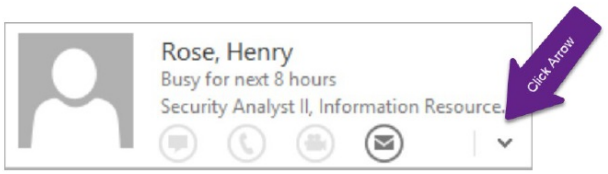
As we approach the end of the semester, we are experiencing an increase in scamming and phishing attempts. Scammers are actively trying to cash in on an unsuspecting public who are spending more time online than ever before. The latest scams are currently targeting our students, faculty & staff through email. These emails are all geared toward getting YOU to respond or take some type of action.

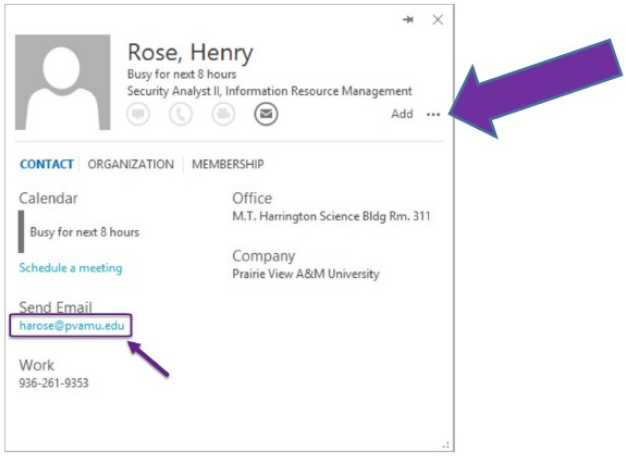
Tips for Spotting a Phishing Email

The email address of the senders appears wrong.

- Make sure the email is from a pvamu.edu account.
  - Watch carefully for subtle variations.
    - Ex: Pv.edu or pvamu.org or pvamu.com or pv.com or pv.org
  - We have seen an increase in emails using PV usernames but being gmail.com or outlook.com.
- Attackers will often 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 following the steps below.



1. Right click on the name and click on the down arrow pointed out.



2. Then check the email address listed in the box on the left hand side.

Notice the Email address in the Drop Card:

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

Look for grammatical errors or unanticipated attachments or links

- Another clear sign of phishing attacks are grammatical and spelling errors in emails that you receive.
- 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 asks 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 or by calling the user.

Do not reply back to the email you received.

- Any requests to wire money to an account or purchase gift cards should follow system, university and departmental procedures. Confirm any emails that request you 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.**

Beware of the "Are You There" or the "Faculty Evaluation" Scam from your Boss

We are still seeing the 1 sentence emails that appear to be coming from your boss or someone in authority with a name that you will recognize even if you do not recognize the email address.

- These emails typically say simply "**Are you there?**"

Once you respond to this email the following will happen:

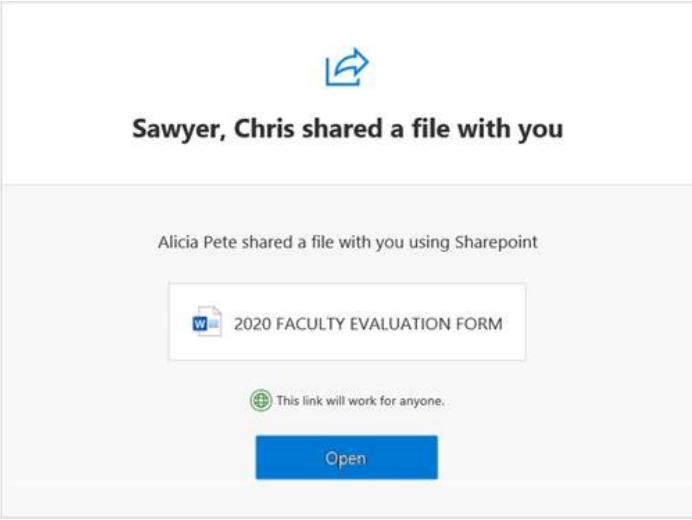
1. **The sender will respond (as the authority figure) saying that they are currently in a meeting with no cell phone access and that they need you to run an errand for them. The sender may also try to get a cell phone number so they can text you instead of communicating via email.**
2. **The errand will be for you to go into town and purchase several "Gift Cards" that your boss needs. You will be told that you will be reimbursed as soon as you can get together.**
3. **You will then be asked to scratch off the codes on the back of the cards and to email those codes to "your boss" who is actually the scammer.**

Once you have performed the above 3 steps – the scam is complete. The sender turns out to not be your boss - the gift cards have already been spent and you are now out whatever amount of money it is that you spent on the cards.

A sample of the Faculty Evaluation Scam Email:

The scam email notifies you that there is a faculty review awaiting your attention.

PVAMU *does not* communicate faculty evaluations through google docs or drop box.



DO NOT FALL FOR THIS – these types of scams are way more common than you might think and they have been around for a very long time. They continue to be used today for one simple reason - **BECAUSE THEY WORK!**

Prairie View A&M University will never send these types of emails to you. If you are

receiving these types of email from someone with a pvamu.edu address - you can be sure that that the sender has already been phished.

Forward anything that you don't think looks right to us at informationsecurity@pvamu.edu and we will quickly get back to you on whether or not it is valid. If it is a scam then we can also take immediate measures to shut them down.

NOTE: In Nearly all Cases where you are Suspicious -Your Suspicions will be Correct

Reach out to us with any questions or if you see anything suspicious,

Henry Rose
Security Analyst II
Center for Information Technology Excellence
informationsecurity@pvamu.edu

PVAMU CITE

PDF of Email