How to Protect Your Data & Devices When Traveling

David Sherry & Tara Schaufler
February 2018
Agenda:

• Traveling with technology
  – Things to know
  – Before you leave
  – On the road
  – When you return
• Upcoming training
• Q & A
Traveling with Technology

• Pros:
  – Increased productivity
  – Entertainment
  – Staying in touch
Traveling with Technology

• Cons:
  – Privacy & security risks
  – Potential for device theft
Traveling with Technology

• **True story #1**: “My bag did not fit in the overhead compartment and I was forced to gate check it. When I retrieved my bag after the flight I noticed that both my iPad and medications were gone.”

*Story courtesy of Northeastern University’s Information Security Office*
Traveling with Technology

• True story #2*:
  – “I was sitting in a café with my purse hanging from the back of my chair. When I got up I noticed that someone had reached into the purse and had stolen my cell phone and wallet.”

*Story courtesy of Northeastern University’s Information Security Office
Things to Know

• Within the U.S., the Transportation Security Administration (TSA) agents at the gate are not allowed to confiscate devices or demand passwords

• Different rules apply to U.S. Customs and Border Protection agents & agents in other countries
Before You Leave
Before You Leave

• Be mindful to travel only with the data you need
• Understand the sensitivity of the data you bring or access
• Leave some (or all) devices at home
• Use a temporary device (loaner)
• Shift data to secure cloud storage
Before You Leave

How can OIT help with business travel?

• Loaner devices
• Loaner cell phones
• Travel service email accounts

For additional information, visit: http://www.princeton.edu/technologyoperations/tech-clinic/loaner-program/
Before You Leave

- If you decide to take devices:
  - Use encryption
  - Backup data before you leave home
Before You Leave

• Remove any saved login credentials (turn off browser cookies & autofill)
• You can temporarily uninstall apps & clear browser history
Before You Leave

- Change passwords or passphrases before you go
- Delete apps you no longer use
- Update software
Before You Leave

• Turn off Wi-Fi & Bluetooth

• Turn on “Find My [Device Name]” tracking and/or remote wiping in case lost or stolen
Before You Leave

• Stay informed of...
  – TSA regulations (tsa.gov)
  – Travel alerts & warnings concerning countries you plan to visit (travel.state.gov)
Before You Leave

• Register your travel with the Smart Traveler Program (STEP)
  – STEP (https://step.state.gov/step/) provides notices and alerts from the U.S. Government to U.S. Citizens while they are traveling or living in a foreign country.
Before You Leave

• The ISO’s website contains useful links & info:

www.informationsecurity.princeton.edu
Before You Leave

- Clear your devices of any content that may be considered illegal or questionable in other countries
- Verify whether the location you are traveling to has restrictions on encrypted digital content
Before You Leave

• Don't overlook low-tech solutions:
  – Cover the camera of your device(s) for privacy
  – Use a privacy screen on your laptop to avoid people "shoulder surfing" for personal information
  – Physically lock your devices and keep them on you whenever possible, or use a hotel safe
  – Label all devices in case they get left behind
On the Road
On the Road

- Public Wi-Fi is often not secure.
  - Do not work with sensitive data when you’re using unsecured public Wi-Fi
  - Use HTTPS everywhere you can
  - Make a habit of using VPN whenever you can
  - Best protection from an untrusted network is not to use it at all
On the Road

More about WiFi...

How many of you use Eduroam?
On the Road

- Eduroam is a global wireless network access service for research and education. An eligible organization (like PU) can provide users with wireless access at participating institutions through the use of their home institution credentials. Eduroam is available at more than 12,000 locations worldwide!*

* If you’ve never used Eduroam, see SN@P KB article for details on configuring your device.
On the Road

• Avoid public workstations
• Use multi-factor wherever it’s offered
• Avoid contact with Princeton’s network in general, specifically when traveling to high risk countries
On the Road

• Do not leave devices unattended
• Do not plug in untrusted accessories
• Use a non-privileged account
• Practice safe web browsing...
On the Road

Practice safer browsing:

• The Internet is full of malicious sites.
  – Some appear okay but may have been compromised
    • Drive by downloads
    • Malvertising
  – Some malicious sites are made to look like real sites
    • On average 46,000* phishing sites are created every day!

*helpnetsecurity.com 9/22/17
On the Road

Practice safer browsing:
• Keep your browser(s) up-to-date!
Browsing practices

• Start your browsing from a browser, not by clicking a link in an email
On the Road

If you happen to encounter a screen like this, what do you do?

There is a problem with this website’s security certificate.

The security certificate presented by this website was issued for a different website's address. The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information
When You Return
When You Return

• If you changed your password prior to departure, change it back
• Run full antivirus scans on your devices
• If business travel, report anything unusual to OIT or your IT staff
In summary our top tips include:

- Identify potential risks/travel restrictions & obey all laws
- Understand the sensitivity of your data
- Consider dedicated travel devices
- Avoid accessing Princeton directly
- Use multi-factor wherever it is offered
- Avoid public workstations
- Use VPN on any open Wi-Fi
- Change your passwords
NEW INFORMATION SECURITY TRAINING OPPORTUNITIES ARE AVAILABLE

Upcoming events include:
• Privacy is Our Shared Responsibility
• Facebook Live: Personal Privacy & Why It Matters
• Free screening of "The Circle," featuring Tom Hanks & Emma Watson, followed by a privacy-related discussion
• How to Protect Your Data and Devices When Traveling
• Spring Cleaning – Properly Recycling or Donating Devices
• Hackers: Who, Why, and What Do I Do?
• Lessons from The WannaCry Ransomware Attack, Equifax Breach, & Other Security Incidents
• Lock Down Your Login

Visit the Learn Center (www.princeton.edu/training) for more information and to sign up for events.
Questions? Email infosec@princeton.edu
Stay Connected & Stay Safe!

@PrincetonISO

@CISOatPrinceton

informationsecurity.princeton.edu

infosec@princeton.edu
Q & A
Thank you!

For more information visit:
informationsecurity.princeton.edu

or contact us at:
infosec@princeton.edu