Quick Tips to Avoid Being a Victim of Social Engineering in the Office or At Home

• ALWAYS check the email ‘From’ field to validate the sender. This ‘From’ address may be spoofed.

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

• ALWAYS note and verify the domain name of the websites you visit or that are revealed in embedded links. For example, www.microsoft.com and www.support.microsoft.software.com are two different domains. (and only the first is real).

• NEVER open any email attachments that end with: .exe, .scr, .bat, .com or other executable files you do not recognize.

• NEVER “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 and verify the domain is safe/secure.

• NEVER respond or reply to spam in any way. Use the delete button.