Wo Ihre Cybersicherheit unterwegs besonders angreifbar ist

Checkliste - im Urlaub

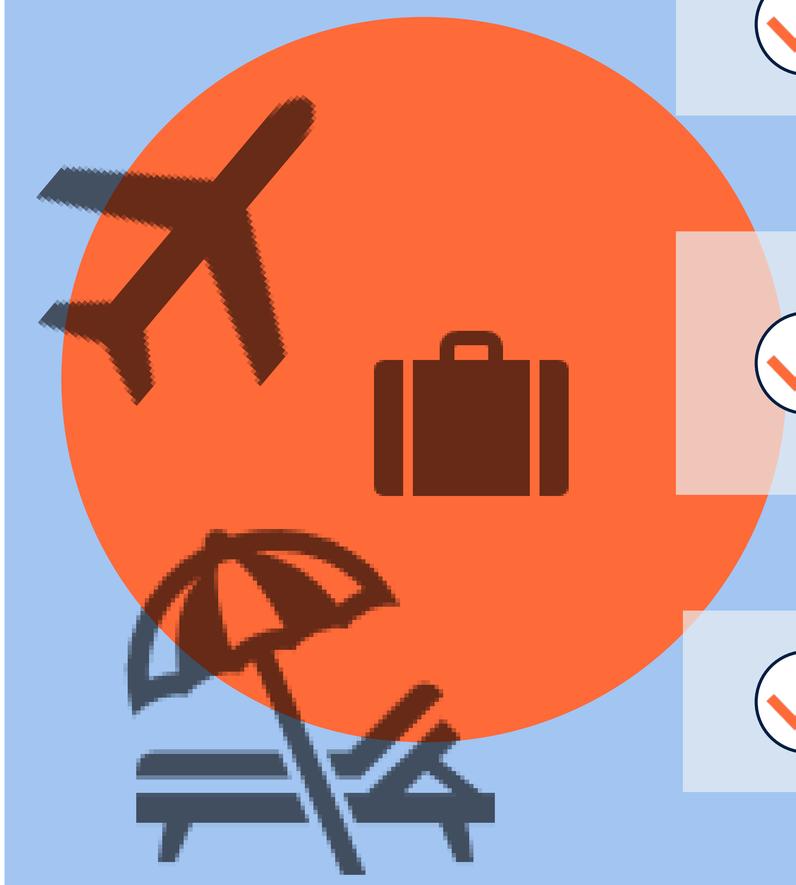
- Nutzen Sie für Ihren **Internetzugang** möglichst das **Mobilfunknetz**, indem Sie Ihr **Smartphone** als **WLAN-Hotspot** für Ihren Laptop verwenden. Diese Verbindung ist oft sicherer als das angebotene WLAN.

- Achten Sie bei der **Nutzung öffentlicher WLAN-Angebote** z. B. von Flughäfen, Bahnhöfen, Cafés und Hotellobbys penibel auf den **korrekten, legitimen WLAN-Zugang**. Denn eine häufige Taktik von Cyberkriminellen ist, als “Man in the middle” vermeintliche WLAN-Hotspots einzurichten, um Daten auszuspähen.

- Lassen Sie daher auch **keine automatische Verbindung mit offenen Netzwerken** zu.

- Nutzen Sie bei allen WLAN-Verbindungen unterwegs **VPN-Software**. Dadurch kann der Datenverkehr nicht so einfach eingesehen werden.

- Melden Sie sich möglichst nur bei **Benutzerkonten** an, bei denen Sie eine **2- bzw. Multi-Faktor-Authentifizierung** verwenden.



- Nutzen Sie **keine öffentlichen Rechner**, um Ihre E-Mails abzurufen, Social-Media-Konten zu checken usw. Denn diese Rechner sind für Cyberkriminelle besonders attraktiv, um die Zugangsdaten vieler Gäste auszuspähen und werden daher gerne mit Malware infiziert.

- Aktivieren Sie **Schnittstellen** wie **Bluetooth** nur wenn und solange Sie diese nutzen.

- Bedenken Sie, dass **öffentlich gepostete Urlaubsbilder** z. B. auf Facebook Kriminellen verraten können, dass Sie nicht zu Hause sind. **Teilen** Sie aktuelle Bilder daher nur im sorgsam **ausgewählten Kreis.**