12/22/2022
Good Afternoon

Please be aware that we have seen an increase in spam and phishing emails this holiday season. The Cybersecurity firm Trend Micro saw the number of phishing attacks more than double, **growing 137% in the first half of 2022 compared to the same period in 2021**, according to the firm's 2022 Mid-year Cybersecurity report
Please remain vigilant and always ask the questions before opening an attachment, clicking a link, or responding to an email.

When you receive a new email, always verify

- Did the email come from an appropriate sender, and it matches the subject matter?
- if there are attachments, do they look correct?
- Is it an unexpected call to action? (Your boss asking you to give them your cell to call you, asking your assistance in an odd manner, etc.)
- Are there misspelled words, improper grammar, etc.?
- If there is a link, hover over the link but don't click it, does the link match where it says it would be going?

Asking these questions will key you in on whether the email is of a questionable nature pretty quickly. If you ever suspect an email of being spam, you can forward it to the helpdesk for review.

If you would like to learn more about recognizing illegitimate emails, I have included a link to a resource from the FTC. It is thorough in covering the many ways to determine if an email is spam or not.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

LINK TO HOLIDAY DINNER TABEL TOPICS

Joe and the rest of the Tech Team wish you a Happy Holidays and relaxing vacation