Email Spoofing - Can you be fooled?

People are getting better at identifying regular phishing emails and questioning suspicious emails that ask them to click a link or open an attachment. Fraudsters may have realized this and have added features to make it more hazardous and harder to recognize scams by using spoofed email.

Email spoofing is used in spam and phishing emails to trick you into thinking a message is coming from a person you know or an organization you trust. How? The sender forges the email headers so the unsuspecting victim sees the fraudulent sender address they recognize, usually marked "Urgent" or time-sensitive to make them feel rushed, or they will add "RE:" to the email - this is called "Prepending" - and it helps fool them into believing it's an email response or an "ASAP" situation.

A quick check of the email, graphics, and contact information all look correct. That company email has its logo, and the login link has its domain in it to look legitimate, just like when you logged in before, so you follow the instructions in the email only to realize you've been scammed!

What more could you do?

- **Check the email addresses more closely -** is anything misspelled, or is something missing or added from the regular email address?
- **Check the subject line -** this is an excellent way to tell right away if the email is legitimate or not. Anything that is unusual or doesn't make sense should be followed up with the person directly before any action is taken.
- **Look at the links -** hover over them and make sure you can tell where they're going. Better yet, go directly to the websites with an address you know is good, and then go to the login page from there.
  - » **Note:** if a link is sending you to a file share site, like Google Docs or Dropbox to pick up a document, it doesn't make the document any safer. You may not be opening it from your email, but it doesn't mean there couldn't be a malicious link in it waiting for you anyway.
- **Look at the content as well -** similar to the subject line, this can give you an indication that it's not legitimate. If the request, comments, or a piece of information does not make sense or is not the normal style you're used to, then don't take chances. Either contact the person directly or the company to verify the email. Then report it and delete it.

Looks can be deceiving. Copying a website or recreating a fake login page to steal a person's credentials makes it harder for most of us to detect scams since we don't think like criminals. If it comes from a familiar name, like a co-worker, a boss, or a company we recognize and use that needs something urgently, the response is usually to get them what they say they need as quickly as possible. Taking a little more time to stop and think - really check some of the details - could save you, your family, and your company from unwelcome consequences.