

Quarterly Security Awareness Newsletter



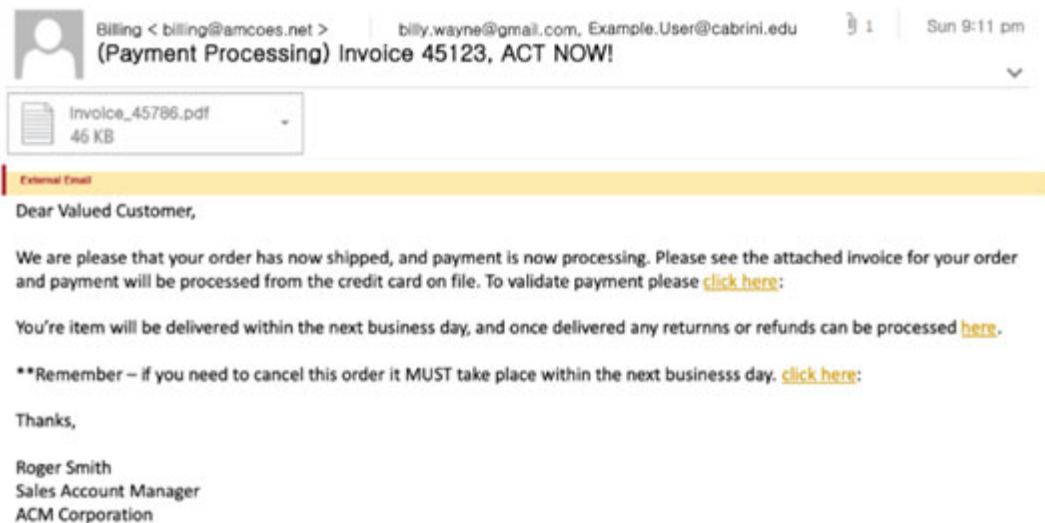
Malicious Email Red Flags

Email is still the primary tool used by hackers to either infiltrate your organization or your personal computers and devices. Understanding the red flag warning signs from a malicious email message can not only save yourself a tremendous amount of time and headache but also protects the organization from potential data breaches and exposures.

Scenario: You've just arrived to work and opened your email only to find this email message.

There are 8 warning signs found within this email example.

Can you
Spot Them
All?

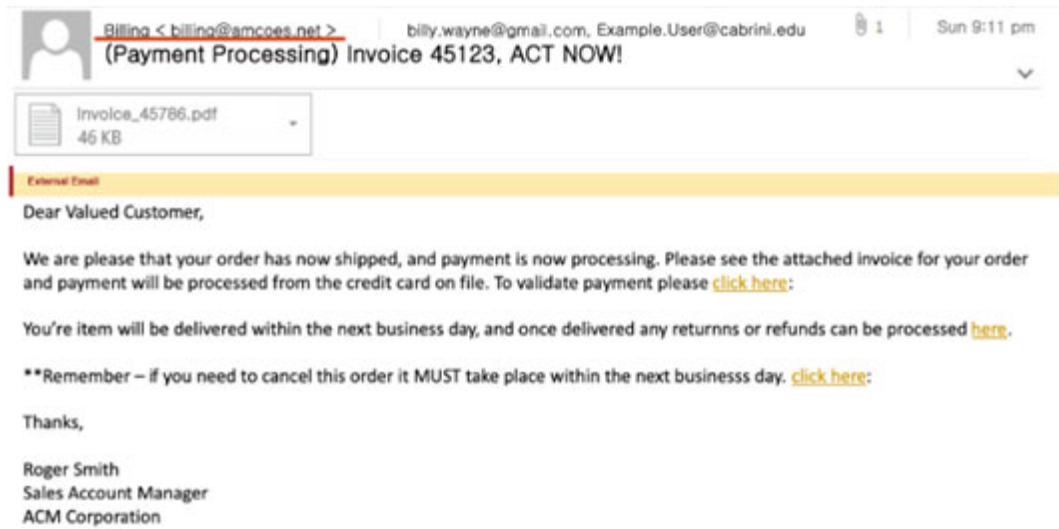


Red Flag Warning 1:

