Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Wifi onderweg: gebruik een VPN

Wifi thuis: gebruik WPA2

Factsheet FS-2008-01
versie 2.0 | 6 augustus 2015

Wifi biedt draagbare apparaten zoals laptops, tablets en smartphones eenvoudig draadloos internettoegang. De voordelen hiervan zijn dat thuis geen netwerkkabels meer nodig zijn, en dat iedereen ook in horecagelegenheden of het openbaar vervoer kan surfen en e-mailen. Er wordt ook gewaarschuwd voor beveiligingsrisico's. Wat zijn die risico's en wat kunt u zelf doen om veilig gebruik te maken van wifi?

Om veilig gebruik te maken van openbaar wifi adviseert het NCSC om altijd gebruik te maken van een Virtual Private Network (VPN) om de eigen verbinding te beveiligen.

Om wifi thuis veilig in te stellen adviseert het NCSC om WPA2-beveiliging met AES-encryptie in te stellen, in combinatie met een zo lang mogelijk wachtwoord.

Wat is wifi?

Wifi is een lokaal draadloos netwerk dat meestal wordt gebruikt om op een bepaalde locatie internet aan te bieden. Het wordt vaak aangeboden in horeca, kantoren en het openbaar vervoer. U kunt het ook thuis gebruiken; internetproviders stellen daarvoor draadloze modems beschikbaar.

U kunt van wifi gebruikmaken met uw smartphone, tablet of laptop. Met name smartphones hebben ook andere technieken voor draadloze communicatie, zoals 3g of 4g. Die technieken werken anders dan wifi; deze factsheet gaat niet in op de beveiligingsrisico's daarvan.

Wat is het risico?

Bij een draadloos netwerk gaat alle communicatie door de lucht via radiosignalen. Deze radiosignalen kunnen door iedereen in de buurt worden opgevangen. Als er kwaadwillenden in de buurt zijn, kunnen zij op die manier uw internetverkeer aftappen of beïnvloeden. Dit betekent dat de inhoud van uw e-mails, uw surfgedrag en zelfs uw wachtwoorden kunnen worden meegelezen of gewijzigd door anderen.

Wat kan ik doen?

Afhankelijk van of u thuis uw eigen wifi-netwerk gebruikt of op een openbare plek verbinding maakt met een aangeboden wifi-netwerk, bestaan er verschillende risico's en zijn er maatregelen te nemen om veilig te kunnen internetten.

Op de volgende pagina's leest u voor elke situatie wat het NCSC adviseert te doen.

Doelgroep
Deze factsheet richt zich op gebruikers van wifi. Het biedt zowel advies aan wie thuis een wifi-netwerk voor eigen gebruik heeft, als aan wie onderweg gebruik wil maken van openbare wifi-netwerken.

Samenwerkingspartners
Deze factsheet is tot stand gekomen in samenwerking met Ziggo en KPN.

Na het lezen van deze factsheet kunt u:

- de risico's van het gebruik van openbaar wifi onderkennen en inschatten;
- voor uzelf bepalen wanneer u met zo min mogelijk risico op afluisteren gebruik kunt maken van openbaar wifi;
- voorkomen dat onbekenden meeliften op het wifi-netwerk bij u thuis.

Onderweg

Wat kan er misgaan als ik van openbaar wifi gebruikmaak?

Een aanvaller kan op twee manieren openbaar wifi misbruiken. De aanvaller kan uw verbinding aftappen en daardoor al het internetverkeer **afluisteren**. Daarnaast kan een kwaadwillende persoon met een eigen apparaat zelf een draadloos netwerk aanmaken, om apparaten (automatisch) verbinding te laten maken met een **vals netwerk**.

Wat gebeurt er als een netwerk wordt afgeluisterd?

Openbaar wifi is voor iedereen toegankelijk. Daardoor kunnen mensen met slechte bedoelingen het netwerkverkeer afvangen en daarop alle langskomende gegevens afluisteren. Hierdoor loopt u onder meer de volgende risico's:

- uw e-mails kunnen worden meegelezen waardoor uw privéleven op straat kan belanden;
- uw inloggegevens kunnen worden gestolen waardoor anderen uw accounts kunnen misbruiken en zich als u kunnen voordoen;
- uw surfgedrag kan worden geregistreerd waardoor partijen ongemerkt een persoonlijk profiel van u kunnen vastleggen.

