

Email & Data Security Training

9/25/2019

 **Mary Lou Fulton**
Teachers College
Arizona State University

Agenda

▣ **Phishing Emails**

- ▣ Identifying a suspicious email
- ▣ What to do
- ▣ What not to do

▣ **Securing Your Data**

- ▣ How to secure data on your device
- ▣ K-12 student/parent data

▣ **Data Security While Traveling**

- ▣ Identifying sanctioned countries
- ▣ Travel security guidance for your electronics
- ▣ Responsibility while mobile

Identifying Phishing Emails

➤ How do I identify phishing/spam emails?

- ❑ Look at the “from” full address that displays, not just the display name of the person- does this look like a valid address
 - ❑ As an example from emails that were going around in the spring
 - Carole Basile <carolebasile223@gmail.com>
 - ❑ If viewing on your phone, you typically only see the display name - to view the email address it is from just click on the name

➤ What do I do if I receive a phishing or suspicious email?

- ❑ **Do not** click on any embedded links contained in the body of the email
- ❑ **Do not** reply to the email - if you do happen to reply, do not include any personal information such as a phone number
- ❑ **Do not** forward the email to anyone - this expands the risk of potential malicious activity
- ❑ If unsure if the email is legitimate, call the person it appears to be from to verify validity when possible

<https://getprotected.asu.edu/>

<https://getprotected.asu.edu/information/phishing>

Reporting Phishing Email

➤ How do I report a phishing/spam email?

- Report the email by sending the internet headers of the email to UTO
 - Copy all of the text that appears in the Internet Headers box and paste into a new email. Send the new email to infosec@asu.edu with the subject line: Phishing Email

➤ How do I locate the email internet headers?

- Outlook on Windows Computer:
 - Double click on the original email - Select File in the upper left corner - Click on Properties - this will open a new window and at the bottom you should see Internet Headers
- Outlook on Mac Computer:
 - Right click on the original email - Select View Source - this will open a new window
- Other Email Applications:
 - Visit this link for support with other email applications:
 - [Trace an email with full internet headers](#)

Data Protection/Security

➤ Securing your data

- Never walk away from computer/phone/tablet without locking screen
- Do not store sensitive or personally identifiable data on computer
- Use ASU approved storage methods: Dropbox, OneDrive, secure storage
 - If you have questions on approved storage for specific types of data, review the [ASU Data Handling Matrix](#)
- Ensure device is encrypted (all ASU issued equipment is encrypted)

➤ K-12 student/parent data

- Do you ever request district/school for data? For what purpose?
- Be aware of student directory/video permissions - have parent's denied permission to have their student video taped?

➤ Security review process for software/hardware purchases


- Software – includes paid and free versions of all software
- Hardware - includes most hardware, exceptions for devices that cannot operate without another device - such as mouse, keyboard.
- Request by sending email to edops@asu.edu
 - Include name of hardware or software, reason for request, how it will be used, data elements that will be collected/entered into system (will there be sensitive or personally identifiable information), level/version/plan type requested, other relevant information to help us with review
- You may also work with your Business Office contact for these items, and they will contact us regarding the required security review documentation

Data Security While Traveling

- Identifying sanctioned countries
- Export Control Wizard
- Travel security guidance for your electronics
- Responsibility while mobile



Sanctioned Programs and Countries

 An official website of the United States Government

[Skip Navigation](#)

[Accessibility](#)

[Languages](#)

[Site Map](#)

[Contact](#)



U.S. DEPARTMENT OF THE TREASURY

[ABOUT TREASURY](#)

[SECRETARY MNUCHIN](#)

[POLICY ISSUES](#)

[DATA](#)

[SERVICES](#)

[NEWS](#)

 [SEARCH](#)

[Consumer Policy](#)

[Economic Policy](#)

[Financial Markets, Financial Institutions, and Fiscal Service](#)

[Financial Sanctions](#)

[Specially Designated Nationals List \(SDN List\)](#)

[Consolidated Sanctions List](#)

[Search OFAC's Sanctions Lists](#)

[Additional Sanctions Lists](#)

[OFAC Recent Actions](#)

[Complete List of Sanctions Programs](#)

Resource Center

[Home](#) » [Resource Center](#) » [Financial Sanctions](#) » [Programs](#)

Sanctions Programs and Country Information

OFAC administers a number of different sanctions programs. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Where is OFAC's country list?

