiddels doorgedrongen tot allerlei toepassingen die we dagelijks gebruiken. Wat eerder misschien als complex werd gezien, blijkt in de praktijk juist een hulpmiddel te zijn dat kan ondersteunen bij schrijven, leren en creatief bezig zijn. Tegelijkertijd zien we dat er meer aandacht is gekomen voor digitale veiligheid. Dat is een positieve ontwikkeling, want vertrouwen en veiligheid zijn essentieel om met plezier gebruik te maken van digitale mogelijkheden.

Vooruitkijkend naar de rest van 2026 verwachten we dat deze ontwikkelingen zich verder zullen verdiepen. Technologie wordt steeds persoonlijker en beter afgestemd op de gebruiker. Digitale hulpmiddelen zullen een steeds grotere rol gaan spelen in ons dagelijks leven — niet alleen op het gebied van communicatie en informatie, maar ook in gezondheid, mobiliteit en sociale verbondenheid.
De HCC!Seniorenacademie blijft zich inzetten om deze ontwikkelingen begrijpelijk en toegankelijk te maken. Met duidelijke uitleg, praktische tips en inspirerende bijeenkomsten helpen we u om digitaal vaardig te blijven en met vertrouwen gebruik te maken van nieuwe mogelijkheden. Zo zorgen we er samen voor dat iedereen kan blijven meedoen – nu en in de toekomst.

Onze redactie heeft ook deze keer weer een mooie en gevarieerde selectie van artikelen samengesteld. Of u nu op zoek bent naar praktische tips, achtergrondinformatie of inspiratie: deze editie biedt voor ieder wat wils.
Ik wens u veel leesplezier.

Dick Elzinga
Voorzitter HCC SeniorenAcademie

Zo helpt de digitale wereld bij het plannen van uw vakantie

Veel mensen beginnen ruim van tevoren na te denken over hun vakantie. Waar gaan we naartoe? Hoe reizen we? En waar gaan we overnachten? Vroeger betekende dit stapels reisgidsen, brochures van reisbureaus en misschien een bezoek aan een ANWB-winkel. Tegenwoordig kan de digitale wereld bij vrijwel elke stap helpen. Met een computer, tablet of smartphone is het mogelijk rustig thuis de vakantie voor te bereiden. Het onderwerp is al in eerdere uitgaven van *CompuLinks* aan de orde gekomen.

Inspiratie voor een bestemming

Het begint vaak met inspiratie. Waar wilt u naartoe? Op internet is daar enorm veel informatie over te vinden. Via apps en websites zoals *YouTube* kunt u bijvoorbeeld filmpjes bekijken van steden, natuurgebieden en wandelroutes. Zo krijgt u een goed beeld van een bestemming voordat u er zelf bent geweest.

Op *Pinterest* delen mensen mooie foto's van bijzondere plekken, terwijl u via *Google Maps* alvast met *Street View* kunt rondkijken in een stad of streek. Het voelt soms bijna alsof u er al even rondloopt.

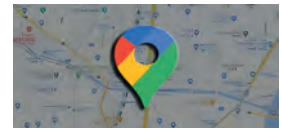
Wie van museumbezoeken houdt, kan in *Google Arts & Culture* al een voorschouw nemen. Ook van theaters, shows, sportgebeurtenissen en weersomstandigheden zijn op internet, zoals genoemd, veel bijzonderheden te vinden.

Reizen en verblijf vergelijken

Als u eenmaal een bestemming hebt gekozen, kunt u online eenvoudig prijzen en mogelijkheden vergelijken. Hotels, vakantiehuisjes en appartementen zijn te vinden via websites zoals Booking.com of *Airbnb*. En anders toetst u *Travel* in bij een zoekopdracht.

Handig is dat u meteen beoordelingen van andere reizigers kunt lezen. Zo krijgt u een indruk van de kwaliteit van een hotel of appartement. Ook organisaties zoals *ANWB* bieden online veel informatie over reizen, campings en accommodaties.

De reis plannen



Ook de reis zelf kunt u digitaal voorbereiden. Met navigatieapps als *Google Maps* of *Waze* ziet u hoe u het beste naar uw bestemming kunt rijden. De apps laten ook zien waar files staan en hoe lang de reis ongeveer duurt.

Neem nota van de verkeersregels in de bestemmingslanden, dan kunt u problemen voorkomen. Voor een verblijf in sommige landen kan het aanbeveling verdienen daar een lokaal sim-kaartje voor in de smartphone te kopen.

Gaat u met het openbaar vervoer? Dan kunt

u in Nederland eenvoudig routes plannen met apps zoals **9292.nl**.

Hulp bij een andere taal

In het buitenland kan de taal soms een uitdaging zijn. Gelukkig bestaan er handige vertaalapps. Online is er *DeepL*, bijvoorbeeld. Met *Google Translate* kunt u tekst typen, inspreken of zelfs een foto maken van bijvoorbeeld een menukaart, een straatnaam of een opschrift. De app vertaalt de tekst vrijwel meteen. Vooral handig als u andere tekens dan 'onze' latijnse letters niet kent.

Vertalen (ook met gesproken woord) gaat handig, voorheen met de app *SayHi*, helaas niet meer ondersteund, maar er is nu *SayHi Translate*, met AI. Ook zijn er uiterst handzame vertaalapparaatjes te koop. Daarnaast bestaan er *Apple Translate*, *Reverso* en *I Translate* voor de Apple-gebruikers. *Microsoft Translator* en de vele (online) vertaalwoordenboeken (vaak met uitspraak). Let er wel op dat er een duidelijk onderscheid is tussen online-vertalers en offline vertalers! Zonder (mobiel) internet kan het een stukje moeilijker worden.

Vertaalapps maken het bestellen van eten of het lezen van informatie gemakkelijker.

Tijdens de vakantie: ontdek de omgeving

Ook tijdens de vakantie blijft de smartphone een handig hulpmiddel. Apps als *Tripadvisor* geven tips voor restaurants, musea en bezienswaardigheden in de buurt.

Voor wandelaars en fietsers is bijvoorbeeld *Komoot* populair. Daarmee kunt u mooie routes ontdekken in de natuur, inclusief informatie over afstand en hoogteverschillen.

Tickets en reserveringen digitaal bewaren

Steeds vaker worden tickets en reserveringen digitaal opgeslagen. Denk aan hotelreserveringen, vliegtickets of toegangsbewijzen voor musea. Veel mensen bewaren deze eenvoudig in hun e-mail of in apps als *Google Wallet*. Dat scheelt een map met papieren en u heeft alles altijd bij de hand op uw smartphone.

Herinneringen vastleggen en delen

Tijdens de vakantie maken we natuurlijk foto's en video's. Met een smartphone gaat dat eenvoudig en snel. Apps als *Google Foto's* bewaren de foto's automatisch online. Daardoor raken ze niet zomaar kwijt als er iets met de telefoon gebeurt. Kijk voor alle zekerheid ook even na wat u moet doen als de smartphone zoek raakt of gestolen wordt. Het IMEI-nummer van uw smartphone heeft u natuurlijk al bij de aankoop van het toestel vastgelegd en genoteerd.

Bovendien kunt u uw foto's gemakkelijk delen met familie en vrienden, bijvoorbeeld via e-mail of sociale media.

Over *Polarsteps*, de veelzijdige reis(verslag)-app, hebben we het in *CompuLinks* al vaker gehad.

Vakantie plannen was nog nooit zo makkelijk

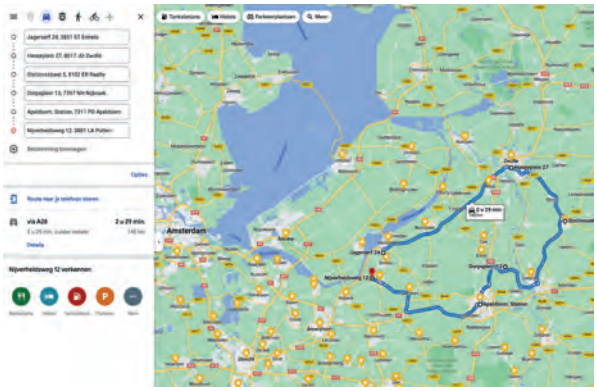
De digitale wereld heeft het plannen van een vakantie een stuk eenvoudiger gemaakt. Van inspiratie en het boeken van een hotel tot navigatie onderweg en het bewaren van foto's: alles kan met een paar klikken.

Voor veel mensen is het daarom prettig om de vakantie rustig thuis achter de computer of met de tablet voor te bereiden. Zo begint het vakantiegevoel eigenlijk al bij het plannen, maar dat was altijd al zo.

De complete handleiding van *Google Maps*

Met verborgen functies en handige tips

De meeste mensen gebruiken Google Maps alleen om een route te plannen. Maar de app kan veel meer. Je kunt er restaurants mee zoeken, de drukte in winkels bekijken, je parkeerplaats opslaan en zelfs kaarten downloaden voor gebruik zonder internet.
In dit uitgebreide overzicht leggen we alle belangrijke functies uit, inclusief verborgen mogelijkheden en praktische tips.



1. Een route plannen

Dit is de functie die bijna iedereen gebruikt.

Zo werkt het

1. Open *Google Maps*
2. Tik op **Route**
3. Vul je **vertrekpunt** en **bestemming** in
4. Kies je vervoermiddel:
   - auto
   - fiets
   - openbaar vervoer
   - lopen

Google Maps laat daarna zien:

- de snelste route
- alternatieve routes
- reistijd
- afstand

Extra opties

Je kunt ook kiezen voor:

- tolwegen vermijden
- snelwegen vermijden
- veerboten vermijden

2. Navigatie met gesproken aanwijzingen

Tijdens het rijden werkt *Google Maps* als een navigatiesysteem.

