Security Tips:

Are you worried about ransomware?

That's smart - you should be.

What are some ways YOU can avoid introducing malicious software?

TIP WEEK 1: DO NOT open any e-mail attachments that end with .exe, .scr, .bat, .com, or other executable files you do not recognize.

TIP WEEK 2: ALWAYS check the email "From" field to validate the sender. This "From" address may be spoofed.

TIP WEEK 3: DO NOT ever click embedded links in messages without hovering your mouse over them first to check the URL.

TIP WEEK 4: 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.

TIP WEEK 5: DO NOT "unsubscribe" - it is easier to delete the e-mail than to deal with the security risks.

TIP WEEK 6: **ALWAYS note that www.microsoft.com and www.support.microsoft.software.com are two different domains - and only the first is real.**

BE SMART. BE SECURE.