ITS Tip Sheet #3

Using Technology when Traveling

Traveling for business?

Use these tips to protect your computer and mobile devices

MiFi mobile Internet "hotspots" are available to provide secure Internet access during business travel

- Hotel, coffee shop, and other public WiFi Internet access points may not be secure
- DoF IT Services provides mobile "hotspot" devices you can take with you to provide secure Internet connectivity while traveling on business
- If you only need basic email and web access while traveling, reserve a loaner laptop from ITS
- Questions? The ITS team contacts are found at the bottom of this Tip Sheet.

Information security risks during business travel continue to rise with the proliferation of public WiFi internet access and the need to transport computing devices around the world. Follow these useful tips to minimize risk to your computer, mobile device, and Penn's networking infrastructure.

For a detailed list of information security travel considerations, visit ISC's page on travel data security at: https://www.isc.upenn.edu/security/aware/practice/travel.

1. **Reserve a mobile Internet hotspot and/or loaner laptop from ITS**. The ITS team keeps a small fleet of mobile Internet hotspots and loaner laptops for business travel. To reserve one for your upcoming trip, submit a Help Desk ticket or call the help line at x8-HLPU (x84578).
2. Depending on the country you travel to, you may be required to share data that you brought with you. If possible, **avoid carrying any sensitive, confidential or regulated data on your laptop or mobile device when traveling**. Not sure? Contact the ITS team (see bottom of page) and we'll help review your data and ensure it is properly secured before you travel.
3. **Avoid losing sight of your laptop or mobile device.** In some countries, computers may be tampered with when they are out of your view, such as during time periods of checked baggage. Try to keep your computing devices with your carry-on baggage.
4. **Use caution with USB "thumb" drives that are given to you**, like those handed out by sales professionals or at business conferences. They may contain malware or malicious software. Consider only using USB drives from trusted sources. If you obtain a USB drive and aren't sure of its contents, bring it to the office and our team will assist in ensuring it is safe to use.

DO:

>report a lost or stolen Penn computing device to the ITS team as soon as possible

>reserve and use a loaner laptop when traveling to high sensitivity countries like Russia, China, Syria or Iran

DON'T:

>log in to a web-based system on a public computer, such as a library or hotel business center computer; your username and password may not be secure

>leave computing devices unsecured in a hotel room; always use a safe

>store Penn data on a personal, non-Penn computer