Security Guidelines for Domestic and Foreign Travel

Joel Rosenblatt
Director, Computer and Network Security
September 10, 2013
General Travel Guidelines

- Heightened Risks
  - Theft of equipment
    - Try not to look like a tourist
    - Never leave your bags unwatched
    - Be aware of your surroundings
  - Theft of credentials
    - Don’t use hotel business centers or web cafés to check your email, bank accounts, stock accounts, etc.
      - There is a good chance that they have key logging programs installed
    - Don’t use unknown WiFi networks
      - If you don’t know, ask
General Travel Guidelines

- Backups of your data
  - Backup everything before you leave
    - If your only copy gets stolen, you’re in trouble
  - Take more than one copy of your presentations
    - Don’t keep them in the same place
    - Email yourself a copy
    - Send a copy to the conference organizers
For domestic travel

- Any device containing University sensitive data
  - Must have a strong password
  - Must have a locking screensaver
  - Must be encrypted

This includes

- Laptops
- Tablets
- Cell Phones
- External Storage (the encryption part)
General Travel Guidelines

- Before you go ...
  - Check to make sure your machine is up to date
    - Check updates for OS, AV, and all applications
  - Make sure you have all of your gadgets, and only take the ones you really need
    - Chargers, cables, anything else you may need
    - For foreign travel, you will need plug converters
  - Test your presentation
    - Better to do that here, then have to call the Help Desk long distance
International travel is not the same as Domestic travel

- Different laws
- Different expectations of privacy
- Language differences may make for complicated interactions
Don’t take sensitive data with you

- See Data Classification policy
  - http://policylibrary.columbia.edu/data-classification-policy
- Loss of data through theft, seizure or search can get very complicated
- If your equipment is not in your possession at all times, you should assume that the hard drive may have been copied
- Even if device is encrypted, you may be required to supply the password in order to clear customs
- If sensitive data is required, make arrangements to download data using a secure encrypted link (VPN) and securely delete data when you are done using it
International Travel Guidelines

- Protect your data in case of loss or theft
  - Encrypt your device (supported devices)
  - Use a strong password and device timeout
    - Setting a password on a smart phone encrypts the data
  - Consider using auto wipe – 10 bad password guesses and the device gets erased (smart phones)
  - If you downloaded data for a meeting, remember to securely erase it when the meeting is over
    - Data you do not have cannot be compromised
International Travel Guidelines

- Protect your identity
  - Do not use the same password for multiple resources
    - Never use your UNI password for another resource
  - Don’t log into any resource on a “free” computer
  - Don’t use unidentified WiFi networks
  - Random web surfing can be very risky, don’t do it
  - If a web site looks different, don’t use it
  - Change your password(s) when you get back using a secure computer
International Travel Guidelines

- Protect your devices
  - Backup your devices before you leave
  - Install all updates before you go (including AV)
    - Installing updates while traveling is risky
  - Consider taking a bare bones or loaner system on your trip – speak to your department
  - Check that any software you are traveling with is allowed in the country you are going to – See:
    - http://finance.columbia.edu/content/export-controls-columbia-international-travelers
  - Don’t cook your device, make sure you have the proper converters
Travel between countries – Crossing the border

- Carrying data across the border can be especially risky
  - Border control officers can request that you enter passwords and take your machine away for inspection
  - If you refuse, you or your device may be detained
- If your device is seized, try and get documentation
  - Contact the U.S. Embassy or Consulate for advice
  - If your device is taken by the U.S. customs, contact Columbia University’s department of Export control
    - [http://finance.columbia.edu/content/emergency](http://finance.columbia.edu/content/emergency)
Travel with electronic devices and data presents additional risks.

Situational awareness is essential for security.

Personal safety is of the highest priority. When an official request is made, turn over the device.

You can send questions to security@columbia.edu
Questions?