Tech

WIFI OP VAKANTIE

Veilig buiten surfen

Pas op met de wifi van de campingbaas als je **op vakantie** online gaat. Vier zaken om op te letten voor wie de verbinding graag veilig houdt.

Door **Timo Nijssen** Foto **Pauline Niks**

De gratis wifiverbinding die veel hotels, campings, cafés en restaurants hun gasten bieden is niet altijd even veilig als de internetverbinding thuis. Met een beetje technische kennis kunnen criminelen op zo'n open netwerk meekijken met wat je doet en proberen om je gevoelige gegevens te ontfutselen. Ze kunnen bovendien een fopnetwerk opzetten. Dan wekken ze met de netwerknaam de indruk dat het de gratis wifi van bijvoorbeeld het hotel is, maar loopt de verbinding via de crimineel.
De Volkskrant stelde vier beveiligingsexperts de vraag: hoe houd je je gegevens buiten de deur veilig?

Maak gebruik van je eigen internetverbinding

Dit is de makkelijkste tip: blijf weg van het openbare wifinetwerk en zorg dat je op de 4G-verbinding van je smartphone blijft. Die is een stuk beter te vertrouwen dan een willekeurige wifi-hotspot, zegt Floor Terra, adviseur bij Privacy Company. Misschien heb je na al dat thuisblijven de afgelopen tijd nog aardig wat MB's over van je bundel. Binnen de Europese Unie is je Nederlandse databundel gewoon geldig en reizen daarbuiten zitten er dit jaar waarschijnlijk toch niet in. Let wel een beetje op: een avondje series bingen kost al gauw meer MB's dan je denkt.

Via de hotspotfunctie van je telefoon kun je de verbinding delen met een tablet of laptop. Stel dan wel een goed wachtwoord in, zodat vreemden niet al je MB's opslurpen. Wil je met het hele gezin online? Dan kun je een mifi-router overwegen. Dat is een internetkastje dat via 4G internet binnenhaalt en vervolgens als een gewoon wifisignaal weer doorstuurt. Nadeel is dat daar een eigen simkaart met internetbundel in moet.

Tegenwoordig surf je bijna altijd versleuteld, maar dat dekt niet alles af

Internetverbindingen zijn de afgelopen tien jaar een stuk veiliger geworden. Het overgrote deel van de websites, 80 tot 90 procent, gebruikt een versleutelde https-verbinding. Die herken je aan het slotje in de adresbalk van je browser. Een versleutelde verbinding garandeert dat wanneer jij op een webshop je creditcardgegevens invult, niemand behalve jij en de winkeluitbater die kunnen inzien. Of dat de inhoud van je mailbox geheim blijft.

Https zorgt er ook voor dat een campingbaas niet kan zien dat je naar de regels voor geluidsoverlast zoekt, zegt Bér Engels van digitaleburgerrechtenorganisatie Bits of Freedom. Maar de uitbater kan het vervolgens wel zien als je vanuit de zoekmachine op een pagina van Rijksoverheid.nl belandt – slotje in de browser of niet.

En zo'n 10 tot 20 procent van de websites heeft dus nog geen versleutelde verbinding. Daar kun je toch gevoelige gegevens achterlaten. Denk maar aan de krakkemikkige website van een campinghouder waarop je een registratieformulier moet invullen, waarschuwt Engels.

De bescherming van https is bovendien beperkt tot je webbrowser, zegt Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit. Andere verbindingen vallen er niet onder, bijvoorbeeld die van een mailprogramma of van videobelsoftware.

Een VPN beveiligt al je verbindingen en houdt je anoniem

Met een VPN (virtual private network) ga je die risico's wel te lijf. Daarmee graaf je een beveiligde tunnel waar alle internetverbindingen van je apparaat doorheen lopen.

Wanneer je zonder VPN een website bezoekt, gaan je gegevens van je apparaat via het netwerk waarmee je verbonden bent naar de internetprovider toe. Daaruit gaan ze weer verder naar de servers van de dienst die je bezoekt. Op al die wisselmomenten kan in theorie meegekeken worden met wat je aan het doen bent. De VPN-tunnel gaat dat tegen. Als de beheerder van het lokale netwerk of de internetprovider dan proberen mee te kijken, zien ze alleen de buitenkant van die tunnel. Pas na de internetprovider komt de tunnel omhoog bij de VPN-aanbieder. Die stuurt het verkeer door naar de website die je wilt bezoeken.

Bijkomend privacyvoordeel: websites kunnen ook minder makkelijk zien wie je bent. Normaal gesproken zien sitebeheerders je ip-adres, waarmee ze op basis van je surfgedrag advertentieprofielen kunnen samenstellen en je locatie kunnen inschatten. Een VPN verhult dat en laat je vaak zelf een locatie kiezen. Daardoor kun je in Frankrijk onbekommerd Nederlandse tv-programma's terugkijken. (Of vanuit Nederland grasduinen in de Amerikaanse Netflix-catalogus.)

> ***De 4G-verbinding op je telefoon is een stuk beter te vertrouwen dan een willekeurige wifi-hotspot***
>
> **Floor Terra**
> Adviseur bij Privacy Company

Kies een VPN-aanbieder die je vertrouwt

De bescherming die een VPN biedt, valt of staat bij de betrouwbaarheid van de aanbieder, waarschuwen Terra en Engels. Wanneer je een VPN instelt, loopt ook echt al je internetverkeer via die dienst, waarmee ze in theorie al je surfgedrag kunnen inzien. 'Maar het product dat ze leveren is juist privacy. Een betrouwbare VPN-provider kiest ervoor niet te kijken', zegt David Janssen van cybersecurity- en vergelijkingssite VPNgids.nl. De hoeveelheid informatie die de aanbieder wettelijk over je moet bijhouden is afhankelijk van het land waarin hij gevestigd is. In landen als Panama of Zwitserland hoeven VPN's geen zogeheten 'logs' bij te houden van je internetgeschiedenis.

Hoe weet je of een VPN betrouwbaar is? Het is lastig te controleren of een aanbieder echt doet wat hij in de voorwaarden beweert. Er zijn gespecialiseerde sites die in de gaten houden of VPN's die beweren niks bij te houden niet toch ineens logs blijken te hebben wanneer de overheid bij een rechtszaak aan de deur klopt. Janssens VPNgids.nl bijvoorbeeld. Bits of Freedom tipt de vergelijkers van Greycoder en voor wie alle details wil doorspitten ThatOnePrivacyGuy.

Neem in elk geval geen gratis VPN, zeggen de experts. 'Die kunnen in veel gevallen meer schade aanrichten dan ze voorkomen', zegt Janssen. In het verleden kwam bijvoorbeeld de gratis VPN van Hola in opspraak, omdat de dienst slecht beveiligd was en bovendien de internetverbinding van gratis gebruikers doorverkocht aan betalende klanten. Heb je echt geen paar euro over voor een beveiligde internetverbinding? Veel aanbieders bieden een gratis proefperiode aan. Wel op tijd weer annuleren.