

4.5 Travel Guide

Core Concepts: All Four

Travel introduces unique risks. Prepare before you go and stay vigilant while away.

4.5.1. Before You Leave

- **Back Up Everything:** Full backup, test restore (see Backups topic)
- **Enable and Test Find My Device:** Verify location tracking works (see Mobile Device Hardening and OS Hardening topics)
- **Update All Devices:** OS, apps, firmware (see OS Hardening and Mobile Device Hardening topics)
- **Know How to Remotely Wipe:** Review the process (see Mobile Device Hardening topic)
- **Install and Test VPN:** Essential for public WiFi (see VPN topic)
- **Enable Strong Lock Screens:** Not just biometrics (see Authentication and Mobile Device Hardening topics)
- **Pack Cable Locks:** Physical security essentials (see Physical Security topic)
- **Use RFID Blocking Sleeves:** for credit cards and passport
- **Create Emergency Contacts List:** Nearest embassy if international, bank fraud numbers; print and store in luggage

4.5.2. During Travel

- **Use VPN on All Public WiFi:** Hotels, airports, cafes (see VPN topic)
- **Don't Use Public USB Charging:** Use AC outlets with your charger (see Physical Security topic)
- **Keep Devices With You:** Never in checked luggage (see Physical Security topic)
- **Lock Screen Every Time:** Even for a moment (see Physical Security topic)
- **Disable Auto-Connect WiFi and Bluetooth:** Prevent automatic connections to malicious networks (see Mobile Device Hardening topic)
- **Be Aware of Shoulder Surfers:** Shield screen and keyboard (see Physical Security topic)
- **Don't Use Hotel Business Center Computers For Sensitive Tasks**

4.5.3. At Border Crossings

- **Power Off Devices Before Crossing:** Cold boot required to access encrypted storage (see OS Hardening topic)
- **Consider Disabling Biometrics Temporarily:** Can be compelled to use (see Authentication topic)
- **Know Your Rights:** Varies by country, research in advance

Plan for Border Crossings

International border agents can legally search devices in many countries.

Standard precautions:

- Turn off devices before border crossing (cold boot required to access encrypted drives)
- Log out of all services and set back up after crossing
- Uninstall social media apps, delete potentially sensitive text messages
- Clear your browser's cache
- Consider changing important passwords after crossing if device was searched
- Don't volunteer passwords or unlock devices unless legally required

High-security approach:

- Travel with a "clean" device containing minimal data
- Access sensitive data through cloud services after crossing the border
- Use a burner phone for international travel
- Wipe device before travel, restore from backup after arrival

Revision #1

Created 2026-07-12 21:56:46 UTC by Chris Landis

Updated 2026-07-12 21:58:18 UTC by Chris Landis