**Email Security Best Practices**

**DO NOT**
- Open any email attachments that end with `.exe`, `.scr`, `.bat`, `.com`, or other executable files you do not recognize.
- Ever click embedded links in messages without hovering your mouse over them first to check the URL.
- “unsubscribe” - it is easier to delete the e-mail than to deal with the security risks.
- 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.)

© 2016 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.