Zesentwintigste jaargang nummer 04: April 2025

De COMPUTERCLUB

Nissewaard

Computerclub Nissewaard voor iedereen en iedere leeftijd

Al meer dan 25 jaar een begrip

Colofon

Dagelijks bestuur

1e Coördinator :	**H.P.Kubbinga**	**Tel. 0181-640669**
2e Coördinator :	**B.W.Tijl**	**Tel. 0654692942**

Vrijwilligers Computerclub Nissewaard

Lesgevende	**:**	**Bart Tijl**
Lesgevende	**:**	**Hans Kubbinga**
Lesgevende	**:**	**Karel Kleijn**
Netwerkbeheerder	**:**	**Peter Mout**
Boekje	**:**	**Bart**
Website	**:**	**Ben Boukes**

Correspondentieadre is:
computerclubnissewaard@gmail.com
of
Mob: 06-54692942

Internet: www.computerclubnissewaard.nl

M.A. de Ruijterstraat 3, 3201CK Spijkenisse

Bestuursmededeling
April 2025
Beste leden,

Het eerste kwartaal van dit jaar 2025 zit er alweer op.
Er hebben zich weer diverse activiteiten plaats gevonden.
O.a. de verhuizing naar het ‘t Centrum wat achteraf toch rustig is verlopen.
Het is even wennen om nu zelf de catering te verzorgen, maar iedereen weet alles te vinden.
Op 8 maart was er de internationale vrouwendag in wijkgebouw Noord.
Wij waren er om promotie te maken en eventueel telefoon/computer of tablethulp en uitleg te geven.
Er waren veel bezoekers maar het heeft helaas nog niet gezorgd voor nieuwe leden.
In April hebben we Goede Vrijdag en Pasen.
Dit is niet op woensdag dus lessen gaan door.
Op 28 mei 2025 zal onze laatste lesdag zijn voor de zomervakantie die dan op 01-10-2025 weer zal starten.
www.computerclubnissewaard.nl
Groet van *Hans, Bart, Karel, Peter en Ben.*

Servicepagina:

Deze pagina is een vast onderwerp in het boekje en geeft u informatie over het doen en laten van Computerclub Nissewaard.
Lidmaatschap kost u maandelijks **€ 10,00**
U kunt bij ons een cursus volgen vanaf **€ 25.00 incl. Lesmateriaal.**
Ons bankrekeningnummer is NL44ABNA0506627470 tav B.W.Tijl
Bij mededelingen vermelden CCNissewaard.

Wilt U zomaar een avondje doorbrengen bij ons dan kan dat ook.
U brengt dan een bijdrage van €2.50 per avond mee.

Hulp bij Computerstoringen of Software problemen kan ook bij ons.
Natuurlijk exclusief de materiaalkosten.

Bij het beëindigen van het Lidmaatschap, dient u een opzeggingstermijn **van één maand** in acht te nemen en dit **schriftelijk** te melden aan :
Computerclubnissewaard@gmail.com,
Tel 0654692942

Hebt u vragen en of opmerkingen, mail ons uw probleem en dan kunnen wij er samen wel uit komen.

Computerclub Nissewaard de gezelligste club in de regio.
Bij ons krijgt u meer voor minder, vertel dit verder

M.A. de Ruijterstraat 3, 3201CK Spijkenisse

Inhoudsopgave

Met dank aan Seniorweb, CTnieuws en Schoone Pc

februari 2025
Bescherm je thuisnetwerk: DNS-filters voor zorgeloos surfen
Veel sites bevatten trackers, vervuilen pagina's met advertenties of nog erger: bevatten malware. Het is dus beter om ze te vermijden, maar hoe doe je dat voor je hele thuisnetwerk? Dit kan met DNS-filtersoftware, die je vanuit de cloud gebruikt of installeert op een pc of NAS.
In dit artikel laten we zien hoe je DNS-filtering instelt om advertenties, malware en trackers op je thuisnetwerk te blokkeren: • **Configureer het DNS-filter voor je netwerk • Beheer filterlijsten en blokkeer specifieke domeinen • Gebruik dynamische DNS (DDNS) om je netwerk continu te beschermen** Wat je moet weten: Van A naar B: zo werken IP-adressen
Wanneer je een webadres invoert, zorgen DNS-servers (Domain Name System) ervoor dat dit adres wordt omgezet naar het bijbehorende ip-adres. Zo kan een applicatie verbinding maken met de juiste server. Meestal gebruik je hiervoor de DNS-server van je internetprovider of een publieke DNS-server, zoals die van Google. Stel nu even dat je software hebt die alle DNS-verzoeken van je systeem onderschept voordat ze naar een DNS-server gaan en die automatisch de toegang tot onveilige websites kan blokkeren. Dit is precies wat DNS-filters doen en als je wilt, geldt dit type filter direct voor je hele thuisnetwerk, inclusief je desktop, laptop en mobiele apparaten.
In dit artikel komen twee gratis tools aan bod. De eerste is OpenDNS Home, een eenvoudige cloudoplossing. Heb je een NAS of een (oude) pc ter beschikking en schrikt enig configuratiewerk je niet af, dan is de tweede een beter alternatief: AdGuard Home, dat je lokaal kunt draaien.
Welk DNS-filter je ook gebruikt, je zult de DNS-server(s) die je systeem of je netwerk momenteel gebruikt, moeten aanpassen. We gaan hierbij uit van IPv4. Een vervelend klusje dat we meteen toelichten, waarna we ons volledig op de filters zelf kunnen focussen.

DNS-instelling op apparaatniveau

We bekijken eerst hoe je een DNS-server wijzigt op je pc of mobiele apparaat, bijvoorbeeld wanneer je het DNS-filter enkel op systeemniveau wilt instellen en niet voor je hele netwerk.

