Tips to avoid increased phishing scams during holiday season

December 13, 2019 12:00 PM Holly Shawhan
hshawhan@tulane.edu

The Cybersecurity Team in Tulane Information Technology has recently seen an increased number of scams and malicious cyber campaigns impacting the Tulane community. These phishing attempts may come from email, text messages, social media platforms, and online shopping sites. Be wary of emails offering a job/position or those requesting sensitive information—it can lead to fraud and identity theft.

The Cybersecurity Team encourages all faculty, staff, and students to take the following precautions:

• Avoid clicking on links in unsolicited emails, chats, and text messages, and be cautious of any email attachments.

• Save and scan any attachments before opening.

• Do business with reputable vendors.

• Be wary of emails/chats requesting information. Do not provide sensitive information through emails or chat.

• Trust your instincts. If the message or file you receive seems suspicious, do not open it, and report it to security@tulane.edu.

• If you have any concerns that your account may have been compromised, you can reset your password online at https://password.tulane.edu or by contacting the Service Desk at (504) 988-8888 or help@tulane.edu.