The **FROM**
line

An email originated from someone you don't know may be malicious, especially if the message seems odd or not specific to your job role. In this case, the email is

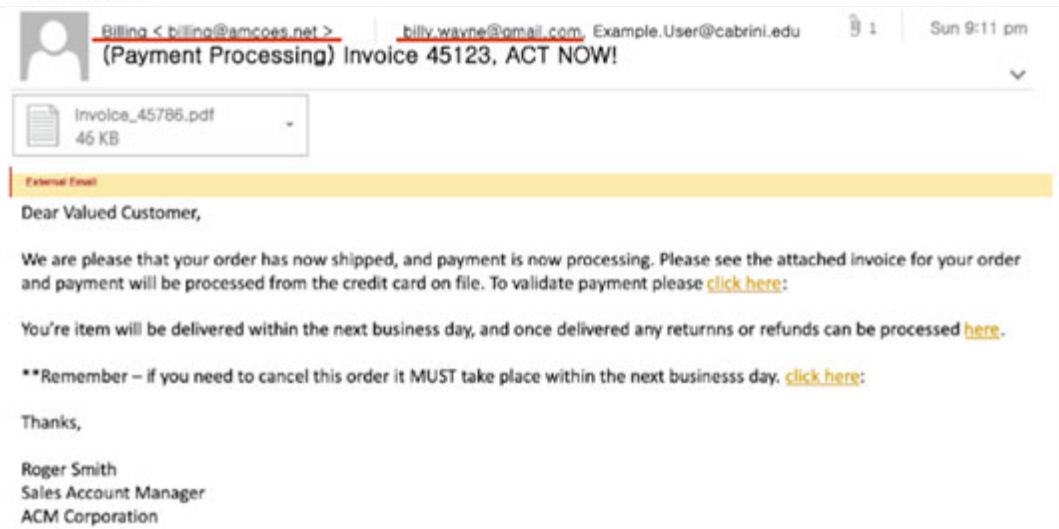
about an order that you have made, but you do not work within the procurement department.



Red Flag Warning 2:

The To line

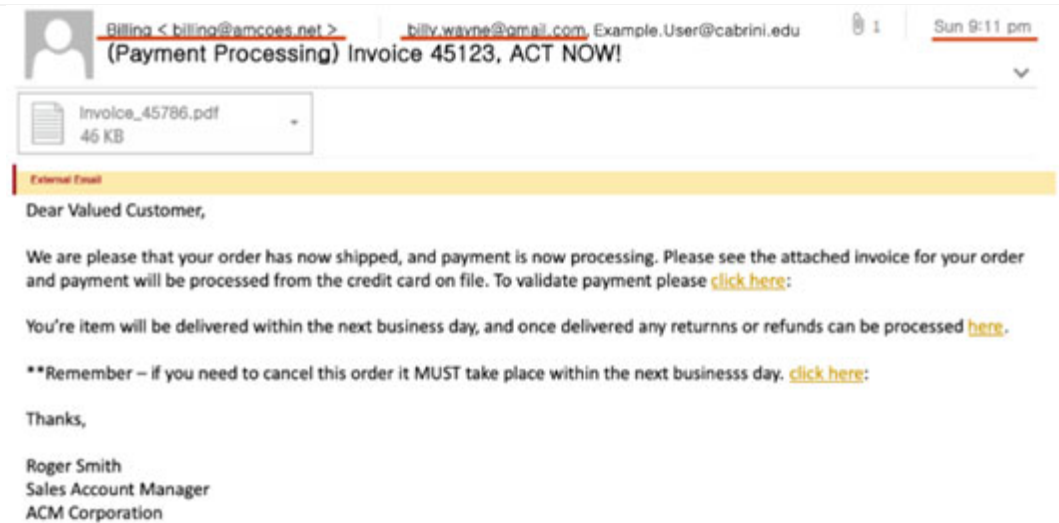
Reviewing the others receiving this email message can also be a red flag warning. If you do not recognize these individuals, especially if these individuals are not part of Cabrini, should alert you to be wary of this message.



