Academic Professionals
Traveling Abroad
Safety Guide
Before you go,

Reserve laptop/cell phone
Get a loaner device and limit the amount of data at risk. You can borrow secure laptops and cell phones from DoIT. Supply is limited. Reserve as soon as you can.

Prepare your device for travel
If you can’t take a loaner device, back up your data and remove all information not needed. Update all anti-malware, security patching and firewalls.

Minimize the information you take with you
Do not take sensitive information. In many countries/cultures, there is no expectation of privacy. Back up all
information and leave the backup at work. Remove external storage media.

**Review university and personal passwords**
Do not use the same login credentials for university and personal business. Passwords for sensitive systems (ISIS, HR) should not be the same as self-service passwords (email, calendar, My UW).

**Familiarize yourself with local laws and security**
Visit the U.S. State Department's site, state.gov, for information on the safety and security of countries you are visiting and to enroll in the Smart Traveler Enrollment Program at travel.state.gov.
During your stay,

Have no expectation of privacy
Eavesdropping is routine in some countries. Limit electronic and face-to-face discussion of sensitive information. Wait to discuss sensitive matters until you return or can use a secure mechanism.

Treat electronic devices as compromised
Do not use computers or faxes at foreign hotels or business centers for sensitive matters. Do not allow foreign storage devices (USB, CDs) to be connected to your computer or phone.
Keep electronic devices in your physical possession
Do not leave these devices unattended, ever. Do not leave them in your hotel room, in hotel safes or in your checked baggage. Do not ask someone to watch them for you.

Disable device’s network capabilities when not in use
Turn off Bluetooth and WiFi capability on your device when you are not using it. Turn off your cellular phone when not in use, especially if you have a data plan enabled.

Do not access systems with sensitive/restricted information
This is particularly advisable in countries where there is no expectation of privacy. See the U.S. State Department’s site for
country-specific issues. When accessing university systems, minimize the time online and amount of information accessed. Use VPN to connect to campus resources, unless you are in a country that doesn't allow encryption.

Upon your return,

Clean and/or rebuild all electronic devices
Return loaner devices to DoIT for analysis and cleaning. Have your personal computer analyzed for malware and unauthorized access. If necessary, have it re-built before next use.

Change passwords
Change passwords for all systems you accessed while traveling.
Report loss or theft of information or electronic devices as soon as possible

help@doit.wisc.edu
1-608-264-HELP (4357)