E-mails That Don't Look Like Phishing

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."

Nothing personal
A common characteristic of a phishing attempt is a generalized or missing greeting. Personalize the opening, indicating familiarity with the intended audience. While institutional graphics are pleasing to the eye, they are not an indication of authenticity as anyone can download an image.

The art is in the details
Similar to impersonalized greetings, phishing attempts tend to be sparse in detail. Referencing a specific date or event adds credibility to mass e-mails, and better yet, is referencing an event with a date.

In case of emergency
Phishing attempts try to induce panic, causing recipients to act before thinking. If urgent or immediate action, consider implementing your institution's emergency broadcast protocol instead of e-mail.

Keep it in house
Avoid including recipients outside of the university system. A wide variety of addresses and naming conventions are characteristics of a malicious e-mail.

Transparency
Using only the "BCC" field prevents recipients from seeing the other addressees and increases suspicion. Take advantage of organizational distribution lists and use the "To" and "CC" fields. If the use of "BCC" is necessary, emphasize content customization.

Don't get attached:
Users are increasingly wary of attachments, and especially if it corresponds with other questionable attributes. If attachments are needed, consider pointing recipients to retrieve documents on a webpage within a USNH institution webpage.

Weakest Link
Many phishing attempts contain links redirecting users to a fraudulent website. Try to incorporate these best practices when including links.

- 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

Please refer to the examples below.

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

No personalized greeting

Recipients are unable to see who else is receiving the message

"Action Required" the use of all capital letters in "DIRECT DEPOSIT" suggests there's an urgency on an important matter

To: Payroll@state.edu
From:Payroll@state.edu
Subject: User Action Required - DIRECT DEPOSIT

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 **MUST** verify their bank information.

Link to an outside webpage

1. Please visit the **MDF PAYMENT** service page.
2. Create a user name and password
3. **Update contact information**
4. **Confirm banking information is correct**

Request for personal and restricted information

Thank you for your prompt attention to this matter,
Payroll Office

No institutional context or reference) other than graphic header

A bulk e-mail incorporating the guidelines listed above

STATE UNIVERSITY

Payroll, Benefits and Tax

Recipients are from institution's Global Address

To: Faculty & Staff GAL
From:Payroll@state.edu
Subject: Payroll Migration update

Subject is specific and references an event that has been previously communicated to the campus community

Greeting specifies intended audience

Greetings State University Community,

The State University Human Resources department appreciates your patience as we continue our financial technology migration. MDF completed the changeover last week. The payroll department recommends that any employee that uses direct deposit verify their bank information is correct in the new system.

Please visit access our web information system **https://www.state.edu/wise** to access MDF's direct deposit allocation.

Link is typed out and directs user to a page on the institutions website

Please contact the HR department if you have any questions

Walk-in: Finance Building 27 State University Drive
Phone: (603) 567-9641
E-mail: **payroll@state.edu**

Provides specific and familiar contact information

Tone is not overly urgent or demand immediate action.

Regards,
Jane Mooney
Senior Payroll Specialist
(123) 456-7891
jmooney@state.edu