Red Flag Warning 3:

The Date line

The time an email is delivered can be an indicator. If the receipt of the email does not fall within normal working hours, this may be another sign.



Red Flag Warning 4:

The Subject line

When the subject does not match the context of the email message, this should be an alert that something is not right with this message. In the case of the example, the subject line indicates a different number than the attachment has.

Billing <billing@amcoes.net> | billy.wayne@gmail.com, Example.User@cabrini.edu | 1 | Sun 9:11 pm
(Payment Processing) Invoice 45123. ACT NOW!

Invoice_45786.pdf
46 KB

External Email

Dear Valued Customer,

We are please that your order has now shipped, and payment is now processing. Please see the attached invoice for your order and payment will be processed from the credit card on file. To validate payment please [click here](#):

You're item will be delivered within the next business day, and once delivered any returnns or refunds can be processed [here](#).

****Remember – if you need to cancel this order it MUST take place within the next business day. [click here](#):**

Thanks,

Roger Smith
Sales Account Manager
ACM Corporation

Red Flag Warning 5:

Attachments

Remember, any file that is not a .txt file can contain malicious content. Any attachment you receive that you were not expecting is a definite warning sign.

Billing <billing@amcoes.net> | billy.wayne@gmail.com, Example.User@cabrini.edu | 1 | Sun 9:11 pm
(Payment Processing) Invoice 45123. ACT NOW!

Invoice_45786.pdf
46 KB

External Email

Dear Valued Customer,

We are please that your order has now shipped, and payment is now processing. Please see the attached invoice for your order and payment will be processed from the credit card on file. To validate payment please [click here](#):

You're item will be delivered within the next business day, and once delivered any returnns or refunds can be processed [here](#).

****Remember – if you need to cancel this order it MUST take place within the next business day. [click here](#):**

Thanks,

Roger Smith
Sales Account Manager
ACM Corporation

Red Flag Warning 6:

Hyperlinks (Hovering)

Taking an addition 3 seconds and hovering the mouse over a link can reveal another warning sign. Looking at the destination, is this a place you want to go.

Billing <billing@amcoes.net> | billy.wayne@gmail.com, Example.User@cabrini.edu | 1 | Sun 9:11 pm
(Payment Processing) Invoice 45123. ACT NOW!

Invoice_45786.pdf
46 KB

External Email

Dear Valued Customer,

We are please that your order has now shipped, and payment is now processing. Please see the attached invoice for your order and payment will be processed from the credit card on file. To validate payment please [click here](#):

You're item will be delivered within the next business day, and once delivered any returnns or refunds can be processed [here](#).

