Tips for detecting Spear Phishing emails and action to take.

1- **The 'Subject'**

The subject of these emails usually attempts to make it seem like an urgent or critical matter.

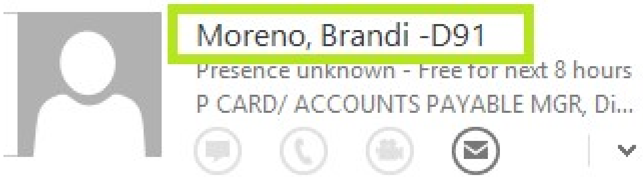
2- **The 'From' address** (from within an open email)

The 'From' address attempts to make it appear that it is from someone you know, like friends or co-workers. See examples below

When viewing a message in Outlook, or Outlook Web App, the 'From' address will be displayed.

It is important to know that in our district, the '**From**' address will always take the district standard format, (*last name, first name* –D91). So for me, Eric Bodily, the format would be "Bodily, Eric –D91".

a. Example 1 shows a '**From**' address that is correct and uses the standard format for district user accounts.

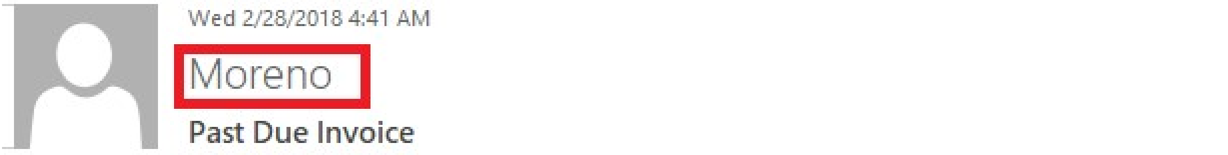


Moreno, Brandi -D91

Presence unknown - Free for next 8 hours

P CARD/ ACCOUNTS PAYABLE MGR, Di...

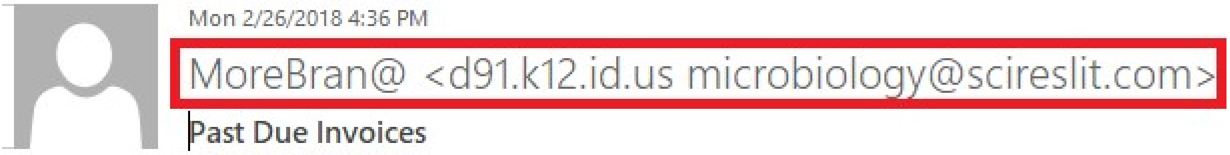
b. The following two examples show a '**From**' address that is spoofed and not real because they do not use the standard format shown in the first example.



Wed 2/28/2018 4:41 AM

Moreno

Past Due Invoice

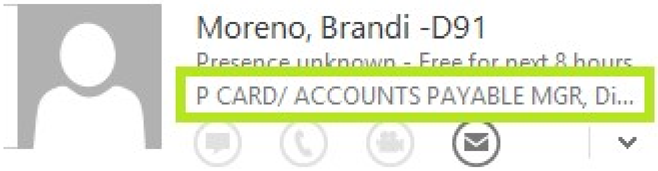


Mon 2/26/2018 4:36 PM

MoreBran@ <d91.k12.id.us microbiology@scireslit.com>

Past Due Invoices

By **double clicking** the '**From**' address that uses the standard format for district user accounts will open a detailed window with district specific information about the sender.

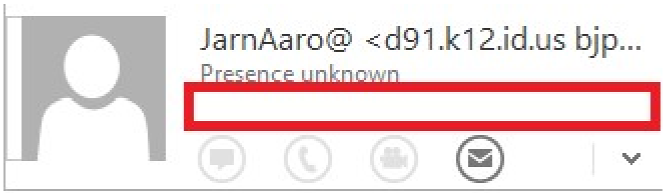


Moreno, Brandi -D91

Presence unknown - Free for next 8 hours

P CARD/ ACCOUNTS PAYABLE MGR, Di...

Double clicking the '**From**' address that is spoofed, and a detail window does not open, or a window opens and displays **no** <u>district specific</u> information. This indicates this email is not from anyone in the district and has a highly probability of being sent by a cybercriminal impersonating a trusted sender. In this example the impersonated trusted sender is our own Aaron Jarnigan.



JarnAaro@ <d91.k12.id.us bjp...

Presence unknown

3- The 'main body' of the message

a. Most of these emails will start by addressing the recipient by the same name that appears in the 'To' address, (*last name, first name* –D91).

   It would be highly unlikely that someone writing you or me an email would use this standard district format. Would you ever write an email to me by starting it with "Hello Bodily, Eric –D91"? Neither would I!

b. These Spear Phishing emails will almost always have a link that will take you to a secluded website where bad things can and do happen. Just as in real life, there are places in this world that we just should not visit.

c. Finally, the cybercriminal will very often close the email by using the impersonated trusted senders standard district format, or even sometimes the email address as shown in these two examples.

Reguards Moreno, Brandi –D91	or	Thanks MoreBran@d91.k12.id.us

   Also very unusual ways to close an email.

Though these are some very good ways to determine the authenticity of a <u>vast majority</u> of received **Spear Phishing** messages, some of these types of email will not be easy to detect. If you have messages that you're not sure of, ask your building tech, or open a ticket, and let us take a closer look before you click on any links within these emails.

And remember, "When in doubt, throw it out!"

Reguards
Bodily, Eric –D91... Just kidding. ☺

Eric H Bodily
Systems Administrator
Ext: 50558