Tik op **Start** en je krijgt:

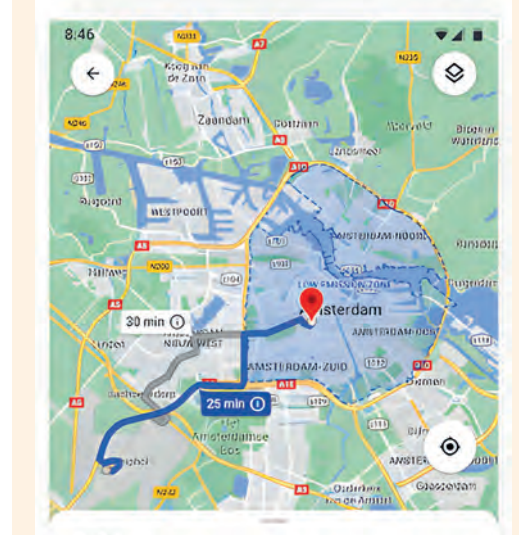
- gesproken aanwijzingen
- waarschuwingen voor files
- meldingen van ongelukken
- snelheidslimieten

3. Verkeersdrukte bekijken

Google Maps toont live verkeersinformatie.

Betekenis van de kleuren

- Groen – verkeer rijdt door
- Oranje – druk verkeer
- Rood – file



4. Restaurants, winkels en andere plekken zoeken

Je kunt zoeken op:

- restaurant
- supermarkt
- apotheek
- tankstation
- pinautomaat
- museum
- park

Bij elke locatie zie je vaak:

- openingstijden
- beoordelingen
- foto's
- routebeschrijving
- telefoonnummer

5. Reviews en beoordelingen

Bezoekers kunnen locaties beoordelen met sterren.

★★★★★ = erg goed
★★★ = gemiddeld

Ook kun je **reviews lezen** van andere bezoekers.

6. *Street View*: virtueel rondkijken

Met *Street View* kun je een straat bekijken alsof je er zelf staat.

Zo werkt het

1. Houd je vinger op een plek op de kaart
2. Tik op de foto

Je kunt dan rondkijken en door de straat bewegen.

7. Satellietweergave

Via **Lagen** kun je kiezen voor:

- kaart
- satelliet
- terrein

Satellietbeelden geven vaak een duidelijker beeld van de omgeving.

8. Drukte bekijken

Bij veel winkels en restaurants kun je zien hoe druk het meestal is.

Je ziet een grafiek met:

- drukte per uur
- drukte per dag

9. Parkeerplaats onthouden

Zo werkt het

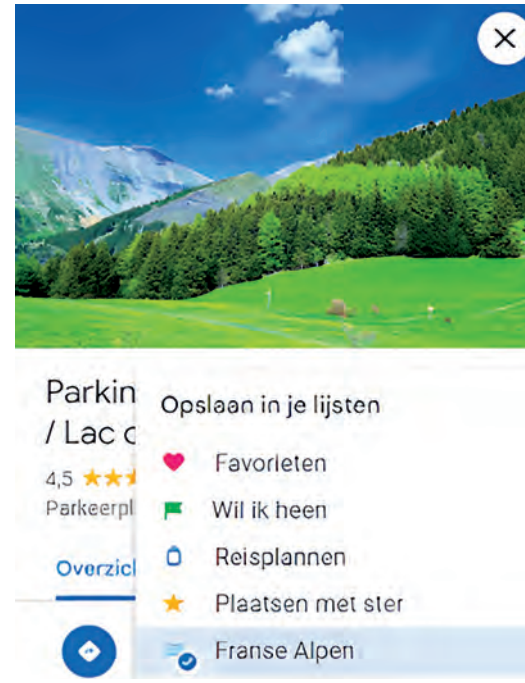
1. Tik op de **blauwe stip**
2. Kies **Parkeerlocatie opslaan**

Google Maps onthoudt waar je auto staat.

10. Favoriete plekken opslaan

Je kunt locaties opslaan als:

- Favoriet
- Wil ik bezoeken
- Sterlocatie



11. Offline kaarten downloaden

Handig op vakantie of in gebieden met slecht internet.

Zo doe je dat

1. Tik op je **profielicoon**
2. Kies **Offline kaarten**
3. Selecteer een gebied

12. Locatie delen

Je kunt je **live locatie delen** met familie of vrienden.

1. Tik op je **profielicoon**
2. Kies **Locatie delen**

13. Lijsten maken

Je kunt eigen lijstjes maken, bijvoorbeeld:

- restaurants
- wandelroutes
- vakantieplekken

14. Openbaar vervoer plannen

Google Maps toont:

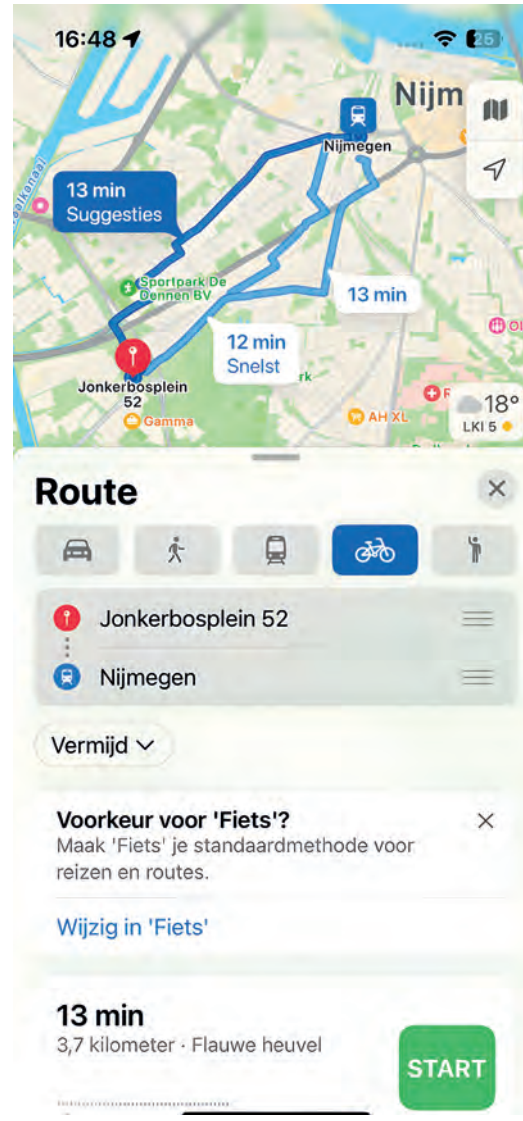
- vertrektijden
- overstappen
- reistijd
- soms vertragingen

15. Fietsroutes

In Nederland erg handig.

Je ziet:

- fietspaden
- reistijd
- rustige routes



Verborgen functies van Google Maps

→ **Met één tik naar huis**
Stel een **thuisadres** in. Daarna kun je met één tik navigeren naar huis.

→ **Navigatie met augmented reality**
Met *Live View* zie je pijlen op het scherm die je de juiste richting wijzen.

→ **Tankstations met brandstofprijzen**
Soms toont *Google Maps* actuele brandstofprijzen.

→ **Elektrische laadpalen zoeken**
Je kunt eenvoudig laadpunten vinden voor elektrische auto's.

15 snelle *Google Maps*-tips

1. Tik op een locatie en kies **Opslaan** om hem later terug te vinden
2. Gebruik **spraak zoeken** in plaats van typen
3. Download **offline kaarten** voor vakanties
4. Bekijk een adres vooraf met *Street View*
5. Controleer de **druktegrafiek** voordat je ergens heen gaat
6. Sla je **parkeerplaats** op
7. Zet **verkeersinformatie** aan op de kaart
8. Gebruik **fietsnavigatie** in steden
9. Deel je **locatie** met familie tijdens een reis
10. Bekijk **openingstijden** voordat je vertrekt
11. Lees **reviews** van restaurants
12. Maak **lijstjes van favoriete plekken**
13. Gebruik **satellietweergave** om de omgeving beter te zien
14. Controleer **alternatieve routes** bij files
15. Gebruik *Live View* in onbekende steden

Veelgemaakte fouten bij *Google Maps*

→ **Alleen de eerste route kiezen**
Google Maps toont vaak meerdere routes. Soms is een andere route sneller of makkelijker.

→ **Geen offline kaart downloaden**
Zonder internet werkt navigatie soms minder goed.

→ **Adres niet controleren**
Soms hebben straten dezelfde naam in verschillende plaatsen. Let ook op de spelling van en afkortingen en toevoegingen in straatnamen.

→ **Navigatie te laat starten**
Start navigatie al voordat je wegrijdt.

→ **Alleen op navigatie vertrouwen**
Blijf ook altijd op verkeersborden letten.

Extra tips speciaal voor senioren

- Gebruik grotere letters
  Vergroot de lettergrootte van je smartphone.
- Gebruik spraakopdrachten
  Tik op het microfoon-icoon en zeg bijvoorbeeld: '*Route naar het ziekenhuis*.'
- Download *Kaarten* vooraf
  Handig bij vakantie of slecht bereik.
- Bekijk *Street View* vooraf
  Zo herken je een gebouw makkelijker.
- Laat familie je locatie volgen
  Dat kan een veilig gevoel geven.

Conclusie

Google Maps is veel meer dan alleen een routeplanner. De app helpt bij navigatie, het vinden van restaurants, het bekijken van drukte en zelfs het terugvinden van je parkeerplaats.

Wie de mogelijkheden kent, ontdekt dat *Google Maps* eigenlijk een 'complete reisgids in je broek is'.

Het broekzak-advies is *niet* van de redactie!

Google Maps Live View

Bescherm jezelf tegen hackers: zo maak je het criminelen een stuk moeilijker

Vrijwel iedere week lezen we in het nieuws over een hack of datalek. Soms gaat het om grote bedrijven of overheden, maar steeds vaker zijn ook gewone internetgebruikers slachtoffer. Een gestolen e-mailaccount, een gehackte Facebookpagina of zelfs toegang tot online bankieren: *het kan iedereen overkomen.*

Toch is het goede nieuws dat je als particulier al met een paar eenvoudige maatregelen veel risico kunt voorkomen. Digitale veiligheid hoeft namelijk helemaal niet ingewikkeld te zijn.

Waarom hackers juist particulieren aanvallen

Veel mensen denken dat hackers alleen interesse hebben in grote bedrijven. In werkelijkheid zijn particulieren juist aantrekkelijke doelwitten. Niet omdat er bij één persoon veel geld te halen is, maar omdat het **in grote aantallen** gebeurt.

