University of Wisconsin-Madison

International Safety and Security Director (ISSD)

The Badger's Discussion of …

Data Security While Abroad




http://internationaltravel.wisc.edu

Before we talk about data security …

Remember … always:

- Enroll in the U.S. Dept of State STEP program for timely US embassy updates on breaking safety/security news: https://step.state.gov/step/
- Enroll in UW-Madison's int'l health and medical insurance (CISI) by calling Ms. Debbie Beich at 262-8926, or visiting the ISSD website and finding her info under the "links" tab! http://internationaltravel.wisc.edu
- Visit the U.S. Dept of State website for your destination country's safety and security information: http://travel.state.gov/content/passports/english/country.html

Best Practices … BEFORE TRAVELING

- ***First and foremost:*** **consider checking out a "loaner" device from DoIT – both laptops and cell phones can be reserved for travel!**
- Disable Bluetooth and GPS functions on your device
- Take only truly "must-have" devices with you … leave all others at home
- *Back-up all information, documents and programs* on the devices you intend to take, protect the back-up with a different PW than that you will use abroad
- Do not inadvertently take external drives/thumb drives that have files or documents on them

Best Practices … BEFORE TRAVELING

- Fortify your passwords! And ensure that work-related passwords are not the same as personal passwords – change passwords just for the trip
- Update all of your commonly used software and applications – *especially your antivirus software*
- Install "full-disk" encryption on your laptop
- Delete any sensitive files from your machine and empty your "trash bin" prior to departure
- Enable your screen lock and timeout functions
- Enable firewalls on your device

Best Practices … BEFORE TRAVELING

- *Remember … you MAY be compelled to share access* to any and all files on your devices while abroad – including a demand to decrypt protected files or drives
- Do NOT take any patentable, proprietary or sensitive materials/files on your devices
- If presenting, try to review the presentation so that content is not so specific that it may allow others to exploit your work

You may lose your work to those who DO NOT CARE about US law, disciplinary standards or professional propriety!!

Best Practices … WHILE TRAVELING

- Terminate your WiFi connections after use, do not just close out of the application – TURN OFF the device's WiFi capability entirely when not in use
- Use VPN log-in to access the network
- Only visit secure websites
- Disable file-sharing programs on your device
- Prior to travel, disable the "remember me" function on your device and always manually enter your UN and PW while abroad—for ALL applications
- Do not click on any links in texts or e-mail messages
- Do not download new applications while abroad

A Few "Other" (sort of related) Best Practices …

- Call your banks and credit card companies and notify them of your destination and dates of travel
- Write down (and take with you) the phone #'s to call in case a credit or debit card is lost or stolen
- Place a file with your credit and debit card institution phone #'s AND a copy of your passport ID page in the cloud or in a place that can be accessed readily by a friend or family member at home
- If you must use a debit card while traveling, leave only an amount that you must access in the account (e.g., move the largest amount from a checking into a savings or money market account prior to the trip)

"Chip and Pin" or "Chip and Sign" -- ?!!

- In the U.S., new credit cards are issued with a data-enabled chip; users then sign a receipt
- In Europe, and most other countries, the standard is the data-enabled chip with the use of a pin number!

MAKE SURE YOUR CARD HAS A CHIP AND YOU KNOW YOUR VALID PIN # PRIOR TO TRAVELING OVERSEAS!!

- If you have forgotten your pin #, request a new one and allow two weeks to receive a new pin # by mail

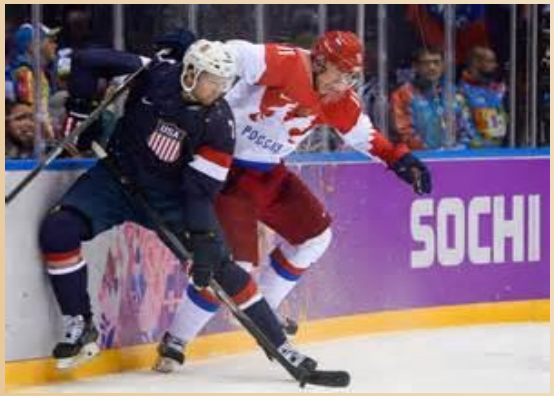
- If you are abroad, some companies will allow you to CHANGE your pin # often—even daily—by phone; **change it again as soon as you depart your host country**

An Example ….