Het afluisteren van internetverkeer is zeer eenvoudig en gebeurt onopvallend. Daardoor vormt dit een groot risico voor u als gebruiker.

Wat gebeurt er als ik met een vals netwerk verbinding maak?

Wanneer u verbinding maakt met een vals netwerk, kan een aanvaller (net als bij het afluisteren van een openbaar netwerk) al uw internetverkeer meelezen. Daarnaast kan het internetverkeer worden omgeleid of aangepast waardoor u de volgende risico's loopt:

- wanneer u ergens voor wilt inloggen kan een namaak-inlogpagina worden getoond die uw wachtwoord steelt;
- websites die u normaliter vertrouwt kunnen misleidende of aanstootgevende informatie of virussen bevatten;
- er kunnen valse updates voor apps worden aangeboden die in werkelijkheid een virus achterlaten.

Welke netwerken zijn veilig?

Uw apparaat kan met het hangslot-pictogram aangeven of een netwerk beveiligd is. Wanneer dat zo is, dan hebt u ook een wachtwoord nodig dat het plaatselijke personeel kan verzorgen. Deze beveiliging maakt de kans op afluisteren kleiner, maar het neemt het risico niet weg. Daarom blijft het raadzaam om uw eigen verbinding met de dienst die u gebruikt goed te controleren.

Bij sommige openbare netwerken moet u op een webpagina inloggen of gebruikersvoorwaarden accepteren voordat u internettoegang krijgt. Deze barrière bevindt zich echter pas op het punt waar verbinding met het internet wordt gemaakt; het verhindert kwaadwillenden niet om verbinding te maken met het lokale netwerk zelf. Al heeft de aanvaller dan zelf geen internettoegang, ook zonder internet kan uw verkeer worden afgeluisterd of beïnvloed.

Hoe kan ik veilig surfen op een publieke wifi-hotspot?

Bepaal als eerste wat u wilt doen en wat de gevolgen voor u zijn als u daarbij wordt afgeluisterd. Bij het lezen van het weerbericht kan er weinig misgaan, maar als u bijvoorbeeld inlogt op een sociaal netwerk dan kan een aanvaller uw wachtwoord misschien aflezen en zich vervolgens als u voordoen.

Gebruik een VPN

Het NCSC adviseert gebruik te maken van een Virtual Private Network (VPN). Een VPN is een beveiligde verbinding tussen uw apparaat en een bepaalde server elders op het internet. Deze verbinding is versleuteld waardoor anderen het niet kunnen lezen, waardoor dit als het ware een privénetwerk is geworden. Al het internetverkeer van en naar uw apparaat gaat via deze afgeschermde route en kan op dit deel niet afgeluisterd worden.

Voordelen van een VPN

- Uw verbinding is geheel beveiligd, u hebt geen omkijken meer naar afluisteraars of beïnvloeding en kunt met een gerust hart internetten.
- U hoeft een VPN slechts eenmaal in te stellen op uw apparaat en kunt daarna vaak met één druk op de knop een veilige verbinding opzetten.

Nadelen van een VPN

- Om een VPN te kunnen gebruiken moet u een account hebben bij een VPN-aanbieder, hieraan zijn mogelijk kosten verbonden.
- Omdat het internetverkeer van alle gebruikers van hetzelfde VPN via één punt gaat kan dit op drukke momenten tot een langzamere verbinding leiden.

Wilt u geen VPN gebruiken? Kijk dan op de volgende pagina, u kunt afhankelijk van wat u wilt doen alternatieve maatregelen nemen.

Het NCSC adviseert gebruik te maken van een Virtual Private Network, VPN (zie het kader op de vorige pagina). Wilt u geen VPN gebruiken? Dan kunt u afhankelijk van wat u wilt doen alternatieve maatregelen nemen:

Ik wil e-mailen

E-mailen kan op verschillende manieren. Mogelijk heeft u uw e-mailaccount ingesteld in het besturingssysteem van uw mobiele apparaat, heeft u een aparte app of maakt u gebruik van webmail (e-mail via een website). Zie voor het gebruik van webmail het kader hieronder, *ik wil een website bezoeken*.

Voor het gebruik van e-mail via een programma, app of ingebouwde functionaliteit van uw apparaat, dient u in de verbindingsinstellingen voor een met TLS beveiligde verbinding te kiezen, of de optie STARTTLS in te schakelen. Neem contact op met uw e-mailprovider als dit niet werkt.

