Think you are getting scammed?

Remember the acronym “SLAM”!

S (Sender) – Does the sender’s name include both a first *and* last name? Is the email address actually owned by the company or person who sent it?

L (Links) – Do the links included in the email look like they’re from a legitimate company?

A (Attachments) – Does the email contain attachments? If you have answered “yes” to the last 2 criteria for a scam email, *don’t open anything attached to the email*.

M (Message) - Does the message include any grammar errors or misspellings interfering with its meaning? Does it include any odd, powerful, or threatening words?

If you have answered “yes” to these critera, the message you received may be a scam.

<u>Remember the two golden rules of scam messages:</u>

1. Never click on a link included in an email or text message. Go directly to the website instead.

2. **Never** call or write the sender of a suspicious email, text message, or phone call back.