How to Identify Phishing Attacks

How to Identify Phishing Attacks

Note if you believe you have already been compromised by a phishing attack please call the service desk at 206-284-6200 and follow the instructions at the bottom of this article to submit a ticket with the attached phishing email.

Phishing attacks now come in many ‘flavors’ and can be hard to spot. Phishing attacks attempt to steal sensitive information through emails that often look to be official communication from legitimate companies or individuals. Although there are anti-spam solutions, the best protection is awareness and education. Here are several tell-tale signs of a phishing scam:

- **Was the message already in your Junk email folder?** – There are many existing email filters in place that will identify a message as a problem and direct it to Junk E-mail on purpose. This gives you the ability to look for false positives. If the message is already in your Junk folder, it can be safely ignored.

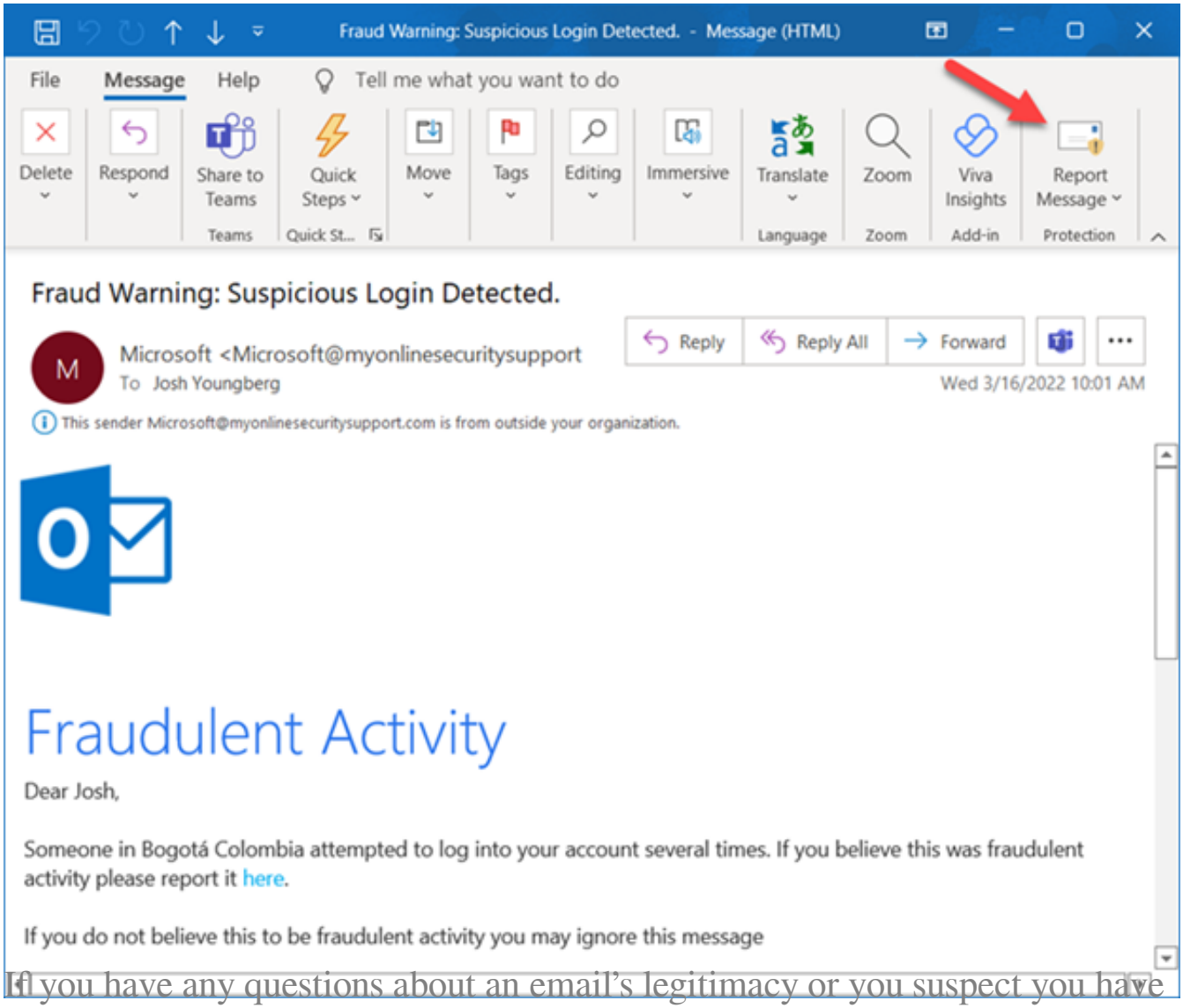
- **Is the message expected?** - If you get a notice from a company saying that your account needs attention, but you haven't used that service in the past it's not likely to be legitimate.
- **Does the Display Name match the sender's email address?** – If the sender's name doesn't match their email address, you should be extra careful.
  Example: " **From:** Mrs Elizabeth Grímsson <lado.chantura@gmail.com>"
- **Is the email specifically addressed to you?** - If a message isn't personalized and is instead titled with something like "Dear Customer" then it's likely part of a mass-mailing and can be safely ignored.
- **Does the email subject include phrases like: "Urgent", "Attention", or "Action Required"** – Many phishing emails attempt to overcome your better judgement by cultivating panic. If you see an email that says something bad is going to happen, take a closer look before clicking.
- **Are the links or URLs not pointing to the expected location?** – Many malicious emails include links that at first glance seem legitimate but take you to a separate website. If you hover your mouse over the link before clicking, you'll be able to see where the link will direct you. In the following example the link looks like it's taking you to "https://www.woodgrovebank.com" but it is pointing to 192.168.255.205/wood.index.htm