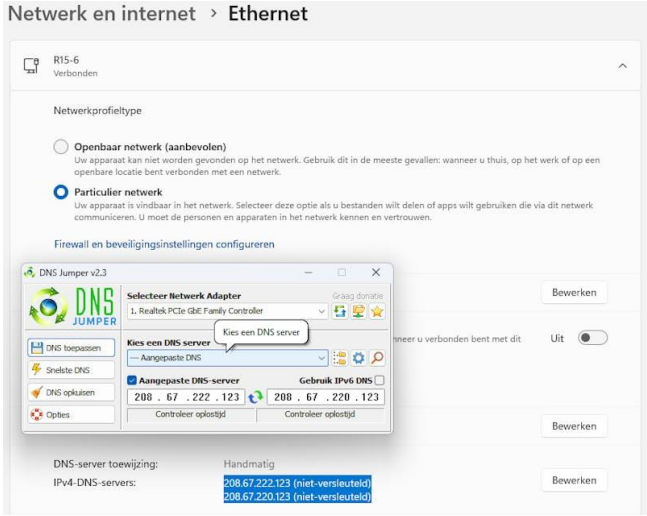
Op Windows 11 ga je naar **Instellingen**, kies je **Netwerk en internet**, en selecteer je **Ethernet** of **Wi-Fi / Hardware-eigenschappen**. Klik bij **DNS-server toewijzing** op **Bewerken**, kies **Handmatig** en activeer **IPv4**. Vul bij **Voorkeurs-DNS** het adres van de primaire DNS-server in en bij **Alternatieve DNS** dat van de secundaire. Bevestig met **Opslaan**.

Je kunt hiervoor ook gratis DNSJumper

https://www.sordum.org/7952/dns-jumper-v2-3/

gebruiken. Start de tool, selecteer de netwerkadapter en noteer de huidige instellingen. Vink vervolgens **Aangepaste DNS-server** aan, vul de primaire en secundaire DNS-servers in en bevestig met **DNS toepassen**.

Ook op mobiele apparaten, bijvoorbeeld een Android-toestel, kun je de DNS-server aanpassen. Ga naar **Instellingen**, kies **Netwerk en internet**, selecteer **Internet** en tik op het tandwiel bij de actieve wifi-verbinding. Tik op het potloodicoon, ga naar **Geavanceerde opties**, kies **DHCP Statisch** en voer de gewenste ip-adressen in bij **DNS 1** en **DNS 2**. De instructies kunnen licht variëren, afhankelijk van je apparaat of Android-versie.



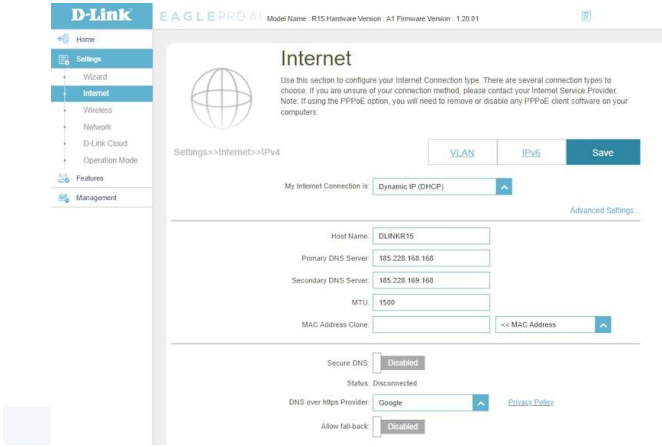
Je kunt de DNS-instellingen op een Windows-pc ook aanpassen via de tool DNS Jumper.

DNS-instelling op netwerkniveau

De bedoeling van dit artikel is om het DNS-filter direct voor je hele thuisnetwerk te activeren door de DNS-server op je router aan te passen. De werkwijze kan per router verschillen, maar de volgende stappen helpen je op weg. Raadpleeg eventueel de handleiding van je router.

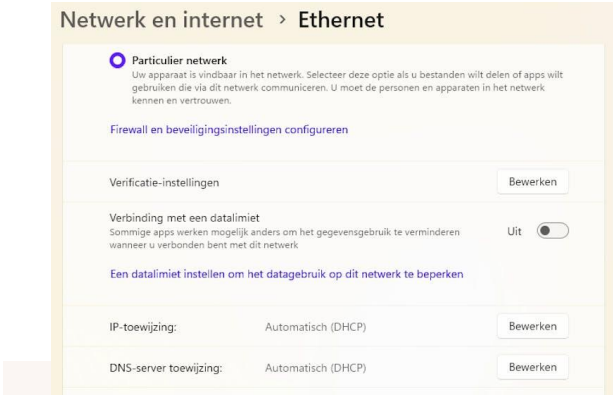
Typ het interne ip-adres van je router in je browser (vaak **192.168.0.1** of **192.168.1.1**). Dit adres vind je door in de Opdrachtprompt het commando **ipconfig** uit te voeren en het adres bij **Default Gateway** van je actieve netwerkadapter te noteren.

Log in op de set-uppagina van je router en open een rubriek als **Internet**, **Network** of **WAN**, eventueel onder **Advanced Settings**. Hier kun je de opties **Primary DNS Server** en **Secondary DNS Server** aanpassen, en bevestigen met **OK** of **Save (afbeelding 2)**.



De exacte plek voor het wijzigen van DNS-servers kan per router verschillen.

Zorg ervoor dat je netwerkapparaten automatisch de DNS-servers van de router overnemen. Dit gaat het makkelijkst als de DHCP-server op je router is ingeschakeld (wat meestal het geval is), en als ip- en DNS-toewijzing op je apparaten automatisch via DHCP verloopt. In Windows 11 vind je deze opties bij **Instellingen / Netwerk en internet**, waarna je **Wi-Fi / Hardware-eigenschappen** en/of **Ethernet** kiest.



