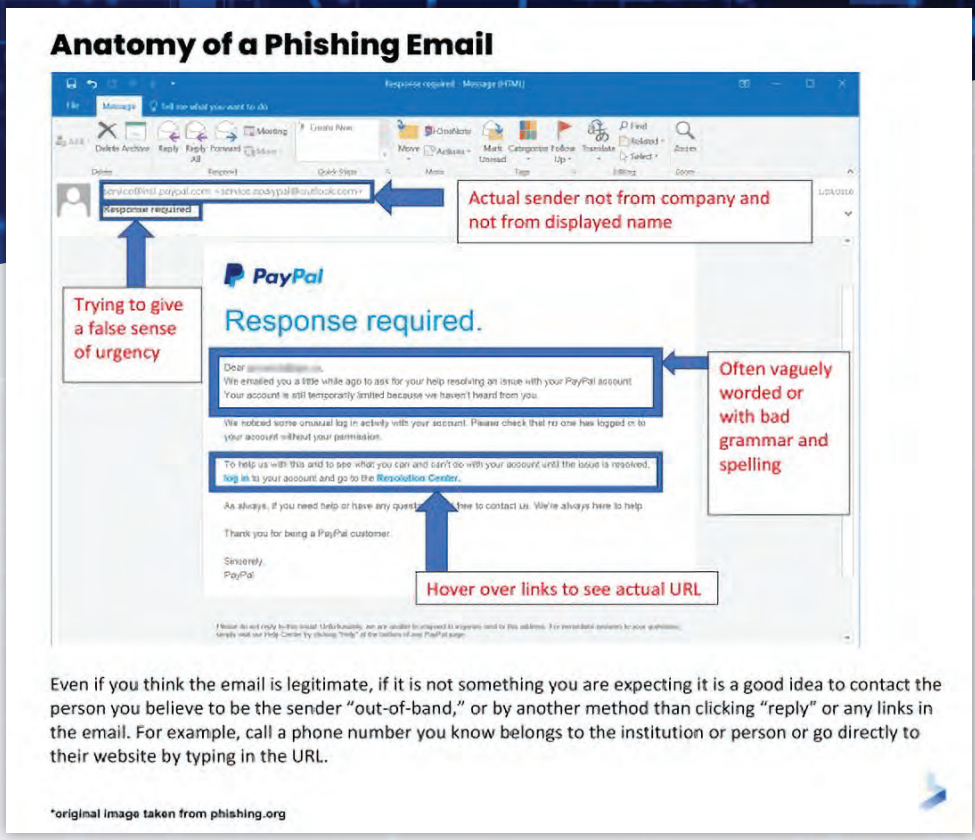
CATCHING A PHISH CAN BE TOUGHER THAN YOU THINK

NOAH L. GIEBEL
MANAGER IT/
SPECIAL PROJECTS

Have you received emails like the one you see here? Phishing scams are one of the most common ways a hacker can gain access to your data and personal information. The goal of Phishing email is to attempt to use various means of social engineering to deceive the recipient into clicking on a malicious link or download a malicious attachment. Social Engineering is the tactic of manipulating or influencing someone for the purpose of gaining access to a computer system for personal or financial gain.



These phishing emails can come in many forms but most recently we have seen an increase in impersonation attacks. An impersonation attack is when an attacker pretends to be a trusted person of an organization for the purpose of stealing data, financial gain or gaining access to a computer system or network.

It's important to slow down and take the time to carefully read through an email before opening attachments, clicking on links or even responding. First look at the sender's email address, is it correct? Next, If the email contains a link, hover over the link with your mouse to validate the credibility of the link. Lastly check the wording and spelling of the email, does the email sound right? If you have questions about the emails validity the best way to prove its legitimacy is to contact the sender. It's tough work catching phishing emails, stay diligent and always remember to **THINK BEFORE YOU CLICK.**