Email Security Best Practices

DO NOT open any e-mail attachments that end with: .exe, .scr, .bat, .com, or other executable files you do not recognize.

DO NOT ever click embedded links in messages without hovering your mouse over them first to check the URL.

DO NOT "unsubscribe" – it is easier to delete the e-mail than to deal with the security risks.

DO NOT respond or reply to spam in any way. Use the delete button.

KnowBe4
Human error. Conquered.

ALWAYS check the e-mail 'From' field to validate the sender. This 'From' address may be spoofed.

ALWAYS report all suspicious emails to your Information Technology help desk.

ALWAYS 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.

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

DP Solutions
Problem Solved.

KnowBe4 PREMIER PARTNER

410.720.3300 | www.dpsolutions.com