This guide will help you pass the quiz for the ASU Information security training (Oct 2014 – Jun 2015).

This guide covers all 26 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 see on the quiz.

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

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. Even if you get unexpected email from a friend with an attachment, you should confirm that the sender really did send the message.

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 Infosec@asu.edu. Do NOT click on any links, download or open any attachments. You can check https://getprotected.asu.edu for recent phishing attacks at asu.

If you have opened an attachment or clicked on a link that you think is “phishy”, report it to the ASU help desk and ask your desk side support staff to help you assess if your computer has been infected.

You can tell that a message or web page is “phishy” by seeing if the URL matches to webpage content, by seeing if the sender of the message matches the content of the email and by verifying with the sender that they did actually send the message.

Remember, that ASU’s email team will never, ever ask you to send them your password over email…. Ever..

Virus Protection

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. If your computer is infected by a virus, it might attack other computers, steal information, and delete important files.

ASU offers free virus protection software for your use. Start at https://getprotected.asu.edu and look for the antivirus section.

- For ASU-owned windows PCs, use Forefront Endpoint Protection
- For home-owned windows PCs, use Microsoft Security Essentials.
- For ASU-owned Macintosh computers, use ClamXav.
- For ASU-owned Linux computers, use ClamAV.

In order for an antivirus software to protect you, it must be running, set to scan routinely and provide real-time scanning of downloads and files on access.

To see if your antivirus software is running: On a PC, look in your software tray in the lower right corner of your desktop. On a Mac, look for a shield in the top toolbar.

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 for options.

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 desk side support staff in your department.

One type of sensitive information is called Personal Identifiable Information or PII. Example of PII include: Insurance transactions, medical records, grades, transcripts, schedules, rosters, driver license, credit card and social security numbers.

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 https://getprotected.asu.edu/governance

To learn more about Personally Identifiable Information and how to keep it safe, review the Data Handling standard at https://getprotected.asu.edu/governance

ACD Computing Policy

According to the computing policy, these are examples of inappropriate use of ASU-owned computers: Sending harassing or intimidating emails, sharing your password with friends, bosses or co-workers, swapping MP3s ripped from your favorite CDs, using the computer to run non-ASU businesses.

ASU can suspend your computer privileges if you violate University policy. Everyone is responsible for creating a safe and stable computing environment.

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 every 180 days.

You are responsible for anything that occurs with your userid/password or from your computer. KEEP IT TO YOURSELF and KEEP YOUR COMPUTER SAFE.

When setting up your password, it should contain three of four types of characters: upper case letters, lower case letters, numbers and symbols. It should be at least 10 characters long, should not be found in the dictionary, and should be different from your bank account password.

The internet of things

Remember that if you can get to one of your devices through the internet, then bad guys may be able to as well. To prevent unauthorized use of your device, change the default password of the device, use only encrypted connections, and unplug when you are not using the device.

Incidents Management

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. Examples of incidents include: the theft of your ASU laptop from your car, your department server slowing down and showing pages of unknown content, students using the network to share advanced (and illegal) copies of a test.

To report an incident, call the help desk at 1-855-278-5080.

The first thing you should do if faced with an information security incident is to determine whether any sensitive information might have been exposed. If so, immediately call the help desk for next steps.