Een restaurant zoeken, het weer checken of Skypen. Op vakantie kunnen we niet zonder internet. Maar het gebruik van wifi op de camping of in hotel is niet zonder risico's.

ILLUSTRATIE **VIJSELAAR & SIXMA** TEKST **DENNIS BAATEN SECURITY CONSULTANT BIJ BAATEN ICT SECURITY**

DE WIFI OPLICHTER

WIFI NIET ZONDER RISICO'S

Je komt thuis van vakantie en gaat naar de supermarkt om de lege koelkast te vullen. Met een volle kar bij de kassa meldt de pinautomaat: 'Betaling niet gelukt. Saldo ontoereikend'.
Toen je vorige week met je laptop aan het zwembad van de camping je bankzaken afhandelde, stond er nog voldoende geld op je rekening. Thuis zie je een aantal onverklaarbare transacties. Je belt met je bank en het wordt duidelijk: je bent slachtoffer van internetcriminelen die het gemunt hebben op toeristen die via publieke wifi-netwerken (zoals de gratis wifi van de camping) verbinding maken met internet.

Wat is er gebeurd?

Laptops, tablets en telefoons zoeken continu naar draadloze netwerken in de omgeving. Vaak zijn deze apparaten ingesteld om automatisch verbinding te maken met bekende netwerken (waarmee eerder verbinding is geweest). Heb je ooit verbinding gemaakt met het netwerk 'camping-wifi', dan zal je laptop ook op andere locaties naar dit netwerk zoeken om automatisch verbinding te maken. Internetcriminelen misbruiken dit mechanisme. Met behulp van speciale apparatuur vangen zij signalen op van apparaten die zoeken naar bekende wifi-netwerken. Wanneer het een zoeksignaal betreft naar een open wifi-netwerk (zonder wachtwoord), zal de internetcrimineel zich voordoen als het desbetreffende netwerk. Je laptop maakt dan automatisch verbinding en denkt verbonden te zijn met het bekende wifi-netwerk, terwijl er in werkelijkheid verbinding is met het netwerk van de internetcrimineel. Vanaf dat moment fungeert het vervalste wifi-netwerk als een doorgeefluik tussen je computer en het internet; de internetcrimineel heeft de volledige controle over je internetverbinding.
De internetcrimineel kan nu het berichtenverkeer tussen je computer en het internet lezen en aanpassen. Concreet: hij kan je wachtwoorden zien. Aangezien veel mensen voor verschillende sites dezelfde wachtwoorden gebruiken, kunnen de gevolgen enorm zijn.
Dit geldt normaliter niet voor beveiligd verkeer, te herkennen aan het 'slotje' in je browser. Echter, de speciale apparatuur van criminelen forceert je browser tot het opzetten van een onbeveiligde verbinding, waardoor vertrouwelijke gegevens misbruikt kunnen worden.
Weet dat de verantwoordelijkheid voor veilig internetten in toenemende mate verschuift naar onszelf. Banken hebben zelfs regels opgesteld voor veilig internetbankieren. Eén van deze regels luidt letterlijk: 'Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken'. **Hou jij je niet aan de regels en word je slachtoffer van misbruik, dan wordt de schade waarschijnlijk niet door je bank vergoed.**

7 tips: veilig internetten op vakantie

1. **Maak liever geen verbinding met een open wifi-netwerk, dus zonder wachtwoord.**
2. **Mocht je toch verbinding met een open netwerk maken, voer geen persoonlijke gegevens in zoals wachtwoorden en inlognamen.**
3. **Ook een verbinding met 'het slotje' is niet altijd te vertrouwen.**
4. **Gebruik je geen wifi, zet deze dan uit op je apparaat.**
5. **Verbind niet automatisch met 'bekende netwerken'.**
6. **Wil je onderweg vertrouwelijke informatie versturen, maak dan gebruik van de 3G- of 4G-verbinding.**
7. **Gebruik een browser die onthoudt wanneer een website vraagt om 'in het vervolg uitsluitend beveiligde verbindingen voor deze website te gebruiken'.**
8. **Varieer je wachtwoord-gebruik.**