Criminelen werken vaak geautomatiseerd. Met speciale software proberen ze duizenden accounts tegelijk te openen met gestolen wachtwoorden. Als daar een klein percentage van werkt, kan het al genoeg geld opleveren.

De meeste hacks ontstaan door drie oorzaken:

- zwakke of hergebruikte wachtwoorden
- phishing (misleidende berichten)
- verouderde software

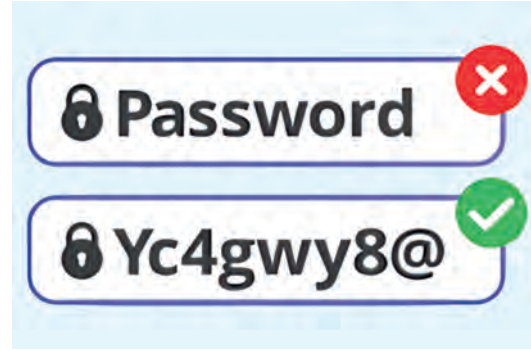
Gelukkig kun je daar zelf veel aan doen.

1. Gebruik sterke en unieke wachtwoorden

Het grootste probleem bij online beveiliging is nog steeds het wachtwoord. Veel mensen gebruiken hetzelfde wachtwoord op meerdere websites. Dat lijkt handig, maar het is riskant. Wanneer één website wordt gehackt en wachtwoorden uitlekken, proberen criminelen die gegevens meteen ook op andere websites.

Een goed wachtwoord:

- bevat minimaal **12 tot 16 tekens**
- gebruikt een **combinatie van letters, cijfers en symbolen**
- wordt **niet op meerdere websites gebruikt**



Omdat het bijna onmogelijk is om tientallen wachtwoorden te onthouden, kiezen steeds meer mensen voor een wachtwoordmanager. Zo'n programma bewaart al je wachtwoorden veilig en vult ze automatisch in.

2. Zet tweestapsverificatie aan

Een van de beste beveiligingsmaatregelen is **tweestapsverificatie** (ook wel 2FA genoemd). Hierbij log je niet alleen in met een wachtwoord, maar ook met een extra controle.

Bijvoorbeeld:

- een code via een app
- een sms
- een bevestiging op je smartphone

Zelfs als een hacker je wachtwoord weet, kan hij zonder die extra code niet inloggen.
Steeds meer diensten ondersteunen deze extra beveiliging, zoals e-maildiensten, sociale media en banken, een vaak irritante, maar noodzakelijke methode, waar we misschien ooit wel weer van afkomen.

3. Let goed op phishing

Veel digitale aanvallen beginnen met **phishing**: een misleidend bericht waarin criminelen proberen je naar een nepwebsite te lokken.
Dat kan bijvoorbeeld een e-mail zijn van een bank, een pakketdienst of een energiebedrijf. De boodschap klinkt vaak dringend: je moet snel inloggen of een betaling controleren.

Let op deze signalen:
- een onverwachte e-mail of sms
- een link die er vreemd uitziet
- druk om snel te reageren, soms met dreigement
- spelfouten of vreemde formuleringen

Klik bij twijfel nooit op een link in een bericht, maar ga zelf naar de website van het bedrijf.

4. Installeer updates

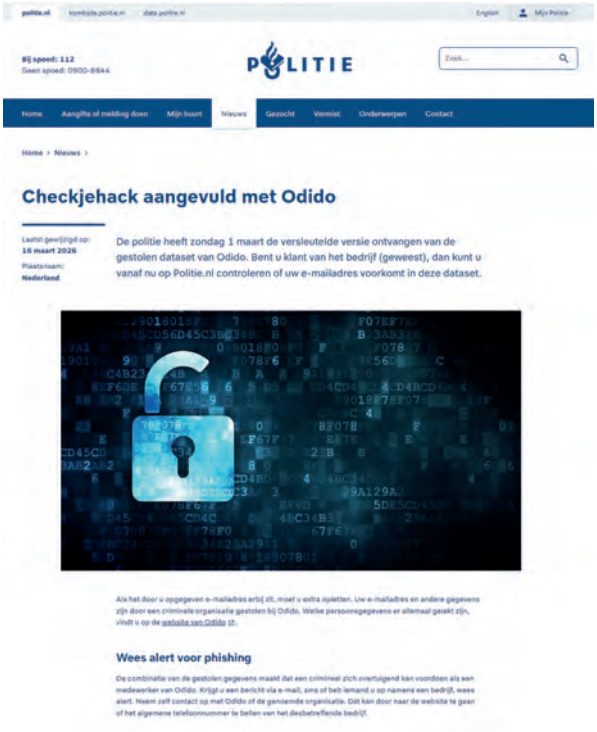
Updates van computers, smartphones en apps bevatten vaak **beveiligingsverbeteringen**. Ze dichten lekken die hackers konden misbruiken.
Veel mensen stellen updates uit omdat het niet gelegen komt. Toch is het verstandig om ze zo snel mogelijk te installeren.

Dat geldt voor:
- je computer
- je smartphone
- je apps
- je internetbrowser

Automatische updates inschakelen is vaak de veiligste keuze.

5. Controleer of je gegevens zijn gelekt

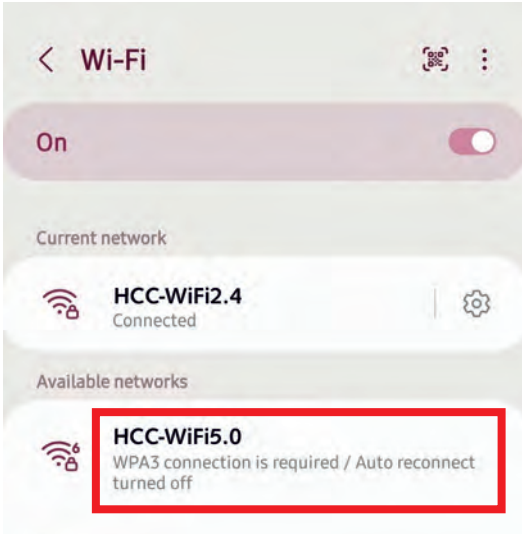
Soms komen e-mailadressen en wachtwoorden terecht op internet na een datalek. Gelukkig zijn er websites waarmee je kunt controleren of jouw gegevens ooit zijn uitgelekt.
Door je e-mailadres te controleren kun je zien of het voorkomt in bekende datalekken. Als dat zo is, is het verstandig om meteen je wachtwoorden te veranderen.



Goede controle websites zijn:
https://www.politie.nl/nieuws/2026/maart/2/checkjehack-aangevuld-met-odido.html en
https://haveibeenpwned.com/

6. Beveilig je wifi-netwerk

Je wifi-netwerk is de toegangspoort tot alle apparaten in huis. Daarom is het belangrijk dat dit goed beveiligd is.



Controleer bijvoorbeeld:
- of je router **WPA2** of **WPA3 beveiliging** gebruikt
- of het standaard wachtwoord van de router is gewijzigd
- of de router regelmatig updates krijgt

Veel moderne routers installeren beveiligingsupdates automatisch.

7. Maak regelmatig back-ups

Een groeiend probleem is ransomware: schadelijke software die bestanden versleutelt. De aanvaller vraagt vervolgens losgeld om de bestanden weer vrij te geven.
De beste bescherming hiertegen is een **goede back-up**.
Bewaar belangrijke bestanden bijvoorbeeld:
- op een externe harde schijf
- in een cloud-opslagdienst

Met een recente back-up kun je bestanden eenvoudig herstellen.

Digitale veiligheid begint bij bewustzijn

Hoewel hackers steeds slimmer worden, geldt nog steeds dat veel aanvallen gebruikmaken van simpele fouten. Een zwak wachtwoord of een verkeerde klik op een link kan al genoeg zijn.
Door bewust met je digitale veiligheid om te gaan, kun je de meeste problemen voorkomen.

De gouden combinatie blijft:

- een wachtwoordmanager
- tweestapsverificatie
- regelmatige updates

Met die drie maatregelen ben je al beter beschermd dan de meeste internetgebruikers.

Wachtwoordmanagers: veilig omgaan met al uw wachtwoorden

In *CompuLinks* hebben we het al eerder over wachtwoordmanagers gehad. Deze keer een 'update' met recente gegevens.

Wie een beetje actief is op internet, heeft al snel tientallen accounts. Denk aan e-mail, webwinkels, de bank, sociale media en allerlei apps. Voor elk account is een sterk en uniek wachtwoord nodig. Maar wie kan al die wachtwoorden onthouden?
Veel mensen gebruiken daarom hetzelfde wachtwoord op meerdere websites. Dat lijkt handig, maar het is ook gevaarlijk. Zodra één website wordt gehackt, kunnen kwaadwillenden vaak ook andere accounts overnemen.
Een goede oplossing is een **wachtwoordmanager**. Dit is een programma dat al uw wachtwoorden veilig opslaat en automatisch kan invullen wanneer u ergens inlogt.
Maar welke wachtwoordmanager moet u kiezen? En waar worden uw gegevens eigenlijk opgeslagen? Hieronder vindt u een overzicht van de belangrijkste mogelijkheden.

Wat doet een wachtwoordmanager?

Een wachtwoordmanager bewaart uw wachtwoorden in een versleutelde digitale kluis. U hoeft dan nog maar één wachtwoord te onthouden: **het hoofdwachtwoord**.
De meeste managers kunnen daarnaast:

- sterke wachtwoorden *genereren*
- wachtwoorden *automatisch invullen*
- controleren of wachtwoorden gelekt zijn
- *synchroniseren* tussen computer, smartphone en tablet

De meeste moderne diensten werken met een zogenoemd **zero-knowledge-model**. Dat betekent dat uw gegevens versleuteld worden voordat ze naar de server worden gestuurd. Zelfs het bedrijf achter de dienst kan de wachtwoorden niet lezen.

Cloud-gebaseerde wachtwoordmanagers

De meeste mensen gebruiken een wachtwoordmanager die zijn gegevens in de cloud bewaart. Daardoor zijn wachtwoorden automatisch beschikbaar op alle apparaten.

bitwarden

Bitwarden

Bitwarden is één van de populairste wachtwoordmanagers.
Het bedrijf komt uit de Verenigde Staten, maar gebruikers kunnen hun gegevens ook laten opslaan op servers in Europa.
Voordelen:

- open-source software
- sterke beveiliging
- gratis versie met veel functies
- werkt op vrijwel alle apparaten

Nadelen:

- de interface is iets minder eenvoudig dan die van sommige concurrenten

Bitwarden wordt vaak aanbevolen door beveiligingsexperts.

