

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. Faculty, staff, students, and other travelers, please use this checklist to prepare yourselves — and your technology—for the unique threats of global travel.

## Before You Leave

### Physical Security

- Be aware of national data protection laws in your home and destination countries.
- Know and follow policies for using various devices, institutional data, and institutional resources.
- Research personal, criminal, and cyber risks in the country or region you're visiting.
- Purchase and pack privacy screen filters, portable chargers, and country specific plug adapters.
- Be aware that border and/or customs officials may search your devices multiple times and copy data therein.
- Understand that legally confiscated electronic devices may not be returned for months.

### Technical Security

- Consult with your IT support professional about special concerns regarding your technology or your destinations.
- See if low-cost, loaner devices are available to mitigate the risk of losing more valuable equipment.
- Ensure your devices have full disk encryption when available and local encryption when not.
- Make sure your antivirus program is updated and performing regular scans.
- Check your cell phone coverage and international data plan options.
- Enable your institution's VPN access. Be aware some countries block VPN. Talk to your IT support for alternatives if needed.
- Set up institutionally approved, centrally provisioned data storage.
- Back up all data prior to travel, and take only essential data with you.
- Create complex passwords, PINS, codes, and screen locks for your device.

## While Travelling

### Physical Security

- Keep safe by carrying only necessities, keeping bags zipped, and practicing situational awareness.
- Protect mobile devices by keeping them secure, locked, and hidden from sight when not in use.
- Protect RFID-enabled devices and bank cards with RFID shielded containers.
- Report stolen devices to your native embassy or consulate and other appropriate authorities immediately.
- Protect your data by using privacy screen filters and avoiding public discussions of sensitive data.

### Technical Security

- Be wary of charging stations; use wall outlets with your own chargers or external batteries instead.
- Avoid using courtesy computers in business centers.
- Disable broadcast services like Wi-Fi access points, Bluetooth devices, and GPS when not needed.
- Don't connect to unknown resources like Wi-Fi access points and Bluetooth devices.
- Assume locally provided technology, such as wireless networks, may be vulnerable to attacks or have risky security settings.
- Use VPN access or a viable alternative whenever possible.
- Don't enter sensitive information while connected to wireless hotspots or unsecured networks.
- Use two-factor authentication whenever possible.
- Don't install software updates or patches while away from trusted, secured networks.
- Choose private browsing when accessing websites.
- Clear your internet browser of history, caches, cookies, and temporary files after each use.

## Upon Returning

### Technical Security

- Review banking and credit card statements for unauthorized transactions.
- Scan devices for unusual activities with the help of your IT support professional.
- Provide feedback to your IT support professional on what did and did not work well.
- Reestablish normal systems and safeguards with the help of your IT support professional.
- Resume your weekly or monthly data check and back up routines as normal.

## Additional Resources and Sources

Travel (Linux) Laptop Setup

<https://paranoidbeavers.ca/travel-laptop-setup.html>

Travel Safety and Securing Technology—Indiana University

<https://protect.iu.edu/emergency-planning/personal-preparedness/travel-safety/technology.html>

Securing Mobile Devices When Traveling—Indiana University

<https://protect.iu.edu/online-safety/personal-preparedness/mobile-devices-traveling.html>

The Motherboard Guide to Not Getting Hacked

[https://motherboard.vice.com/en\\_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide](https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide)

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

<https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view>

REN-ISAC Discussion email list

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