*Je stelt de toewijzingen het best in op automatisch om de DNS-servers van je router over te nemen.*DNS-servers met filter

Als je de eerste paragrafen hebt doorgenomen, kun je direct starten

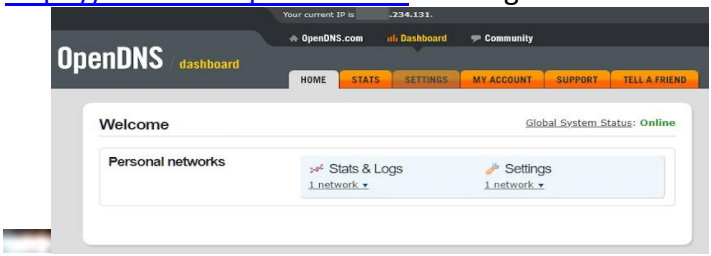
Dienst/server	Primair ip-adres	Secundair ip-adres	Filters
OpenDNS FamilyShield (Cisco), www.opendns.com/home-internet-security	208.67.222.123	208.67.220.123	Malware, phishing, pornografie
AdGuard DNS, https://adguard-dns.io	94.140.14.14	94.140.15.15	Advertenties, malware, trackers
Quad9, www.quad9.net	9.9.9.9	149.112.112.112	Botnets, malware, phishing
CleanBrowsing Family, www.cleanbrowsing.org/filters	185.228.168.168	185.228.169.168	Malware, phishing, pornografie

met een cloud-DNS-server met ingebouwd filter. Vul de ip-adressen van een van de gratis DNS-diensten uit de tabel in bij je primaire en secundaire DNS-server (van je systeem of nog beter op je router). Nadat je de adressen hebt ingevoerd en indien nodig je apparaat opnieuw hebt opgestart, ben je klaar om verder te gaan. Let wel, als eindgebruiker kun je deze filters niet zelf configureren. Het is dus alles of niets.

OpenDNS Home

In de tabel vind je bijvoorbeeld OpenDNS FamilyShield: een DNS-filter waar je niets zelf kunt aanpassen. Wil je meer controle over de filters en toegang tot logs, dan is het gratis OpenDNS Home een betere keuze. Registreer je op https://signup.opendns.com/homefree via **Get a free account**. Je

krijgt de ip-adressen van de DNS-servers (**208.67.222.222** en **208.67.220.220**) die je invult in je router of specifieke systemen, zoals eerder uitgelegd.
Klik op de link in de bevestigingsmail om toegang te krijgen tot je online dashboard op https://dashboard.opendns.com. Druk op de knop **Add a network** en voer het publieke ip-adres van je router of thuisnetwerk in. Dit staat meestal al correct ingevuld, maar je kunt het ook vinden via www.whatismyip.com (zie kader 'Dynamisch adres'). Bevestig met **Add this network**, geef een naam op en klik op **Done**.
Controleer of het DNS-filter actief is door naar https://welcome.opendns.com te navigeren.



We hebben ons thuisnetwerk toegevoegd aan OpenDNS Home.

Configuratie OpenDNS Home

Open het tabblad **Settings** in je dashboard, klik op je ip-adres en kies **Custom** bij **Choose your filtering level**. Hiermee bepaal je zelf welke van de ongeveer zestig filtercategorieën je wilt activeren door een vinkje te zetten. Voorbeelden zijn Weapons, Adware, Drugs, Gambling, Pornography en Web Spam. Bevestig met **Apply**.
Onderaan kun je eigen domeinnamen toevoegen en kiezen voor **Always block** of **Never block**. Bevestig met **Add Domain**. Het kan enkele minuten duren voordat de filters actief zijn; de geblokkeerde site toont dan een melding. Je kunt dit veilig testen op https://phish.opendns.com.
Je kunt dergelijke meldingen aanpassen via de rubriek **Customization** linksboven. Ga naar **Stats and Logs**, vink **Enable stats and logs** aan om (enige tijd later) op het tabblad **Stats** alle DNS-aanvragen, inclusief geblokkeerde, van je

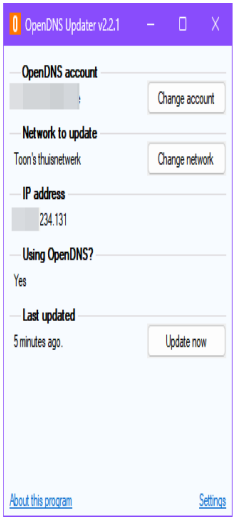
systeem of netwerk te bekijken. Het is ook aan te raden om in de rubriek **Security** zowel **Malware/Botnet Protection** als **Phishing Protection** ingeschakeld te houden.

OpenDNS Home heeft enkele tientallen filtercategorieën.

Dynamisch adres

Diensten als OpenDNS Home gaan ervan uit dat het ip-adres van je router of netwerk altijd hetzelfde blijft. Bij de meeste thuisnetwerken is dit adres helaas dynamisch, wat betekent dat je provider het zomaar kan wijzigen, bijvoorbeeld na een herstart van je router. Je hebt daarom een techniek nodig die adreswijzigingen direct aan de dienst doorgeeft: Dynamische DNS (DDNS). We leggen uit hoe je dit instelt voor OpenDNS Home.

Controleer eerst in je online dashboard bij **Settings** en **Advanced Settings** of de optie **Enable dynamic IP update** is aangevinkt. Download vervolgens een tool die je op je pc (Windows of macOS) kunt installeren: OpenDNS Dynamic IP Updater Client. Installeer deze met een muisklik en log in met je OpenDNS-account. De tool detecteert automatisch elke wijziging van het ip-adres van je netwerk en meldt dit aan OpenDNS. De updater start automatisch mee bij het starten van Windows.



Een speciaal tooltje zorgt ervoor dat de koppeling tussen jouw externe ip-adres van je netwerk en OpenDNS intact blijft, ook als het wijzigt.

Installatie AdGuard Home

Een dienst als OpenDNS Home is handig, maar je DNS-verzoeken worden wel allemaal naar die server gestuurd. Als je je privacy belangrijk vindt, kun je een lokale oplossing overwegen, zoals AdGuard Home. Dit programma is te installeren op Windows, maar ook op Linux of een NAS (zie kader 'AdGuard Home: Linux en NAS').

