



## **AdBlockers en Privacybescherming 3**

**Handleiding van Helpmij.nl**

**Auteur: CorVerm**

**maart 2017**

**“ Dé grootste en gratis computerhelpdesk van Nederland ”**



## Privacybescherming

Een Adblocker houdt ongewenste advertenties tegen, maar doet weinig voor de bescherming van je privacy zoals het tegenhouden van tracking cookies. Veel websites plaatsen dit soort cookies op je PC die bijhouden welke websites je bezoekt. Maar ook zoekmachines zoals Google Chrome houden bij wat je zoekt, waar je geweest bent en waar vermoedelijk jouw interesses liggen. Vervolgens wordt je op basis van die informatie gericht bestookt met pop-up-reclames en mail. Daar komt ook een deel van de ongewenste mail (spam) vandaan. Alle reden dus om ook daar iets tegen te doen. Er zijn weliswaar filters die aan een advertentieblokker kunnen worden toegevoegd (zie hierboven) om tracking tegen te gaan, maar om je privacy beter te beschermen is het goed een speciale anti-tracking/privacy beschermer aan de browser toe te voegen.



Er zijn vele privacy beschermers, maar de meest gebruikte zijn Ghostery en DNT(Microsoft). DNT is de afkorting van Do Not Trackme

Ghostery vindt je hier: <https://www.ghostery.com/try-us/download-browser-extension/> en is beschikbaar voor de browsers Google Chrome, Firefox, Safari, Opera, IE (met beperkte functionaliteit, tracking wordt slechts gesignaleerd en niet geblokkeerd) en sinds kort ook Edge. Op de volgende besturingssystemen: alle Windows versies, Linux, Android en ios.

Uitgebreide informatie over Ghostery is hier te vinden: <http://pc-en-internet.infonu.nl/> Ghostery is van het bedrijf Evidon. Evidon verdient o.a. zijn geld door anonieme en geaggregeerde gebruikersgegevens te verzamelen ten behoeve van onderzoek (Ghostrank).

DNT(DoNotTrackme) van Microsoft is ingebouwd in IE, maar in de praktijk blijkt dat niet voldoende te werken. Hier is informatie over DNT van MS: [Privacy instellingen IE-11](#).

Edge heeft ook een DNT-functie, maar die staat standaard uit (dat schiet lekker op :- ) Hier de instructie hoe dat aan te zetten: [Edge-browser-do-not-track](#).

## Google en je privacy (Privacy herinnering van Google)



Google streeft er naar zo veel mogelijk over je te weten te komen. Als je meer wilt weten hierover lees dan dit artikel van de [Consumentenbond](#) en dit artikel van [Bits-of-Freedom](#). Maart 2012 veranderde Google zijn voorwaarden met als doel meer vrijheid voor het verzamelen van jouw gegevens te krijgen. Dat was reden voor de wetgever om in 2014 Google te verplichten duidelijk te maken aan de gebruiker welke informatie ze vergaren en tevens de mogelijkheid te bieden dat tegen te houden. Dit heeft geresulteerd in het tonen van "Een privacy herinnering van Google" bericht. Nu is het aan jou om daar ook iets mee te gaan doen in de vorm van het drukken op de knop "Bekijken" en vervolgens het uitzetten van alle

opties. Eén van die opties is het aan de browser toevoegen van een "Analytics-Opt-out-extensie" die de functie van een Do-not-trace-me heeft.

**Let op!** Het invoegen van deze extensie in de browser lukt alleen als de Adblocker en Ghostery in je browser uitgezet zijn (en daarna weer aanzetten natuurlijk).

## Installeren Ghostery.



De eenvoudigste manier om Ghostery te installeren is door de browser te starten waar Ghostery ingezet moet worden en vervolgens naar <https://www.ghostery.com/try-us/download-browser-extension/> te gaan en daar te klikken op de knop van de betreffende browser.

Als voorbeeld hoe dat werkt in IE:

- Start IE en ga naar de website van [Ghostery](#)
- klik op de balk "Add to Internet Explorer"
- onderin IE kies je voor "Uitvoeren"
- Er verschijnt nu een Ghostery scherm "Welcome bij de Ghostery Wizard"
- Klik op "Installeren"

Helaas laat IE niets zien waaruit op te maken is dat Ghostery geïnstalleerd. Om dat te controleren gaat je naar het menuscherm van IE en klikt dan op "Invoegtoepassingen beheren". Dat geeft een overzicht van de invoegtoepassingen, waaronder Ghostery. In IE is er in Ghostery niets in te stellen en/of aan te passen waardoor het nut beperkt is. Daar Microsoft van plan is de support voor IE te beëindigen is het wellicht ook verstandiger om op een andere browser over te stappen, zoals bijvoorbeeld Firefox, Chrome, of Edge.

## Installatie van Ghostery in Firefox:

- Start Firefox en ga naar de website van [Ghostery](#)
- Klik op de balk "Add to Firefox"
- De installatie gaat nu naar het Firefoxscherm met de vraag de Ghostery extensies toe te mogen voegen (groene knop "+Add to Firefox"). Druk op de groene knop.
- Nu verschijnt er nogmaals een (wit) schermje met de vraag om een Add-on te installeren.
- Druk op "Installeren".

