OSAC

TRAVELING ABROAD WITH MOBILE DEVICES

Best Practices for the Private Sector

Overseas Security Advisory Council | www.OSAC.gov

Mobile phones and other personal communication devices transmit and store a variety of sensitive information. This makes them a valuable target for adversaries who seek to intercept communications or plant malware. Many features of mobile devices that enable essential capabilities and convenience during travel abroad may also present security risks, making devices more susceptible to intrusion. Travelers should take increased precautions to protect both personal and business mobile devices during travel abroad, especially when traveling to specific high-risk locations like Russia and China. Travelers should also take advantage of related travel resources provided by their organization, such as loaned travel devices or pre- and post-travel device analysis to detect malware.

BEST PRACTICES FOR TRAVEL

BEFORE

Update all software and apps, backup all important data, and delete sensitive information. Enable security features like PINs, biometrics, and timeouts. Leave all nonessential devices behind.

DURING

Do not connect to unknown devices (e.g. charging stations) or networks, terminate Wi-Fi connections immediately after use, and do not click any suspicious links or download apps.

AFTER

Avoid immediately reconnecting devices to personal or business networks. Consider wiping and reloading devices, changing passwords, updating security software, and/or scanning for malware.*

OTHER SECURITY PRECAUTIONS

Physical Control

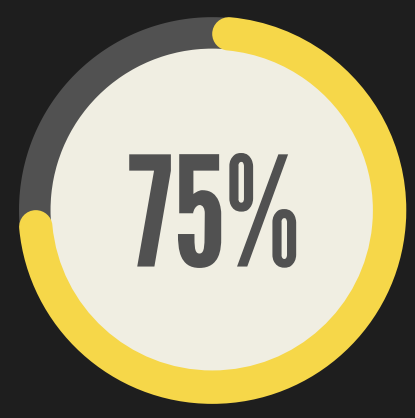
Always maintain physical control of your devices and accessories (e.g. charging tools). Do not leave them in checked baggage or hotel safes.

Encryption

Use a Virtual Private Network (VPN) from a reliable vendor, as well as an encrypted messaging app for mobile communications.

Wireless Features

Avoid using public Wi-Fi networks, and disable all unused wireless features, like Wi-Fi, Bluetooth, near-field communication, and GPS, when not in use.



In a recent OSAC survey, 75% of respondents noted that their organization provides guidance on best practices for traveling overseas with mobile devices. Find it, and apply it!

* Malware scanning tools do not exist for many popular devices, such as iPhones or iPads.