Email Security Best Practices

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

**ALWAYS** do not click embedded links in messages without hovering your mouse over them first to check the URL.

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

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

**ALWAYS** do not “unsubscribe” - it is easier to delete the e-mail than to deal with the security risks.

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

**ALWAYS** do not respond or reply to spam in any way. Use the delete button.

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

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

**ALWAYS** do not “unsubscribe” - it is easier to delete the e-mail than to deal with the security risks.

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

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

**ALWAYS** do not respond or reply to spam in any way. Use the delete button.

© 2019 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.