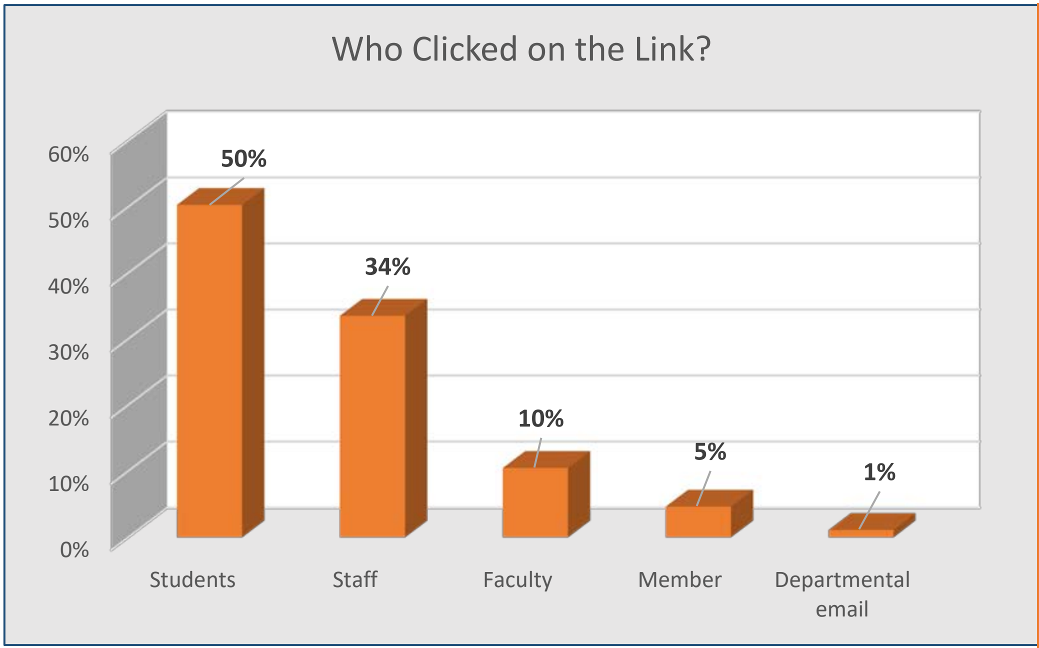
UTHSC G.U.A.R.D.

December 2017



Phishing Testing Results Campus Wide

by Chris Madeksho, Information Security Coordinator

Phishing is the fraudulent attempt to obtain sensitive information, such has credentials or other sensitive information. Phishing attempts usually are in the form of an email, but can be via other forms of communication, such as a text message, social media, or a verbal conversation (also known as social engineering).

Because phishing attempts are so wide spread and are sometimes very hard to recognize, the Information Security Team was tasked to test the entire UTHSC campus community with fake phishing schemes to see who would catch the bait and fall for the phish.

In 2017, every email address at UTHSC was sent a phishing email to measure how many users would click on a link and give away their NetID and password. In total, 14,739 email address were tested. Out of those, 1013 people (6.87%) clicked on the link in the email. Of those that clicked, 506 people (50%) actually typed in their NetID and password.

Users who fell for the phish and clicked on the link got an email from me as the Information Security Coordinator letting you know that you were caught in the phish, but that your credentials were not compromised (this time). If you did not get an email from me, you passed the test. The graph above shows the percentage of users based on classification that clicked on the link.

New hires and new students were also tested within the first three months of getting their email address. People new to the campus were more willing to click on links found in emails. Out of the 3460 new email addresses added in the first three quarters of this year, 466 people (13.47%) clicked on the link. Of those that clicked, 299 people (64%) gave away their NetID and password.

Partially based on these statistics, new hires cannot access the network until they have completed their Information Security Training. If you would like more information about the testing program or the results found, please contact the Information Security Team at itsecurity@uthsc.edu or (901) 448-1880.

IN THIS ISSUE

You Have Been Phished!

Check out the results of the yearlong phish testing

Holiday Scams are out there

Watch out for fake charities and social media scammers

Avoiding Holiday Scams

by Thomas F. Duffy, MS-ISAC Chair

The holiday season is a great time to make charitable gifts to support the causes you care about, and charities often run end-of-year fundraising campaigns. However, criminals take advantage of this fact and run scams and frauds of their own to fool consumers into giving them money instead. Below are some common scams and frauds used by cybercriminals and some tips on how to avoid them. If you can spot these seasonal tricks, you are more likely to ensure your donation goes where you intend it to go.

One of the most convincing ways for cybercriminals to exploit charitable giving is by creating convincing charity websites. These websites are in fact fraudulent and may copy an existing charity's site or use the charity's name and branding. While few techniques are foolproof for detecting fake or malicious websites, try to follow these recommendations:

- Whenever possible, browse directly to the charity by entering the charity's URL directly into your browser's address bar.
- If you are not sure of the charity's URL, an Internet search can help, but instead of automatically clicking on the first link, look at the top few links. If the top link is what you want, great, but if you see several very similar links this could indicate one of them is a potentially fraudulent website.
- Carefully study the website's URL for typos, such as two "v" characters in place of a "w" or an "i" instead of an "l." If you're not sure about a potential typo, try changing to all capitals or a different font.
- Fraudulent charity websites frequently use domain names and email addresses that sound legitimate. You can do a little research into what the correct domain name and email address should be by looking into the organization using resources recommended by the Federal Trade Commission in their charity guide, or through resources like GuideStar, Charity Navigator, and Charity Watch.

Scammers commonly impersonate staff from major charities via social media channels, as this makes it easier for them to impersonate someone else. Avoid making donations through social media and never send your personal or payment information in a social media message. Instead, consider heading directly to a charity's established website.

In addition to traditional charity scams at this time of year, social media is also susceptible to the spread of a variety of pyramid schemes and other charity scams. Pyramid schemes involve the simple but unsustainable premise of receiving more than you give. One of the most common schemes on social media right now involves 7 bottles of wine. You receive the message indicating that to participate you should send one bottle of wine to the person who tagged you and post the message, tagging 6 other people who will each send you a bottle. Another scheme purports to be from a sick child who wants something – holiday cards for example and asks you to send a card and share the post with all your friends so that they will send a card, too. If you come across one of these viral posts, let it stop with you! Don't share it, repost it, or send anything along, and do take a moment to educate your friends!

When donating to a charity, make sure that the charity is a registered charity under U.S. or international tax law. U.S. 501 charities have to make certain information public and you can look the charity and its information up under any of the several charity tracking websites.