de Correspondent

Update

20.03.2014 • Leestijd 2 minuten

De wifinetwerken van cafés, treinen en andere openbare plekken zijn inherent onveilig. Welke maatregelen kun je als terrasbezoeker of treinreiziger treffen?

Hoe kun je veilig gebruikmaken van een openbaar wifinetwerk?

Correspondent Technologie & Surveillance

Maurits **MARTIJN**

Illustratie: Esther Aarts (voor De Correspondent)

Publieke wifinetwerken zijn onveilig. Hackers kunnen, als zij willen, relatief simpel toegang krijgen tot de laptops en smartphones die ermee verbonden zijn. Ethisch hacker Wouter Slotboom heeft laten zien wat 'toegang' zoal kan betekenen: van het meekijken met het surfgedrag tot het achterhalen van wachtwoorden van banken. Goed, maar we willen wel blijven internetten op het terras of in de kroeg. Ik legde een aantal experts de vraag voor: welke maatregel kun je als gebruiker van openbare netwerken nemen?

1. Maak geen gebruik van een openbaar wifinetwerk

Eigenlijk is het heel simpel: als je echt zeker van je zaak wilt zijn, maak je geen verbinding met een openbaar netwerk. Twee weken geleden zei de baas van Interpol, Troels Oerting, nog tegen de BBC: 'Alles wat je verstuurt via wifi loopt potentieel gevaar.' Ook het Nederlandse Nationaal Cyber Security Centrum raadt af om gebruik te maken van een publiek wifinetwerk. Dit betekent dat als je onderweg toch het internet op wilt, je het beste gebruik kan maken van mobiele data. Dat kost relatief veel geld, maar is het waard.

2. Virtual private network (VPN)

Als je dan toch besluit om in te loggen op openbare wifinetwerken, dan is er eigenlijk maar één maatregel die jouw internetverkeer kan beschermen: een VPN, een *virtual private network*. Dit stelt de gebruiker in staat om op het wifinetwerk een versleutelde tunnel op te zetten naar een server die je wel vertrouwt. Je verkeer wordt dan eerst versleuteld naar die server gestuurd (van de VPN-provider of thuis) om vanaf daar het internet op te gaan.

Er zijn heel veel verschillende VPN-aanbieders. Sommige zijn betaald, zoals bijvoorbeeld Vpntunnel.se, Ipredator.se en Privateinternetaccess.com. Andere zijn gratis, zoals bijvoorbeeld (deels) Proxpn.com en Openvpn.net.

Veel smartphones hebben tegenwoordig ingebouwde VPN-software die je, na enkele handelingen, kunt activeren. Er zijn ook VPN-apps te downloaden voor verschillende besturingssystemen. Dé tip van experts: neem de tijd om je in VPN te verdiepen en te bepalen welke dienst het beste bij jou, jouw apparaten en je internetgedrag past.

3. Zet wifi uit

Zorg altijd dat je smartphone, tablet of laptop niet standaard naar wifinetwerken zoekt. Zorg er in ieder geval voor dat je apparaat niet automatisch verbinding maakt met 'bekende netwerken,' want die zijn misschien helemaal niet zo bekend als ze zich voordoen. Verwijder, indien mogelijk, de wifinetwerken uit je instellingen en schakel de optie uit dat verbonden netwerken standaard worden onthouden.

context te voorzien. Door het nieuws in een breder perspectief of in een ander licht te plaatsen, willen wij het begrip 'actualiteit' herdefiniëren: niet om je aandacht te trekken, maar om je inzicht te bieden in hoe de wereld werkt.