

Meerderheid Nederlanders maakt onveilig gebruik van openbare wifi

17 augustus, 2021



Het gebruik van een openbare wifi, bijvoorbeeld bij een treinstation, vliegveld of hotel is heel gebruikelijk. Helemaal in deze zomerperiode, waarin iedereen er weer wat meer op uittrekt.

Er zitten echter wel gevaren aan het verbinding maken met een wifi hotspot. Als je niet weet wat je doet, kan het hackers gemakkelijker toegang geven tot jouw gegevens. Daarom hebben wij van VPN.nl een representatief onderzoek laten uitvoeren naar het gebruik van openbare wifiverbindingen. Dit onderzoek is gedaan onder 1.075 Nederlanders en uitgevoerd door Panelwizard.

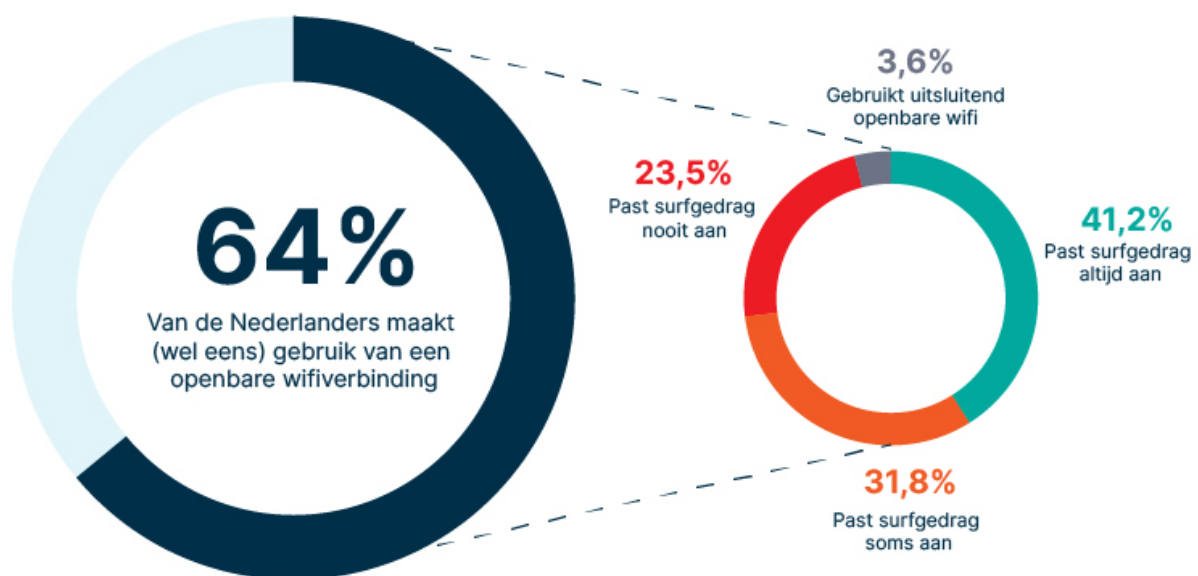
Onderzoekresultaten

De belangrijkste conclusie uit het onderzoek is dat het merendeel van de Nederlanders zijn of haar sufgedrag lang niet altijd aanpast bij het gebruik van een [openbare wifiverbinding](#). Dat terwijl een ruime meerderheid wel op de hoogte is van de risico's die hieraan verbonden zijn.

Zo geeft maar liefst 88 procent van de Nederlanders aan te weten dat een openbare wifi hotspot onveilig kan zijn. 92,1 procent van de mannen zijn zich bewust van de gevaren. Bij vrouwen is dit 84,3 procent.

Ondanks dit besef geeft slechts **41,2** procent van de Nederlanders – die een openbare wifi gebruiken – aan altijd hun surfgedrag aan te passen. Deze groep is over het algemeen verstandig en gebruikt de openbare verbinding alleen voor het hoognodige. Sommigen binnen deze groep kiezen voor een [VPN](#) om de verbinding te beveiligen.

Vrouwen zijn overigens iets veiliger bezig dan mannen: 44,2 procent pas het surfgedrag altijd aan. Bij mannen is dit 37,7 procent.



31,8 procent van de gebruikers past het surfgedrag alleen soms aan bij het gebruik van een wifispot, bijvoorbeeld bij het gebruik van bankapps. Een hacker dan in ieder geval niet bij financiële gegevens komen.

Als toelichting geeft deze groep gebruikers bijvoorbeeld het volgende:

- “Ik pas mijn surfgedrag aan als ik er aan denk”
- “Ik bekijk geen bankzaken”
- “Ik log niet in bij belangrijke sites”
- “Het is afhankelijk van wat ik ga doen”

Er ‘soms’ mee rekening houden is niet voldoende

Toch is het ‘soms’ aanpassen van het surfgedrag niet genoeg om de veiligheid te garanderen. Een hacker kan namelijk allerlei gevoelige informatie onderscheppen, zoals mailtjes en berichtjes die je verstuurt of inloggegevens

die worden ingevoerd op een website. Het is daarom belangrijk om altijd op de hoede te blijven.