1Password

1Password komt uit Canada en staat bekend om zijn gebruiksgemak.
De dienst voegt een extra beveiligingslaag toe in de vorm van een zogenaamde **Secret Key** naast het hoofdwachtwoord.

Voordelen:

- zeer gebruiksvriendelijk
- veel extra functies
- goede ondersteuning voor gezinnen

Nadelen:

- geen gratis versie
- niet open source

Dashlane

Dashlane is een Amerikaanse wachtwoordmanager met een moderne interface.
Een bijzonder kenmerk is dat sommige abonnementen een VPN-dienst bevatten.

Voordelen:

- eenvoudig te gebruiken
- goede beveiligingsanalyse van wachtwoorden
- automatische waarschuwingen bij datalekken

Nadelen:

- relatief duur
- gratis versie beperkt

NordPass

NordPass is ontwikkeld door het bedrijf achter de VPN-dienst NordVPN. Het bedrijf heeft zijn hoofdkantoor in Litouwen.

Voordelen:

- moderne encryptietechniek
- eenvoudige interface
- goede integratie met andere Nord-diensten

Nadelen:

- gratis versie werkt slechts op één apparaat tegelijk

Proton Pass

Proton Pass is een relatief nieuwe wachtwoordmanager uit Zwitserland.
Het bedrijf staat bekend om privacy vriendelijke diensten zoals Proton Mail.

Voordelen:

- servers in Zwitserland en Europa
- sterke privacywetgeving
- open-source software
- gratis versie beschikbaar

Nadelen:

- nog niet zo uitgebreid als sommige oudere diensten

Keeper

Keeper is vooral populair bij bedrijven, maar ook voor particuliere gebruikers beschikbaar.

Voordelen:

- zeer uitgebreide beveiligingsfuncties
- veel extra modules

Nadelen:

- vrij duur
- sommige functies zijn alleen tegen extra betaling beschikbaar

Wachtwoordmanagers zonder centrale cloud

Sommige mensen willen hun wachtwoorden liever niet op servers van een bedrijf opslaan. Voor hen bestaan er managers die volledig lokaal werken.

KeePass

KeePass is een gratis open-source wachtwoordmanager.
Alle gegevens worden opgeslagen in een bestand op de eigen computer.

Voordelen:
- volledige controle over gegevens
- zeer veilig
- gratis

Nadelen:
- minder gebruiksvriendelijk
- synchronisatie tussen apparaten moet zelf geregeld worden

KeePassXC

KeePassXC is een modernere variant van KeePass.
Het programma werkt op Windows, macOS en Linux en heeft een wat modernere interface.

Wachtwoordmanagers van grote techbedrijven

Veel mensen gebruiken zonder het te weten al een wachtwoordmanager. Grote technologiebedrijven hebben namelijk hun eigen oplossingen.

Google Password Manager

Deze manager zit ingebouwd in de Chrome-browser en Android-telefoons.

Voordelen:
- automatisch beschikbaar
- gratis
- eenvoudig te gebruiken

Nadelen:
- minder functies dan gespecialiseerde managers
- afhankelijk van Google-account

Apple iCloud Keychain

Apple heeft een eigen wachtwoordmanager die werkt op iPhone, iPad en Mac.

Voordelen:
- zeer gebruiksvriendelijk
- sterke beveiliging

Nadelen:
- alleen bruikbaar binnen het Apple-ecosysteem

Microsoft Authenticator

Ook Microsoft heeft een wachtwoordmanager ingebouwd in de app Microsoft Authenticator en de Edge-browser.

Voordelen:
- gratis
- goed geïntegreerd met Windows

Nadelen:
- minder uitgebreid dan gespecialiseerde oplossingen

Waar staan de gegevens eigenlijk?

Veel mensen maken zich zorgen over de locatie van hun gegevens. In de praktijk maakt dat vaak minder verschil dan gedacht.
De meeste wachtwoordmanagers versleutelen gegevens namelijk **op het apparaat van de gebruiker** voordat ze naar de server worden gestuurd. Daardoor kan zelfs het bedrijf achter de dienst de wachtwoorden niet lezen.
Toch kiezen sommige gebruikers liever voor een Europese dienst zoals Proton Pass, omdat die onder strengere privacywetgeving valt.

Welke wachtwoordmanager is het beste?

Er is niet één perfecte keuze. Dat hangt vooral af van uw wensen.
Wie een eenvoudige oplossing zoekt, kan prima uit de voeten met diensten als Bitwarden of 1Password.
Wie maximale privacy wil, kan kijken naar Proton Pass of een lokale oplossing zoals KeePass.

Het belangrijkste blijft echter dat u **überhaupt een wachtwoordmanager gebruikt**. Daarmee wordt het veel makkelijker om voor elke website een uniek en sterk wachtwoord te gebruiken.
En dat is nog altijd de beste bescherming tegen hackers.

Pas op bij Android 12 of oudere versie

Als je een **Android-telefoon hebt die nog op Android 12 of ouder draait**, dan betekent dat:

- De officiële **beveiligingsupdates van Google zijn gestopt** sinds 31 maart 2025. Dus al meer dan 1 jaar geleden.
- Je apparaat krijgt dus geen patches meer voor nieuwe kwetsbaarheden.)
- Daardoor wordt het **kwetsbaarder voor malware, phishing en andere aanvallen** – vooral als je gevoelige dingen op je telefoon doet, zoals online-bankieren of e-mailen.

Dat betekent **niet automatisch dat je telefoon direct onveilig is**, maar het verhoogt je risico aanzienlijk. Zeker naarmate oudere systemen langer zonder updates blijven, kunnen nieuwe exploits nooit meer door Google dichtgemaakt worden. (zie ook **https://android.hcc.nl/nieuws/de-ondersteuning-voor-android-12-is-gestopt**)

Wat kun je doen als je huidige Android niet meer ondersteund wordt?

1. Zoeken naar een beveiligings-upgrade

- Controleer of jouw telefoon nog een fabrikant-update naar Android 13 of hoger kan krijgen.
  Soms stopt Google zelf met updates, maar geeft de fabrikant nog eigen beveiligingspatches.
- Zo ja → installeer die update, want dat is de beste bescherming.

2. Apps en beveiligingstools om risico's te verminderen

Zelfs zonder besturingssysteem-patches kun je je beveiliging verbeteren met extra tools. Goede beveiligingsapps (meestal via de Google Play Store) helpen je risico's te beperken:

Antivirus en beveiligingsapps

- *AVG AntiVirus & Security* – Populaire gratis optie om malware te detecteren en wifi-netwerken te scannen.
- *Bitdefender Mobile Security* – Sterke bescherming tegen apps met malware, phishinglinks en schadelijke bestanden.
- *Avast Mobile Security* – Gratis versie biedt malware-detectie, wifi-controle en meer.
- *Norton Mobile Security* – Uitgebreide beveiliging inclusief bescherming tegen gevaarlijke websites.

- *Malwarebytes* – Goede gratis optie met basis-antimalware-bescherming.
- *Kaspersky Antivirus* – Bekende naam met reputatie voor betrouwbare malware-detectie.

Let op compatibiliteit:
Sommige moderne beveiligingsapps hebben minimum Android-vereisten. Bijvoorbeeld Norton vereist Android 10 of hoger.
(**https://nl.norton.com/products/mobile-security-for-android)**

3. Extra veilige gewoontes
Zelfs zonder extra apps kun je een hoop problemen voorkomen:
- Installeer alleen apps via de *Google Play Store* (niet van onbekende sites).
- Houd je apps up-to-date.
- Zet *Google Play Protect* aan via de *Play Store-instellingen* (dit scant op malware).
- Wees voorzichtig met openbare wifi-netwerken: gebruik waar mogelijk een VPN.
- Beperk app-machtigingen (bijv. locatie, microfoon, etc.).
- Gebruik *tweefactorauthenticatie (2FA)* voor belangrijke accounts.

4. Overweeg een nieuwere telefoon
Het meest effectieve is over het algemeen om te kiezen voor een nieuw model dat nog wél beveiligingsupdates krijgt — meestal minstens 5-7 jaar sinds lancering.
Zelfs de beste beveiligingsapps kunnen een verouderd besturingssysteem niet volledig compenseren, want ze kunnen niet alle diepere systeemlekken afdichten die alleen via OS-patches worden opgelost.

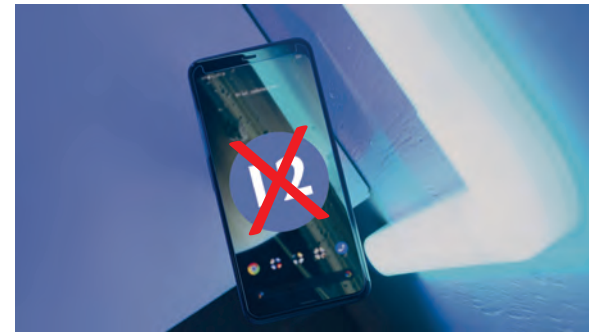
Samengevat
- Android 12 krijgt sinds maart 2025 geen Google-beveiligingsupdates meer.
- Dat maakt je toestel op den duur kwetsbaarder voor malware en exploits.
- Mobile security apps zoals AVG, Bitdefender, Avast en Norton kunnen helpen je risico's te verkleinen.
- Voor maximale veiligheid is upgraden naar een toestel met actieve update-ondersteuning nog steeds de beste optie.

Zo check je welke Android-versie je gebruikt
1. Open *Instellingen* op je Android-telefoon
2. Ga naar *Over de telefoon* (soms: *Info over de telefoon*)
3. Zoek naar *Android-versie*
   Daar zie je bijvoorbeeld: *Android 12*, *Android 13* of hoger staan.

Staat er Android 12 of lager?
Dan krijgt je toestel geen beveiligingsupdates meer van Google.

