REN-ISAC

Effective Practices: International Security for the IT Support Professional

TLP: WHITE

For those traveling internationally for work, research, or vacation, protecting personal and institutional data and mobile devices is critical. Individuals face a variety of threats when traveling, and best practices start long before boarding the plane. IT and cybersecurity specialists, please use this checklist to prepare your faculty, staff, and students—and their technology—for the unique threats of global travel.

Before They Leave

Support

- ☐ Provide cybersecurity awareness training for the following:
  - Understanding institutional data policies.
  - Connecting safely to institutional data while traveling.
  - Clearing Internet browser by deleting history files, caches, cookies and temporary files.
  - Turning encryption on and off.
  - Recovering from encryption lockouts.
  - Performing virus/malware scans.
  - Using remote wipe capabilities.
  - Reporting lost or stolen devices.
  - Preparing for possible situations where a multi-factor authentication device is unavailable (failure, data plan restrictions) or is confiscated.
- ☐ Make sure user knows their administrative password and how to perform an administrative password reset if necessary.
- ☐ Help travelers understand data protection laws of countries and regions on their itinerary. [1]
- ☐ Encourage travelers to leave personally owned or personal business provided devices at home and use loaner laptops when possible.
- ☐ Ensure the traveler is familiar with their chosen device before leaving, including how to disable wireless, Bluetooth, and GPS access when not in use.
- ☐ Encourage frequent global travelers to set up a dedicated email account with a separate password to use while traveling.
- ☐ Provide information on cell phone coverage and international data plans.
- ☐ Schedule a post-trip consultation with traveler.

[1] https://travelmaps.state.gov/TSGMap; https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/; https://travel.gc.ca/travelling; https://www.gov.uk/foreign-travel-advice; https://www.safetravel.govt.nz

Equipment

- ☐ Prepare a stock of encrypted, sanitized, stripped-down loaner laptops.
- ☐ Ensure the device has the latest operating system (OS) and application updates.
- ☐ Install updated protections for antivirus, spyware, security patches, and firewalls.
- ☐ Set up data protection programs for automated scanning and filtering.
- ☐ Set up VPN or viable alternative on travelling devices.
- ☐ Add bookmarks or short cuts to travelling devices for pertinent regional travel alerts, contact information for consulates and embassies, and easy access to emergency resources including 24-hour IT professional or Help Desk contact information.
- ☐ Provide back-up token or off-line one-time use codes for multi-factor authentication on traveling devices.
- ☐ Set up all portable devices with full disk encryption if permitted by destination countries.
- ☐ Enable mobile device lock, recovery, and remote-wiping features.
- ☐ Back up all non-essential data on institutionally approved and managed systems; options may include cloud-based storage systems, back-up storage devices, and printed copies.
- ☐ Remove all non-essential data from the device.

While They Are Gone

Support

- ☐ Provide support for traveler as needed.
- ☐ Monitor unusual behavior on accounts and systems during travel.

Upon Their Return

Support

- ☐ Host post-travel consultation with traveler to scan for unusual circumstances and reestablish normal systems and safeguards.
- ☐ Query traveler whether the device and systems showed signs of suspicious activity, review any such activity.
- ☐ Ask traveler what worked/didn't work to better future staff preparation and service.

Equipment

- ☐ Check system logs for suspicious activity and investigate/respond as necessary.
- ☐ Delete any unauthorized and unnecessary applications.
- ☐ Change passwords on devices and accounts used during travel.
- ☐ Clear Internet browser by deleting history files, caches, cookies and temporary files.
- ☐ Ensure encryption is enabled.
- ☐ Perform virus and malware scanning.
- ☐ Ensure network access works correctly.
- ☐ Wipe, re-image, or dispose of loaned devices upon return.

Additional Resources and Sources

Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices—The National Counterintelligence and Security Center

Prepare Your Laptop for Traveling—Brown University

Travel Safety and Securing Technology—Indiana University

Securing Mobile Devices When Traveling—Indiana University

The Traveler's Guide to Cybersecurity—Syracuse University

Recommendations for Travelers to High Risk Countries—Stanford University

The Motherboard Guide to Not Getting Hacked

Safety and Security for the Business Professional Traveling Abroad—Federal Bureau of Investigation

REN-ISAC Discussion email list

Global Resilience Federation: Best Practices for Corporate Foreign Travel GRF Report #6, August 2018