Traveling Abroad? Are Your Devices Secure?
BY LENETTE VOTAVA, OIT

When travelling abroad, faculty, staff and students all take mobile devices to work and maintain contact with the University, colleagues, family and friends. These devices, including laptops, cell phones and tablets, may be exposed to malware and/or automated attack tools that can compromise work or research files, as well as personal information.

Even those devices with current security software installed may not be able to escape such an attack. Here are some guidelines to follow that will help reduce the risks associated when traveling abroad, including the potential of loss, seizure, or tampering of devices.

Set-Up & WiFi Guidelines

- **DO** configure a password to logon to any device you will take on the trip. A password prevents others from accessing your data if your device is lost or stolen.

- **DO** set Wi-Fi to “Do Not Automatically Connect to Wi-Fi” on all devices capable of wireless connections.

- **Do** disable Bluetooth on your laptop, mobile phone, and other devices.

- **DO** set your mobile device to be wiped after 10 login attempts. Back-up your device before traveling in case your device is wiped.

- **DO NOT** update your computer while connected to a public or hotel wireless network.

Safe Data Handling Guidelines

- **DO** store data needed while traveling in a Notre Dame Box account or on Notre Dame's network. You can access your files through the Notre Dame VPN at [vpnaccess.nd.edu](http://vpnaccess.nd.edu).

- **DO** encrypt your devices to protect your data. Most staff laptops are already configured with device level encryption. However, some countries, like China, generally do not allow travelers to bring encrypted devices into the country. Be sure to check the guidelines for countries.

- **DO** immediately change your NetID password and the passwords of any accounts used while abroad upon your return.

- **DO NOT** store sensitive data (e.g., social security numbers, FERPA data, credit card numbers), on any device you are take with you.
• DO NOT copy sensitive data to memory sticks or other easily lost media.

You can find additional information when traveling abroad here: fbi.gov/about-us/investigate/counterintelligence/business-travel-brochure.

When going through security, sometimes airport or other security officers will ask you to start your device to prove that it works. Comply by starting your system and entering the password yourself. If the security officer wants you to give him/her the password, state that University policy requires employees not to share passwords. If he/she requires your password, provide it and change the password as soon as possible.

**Travel to High-Risk Countries**

Traveling with mobile devices to some countries, including China and Russia, is considered high-risk. The U.S. government has issued several advisories for travelers to be aware that they may become targets of espionage activity when visiting these countries.

Before you leave for high-risk countries, be sure to take a loaner laptop and phone. Do not travel with your own mobile devices. There is a high probability that they will be subject to compromise and tampering.

Be sure your mobiles devices are encrypted. However, you cannot travel with encrypted devices to China unless you have advance approval. China severely restricts the import of unapproved encryption. If you attempt to cross the border with an encrypted device, you may be asked for the decryption key or your device may be confiscated.

Additionally, the U.S. government prohibits traveling with encrypted devices to countries that are considered to support terrorism, including Cuba, Iran, North Korea, Sudan, and Syria. Do not bring encrypted devices to these countries. You can find more information by country at: cryptolaw.org

For additional information when traveling overseas, go to: oithelp.nd.edu/information-security/stay-secure/traveling-securely/