****Remember – if you need to cancel this order it MUST take place within the next business day. [click here](#):**

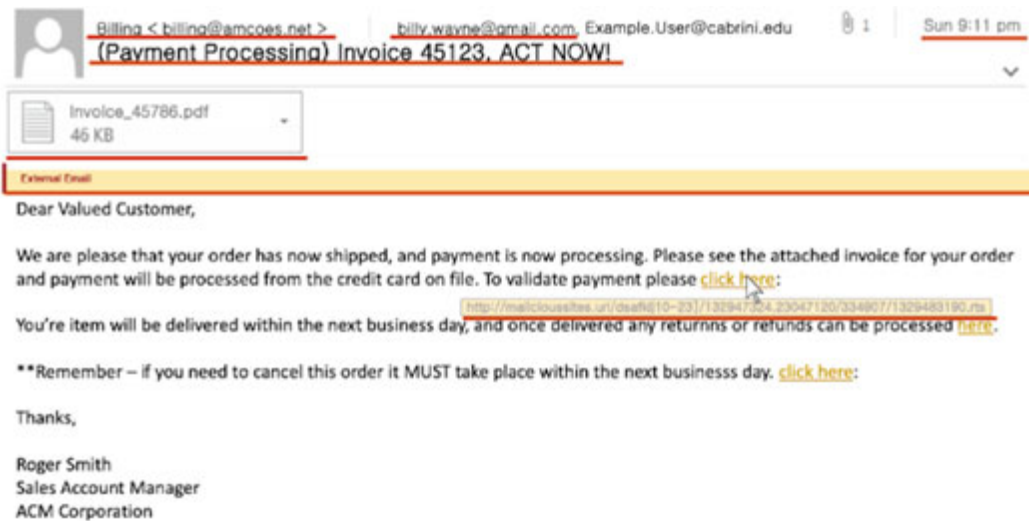
Thanks,

Roger Smith
Sales Account Manager
ACM Corporation

Red Flag Warning 7:

External Email

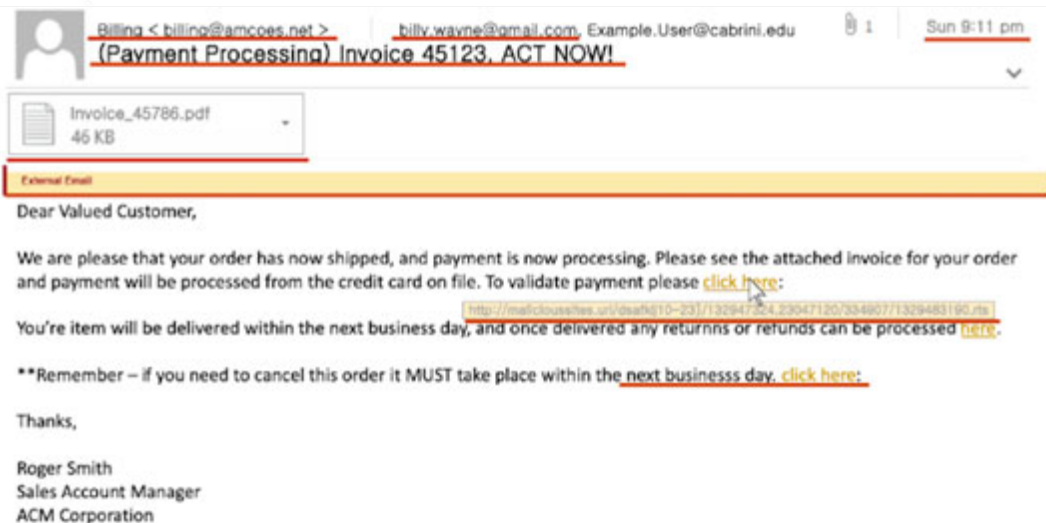
Email originating from outside the organization triggers the **External Email** flag. This automated warning is here to help you identify those messages that require a closer investigation.



Red Flag Warning 8:

Message Content

Is there a sense of urgency, or you feel an emotional pull to click the link, open the attachment, these are signs. Also, don't forget about those misspellings.



Reporting or Reacting to Malicious Email Messages

If you get SCAMMED!

1. Contact the ITR to change your password **IMMEDIATELY!**
 - a. The faster your response, the less likely the attackers will leverage your information against you.
2. Contact IT Security: Security@cabrini.edu
 - a. Be sure to include as much information as possible, so this incident can be investigated.

Reporting Emails with Phish Alert Button

With the suspected email message selected in outlook, find the Phish Alert button on the ribbon:



Once you have click Phish alert, and then **Report**. The email will auto-generate a support ticket, and the suspected messages is moved to your trash.

Reporting Emails without the Phish Alert Button

To assist in the investigation, please forward a copy of the malicious email directly to Security@cabrini.edu.

To forward a copy of an email message:

1. Select the suspicious email message in Outlook
2. Select **More** within the respond section of the ribbon, and then choose **Forward as Attachment**.
(You may also press **CTRL+ALT+F**)
3. Address this message to Security@cabrini.edu and use the subject: **Malicious Message**

