Suspicious E-mails

The companion PDF file **22 E-mail Red Flags** describes 22 red flags to help you determine whether an e-mail is legitimate or not. Even if you don't consider all 22 red flags, you can always note these three things:

1. Always ask for independent confirmation (such as a phone call or message) before clicking and opening any suspicious document. A quick confirmation is simply due diligence today.
2. Report anything suspicious. If you accidentally executed anything that you later became suspicious about, report that as well. Don't be embarrassed that you were fooled. Given the sophistication of the attacks, anyone -- even security experts -- can be tricked today.
3. Question any unexpected e-mails asking for credentials or to execute programs. Having employees question your legitimate e-mails is a welcome symptom of a good e-mail security education program.

Some telltale signs of suspicious e-mails include but are not limited to:

- Unrecognized/unofficial email address
- Prompts such as "Urgent Action Required" or threats
- Prompts for personal information such as passwords
- Generic greetings such as "Dear Member" instead of your name
- Overly formal greetings
- Foreign origins
- Bad English and spelling errors
- Run-on sentences
- Needless use of initial capital letters
- Improper use (and almost no use) of punctuation
- Needless use of centering text
- Overly solicitous efforts to send us millions of unearned dollars or to sell us dubious products.

Do not open e-mails from unknown senders; those e-mails may contain viruses and other malware. If an e-mail comes from a known sender but includes a suspicious attachment, do not open the attachment. Contact the sender first to verify the e-mail and attachment are legitimate. Do not click on unfamiliar links as they may direct you to a malicious website or automatically download malicious files or programs.

If you get suspicious e-mails, your only available two actions to take are:

1. Forward any suspicious e-mails to junk@office365.microsoft.com , and then
2. Right-click the e-mail and select **Junk -> Block sender**.

Never forward suspicious e-mails to anyone in DNR.