Who we are

Center for Information Technology Services (CITS)

Contact Us

601 W. Lombard Street
Baltimore, MD 21201

Phone: 410.706.4357
Web: http://www.umaryland.edu/CITS/

Security is everyone's responsibility!

UNIVERSITY of MARYLAND BALTIMORE

International Travel Tips for Information Security

CENTER FOR INFORMATION TECHNOLOGY SERVICES (CITS)

Top 10 Tips

Tip 1

Always use a virtual private network (VPN) when connecting ALL devices to a wired or wireless network. **Use Express VPN**, not a UMB VPN!

Tip 2

Do not take USB drives, they can easily be lost or corrupted.

Tip 3

Do not leave personal devices unattended. Even hotel safes are not secure as hotel personnel have access to the safes.

Tip 4

Use a mobile app or the Office 365 portal to reach UMB email and files. Do NOT connect directly to any University system. Do NOT remote desktop to your UMB computer.

Tip 5

Use a RFID wallet/purse to protect against electronic pickpocketing of credit cards, passports, and driver licenses.

Tip 6

Keep your passport on your person at all times.

Tip 7

Use an iPad or MacBook Pro, and preferably a loaner. A loaner would prevent malicious software from being installed on your personal computer when in a foreign country. Upon your return, documents created during travel can be saved and all of the data on a loaner device can be erased and wiped back to factory settings.

Tip 8

Avoid discussing or transmitting sensitive information as it can be intercepted with remote microphones, clandestine recording/listening devices, technical implants, or hacks.

Tip 9

Ensure that ALL devices are password protected. Log off devices when not in use.

Tip 10

BEFORE YOU TRAVEL, make sure you have the following items:

- Sync Stop USB device (adapter for standard USB cord) to ensure data is never stolen during charging
- Express VPN installed and configured
- RFID wallet/purse – to store your passport and other important cards/documents

Additional International Travel Tips and Information

- If you don't have access to a loaner iPad of MacBook Pro, and you must take your personal laptop, it is recommended that you take the following steps before you leave:
    - Make a complete back-up before leaving
    - Make sure that your laptop is encrypted
    - Remove any moderate or high risk data
    - Upon return, save any documents created during travel, completely wipe the computer and restore from back-up made before leaving.

- Consider whether you really need a mobile phone. The best thing to do is to use a device you don't ever need to use again. This can be a burner phone, or a phone that is purchased or rented at the airport or hotel when you arrive at your destination.

When you return:

- Change your UMID password
- If you took your personal computer, have it wiped clean before re-connecting to the campus network
- If you brought your computer, save any documents that were created while traveling to an external drive and restore from your pre-departure back-up.
- If you checked your voicemail while traveling, change your voicemail passcode.

China:

- It is a special travel situation
- Travelers to the People's Republic of China have experienced a range of issues
- Access to services that are taken for granted in the United States, like Gmail and other Google apps, Wikipedia, Yahoo Web Mail, etc. are often blocked or filtered
- Skype connections may be monitored by the government
- The VPN connection may have intermittent interruptions

International SOS is a subscription service. You can download an app that provides travel security expertise for business travelers. The following URL takes you to the website:
www.internationalsos.com