Information Security

SecureCat Courier — Summer 2015

IN A FEW DAYS, THE CAMPUS POPULATION WILL SCATTER.

Students will graduate or go home for the summer, and faculty and staff will begin summer travel, either for pleasure or work, or both.

Travel requires preparation, and information security should also be part of your checklist.

In this issue, you will find important tips on protecting your devices and identity so that you can relax and enjoy the change of scenery. If your travel is work-related, this issue is a must-read, since your trip includes protecting not only your own information, but the University's assets.

In This Issue:

SecureCat Courier is the University of Arizona's quarterly security newsletter.

UA InfoSec Resources

- Security-Faculty and Staff
- All-Employee Security Awareness
- Report an Incident
- Phishing Alerts
- NetID+ Two-Factor Authentication

Security News

- Sophos Naked Security
- OnGuard Online
- GetNetWise
- Macworld News
- eWeek Security News
- CNet Security

Traveling can be fun, but includes some risk, such as increased opportunities for the loss or theft of computing devices, as well as exposure to untrusted Internet connections. These risks are especially significant when you travel internationally.

Approach securing your devices and data when traveling as you would a painting a house. Invest time up front (e.g., put down drop cloths, tape around windows and edging) and the job will go much smoother and most likely without incident.

The following checklist should help to make your trip more enjoyable and secure. The "before" list is on the lengthy side, but this approach will help you stay secure while enjoying your travels. While these tips cannot guarantee security, they will help risk mitigation, and hopefully prevent a nasty cleanup job when you return home.

BEFORE YOUR TRIP

- ❑ **Travel light:** If you don't *absolutely need* a device, leave it at home.
- ❑ **Get a loaner:** If you're traveling on University business, ask if your department can provide an encrypted loaner laptop.
- ❑ **Travel with "clean" devices:** If you must take your own device, remove all regulated and confidential data.
  - ➢ Backup data to a secure location, and then remove the data **completely and securely** from your device.
  - ➢ If you must carry confidential data, your device must be **encrypted**.

  NOTE: DO NOT BRING REGULATED UNIVERSITY DATA OUT OF THE COUNTRY UNLESS YOU HAVE RECEIVED APPROVAL FROM APPROPRIATE COMPLIANCE OFFICERS.
- ❑ **Use strong passwords and device timeouts** for all accounts and devices that you will use overseas
- ❑ **Go disposable:** Consider purchasing a "burner" or disposable phone in your destination country.
- ❑ **Clean other mobile devices, too:** If you *must* take your cell phone or tablet with you, securely erase all sensitive data, including stored passwords.

- ❑ **Encrypt devices:** All devices, whether University-owned, personal, or "loaners," should be encrypted. ***NOTE: Some countries, such as China, Israel, and Russia, have restrictions on the import and use of encryption tools and do not allow cryptography tools to be imported or used within their borders without a license, or in some extreme cases, at all.***
- ❑ **Install Security Software and keep it up-to-date on all devices.** UA provides Sophos Endpoint Security and Control free of charge to all faculty, staff and students.
- ❑ **Update all operating systems and applications. :** If you no longer need an application, uninstall it.
- ❑ **Sign up for** Global NetID+ Two-Factor Authentication**.** Doing so decreases the risk that your sensitive personal information will be accessed, should your UA NetID become compromised while traveling.
- ❑ **Use the UA Virtual Private Network (VPN).** .UA's VPN provides a secure connection from your computer to the Internet, and can be used on multiple platforms and devices. ***NOTE: YOU WILL NOT BE ABLE TO CONNECT USING THE VPN UNLESS YOU ARE SIGNED UP FOR NetID+.***
- ❑ **If available, use eduroam for wireless service**. For more information, visit the eduroam webpage.