Startschermen van Ghostery:

- Je komt nu in een serie van schermen om Ghostery in te stellen. De eerste is een welkomstscherm met de vraag of je gegevens over de trackers die Ghostery afvangt wil delen. Het is aan je om daar Ja of Nee op te antwoorden.
- Het volgende scherm vraagt of je een account aan wilt maken. Zo'n account is vooral interessant voor mensen die meer willen weten over deze materie.
- Het volgende scherm geeft de keuze voor een rondleiding en uitleg, maar het belangrijkste is
- toch wel de mogelijkheid aan te geven welke zaken geblokkeerd moeten worden. Mijn advies:

- kies voor "Alles blokkeren".

Voor Chrome en Edge is er de mogelijkheid bepaalde websites NIET te blokkeren door deze op te nemen in de lijst met "Vertrouwde websites". Zie even verderop hoe dat gaat.

## Installatie van Ghostery in Edge:

- Start Edge en ga naar de website van Ghostery .
- Klik op de balk "Add to Edge".
- De installatie gaat nu naar het Edgescherm met de vraag de Ghostery extensie uit de webwinkel te downloaden. Druk op de blauwe knop "Downloaden".
- Na download en installatie dient de app gestart te worden. Druk op de blauwe knop "Starten".
- Maar dat is nog niet genoeg voor Edge. Nu moet je nog aangeven dat de Ghostery extensie ook echt ingeschakeld moet worden (het lijkt wel of ze deze extensie niet echt willen).
- Nu volgt er een serie van Ghostery-schermen die gelijk is aan die hierboven beschreven bij de installatie van Ghostery in Firefox (Startschermen van Ghostery).



Als je Edge nu herstart is er niets te zien van Ghostery! Edge verstopt graag zijn extensies. Om deze toch zichtbaar te maken (handig als je Ghostery wilt aanpassen) druk dan op de drie puntjes rechts bovenin in Edge en kies voor "Extensies". Dat geeft een overzicht van de geïnstalleerde extensies, waaronder Ghostery. Beweeg de muisaanwijzer naar de Ghostery-regel in het extensiesoverzicht, ga een beetje naar rechts, en dan verschijnt er een radertje. Klik erop. Dan komt er nu een overzicht waarin te zien is dat Ghostery nog niet zichtbaar is rechts van de adresbalk. Zet deze nu aan.

## Ghostery installeren via de webwinkel

Alle browser, behalve IE, bieden de optie om te installeren via de webwinkel. Dat is veiliger dan via een aparte website. Deze manier van toevoegen van Ghostery kan in Chrome, Firefox en Edge. Installeren van Ghostery via de webwinkel gaat op de zelfde wijze als hierboven beschreven voor de advertentieblokkers.

## Vertrouwde websites

Ghostery kent twee manieren om aan te geven dat bepaalde websites te vertrouwen zijn en niet gefilterd hoeven te worden:

1. door naar de betreffende website te gaan en dan met de linkermuisknop op het Ghostery-icoontje te drukken en dan klikken op de knop "Vertrouwen" Dat kan in Chrome, Firefox en Edge.
2. door naar het optiescherm van Ghostery te gaan en daar dan de door jou te vertrouwen websites aan een lijst toe te voegen. Dat kan in Chrome en Edge. Daarin kunnen websites geplaatst worden waarvoor geen enkele vorm van blokkering toegepast mag worden.

In Chrome: klik met de rechtermuisknop eenmaal op het icoontje van Ghostery en dan op "Opties". Dat opent het optiescherm van Ghostery. Klik op de tab "Vertrouwde websites". Nu kunnen door jou vertrouwde websites ingevoerd worden. Vergeet niet om op de groene knop met het + teken te drukken om de website ook echt aan de lijst toe te voegen.

## Windows 10 en je privacy



Tenslotte een paar woorden over Windows 10 en je privacy. Niet alleen Google wil zo veel als mogelijk over jou te weten komen, ook bij Microsoft gaat het die kant op. Windows 10 is een belangrijke stap op dat gebied. Een aanrader voor iedereen die zich zorgen maakt over het aantasten van zijn/haar privacy bij het gebruik van Windows 10 is het gratis toeltje Shutup10. Hiermee worden niet alleen alle privacygevoelige elementen van Windows 10 blootgelegd, maar kunnen deze ook worden uitgezet. Aan te raden is om periodiek Shutup opnieuw te laten werken, daar gebleken is dat Microsoft na een belangrijke update soms bepaalde settings weer aan zet.

### IP-nummer afschermen

Wil je tevens dat het IP-nummer van je internetverbinding niet doorgegeven kan worden dan is het gebruik van een VPN-verbinding een goeie oplossing. VPN=Virtual Private Netwerk. Veel antivirussoftware biedt tegenwoordig de mogelijkheid van het inschakelen van een VPN-verbinding.

Daarnaast zijn er gratis en betaalde VPN-diensten van VPN-gespecialiseerde bedrijven.

Hier kun je meer lezen over VPN: [consumentenbond](#), wat het is en welke aanbieders er zo al zijn.

### SR-PC-HULP