What to do next?

Messages that your Microsoft 365 email account marks as junk are automatically moved to your Junk Email folder. However, spammers and phishing attempts are continually evolving. If you receive a junk email in your inbox, you can use the Report Message add-in to send the message to Microsoft to help improve their spam filters.

If you find an email in your Junk Email folder that's not spam, you can use the Report Message add-in

to mark it as a legitimate email, move the message to your Inbox, and report the false positive to help Microsoft improve their spam filters.

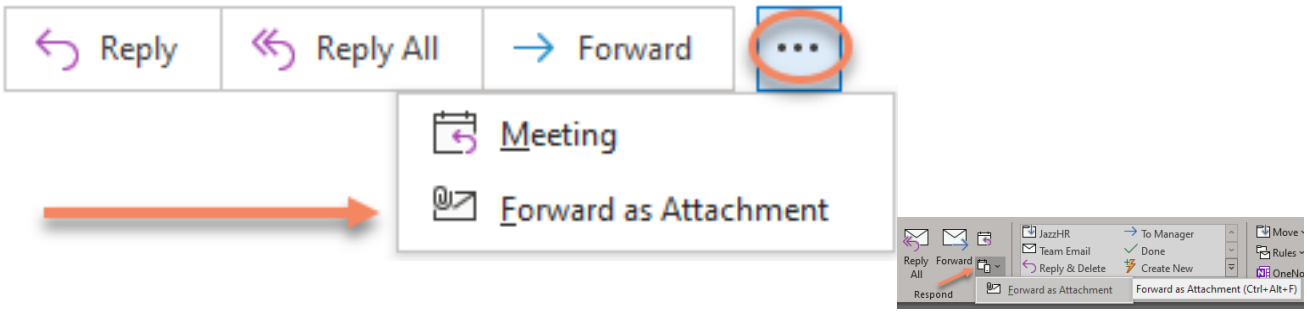


If you have any questions about an email's legitimacy or you suspect you have already been compromised please notify us so we can verify the email.

You can open a service ticket with the following steps. We need a full copy of the email in order to properly do an investigation. :

1. Select the suspicious email
    1. Click on the ellipsis (…) in the top right corner of the Outlook window
    2. OR click on "More Respond Actions" button in the top pane.
2. Select “Forward as Attachment"

3. Send to service@dyncomputing.com



The Support Team
Dynamic Computing, Inc.
1011 Western Avenue, Suite 920 | Seattle, Washington 98104
Main: (206) 284·6200 | Toll Free: (855) 284·6200
service@dyncomputing.com

Custom Fields

- **Article Status:** Specialist Reviewed

Online URL: https://dyncomputing.knowledgebase.co/article.php?id=1420