

# AVOID THE BAIT & HOOKS OF PHISHING SCAMS



## SUSPICIOUS SENDER



The hacker may use an email address or phone number posing as a familiar source, but it may be slightly different in the details - such as the **top level domain** or phone number sequence.



## UNSOLICITED REQUESTS



The email or text may contain a request for **sensitive information** - even if you have not done business with the sender before. It may request specific passwords, or bank account numbers.



## INCLUDED ATTACHMENTS



The email or text may contain **attachments** that you did not request or that seem out of place. It may request that the recipient download a file or click on a hyperlink.



## NON-PERSONALIZED SALUATATION



The email may address you as "Dear customer" or "Dear valued member" instead of using your **personal name**.