Santa Clara University
Information Security Office
1-408-554-5554
iso@scu.edu

GUIDELINES FOR INTERNATIONAL TRAVEL WITH TECHNOLOGY

Always use additional precautions when traveling internationally with electronic devices. International travel increases the likelihood that both personal and university owned devices and data will be compromised.

The Santa Clara University Information Office (ISO) recommends the following baseline precautions be taken to reduce the likelihood that your devices will be compromised. If any of your devices are compromised, having taken these precautions will reduce the negative impacts for you and for SCU.

For questions about any of the recommendations listed here, please consult with the IT Service Center (408-554-5700) or the ISO (iso@scu.edu).

Pre-Travel: What to Do Before Leaving on an International Trip

- **Start preparing** weeks before leaving for your trip.

- **Whenever possible, use loaner** laptops and/or handheld devices while traveling. Take the computer, but leave your data behind. This reduces the likelihood of theft or compromise that will expose your data. Upon your return, the device can be wiped clean, which reduces the risks of importing threats back into your home environment.

    - **Check with the IT Service Center** for more information on loaner devices.

- **Encrypt all mobile devices** that you are taking with you (computers, tablets, mobile phones, etc.) You should check to see if the country you are travelling to has any encryption import restrictions.

- **Some countries** (such as China, Israel, and Russia) have restrictions on the import and use of encryption tools and do not allow cryptography tools to be imported or used within their borders without a license, or in some extreme cases, at all.

    - **If there are restrictions,** the ISO recommends you take a loaner device. For more information on encryption restrictions, consult: http://en.wikipedia.org/wiki/Restrictions_on_the_import_of_cryptography

  - **Loaner devices do not need encryption.** If you aren't carrying around all your usual data and information, the chances of something being compromised is reduced. This is especially handy when travelling in countries that don't allow encryption.

- **Do not store passwords** or other credentials on the device

  - **Do not store passwords** on the device outside of password management applications designed to securely store and handle login credentials (usernames/passwords combinations). Be sure to reconfigure the web browser(s) to not save passwords. This prevents the login credentials from being saved in the browser cache.

  - **The IT Service Center or the ISO** can provide recommendations for safe password storage options.

- **Leave sensitive data** stored securely on SCU servers and access it remotely only via SCU's Virtual Private Network (VPN) service.

  - **This requires planning in advance (**to install VPN on your device), but it goes a long way toward providing secure access to your data without transporting it with you. Make sure that you test your ability to get to your data using VPN from some place off campus before leaving.

  - **Get VPN at:** http://vpn.scu.edu

- **Make sure all operating systems** and applications are updated and patched before leaving for your trip.

- **If you aren't using a loaner computer**, uninstall unused and unnecessary applications and turn off unneeded services on your computer. Leaving them installed and/or running only serves to provide additional, possibly "unlocked" doors for intruders to gain access through when attacking your device.

- **When you use a loaner device,** you should still make sure all operating systems and applications are updated and patched before leaving. You don't have to worry about turning off unused and unnecessary applications, because the loaner should not have a bunch of extra stuff running on it—*it's a blank slate for you to safely use while traveling.*

- **If you take your own computer** or loaner, don't accept any patches or updates while in foreign countries, as infected updates are becoming a more common attack vector.

- **Make sure you are running** in the lowest possible privilege level.

  - **While travelling, do not use an administrator account** as your primary user account. Running as a non-administrative user on your system will defeat a significant number of malware and browser exploits, because your computer is less likely to allow software, including malicious software (malware), to be installed without you (1) clicking "install" and (2) typing your administrative password.

- **Only connect to known** and trusted networks.

- **On all your mobile devices, turn off** "join wireless networks automatically." Always manually select the specific network you want to join, only after confirming its name and origin with the provider. Turn off wireless and Bluetooth, when not actively being used.

- **Keep track of what credentials** you use while travelling.

  - **Whether you sign into personal or SCU accounts,** keep track of the services you have accessed. The ISO strongly recommends that you change these passwords when you return. If you're on an extended trip, change them periodically. Don't use the same password for multiple services.

Post-Travel: What to Do When You Return to Campus After Travelling Internationally

- **Change passwords for all services** you accessed during your trip, on a trusted computer.

  - **When changing passwords,** remember to pick strong, complex passwords. Do not reuse the same password for multiple services.

  - **For tips:** http://scu.edu/is/secure/guides/passwords.cfm

- **As a rule of thumb,** have the devices you took on the trip assessed by IT Service Center staff or the ISO for signs of intrusion—*before you connect to SCU's network or your home network.*

Additional Tips and Advice

We strongly recommend that you use loaner devices because the risk of compromise while travelling internationally is high.

- If for some reason you cannot take a loaner laptop, be advised that it can be extremely time consuming and difficult to determine if a device has been compromised. As such, it is best to act accordingly—*if you didn't travel with a loaner device, seek help from your local IT support to format and reinstall the operating system and applications upon returning to campus.*

- Return your mobile devices to their pre-travel configuration. This includes any device you are taking with you (computers, tablets, mobile phones, etc.).

- Before connecting to another system on campus, turn off any services that you enabled specifically to facilitate your work while traveling, update and apply any patches that were released while you were away, and scan any data you brought back for malware.

- For additional information on international travel security best practices, consult: http://www.ncix.gov/publications/reports/docs/traveltips.pdf

- For more information on travel to specific countries, consult: http://travel.state.gov/travel/travel_1744.html