Bij **23,5 procent** van de Nederlanders die wifi hotspots gebruiken, is het surfgedrag niet anders bij het gebruik van een openbare wifi-verbinding. Deze groep houdt dus geen rekening met de risico's en zijn daardoor zeer kwetsbaar voor hacks van hun gegevens.

Veelgehoorde uitleg die hierbij wordt gegeven:

- "Denk er niet bij na"
- "Sta er niet bij stil"
- "Ik wist niet dat het onveilig was"
- "Ik heb geen geheimen"

Tot slot geeft **3,6 procent** van de ondervraagden aan uitsluitend openbare verbindingen gebruiken en daarom het surfgedrag ook niet aanpassen ten opzichte van een beveiligde verbinding.

Wat zijn de gevaren?

Een openbare wifi hotspot is zelden veilig. Dat komt omdat de verbinding doorgaans niet is versleuteld en iedereen zonder wachtwoord verbinding kan maken met het netwerk. Dat geldt ook voor kwaadwillende hackers. Zij zien hier hun kans om toe te slaan en gebruiken verschillende trucs om gevoelige informatie te ontfutselen.

Wat regelmatig gebeurt, is dat een hacker tussen het jouw apparaat en het verbindingspunt gaat zitten en informatie onderschept die jij verstuurt en ontvangt. Als wifigebruiker merk je daar niets van, maar je loopt wel gevaar.

Koen Kuijper (VPN.nl)

Het meest gevaarlijke is als een hacker zelf een nep openbaar wifinetwerk beschikbaar stelt, bijvoorbeeld onder de naam "IKEA Free Wifi" of "NS Reizigers Wifi". Klinkt betrouwbaar toch? Als slachtoffer word je zo misleid en maak je verbinding met de apparatuur van een hacker.

Met deze werkwijze kunnen mailtjes, creditcardgegevens en inloggegevens worden buitgemaakt. In het ergste geval kan een hacker toegang krijgen tot systemen of accounts die op jouw naam staan.

Wie gebruik maakt van een openbare wifi, zou het internet eigenlijk alleen moeten gebruiken voor neutrale bezigheden, zoals het bezoeken van een internetpagina of nieuwssite, zonder daarbij in te loggen. Nog beter is om een

VPN (Virtual Private Network) te gebruiken die alle verstuurd en ontvangen gegevens versleuteld.

Koen Kuijper (VPN.nl)

Ruim 2 miljoen hotspots

Volgens de Consumentenbond zijn er in Nederland meer dan 2 miljoen locaties waar je met je laptop, smartphone of tablet kunt inloggen op een gratis wifinetwerk.

Populaire locaties zijn:

- Treinen en treinstations
- Luchthavens
- Grote ketens, zoals IKEA, McDonalds en Starbucks
- Campings en vakantieparken
- Horecagelegenheden

Vooraf jongeren lopen risico

Uit het onderzoek blijkt verder dat vooral jongere volwassenen (onder de 30 jaar) kwetsbaar zijn voor een hack via een openbare wifispot:

- Bijna 75 procent van hen maakt wel eens gebruik van zo'n onbeveiligde verbinding.
- Slechts 29 procent van de jongeren altijd hun surfgedrag aanpassen
- 38 procent van hen doet dit alleen soms, bijvoorbeeld voor bankapps
- 34 procent van de jongvolwassenen past zijn of haar surfgedrag nooit aan, met alle risico's van dien

Het is belangrijk dat jongvolwassenen begrijpen wat de gevaren kunnen zijn van een onbeveiligde wifi. Hopelijk draagt ons onderzoek daar aan bij.

Koen Kuijper (VPN.nl)

Steeds populairder

Ondanks de risico's groeien wifi hotspots in populariteit. 64 procent van de Nederlanders maakt er tegenwoordig (wel eens) gebruik van, blijkt uit het onderzoek. Dat is ruim [14 procentpunt](#) meer dan in 2016 (CBS).

60-plussers zijn minder happig op het gebruik van openbare wifi verbindingen. Slechts 57 procent maakt er gebruik van. Zij zijn zich overigens ook minder bewust van de potentiële gevaren.

De vraag is of de populariteit van wifi hotspots blijft. Telefoonabbonementen met 4G worden steeds goedkoper. Ook de dekking en snelheid van deze netwerken wordt steeds beter. Niet alleen in Nederland, maar ook in de rest van de wereld.

Over het onderzoek

De verantwoording voor dit onderzoek is [hier terug te lezen](#).

Voor vragen of opmerkingen kan er contact worden opgenomen via koen@vpn.nl of 010 – 34 000 12.