Checklist—Protect Yourself Against Phishing Attacks

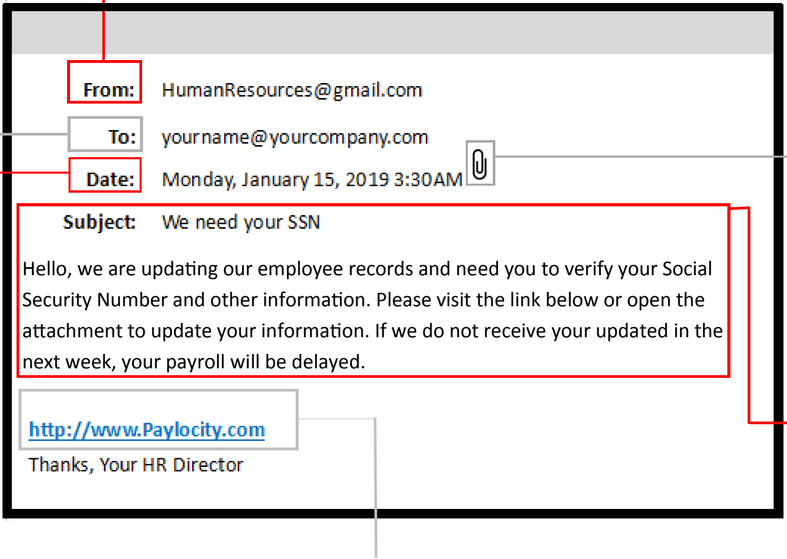
Evaluate, Examine, When In Doubt DO NOT Click!

FROM

- Do you know the sender
- Does the full email address of the sender match the one you were expecting or are there subtle changes made to the person's email address?
- Does the email seem out of character for the sender

TO

- Were you one of many recipients in the office to receive the email and no one is familiar with sender
- Was the email sent to multiple people in my organization, but the group is unusual or all the last names start with the same letter



From: HumanResources@gmail.com

To: yourname@yourcompany.com

Date: Monday, January 15, 2019 3:30AM

Subject: We need your SSN

Hello, we are updating our employee records and need you to verify your Social Security Number and other information. Please visit the link below or open the attachment to update your information. If we do not receive your updated in the next week, your payroll will be delayed.

http://www.Paylocity.com

Thanks, Your HR Director

ATTACHMENTS

- Does the email contain an attachment with one of the following extensions; .exe, .scr, .bat, .com, .zip or other extensions you don't recognize
- Does the email contain an attachment that was unexpected

SUBJECT/CONTENT

- Is the sender asking for some type of action such as; reply, click on a link, open an attachment or forward the email
- Is the request out of the ordinary for the sender or does it contain misspellings
- Does the email claim that negative consequences will occur if action isn't taken
- Does the content of the message match the subject line

HYPERLINKS

- Does the hyperlink have a misspelling or missing letters for well known websites? For example: www.micrsoft.com or www.netflecs.com.
- When you hoover over the hyperlink, the web address is different from the entity sending you the email **(Huge Red Flag)**

DATE

- Does the date sequence make sense (Would your HR Director typically email you at 3:30 AM?)