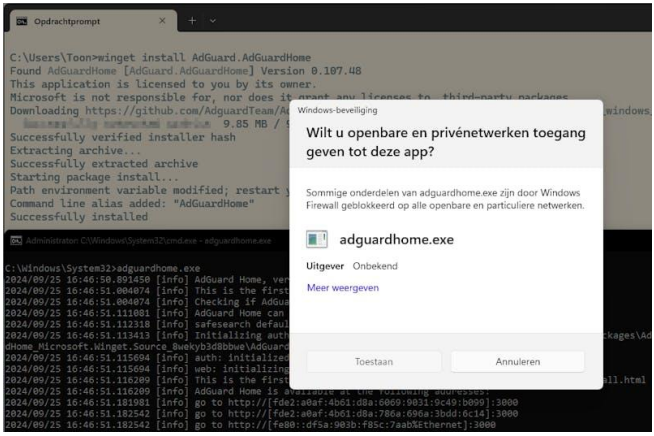
We gaan hier uit van Windows. Een oudere pc volstaat, maar besef dat deze altijd ingeschakeld moet zijn als je op internet wilt via een netwerkapparaat dat AdGuard Home als DNS-server gebruikt. De systeemeisen zijn in elk geval minimaal.

Open op die pc de Opdrachtprompt en voer het volgende commando uit:

winget install AdGuard.AdGuardHome

Sluit na de download en installatie de Opdrachtprompt. Start deze nogmaals op met administratorrechten en voer **adguardhome.exe** uit. Negeer de commando's in het Opdrachtprompt-venster, maar laat hem geopend. Krijg je een melding van je (Windows-)firewall, klik dan op **Toestaan** voor de benodigde netwerkverbindingen.

Start je browser en ga naar **127.0.0.1:3000** om de webinterface van AdGuard Home te openen. Vanaf een andere netwerk-pc kun je deze in principe ook bereiken via **IPADRES:3000**, waarbij je in plaats van **IPADRES** het interne ip-adres van de pc invult waar AdGuard Home op draait.



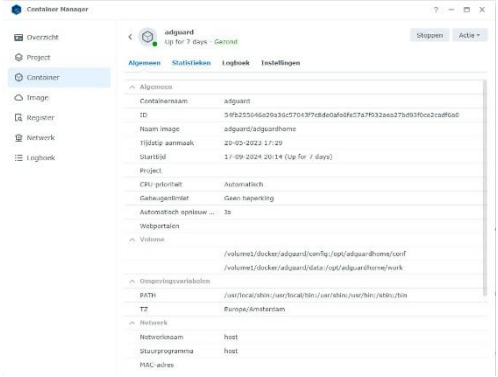
Installeren, starten en je firewall sussen.

AdGuard Home: Linux en NAS

AdGuard Home is ook eenvoudig op Linux te installeren. De benodigde commando's (met curl, wget of fetch) vind je hier.

Voor installatie op een NAS, zoals Synology, is de aanpak iets complexer. Het is het best om eerst Container Manager te installeren, een aangepaste versie van Docker door Synology, via het Package Center van DSM.

Een volledige uitleg hiervoor past helaas niet in dit artikel, maar via deze pagina vind je een duidelijke Engelstalige handleiding die je stapsgewijs door het proces leidt. We hebben deze instructies zelf succesvol getest. In de voorbeeldcode wijzig je **-e TZ=Europe/Bucharest** in **-e TZ=Europe/Amsterdam**.

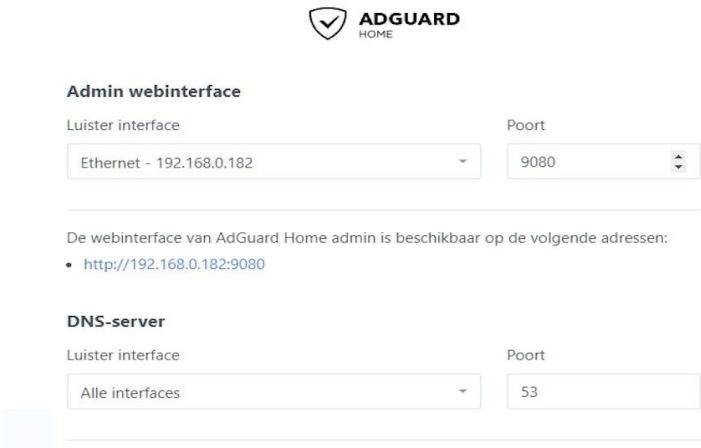


AdGuard Home, via Container Manager geïnstalleerd op een Synology-NAS.

Configuratie AdGuard Home

Bij de eerste keer starten van de webinterface van AdGuard Home start je een configuratiegids met vijf stappen.

Klik op **Beginnen**, en kies eventueel de netwerkinterface en poort voor de admin-webinterface, standaard ingesteld op **Alle interfaces** en poort **80**. Stel dit ook in voor de optie **DNS-server**, standaard ingesteld op **Alle interfaces** en poort **53**, wat je gerust zo kunt laten. Klik op **Volgende**, en vul de velden **Gebruikersnaam** en **Wachtwoord** (2x) in voor de beheerder. Klik weer op **Volgende**.
Je krijgt nu uitleg over waar je AdGuard Home als DNS-server kunt instellen. Dat zal wellicht op je router zijn of eventueel alleen op specifieke apparaten (dit hebben we aan het begin al toegelicht). Rond de configuratie af met **Volgende** en met **Open Dashboard**.
Om AdGuard Home als Windows-service te laten draaien, zodat aanmelden niet nodig is, ga je naar het openstaande Opdrachtprompt-venster. Druk op **Ctrl+C** om AdGuard Home te stoppen en voer deze opdracht uit:
adguardhome.exe -s install
Je kunt nu de voorkeurs- en alternatieve DNS-server van de AdGuard Home-pc handmatig instellen op het eigen ip-adres, aangezien deze als DNS-server fungeert. Zorg er op je router tevens voor dat deze pc een vast ip-adres krijgt, buiten het DHCP-adresbereik.



Draait bijvoorbeeld al een andere service op poort 80, dan kies je gewoon een andere.

Filters en lijsten

Controleer of de AdGuard Home-service draait door **Windows-toets+R** te drukken en **services.msc** uit te voeren: AdGuard Home Service zou actief moeten zijn.