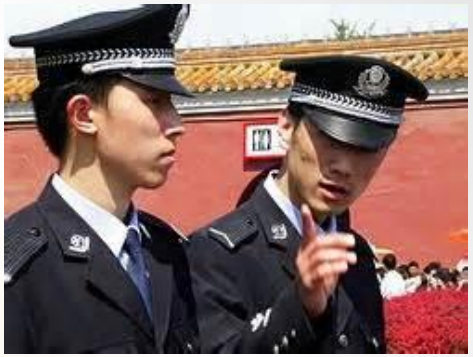
Russia

- ***No expectation of data privacy whatsoever!***

Since July 2000, the "System for Operative Investigative Activities." Commonly known as "SORM," this law **permits the monitoring, retention and analysis of all data that traverses Russian communications networks**, including fax, telephone calls, internet use, and e-mail messaging. **U.S. citizens should remain aware of this law when using any means of communication.**



Another example …



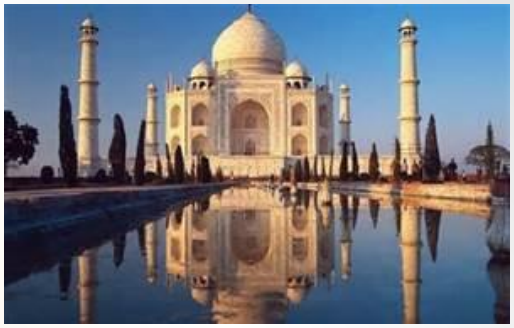
China

From the US Dept of State:

- "… Hotel rooms (including meeting rooms), offices, cars, taxis, telephones, Internet usage, and fax machines may be monitored onsite or remotely, and personal possessions in hotel rooms, including computers, **may be searched without your consent or knowledge. "**

- Telephones and SIM cards are widely available, and minutes can be purchased at many convenience stores. Vendors require identification, usually a U.S. passport from U.S. citizens, from anyone purchasing a SIM card, **and the purchaser's identity is registered with the government.**

And one more example …



India

From the US Dept of State:

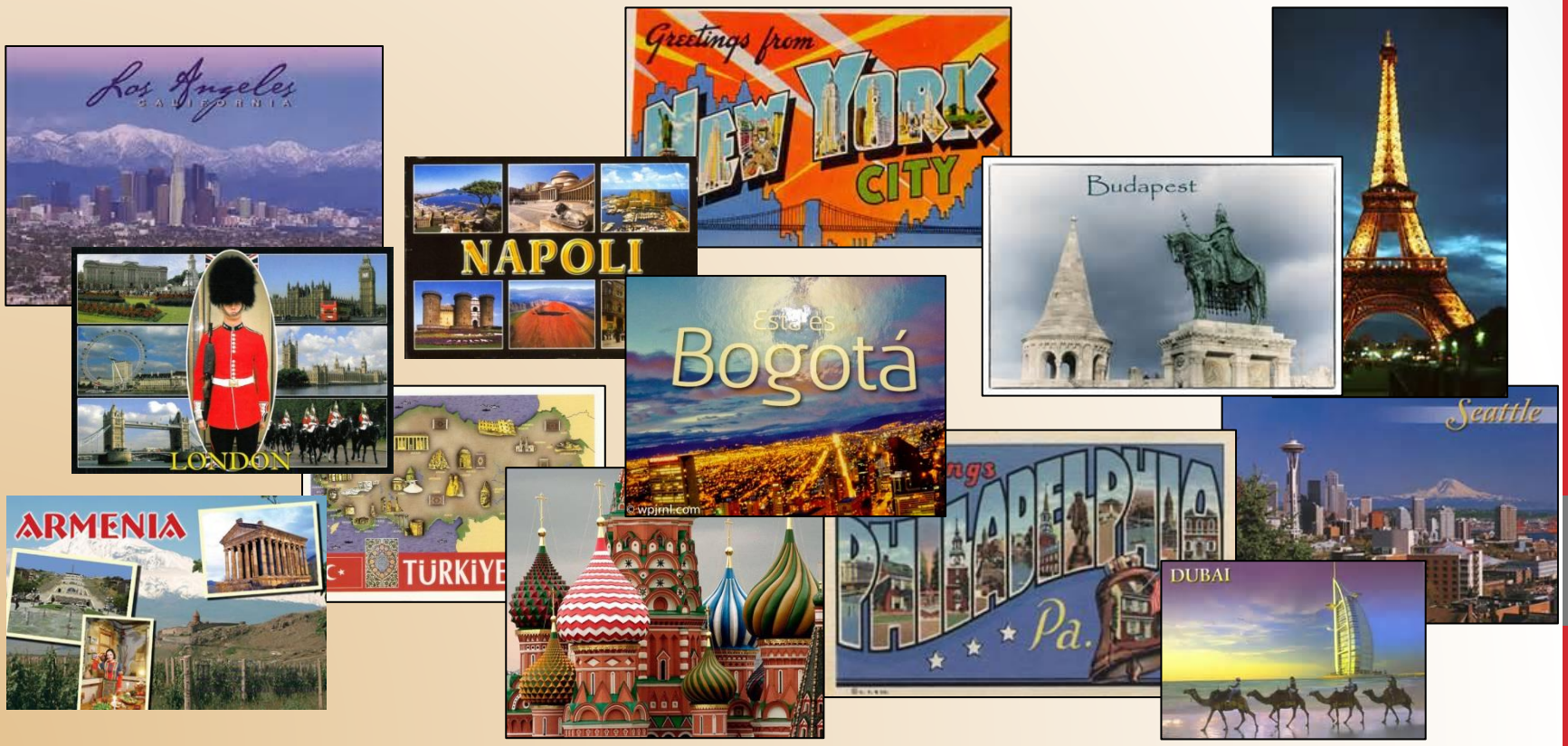
- "Networks in India are among the most highly targeted across the globe…. incidents in India increased by 117 % during the last year."
- The Indian govt's "Digital India" initiative will extend internet access and turn the country into a "digitally empowered" society – infrastructure laws and enforcement are lagging behind this admirable vision
- 235 million Indian users access the Internet thru mobile devices – India ranks 2nd in the world for malicious mobile software attacks*

* Kaspersky Lab data in US Dept of State, 10.15.15

Countries of Concern … ?!