Extra tip:
In hetzelfde scherm staat vaak ook *Beveiligingsupdate van Android*.

Zie je daar een datum van langer dan een jaar geleden, dan is je toestel niet meer actueel beveiligd.

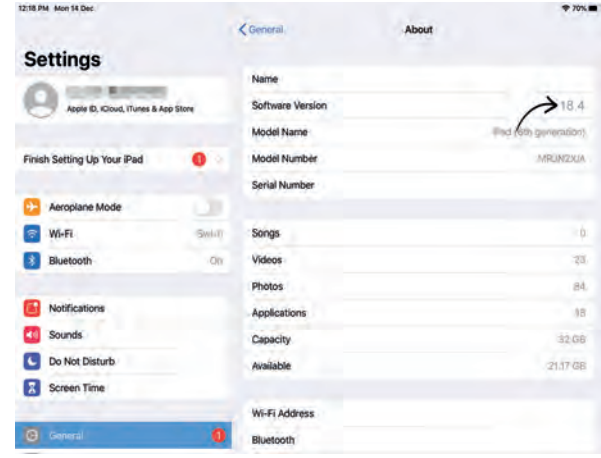


Welke iOS- of iPadOS-versie ondersteunt mijn iPhone of iPad?

Apple brengt regelmatig nieuwe updates uit voor de iPhone en iPad. Die updates zorgen voor **betere beveiliging**, **oplossingen voor problemen** en soms **nieuwe functies**.
Maar niet elk toestel krijgt altijd de nieuwste versie. Controleer dit zelf.

Welke versie staat er nu op mijn iPhone of iPad?
Zo zie je welke versie je gebruikt:
1. Open *Instellingen*
2. Tik op *Algemeen*
3. Tik op *Info*
4. Kijk bij *iOS-versie* (iPhone) of *iPadOS-versie* (iPad)
   Je ziet daar bijvoorbeeld: *iOS 18.1* of *iPadOS 18.0*.

Kan mijn toestel nog worden geüpdatet?
Zo controleer je of er een update beschikbaar is:
1. Open *Instellingen*
2. Tik op *Algemeen*
3. Tik op *Software-update*



Wat zie je nu?
- **Er staat een update klaar**
  → Je toestel wordt nog ondersteund en je kunt veilig bijwerken.
- **Uw software is up-to-date**
  → Dit is de nieuwste versie voor jouw toestel.

Belangrijk:
Ook als je geen grote nieuwe versie meer krijgt, stuurt Apple vaak nog beveiligingsupdates. Dat is heel belangrijk voor veilig gebruik.

Hoe lang ondersteunt Apple iPhones en iPads?
- iPhones en iPads krijgen gemiddeld **6 tot 7 jaar** updates
- Oudere toestellen vallen uiteindelijk af voor nieuwe functies
- Vaak blijven ze nog wél veilig dankzij beveiligingsupdates

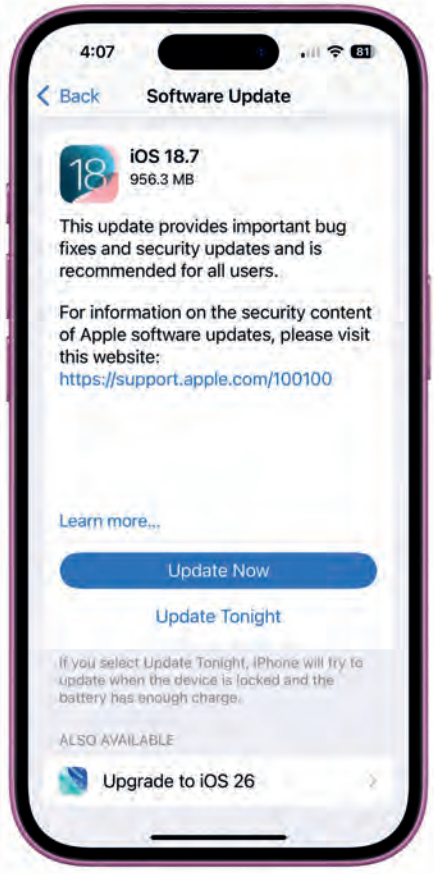
Voorbeeld:
- Nieuwere iPhones en iPads → nieuwste functies
- Oudere modellen → blijven bruikbaar, maar zonder vernieuwingen

Is mijn toestel dan meteen 'verouderd'?

Nee hoor

Je kunt je toestel vaak nog prima gebruiken:
- ✓ Bellen, mailen en internetten blijft gewoon werken
- ✓ Apps blijven meestal nog lange tijd bruikbaar
- ✓ Bankieren en DigiD werken vaak nog prima

Wel goed om te weten:
- Op termijn stoppen sommige apps met ondersteuning
- Nieuwe functies komen niet meer beschikbaar



Zo update je veilig (belangrijk!)

Voordat je gaat updaten:
- ✓ Zorg dat de **accu voldoende vol is** (of sluit de oplader aan)
- ✓ Maak een **reservekopie**
  - via **iCloud**
  - of via een computer (Finder of iTunes)

Daarna kun je met een gerust gevoel updaten.

Twijfel je? Dit is de snelste controle

Ga naar:

Instellingen → Algemeen → Software-update

Daar zie je meteen:
- of je toestel nog updates krijgt
- of je al helemaal bij bent

Makkelijker wordt het niet

Tip voor senioren

Voor 'belangrijke' toepassingen zoals:
- bankieren
- DigiD
- zorgapps
- e-mailen
- sociale media e.a. communicatie

Zorg dan altijd dat je **beveiligingsupdates** installeert. Die zijn minstens zo belangrijk als nieuwe functies.

HarmonyOS:
Huawei's alternatief voor Android en iOS

HarmonyOS is het besturingssysteem dat Huawei heeft ontwikkeld als alternatief voor Android en andere bekende platforms. Het systeem is bedoeld voor een brede reeks apparaten: smartphones, tablets, smartwatches, tv's, slimme apparaten in huis èn sinds kort ook laptops. Met *HarmonyOS* wil Huawei, zoals dat geformuleerd wordt: één samenhangend ecosysteem creëren, waarin apparaten naadloos samenwerken.

Waarom HarmonyOS?

Huawei begon de ontwikkeling van *HarmonyOS* in 2019. Aanleiding waren onder meer de beperkingen die het bedrijf kreeg opgelegd in de samenwerking met Amerikaanse technologiebedrijven. Daardoor kon Huawei niet langer volledig vertrouwen op Android en Google-diensten. U herinnert zich de 'reserve' die ook in Nederland ontstond bij het (voorgenomen) gebruik van Chinese apparatuur voor het mobiel 5G-data-/communicatie netwerk.
HarmonyOS werd het antwoord op Google's Android: een zelfstandig besturingssysteem, volledig in eigen beheer.

Eén systeem voor al je apparaten

Wat *HarmonyOS* onderscheidt van andere besturingssystemen, is het idee van een **universeel platform**. In plaats van aparte systemen voor telefoon, tablet, horloge en tv, gebruikt *HarmonyOS* één basis die zich aanpast aan het apparaat waarop het draait.
Huawei noemt dit een **distributed operating system**. In de praktijk betekent dit dat meerdere apparaten samen kunnen werken alsof ze één geheel vormen.
Voorbeelden:

- je smartphone fungeert als afstandsbediening voor je tv
- bestanden verplaatsen tussen telefoon en tablet zonder kabels
- het toetsenbord en de muis van een laptop gebruiken op een tablet
- meldingen en apps delen tussen meerdere schermen

Huawei noemt deze aanpak ook wel in alle bescheidenheid: **Super Device**.

Van Android-basis naar volledig eigen systeem

De eerste versies van *HarmonyOS* (vooral op smartphones) waren aanvankelijk deels gebaseerd op de open Android-broncode. Dat maakte het mogelijk om Android-apps te blijven gebruiken.

Sinds **HarmonyOS NEXT** (de nieuwste generatie) is Huawei echter een andere weg ingeslagen:

- geen Android-laag meer
- geen ondersteuning meer voor Android-apps
- volledig gebouwd op Huawei's eigen technologie

Apps moeten nu speciaal voor *HarmonyOS* worden ontwikkeld. Huawei zet daar stevig op in met eigen ontwikkeltools en een groeiende *AppGallery*.

Gebruiksgemak en uiterlijk

Voor gebruikers moet *HarmonyOS* modern en overzichtelijk aanvoelen. Het systeem lijkt op het eerste gezicht vertrouwd voor wie Android kent, maar heeft duidelijke eigen accenten.

Kenmerkende elementen:

- grote, informatieve widgets op het startscherm
- een overzichtelijk bedieningspaneel
- soepele animaties en duidelijke iconen
- consistente bediening op verschillende apparaten

Voor veel gebruikers is *HarmonyOS* vooral prettig omdat alles binnen het Huawei-'ecosysteem' logisch samenwerkt.

HarmonyOS op laptops en pc's

Sinds 2025 zet Huawei *HarmonyOS* ook in op laptops. Deze versie is geen aangepaste mobiele omgeving, maar een volwaardig desktopbesturingssysteem.

Belangrijke kenmerken:

- meerdere vensters en multitasking
- nauwe samenwerking met telefoon en tablet
- bestanden en apps delen tussen apparaten
- focus op productiviteit en creatief gebruik

Huawei positioneert *HarmonyOS* hiermee nadrukkelijk als alternatief voor Windows en macOS, al is deze ontwikkeling voorlopig vooral zichtbaar in China, alwaar de overheid alom tegenwoordig is.

Beschikbaarheid en gebruik buiten China

In China is *HarmonyOS* inmiddels wijdverbreid en wordt het op miljoenen apparaten gebruikt. Buiten China is de situatie anders:

- smartphones in Europa draaien vaak nog op *EMUI* (Huawei's Android-achtige schil)
- de beschikbaarheid van apps verschilt per regio
- nieuwe *HarmonyOS*-versies verschijnen meestal eerst in China

Toch breidt het 'ecosysteem' zich langzaam uit, ook internationaal.

Voordelen en aandachtspunten

Het moge duidelijk zijn dat Huawei zelf niet spreekt over 'nadelen', maar over 'aandachtspunten'.

