INTERNATIONAL PROGRAMS
COLORADO STATE UNIVERSITY

Safety Tips for Technology Abroad

Along with the many benefits of your education abroad experience, there may be some risks, including those surrounding your technology. Using the internet always exposes your information, and possibly more so when you're abroad, due to unsecured Wi-Fi networks and where internet laws and security may be very different to the ones you are used to at home. The theft of personal information may damage you personally or financially. Lack of preparation could leave you the victim of a hack, identity theft or even subject to harsh penalties. The following tips will help minimize your risk.

Three critical considerations for tech abroad:

1. **Consider your "digital footprint".** Immigration officers have been reported to search Instagram, Twitter etc., before admitting travelers to the country. Be aware that laptops and phones can be subject to search. Ensure your media does not antagonize local issues or violate laws in that country. Delete any applicable content and make your social media private.
2. **Research your destination in advance** as some countries have censorship laws as well as regulations regarding free speech online. Know that in some countries certain website accessibility is restricted.
3. **Keep in mind that local networks** (like unsecured Wi-Fi networks) **may introduce malware, capture usernames and passwords, or download your contacts and personal info.** Do not access data sensitive websites, such as banking or RamWeb, when on an unsecured network.

A few other tips to keep in mind:

- Take along only the data and documents you need. The safest approach is to have a device that provides access to the bare minimum, which reduces the risk if it is compromised.
- Turn off any extra features you don't need such as Bluetooth and location tracking. Not only do you run the risk of data charges but also these networks can be more easily hacked.
- Update all software and apps before you go. Do not update apps or allow changes to your computer through internet connections abroad. The FBI has identified malicious software disguised as updates to legitimate software.
- Are you taking or shipping any specialized equipment or materials that might have military or dual military-civilian use? Do some research; for example, a photography drone falls into this category. If so, it is recommended to leave it at home.
- Before leaving the country, you should backup the devices that you're taking with you to an external hard drive or the cloud.
- Use password protection on devices to limit access without your knowledge. Turn them off when not in use.

If you have any questions about these tips, please connect with your Education Abroad Coordinator or CSU's Secure and Global Research Office at +1 (970) 491-1563 or vpr_export_control@colostate.edu. If you suspect that your CSU email account has been compromised, contact Academic Computing and Networking Services (ACNS) at soc@colostate.edu.