Phishing Protection

How to Spot a Phishing Email

It could be a phishing email if…

• There are misspelled words in the e-mail or it contains poor grammar
• The sender’s name doesn’t seem related to the sender email address
• The message is making you an offer that is too good to be true
• The message is asking for personally identifiable information such as credit card numbers, account numbers, passwords, PINs, or Social Security Numbers.
• There are “threats” or alarming statements that create a sense of urgency.
• The name in the message isn’t the one you’re used to seeing.
• Beware that some phishing emails use attachments (coupons, etc) which can house malware.
• Shortened URLs can present danger. Be careful to verify all web addresses. It is safer to simply manually enter URL’s into your web browser.