PHISHING LESSONS

Phishing is one of the most common cyberattacks against higher education institutions and their students, faculty, and staff. Such attacks can take many forms, but they all share a common goal — getting you to share sensitive information such as login credentials, credit card information, or other restricted and/or sensitive data. Although the University of Utah maintains controls to help protect our networks and computers from cyberthreats, we rely on you to be our first line of defense.

PHISHING

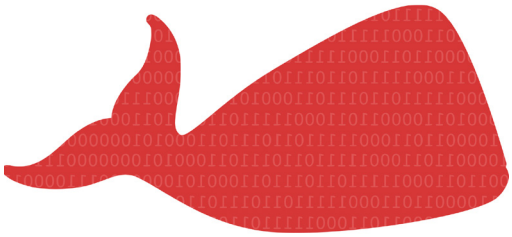
In this type of attack, criminals impersonate a real organization to obtain your uNID and password, or other restricted/sensitive information. You might receive an email asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.

SPEAR PHISHING

Spear phishing is a more sophisticated phishing attack that includes customized information that makes attackers seem like legitimate sources. They might use your name and phone number and refer to the university in the email to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.

WHALING

Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real university employee. Using a fake domain that appears similar to ours, whaling attempts look like normal emails from faculty or staff, possibly even the president or a senior vice president, and ask you for sensitive information (including user names and passwords).



SHARED DOCUMENT PHISHING

You might receive an email that appears to come from file-sharing sites like **UBox**, Dropbox, Google Drive, or **OneDrive** alerting you that a document has been shared with you. The link provided in these emails will take you to a fake login page that mimics the real login page and will steal your account credentials.

WHAT YOU CAN DO

To avoid these phishing schemes, please observe the following email best practices:

- Do not click on links or attachments from senders you do not recognize. Be especially wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal information (like user names and passwords) over email, ever.
- Watch for email senders who use suspicious or misleading domain names.
- Inspect URLs carefully to make sure they're legitimate and not imposter sites.
- Do not try to open any shared document that you're not expecting to receive.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

If you cannot tell whether an email is legitimate, please forward it to **phish@utah.edu** or call your respective central IT help desk: Main campus, 801-581-4000, option 1; University of Utah Health, 801-587-6000.