

7 EMAIL RED FLAGS

1. From

- If you do not know the sender personally
- If the email is from someone you don't regularly communicate with
- If the email looks like it might be sent from someone you know, but it's very unusual that they would be contacting you

2. To

- Cc'd on an email sent to more than one person who you don't know personally
- The other email recipients are an unusual mix of people
- If all the names on the email send list start with the same letter

3. Date

- Date and time of the email is abnormal (such as outside of business hours)

4. Subject Line

- Are there typos in the subject line?
- Is the email a reply to something that you never sent?
- Does the subject line not match the content of the email?

5. Content

- Does the email not make sense or have bad spelling errors?
- Are you being asked to click on a link to gain something?
- Is there a negative consequence associated with not clicking the link or opening an attachment?
- Many phishing emails will claim to have an embarrassing picture of you or someone you know

6. Hyperlinks

- Did you receive an email with no message and just a long hyperlink?
- The hyperlink has a misspelling of a website you're familiar with
- When hovering over the hyperlink with the mouse, it is directing to a different website than expected (DO NOT click, just hover over)

7. Attachments

- The attachment is not expected or file name doesn't fit with the content of the email message
- A true .txt file cannot contain malware. However, hackers may attempt to disguise a .txt file name to make it malicious.