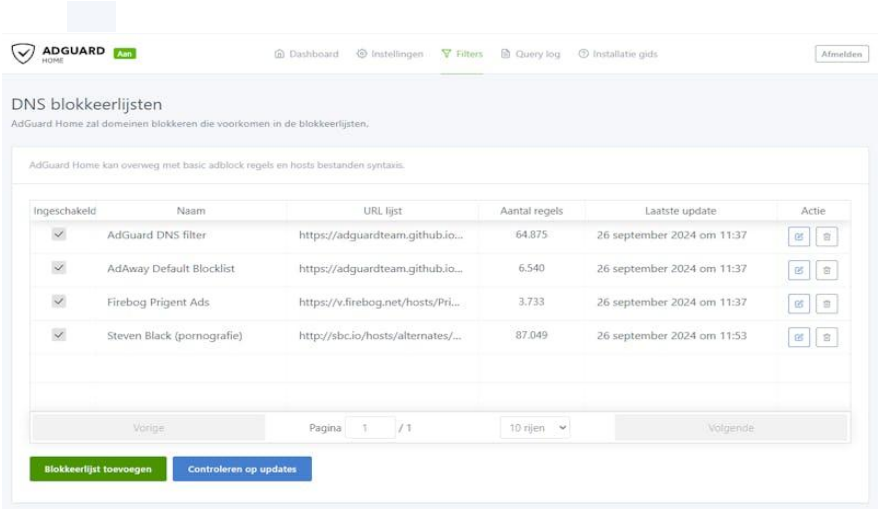
Ga vervolgens naar het dashboard via de webinterface en log in met je beheeraccount. Bovenaan zie je een knop om de AdGuard-bescherming tijdelijk uit te schakelen. Klik op **Ververs statistieken** voor een actueel overzicht van de DNS-verzoeken van je apparaten.

Als er ongewenste sites doorheen glippen, ga dan naar het tabblad **Filters** en kies **DNS Blokkeerlijsten**. Klik op **Blokkeerlijst toevoegen** en selecteer **Uit de lijst selecteren** voor extra filterlijsten. Met het **I**-knopje krijg je een overzicht van de geblokkeerde domeinen. Meer blokkeerlijsten vind onder meer op de sites in het kader 'Sites met blokkeerlijsten'. Om een lijst toe te voegen, kies **Blokkeerlijst toevoegen / Aangepaste lijst toevoegen** en voer de naam en complete url in, bijvoorbeeld https://v.firebog.net/hosts/Prigent-Ads.txt (let op: deze url is hoofdlettergevoelig!).

Met reguliere expressies (ook wel regex genoemd) kun je specifieke domeinen met trefwoorden blokkeren via **Filters / Aangepaste filter**. Meer informatie hierover vind je op deze webpagina.

Via **Instellingen / Algemene instellingen** kun je de webservice AdGuard Ouderlijk Toezicht activeren en veilig zoeken op zoekmachines afdwingen. Onder **Filters / Geblokkeerde services** kun je bijna 120 diensten blokkeren, waaronder Discord, Netflix en Temu.

In de rubriek **Query log** vind je een chronologische lijst van alle DNS-aanvragen, met details over welke apparaten wat en wanneer hebben aangevraagd.



Extra blokkeerfilters en -criteria toevoegen is snel gebeurd.

Sites met blokkeerlijsten

- Adlists for piHole
- Big Blocklist Collection
- OISD Domain Blocklist
    - https://oisd.nl/includedlists/small
    - https://oisd.nl/includedlists/big/0

Bezochte locaties zien in Google Maps

Artikel: Seniorweb

Terugzien welke plaatsen u bezocht in mei vorig jaar, tijdens de vakantie, of gewoon zomaar vorige week zaterdag? Dat kan met de tijdlijn van Google Maps.

Tijdlijn

Een onderdeel van Google Maps is de zogeheten tijdlijn. In dat overzicht staat welke locaties iemand bezocht met zijn smartphone (waarop de app van Google Maps staat). Dat werkt niet alleen in Nederland, maar ook in het buitenland, zelfs zonder internetverbinding. De functie werkt via de gps op de mobiele telefoon. Gebruikers zijn natuurlijk niet verplicht om hun locatie(geschiedenis) met Google Maps te delen. Alleen zijn sommige functies dan niet beschikbaar. Overweeg dus eerst of u het goed vindt om uw locatie te delen.

Bezochte locatie op datum bekijken (app)

Wilt u de tijdlijn inzien? Via de app op smartphones en tablets werkt dat zo:

- Open de app Maps.
- Tik rechtsboven op de cirkel met uw profielfoto of initialen.
- Tik op **Je tijdlijn**.
- Tik bij het eerste gebruik op **Aan de slag**.
- U ziet de huidige dag, met de locaties die daarbij horen. Tik op **Vandaag** om te wisselen naar een andere dag. Ziet u dit niet? Zet dan eerst uw locatiegeschiedenis aan door op **Aanzetten** te tikken.
- Veeg van links naar rechts om naar een vorige maand te gaan.
- Tik een dag aan om meer informatie te zien.

- Tik een los onderdeel aan, zoals een autorit, een bezoek aan een winkel of restaurant om specifieker te tonen hoe laat u daar geweest bent. Tik eventueel op de drie puntjes om details te bekijken.

Bezochte locaties bekijken (app}

U kunt ook per plaats bekijken hoe vaak u daar geweest bent.

- Tik in Maps rechtsboven op de cirkel waar uw profielfoto staat.
- Tik op **Je tijdlijn**.
- Tik boven in op een van de tabbladen **Dag**, **Reizen**, **Inzichten**, **Plaatsen**, **Steden** of **Wereld**. Veeg over tabbladen om ze allemaal te kunnen zien.

    - Dag: hier staat per dag aangegeven waar u bent geweest die dag.
    - Reizen: hier staat een overzicht van reizen die u heeft afgelegd. Tik op een reis om bezochte plaatsen en bijvoorbeeld gefietste routes te bekijken.
    - Inzichten: dit tabblad geeft inzicht in je maandelijkse gebruik van Maps. Er zijn bijvoorbeeld reizen en hoogtepunten te vinden.
    - Plaatsen: hierbij worden categorieën getoond, zoals winkelen, eten en drinken, sport of cultuur.
    - Steden: tik op een stad om verschillende bezochte locaties in die stad te zien.
    - Wereld: kies het land, en selecteer daarna een stad.

