Traveling with Devices and Connecting to the Internet

When traveling for business or for pleasure, many of us find it essential to take a laptop, tablet or smartphone with us to stay connected to our office and family. Since our devices are prime targets for thieves, it’s important to understand how to protect yourself, your devices, and personal or university data when traveling. The following tips are designed to help students and employees secure their mobile devices and personal and work-related information while traveling.

PREPARING YOUR DEVICE

1. Back up your devices before traveling. Should your device be lost or stolen, your data will be stored safely elsewhere.
2. Do not store the backup on mobile media (like a USB drive) and pack it with your luggage! Leave the backup at home or at the office in an appropriately locked container.
3. Use a password, passphrase, or passcode on your device, but never store it with the device.
4. Enable a firewall on your laptop.
5. Install anti-virus software and keep it updated.
6. Update and patch your devices with the latest software prior to leaving and after you return.
7. Use encryption to protect your personal confidential information on mobile devices.
8. Don’t store Cal Poly confidential data on your mobile devices.
9. Employees: Install a VPN (Virtual Private Network) client on your device, but only use Cal Poly’s VPN if you absolutely need to.
10. Employees: Always check with your IT support for help making changes to a university device.

WHILE TRAVELING

1. Bring a minimum number of devices and keep them with you as much as possible.
2. When using cell phones, stay off the local telecommunications network if possible. Foreign intelligence services may tamper with phones via telecommunication networks; avoid roaming on these networks. To make voice calls, consider acquiring a disposable phone in-country, use Skype, or a similar application.
3. Be wary of wireless networks. Don’t connect to a wireless network you don’t recognize. If you aren’t sure what’s available, ask someone in authority.
4. Use only secure networks such as those found in a United States embassy, university or corporate office. Always check with someone you know and who is knowledgeable first.
5. When connecting to wireless data networks, activate your VPN as soon as possible. VPN software is available for almost all mobile and laptop platforms. Connect back to Cal Poly network when doing anything on the internet.
6. Never accept or install software updates of any kind when traveling. Some intruders push malware application updates to hotel network users. It’s better to update your applications before traveling and then avoid updates until you return home.
7. If you don’t have your own device, avoid using a public computer such as those found in libraries and hotels that are available for anyone to use. There is no way to tell if someone before you has infected the machine with spyware, malware, or keylogger software to capture the keystrokes of information you provide while using it.
8. If you have no choice but to use a public computer to communicate sensitive information, assume that all information and your login and password you used have been compromised. Keep track of the accounts you had to access and change your passwords immediately when you have access to a trusted computer and network, or contact the ITS Service Desk for assistance.
9. If possible, bring only clean ‘disposable’ devices, especially when visiting overseas.
10. Do the minimum amount of business necessary while traveling following these tips.
11. Employees: When you get home, relinquish your loaner devices to your IT support staff. They may wish to perform forensics to determine if the device contains rogue software or hardware.
ADDITIONAL TIPS FOR SMARTPHONE/TABLET USERS
1. When authorizing any access to an application, ask yourself: “Does your application really need those permissions?”
2. Leave your BlueTooth turned off when you are not using it.
3. Record the International Mobile Equipment Identifier (IMEI) of your handset. The IMEI is a 15 or 17 digit number usually printed on a label under the battery. If your device is lost or stolen, you can report this number to your provider and they can block the handset from being used.
4. Turn on the security feature of your device; all devices have them.
5. Set a strong password.
6. Use remote tracking (via GPS), enabling the locking and or wiping functionality if your device supports it.
7. Turn off cookies and autofill.
8. Do not save passwords or PINs as contacts on your phone.
9. Know that passers-by could be watching what you are typing (known as shoulder-surfing).

ADDITIONAL TIPS
1. Use dual authentication to access your personal email whenever possible
2. Change your password frequently
3. Don’t do any banking via the Internet; instead, go to a local branch office
4. Don’t shop using your credit card online while traveling
5. Don’t let anyone else use your device
6. Don’t let anyone repair or service your device; you are better off bringing your device home to repair it with a certified dealer

CONNECTING TO THE INTERNET USING “PUBLIC NETWORKS”
A public network is a network that is generally open (unsecured) allowing anyone access to it. These networks are available in airports, hotels, restaurants, and coffee shops, usually in the form of a Wi-Fi (wireless) connection. When you connect to a public network, your online activities and data transmissions can be monitored by others, and your device may be at risk to a potential attack. Here are some safety tips when using public networks.
1. Avoid entering any personal or confidential information, such as passwords, credit cards, etc., until you have a more secure network connection.
2. Limit your use to casual browsing only, e.g., checking the news, looking up restaurant or movie information, or flight information, etc.
3. Read, understand, and heed ALL browser warnings you see (i.e. pop-ups.)
4. Beware of unusual computer behavior- operating extremely slowly (indication of snooping).
5. Consider alternative Wi-Fi connections such as using a cell phone to connect to the Internet (tethering).

NOTE: Some information on this page was adapted from “Seven Tips for Digital Security Overseas” by Richard Bejtlick, 5/23/13, on the FireEye Blog

I have read and understood the information provided by Information Security on Traveling with Devices and Connecting to the Internet and will follow the recommendations therein.

Signature: ________________________________ Date: ________________________________

Print Name: ________________________________