This guide will help you pass the quiz for the ASU Information security training (Jul 2013 - Jun 2014).

This guide covers all 33 questions in the quiz pool. Only 15 questions are randomly selected from the pool when you take the quiz. Therefore, there is information on this guide that you will not be asked about.

You may take the quiz as many times as you wish. You need a score of 12 or better to get credit for taking the class.

**Topics**

**Email**

One way you can get a virus is by opening an email attachment. The bad guys have gotten pretty clever at making email look like it comes from someone you know and is safe to open. Make sure first, by checking with the person who sent it to you!

Email can be forged so that it looks like it came from your Mom (or anyone else). Or she might have a virus that is trying to spread itself to your computer. If you're not expecting an attachment, check with the sender before you open it.

An email message from the Spanish Lottery is most likely an example of phishing, an attempt to gather personal information such as your credit card number, Social Security number, Paypal account, or email password for the bad guy to use in identity theft activities. Most companies (and ASU) would never send you an unsolicited email message of this nature.

ASU's Computer, Internet and Electronic Communications policy prohibits electronic communications (e.g., email) that are anonymous (no identity) or pseudonymous (fake identity). For details, see the policy at [http://www.asu.edu/aad/manuals/acd/acd125.html](http://www.asu.edu/aad/manuals/acd/acd125.html)

**Phishing**

Phishing is an attempt to gather personal information such as your credit card number, Social Security number, Paypal account, or email password for the bad guy to use in identity theft activities. It often involves an email message urging you to "update your account information" using a very official-looking Web site.

Remember, if it sounds too good to be true, it probably is. Retaliation is against ASU's Computer, Internet and Electronic Communications policy (not to mention a few laws), and the sender is likely to be an innocent victim anyway. The best
thing to do with a phishing message like this is to forward it with headers intact to antiphishing.org. Or you can just delete or ignore the message.

**Infosec crime**
People break into computers for many, many reasons. Even if you don't keep any sensitive information on your computer, the computer itself might be useful to someone who wants to attack another computer without being traced, or to someone who wants to distribute illegal software, pornography, movies or games.

**Viruses**
Different viruses are designed to cause different kinds of mischief, even using your computer to cover a criminal's tracks. This is why it's important to protect your computer from viruses even if there is no sensitive or important information on your computer.

**Physical Threat**
Any time there is a credible physical threat, you should contact law enforcement for assistance. In an emergency, dial 911. In a less urgent situation, dial (480) 965-3456 to reach police on any ASU campus.

**Inappropriate use of computers**
Harassing people via email, sharing passwords, swapping MP3s ripped from your CDs are all in violation of ASU's policy governing Computing, Internet, and Electronic Communications. All of them can result in disciplinary action. See the policy at [http://www.asu.edu/aad/manuals/acd/acd125.html](http://www.asu.edu/aad/manuals/acd/acd125.html)

Use of ASU computer resources for private business or commercial activities, fund-raising or advertising on behalf of non-ASU organizations, is a violation of ASU's policy governing Computing, Internet, and Electronic Communications (ACD125) and can result in disciplinary action. See the policy at [http://www.asu.edu/aad/manuals/acd/acd125.html](http://www.asu.edu/aad/manuals/acd/acd125.html)

**Passwords**
Cracking passwords takes some time, so changing your password frequently can help keep bad guys from getting access to your personal information and logging into computer systems as you. You should change your ASURITE password at least once every semester, or every six months.

You are responsible for anything that occurs with your userid/password or from your computer. KEEP IT TO YOURSELF and KEEP YOUR COMPUTER SAFE.
Suspended Privileges
Upon receiving notice of a violation, ASU may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings.

When you signed up for your ASURITE id, you agreed to ASU's Computer, Internet and Electronic Communications policy, which, among other things, prohibits "negligent or intentional conduct leading to disruption of electronic networks or information systems." In accordance with this policy, ASU can and will disable your network access if you allow your computer to impact network performance. See the policy at http://www.asu.edu/aad/manuals/acd/acd125.html.

