





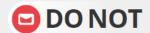
open any email attachments that end with:
.exe. .scr. .bat. .com. or other evecutable. files you do not recognize.



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



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



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





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.



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