Voordelen

- sterke samenwerking tussen apparaten
- modern en overzichtelijk systeem
- steeds meer eigen apps en diensten
- onafhankelijk van Google en Android

Aandachtspunten

- beperkter app-aanbod buiten China
- Android-apps werken niet meer op de nieuwste versies
- minder bekend bij het grote publiek in Europa

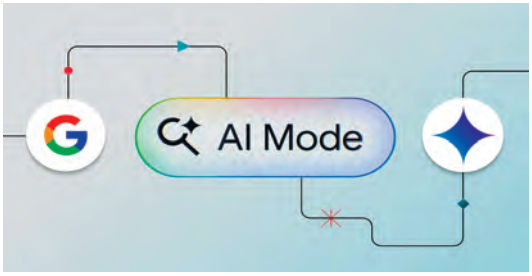
Conclusie

HarmonyOS is veel meer dan 'Android zonder Google'. Het is een ambitieus besturingssysteem dat is ontworpen rond het idee van één verbonden 'ecosysteem'. Vooral voor gebruikers die meerdere Huawei-apparaten gebruiken, biedt het duidelijke voordelen in gemak en samenwerking.

Of *HarmonyOS* ook buiten China echt een grote rol gaat spelen, hangt vooral af van de groei van het app-aanbod en de internationale beschikbaarheid. Recente politieke ontwikkelingen hebben ook de behoedzaamheid t.o.v. Amerikaanse software en diensten doen toenemen. Eén ding is zeker: Huawei ziet *HarmonyOS* als een kernonderdeel van zijn toekomst. Al blijft **de** weg die bescherming biedt tegen verborgen (staats- of commerciële) inmenging: **Open Software**.

De nieuwste ontwikkelingen in Google Foto
Meer AI, gratis tools en slimmer bewerken

Google Foto's blijft zich verder ontwikkelen: van ooit een simpele opslagdienst naar een krachtig, AI-gedreven bewerkingshulpmiddel nu. De nieuwste updates bergen geavanceerde functies in zich en maken – aldus Google – het bewerken en terugvinden van herinneringen makkelijker dan ooit. Dit zijn de belangrijkste veranderingen die men zou moeten kennen. U verwachtte het al: *AI* en *Gemini* voeren de boventoon.



Massale Vrijgave van AI-bewerkingshulpmiddelen (Voor Iedereen!)

Het grootste nieuws is dat Google een groot deel van zijn geavanceerde, AI-gestuurde bewerkingstools nu **gratis beschikbaar** stelt voor *alle* gebruikers (niet alleen Pixel-eigenaren of Google One-abonnees).

- de ***Magische Gum*** (***Magic Eraser***): Hiermee kunt u ongewenste objecten of personen moeiteloos uit uw foto's verwijderen.
- ***foto's verscherpen*** (***Unblur***): Red nu wazige of onscherpe foto's door de AI de focus te laten verbeteren.
- ***cinematische Foto's***: Transformeer uw statische foto's in korte 3D-achtige video's.

Let op: Hoewel deze tools gratis zijn, kan het zijn dat er voor de meest geavanceerde functie, de **Magic Editor**, een limiet van 10 exporten per maand geldt voor niet-abonnees.

'Help me bewerken': De kracht van *Gemini* in uw Editor

Google introduceert slimme, door *Gemini* aangedreven bewerkingsmogelijkheden om complexe aanpassingen uit te voeren met simpele opdrachten.

- **Eenvoudige tekstcommando's**: U kunt nu in natuurlijke taal vragen om wijzigingen, zoals: '*Verwijder de zonnebril van mijn vader*' of '*Maak de lucht blauwer*'.
- **Restyle met *Nano Banana***: Een spectaculaire nieuwe functie waarmee u de stijl van een afbeelding volledig kunt transformeren. Denk aan het veranderen van een gewone foto in een schilderij in de stijl van Van Gogh of een Renaissance-portret.

De Zoekfunctie wordt veel slimmer met *Ask Photos*

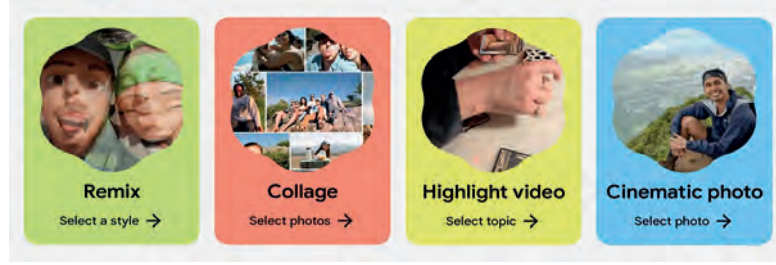
Het doorzoeken van duizenden foto's en video's wordt nu een gesprek. De ***Ask Photos***-functie heeft meer functionaliteit gekregen en maakt gebruik van de kracht van *Gemini* om context te begrijpen in plaats van alleen trefwoorden.

- **vraag in natuurlijke taal**: U hoeft niet langer te zoeken op trefwoorden. Vraag simpelweg: '*Laat de foto's zien van de laatste keer dat we met tante Karin gingen wandelen.*' of '*Wat is het kenteken van de auto die ik vorig jaar heb gehuurd?*'
- **resultaten op basis van context**: De AI koppelt namen, locaties, objecten en gebeurtenissen aan elkaar voor nauwkeuriger resultaten dan voorheen.

Verbeterde organisatie en nieuw 'Creëren'--Tabblad

De interface van Google Foto's heeft een nieuw tabblad om uw creativiteit de vrije loop te laten:

- **vernieuwde Editor**: De bewerkingsinterface is gestroomlijnd en gebruiksvriendelijker.
- het **'Creëren'-tabblad**: Dit is een nieuwe, centrale plek voor alle opties om iets nieuws te maken, zoals **collages, animaties** en **highlight-video's**.



- **eenvoudig delen met QR-codes**: U kunt nu direct een album delen door een unieke QR-code te genereren die anderen kunnen scannen, aantrekkelijk bij evenementen.

Conclusie: de toekomst is AI-gedreven

Google Foto's is, zoals vele geautomatiseerde toepassingen, de weg ingeslagen van geavanceerde, AI-gedreven data-verwerking, en heeft die in Google Foto's beschikbaar gesteld voor het 'grote publiek'. 'Google denkt groot', zoals algemeen bekend mag worden verondersteld. Of u nu snel een ongewenst element wilt verwijderen of een compleet nieuwe stijl wilt creëren, de updates maken Google Foto's: *tot een onmisbare app op elke Android-telefoon*.
Dank u, Alphabet Inc., dat ook door *AI* zijn gebruikers meer en meer kent en boeit.

Voordelig Apple Watch alternatief met lange accuduur

Bert van Dijk

De Apple Watch is veruit de meest verkochte smartwatch. Een groot nadeel is echter de korte accuduur, waardoor je hem vaak elke dag moet opladen. Een interessant voordelig alternatief voor de Apple Watch is bijvoorbeeld de *Xiaomi smart band 9 Pro*. Met de standaard-instellingen hoef je deze fitnesstracker pas na ongeveer drie weken op te laden. Zet je veel extra functies aan, zoals een allways on-scherm, dan haal je nog steeds een accuduur van 8 dagen.

Dit slimme horloge met GPS en fitnesstracker lijkt uiterlijk heel sterk op de Apple Watch maar kost bij *Xiaomi* zelf maar € 59,99. Door de vormgeving en presentatie van hun producten wordt Xiaomi vaak de Chinese Apple genoemd. Via de *Mi Fitness*-app kun je dit slimme horloge met iPhone- en Android-smartphones gebruiken.

Ondanks de lage prijs is de Smart Band 9 Pro degelijk gebouwd met een aluminium kast in drie kleuren (zilver, mat zwart en roze) en een helder 1,74" Amoled-scherm, dat met 1200 nits ook goed afleesbaar is in zonlicht. Door de licht gebogen randen met een smalle schermrand komt het uiterlijk heel dichtbij een Apple Watch.

Ervaringen in het dagelijks gebruik

De Smart Band 9 Pro heeft een handig systeem om snel van horlogeband te wisselen. Omdat het standaard zwarte sportbandje wat lastig was om vast te maken, heb ik via Amazon voor slechts € 6,78 drie elastische *Sugarjar Nylon* horlogebandjes gekocht die je met een klitsysteem heel gemakkelijk om kunt doen en die ook veel fijner aanvoelen.

Door het lage gewicht voel je bijna niet dat je de Smart Band 9 Pro om hebt. Met de always-on schermfunctie ingeschakeld hoefde ik pas na 8 dagen weer op te laden. Dit volledig opladen duurt 1 uur en 15 minuten.

Heel fijn is ook de hoge krasbestendigheid. Na weken intensief gebruik zag ik nog geen gebruikssporen. In vergelijking met mijn oude Apple Watch miste ik nog het meest het betalen met Apple Pay. Ook meldingen van nieuwe Whatsapp-berichten kwamen nog niet goed door. Mogelijk dat dit pas goed gaat werken als ik de Apple Watch verwijder van mijn iPhone. In Europa heeft Apple van de EU namelijk wat aanpassingen moeten doen, waardoor meldingen beter kunnen doorkomen op smartwatches van andere fabrikanten. Dit was ook een reden voor deze review. Wat mij daarbij erg opviel was hoe

Xiaomi ook het uiterlijk en de bediening van veel schermen op de Apple Watch laat lijken.

Een uitgebreide uitleg van alle mogelijkheden vind je in de Youtube-video Best Fitness Tracker (**https://youtu.be/Awa-dfug1kw?si=-A2dIJZUeGKXW3KM**) van 2025? als je zoekt op *smart band pro 9* en *Tech Spur*t.

Uitgebreide meetfuncties

De Band 9 Pro beschikt over een ingebouwde GNSS-chip die met signalen van meerdere satellietsystemen nog nauwkeuriger je locatie bijhoudt. Zo kun je precies vastleggen waar je bent geweest. De *Xiaomi Band 9* heeft een continue monitoring van je hartslag. Bij een abnormale hartslag krijg je een melding.

