Device Safety While Traveling Abroad

Advice from the Colorado School of Mines Office of International Programs (oip.mines.edu) and Computing, Communications, and Information Technologies (ccit.mines.edu)

While traveling outside the United States it is especially important to protect your electronic devices and data. Smartphones, tablets, and laptops are particularly vulnerable to theft or intrusion by criminals or even by state actors. These tips will help you keep your information safe while traveling for leisure, study, or work.

PRIOR TO DEPARTURE

- **Bring as few devices as needed.** More devices = more opportunities for hacking or data loss.
- **Bring only the data you need** for your work—no more.
- **Back up your data** before you leave. In the event your device is lost or stolen, you will still have a copy.
    - If you back up your data to a USB drive or external hard drive, leave that drive home in a safe location. **Do not** travel with it in your luggage.
    - Cloud storage back up allows for easier recovery of data. However any data covered under FERPA regulations or other confidentiality requirements should be uploaded to Mines servers **only**.
    - For added security, encrypt your backups. CCIT can show you how.
- **Update your operating systems and all software** on all of your devices. Updates frequently include security fixes. (Do not update while abroad unless you are certain that you're on a secure network. Turn off auto-updates and only update manually if this could be a consideration.)
- **Activate a firewall** on your laptop and **install/update antivirus software**. Ask CCIT for help if needed. Mines offers free antivirus software for Windows and macOS (http://ccit.mines.edu/CCIT-Antivirus). Free or inexpensive antivirus packages are also available for iOS and Android devices in their respective app stores.
- **Set a passcode** for all of your devices.
- **This is very important: Encrypt your entire hard drive**—whether it's on a phone, tablet, or laptop—and use a strong passphrase to lock it. **Any mobile device that contains Mines data must be encrypted, regardless of who owns the device.** Most operating systems now come with encryption available standard—you just need to turn on encryption if it is not already enabled.
    - For Windows, look for "Bitlocker."
    - On a Mac, turn on "FileVault."
    - On iPhones and iPads encryption is on by default if you set a passcode. Do so. Set the "erase data" option so that your phone is wiped after 10 incorrect attempts (this avoids a brute-force attack).
    - On Android devices, turn on encryption if not otherwise enabled then set a passcode. Without a passcode, anyone can access your machine even if the drive is encrypted.
- **Encrypt your email and messaging.** For sensitive data, you may want to consider encrypting your email. Mines email supports encryption (with some further configuration and a $29 fee for an encryption certificate). Third-party apps like Signal allow fully secure text messaging. CCIT can help set up these services.
- **Install a VPN** ("virtual private network") client—available at **vpn.mines.edu**—and use it whenever you connect to the Internet. If you do not encrypt your email, then this step is critical. Connecting to our VPN will also allow you to access Mines resources such as online journals available through Arthur Lakes Library. The approved Mines VPN is also available for mobile devices.
- If you are visiting another educational or research institution be sure to configure your devices for **eduroam** access before leaving campus. See https://ccit.mines.edu/CCIT-eduroam for more information.
- Some countries do not allow laptops to be encrypted. In that case you may **check out a laptop from the Computer Commons** (CT156) and copy to it only the (non-confidential) data needed for travel. These laptops are not encrypted by default (though they can be, upon request), so assume that a foreign agent will see everything on that device, and that they will install surveillance software. When you return from travel, return the laptop and CCIT will wipe the hard drive clean.

- Finally, be aware that **US regulations regarding H1B visa holders, Green Card holders, and foreign nationals** are in flux. In general, entering or exiting the United States may pose special challenges for such individuals, who may want to consult an immigration attorney before traveling abroad. And, of course, entering or exiting another country subjects you to the laws of that country as well.

DURING TRAVEL

- **Keep your devices with you** and secure at all times, if possible. Consider the risks of hacking at your destination. Hackers can be independent or state sponsored. Hacking is easier if someone has physical access to your device.
- **Be aware of laws** regarding telecommunication where you travel. Encrypted Internet connections may be blocked or illegal. This may affect what things you can and can't do over the Internet.
- **Be wary of public wi-fi networks**. Some, such as those available at a US embassy, a university, or a large corporation, are likely to be more trustworthy. Don't be afraid to ask someone familiar with the network to tell you about it. Other public locations, like coffee shops, may offer less-trustworthy free wi-fi. Ensure that you connect to their network (not ad hoc networks that may spring up around it), then take further precautions:
    - Activate your VPN as soon as you connect to the network.
    - Avoid sending or receiving sensitive or confidential information over public networks.
- **Be wary of software updates** while abroad. Malware can be pushed over public networks in the form of updates. Only install updates via secure networks and only when you initiate the update. Never update your device in response to unusual messages or notifications.
- **Scan for viruses** frequently and watch for unusual behavior while using your devices.
- **Avoid using public computers** with any sort of personal or confidential information. These computers could be infected by anyone who has used them previously. Any information or passwords you enter could be compromised. If you do use a public computer, assume that any passwords you entered are compromised. Change them via a secure network as soon as possible.
- In the US, the Transportation Safety Administration (**TSA**) has the right to search your computer or phone when you enter (or leave) the country. You have a right to encrypt and lock it. If you have set a password, you cannot be compelled to provide it. If you have set a TouchID (fingerprint unlock), you *can* be compelled to provide that. The TSA may hold you for quite some time if you refuse to unlock your device. There may be circumstances when you have confidential information on a device that you are contractually obligated to keep secret. This is currently a legal grey area. Of course, if a school-owned laptop is confiscated by the TSA, please let CCIT know.
- Return checked out laptops to the CCIT Computer Commons front desk (CT156), where the hard drive can be wiped and a new, clean operating system installed.
- If using your own device, scan for viruses immediately upon return to the US.

UPON RETURN

- Update your operating system and applications as needed. Re-enable software auto-update, if appropriate.
- Update any passwords that were exposed during your trip abroad.
- Precautions taken abroad are often good security measures in general. Encryption, regular VPN use, strong passwords, firewalls, antivirus software, and secure backups are all recommended at home as well.

*Need help with any of this? For travel advice call OIP at **303.384.2120**. For tech advice, contact CCIT at **helpdesk.mines.edu** or call the CCIT Technology Support Center at **303.384.2345**.*

OFFICE OF INTERNATIONAL PROGRAMS
COLORADO SCHOOL OF MINES

INFORMATION TECHNOLOGY (CCIT)
COLORADO SCHOOL OF MINES