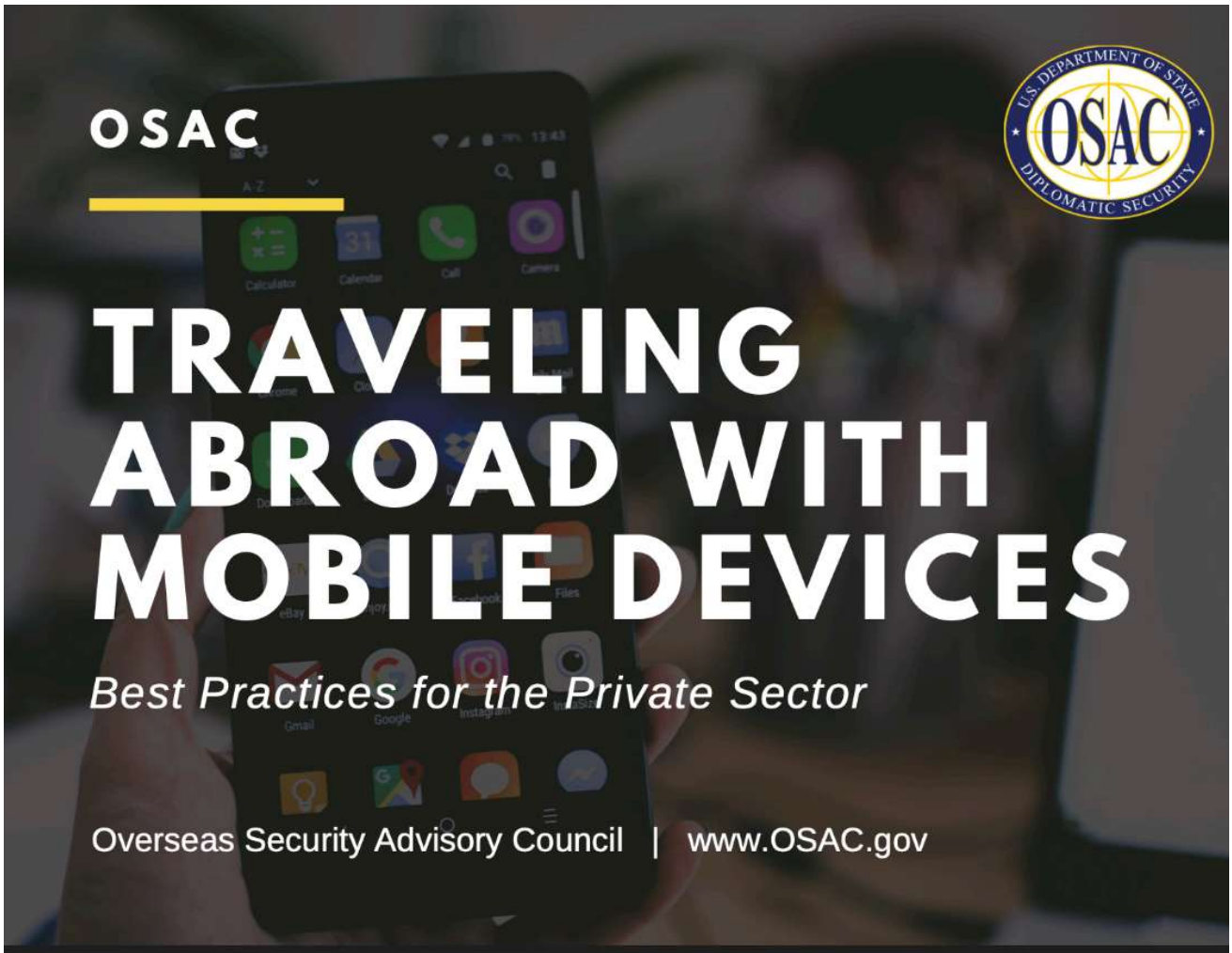
OSAC
Bureau of Diplomatic Security
U.S. Department of State

