Security Tips When Traveling Abroad

Extra consideration must be taken when traveling outside the United States with technology. Concerns range from basic theft of belongings to targeting of data used by academics. It is important to prepare properly, and use appropriate safeguards while traveling. Travel to friendly countries, such as those in Western Europe may not require all of these safeguards, while travel to US embargoed countries (Cuba, Iran, Syria, Sudan and North Korea) or countries with active espionage programs (including China and Russia) require additional caution.

Before You Leave

1. Bring only what you need – leave personal and Restricted Data, devices, and other items like ID cards and credit cards at home.
2. Verify encryption on your laptop and mobile devices. If you do not have this contact ITS.
3. Make sure you are not traveling with hardware or software that is subject to export controls. Contact the Department of Research Compliance for more information, especially if traveling to an embargoed country.
4. If possible, use a temporary laptop that has had its storage securely deleted and the operating system and applications freshly installed or sep hard drive.
5. Use an inexpensive prepaid phone instead of traveling with your own personal devices.
6. Look at State Dept travel guides
7. Ask Legal before you go in case you are physically searched

For mobile devices

1. Contact your mobile provider to find out your plan's roaming policy.
2. When you arrive to your destination, quit all applications and enable Wi-Fi to avoid roaming charges.

For laptops

1. Make sure your laptop is up-to-date with all operating system and antivirus software updates.
2. Back up your data before traveling.
3. Securely delete personal data and Sensitive and Restricted Data.
4. Turn off file and print sharing to avoid unauthorized access to your files. Disable automatic connections to open Wifi networks.
5. When return-no hook to network. Must be examined first
6. Don't leave in hotel without securing
7. If computer disappears for 24 hrs it is infected-do not use to link to university

When traveling

1. Assume that any activity on your device, especially on the Internet, will be intercepted. Be especially mindful of any security warnings from web browsers and applications.
2. Keep laptops and devices in your sight at all times. Hotel rooms are not a secure place to leave devices.
3. Turn off your electronics when they are not in use. Do not leave them in sleep mode.

4. Never use shared devices, such as public computers in Internet cafes for anything that requires entry of any password.
5. Only connect to secure wireless networks, like what might be provided in a hotel.
6. Always use University VPN which will protect your Internet traffic.
   We will put in updated instructions after we upgrade to the new Palo Alto VPN client
7. Make sure you have contact information for the University Help Desk
8. When returning home, discontinue use of devices and change all passwords used abroad.