Risiken in öffentlichen Wlan-Netzen:

Wie Sie sich schützen können

Um für den Internetzugang außerhalb des eigenen Wlans nicht extra zu zahlen, können öffentliche und oft unverschlüsselte Wlan-Hotspots in Hotels, Zügen oder Cafés Abhilfe schaffen. Sie setzen Nutzer aber auch erheblichen Gefahren durch Cyberkriminelle aus, die Daten abfangen oder Schadsoftware einschleusen können. Öffentliche Netzwerke in Zügen, Hotels oder Cafés bergen erhebliche Risiken. Ein Drittel der Opfer von Cyberangriffen erleidet finanziellen Schaden.

VPN zu deinem eigenen Router ?
Nutzung eines VPN (steht für *Virtual Private Network* = virtuelles privates Netzwerk und bezeichnet eine Technologie, die eine *sichere, verschlüsselte Verbindung* zwischen einem Endgerät und dem Internet herstellt) zu deinem eigenen Router („Home-VPN“). Dein Handy oder Laptop baut dann unterwegs einen verschlüsselten Tunnel zu deinem Router zu Hause auf; der Router ist anschließend dein sicherer Ausgangspunkt ins Internet
Vorteil: Du nutzt nicht den VPN-Server eines fremden Anbieters, sondern dein eigenes Zuhause als vertrauenswürdigen Ausgangspunkt

Doch: Die Einrichtung ist für Laien nicht ganz einfach siehe hier >>>

Alternative: das eigene Mobilfunknetz mit dem eigenen Datenvolumen

Situation	Sicherheit	Wann sinnvoll
Eigenes Datenvolumen	Sehr gut, einfacher Standard	Banking, sensible Apps, wenn Datenvolumen reicht. bsi.bund
Hotel-WLAN + VPN zum Heimrouter	Sehr gut, wenn VPN korrekt aktiv ist	Große Downloads, wenn Mobilfunk langsam oder Datenvolumen knapp ist. bsi.bund +1
Hotel-WLAN ohne VPN	Riskant	Nach Möglichkeit vermeiden, besonders für sensible Zugänge. bsi.bund

Ein gut eingerichtetes VPN erhöht zusätzlich die Anonymität im Internet. Die Einrichtung kann für Laien jedoch beschwerlich sein.
Das Datenvolumen des Mobilfunktarifs sollte zum eigenen Bedarf passen. Mehr Datenvolumen ist heute oft günstig zu bekommen.

Kurz: Mobilfunk ist meist die sicherere Alltagswahl; öffentliches WLAN plus VPN zu deinem Heimrouter kann ähnlich sicher sein, erfordert aber korrekte Einrichtung.(bsi.bund)

Was zudem immer zu beachten ist:

- Nutze bevorzugt https://-Websites; das schützt die Verbindung zwischen Router und Website zusätzlich.
- Halte Router-Firmware, Betriebssystem und Browser aktuell.
- Verwende ein langes, einzigartiges WLAN-Passwort; WPA2/WPA3 ist der sinnvolle Standard.
- Deaktiviere unnötige Routerdienste und den allgemeinen Fernzugriff; das reduziert Angriffsflächen.
- Richte ein separates Gast-WLAN für Besucher und unsichere Geräte ein