ASU Web Hosting
According to ASU's Computer, Internet and Electronic Communications policy, ASU Web pages may be used only for ASU business and only authorized individuals may modify or post materials to these pages. No other pages may suggest that they are University Web pages. If confusion is possible, pages should contain a disclaimer and links to ASU sites. See the policy at http://www.asu.edu/aad/manuals/acd/acd125.html.

Wireless Networks
Wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services, is prohibited unless approved by an authorized network administrator. This includes creating your own wireless network using a wireless hub at ASU. The good news is that ASU provides free wireless network coverage across all campuses.

ASURITE ID
Your ASURITE userid and password are the key to many online services at ASU. You should never supply your password in an email message. ASU staff will never, ever send you a message or initiate a phone call asking for your password. Nor will ASU staff send you a program as an email attachment and ask you to run it. If you receive a message of this nature, don't open it and don't respond: It's a scam.

InfoSec Incidents
Information security incidents include theft, damage, or unauthorized access to data or physical IT assets including servers, workstations, and media; abuse of authorized access to services, information, or IT assets; And evidence of a network attack from inside or outside the university.
**Protecting your computer**

When leaving your computer unattended for a short time, you should always lock the system, log out, or use a password-protected screen saver. When leaving it unattended for a longer time, you may prefer to shut it down.

Physical access usually implies data access. Given unfettered physical access to a computer, a criminal may boot the computer from a CD or USB device and access the disk directly, or even steal the disk from the computer.

**ASU Hotline**

The ASU Hotline is a third-party service that allows you to report potential safety issues or non-compliance issues anonymously. See [http://hotline.asu.edu](http://hotline.asu.edu) for further information.

**Handling Sensitive Information**

Information of a sensitive nature should not be stored on local hard drives, personal USB devices, electronic mail, unsecured Web sites, or any place where unauthorized people may have access. ASU's centrally provided network servers are secured and backed up regularly. Other suitable options may exist in your unit; consult the technical staff in your area if you wish to know.

Your department may have procedures for handling specific types of information based on laws or regulations that apply to your area, such as FERPA, HIPAA, or PCI. Your best resource to find out about those procedures is the deskside support staff in your department.

Except for archiving required by law, sensitive information should not be kept if it's no longer needed. Nor should it be transmitted via email or unsecured Web sites, nor saved locally on personal devices. Sensitive information should be backed up securely and should be encrypted in storage and in transit wherever possible.

For information on storing data in the cloud, review the helpful checklist in ASU's Data Storage Guidelines, available online at [getprotected.asu.edu/governance](http://getprotected.asu.edu/governance).

Your departmental management controls authorization to access department-specific information resources. This is usually addressed in new-hire procedures, but you may find that you need to request additional access from your supervisor. Your computer support staff can help you gain access after you've received the appropriate authorization.

To learn more about Personally Identifying Information and how to keep it safe, review the Data Handling standard at [getprotected.asu.edu/governance](http://getprotected.asu.edu/governance).
Classifying ASU’s data

ASU’s Data Classification Standard, which identifies types of information and responsibilities for handling sensitive information, is available to read on getprotected.asu.edu.

The Data Handling standard classifies information according to how sensitive it is and provides guidelines for handling information based on that sensitivity level. For more information, read the standard online at getprotected.asu.edu/governance

Reporting an Information Security Incident

Information security incidents include theft, damage, or unauthorized access to data or physical IT assets; abuse of authorized access to services, information, or IT assets; or evidence of a network attack from inside or outside the university. To report an information security incident, open a CRM case for UTOSECISUE.

If you’ve witnessed a possible incident, here’s what to do. First, determine whether any sensitive information might have been exposed. Refer to the Data Handling standard for help with this, and ask the Information Security Office for guidance if in doubt. Next, contact the ASU Help Desk to report the details.

You’ll probably want to notify your management as well. The Information Security Office will determine how to classify the situation and where to route it for investigation and response.

Security is Everyone’s Responsibility!

As outlined in ACD125,
- Security is everyone’s responsibility
- Everyone is required to keep their own credentials protected and safe
- Individuals who manage university servers, applications, and technology resources are responsible for securing those resources