Ook wordt het zuurstofgehalte in je bloed gemeten. Verder biedt het slaaptracking, stress monitoring en kan het bij vrouwen de menstruatiecyclus bijhouden. Het apparaatje heeft meer dan 150 sportmodi voor o.a. hardlopen, fietsen, zwemmen, yoga en gespecialiseerde sporten zoals roeien en dansen. Voor hardlopers zijn er extra gegevens, zoals stapfrequentie, grondcontacttijd en verticale oscillatie, om je looptechniek te verbeteren. De smartwatch is met 5 atm volledig waterdicht, zodat je hem bij het zwemmen en douchen altijd om kunt houden.

Conclusie

Met deze Xiaomi Smart Band 9 Pro is ook de prijs geen reden meer om een gewone horloge te dragen. Je hebt keuze uit een groot aantal bandjes en schermindelingen, zodat je het voor elke gelegenheid kunt aanpassen. Omdat dit model al ongeveer anderhalf jaar op de markt is, wordt dit jaar wel een opvolger verwacht met waarschijnlijk nog wat nauwkeuriger GPS-prestaties.

Plus

- afstandsbediening camera
- ook vanuit iPhone komen veel meldingen door
- vastleggen routes
- ondersteunt meer dan 150 sporten

Min

- minder functies (o.a. geen speaker, nfc, crashdetectie en navigatie)
- geen 'beantwoorden' berichten
- geen home-knop

AirDrop: Alles wat je moet weten

Van Apple-only naar cross-platform: hoe *AirDrop* werkt en wat er nieuw is in 2026

Wat is *AirDrop*?

AirDrop is Apple's draadloze technologie, waarmee je bestanden, foto's, links en meer kunt delen tussen apparaten. Je hebt er geen internetverbinding voor nodig. *AirDrop* maakt gebruik van een combinatie van wifi en Bluetooth om een directe verbinding tussen apparaten op te zetten. Bestanden worden overgedragen in originele kwaliteit, zonder compressie. De technologie is beschikbaar op iPhone, iPad en Mac, en is al jaren een van de meest geliefde functies binnen het Apple-ecosysteem. Maar dat ecosysteem is aan het veranderen.

Wat kun je delen via *AirDrop*?

AirDrop ondersteunt vrijwel elk type bestand of inhoud dat je op je Apple-apparaat kunt vinden:

- foto's en video's (in originele, ongecomprimeerde kwaliteit)
- documenten, pdf's en Office-bestanden
- contacten (.vcf)
- locaties via de Kaarten-app
- websites en links vanuit Safari
- wachtwoorden en passkeys (vanuit *Instellingen* of de *Wachtwoorden-app*)
- notities en herinneringen
- app-suggesties uit de App Store
- muziek, playlists en podcasts via Apple Music

Hoe werkt AirDrop?

AirDrop gebruikt Bluetooth om apparaten in de buurt te ontdekken en schakelt vervolgens over op een directe wifi-verbinding voor de daadwerkelijke overdracht. Dit maakt de overdracht snel - ook voor grote bestanden. De reikwijdte van Bluetooth is ongeveer 9 meter.

Je kiest zelf wie jou kan vinden via *AirDrop*. Er zijn drie opties:

- niemand - *AirDrop* staat volledig uit
- alleen contacten - alleen mensen in jouw adresboek kunnen je zien
- iedereen - alle Apple-gebruikers in de buurt kunnen je een verzoek sturen (tijdelijk in te stellen)

De ontvanger krijgt altijd een melding met een voorvertoning van het bestand, en moet de overdracht handmatig accepteren. Zo kun je nooit ongewenst bestanden ontvangen.

Nieuw in 2025–2026: *AirDrop* naar Android

Een van de grootste veranderingen in de geschiedenis van *AirDrop*! Apple heeft de technologie opengesteld voor Android. In 2025 werd *AirDrop*-interoperabiliteit gelanceerd, te beginnen met de Google Pixel 10-serie. In 2026 wordt de ondersteuning uitgebreid naar meer Android-apparaten.

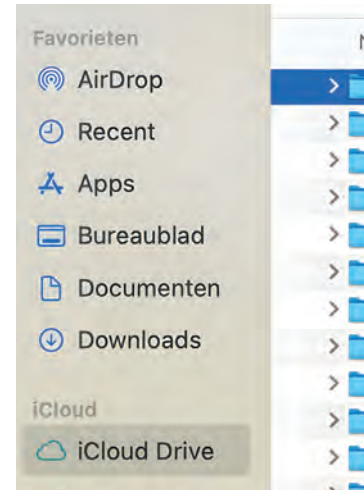
Dit betekent dat je straks rechtstreeks van een iPhone naar een Android-telefoon kunt delen - en vice versa - zonder tussenkomst van apps als WhatsApp of Google Drive. Apple werkt samen met fabrikanten om de integratie zo breed mogelijk beschikbaar te maken.

AirDrop en Windows: alternatieven

Directe *AirDrop*-ondersteuning voor Windows bestaat nog niet. Maar Microsoft biedt met *Phone Link* (op de pc) en *Link to Windows* (op Android) een vergelijkbare functie aan: naadloos bestanden uitwisselen tussen Windows en Android, zonder kabels of apps van derden.

Andere draadloze alternatieven voor bestandsdeling tussen platforms:

- *Quick Share* (voorheen Nearby Share) - Google's eigen *AirDrop*-equivalent voor Android en Chrome OS, ook beschikbaar op Windows
- *Snapdrop* / *LocalSend* - open-source webtools die werken op elk apparaat in hetzelfde wifi-netwerk
- *iCloud Drive* - handig als je al in het Apple-ecosysteem zit en wilt delen met Mac/Windows



Handige tips voor dagelijks gebruik

- deel tussen je eigen apparaten: *AirDrop* werkt ook uitstekend om snel iets van je iPhone naar je Mac te sturen, zonder iCloud of een kabel.
- ontvangen bestanden op Mac staan altijd in de map Downloads.
- zet *AirDrop* op 'Iedereen' alleen wanneer je het actief gebruikt - daarna weer terugzetten voor je privacy.
- zit de ontvanger niet in je contacten? Vraag hem of haar even *AirDrop* open te zetten op 'iedereen'.
- grote bestanden (zoals onbewerkte video's) gaan via *AirDrop* veel sneller dan via e-mail of WhatsApp.

Conclusie

AirDrop is al jaren een van de meest gebruiksvriendelijke manieren om bestanden te delen - snel, betrouwbaar en zonder kwaliteitsverlies. Met de opening naar Android in 2025 en de verdere beschikbaarheid in 2026 wordt de functie steeds minder gebonden aan het Apple-ecosysteem.

Android Auto
Hoe werkt het en wat kun je ermee?

Android Auto dient om de functies van je Android-telefoon veilig te gebruiken in de auto bijvoorbeeld: navigatie, bellen, berichtjes, muziek en spraakbediening, maar dan via het grotere scherm van je auto – of via je telefoon als je auto geen display heeft.

Android Auto werkt op twee manieren

a) Via het scherm van je auto (de dashboard-versie)

Je koppelt je telefoon met:

- *USB-kabel* (stabiel en in elke ondersteunde auto)
- *Draadloos* (werkt bij de meeste nieuwere auto's)

Daarna verschijnt een speciaal, vereenvoudigd Android Auto-scherm op de *infotainmentunit* (mooier kunnen we het woord niet maken) van de auto.

Bediening kan via:

- touchscreen
- knoppen aan het stuur
- spraak (Google Assistant)

b) Zonder auto-scherm: Android Auto op je telefoon

Is je auto ouder en heeft hij geen ingebouwd scherm, dan kun je Android Auto ook **rechtstreeks op je smartphone gebruiken** (met de *Bestuurdersmodus*), bijvoorbeeld in een telefoonhouder.

De belangrijkste functies

✓ **Navigeren**

- *Google Maps*, *Waze*, *TomTom AmiGO*, enz.
- Live verkeersinformatie
- Flitsers/gevaarlijke situaties (afhankelijk van app)
- Automatisch route aanpassen

✓ **Bellen & berichten**

- Handsfree bellen
- WhatsApp-, SMS- en Signal-berichten laten voorlezen
- Nieuwe berichten dicteren via spraak

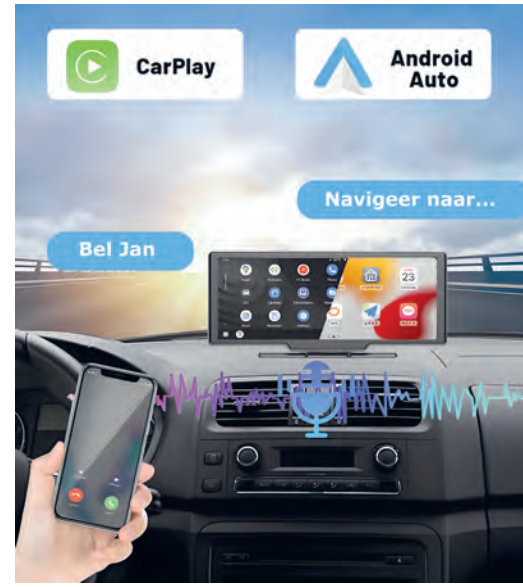
✓ **Muziek & podcasts**

- Spotify
- YouTube Music
- Audible
- NPO Luister / podcasts

  Goedkoop en veilig te bedienen tijdens het rijden.

✓ **Spraakbesturing (Google Assistent)**

- 'Hey Google, navigeer naar huis'
- 'Speel mijn favoriete playlist'
- 'Lees mijn berichten voor'
- 'Bel Jan'



✓ **Slimme auto-functies (bij nieuwere modellen)**

Niet elke auto heeft dit, maar mogelijk zijn:

- Weersinformatie
- Agenda
- Energieverbruik (bij electrische auto's via merk-apps)
- Smart Home-commando's (bijv. 'Zet de verwarming thuis alvast aan')

Auto's die Android Auto ondersteunen

Android Auto werkt in auto's:

- met een compatibele infotainmentunit
- meestal vanaf bouwjaar **2016–2017**
- veel merken ondersteunen het standaard: Volkswagen, Toyota, Hyundai, Kia, Peugeot, Opel, Ford, Renault, Volvo, BMW (vanaf 2020), Mercedes, enz.

