Wo Ihre Cybersicherheit unterwegs besonders angreifbar ist

Checkliste - vor dem Urlaub

- Bringen Sie **alle Geräte**, die Sie mitnehmen möchten, **per Updates auf den aktuellsten Stand**. Das gilt für die **Betriebssysteme, Programme und Apps**. Aktivieren Sie automatische Updates, um diesen Zustand auch unterwegs zu erhalten.

- Richten Sie auf allen Geräten eine **Zugangssperre per Passwort, PIN, Fingerabdruck** o. ä. ein.

- Erstellen Sie von allen Geräten **Backups**, die Sie zu Hause sicher verwahren. Als Tipp: befolgen Sie die 3-2-1-Backup-Regel.

- Richten Sie für sensible Konten eine **2- bzw. Multi-Faktor-Authentifizierung** ein. Zum Beispiel für E-Mail-Konten, Social Media Konten etc. Achten Sie darauf, dass Sie sich bei **jeder Anmeldung authentifizieren** müssen, anstatt Optionen wie „Diesem Gerät vertrauen“ zu aktivieren.

- **Optimieren Sie die Passwörter** aller Nutzungskonten, auf die Sie unterwegs vielleicht zugreifen werden. Verwenden Sie für jedes Konto ein **sicheres, einzigartiges Passwort.**

- Wenn möglich, **löschen Sie arbeitsbezogene Daten** von den Geräten. Alternativ **verschlüsseln** Sie diese. Verschlüsseln Sie auch wichtige digitale Unterlagen wie z. B. Flugtickets oder Scans Ihres Impfpasses. Eine Anleitung für die Betriebssysteme Microsoft Windows und Mac OS X finden Sie z. B. beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

- **Installieren und testen Sie eine VPN-Software**, die Sie im Urlaub für alle WLAN-Verbindungen nutzen können. Mehrere von Perseus empfohlene Anbieter bieten kostenlose Versionen oder 1-monatige Nutzungszeiträume an – perfekt für den Urlaub.

- Falls Sie es noch nicht wissen, finden Sie heraus, wie Sie Ihr Smartphone als **WLAN-Hotspot** für Ihren Laptop nutzen können.

- Wenn sich besonders sensible Daten auf Ihren Geräten befinden oder sie auf Nummer Sicher gehen möchten: Richten Sie die **Möglichkeit zur Fernlöschung Ihrer Geräte** ein.