UTHSC G.U.A.R.D.

September 2017

IN THIS ISSUE

Changes Coming for Information Security Training

by Chris Madeksho, Information Security Coordinator

Information Security Training and Awareness is a core part of a foundation of a safe environment. A community is only as strong as its weakest link. If there are users on campus that are not aware, or have not been trained in Information Security, we all are at risk. In the past, UTHSC Information Security Awareness Training was required training that happened every year. However, if a person decided not to take the training, there were no consequences for this decision.

Starting with this year's 2017-18 Information Security Awareness Training, those employees new to the campus (hired on or after October 01, 2017) will not be permitted to access the network until their training is complete. When an attempt is made to log into the network, the system will check Blackboard and confirm that the user has completed the course. If the course is not complete, the user will only be able to access Blackboard to complete the training. After training is complete, the user is free to access the UTHSC network.

For those users who are not new to campus, i.e. have a start date on or before September 30, 2017, refresher training is required. When a deadline has been set for everyone to complete the training, it will be announced campus wide. Everyone will be given ample opportunity to complete the refresher course if it has been assigned to them.

If a current employee does not complete the training before the deadline, network access will be discontinued for that employee until they complete the training. Therefore, complete the training as to not lose network access.

Further communications will be delivered via digital signage and email notifications. If you have any questions regarding the training, do not hesitate to contact the Information Security Coordinator, Chris Madeksho at mmadesh@uthsc.edu or 448-1579.

Information Security Training is Mandatory

Get information on what is changing for Information Security Training on campus

How safe are you socially?

With many social media outlets these days, how can you spot the scammers?

Staying Secure on Social Media

by Chris Madeksho, Information Security Coordinator

Scams and malware that take advantage of social media users and platforms are becoming more and more common. Social media scams are easy to create and can target thousands of people at once due to how users interact with pages, posts, and contacts. Once your account is compromised, it can be used to spread scams and malware to your network of friends or contacts. Facebook, Twitter, LinkedIn, and Instagram are a few common examples of social media sites where you or your account could be at risk. Here are some ways that you can keep your social media accounts more safe through smart online practices.

Shortened URLs are a common tactic used by scammers to conceal where malicious links lead since many social media sites have a character limit. Never enter your login credentials in a website that you linked to from a social media post, message, or email. Malicious websites that look like the real thing are often used to steal login credentials to compromise accounts. Never enter your login credentials in a website that you linked to from a social media post, message or email.

Fake coupons are another tactic scammers use commonly on social media platforms. The scammers create a fake coupon requiring you to click a link to download it and put the coupon on a malicious website that can infect your device with malware.

Click baiting is another scam where a "teaser" is used to get you to click on the link. For instance, it might suggest a really interesting story ("you won't believe what happened next…"), challenge you ("I bet you can't…)," or promise a "giveaway" or "sweepstake." With the sweepstakes and giveaways, the scammer creates a fake website giving away a product. They then post the link on social media, directing users to the website to take part in the giveaway. Once there, you may be prompted to enter information, thus exposing your personal data. Treat these with the same skepticism as other suspicious emails and messages.

Consistently ask yourself if what you are reading is too good to be true. Look for spelling errors in the scams. Also, avoid friend request from people you do not know. If you do not trust it, delete it. For more information about staying safe in the social media arena, contact the Information Security Team at itsecurity@uthsc.edu or (901) 488-1579.