Phishing examples

• The following examples are real phishing messages received by Emory in January 2010
• If you receive a suspicious message like these, DO NOT reply, click any links or open any attachments. Just delete the message.
• If you’d like to report the message, you can forward it to abuse@emory.edu.
Phishing emails often motivate people to respond with the threat of an eminent loss of service or money. Some link to a website where the criminal asks for your username and password, bank account information, credit card information, or other information they can use for profit. Often these links are to legitimate sites that were hacked, or ones that were named to sound like a legitimate site.

Sent from a legitimate email address that may have been a phishing victim

Pressuring response with a threat of loss of email service

Using a legitimate website set up with a page that requests your username and password
Other messages ask for you to reply with your password or personal information. These messages often use misdirection to make you think the reply is going to a legitimate email address. Emory will never ask for your password in email or over the phone. If someone at Emory makes this request, notify the IT service desk.

Email reply example

Sent from a legitimate email address that may have been a phishing victim

Asking for a username and password – Emory will not do this

Pressuring response with a threat of loss of email service

Reply email address doesn’t even go to an Emory account