TIPS FOR CATCHING A PHISH

DON’T TRUST THE SENDER’S DISPLAY NAME
Just because it says it’s coming from the name of a person you know or trust, doesn’t mean that it truly is. Be sure to look at the email address to confirm the true sender. Better yet, analyze the message header.

CHECK FOR SPELLING ERRORS
Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be. This is typically not the case in targeted phishing attacks.

CONSIDER THE SALUTATION
Is the address general or vague? Is the salutation “To Valued Customer,” or “Dear [insert title here],”?

BE CAREFUL WITH ATTACHMENTS
Attackers like to trick you with juicy attachments. It might have a long name. It might be a fake icon of Microsoft Excel that isn’t the spreadsheet you think it is. Macro enabled documents should be scrutinized.

IS THE EMAIL ASKING FOR PERSONAL INFORMATION?
Legitimate companies are unlikely to ask for personal information in an email.

DON’T BELIEVE EVERYTHING YOU SEE
If something seems slightly out of the norm, it’s better to be safe than sorry. If you see something off, then it’s best to delete or contact the person with a known good contact – email may not be the best method.

CHECK THE EMAIL SIGNATURE
Most legitimate senders will include a full signature block at the bottom of their emails. This is not always the case, but can help verify the legitimacy of an email.

BEWARE OF URGENCY
Urgency through email should not be expected. If the matter is extremely important, typically an email is not the best method of contact.

LOOK BUT DON’T CLICK
Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn’t match what the link description says, don’t click on it.

WHEN IN DOUBT, THROW IT OUT
Deleting a good email is not as bad as introducing malicious content to your network.