E-mail is an efficient way to communicate with the USNH community and target smaller divisions and departments. Often legitimate institution-wide messages contain critical information and action items. However, they can share the same attributes as a phishing attempt. The similarities can lead to recipients deleting and flagging valid e-mails. Learning to receive messages that look suspicious diminishes one's ability to distinguish between what is genuine and fraudulent. The following guidelines will assist the USNH community in drafting bulk e-mails that smell less "phishy."

A common characteristic of a phishing attempt is a generalized or missing greeting. Personalize the opening, indicating familiarity with the intended audience.

Limit links to pages within the University of New Hampshire System's domains (granite.edu, keene.edu, plymouth.edu, unh.edu, usnh.edu, keene.edu)

If an outside link is required, spell out the link *completely* rather than embedding the link in a picture or text.

Do not link to executable files

A legitimate e-mail that may be confused for a phishing attempt:

From:Payroll@state.edu

Support has been discontinued for the HRIS-based Direct Deposit users are required to migrate to the new MDF-based Payment Information by following the steps outlined below.
All employees using direct deposit verify their bank information.

1. Please visit the _____ service page.
2. Create a user name and password