Data crimes and privacy breaches <u>can happen anywhere</u>! Travel just makes you more vulnerable!!

- *Simply because you are not in a place where there is a high security concern, does not mean that you won't be targeted!*



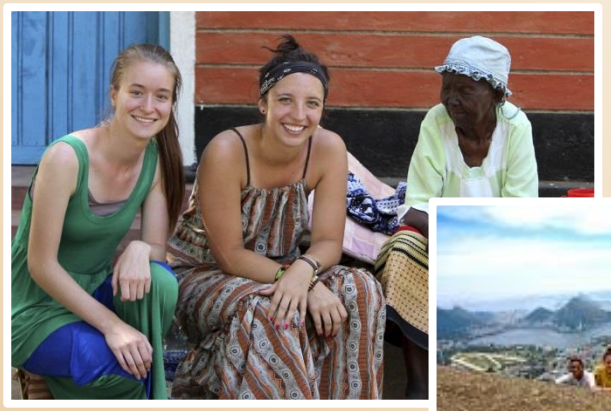
Best Practices … AFTER RETURN

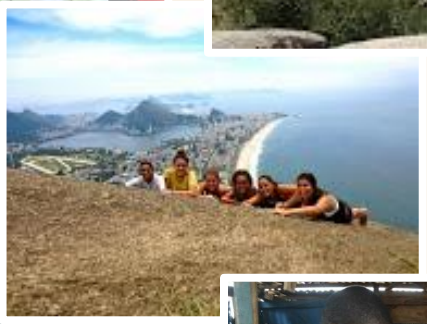
- Do NOT connect to a personal or business network until after you have:

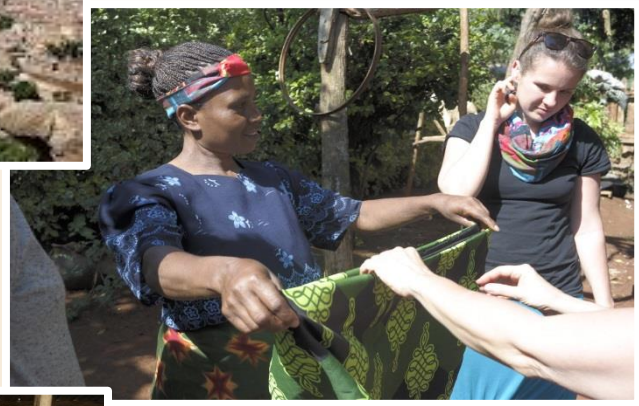
- run your antivirus and malware software or better yet, have taken your device and laptop into your organization's IT specialist to be scanned

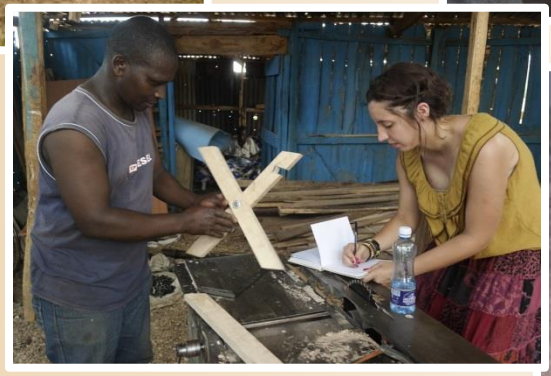
- changed all of your passwords and pin #'s (ASAP)!

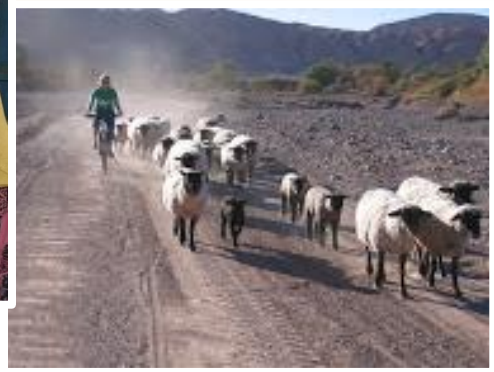
The goal … vibrant, successful *learning, research and outreach experiences* for UW-Madison students, faculty and staff who travel abroad!











A Great Link for Reference …

https://www.cio.wisc.edu/security/academic-professionals-guide-safe-computing-traveling-abroad/

http://internationaltravel.wisc.edu

Discussion … ?!

http://internationaltravel.wisc.edu