

Identifying Phishing Emails



What is a Phishing?

- Phishing is an attempt to steal information via email through deception and manipulation of a targeted entity
- While Phishing is done specifically through email, there are many other ways people try to steal information. Common ways include:
 - In-person attacks using thumb drives or tailgating into restricted areas
 - Mobile and phone attacks using text messages and calls
- Phishing attacks are not always obvious and the best defense against one is to identify it before it can steal anything

How to Identify a Phishing Attempt

- There are many tell-tale signs of a phishing email. While not all signs will be present in every attempt, any attempt will carry a number of these signs.
- The most common signs include:
 - Suspicious sender email address
 - Unknown additional recipients
 - Significant grammar and spelling errors
 - Requesting that you click a link within the email
 - Strange attachments (i.e. file has a suspicious name or is a .zip file)
 - Requesting sensitive information (such as a password) or asking for money

What to do With Phishing Emails

- Simply viewing a phishing email is not dangerous. Damage can only be done if you click any links, open attachments, or respond to the email itself.
- If you do become compromised by a phishing attempt, immediately disconnect from the internet and run a full system scan using your anti-virus software. If you are unsure how to do this, shut down the computer and arrange for someone to assist you.