Average Rating

9/15/2020 | OSAC Analysis

978 all time - 21 last 7 days ★ 4.00 Average rating

# Traveling Abroad with Mobile Devices: Best Practices for the Private Sector



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

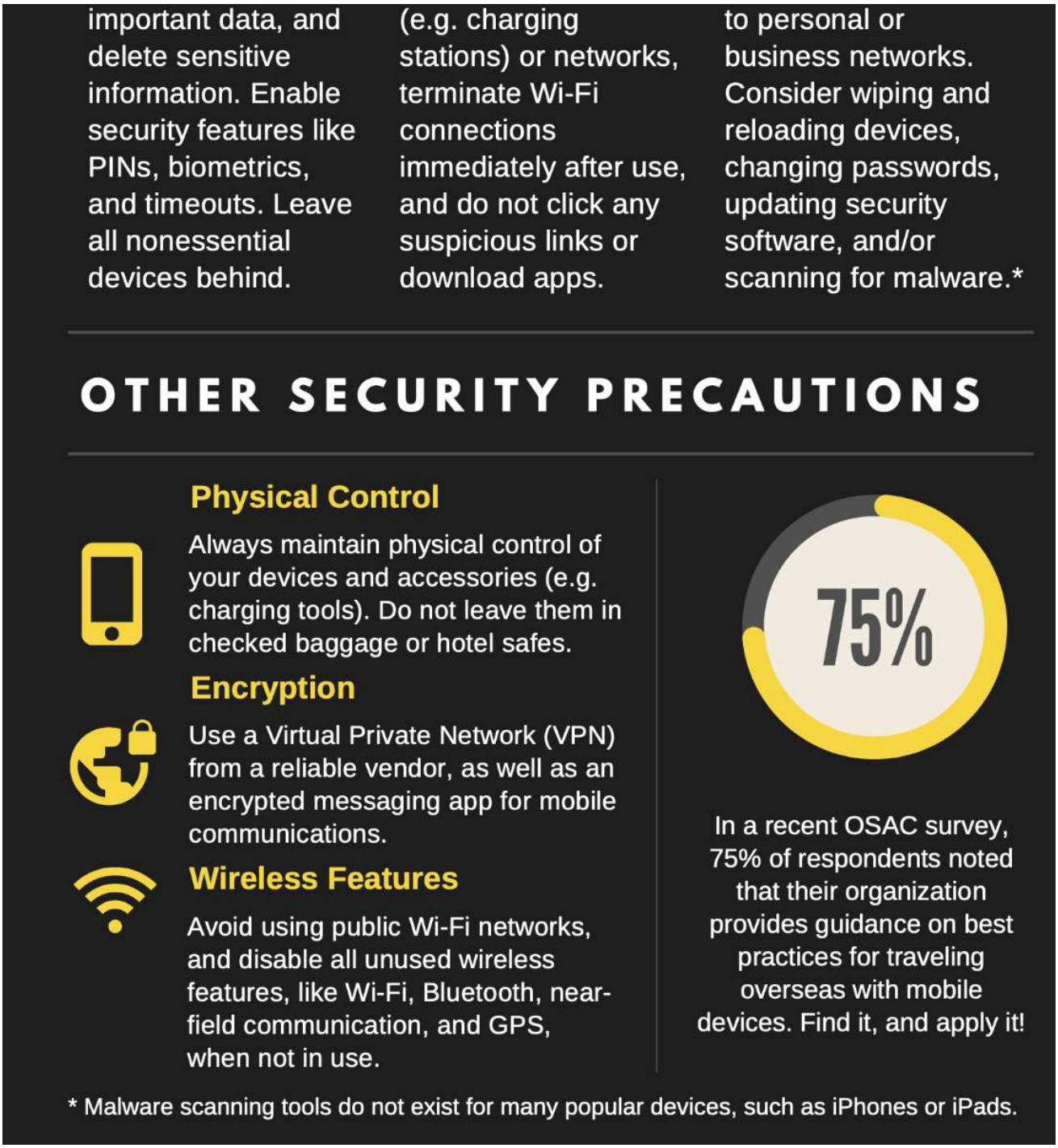
Update all software and apps, backup all

### DURING

Do not connect to unknown devices

### AFTER

Avoid immediately reconnecting devices




**Attachments**

OSAC - Traveling Abroad with Mobile Devices Infographic.pdf

**Related Content**

Traveling Abroad with Mobile Devices: A Comparison of OSAC Benchmarking Results from 2015 and 2020
9/11/2020 | Report

Traveling with Mobile Devices: Trends & Best Practices
2/15/2019 | Report

*purposes only. Publishing or otherwise distributing OSAC-derived information in a manner inconsistent with this policy may result in the discontinuation of OSAC support.*