EMAIL SECURITY BEST PRACTICES

KnowBe4
Human error. Conquered.

DO NOT

Open any email attachments that end with: .exe, .scr, .bat, .com, or other executable files you do not recognize.

"Unsubscribe" - it is easier to delete the e-mail than to deal with the security risks.

Never click embedded links in messages without hovering your mouse over them first to check the URL.

Respond or reply to spam in any way. Use the delete button.

ALWAYS

Check the email 'From' field to validate the sender. This 'From' address may be spoofed.

Check for so-called 'double-extended' scam attachments. A text file named 'safe.txt' is safe, but a file called 'safe.txt.exe' is not.

Report all suspicious emails to your Information Technology help desk.

Note that www.microsoft.com and www.support.microsoft.software.com are two different domains. (and only the first is real)