Field guide to phishing emails

Described below are some characteristics of potential phishing emails. That being said, sometimes companies create legitimate emails that break all of the below conventions.

- **Suspicious sender**

You may encounter emails which have unusual sending addresses. For example, an email claiming to be Microsoft being sent from microsoft@gmail.com would be highly suspicious as official emails would come from a @microsoft.com email address.

- **Suspicious URLs**

Take a close look at the link that an email may be prompting you to click. Do URLs look legitimate, ie. microsoft.com, or does a URL look more like microsoft.weebly.com?

- **Typos or unusual formatting**

The subject line and/or email body could be rife with typos, grammar mistakes, or unusual formatting, such as a random location with   an extra amount of spacing, like this.

- **Sense of urgency**

Phishing emails try to elicit a response from recipients by creating a sense of urgency, such as needing to click a link for an account not to expire, or winning a prize that must be claimed in the next 24 hours. Some even get really creative by threatening you with your password in the subject line and claiming they have more info than just the password (the reality is that the phisher likely obtained your password from a database of account data, and as long as you use different passwords for different platforms, you should have nothing to worry about).

- **Spam label on your email client**

Sometimes, your email client can help you out and place a spam label on emails it’s identified as being potentially spam. This label isn’t always 100% accurate, but can be a helpful reminder at times.

Still unsure about what phishing emails look like? See https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive or type “phishing email database” into your search engine of choice to see some real examples of phishing emails.

What happens if I fall for a phishing email and click a link? Many links may request your login credentials on a fake login page for a service such as your bank, then may use your credentials on a real login page maliciously. However, it’s best not to click on phishing links at all, if possible. Even if the link does not take any malicious action without user input, which could also be possible, some workplaces send employees false phishing emails intentionally to test them, and have policies ranging from extra training to firing after falling for enough security tests.