Active Sanctions Programs:

[Balkans-Related Sanctions](#)

[Belarus Sanctions](#)

Program Last Updated:

02/03/2017

10/24/2018

<https://www.treasury.gov/resource-center/sanctions/programs/pages/programs.aspx>

Export Control Wizard

Research Integrity and Assurance

- [Home](#)
- [Human subjects](#)
- [Animals](#)
- [Biosafety](#)
- [Conflicts of interest](#)
- [Export controls and security](#)
- [Responsible conduct of research](#)
- [Scientific diving](#)
- [About](#)

[Home](#) / [Export controls and security](#) / [Export Control Wizard](#)

Export controls and security

[Forms](#)

[New and departing investigators](#)

[Regulations and resources](#)

[Glossary](#)

[Contact us](#)

Export Control Wizard

Export controls may apply when you send an item, information or software outside the United States' borders or when you share it with "foreign persons or entities" inside the United States. The Export Control Wizard has been designed to assist investigators in determining if they need an export license. For additional assistance, [contact us](#).

[Start Wizard](#)

<https://researchintegrity.asu.edu/export-controls-and-security/export-control-wizard>

GetProtected's Going Mobile

Going Mobile

ASU Top 5

Effective Practices

Identity Theft Protection

Infosec at a Glance

Internet Security

Latest news

- The U.S Department of State issued a travel advisory on 1/3/2019 for increased caution when travelling to China. <https://travel.state.gov/content/travel/en/international-travel/Internat...>
- China Starts Issuing \$145 Fines for Using a VPN

https://www.pcmag.com/news/365860/china-starts-issuing-145-fines-for-using-a-vpn?utm_source=email&utm_campaign=whatsnewnow&utm_medium=image

Travel Security Guidance for Your Electronics

<https://getprotected.asu.edu/content/going-mobile>

Travel Security Guidance for Your Electronics

- Ensure your equipment is encrypted prior to your departure.
- Remove sensitive data you don't need.
- Take a loaner or alternate device that contains no data and then wiped clean upon return.
- Always use a VPN when connecting to any ASU or other sensitive resources

Travel Security Guidance for Your Electronics

If your laptop is lost or stolen, immediately report the loss or theft to ASU Information Security Office at infosec@asu.edu



With Mobility Comes Responsibility

**It is everyone's responsibility
to keep sensitive information
secure and confidential.**

With Mobility Comes Responsibility

Purpose

ASU's Information Security Policy requires controls to manage risks to the confidentiality, availability, and integrity of University information. This standard defines the controls required for handling all University managed information. These required controls represent a minimum standard for protection of University information. Additional controls required under applicable laws, rules and regulations or standards governing specific forms of data (e.g. health information, credit cardholder data) may also apply.

The goals of this document are to (1) identify classifications of information handled at the University, and (2) define requirements for handling all data including Sensitive and Highly Sensitive data.

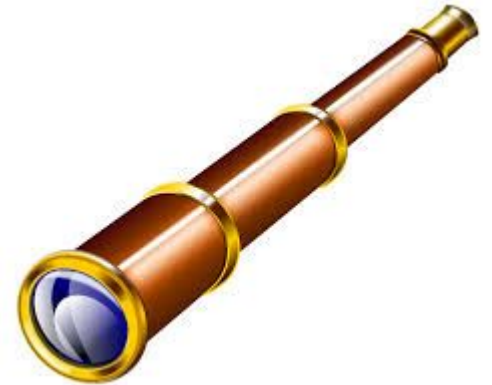
Applicability

This Standard applies to all users of ASU's computing, internet, and communications resources, including all students, faculty, staff (including student employees), courtesy affiliates, contractors, vendors, consultants, temporary and other workers for ASU and Component Units (Users). This standard applies to all information handled by University employees, and University affiliates, contractors and vendors. Each such entity and individual who creates, collects, records, organizes, stores, adapts, alters, retrieves, uses, processes, has access to, transfers, discloses, administers and/or destroys University information is responsible and accountable for compliance with this standard. University information includes but is not limited to information about prospective, current, and former students, and employees, and other University affiliates, research data, and intellectual property.

<https://docs.google.com/file/d/0B7bqVGx3GJQbM2JwMFIkdI91clk/edit>

GetProtected's Additional Information

- Using public Wi-Fi and hotel internet
- Mobile Device Security Checklist
- Links to FBI's Business Travel Brochure
- Portable Storage Devices Security Checklist



Send questions to:

edops@asu.edu

ASU Mary Lou Fulton
Teachers College
Arizona State University