Cyber Security 101

How-to Spot a Fraudulent E-Mail

There are key things you can look for when you receive an unexpected email from an unknown source or an email from a known source that doesn't quite feel like the sender's usual tone/correspondence style.

Below are a few items you should check, before responding or clicking any links in emails:

- Take a close look at the email address. One character changes the entire domain and is an easy way for hackers to make recipients trust the source.

  Julia Pineda <julia@stratus-gp.com>

- If your name does not appear in the "To:" section of the email, it was likely sent by blind carbon copy (BCC:) and may have been sent to a large number of people at once.

  JP Julia Pineda <julia@stratus-gp.com>
  To:

- If they ask you to take actions that are unusual in standard business practices (create your own Zoom account) or (reply to a generic email account "...@gmail.com"), these actions may be to gain access to (hack) your computer system.

  You are to setup a Zoom account and add his email to your contacts (hr.petergray@gmail.com)

- Any time an unsolicited email tries to create a sense of urgency to prompt you to take immediate action, you should ask yourself why they are trying to rush you.

  You are to setup a Zoom account and add his email to your contacts (hr.petergray@gmail.com) and once you've added him, you're to send a message right away to proceed with the job briefing and interview.

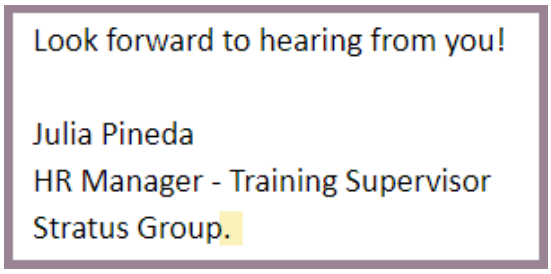
- Phrases that seem out of place may also indicate the sender is not legitimate. The samples below include "and training is available" after stating an interview will be conducted online. Ask yourself, "Training for what?"

  This interview will take place online and training is available.

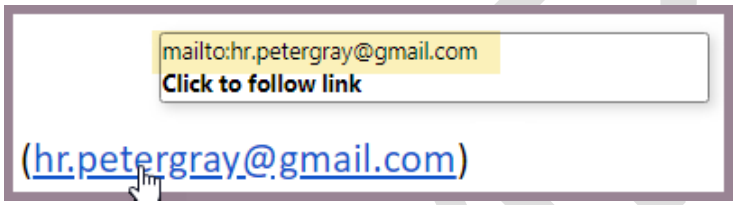
Cyber Security 101

How-to Spot a Fraudulent E-Mail

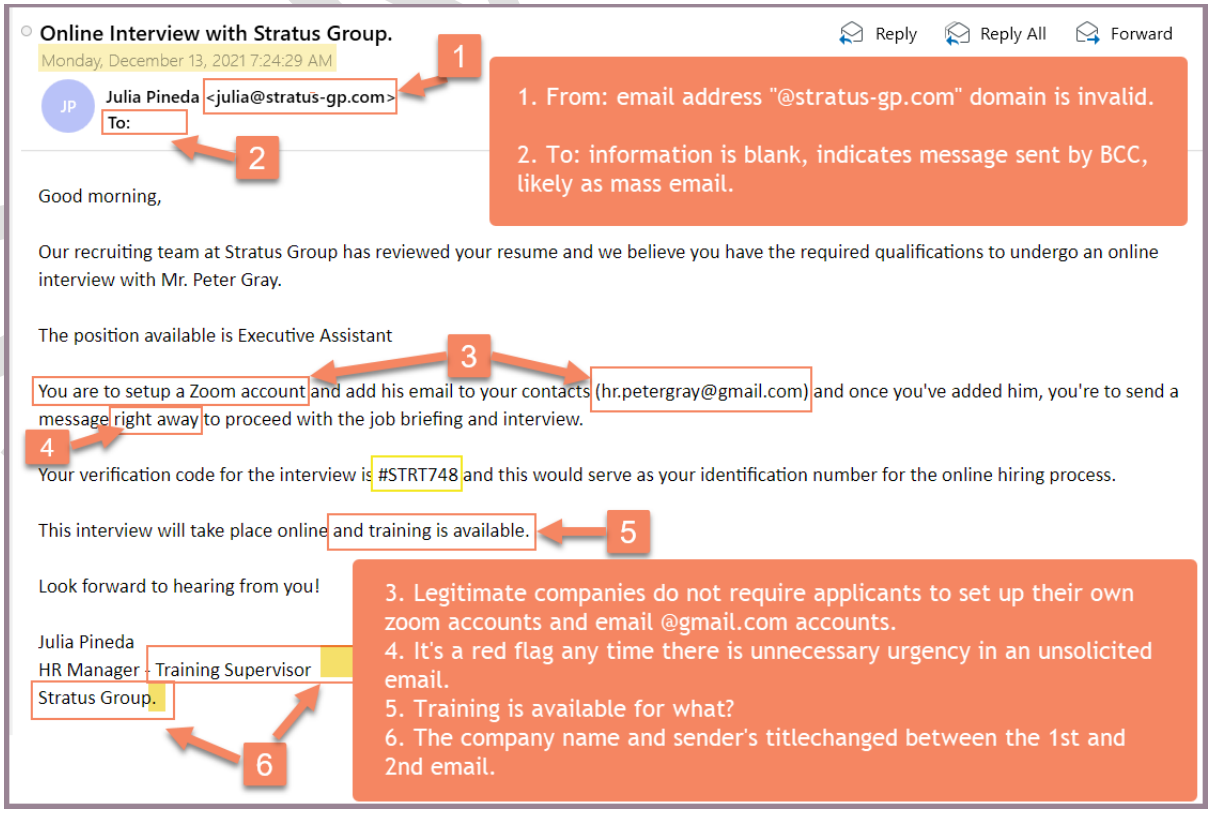
- Verify the signature line. If the email appears to be from someone you know, does it look the same as other emails they've sent you? If the message is from an unknown/unsolicited sender, is there anything odd about the signature information?



- Be extremely careful about clicking links! Even if the rest of the items above seem legitimate, is there a reason for the sender to include a link?
    - **Before** clicking a link, hover the pointer over the link and verify where the link is sending you!



FRAUDULENT EMAIL SAMPLE:



By: Julia Wilkes
12/13/2021