Cybersecurity for the Vanderbilt Business Traveler

With today's technology, it's easier than ever to stay connected while traveling, which allows us to stay productive and stay in touch. Unfortunately, traveling with electronic devices can make it more difficult to keep your personal and university information private. It can also increase the potential of device theft.

Leaving devices at home is recommended, if possible. If you don't need it, don't take it. However, if you must take your electronic devices on a trip, consider these tips:

Before Your Trip

- Less is more; only take what you need.
- Contact the VUIT Help Desk to ensure your device is encrypted (including USB) and end point protection is installed.
- Ensure patches and updates are applied.
- Password protect your devices.
- Back up your information.

While Traveling

- Be aware that your device maybe searched, seized, copied, or stolen.
- Avoid public wireless networks and charging stations.
- Utilize a Virtual Private Network (VPN), but be aware some countries may block VPN*.
- Turn off automatic connect services such as Wi-Fi, Bluetooth, and GPS.
- Do not plug in untrusted electronic accessories; they may contain malware.
- Do not leave devices unattended.
- Immediately report lost or stolen devices to the VUIT Help Desk at **+1-615-343-9999**.

After Your Trip

- Change your password(s).
- Monitor your devices and report any anomalies immediately.

A Note on International Travel

Did you know everything you take abroad is considered an export? Export restrictions are not limited to physical items but can also include intangibles such as software and data. Certain items and information may require an export license or other U.S. government approval to take abroad. Contact Vanderbilt Export Compliance (VEC) for the most up to date international travel restrictions and licensing requirements.

* Due to the cyber espionage threat, use of encryption is a standard practice when traveling internationally. In some foreign countries, however, encryption may be illegal. When applicable, the Wassenaar Arrangement allows encryption to be taken uninhibited between participating countries to promote international transparency and cooperation. Before you travel with encryption, ensure your destination is listed as a participating country here. Some countries do not fully participate in the Wassenaar Agreement and travelers should be cautious. Restrictions can range from requiring a permit to outright bans. In these cases, contact the VEC office for further information.

ADDITIONAL RESOURCES:

- Department of Homeland Security Tip Card
- Federal Bureau of Investigation Travel Brochure
- (REN-ISAC) Research & Education Networks Information Sharing & Analysis Center) Cybersecurity for the International Traveler
- Educause Security Tips for Traveling Abroad

CONTACTS

Export questions: vec@vanderbilt.edu

IT Security questions: it.risk@vanderbilt.edu