Mobile Device Best Practices When Traveling OCONUS

In their brief history, mobile devices have evolved to become the critical link between a remote user and the home office, providing travelers with access to business applications and data they would otherwise lack. Ensuring that this line of communication is private and secure is imperative. The security guidance outlined below applies to U.S. Government personnel using Government-issued commercial mobile devices in a public network as they travel in foreign countries. The purpose is to minimize an adversary's ability to obtain sensitive data through mobile devices and limit damage should one be compromised. The mitigations address a range of threats that might be encountered in foreign countries.

Mobile devices have inherent vulnerabilities associated with their software and hardware. Foreign countries often leverage their security apparatus, especially airport security and customs, and connections to the tourism industry, to conduct physical attacks on mobile devices. Also, in many foreign countries the government has direct or proxy control of the commercial cellular infrastructure, which gives them a remote conduit to attack connected mobile devices. Cellular borne attacks are particularly damaging, as most mobile devices, as designed, trust the low level communication from the cellular network.

Successful exploitation can allow adversaries to remotely activate microphones and cameras, geolocate and track specific devices, and steal the information processed by or stored on the device. A compromised device can also be used as a vector to attack networks to which it later connects. High profile U.S. Government personnel are top targets and should not carry or employ any commercial mobile devices in high threat environments.

For those personnel that must carry and use unclassified official government-issued, commercial mobile devices when traveling OCONUS, certain countermeasures can be employed to mitigate some of the vulnerabilities. These recommendations are based on current DoD guidance and known security risks.

General Risk Mitigations

- Keep all software (operating systems and apps) up-to-date.
- Use strong lock-screen pins/passwords (minimum 6 character length).
- Set displays to automatically lock after 5 minutes or less.
- Set password attempts to 10 or less.
- Disable lock-screen notifications.
- Encrypt data stored on devices.
- Use a VPN and encrypted VoIP applications whenever possible. Ensure that all VPN/VoIP providers are reputable and US-based.
- Connect devices only to authorized computers and peripherals.
- Cover all cameras with opaque tape and disable in settings whenever possible.
- Install applications only from trusted sources.
- Do **not** charge your devices by connecting them to charging stations, computers, televisions, DVRs, etc. Use only issued chargers or those acquired with sufficient OPSEC.
- Do **not** open any unknown email attachments.
- Do **not** click on any unknown web links sent via email or text messaging.
- Do **not** circumvent restrictions on government issued devices.
- Report suspicious device behavior to your IT department as soon as possible.

Pre-Travel Guidance

- Prepare dedicated devices with limited contacts and emails for the exclusive purpose of your imminent travel.
- Acquire and install new SIM cards for the destination service area. Using international SIM cards purchased domestically is preferable; however, if this is not possible, make sure to utilize good OPSEC by purchasing SIM cards from standalone stores and not from a store or kiosk at the airport.

On-Travel Guidance

- Maintain positive physical control of devices at all times (Do not leave in hotel safe).
- Turn off unused wireless communications (e.g., Bluetooth®[1], NFC, Wi-Fi).
- Disable GPS and location services (unless required).
- Do **not** connect to open Wi-Fi networks.
- Do **not** connect personal devices with official devices.
- Regularly inspect devices for signs of tampering.
- Avoid logging into USG networks unless absolutely necessary.
- Avoid surrendering devices to Foreign Customs Officials.

Post-Travel Guidance

- Physically inspect your travel devices.
- Wipe and reload your travel devices.

Contact Information
Client Requirements or General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov

[1] Bluetooth is a registered trademark of Bluetooth SIG, Inc.