

Grote kans dat jij soms tot vaak gebruik maakt van een gratis, openbaar wifi-netwerk. Lekker makkelijk natuurlijk, maar niet zo veilig. Als je geen maatregelen neemt, kunnen hackers relatief eenvoudig meekijken.

Met onderstaande tips houd je kwaadwillenden zoveel mogelijk buiten de deur. Van het vliegveld en je favoriete koffietent tot de trein en de hotellobby op vakantie: openbare wifi-netwerken vind je overal. Soms hoef je alleen akkoord te gaan met de voorwaarden, maar het kan ook zijn dat je een wachtwoord als 'guest' of 'welkom' moet invullen.

Openbaar wifi-netwerk met wachtwoord is niet veiliger

De eerste tip is dan ook: een openbaar wifi-netwerk is onveilig, maar dit geldt ook voor een openbaar wifi-netwerk met een algemeen wachtwoord. Je denkt misschien dat een beveiligd netwerk risicovrij is, maar schijn bedriegt. Als het wachtwoord op de muur staat geschreven en iedereen dus hetzelfde wachtwoord moet invullen, heb je in feite nog steeds een open netwerk. Een

kwaadwillende met een laptop en wat kleine apparatuur hoeft alleen maar het wachtwoord in te vullen en het een en ander te ontsleutelen. Vervolgens heeft hij – net als op een openbaar wifi-netwerk – inzicht in jouw internetverkeer. Onthoud dus dat een wifi-netwerk niet veilig is als iedereen hetzelfde wachtwoord invult en het wachtwoord publiekelijk toegankelijk is.



Vermijd nepnetwerken

Een groot gevaar van een openbaar wifi-netwerk zonder wachtwoord is dat een kwaadwillende een nepnetwerk kan aanmaken. Hiervoor gebruikt hij een apparaatje dat dezelfde naam heeft als het echte netwerk, bijvoorbeeld 'Starbucks', 'Wifi in de trein' of 'Airport_Guest'. Verbind jij je toestel met dit netwerk dan gaat al je internetverkeer via het apparaat van de hacker. Die ziet niet alleen welke websites jij bezoekt, hij (of

zij natuurlijk) kan ook webpagina's manipuleren en die tonen in plaats van de echte webpagina. Je krijgt dan bijvoorbeeld een vervalste Instagram- of Gmail-site te zien, en vult braaf je inloggegevens in. Die krijgt de hacker dus in zijn schoot geworpen, en grote kans dat jij er niets van merkt.

Het is daarom raadzaam om het wifi-netwerk te controleren voordat je de verbinding maakt. Vraag

bijvoorbeeld de exacte naam van het netwerk aan een medewerker van de koffiezaak of winkel die gratis openbaar wifi aanbiedt. Ga ook naar de wifi-instellingen van je toestel en verwijder opgeslagen publieke wifi-netwerken. Zo voorkom je dat je apparaat automatisch verbindt met een ouder nepnetwerk. In de wifi-instellingen kan je ook aangeven dat je toestel niet automatisch mag verbinden met openbare wifinetwerken zonder wachtwoord.

Gebruik een VPN

Het beste middel om veilig te internetten op een gratis, openbaar wifi-netwerk is door een vpn te gebruiken. Een vpn staat voor Virtual Private Network en leidt je internetverkeer als het ware door een digitale tunnel. Dit heeft twee



belangrijke voordelen, bevestigt onder andere het Nationaal Cyber Security Centrum. Allereerst stuurt een vpn je dataverkeer versleuteld naar de server van de vpn-dienst, en pas daarna ga je het openbare internet op. Dit maakt het voor kwaadwillenden veel lastiger om je internetverbinding te hacken. Met een vpn is de kans veel kleiner dat je bijvoorbeeld een nepwebpagina te zien krijgt. Ten tweede vergroot een vpn je online privacy. Je internetverbinding loopt namelijk via de server en dus ook het ip-adres van de vpn-aanbieder. Wat jouw echte ip-adres is, weet niemand. En dus kan niemand je

internetverkeer naar jou herleiden. Een tegenvaller voor hackers en adverteerders, want die kunnen ze je geen gepersonaliseerde reclames voorschotelen.

Er zijn honderden gratis en betaalde vpn-diensten. Onthoud dat een vpn-aanbieder altijd geld moet verdienen. Is de vpn gratis, dan bestaat de kans dat de aanbieder jouw gegevens doorverkoopt aan derde partijen. Dat wil je niet. We raden je daarom aan te kiezen voor een betaalde vpn-dienst van een gerenommeerd bedrijf, bijvoorbeeld [Bitdefender Premium VPN](#).

Installeer een antivirusprogramma

De kans dat jij alle digitale gevaren op tijd opmerkt, is klein. Aanvallers zitten niet stil en maken hun apparatuur en malafide software steeds geavanceerder. Kenners adviseren daarom een

antivirusprogramma te gebruiken op je laptop, smartphone en andere toestellen. Antivirus krijgt doorlopend updates en houdt (potentieel) gevaarlijke activiteiten vooraf tegen. Het [Bitdefender](#)

[Internet Security 2019-pakket](#) heeft allerlei functies die je digitale veiligheid vergroten. De antivirus blokkeert bijvoorbeeld dubieuze (nep)websites en filtert gevaarlijke sites uit je zoekresultaten.

Stel gevoelige zaken uit

Als je zonder vpn gebruikmaakt van een openbaar wifi-netwerk, kan je beter geen belangrijke zaken regelen. Bankieren, inloggen op websites, iets bestellen bij je favoriete kledingwebshop: stel het als het kan uit. Je bent immers kwetsbaar en dan wil je geen risico nemen dat een hacker aan de haal gaat met jouw inloggegevens of andere gevoelige data. Met een (goede) vpn ben je

veiliger, al raden we aan om echt gevoelige zaken alleen te doen op

vertrouwde wifi-netwerken – en dan het liefst ook met een vpn.

Bonus: gebruik geen publieke wifi

Hoewel er genoeg manieren zijn om je te beschermen op een publiekelijk wifi-netwerk, is het beste advies om helemaal geen gebruik te maken van een openbaar netwerk. Met of zonder algemeen wachtwoord: zo'n netwerk is veiliger dan je wifi thuis. Een vpn verbetert je beveiliging aanzienlijk, maar biedt nooit honderd procent veiligheid. Je kan daarom het beste gebruikmaken van een eigen wifi-netwerk of je mobiele databundel (eventueel in combinatie met een vpn). Als je een grotere databundel hebt en op een ander apparaat wilt internetten, kan je de tether-functie gebruiken om een hotspot op te zetten.