Tijdlijn bekijken via de computer
Hoewel een computer natuurlijk niet meegaat op uitstapjes, kunt u deze wel gebruiken om de tijdlijn te bekijken. Dat gaat zo:

- Ga naar www.google.nl/maps
- Log in met een Google-account als u nog niet ingelogd bent.
- Klik op het pictogram met de drie streepjes, linksboven aan de pagina.
- Klik op **Je tijdlijn**.
- Bij het eerste bezoek is er een korte uitleg.
  Klik steeds op de pijlen om verder te gaan.
  Klik bij het laatste punt op **Vergelijk de momenten**.
- Klik onder 'Tijdlijn' op **Jaar** en selecteer een jaartal.
- Klik onder 'Tijdlijn' op **Maand** en selecteer een maand.
- Klik onder 'Tijdlijn' eventueel nog op **Dag** en selecteer een datum.

Google laat zien op welke plekken u bent geweest.
Klik op een van de rode stippen op de kaart om te zien wat voor plaats het is.
Klik nogmaals voor meer details.

AI-hulp voor cyberaanvallen

Google Gemini blijkt populair te zijn

Elwin februari, 2025

Door de staat gesteunde hackersgroepen misbruiken de AI-assistent Gemini van Google voor onder meer onderzoek naar potentiële aanvalsdoelen.

Efficiënter werken voor hackers: Volgens Google maken meerdere door de staat gesteunde hackergroepen gebruik van Gemini om hun productiviteit te verhogen en potentiële doelwitten te onderzoeken. Volgens een bericht van Bleeping Computer heeft de Google Threat Intelligence Group (GTIG) vastgesteld dat hackers Gemini voornamelijk inzetten om efficiënter te werken, en niet om nieuwe AI-gestuurde cyberaanvallen te ontwikkelen die traditionele verdedigingsmechanismen kunnen omzeilen.

Meest voorkomende toepassingen Gemini van hackers: Volgens Google waren vooral advanced persistent threat-groepen (ook wel bekend als APT) uit Iran en China bijzonder actief.

Toepassingen van Gemini door deze hackers omvatten:

- Ondersteuning bij programmeertaken, zoals het ontwikkelen van tools en scripts
- Onderzoek naar bekende beveiligingslekken
- Vertalingen en uitleg over technologieën
- Verzamelen van informatie over doelorganisaties
- Zoeken naar methoden om detectie te omzeilen, rechten uit te breiden of geïnfiltreerde netwerken verder te verkennen

Gebruik van Gemini in verschillende aanvalsfases

De hackers zetten het gebruik van AI in diverse fasen van hun aanvalscyclus in, waarbij de focus per land verschilde:

- Iraanse hackers gebruikten Gemini vooral voor verkenning, phishingcampagnes en beïnvloedingsoperaties.

- Chinese groepen richtten zich op Amerikaanse militaire en overheidsinstanties, onderzoek naar kwetsbaarheden, laterale bewegingen binnen netwerken en het uitbreiden van toegangsrechten na een inbraak.
- Noord-Koreaanse APT's gebruikten Gemini ter ondersteuning van verschillende fasen van de aanvalscyclus, waaronder verkenning, malware-ontwikkeling en verduisteringstechnieken. Eén van de aandachtspunten was het geheime IT-werkprogramma van Noord-Korea.
- Russische hackers maakten slechts beperkt gebruik van Gemini, voornamelijk voor script-ondersteuning, vertalingen en het genereren van payloads. Mogelijk geven zij de voorkeur aan in Rusland ontwikkelde AI-modellen of mijden ze westerse platforms uit operationele veiligheidsoverwegingen.

Pogingen om de veiligheidsmaatregelen te omzeilen
Google merkte ook pogingen op om publieke jailbreaks op Gemini toe te passen of prompts aan te passen om de beveiligingsmaatregelen te omzeilen. Tot nu toe zijn deze pogingen onsuccesvol gebleken.
Een vergelijkbare waarschuwing kwam in oktober 2024 van OpenAI, de ontwikkelaar van de populaire chatbot ChatGPT. Naarmate generatieve AI-systemen steeds breder worden toegepast, neemt ook het risico op misbruik toe, vooral bij modellen met onvoldoende beveiliging.
Zo hebben beveiligingsonderzoekers al aangetoond dat bij systemen zoals DeepSeek R1 en Qwen 2.5 van AliBaba, de beperkingen relatief eenvoudig te omzeilen zijn.
Tot slot
Al met al onderstreept het toenemende gebruik van AI door hackers de noodzaak van robuuste beveiligingsmaatregelen en continue monitoring om misbruik te beperken en de impact van digitale dreigingen te minimaliseren.

Kies of Google uw locatiegeschiedenis mag wissen

Gebruikers van Google Maps krijgen de laatste tijd een melding of e-mail over de Tijdlijn. Wat moeten ze daarmee doen?

Nynke

Als Tijdlijn aan staat, houdt Google Maps de hele tijd bij waar het toestel is. Handig voor mensen die op de kaart willen terugzoeken waar ze geweest zijn. Bijvoorbeeld tijdens een vakantie. Die locatiegeschiedenis sloeg Google tot nu toe op in zijn eigen cloudopslag. Maar dat verandert. Voortaan staat die informatie alleen op het toestel van de gebruiker. Google verwijdert de oude gegevens dus uit de cloud .

Keuze: bewaren of niet

Gebruikers van de Tijdlijn staan dus voor een keuze: willen ze hun locatiegeschiedenis bewaren of niet?

Zo ja, dan moeten ze actie ondernemen voor 18 mei 2025. Wie niks wil bewaren of opslaan, hoeft niks te doen.

Google verwijdert dan vanzelf de locatiegeschiedenis en de Tijdlijn-functie gaat uit.

Wel bewaren?

Wie de geschiedenis wél wil bewaren op zijn eigen toestel, moet de instellingen controleren en kiezen.

- Tik in de e-mail op **Instellingen checken en kiezen** of tik bij de melding in Google Maps op **Volgende**.
- Tik onder ‘Hoelang wil je je Tijdlijn-gegevens bewaren? op **Bewaren tot verwijdering** om niks weg te gooien. Of tik onder ‘Automatisch verwijderen na’ op het uitklapvenster en kies een aantal maanden, bijvoorbeeld **3 maanden**.
- Tik op **Aan laten staan**.

