In-Person Information Security Training: A Preference Amongst the UTHSC Community

by The UTHSC Information Security Team

Though it is 2015 and we are at the height of the technology age, nevertheless, many prefer conventional interaction. The 2015 Information Security Training is offered via Blackboard so users may access and complete it at their leisure. However, some employees and students would rather take time out of their busy schedules to attend one of several In-Person Information Security Training classes. Information Security Training was created to provide awareness for the UTHSC community in the area of secure computing. It is our mission to provide you with training and tools to ensure you meet policy requirements while changing human computing safety behaviors and reducing risks.

During in-person training, attendees are able to interact with the instructor, ask questions, and give honest feedback. The instructor also stays after the training for fifteen minutes for one-on-one questions. Because of in-person training, requests to present detailed Information Security seminars to respective department, college or unit have increased. Topics ranging from password management to secure emailing are all vital areas that affect our organization daily.

You may attend in-person training. Please visit the UTHSC HR Training Portal and enroll a 2015 Information Security Training session.

You can also begin the computer-based training by logging into UTHSC Blackboard and accessing the 2015 UTHSC Information Security Training course.

For current students, faculty, and staff, training must be completed by February 15, 2015. For more information, visit http://uthsc.edu/its/information-security/training.php, contact the UTHSC Information Security Team at (901) 448-1579 or itsecurity@uthsc.edu.

In-Person Information Security Training

Do you have 1001 questions regarding information security? In-Person Information Security Training classes are becoming popular due to the increase of technology usage. Read how you can take advantage of in-person training.

Patching and Updating

In this newsletter we explain why you must check for updates, and what you can do to protect yourself.
Patching and Updating: Is Your Computer Up-to-date?
by L. Kevin Watson of the UTHSC Information Security Team

You have probably noticed that your computer at work and home prompts you to restart due to updates once or twice a month. Several other applications, like Adobe Acrobat, probably prompt you for updates as well. These updates are a critical part of maintaining a secure and stable computer. These patches or updates address issues that the publisher has found, some are performance or stability related, others are due to security vulnerabilities. Both are very important. Having your computer crash that leads to the loss of an important file, or having that file stole are outcomes that no one wants. Hackers use these unpatched vulnerabilities to break into computers all over the world every day.

Patching and updating your computer software is very similar to car maintenance. If you don’t do them, eventually, your car (and computer) will cease to work. Updating your applications has become more important that updating your Windows or OSX in the last 7 or 8 years. More hacks leverage problems within installed software than problems with the Operating Systems themselves. You can liken monthly patching to an oil change. Relatively quick, and little changes are visible once you are done.

The bigger updates, Service Packs/Apple named updates (like Mavericks) are more like car brake work. They take longer, and can have a bigger impact on performance, security and features that patches. The last category of updates, retiring of versions, is a bit harder for most people to grasp. However, do you know many people who drive a car daily that requires leaded gasoline? Like leaded gasoline, some technologies run their course, and become obsolete. Windows XP is a recent example, about a year ago, support ended. To prepare for this, we moved every machine we could off Windows XP, and took special precautions with the few that could not be replaced. This would be the equivalent of keeping a few classic cars requiring leaded gas for car shows, and using a special lead additive so the car will run correctly. While ok for a classic car you take out 4 times a year; it is not something you want to do for a daily driver.

Later this year, Windows Server 2003 is reaching End of Support. This will happen just after the new fiscal year for UT starts. To manage this issue, we will be migrating every server running Windows Server 2003 that can be upgraded to a later Server Operating System, and taking similar special precautions with those that cannot be. If you manage such a server, the time, and haven’t started planning a migration, it is definitely time to start.

Most people don’t enjoy monthly updates. They seem to always come at an inconvenient time. Some people put them off for months whenever possible. Using our parallel example of cars, can you imagine not changing your oil for a year or two? People who change their oil that often buy new engines instead of changing 24 month old oil since it typically is destroyed from dirty oil. Leaving your computer behind on updates carries a similar risk. Updates are a good idea, but they are also mandated by some of the laws that govern our institution. HIPAA requires us to not use End of Life Operating Systems for computers uses for electronic Protected Health Information (ePHI).

For more information regarding secure computing, contact the UTHSC Information Security team at (901) 448-1579 or itsecurity@uthsc.edu.