**Help Keep [Company Name] Secure with New Phishing Reporting Tool**

We are excited to announce a new phishing reporting feature in Outlook that serves as an additional layer of defense from phishing attacks and empowers you to keep your organization secure.

You are probably used to seeing the warning banners on top of suspicious but possibly legitimate emails that ask you to either “Report Phishing” or “Mark as Safe”.  This feature will continue to remain in place. However, occasionally you may receive an email that doesn’t have a warning banner, but still looks suspicious to you.

You can now quickly and seamlessly report it to [IT] using the new tool, which will also automatically remove the email from your inbox and from inboxes of any other employees who may have also received it. [The IT team] will analyze the email to determine whether it’s malicious or safe.  If it’s found to be malicious, you will be notified and the email will be kept in quarantine. If it’s found to be safe, you will also be notified and the email will be released from quarantine and returned to the inboxes of the recipients.

The feature has been activated within the [company name] Outlook environment, but you need to re-start Outlook to begin seeing the new button.

**How to locate and use the feature:**

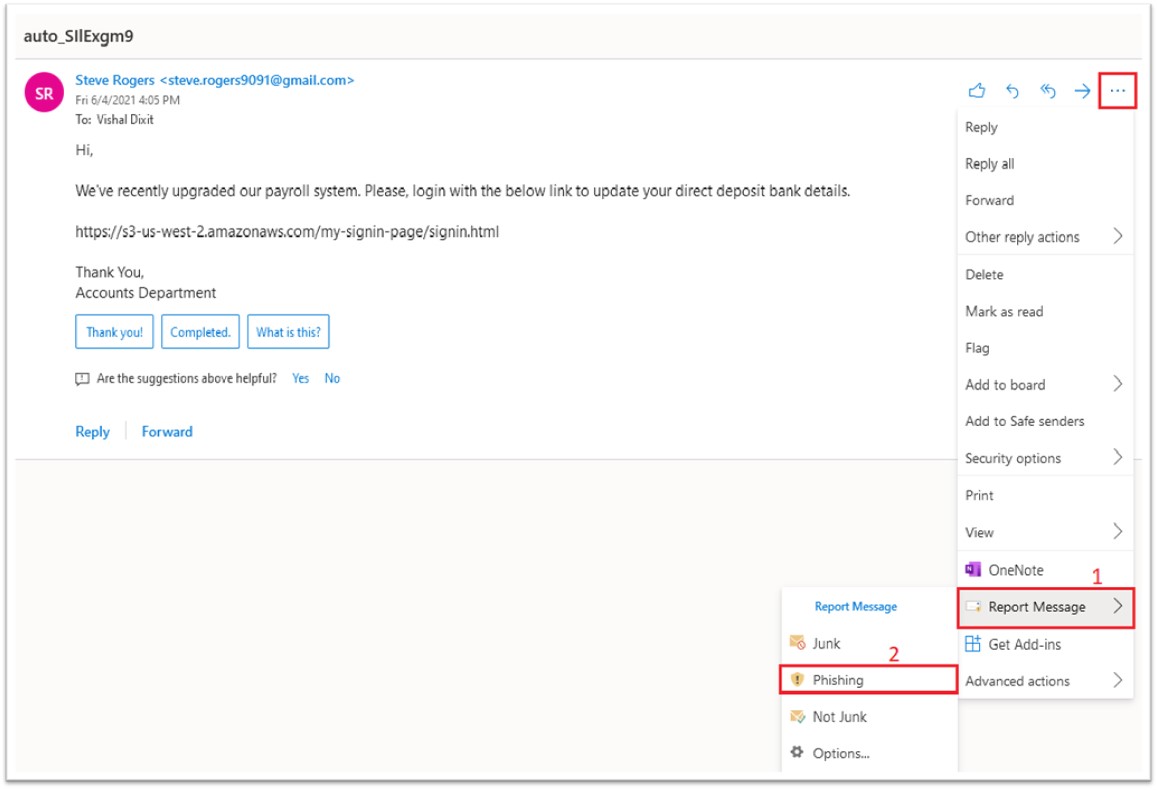
* If you use the **Outlook desktop client**, click on the **Report Message** button at the top of the email in question and select **Phishing** from the dropdown menu:

Graphical user interface, application, Word

Description automatically generated

* If you use the **Outlook web app**, there are two ways to report a suspected phishing email:

1.  Click **three dots** in the top right corner > **Report Message** > **Phishing:**

****

1. Click on **Junk at the top of the email, then Phishing** in the dropdown menu:

Graphical user interface, text, application, email

Description automatically generated

**Whenever this action is taken, the email will disappear from your inbox and will be sent to [IT] for analysis.**

Stay vigilant, do your part to keep our company secure, and use this new tool to report suspicious messages to [IT].

If you have any questions, please contact [the IT Support team].