Google voert gefaseerde invoering van multifactor-authenticatie door.

Elwin februari, 2025

In november kondigde Google het al aan, en nu ligt het tijdschema vast voor de verplichte overstap naar multifactorauthenticatie (MFA) voor Google-accounts.

Waarom multifactorauthenticatie verplichten?

MFA biedt betere bescherming tegen phishing en het misbruik van inloggegevens uit datalekken. Om deze reden heeft Google in november aangekondigd dat MFA verplicht zal worden voor online accounts bij het bedrijf. Inmiddels heeft Google het tijdspad voor deze implementatie definitief vastgesteld.

In een artikel over Google Cloud licht het bedrijf de veranderingen en details toe. Volgens Google zijn accounts die met MFA zijn beveiligd met 99% zekerheid niet te kraken. Daarom wordt de MFA-verplichting stapsgewijs voor alle Google Cloud-accounts ingevoerd.

Gefaseerde uitrol van MFA-verplichting

De uitrol begint met de accounts van resellers. Voor hen wordt multifactorauthenticatie vanaf 28 april 2025 verplicht.

Klantenaccounts van resellers vallen in deze fase nog niet onder de verplichting.

Voor particuliere Google-accounts, zoals die van Gmail, wordt MFA geactiveerd vanaf 12 mei 2025. Vervolgens komen in het derde kwartaal van 2025 zakelijke Cloud Identity-accounts zonder Single Sign-On (SSO) aan de beurt. Ten slotte worden zakelijke accounts met federatieve authenticatie in het vierde kwartaal van 2025 of later verplicht om MFA te gebruiken.

Gebruikers krijgen tijdige waarschuwingen

Google zal betrokken gebruikers tijdig informeren over de veranderingen. In de Cloud Console wordt minimaal 90 dagen vóór de verplichte invoering een herinnering weergegeven, en ook per e-mail worden gebruikers op de hoogte gebracht. Resellers en hun klanten ontvangen deze meldingen 60 dagen van tevoren.

Particuliere gebruikers krijgen momenteel al een informatie-e-mail, ongeacht of zij tweestapsverificatie (2FA) al hebben ingeschakeld of niet. Deze e-mail bevat een link naar de beveiligingsinstellingen van het Google-account, waar gebruikers kunnen controleren of MFA al is ingeschakeld en welke verificatiemethoden (zoals passkeys, beveiligingssleutels, authenticator-apps of telefoonnummers) zijn ingesteld.

Welke diensten worden beïnvloed?

De wijziging heeft invloed op de toegang tot de Google Cloud Console, de gcloud CLI en de Firebase Console. Aanmelden bij een Google-account en het gebruik van Google Workspace (zoals Gmail, Google Drive en YouTube) blijft mogelijk zonder MFA. Echter, Google Workspace-producten, zoals Spreadsheets en Presentaties, vallen onder aparte MFA-vereisten.

Google adviseert alle gebruikers om nu al multifactorauthenticatie in te schakelen en zich goed voor te bereiden op de aankomende verplichtingen. Voor particulieren lijkt er geen manier te zijn om MFA te omzeilen, terwijl voor zakelijke klanten mogelijk een opt-out-programma wordt onderzocht.

Achtergrond van de MFA-verplichting

In november 2024 maakte Google bekend dat gebruikers van het Google Cloud Platform (GCP) voortaan een extra verificatiecode nodig hebben naast hun wachtwoord en gebruikersnaam. De invoering van multifactorauthenticatie is bedoeld om hacking te voorkomen. Destijds werd slechts een globaal tijdschema genoemd, maar dat is nu verder uitgewerkt.

Adresboek beheren met app Contacten op Mac.

Bewaar contactgegevens van vrienden, familie en kennissen in de app Contacten op de Mac. Zo hebt u hun gegevens snel bij de hand.

Sanne feb 2025

Adresboek in een app

Het papieren adresboekje kan de deur uit. De gegevens van contactpersonen zijn namelijk ook op de computer op te slaan. Op een Mac-computer kan dat met de app Contacten. Dat is eigenlijk een digitaal adresboekje.

Het voordeel van Contacten is dat de app samenwerkt met andere apps, zoals de app Mail. Daarnaast zijn de gegevens uit te wisselen met andere Apple-apparaten. Denk aan een iPhone of iPad. Dit heet synchroniseren . Zo hebt u de contactgegevens altijd bij de hand.

App Contacten openen

De app Contacten staat standaard op de Mac. Bij de meeste gebruikers staat de app in het dock . Open de app door te klikken op het bruine boekje. Ziet u dit pictogram niet? Volg dan onderstaande stappen:

- Open de Finder via het lachende gezichtje  in het dock.
- Klik op **Apps**.
- Dubbelklik op het programma **Contacten**.

Contacten bekijken

De app Contacten bestaat uit drie kolommen. In de kolom links staan groepen. Klik op **Alle contacten** om alle opgeslagen contactpersonen te bekijken. De namen van deze contacten ziet u in de middelste kolom. Hier kunt u doorheen scrollen. Klik op een contactpersoon. De gegevens van deze persoon ziet u in de rechterkolom.

Contactpersoon toevoegen

Voeg zo een contactpersoon toe aan de app:

- Klik op het plusteken onderin in de rechterkolom  .

- Klik op **Nieuw contact**.
- Klik op **Voornaam** en typ de voornaam van de contactpersoon.
- Klik op **Achternaam** en typ de achternaam van de contactpersoon.
- Vul daarna de gewenste gegevens in. Denk aan een telefoonnummer, e-mailadres, verjaardag of adres.
- Klik tot slot rechtsonder op **Gereed**.

Contactpersoon wijzigen
Heeft een contactpersoon een nieuw telefoonnummer of is hij/zij verhuisd? Geen probleem. Werk de contactgegevens gemakkelijk bij:

- Klik in de middelste kolom op een contactpersoon.
- Klik rechtsonder op **Wijzig**.
- Klik op de informatie die u wilt aanpassen.
- Haal oude gegevens weg met de Backspace-toets op het toetsenbord.
- Typ de nieuwe gegevens.
- Klik op **Gereed**.