Ik wil werken

Informeer bij uw werkgever hoe u verbinding kunt maken met de systemen op het werk. Uw beheerder kan bijvoorbeeld zorgen voor een beveiligde (VPN-)verbinding. Uw werkgever kan aangeven of het veilig genoeg is om via openbare wifi in te loggen op het werk.

Ik wil een website bezoeken

U kunt een beveiligde verbinding met een website herkennen aan de vermelding in de adresbalk. Wanneer het internetadres begint met https://, dan is er een beveiligde verbinding. Vaak vermeldt uw browser ook een icoon van een hangslot. Wanneer u daarop klikt ziet u het beveiligingscertificaat dat bij de website hoort.

Het beveiligingscertificaat geeft aan dat u een directe en beveiligde verbinding hebt met de juiste server achter het adres dat u bezoekt. Het is daarbij wel belangrijk dat u goed let op het juiste adres. Typ daarom zelf het adres in de adresbalk van uw browser. Klik niet op links in e-mailberichten en gebruik geen zoekmachine om inlogpagina's te openen.

Als er iets niet in orde is met het certificaat, zal uw browser een waarschuwing geven. In dat geval is het mogelijk dat uw verbinding wordt afgeluisterd of beïnvloed. Ga dan niet verder naar die website.

Ik wil een app gebruiken

Van mobiele apps is de veiligheid van de verbinding niet te beoordelen door de gebruiker. De verantwoordelijkheid ligt hierin bij de uitgever van de app. Informeer bij de uitgever of deze veilig gebruikt kan worden over openbare wifi. Zo niet, dan kunt u de app beter via VPN of uw 3g- of 4g-verbinding gebruiken.

Officiële apps van veelgebruikte diensten zijn meestal veilig. Vanwege de bekendheid van deze apps kunnen beveiligingsproblemen daarin sneller worden ontdekt en opgelost. Sommige apps voor internetbankieren of van grote sociale netwerken zijn in het verleden in het nieuws geweest vanwege gebrekkige beveiliging in hun verbinding. In antwoord daarop hebben die organisaties de bekende problemen opgelost.

Thuis

Waarom moet ik mijn wifi-netwerk thuis beveiligen?

Draadloos internet heeft een bepaald bereik vanaf het apparaat dat het aanbiedt, maar blijft niet binnen de muren van een huis. Dit betekent dat uw buurman of iemand op straat ook verbinding kan maken met uw netwerk.

Als u uw netwerk daar niet tegen beveiligt, dan kunnen de meelifters daar misbruik van maken. Zij kunnen bijvoorbeeld grote bestanden downloaden waardoor uw verbinding langzaam wordt. Daarnaast kunnen zijn aanvallen uitvoeren op anderen waar u zelf geen last van heeft, maar waarbij uw adres uiteindelijk bij de opsporing naar boven komt. Afhankelijk van de ernst kan dit leiden tot afsluiting van uw internetverbinding of een strafrechtelijk proces.

Daarnaast zijn de apparaten op uw netwerk zichtbaar voor aanvallers. Zij kunnen dan, afhankelijk van de beveiligingsinstellingen van het apparaat, mogelijk bij uw privébestanden of eenvoudig malware op uw systemen installeren.

Hoe stel ik mijn draadloze router of modem veilig in?

Stel uw draadloze netwerk in op WPA2-beveiliging met AES-encryptie. AES-encryptie zorgt ervoor dat uit de ether afgetapt netwerkverkeer niet leesbaar is voor derden. WPA2 zorgt ervoor dat een wachtwoord nodig is om verbinding te maken. Stel een zo lang mogelijk wachtwoord in, bij voorkeur meer dan 20 tekens. Gebruik niet het automatisch gegenereerde wachtwoord van uw router of modem, maar kies er zelf een.

Raadpleeg de handleiding van uw modem of router om deze te kunnen instellen.

Voor een zakelijke omgeving adviseert het NCSC om WPA2-Enterprise met AES en een authenticatieserver te gebruiken. Zo kunnen alleen geautoriseerde apparaten verbinding maken met het netwerk.

Aanvullende maatregelen

Naast het beveiligen van de verbinding kunt u nog meer maatregelen treffen om uw wifi-netwerk te beveiligen.

- Wijzig het wachtwoord van uw modem of router elk jaar.
- Stel uw modem of router zo in dat er alleen op kan worden ingelogd vanaf een computer die met een netwerkkabel verbonden is.
- Als uw modem of router UPnP (Universal Plug-and-Play) of WPS (Wireless Protected Setup) aanbiedt, schakel dit dan uit. Deze technieken zijn kwetsbaar bevonden voor verschillende aanvallen.