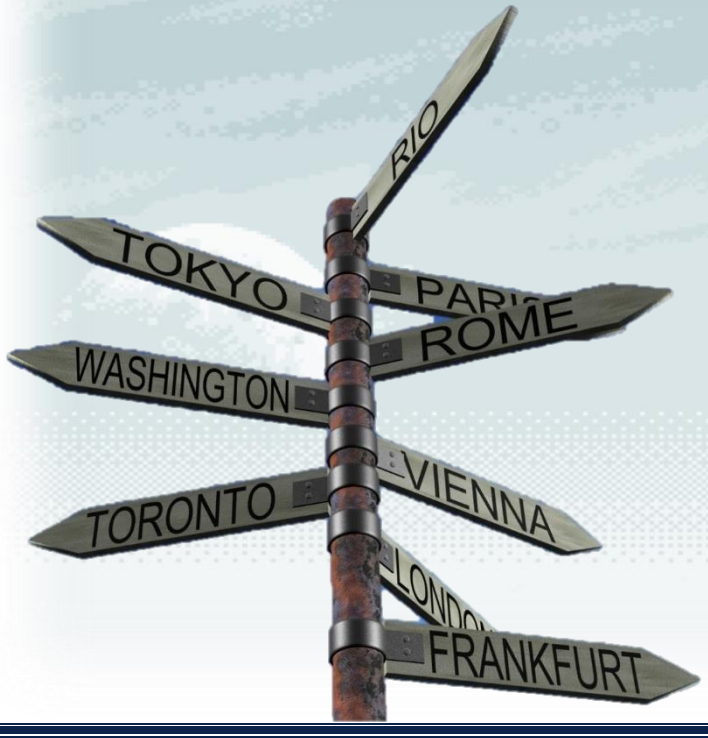
DURING YOUR TRIP

- ❑ **Use the lowest possible privilege level (e.g., user account) when logging on to your devices**.
- ❑ **"Opt out" of automatic connections**: In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. To protect yourself, do the following:
  - ➢ Turn off "join wireless networks automatically" on ALL devices.
  - ➢ Manually select the specific network you want to join, only after confirming its name and origin with the provider.
  - ➢ Turn off wireless and Bluetooth, when not actively being used.
- ❑ **Use care when using a "public" device:** Avoid logging into sensitive accounts on public computers. Also, be aware that keyloggers, "shoulder surfing" and cameras pointed toward keyboards are common ways that credentials are compromised.
- ❑ **Keep track of what credentials you use while traveling.**
- ❑ **Keep your technology with you or securely hidden and locked.**
- ❑ **Clear your Internet browser after each use.**
- ❑ **Report when something goes wrong:** If your phone or laptop is stolen, report the theft immediately to the following:
  - ➢ The local US Embassy or Consulate
  - ➢ Your department head
  - ➢ Your departmental IT support or the 24/7 IT Support Center.

AFTER YOUR TRIP

- ❑ **Change passwords for all services you accessed while away.** When changing passwords, remember to pick strong, complex passwords, and do not reuse the same password for multiple services.
- ❑ **Scan your devices:** Scan all of your electronic devices for malware. Should you need assistance with this, consult with your local IT support, or contact the 24/7 IT Support Center.

Visit our travel security webpage for more tips.



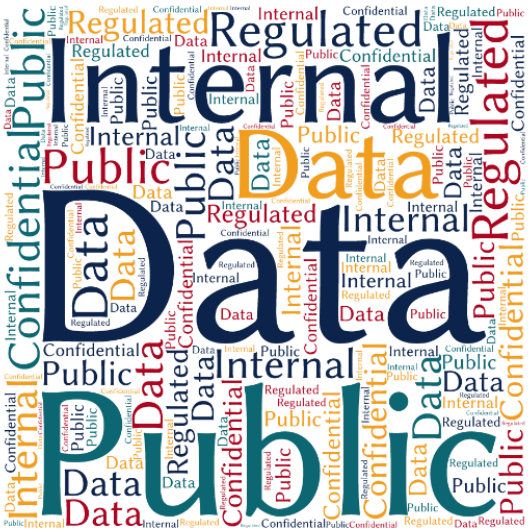
UA International Travel Information and Resources

If you are traveling as a representative of the University of Arizona or on University Business, you must comply with the University International Travel Safety and Compliance Policy. Below are links to the policy, as well as other important UA travel information and resources.

- ❑ International Travel Safety and Compliance Policy
- ❑ University International Travel Registry and Resource Portal
  - ➢ Export Control Program
  - ➢ Risk Management Information
  - ➢ Travel to Countries with Travel Warnings
  - ➢ Supplemental Travel Authorization Form
- ❑ International Travel Team
- ❑ International Travel Health and Safety Portal
- ❑ Travel Health Clinic

UNIVERSITY DATA CLASSIFICATION AND HANDLING STANDARD

UA Information Security has updated the University's Data Classification and Handling Standard (IS-2321) in order to provide more prescriptive guidance for the classification and handling of University information assets. The new standard clearly defines four categories of data:



Regulated: Data controlled by federal, state, local and/or industry regulations. These data are covered by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information.

Confidential: Data protected as Confidential by law, contracts, or third-party agreement, and by the University for confidential treatment. Unauthorized disclosure, alteration, or destruction of this data type could cause a significant level of risk to the University or its affiliates.

Public: Data that may be disclosed to any person, regardless of affiliation with the University. Some level of control is required to protect the integrity and availability of Public data (e.g., protecting original (source) documents from unauthorized modification).

Internal: Data not intended for public use or exposure. Internal data generally should not be disclosed outside of the University without the permission of the person or group that created the data. Any data not specifically classified as Regulated, Confidential, or Public should be considered Internal.

Please click **here** to view the full standard.

STAY INFORMED ON

Sign up for UA Information Security's listserv.
Open to all faculty and staff.

DID YOU KNOW?

UA faculty and staff are required to complete all-employee security awareness training. To access and complete this training, click here.

UA InfoSec Website | Contact Us
UA Information Security
1077 North Highland Avenue
Tucson, AZ 85721
520.621.8476 (UISO)