Bij sommige oudere auto's moet Android Auto:

- vrijgeschakeld worden via een update
- of je moet een 'aftermarket'-radio gebruiken (bijv. Pioneer, Kenwood)

Auto's zonder ingebouwd scherm

Dan kun je:

- Android Auto op je telefoon gebruiken
- of een los Android Auto-scherm kopen (bijv. van *AAWireless*, *Pioneer* of kleine dashboard-schermen, 7 tot 9 inch, prijzen van ca. 60 – 200 Euro)

Wat heb je nodig om Android Auto te gebruiken?

- Android-telefoon met minimaal ***Android 6.0*** (bij voorkeur Android 10+)
- de ***Android Auto-app*** (meestal al ingebouwd)
- een ***geschikte auto*** of een losse unit
- USB-kabel of draadloze verbinding (WiFi + Bluetooth)

Voordelen

- veilig: minder handelingen, meer spraakbediening
- overzichtelijk: grote knoppen, eenvoudige interface
- altijd up-to-date navigatie (geen dure auto-kaarten meer)
- je eigen muziek- en chatapps in de auto
- werkt met bijna elke moderne Android-telefoon

Nadelen

- je telefoonaccu gaat sneller leeg (vooral bij draadloos gebruik)
- niet elke app werkt (bijv. video is geblokkeerd tijdens het rijden)
- draadloze Android Auto werkt niet op elke auto
- soms is een goede USB-interface of -kabel nodig voor stabiele verbinding

***PS** (van de redactie)*

Ook Apple heeft soortgelijke voorzieningen: *Apple CarPlay*

Heb je nog een virusscanner nodig op je Windows-pc?

Wie al wat langer met computers werkt, herinnert zich vast nog de tijd dat een virusscanner onmisbaar was. Zonder antivirussoftware liep een Windows-computer al snel een virus op. Fabrikanten van beveiligingssoftware hadden het dan ook druk met het bestrijden van allerlei digitale bedreigingen.
Maar de wereld van computerbeveiliging is veranderd. Moderne versies van **Microsoft Windows 11** en **Windows 10** hebben namelijk al een uitgebreide beveiliging ingebouwd. Daardoor vragen veel mensen zich tegenwoordig af: **heb je nog wel een aparte virusscanner nodig?**
Het korte antwoord: meestal niet. Maar er zijn wel een paar nuances.

De ingebouwde beveiliging van Windows

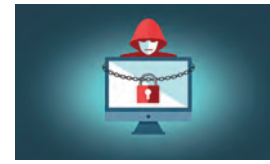
In elke moderne Windows-computer zit standaard *Microsoft Defender*. Dit beveiligingspakket draait automatisch op de achtergrond en beschermt de computer tegen virussen, malware en andere digitale bedreigingen.
Microsoft Defender biedt onder andere:

- realtime bescherming tegen virussen en malware
- controle van downloads en programma's
- bescherming tegen phishingwebsites
- bescherming tegen ransomware
- een ingebouwde firewall
- automatische beveiligingsupdates

Een groot voordeel is dat alles **automatisch wordt bijgewerkt via Windows Update**. De gebruiker hoeft dus nauwelijks iets te doen om de beveiliging actief te houden.
Tot ongeveer tien jaar geleden werd *Microsoft Defender* nog niet altijd serieus genomen. In die tijd scoorden commerciële virusscanners vaak beter in onafhankelijke tests. Maar Microsoft heeft de beveiliging de afgelopen jaren flink verbeterd.
Tegenwoordig scoort *Defender* in tests van beveiligingslaboratoria vaak **net zo goed als veel betaalde antivirusprogramma's**.

Wat doen virussen tegenwoordig eigenlijk?

Het klassieke computervirus – dat zichzelf verspreidt via bestanden – bestaat nog steeds, maar moderne digitale dreigingen zijn vaak ingewikkelder.
Veel voorkomende vormen van malware zijn bijvoorbeeld:



Ransomware
Kwaadaardige software, die bestanden versleutelt. De aanvaller vraagt vervolgens losgeld om de bestanden weer toegankelijk te maken.

Spyware
Software die ongemerkt informatie verzamelt, zoals wachtwoorden of surfgedrag.

Phishing
Misleidende e-mails of websites die proberen gebruikers te laten inloggen op een nepwebsite om zo wachtwoorden te stelen.

Malware via downloads
Soms zit schadelijke software verstopt in gratis programma's of illegale downloads.

Een goede virusscanner – of dat nu *Defender* is of een ander programma – probeert deze bedreigingen automatisch te herkennen en te blokkeren.

Bekende virusscanners voor Windows

Hoewel *Microsoft Defender* tegenwoordig veel kan, bestaan er nog steeds veel aparte antivirusprogramma's. Bekende voorbeelden zijn:

- **Norton 360**
- **Bitdefender Antivirus**
- **McAfee Total Protection**
- **ESET NOD32 Antivirus**
- **Avast Free Antivirus**
- **Avira Free Security**

Deze programma's bieden in de basis dezelfde bescherming als *Microsoft Defender*: ze controleren bestanden, downloads en websites op schadelijke software.
Het verschil zit vaak in de **extra** functies die worden aangeboden.

Extra functies van betaalde beveiligingspakketten

Veel commerciële antiviruspakketten proberen zich te onderscheiden met aanvullende mogelijkheden. Denk bijvoorbeeld aan:

- een **VPN-verbinding** om veiliger te internetten op openbare wifi
- een **wachtwoordmanager**
- controle of je e-mailadres voorkomt in een datalek
- bescherming tegen identiteitsfraude
- ouderlijk toezicht voor gezinnen
- bescherming van meerdere apparaten met één abonnement

Voor mensen die zulke functies willen gebruiken, kan een betaald pakket aantrekkelijk zijn. Maar strikt genomen zijn die extra's **niet noodzakelijk voor de basisbeveiliging van een Windows-pc**.

Twee virusscanners tegelijk: liever niet

Een veelgemaakte fout is het installeren van meerdere virusscanners tegelijk. Dat lijkt misschien extra veilig, maar het kan juist problemen veroorzaken.
Virusscanners controleren voortdurend bestanden en programma's. Als twee beveiligingsprogramma's dat tegelijk doen, kunnen ze elkaar in de weg zitten.
Dat kan leiden tot:

- een trager systeem
- foutmeldingen
- conflicten tussen programma's

Daarom is het verstandig **slechts één realtime virusscanner actief te hebben**.

Een handige tussenoplossing

Sommige computergebruikers kiezen voor een praktische tussenweg. Zij laten *Microsoft Defender* gewoon actief en gebruiken daarnaast af en toe een extra scanner voor een controle.

Een bekend programma hiervoor is *Malwarebytes*. Dit kan bijvoorbeeld één keer per maand een extra scan uitvoeren om te controleren of er niets over het hoofd is gezien.
Omdat zo'n programma niet continu op de achtergrond draait, veroorzaakt het meestal geen conflicten met de standaard Windows-beveiliging.

De belangrijkste beveiliging: gezond verstand

Hoe goed een virusscanner ook is, uiteindelijk blijft de gebruiker zelf de belangrijkste beveiliging.

Veel infecties ontstaan doordat mensen:
- programma's downloaden van onbekende websites
- op verdachte links in e-mails klikken
- nepwebsites vertrouwen
- illegale software installeren

Met een paar eenvoudige regels kun je al veel problemen voorkomen:
- download software alleen van betrouwbare websites
- open geen verdachte e-mailbijlagen
- houd Windows en programma's up-to-date
- gebruik sterke en unieke wachtwoorden
- maak regelmatig een back-up van belangrijke bestanden

Wie deze basisregels volgt, verkleint de kans op problemen aanzienlijk.

Conclusie

De tijden dat elke Windows-computer per se een aparte virusscanner nodig had, zijn voorbij. Dankzij *Microsoft Defender* beschikken Microsoft **Windows 11** en **Windows 10** al over een krachtige standaardbeveiliging.

Voor de meeste thuisgebruikers is die bescherming ruim voldoende. Extra antivirussoftware kan interessant zijn vanwege aanvullende functies, maar is voor de basisbeveiliging meestal niet noodzakelijk.

Wie daarnaast ook nog verstandig met internet en downloads omgaat, heeft al een **sterke eerste verdedigingslinie tegen digitale dreigingen**.

Praktische vuistregel

Met een actuele Windows-computer, *Microsoft Defender* ingeschakeld en de vijf in de kadertekst genoemde basisregels ben je al verrassend goed beschermd tegen de meeste digitale gevaren.

Maar blijf natuurlijk waakzaam, bijvoorbeeld bij wachtwoordprocedures en het verlenen van online-toestemming, de cookiesfabriek is nog lang niet gesloten, ook al zijn ongewenste koppelingen en reclame niet meteen gelijk aan malware. En AI zal ons nog de nodige 'uitdagingen' bieden!

5 tips om je Windows-pc veilig te houden

1. **Houd Windows altijd up-to-date**
   Updates zijn niet alleen bedoeld voor nieuwe functies, maar vooral voor beveiliging. In Microsoft Windows 11 en Windows 10 worden beveiligingslekken regelmatig gerepareerd via Windows Update. Zet automatische updates daarom altijd aan.

2. **Gebruik sterke en unieke wachtwoorden**
   Veel hacks beginnen met een zwak wachtwoord. Gebruik daarom lange wachtwoorden en bij voorkeur voor elke website een ander wachtwoord. Een wachtwoordmanager kan daarbij helpen.

3. **Let op verdachte e-mails en links**
   Cybercriminelen proberen vaak via phishing toegang te krijgen tot accounts. Klik daarom niet zomaar op links in e-mails en controleer altijd het webadres van een website voordat je inlogt.

4. **Download software alleen van betrouwbare websites**
   Gratis programma's van onbekende websites kunnen verborgen malware bevatten. Download software bij voorkeur van de officiële website van de maker of via betrouwbare downloadsites.

5. **Maak regelmatig een back-up**
   Mocht er toch iets misgaan, bijvoorbeeld door een virus of ransomware, dan kun je met een back-up altijd je bestanden terughalen. Dit kan eenvoudig met een externe harde schijf of met een online dienst zoals Microsoft OneDrive of Google Drive.