Contactpersoon verwijderen
Een contactpersoon helemaal verwijderen uit de app kan ook. Doe dat zo:

- Klik met de rechtermuisknop met twee vingers in de middelste kolom op een contactpersoon.
- Klik op **Verwijder kaart**.
- Klik ter bevestiging op **Verwijder**.

Bellen en berichten vanuit Contacten
De app Contacten werkt samen met andere apps op de Mac. Zo is het mogelijk om via de app een ander programma te starten. Bijvoorbeeld iemand een bericht sturen, bellen of FaceTimen. Welke opties er zijn, hangt af van de gegevens die u hebt opgeslagen.

- Klik in de middelste kolom op een naam van een contactpersoon.
- In de rechterkolom staan pictogrammen met de mogelijkheden. Dit zijn: 'bericht', 'bellen', 'video' en 'e-mail'. Is het pictogram blauw? Dan is de optie beschikbaar.
- Klik op zo'n pictogram, bijvoorbeeld 'bericht'. De app 'Berichten' opent. U kunt nu een bericht sturen aan de geselecteerde contactpersoon. De bijbehorende app opent en richt zich tot de contactpersoon.

Toegang tot Contacten
Het werkt ook andersom. Vanuit een andere app hebt u toegang tot de gegevens uit de app Contacten. Als u bijvoorbeeld in de app Mail een nieuwe e-mail opstelt.

- Open de app Mail.
- Klik op **Maak een nieuw bericht aan**  .
- Klik achter 'Aan' op het rondje met plusteken.
- De contactpersonen uit de app Contacten komen in beeld.
- Klik op een contactpersoon om deze toe te voegen aan de geadresseerden.
- Klik op het e-mailadres om de keuze te bevestigen.

Het e-mailadres van de contactpersoon staat nu achter 'Aan'.

Adreslabels printen vanuit Contacten op Mac

Familie uitnodigen voor een jubileum of een verhuisbericht versturen? Vanuit het programma Contacten op de Mac maakt en print u adreslabels. Handig

feb 2025

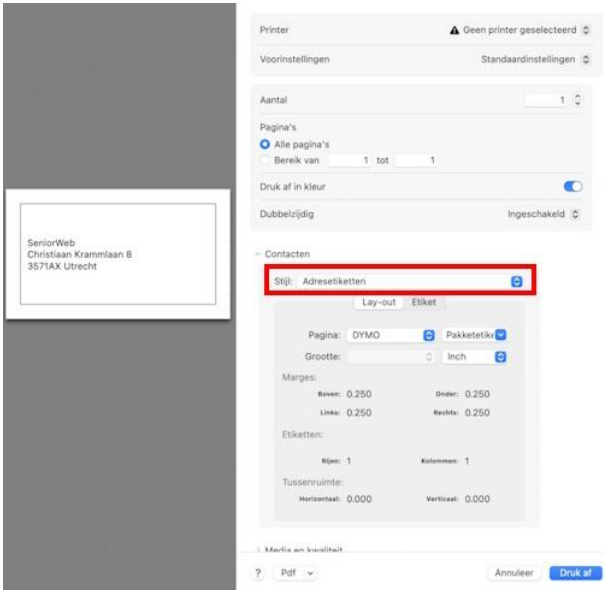
Automatisch adreslabels maken

Een uitnodiging versturen, kerstkaarten maken of een verhuisbericht rondzenden. Adreslabels komen altijd van pas. Hebt u gegevens van familieleden, vrienden en kennissen opgeslagen in Contacten op de Mac? Dan maakt het programma er automatisch adreslabels van als u ze wil afdrukken.

Adreslabels printen vanuit Contacten

Open het programma Contacten en print zo adreslabels:

- Selecteer de contacten waarvoor u een adreslabel wilt maken.
    - Moet er van alle contacten een label komen? Klik dan op het bovenste contact, houd de **Shift-toets** ingedrukt en klik op het onderste contact. Shift is de toets met de pijl omhoog.
    - Zijn er alleen labels nodig van een deel van de contactenlijst? Selecteer dan het eerste contact waarvan u een label wilt, houd de knop **Cmd** (Command) ingdrukt en klik één voor één op de andere contacten.
- De gekozen contacten zijn nu blauw. Klik in de menubalk bovenaan het scherm op **Archief** > **Druk af**.



- Een nieuw venster opent. Links staat een voorbeeld van het adreslabel dat wordt afgedrukt. Rechts staan de printgegevens met een aantal uitklapmenu's, zoals 'Contacten' en 'Lay-out'. Klap eventueel het menu onder 'Contacten' uit door erop te klikken.
- Klik achter 'Stijl' op het uitklapmenu en klik op **Adresetiketten**.
- Achter 'Pagina' kunt u het juiste type etiket kiezen waarop u gaat afdrukken, bijvoorbeeld 'DYMO'.
- Klik naast 'Lay-out' op **Etiket**.
- Pas eventueel het lettertype aan door achter ‘Lettertype’ op **Stel in** te klikken.
- Controleer bovenaan bij 'Printer' of uw Mac met de printer verbonden is.
- Klik op **Druk af**.

Valse e-mail van CJIB over verkeersboete

Oplichters sturen op het moment een nepmail over een openstaande verkeersboete van honderden euro's.

Sanne feb 2025
Ontvangt u een mail uit naam van het Centraal Justitieel Incassobureau? Wees alert! Momenteel gaat er een nepmail rond over een verkeersboete.
Daarin staat uitgelegd dat u door het rood reed.
Met als gevolg een flinke verkeersboete, die u nog niet betaald zou hebben.
Daarna volgt een overzicht met de details van de overtreding en de boete.
Tot slot staat er de oproep om het bedrag te betalen via een tikkie.

Nooit via mail

Ga niet in op de mail. Het CJIB mailt, sms-t of appt u nooit over een boete, aanmaning of betalingsachterstand.
Verwijder daarom elk bericht van het CJIB hierover.

Wilt u een cursus volgen of gewoon info over

WWW.Computerclubnissewaard.nl

Tel : 0181-640669

Mob: 06-54692942

M.A. de Ruijterstraat 3, 3201CK Spijkenisse

En via e-mail

computerclubnissewaard@gmail.com