**Merkblatt: Regeln für Mitarbeitende auf Geschäftsreisen**

## Geräte sperren

Die meisten Smartphones, Laptops und Tablets sind mit Sicherheitseinstellungen ausgestattet, die es ermöglichen, das Gerät mit einer PIN-Nummer oder einer Fingerabdruck-ID zu sperren. Zudem kann man eine Funktion aktivieren, die das Gerät nach einer bestimmten Zeit der Inaktivität automatisch sperrt – das ist wichtig. So müssen die Geräte für die nächste Benutzung zuerst entsperrt werden.

→ Weisen Sie Ihre Angestellten an, diese Funktionen bei jedem ihrer Geräte zu aktivieren. Sind Mitarbeitende auf Reisen, sollen sie zudem die PIN-Nummern, die sie regelmässig verwenden, ändern.

## Vorsicht bei öffentlichem Wi-Fi

Freier Wi-Fi-Zugang kann für Geschäftsreisende sehr attraktiv sein, ist aber auch besonders anfällig für Sicherheitsprobleme.

→ Angestellte auf Reisen sollen deshalb unverschlüsselte Wi-Fi-Netzwerke meiden. Im Hotel sollen sie nach dem Sicherheitsprotokoll fragen, bevor sie sich mit dem Internet verbinden. Insbesondere WEP und WPA sind risikobehaftet, besser ist [WPA2 oder WPA3](https://www.gryps.ch/ratgeber/it-sicherheit-unternehmen/sicheres-firmen-wlan/#176710).

## Standortfreigabe minimieren

Es kommt oft vor, dass Reisende die Social-Networking-Sites aktualisieren, wenn sie sich an neuen Orten bewegen. Wer jeden seiner Standorte freigibt, macht es einem Kriminellen leicht, festzustellen, dass er beispielsweise nicht im Hotelzimmer ist.

→ Weisen Sie Ihre Mitarbeitenden an, unterwegs Standortangaben auf ein Minimum zu beschränken.

## Virenschutz installieren

Dies ist eine der einfachsten und effektivsten Methoden, mit denen Geräte abgesichert werden können.

→ Achten Sie darauf, dass Ihre Angestellten keine ungeschützten Geräte nutzen – egal ob im Büro oder auf Reisen.

## Betriebssysteme aktualisieren

Genau wie die Antivirensoftware müssen auch die Betriebssysteme so aktuell wie möglich sein.

→ Achten Sie darauf, dass die Betriebssysteme auf Firmengeräten regelmässig aktualisiert werden. Dies gilt auch für Apps auf dem Smartphone, die Ihre Angestellten regelmässig nutzen.

## Passwörter aktualisieren

Passwörter sind unterwegs besonders angreifbar. Geschäftspasswörter sollten deshalb nicht auf Reisen gehen.

→ Vor einer Reise sollen Mitarbeitende alle Passwörter ändern, die sie regelmässig verwenden.

## Bluetooth-Konnektivität aktualisieren

Genau wie die automatische Wi-Fi-Konnektivität eines Smartphones, Tablets oder Laptops kann auch die Bluetooth-Konnektivität Probleme bereiten. Bluetooth-Signale können von überall her kommen. Bleibt Bluetooth eingeschaltet, können Angreifer in der Nähe eine Verbindung zum Gerät herstellen und sich möglicherweise in das Gerät einhacken.

→ Ihre Angestellten sollen Bluetooth so weit wie möglich deaktiviert lassen, wenn sie unterwegs sind.

Quelle: Norton.com