

## **New security measure: External emails labeled to reduce email fraud and phishing attempts**

April 16, 2019 6:30 PM Tulane Today staff  
today@tulane.edu

Beginning April 22, [Tulane Information Technology \(IT\)](#) will be adding a notification banner to incoming messages from senders outside Tulane. Most email fraud and phishing attempts originate from external sources. This new banner will help remind members of the Tulane community to take extra precautions when clicking links or opening attachments and to avoid divulging account credentials to an external sender or website.

Attempted email spoofs are on the rise nationwide, and we have been impacted at Tulane. In response, IT is implementing new measures to alert, notify and protect our user community from attempted email fraud and sophisticated phishing. We are working on a comprehensive safety net, and the new external email banners are the first step.

Initial tests have helped us generate a list of trusted non-Tulane sources, such as notifications from Microsoft.com, InterFolio, our voicemail system, Concur, etc., that we frequently do business with and which are also not commonly used for attempted fraud or phishing. With these customizations the banners should be an effective tool in reducing compromised accounts and malware. Fine-tuning will continue as we implement additional protective features to our email system.

As always, when in doubt, contact the Service Desk at (504) 862-8888, or [help@tulane.edu](mailto:help@tulane.edu). Thank you for your patience as we implement these improvements.