IT Security Guidelines for Domestic and International Travel

General Overview

Traveling can pose significant risks to information stored on or accessible through portable computing devices (laptops, tablets and smartphones, etc) and portable electronic storage media (Thumb/Flash USB Drives, CDs/DVDs, external/mobile storage).

Combining busy itineraries, unfamiliar surroundings and fatigue increases chances for the loss or theft of these devices while we travel. Flying poses additional risk since we lose physical and visual control of our belongings during the harried processing through airport security.

The Risks Associated with Traveling with Electronic Devices

While the loss of a smartphone, tablet, or laptop presents a financial loss to the institution, the greater risk from the loss or compromise of the device is the potential exposure of the sensitive or confidential data stored on the device. Data exposure may occur either because the device has been lost or stolen, or because it has become infected with malware. The likelihood of being compromised by malware is greatest when traveling outside of the US and especially high in areas where governments operate and manage the Internet.

What Should I do?

Information Technology Services (ITS) has some recommendations and tips that will help ensure the safety of both your portable computing devices as well as the data contained therein and reduce the impact if you are compromised:

1.) Before embarking on international travel you should always visit the U.S. Department of State web site: http://travel.state.gov/content/passports/english/alertswarnings.html. Destinations experiencing restive political, social and economic situations increase the likelihood that mobile devices may be stolen or confiscated.
2.) When using a mobile device, create a strong password (numbers, upper and lower case letters, special characters – at least 6 characters long) and make sure the device auto-locks. If your device has a password lock-out threshold set this to a reasonable number.
3.) Never store passwords, or sign-on sequences with the device or in its case.
4.) Be wary of text messages coming in from unknown numbers. Links contained in text message can be used to install malware and spyware onto your device. Malware can gather information that is transmitted through your device as it goes from application to application.
5.) Keep your applications and smartphone operating system up to date.
6.) Don't tamper with the built-in security measures on your phone, as this removes protections against unauthorized apps (sometimes called jail breaking or rooting your phone).
7.) Avoid using public Wi-Fi networks for online shopping, banking or accessing other sensitive information.
8.) Be sure to disable broadcast services including Bluetooth, Wi-Fi, Location Services, and Global Positioning Information if not necessary. These services can used to potentially launch attacks against your device, and can be used to locate and introduce malware.
9.) If possible, do not take your work or personal devices with you when you travel. Use a temporary device, such as an inexpensive laptop (you may be able to check one out from your department). Use a prepaid cell phone purchased specifically for travel.
10.) While traveling, remove any information from the device that you do not need on your trip. This may mean carrying a "clean" laptop, void of student grades, proprietary information (including unpublished research or articles), and personal information.

11.) If you require your personal or business laptop, back the equipment up in case of loss or theft, use a complex password to encrypt sensitive or confidential data, or verify that all student, personal, and proprietary information is removed.
12.) Update your equipment with the latest patches, updates, firewall and antivirus software before traveling.
13.) Use a VPN (Virtual Private Network) to access university resources.
14.) Consider purchasing tracking software in case of theft or loss, such as Lojac for Laptops, or enable Find my iPad/iPhone.
15.) Assume that any equipment other than your own is insecure. This includes equipment owned by friends, at cybercafes, libraries, etc. Furthermore, avoid entering sensitive information (credit cards, bank accounts, passwords) when using public wi-fi hotspots, or other insecure locations. Look for *https://* preceding the web address as a sign of a secure web page prior to providing information. The "s" at the end of https means the transmission is encrypted.
16.) Portable equipment, such as data sticks/flash drives, CDs, tablets, phones, etc., containing sensitive data should be kept secure, and locked when unattended. These items are especially vulnerable to theft and loss. Whenever possible, encrypt these devices.
17.) When not in use, turn off the device(s). Do allow them to be in "sleep" or "hibernation" mode when they are not in active use.
18.) When you return from your travel, be sure to update your virus tables and scan for viruses and malware. It's also a good idea to change your UWG ID password.