

Niet elk wifi-netwerk is veilig!

Onlangs hebben we met een [poll](#) gevraagd of je verbinding zou maken met een “gratis” wifi-netwerk. Daaruit bleek dat ruim een kwart van de medewerkers van een openbaar wifi-netwerk gebruik zou maken.

Er zijn veel openbare wifi-netwerken beschikbaar. Echter, je weet nooit of een gratis openbaar wifi-netwerk (ook hotspots genoemd) van bijvoorbeeld een café, hotel, camping, vliegveld, trein of bus veilig is. Ook niet als je een wachtwoord (icoontje met slotje) nodig hebt. Ook als er een wachtwoord wordt gevraagd weet je namelijk niet hoe goed de beveiliging is en wie de anderen zijn die ook op dat wifi-netwerk zitten.

Zodra je inlogt op een openbaar wifi-netwerk, kan een kwaadwillende vrij eenvoudig toegang krijgen tot je internetverkeer en daardoor tot je persoonlijke gegevens. Want soms is een wifi-netwerk nep (maar lijkt deze echt), of heet deze exact hetzelfde als een bekend wifi-netwerk (waarmee indien zo ingesteld automatisch verbinding wordt gemaakt), of doet het zich met een minieme naamsverandering voor als een bekend wifi-netwerk.

Het grootste veiligheidsrisico van gratis wifi is dat de kwaadwillende (hacker) tussen jouw apparaat en het verbindingspunt kan gaan zitten. In dat geval communiceer je niet rechtstreeks met de hotspot, maar verzend je je informatie naar de hacker, die deze weer doorstuurt.

In dat geval kan de hacker rechtstreeks toegang krijgen tot alle informatie die je naar internet verzendt, zoals bankgegevens, inloggegevens en e-mails. Wanneer hij/zij deze informatie bemachtigt, kan die persoon onder jouw naam toegang krijgen tot jouw systemen en gegevens en kan zo gegevens manipuleren of bijvoorbeeld uit jouw naam malware verspreiden.

Wil je zien hoe dit werkt? Bekijk [dit filmpje](#) om te zien hoe hackers kunnen inbreken op een openbaar wifi-netwerk.

Neem een paar veiligheidsmaatregelen en blijf alert. Let hierbij op de volgende zaken:

Maak op kantoor alleen verbinding via ons eigen netwerk en maak buiten het gemeentehuis verbinding via de token

Op kantoor log je rechtstreeks in op ons eigen beveiligde wifi-netwerk “Medewerkers”, ook als je inlogt via smartphone, laptop of tablet. Van buiten het gemeentehuis is een VPN-verbinding (Virtual Private Network) een must als je veilig op het bedrijfsnetwerk wilt komen. Dit gebeurt al vanzelf als je “buiten”

via Citrix op je laptop met je token inlogt. Op je smartphone veilig e-mail van je werk checken, doe je via de Secure Hub of Secure Mail app (ook van Citrix). Zelfs áls het een hacker lukt om zichzelf te positioneren tussen jou en het verbindingspunt, zijn de gegevens nog steeds sterk versleuteld en dus onleesbaar. Maak in geen geval gebruik van wifi-netwerken die je niet kent of herkent.

Wissel geen gevoelige gegevens uit via een openbaar wifi-netwerk

Als je bijvoorbeeld toegang wilt krijgen tot je sociale netwerk, webwinkel of internetbankieren, kan je die beter bezoeken via je 3G of 4G (of straks 5G) verbinding in plaats van via een open wifi-verbinding. Gebruik je toch open wifi? Houd het dan alleen bij surfen of muziek luisteren, bezoek alleen websites via HTTPS en deel in geen geval persoonsgegevens.

Let op het automatisch verbinden

Ook als je geen verbinding hebt gemaakt met een netwerk, verzendt jouw apparaat gegevens naar alle netwerken binnen het bereik. Zet het “automatisch verbinden” met wifi-netwerken daarom uit en ruim af en toe de ongewenste draadloze netwerken die jouw apparaat heeft onthouden op. Dit laatste doe je door opgeslagen netwerken te verwijderen/vergeten op het toestel. Zet daarnaast wifi (evenals bluetooth overigens) uit als je die niet nodig hebt. Een bijkomend voordeel is dat de accu dan langer meegaat.

Vragen of opmerkingen over dit artikel? Laat het weten!

Aangemaakt door:



Bernard Jansen

5 augustus, 14:32

Laatst gewijzigd door:



Bernard Jansen

5 augustus, 14:43