Phishing Email Quick Tips

One of the most prevalent types of cyberattacks is the use of phishing emails. This action continues to be very successful due to its reliance on manipulating people's trust. It only takes one individual to click on a malicious link for attackers to infiltrate university databases in order to get their desired outcome – whatever this may be.

Several phishing attempts have recently been directed at our campus community. These scams may request the recipient to update banking information, purchase gift cards or wire money.

- **Please do not respond to these emails or click on any links.**
- If you have received any suspicious emails, please email **informationsecurity@pvamu.edu**.
    - Please attach a copy of the email as an attachment to be evaluated

---

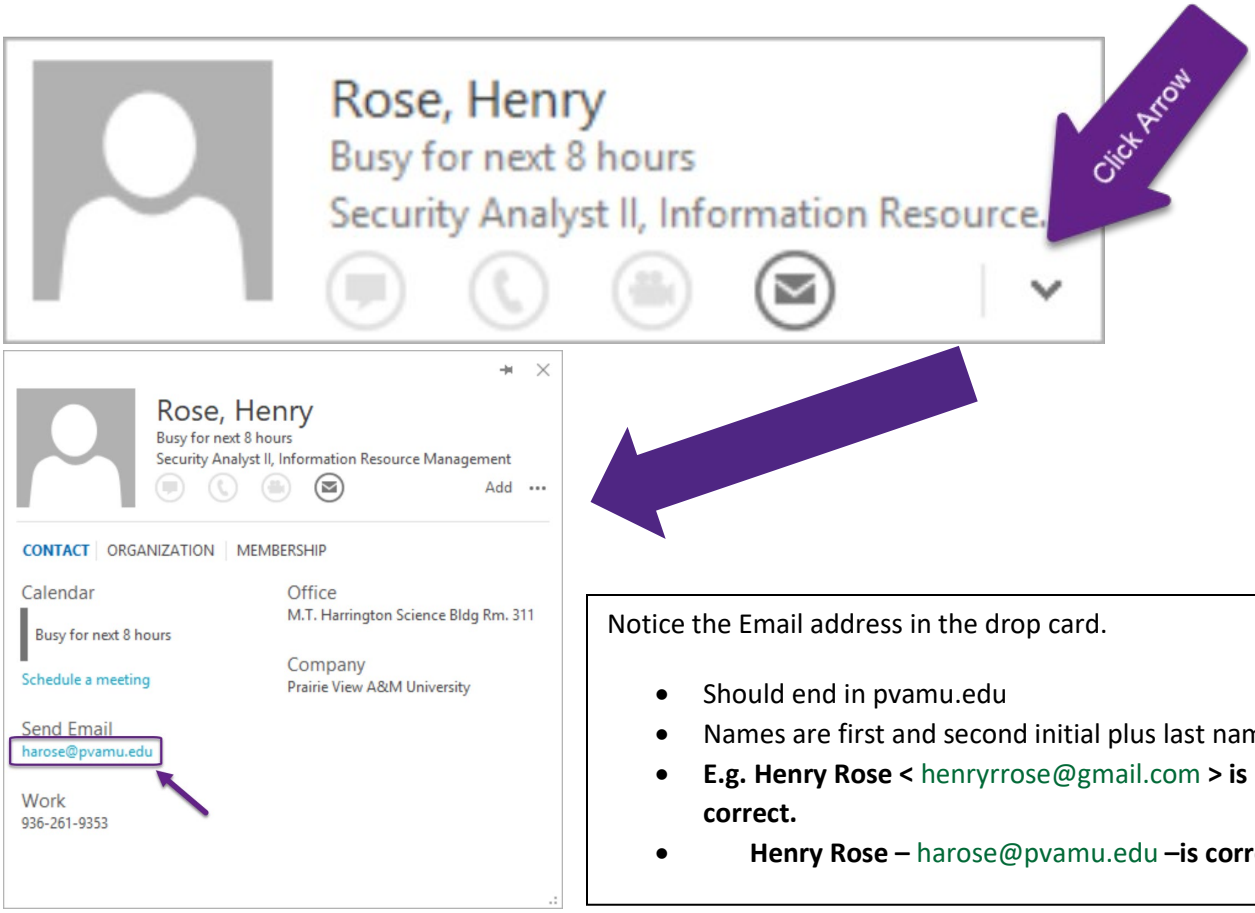
Quick Tips to Spot a Phishing Email

If an email ask you to make changes to personal information such as passwords and account information:

- When updating any information in SSO or any other System, do not click on a link to go the page. Always access the page by typing in the URL.
- Confirm any emails that request you to update a user's account information with the user by selecting the user's email from outlook contacts and/or calling the user. **Do not reply back to the email that you received.**
- Any requests to wire money to an account or to purchase gift cards should follow system, university and departmental procedures. Confirm any emails that request you to purchase gift cards with the user by selecting the user's email from outlook contacts and/or calling the user. **Do not reply back to the email that you received.**

If the email address of the sender appears to be incorrect, or seems suspicious:

- Attackers will often try to use the name of a person, department or organization you are familiar with.
- If the email address is not present in the "**From**" line, verify the address in outlook by right-clicking on the sender name and select "view contact information." **(See the images provided)**.
- **The email should be from @pvamu.edu.**
    - Watch carefully for subtle variations
        - Ex: Pv.edu or pvamu.org or pvamu.com or pv.com or pv.org



Notice the Email address in the drop card.

- Should end in pvamu.edu
- Names are first and second initial plus last name.
- **E.g. Henry Rose <** henryrrose@gmail.com **> is not correct.**
- **Henry Rose –** harose@pvamu.edu **–is correct**

Look for grammatical errors:

- Other clear signs of phishing attacks are grammatical and spelling errors in emails that you receive.

There's a suspicious attachment or link:

- If you receive an email requesting you to click on a link or to download an attachment from a user that you are not familiar with, try to contact the user by some other method other than email.
- Even if you know the user but you were not expecting any attachments or links from them you should contact the user through another email address or over the phone.

The email has an urgent tone and is designed to make you panic:

- Emails requesting you to update your password or to verify your account information within a short period are often signs of a phishing attempt.
- If you are note sure on the authenticity of an email, contact **informationsecurity@pvamu.edu**.

The email is not addressed to you:

- If you receive an email with an urgent tone that is **not** specifically addressed to you, this may be a phishing email.

There is an external banner at the top of the email:

- Prairie View will be adding a banner to all emails that are not from a Prairie View email addresses. If you receive an email that appears to be from a PVAMU employee but has this banner at the top, contact **informationsecurity@pvamu.edu**.
- A copy of the banner is below.

> **CAUTION:**This Email is from an EXTERNAL source. Ensure you trust this sender before clicking on any links or attachments.