Can You Hear Me Now?
OSAC's Guide for Mobile Device Usage Overseas

Date Published: December 18, 2024

Summary

Mobile phones are a critical part of conducting business, and during overseas travel they simply cannot be left at home. Nonetheless, traveling abroad with a mobile phone, especially to countries with high levels of theft or strict speech laws, carries significant risk. Mobile phones are a valuable target for adversaries, both monetarily and informationally. This report examines the precautions travelers should take before and during travel to ensure their devices are not stolen or maliciously accessed.

Preparing for Travel

Before travelling abroad, research whether domestic SIM cards can be utilized, or if your cell-carrier may be able to provide a temporary international plan. Crime rates, speech laws, and customs should also be consulted before traveling. In countries that pose a high risk for corporate espionage, it may be safer and easier to simply travel with a "clean" or "dry" phone, a device that has no connection to personal or business accounts. When traveling to high-crime locales ensure that tracking features are enabled, and that critical information or financial records are not accessible. Even when traveling to low-crime or low-risk countries, phones are an easy target for petty crime.

In-Country Risks and Mitigation

Device usage in-country will vary greatly depending on the location, but there are some common issues that private-sector travelers experience abroad.

- **Theft:** Avoid using your phone in heavily congested or busy areas, as phone-snatching is a growing avenue of petty theft across the globe. Call for ridesharing/taxis before venturing outdoors, and do not take calls in public without using headphones. Store phones in front pockets or in closable bags. Use phones with passcodes when available to decrease the impact of a stolen device. If a phone is stolen, contact local law enforcement; do not try to follow or fight thieves. Find a safe location to report the loss to relevant parties (corporate IT, financial institutions, colleagues, etc.)

- **Data Security:** Use biometric locks or passwords when possible. Do not connect to unfamiliar wi-fi networks, do not conduct sensitive personal or professional business on public networks, and use a company-sponsored VPN when possible. In addition, do not access sensitive personal or professional business data while in public, when possible, to avoid physical breaches like "screen peaking". It is also good practice to clear device

caches before and after overseas use, and not to plug in devices to any public charging stations; this includes free wall-outlet chargers, as well as standard USB or USB-C cables. Do not accept or click on documents or links from unknown sources.

- **Financial Systems:** It is generally recommended that travelers not access banking systems on phones while traveling abroad. In addition, many countries lack the financial infrastructure to accept phone-based payments, so travel with physical alternatives (credit cards or cash). Consider changing passwords after accessing financial accounts abroad.

- **Social Media and Communications Platforms:** To mitigate the risk of targeted theft, avoid posting your specific locations or destinations on social media until no longer in-country. Some countries, specifically those with strict speech laws, necessitate further self-regulation when using devices. In these countries, refrain from posting, texting, or emailing pornographic material, or commentary that could be construed as political in nature. It may be advised to completely wipe social media accounts of past posts of this nature, and sometimes using "clean" or "dry" phones may be appropriate. In very limited cases, if a traveler has posted commentary that could be considered political, they may face social or legal consequences even if posts have been deleted.

Other Security Precautions

In a 2020 OSAC Benchmarking Survey, over 75% of OSAC member organizations reported having company-wide best practices for employee mobile device usage; always abide by company policies. In addition, ensure that company policies are accurate and timely, as cyber-threats are constantly shifting, and usage regulations change rapidly in some countries. When planning travel to a high-risk location, reach out to local contacts, company security teams, and OSAC regional analysts for more specific best practices.

While using a mobile phone is often critical to perform work functions, when in doubt, leave it out. Deciding to bring a cheaper, temporary mobile device may be a more suitable alternative to bringing a personal or business smartphone and can mitigate the risk of being impacted by petty theft or local speech restrictions.

Additional Information

For more information on this topic, please contact OSAC's regional teams.

- Office of the Director of National Intelligence: Travel Tips (Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices)