

Vorsicht im Urlaub: 90 % der Handynutzer gefährden ihre Daten!

Urlaubszeit steht vor der Tür! Tipps zur sicheren Nutzung von WLAN im Ausland und zur Vermeidung von Datenschutzrisiken.



Deutschland - Mit dem anhaltenden Ansturm auf die Urlaubssaison, die sich ihrem Höhepunkt zuneigt, stehen viele Reisende vor der Herausforderung, ihre digitalen Geräte sicher zu nutzen. Laut einer aktuellen Umfrage von YouGov im Auftrag von Kaspersky sind 90 Prozent der Handy-Nutzer gefährdet, während 15 Prozent sogar ohne jegliche Schutzmaßnahmen auf öffentliches WLAN zugreifen. Diese Zahlen verdeutlichen die Risiken, die mit der Nutzung von ungesicherten Netzwerken verbunden sind, insbesondere in Ländern, in denen man auch auf das Hotel-WLAN angewiesen ist.

Öffentliches WLAN ist populär, doch es birgt erhebliche Gefahren. Diese ungesicherten Netzwerke sind oft nicht nur in

Deutschland, sondern weltweit verbreitet. 28 Prozent der Befragten geben an, dass sie vermeiden, Passwörter oder Bankdaten in unsicheren Netzwerken einzugeben. Trotzdem nutzen 12 Prozent persönliche WLAN-Hotspots durch Tethering, um ihre Verbindungen abzusichern. Nur rund 10 Prozent setzen auf VPN-Dienste, um ihren Datenverkehr zu schützen. Allerdings sollten Reisende darauf achten, dass nicht alle VPN-Anbieter zuverlässig sind, da einige ebenfalls Daten gefährden können.

Risiken durch ungesicherte Netzwerke

Die Gefahren im Zusammenhang mit unverschlüsselten öffentlichen WLAN-Hotspots sind gravierend. Angreifer können Schadsoftware einschleusen und Benutzer ausspionieren. Daher ist es besonders wichtig, nicht nur einen VPN-Client zu nutzen, sondern auch auf verschlüsselte Internetseiten zu achten. Diese sind an `https://` in der Adresse erkennbar, wobei ein grünes Symbol oder ein Vorhängeschloss oft einen Hinweis auf die Sicherheit der Seite gibt. Dennoch garantiert selbst ein `https://` nicht die Seriosität der Webseite.

Die Verbraucherzentrale rät, die Datei- oder Verzeichnisfreigabe zu deaktivieren, um ungewollten Zugriff auf persönliche Dateien zu verhindern. Ein weiteres Sicherheitsrisiko stellen gefälschte WLAN-Netzwerke dar, mit denen Kriminelle ahnungslose Nutzer in präparierte Netzwerke locken können. Um sich davor zu schützen, ist es ratsam, gespeicherte Netzwerke regelmäßig zu löschen, um nicht ungewollt mit solchen Fake-Netzen verbunden zu werden.

Maßnahmen zur Sicherung der Daten

Um sich im öffentlichen WLAN sicherer zu fühlen, sollten Nutzer einige Vorsichtsmaßnahmen treffen. Zu den Empfehlungen gehört die Nutzung eines VPN-Tunnels, der den Datenaustausch zwischen dem Endgerät und dem Router verschlüsselt. Dazu gibt es verschiedene Programme oder Apps von Anbietern, und versierte Nutzer können sogar einen eigenen VPN-Server

einrichten.

Die Nutzung öffentlicher WLAN-Netzwerke ist in vielen Ländern unvermeidlich, insbesondere für Reisende. Es ist jedoch wichtig, sich über die potenziellen Risiken zu informieren und geeignete Maßnahmen zu ergreifen, um die eigene digitale Sicherheit zu gewährleisten. Für weitere Informationen zu diesem Thema bieten **Inside Digital** und **Verbraucherzentrale** umfassende Ressourcen an.

Details	
Ort	Deutschland
Quellen	• www.inside-digital.de • www.verbraucherzentrale.de

Besuchen Sie uns auf: eine-reise.de