IT Security Recommendations

for International Travel

Overview

University faculty, staff, and students, who travel internationally with laptops, phones, and other mobile devices, are subject to many risks. Please use these recommendations as a guide to reduce the risks associated with traveling with these devices, namely that of loss, seizure, or tampering. If you have any questions regarding these recommendations or where you are traveling, please contact infosec@nd.edu.

General Recommendations

1. Configure a password to logon to any devices you are taking. A password prevents others from accessing your data if your device is lost or stolen.

2. Practice safe data handling:
   
   A. DO NOT store sensitive data, e.g., social security numbers, FERPA data, credit card numbers, on any devices you are taking with you.
   
   B. DO NOT copy sensitive data to memory sticks or other easily lost media.
   
   C. DO store data that you need for your trip in a Notre Dame Box account or on Notre Dame’s network. You can access your files stored on Notre Dame’s network and other campus resources through the Notre Dame VPN at vpnaccess.nd.edu.

3. Encrypt your devices to protect your data. Most staff laptops are already configured with device level encryption. However, check that the countries you are traveling to allow device encryption, e.g., China generally does not allow encrypted devices for travelers.

4. Upon your return, immediately change your NetID password and the passwords of any accounts used while abroad.

5. For additional information, please consult the following FBI advisory:


Security Checks

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 them the password, state that it is University policy to NOT share passwords. If they require that you provide the password to them, give them the password, and change immediately following the event or as soon as possible.
Travel to China, Russia, and other high risk countries

Traveling with IT devices to some countries, most notably China and Russia, is considered high risk. The U.S. government has issued several advisories that travelers be aware that they could be targets of espionage activities when visiting these countries. Travelers are strongly encouraged to follow these recommendations:

1. Take a loaner laptop and phone. DO NOT travel with your own mobile devices as there is a high probability that they will be subject to compromise and tampering.

2. Traveling with encrypted devices:
   a. DO NOT 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.
   b. The U.S. government prohibits traveling with encrypted devices to countries that are considered to support terrorism, namely Cuba, Iran, North Korea, Sudan, and Syria. DO NOT bring encrypted devices to these countries.
   c. Additional information by country can be found at this website: http://www.cryptolaw.org

Additional Recommendations

1. Set Wi-Fi to “do not automatically connect to Wi-Fi” on all devices capable of wireless connections.

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

3. Disable Bluetooth on your laptop, mobile phone, and other devices.

4. Set your mobile device to be wiped after 10 login attempts. Backup your device before traveling in case your device is wiped.

Resources:

Notre Dame VPN: https://vpnaccess.nd.edu

File storage: https://box.nd.edu

Laptop rental from the OIT Service Center: http://oit.nd.edu/computer-service-center/computer-rental

U.S. Government references:
