












# HOW TO SPOT PHISHING

Watch out for these signs of a phishing email. If you think you may have been tricked by a phishing attempt, report it right away.

-  A request for you to email sensitive information.
-  An offer that sounds too good to be true.
-  The sender allegedly representing a company uses a personal email address, such as @gmail.com.
-  A message with a strong sense of urgency.
-  A generic greeting, such as "Dear Account Holder" or "Dear Customer."
-  An "official" email with misspelled words and inconsistent graphics.
-  Language that suggests you bypass your company's security policies.
-  A message that attempts to invoke curiosity or fear.
-  An email with an unsolicited attachment.
-  If a link in the text isn't identical to the URL displayed as your cursor hovers over the link.
-  The body of the email is an expansive hyperlink.