# Wat is VPN en hoe veilig is deze versleutelde verbinding?

**Misschien ben je van mening dat je niets te verbergen hebt. Maar zou jij je e-mailadres, wachtwoorden, bankrekeningnummer en pincode aan een wildvreemde op straat geven? Op een openbaar wifi-netwerk geef je soortgelijke informatie mogelijk wel weg. Een VPN-verbinding kan voor bescherming zorgen.**

Uit onderzoek van beveiligingsbedrijf Symantec blijkt dat veel mensen een onveilig wifi-netwerk niet herkennen. Kwaadwilligen kunnen via een onveilig netwerk zomaar toegang verkrijgen tot bankgegevens en andere gevoelige gegevens. Een mogelijk hulpmiddel is VPN.

Lees ook: Veilig internetten op een openbaar wifi-netwerk: 4 tips

## Wat is VPN?

VPN staat voor Virtual Private Network, in het Nederlands: virtueel privénetwerk. Een VPN-verbinding kun je het beste zien als een soort van afgeschermde tunnel naar een andere hoek van het internet. De informatie die je over het internet verstuurt, wordt eerst versleuteld naar de aanbieder van de VPN-dienst geleid en gaan vanaf daar pas verder naar de website die je bezoekt.

## Wanneer is het handig om VPN te gebruiken?

Doordat alle informatie eerst beveiligd naar de VPN-dienst gaat, is het voor een hacker op een openbaar netwerk niet mogelijk om je af te luisteren. Hierdoor is het verstandig om een VPN te gebruiken als je op een openbaar netwerk gevoelige gegevens verstuurt.

Een ander voordeel van de omleiding via de VPN-dienst is dat voor de instantie aan de andere kant van de lijn niet jouw IP-adres, maar dat van de VPN-dienst ziet. Is deze dienst gevestigd in een ander land, lijkt het dus alsof je vanaf dat land aan het surfen bent. De BBC blokkeert bijvoorbeeld de toegang tot bepaalde services als je buiten Groot-Brittannië bent. Als je met een VPN doet alsof je wel in Groot-Brittannië bent, dan kun je daar alsnog bij.

Hoewel VPN steeds meer inburgert onder consumenten, maken bedrijven al langer gebruik van dit type verbinding. Bij sommige bedrijven kunnen werknemers alleen toegang krijgen tot het interne netwerk via een VPN-verbinding. Hierdoor blijft bedrijfsgevoelige informatie binnen het interne netwerk en wordt er geen informatie naar buiten gelekt vanuit de verbinding.

We vroegen aan het Testpanel wie er allemaal van een VPN gebruikmaakt en waarom. Er werden verschillende redenen genoemd:

Internetten via VPN voor privacy en veiligheid doet lang niet iedereen

## Hoe anoniem is VPN?

Hoewel een VPN-verbinding je internetverkeer anonimiseert en je eigen ip-adres niet zichtbaar is, betekent het niet dat je ook direct anoniem bent. Zo weet de VPN-dienst die je gebruikt welke websites je bezoekt. Veel VPN-diensten geven aan dat ze niet bijhouden wat jij precies doet, zodat je privacy niet in het geding komt. Maar omdat je niet kan controleren of een VPN-dienst daadwerkelijk geen logbestand bijhoudt, is het een kwestie van vertrouwen. Ook kan het zomaar zijn dat overheden of geheime diensten via een achterdeurtje alsnog proberen binnen te komen.

## Heeft een VPN invloed op de internetsnelheid?

Doordat er een extra stap wordt toegevoegd tussen jou en de website die je probeert te bezoeken, levert dit altijd wat extra vertraging op. Als de VPN-omleiding niet heel ver van je vandaan is en hij genoeg snelheid ondersteunt, dan merk je daar in de praktijk niets van.

Maak je echter verbinding met een VPN aan de andere kant van de wereld of biedt de VPN niet veel bandbreedte (internetsnelheid) aan, dan gaat het internetten merkbaar langzamer.

## Moet je altijd betalen voor een VPN?

Je hebt zowel de keuze uit gratis als betaalde VPN-diensten. De gratis VPN's hebben vaak wel beperkte functionaliteiten: de snelheden liggen lager, je zit vast aan een maximum qua dataverbruik en je mag niet gebruikmaken van een eindeloos aantal verbindingen. Bovendien is de kans aanwezig dat je betaalt met je privacy omdat het onderhouden van een VPN-dienst nou eenmaal geld kost. Veel betaalde diensten kun je overigens gratis uitproberen.

## Voor welke VPN moet je kiezen?

Er zijn verschillende zaken waar je rekening mee kunt houden bij de keuze voor een VPN. Is hij gemakkelijk in het gebruik? Kan hij een ‘tunnel’ naar een voor jou geschikte situatie creëren? Hoeveel snelheid biedt hij? Wat zijn de kosten?

Ook is privacy een belangrijke overweging bij het kiezen van een VPN. Een VPN die in de VS gevestigd is, moet mogelijk informatie delen met de Amerikaanse overheid.

Veel streamingservices, zoals Netflix, proberen te detecteren wanneer je via een VPN van de dienst gebruik probeert te maken en blokkeren dat. Ze is immers voorkomen dat je vanuit Nederland series kunt kijken die exclusief voor de Amerikaanse markt bedoeld zijn. Desondanks lukt het met sommige VPN-providers wel om Netflix via een VPN te bekijken.

De website VPNGids.nl vergelijkt verschillende VPN-diensten op allerlei punten.

## Hoe stel je VPN in?

Veel VPN-diensten hebben tegenwoordig een eenvoudige app die je op je telefoon of computer kunt installeren. In sommige situaties moet je de verbinding nog handmatig instellen. Je VPN-aanbieder geeft je dan gegevens die je in moet vullen. Waar je die gegevens in moet vullen, vind je hier:

### Windows

1. Ga naar Instellingen
2. Kies voor Netwerk en internet > VPN > Een VPN-verbinding toevoegen
3. Vul de gegevens van de VPN-dienst in

### Mac

1. Ga via het Apple-menu naar Systeemvoorkeuren
2. Klik bij netwerk op het plusje om een nieuwe verbinding aan te maken
3. Kies in het menu Interface voor VPN
4. Voer de gegevens in van de VPN-dienst

### Android

1. Ga op je Android-toestel naar Instellingen
2. Kies voor Netwerk en internet en klik dan op Geavanceerd
3. Klik op VPN
4. Klik op het plusje om een nieuwe verbinding toe te voegen
5. Voer hier de gegevens in van de VPN-dienst

### iPhones / iPads

1. Ga op je iPhone of iPad naar Instellingen
2. Kies bij Algemeen voor VPN
3. Klik op 'Voeg VPN-configuratie toe'
4. Vul de gegevens in van de VPN-dienst