Security Tips for Travelers

Here are several security tips you can do before, during, and after your foreign travels. Be sure you contact the University's Export Control Department before taking any device, electronic equipment, or encryption software overseas to high-risk countries.

Before You Leave...

- Inventory the devices you will be taking with you and label them in case they get lost or stolen. Avoid referencing the name of your organization instead include only your first name and personal contact information.
- Make sure your devices are fully patched. Also ensure the anti-virus software is working properly and up-to-date.
- Enable the startup password for your devices and choose strong passwords.
- Make a full backup of your devices and important data.
- Avoid taking any University information that’s confidential, sensitive, or anything that would bring harm to the University unless it’s absolutely necessary. If you must take them, encrypt the data. Keep in mind, however, that some border-crossing checkpoints may require you to log into your device and decrypt your data so they can inspect them further. Some of these inspections may take several days.

Be More Secure:

- Encrypt the entire hard drive and consider using location services and remote wiping software. Better yet, take a clean, loaner computer with you on your trip and don't take anything confidential or sensitive.
- Bring along a charge-only USB cable and use it to charge your devices. This prevents data from being downloaded or uploaded to your device with your knowledge.
- Disable USB autoplay/autorun on your Windows computer in case you need to use USB devices on your trip.

While You're Away...

- Turn off Wi-Fi when you're not using it and avoid using unknown Wi-Fi hotspots. Even airport, hotel, and coffee shop Wi-Fi hotspots can be suspect. Limit your web browsing to only HTTPS sites if possible.
- Watch out for shoulder-surfers and shield your hands while entering your passwords.
- Avoid using public computers and kiosks unless it’s for general browsing. Never use them to log into secure websites like banking, webmail, or social networks since your keystrokes may be captured.
• Keep your devices with you at all times. Don't leave them in your room or locked in the hotel safe since you may not know if anyone has accessed them.

• Avoid charging your device using unknown USB ports. Never insert unknown USB devices to your computer. If you must use storage devices or media, scan them first with anti-virus.

**Be More Secure:**
- Turn off Wi-Fi and use cellular wireless instead because it's more secure.
- Use VPN for web browsing since it will encrypt all of your traffic.

---

**When You Return...**

• Update your anti-virus then scan all of your devices. Delete all unneeded files you got on your trip.

• Change the passwords for your online accounts you accessed in case any were inadvertently disclosed.

• Consider wiping the hard drive and reloading your files from the backup you made prior to your trip. Transfer the new (necessary) documents from your trip back to your device after scanning them with anti-virus first.

**Be More Secure:**
- Return the loaner computer and transfer only the new (necessary) documents to your regular device after scanning them.