Traveling Internationally with Electronic Devices

Cory Crew - 2025-02-13 - Comments (0) - Physical Security

Brown's Office of Information Technology (OIT) recommends community members familiarize themselves with the following information before traveling internationally with electronic devices. Adhering to these basic precautions will reduce risk to both you and the University if your electronic devices are lost, stolen, or altered while traveling.

Before, During, and After Travel

Before

- **Leave Unnecessary Devices:** Only bring essential electronic devices.
- **Update Devices:** Ensure all devices are patched, up-to-date, and using the latest security features.
- **Secure Passwords and Verification:** Use complex passwords for devices and online accounts. Enable Two-Step Verification wherever possible.
- **Back-Up Data:** Back up all critical data before departure.
- **Enable Remote Wiping:** If available, enable remote wiping capabilities in case the device is lost or stolen.
- **Keep Devices Charged:** Ensure devices are fully charged for possible customs inspections.
- **Encrypt Sensitive Data:** Encrypt devices containing sensitive data or personally identifiable information (PII), *unless legally prohibited at your destination.*
- **Consider a Loaner Device:** If deemed appropriate by Export Control personnel with the Office of Research Integrity, consider using a loaner device instead of your personal device.

During

- **Keep Devices With You:** Do not leave devices unattended. If you must leave them behind, ensure they are locked, powered off, and stored in a secure location.
- **Avoid Untrusted Accessories:** Do not use untrusted charging tools or USB drives.
- **Avoid Public Computers:** Do not enter credentials on untrusted or public access computers.

- **Connect to Trusted Networks:** Avoid public Wi-Fi if possible, instead leveraging cell coverage when able.
- **Use a VPN:** Use a reputable VPN for secure connections, if legal in your destination.
- **Disable Unused Connections:** Turn off Wi-Fi and Bluetooth when not in use.
- **Practice Safe Browsing:** Use secure, HTTPS websites and avoid clicking on suspicious links or downloading unknown files.

After

- **Scan Personal Devices:** Scan personal devices with reputable anti-malware software to ensure no viruses were introduced.
- **Update Passwords:** Consider updating passwords for devices and critical accounts used during travel, especially if public Wi-Fi was used.
- **Return Loaner Devices:** Return loaner devices to OIT for wiping and formatting, if applicable.

Travelers should not rely solely on Brown University services and technology for critical updates while abroad. The functionality of these services can vary significantly with the technological and regulatory environment of your destination. As such, it's crucial that you take the initiative to ensure your personal devices are well-prepared. Make sure you can independently access important travel information such as travel documents, State Department travel alerts, digital IDs, etc. Remember to plan ahead and check the availability of these resources before your departure.

When to Request a Loaner Device

The Office of Information Technology has a limited number of encrypted and unencrypted loaner laptops available to approved faculty and staff traveling to countries deemed high-risk by the Office of Research Integrity. Faculty and staff planning international travel should first consult with the Office of Research Integrity to determine if a loaner device is necessary before contacting their respective ITSCs to request one.

Travel advisories for specific countries are subject to frequent updates. If you are concerned about your destination, the U.S. State Department provides an actively updated database of international travel advisories, categorized by a 4-tier rating system:

1. Exercise normal precautions
2. Exercise increased caution
3. Reconsider travel
4. Do not travel

Customs and Border Security

Travelers should be aware that Customs and Border Security staff, both in the U.S. and abroad, often have the right under applicable law to search electronic devices upon entry/exit. In extreme circumstances, content on electronic devices, including social media postings and other online communications, may result in denial of entry.

Export Controls and Electronic Devices in International Travel

It is crucial for academics and researchers to understand the complex regulations that govern the transfer of technology and information, especially when traveling to countries subject to stringent U.S. export controls such as North Korea, Iran, Cuba, and the Russian Federation. Export control laws restrict the shipment, transmission, or transfer of certain items, software, technology, and related data overseas, which can include seemingly innocuous materials like research data, publications, and even the features of your electronic devices. In some cases, you may require a license to carry certain encrypted devices, software, or data.

Items on the United States Munitions List (USML) or those with an export control classification number (ECCN) other than “EAR99” may require an export license, depending on the destination and end-use. While many everyday items fall under the “EAR99” classification, numerous items used in academic research do not. Often, an export license exception can be applied, but it's advisable to consult with Brown’s Export Control personnel from the Office of Research Integrity to confirm if an exception is applicable.

Encryption

When traveling internationally with electronic devices, it's important to be aware of the diverse and complex regulations surrounding encryption. Some countries, such as China, Israel, and Russia, have restrictions on importing and using encryption tools and do not allow cryptography tools to be used within their borders without a license, or in some extreme cases, at all. This regulatory landscape presents a significant consideration for international travelers carrying electronic devices, as an increasing number of modern electronics use encryption mechanisms to protect user data by default.