Wat als mijn provider wifi aanbiedt vanaf mijn router?

Meerdere internetproviders in Nederland bieden hun abonnees wifi aan via de draadloze modems van andere klanten.

Internetproviders kunnen verscheidene maatregelen nemen om de beveiliging te waarborgen.

- Versleuteld: de verbinding is versleuteld om afluisteren te verhinderen.
- Gescheiden: de wifi-gebruiker heeft een verbinding met internet die gescheiden is van die van de thuisgebruiker; zij kunnen elkaars apparaten en netwerkverkeer niet zien.
- Exclusief: alleen klanten mogen verbinding maken.
- Geauthenticeerd: beveiligingscertificaten zorgen ervoor dat uw apparaat niet met een vervalst netwerk verbinding maakt.

Is het veilig om anderen toe te laten tot mijn router?

Informeer bij uw provider welke van bovenstaande (en eventuele andere) maatregelen zijn getroffen. In de meeste gevallen zullen apparaten op uw netwerk niet direct benaderbaar zijn via de openbare wifi. Indien u het toch niet vertrouwt kunt u bij uw provider aangeven niet mee te willen doen.

Kan ik zelf veilig surfen op deze wifi-netwerken?

Informeer bij uw provider welke van bovenstaande (en eventuele andere) maatregelen zijn getroffen. Bij een goede beveiliging kunt u dergelijke netwerken als even veilig als uw thuisnetwerk beschouwen.

Ziggo WifiSpots zijn met alle bovenstaande maatregelen beveiligd en bieden daarom hetzelfde veiligheidsniveau als uw thuisnetwerk.

KPN WiFi HotSpots en KPN Fon zijn niet versleuteld en kunnen daarom afgeluisterd worden. Gebruik een VPN, bijvoorbeeld zoals KPN die bij HotSpots aanbiedt.[1] Volg ook de aanbevelingen op in het onderdeel ‘Onderweg’ in deze factsheet wanneer u van deze netwerken gebruikmaakt.

[1] Zie https://www.kpn.com/prive/mobiel-internet/hotspots-hoofd-nl/hotspots-veilig-internetten.htm.

Sommige bronnen vermelden onderstaande maatregelen. Hiervoor geldt dat zij op zichzelf geen beveiliging bieden en uitsluitend aanvullend kunnen worden gebruikt. Het NCSC plaatst kanttekeningen bij deze maatregelen.

- Door de SSID-broadcast uit te schakelen kunnen andere apparaten het netwerk niet zien, maar kan alleen verbinding gemaakt worden als de gebruiker de netwerknaam weet. Die naam is vaak eenvoudig te achterhalen voor aanvallers, en tegelijkertijd vermindert het de gebruiksvriendelijkheid voor uzelf. Het NCSC beschouwt dit daarom niet als een effectieve beveiligingsmaatregel.
- Met een Access Control List (ACL) kunt u op basis van mac-adressen van apparaten een lijst opstellen van de apparaten die verbinding mogen maken. Aanvallers kunnen hun eigen mac-adres vervalsen, als zij een geldig adres te weten komen. Het NCSC raadt aan om dit alleen toe te passen als de beheerlast van het bijhouden van de lijst proportioneel is.

Wiefie of waifai?

Wi-Fi is een handelsmerk van de Wi-Fi Alliance. Het is een variatie op HiFi, een term uit de audiotechniek. Oorspronkelijk werd de slagzin “De standaard voor Wireless Fidelity” gebruikt, maar de Wi-Fi Alliance heeft die snel ingetrokken en verklaard dat Wi-Fi geen afkorting ergens voor is.

Vandaag de dag komt de spelling wifi vaak voor, en wordt wifi gebruikt als soortnaam voor draadloos internet volgens de 802.11-techniek, ongeacht of het apparaat officieel gecertificeerd is om de merknaam Wi-Fi te dragen.

Daarnaast wordt wifi in toenemende mate in vernederlandste vorm uitgesproken, dus als /ʋifi/ in plaats van /wajfaj/.

Veilig internetten
wat je kan doen en laten

Kijk op veiliginternetten.nl voor meer informatie en advies over veilig internetten.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55 | F 070-322 25 37
Publicatienr: FS-2008-01 2.0 | Aan deze informatie kunnen geen rechten worden ontleend.