

Barrierefreie Version

CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: Öffentliche WLAN-Netzwerke & VPN

Vorsicht bei der Nutzung öffentlicher WLAN-Netzwerke!

Die Nutzung öffentlicher WLAN-Netzwerke, beispielsweise in der Bahn oder in Hotels, birgt die Gefahr des Datendiebstahls und der Einschleusung von Schadsoftware. Um die Datenübertragung zu verschlüsseln und damit die Risiken zu minimieren, empfiehlt sich die Nutzung eines Virtual Private Network (VPN).

Öffentliche WLAN-Netzwerke

Öffentliche WLAN-Netzwerke können unverschlüsselt sein. Andere Nutzende des WLAN-Netzwerks können dann die zwischen Ihrem Endgerät und dem WLAN-Hotspot übertragenen Daten abfangen und/oder mitlesen. Schlimmstenfalls kann Ihr Gerät außerdem mit Schadsoftware infiziert werden.²

Handlungsempfehlungen zur Nutzung öffentlicher WLAN-Netzwerke: ²

1. Nutzen Sie ein Virtual Private Network (VPN).
2. Nutzen Sie möglichst nur Webadressen, die mit „**https://**“ beginnen. Diese Seiten übertragen Daten verschlüsselt.
3. Deaktivieren Sie die Dateifreigabe und/oder die Verzeichnisfreigabe bei der Verbindung mit einem WLAN-Netzwerk, so dass der unberechtigte Zugriff auf Daten unmöglich ist.
4. Löschen Sie genutzte und gespeicherte öffentliche WLAN-Netzwerke aus Ihren Verbindungen, damit sich das Gerät bei Verfügbarkeit des Netzes nicht automatisch damit verbindet.
5. Schalten Sie WLAN unterwegs nur an, wenn Sie es tatsächlich benötigen.

