...IT COULD HAPPEN TO YOU

Phishing attacks may occur in all shapes and forms, in all styles and formats, and in **all** inboxes. That's right...We are talking about **you**!

Now that you are an expert at deciphering potentially harmful emails, let's see if you can harness what you have learned and apply it to your own inbox.

DIRECTIONS:

1. Go back to your computer and open up your email account
2. Take a look at all emails that have been sent within the past seven (7) days
3. Skimming through subjects and messages, grab a piece of paper and make a tally of how many emails could be flagged as "phishing threats"
4. Print a screenshot* of what you deem the most obvious potential threat

*NOTE:

Make sure that the screenshot you use does not contain any personal information. If it does, use a sharpie to block it out after you print it.

DISCUSSION GROUP:

1. Return to your discussion group with two items:
    a. Your tally of potential phishing attacks
    b. A screenshot of the most obvious phishing scam
2. Discuss your findings with the group and see if there are any similarities in your findings.
3. Here are a few questions to spark discussion:
    a. Was there a trend in "sender" information?
    b. What were most common: links or attachments?
    c. Did emails masque the identity of common aliases (common banking institutions, email providers, travel sites, etc.)?
    d. How many emails gave a "red flag" before you even had to open them?