WLAN im Hotel: So surfen Urlauber sicher

VERBRAUCHERINFORMATION IT-Experten informieren, wie Urlauber ihre Daten auf Reisen schützen

IM NORDWESTEN/ARAG – Fast 44 Prozent der Deutschen nutzen im Urlaub häufig öffentliche WLAN-Netze. Auch Hotels bieten ihren Gästen fast immer einen WLAN-Zugang an, meistens kostenlos. Doch genau dieser Service kann zur Sicherheitslücke werden. Die ARAG IT-Experten informieren, was Urlauber beachten sollten, damit sie auch im Hotel-WLAN sicher surfen.



Auch im Hotel-WLAN sollten Urlauber auf den Schutz ihrer persönlichen Daten achten und einige wichtige Sicherheitsvorkehrungen treffen. BILD: PEXELS

Warum Hotel-WLANs ein Einfallstor für Angriffe sein können

Ein Passwort für das Hotel-WLAN vermittelt zunächst ein Gefühl von Sicherheit. Tatsächlich ist diese Hürde laut IT-Experten jedoch oft gering: Zugangsdaten sind leicht zu erfragen oder werden an viele Gäste gleichzeitig vergeben. Hinzu kommt, dass Kriminelle gezielt sogenannte „WLAN-Zwillinge“ einrichten. Diese Netzwerke tragen täuschend echte Namen wie „Hotel Free WiFi“ und verleiten Gäste dazu, sich unbemerkt mit einem fremden Zugang zu verbinden.

Die Folge: Daten werden unter Umständen unverschlüsselt übertragen und können abgefangen werden. Besonders kritisch wird es, wenn persönliche Informationen wie Passwörter, Fotos oder Zahlungsdaten betroffen sind. Zudem besteht die Gefahr, dass Schadsoftware auf das Gerät gelangt und später, sobald man zu Hause wieder das heimische WLAN nutzt, weitere Systeme infiziert.

Sensible Daten besser nicht im Hotelnetz eingeben

Gerade bei Tätigkeiten wie Online-Banking oder Einkäufen im Internet ist Vorsicht geboten. In offenen oder schlecht gesicherten Netzwerken können Angreifer vergleichsweise leicht auf übertragene Daten zugreifen. Deshalb empfehlen die IT-Experten, für solche Anwendungen auf das mobile Datennetz zurückzugreifen, auch wenn dadurch eigenes Datenvolumen verbraucht wird. Wer dennoch lieber das Hotel-WLAN nutzt, sollte darauf achten, dass die aufgerufenen Seiten verschlüsselt sind. Erkennbar ist dies an „https“ in der Adresszeile des Browsers. Das ersetzt jedoch keine umfassende Sicherheitsstrategie, sondern ist nur ein zusätzlicher Schutz.

Mit einfachen Einstellungen das Risiko deutlich senken

Schon vor Reiseantritt lassen sich wichtige Vorkehrungen für ein sicheres Surfen treffen. Wer seine Betriebssysteme und Apps stets aktualisiert, schließt bekannte Sicherheitslücken und erschwert Angriffe. Ebenso sinnvoll ist es laut ARAG IT-Experten, die automatische Verbindung zu bekannten Netzwerken zu deaktivieren. So wird verhindert, dass sich das Gerät unbemerkt mit einem unsicheren WLAN verbindet.

Die automatische Verbindung zu bekannten WLAN-Netzen lässt sich direkt in den Geräteeinstellungen ausschalten: Auf dem Smartphone (Android oder iOS) öffnet man die WLAN-Einstellungen und deaktiviert die Option „Automatisch verbinden“ oder entfernt gespeicherte Netzwerke, bei denen sich das Gerät nicht mehr selbstständig einwählen soll. Bei vielen Geräten gibt es zusätzlich eine Funktion wie „Automatisch Hotspots beitreten“, die ebenfalls ausgeschaltet werden kann.

Am Laptop (Windows oder macOS) wählt man in den WLAN-Einstellungen das jeweilige Netzwerk aus und entfernt den Haken bei „Automatisch verbinden“ oder löscht das Netzwerk komplett aus der Liste der bekannten Verbindungen.

Nach der Nutzung raten die IT-Experten, die Verbindung zum Hotelnetz aktiv zu trennen. Andernfalls könnten Apps im Hintergrund weiterhin Daten übertragen, ohne dass Nutzer dies bemerken. Auch das bewusste Auswählen des richtigen Netzwerks, beispielsweise durch einen Abgleich mit den offiziellen Angaben des Hotels, hilft, Fehlverbindungen zu vermeiden.

Zusätzlicher Schutz durch verschlüsselte Verbindungen

Wer auch unterwegs nicht auf sensible Online-Dienste verzichten möchte, dem raten die ARAG IT-Experten, auf ein sogenanntes VPN (virtual private network) zurückzugreifen. Ein virtuelles privates Netzwerk verschlüsselt den gesamten Datenverkehr und leitet ihn durch einen geschützten Tunnel. Dadurch wird es für Dritte deutlich schwieriger, Daten mitzulesen oder abzufangen. Für Privatanwender gibt es zahlreiche VPN-Angebote, die sich einfach installieren lassen. Kostenpflichtige Dienste bieten in der Regel mehr Stabilität und Datenschutz als kostenlose Varianten, die häufig Einschränkungen beim Datenvolumen oder zusätzliche Werbung mit sich bringen.



