Technology Travel Tips for Laptops

Physical Tips:

- **Consider a locking laptop bag. (While someone can always steal your bag, this will prevent someone from quickly removing the laptop from your bag without your notice.**
- **Utilize a privacy screen on the monitor.**
- **Protect your laptop with a case, sleeve, and padded laptop bag.**
- **Make sure you have the appropriate power adapter/converters.**

Cybersecurity Tips:

- **Remove all data stored locally on your computer—for example, un-sync local copies of OneDrive, Dropbox, etc.**
- **Consider your passwords carefully; they should be strong and different for every account (no repeats).**
- **Implement Multi-Factor Authentication on every account you can.**
- **Implement full-disk encryption on your hard drive.**
- **Utilize a VPN.**
- **Ensure that you have backed up your data before leaving the United States.**
- **Ensure your computer contains all up-to-date operating system and application patches/fixes.**
- **Ensure the antivirus is up to date.**
- **Consider using web-based applications instead of locally installed applications, i.e., Outlook, Word, and Excel.**
- **Use privacy-focused applications, i.e., Brave, ProtonMail, DuckDuckGo.**
- **Disable Bluetooth on the laptop and leave all Bluetooth devices at home.**
- **Disable Wi-Fi on the laptop when you are not using it.**

This is not a definitive list and is ever-changing, but this is a great start to keep your computer and its data safe.

Technology Travel Tips for Mobile Devices

If you have a long-term mission where you may need your standard mobile device, you may also consider the following:

- **Back up your data beforehand.**
- **Ensure Pins/Passcodes on the device are strong – Biometrics such as facial recognition or fingerprint is not necessarily the strongest.**
- **Consider turning Wi-Fi/Bluetooth/NFC off when not in use.**
- **Do not download any apps; be extra cautious while on public Wi-Fi.**
- **Do not use public Wi-Fi to access accounts or make purchases where financial information is involved.**
- **If you need to access sensitive data while traveling, prepare to store it in the cloud (encrypted). Sign out of the cloud account, and delete any applications or evidence of the account while traveling. Only access what you need (not on public Wi-Fi) after you've reached the destination.**
- **Use encrypted calling/texts such as the application "Signal." Available on Android and iPhone.**
- **Install a mobile antivirus and anti-spyware/malware application with up-to-date definitions.**
- **Run spyware/malware/antivirus scans regularly for signs of compromise.**

If you choose to take a mobile device with you on your short-term mission trip, we also recommend purchasing a prepaid phone with zero data stored on the device.

This is not a definitive list and is ever-changing, but this is a great start to keep your computer and its data safe.