NordVPN
powered by NORD SECURITY

Online security starts with a click

Press Release

10 augustus, 2022
Meer informatie: brigita@nordsec.com

1 op 4 mensen wordt gehackt op weg naar hun vakantiebestemming

Reizigers opgelet: hackers compromitteren wifi op luchthavens en in treinen

Volgens recent onderzoek van NordVPN wordt 1 op de 4 reizigers gehackt wanneer ze gebruikmaken van openbare wifi tijdens het reizen in het buitenland. De meeste reizigers worden gehackt op treinstations, busstations of luchthavens terwijl ze op doorreis zijn.

"Het is gebruikelijk om met je telefoon bezig te zijn terwijl je op een vlucht of trein wacht. Wanneer mensen op vakantie zijn, hebben ze echter de neiging om hun online beveiliging te vergeten", zegt Daniel Markuson, een cybersecurity-expert bij NordVPN. "Hackers maken daar misbruik van en gebruiken de zwakke plekken in het openbare wifi-netwerk op vliegvelden en treinstations om gevoelige persoonlijke informatie of bedrijfsgegevens in handen te krijgen."

Wat zijn de gevaren van openbare wifi op luchthavens en treinstations?

Reizigers zijn gemakkelijker te misleiden omdat ze meestal niet weten wat de legitieme wifi-naam op een bepaalde plek in het buitenland is. Dit maakt het voor hackers gemakkelijker om een "**evil twin**" — oftewel nep wifi-spot — op te zetten op plaatsen die vaak door toeristen worden bezocht, zoals luchthavens of treinstations. Als een reiziger verbinding maakt met zo'n hotspot, wordt al zijn persoonlijke informatie (waaronder betaalkaartgegevens, privé-e-mails en diverse inloggegevens) naar een hacker gestuurd.

Legitieme openbare wifii-netwerken kunnen echter ook onveilig zijn, omdat ze nog steeds openbaar zijn. Een hacker kan op elk moment verbinding maken met een open netwerk, de online activiteiten van gebruikers afluisteren en hun wachtwoorden en persoonlijke informatie stelen. Deze aanval wordt een **man-in-the-middle-aanval** genoemd en wordt door cybercriminelen opgezet door hun apparaat tussen de verbinding met het apparaat van een gebruiker en de wifi-spot te plaatsen.

"De enige manier om je apparaat tegen een man-in-the-middle-aanval te beschermen is het gebruik van een VPN. Uit ons onderzoek blijkt dat meer dan 78% van de mensen geen VPN gebruikt als ze op reis verbonden zijn met openbare wifi, waardoor ze kwetsbaarder zijn voor aanvallen van hackers", aldus Daniel Markuson.

Zo kunnen reizigers zichzelf beschermen

Hoewel openbare wifi risico's met zich meebrengt voor onze gegevens, blijft het nog steeds een noodzaak voor veel reizigers. Experts bij NordVPN zetten op een rijtje wat gebruikers kunnen

doen om hun apparaten tijdens het reizen te beschermen:

- **Gebruik een VPN**. De beste en meest effectieve manier om de veiligheid van reizigers op een open wifi-verbinding te garanderen, is door gebruik te maken van een VPN-dienst. Een VPN versleutelt gegevens en zorgt ervoor dat derden de gegevens van een gebruiker niet kunnen onderscheppen.
- **Schakel automatische verbindingen uit**. Dit voorkomt dat je verbinding maakt met een netwerk waarmee je geen verbinding wilt maken.
- **Deel je gegevens niet**. Reizigers maken graag onderweg reserveringen. Dit is natuurlijk handig, vooral als je veel vrije tijd voor je vlucht hebt. Omdat dit je gegevens ook kwetsbaarder maakt, raden we je af om hotels of vliegtickets te boeken terwijl je met een openbaar netwerk bent verbonden. Een hacker zou zomaar online bankgegevens of creditcardgegevens kunnen buitmaken.

OVER NORDVPN

NordVPN is 's werelds meest geavanceerde VPN-dienstverlener en wordt wereldwijd door miljoenen internetgebruikers gebruikt. NordVPN biedt dubbele VPN-encryptie, Onion Over VPN, en garandeert privacy met zero tracking. Een van de belangrijkste kenmerken van het product is Threat Protection, wat kwaadaardige websites, malware, trackers en advertenties blokkeert. NordVPN is zeer gebruiksvriendelijk, biedt een van de beste prijzen op de markt en heeft meer dan 5.000 servers in 60 landen wereldwijd. Voor meer informatie: http://nordvpn.com/nl/.

FOTO