CYBERSECURITY COMMUNICATION
Please circulate

August 24, 2017

To: University Cybersecurity Communication Recipients
From: University Systems
RE: Phishing Messages Posing as Voicemail Messages

A number of universities are being targeted by phishing messages posing as voicemail notifications. These messages contain attachments that appear to be the voicemail, but are really a .zip file with malicious software. Some messages contain links that direct users to websites that attempt to install malicious software.

Please remember to examine all email for signs of phishing:

x Does the file extension of the attachment match what you expect? Avoid attachments ending in .wav.zip; these are attempting to hide the true file type.

x Hover your mouse over links included in the message. You can see the URL before clicking on the link. Is the URL a website you trust?

x Did you miss a call? Is the message light on your phone lit? Be suspicious of any message indicating you have a voicemail if there is no evidence to support that you missed a call.

If you have any questions a