Reporter Button User Guide

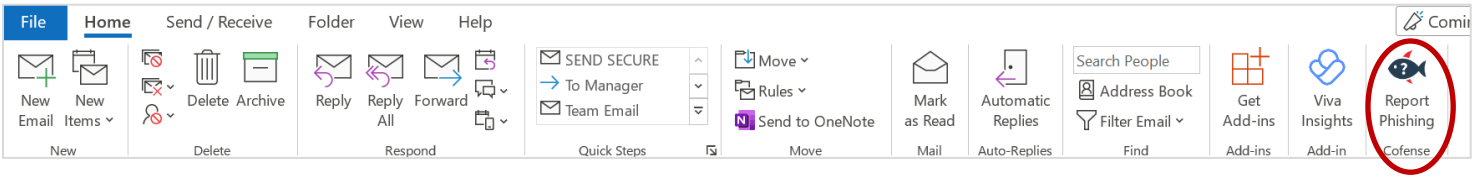
The **Cofense Report Phishing** button is an add-in to our current email client that provides a simple way for users to directly report suspicious emails to CWOPA Spam for evaluation.

The Report Phishing button can be found in your Outlook desktop client, Outlook on the Web (OWA) or the Outlook app on your commonwealth-issued mobile device.

Where to find the button?

Outlook Desktop Client

The location of your button will vary depending on your view settings within your mailbox (these are user-configured). If you have a reading pane engaged on your mailbox (*can be found under the View tab/Reading Pane*), the Report Phishing button will display under your default ***Home*** tab to the far right, as shown below. This button may appear grayed out when an email is not engaged (highlighted). To activate, simply click on an email which will re-engage your button and allow you to report.



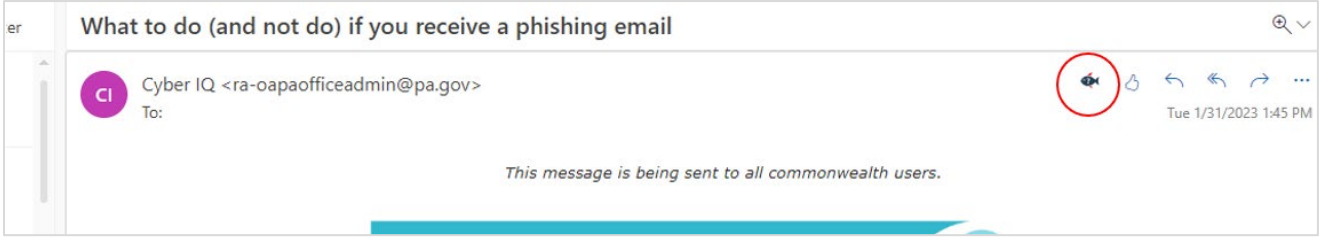
For users who do not have the reading pane engaged on their mailbox, to display the Report Phishing button the suspicious email you wish to report will need to opened. The button will display under the default ***Message*** tab to the far right.

> **NOTE:** If you must open a suspicious email to report, please exercise caution and ensure you do not click on any links, the message body or attachments.

Outlook on the Web

Like the desktop client for Outlook, this will vary as well depending upon your settings.

If your reading pane is enabled (*can be found under Settings/Mail/Layout/Reading Pane*), the Report Phishing button will display within the reading pane along with your email message. You can find the Report Phishing symbol to the far right next to the other email quick command buttons.



Like the Outlook client, if the reading pane is not engaged, you will need to open the suspicious email in order to report utilizing the Report Phishing button.

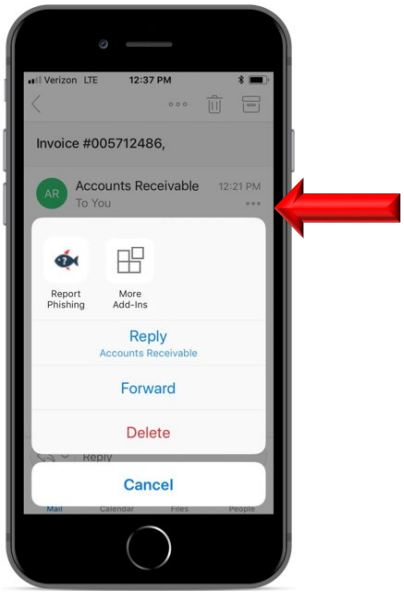
> **NOTE:** If you must open a suspicious email to report, please exercise caution and ensure you do not click on any links, the message body or attachments

Mobile Devices

When utilizing a mobile device to report a phishing email, the suspicious email must be opened and additional email options will need to be selected within the email to navigate to the Report Phishing button. Below is information on how to access the additional email options on both iOS and Android devices.

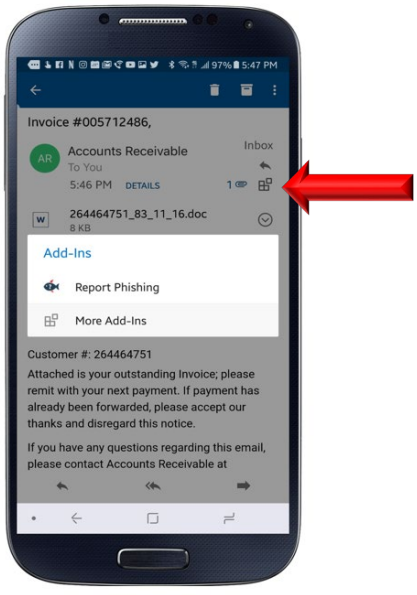
iOS Mobile Devices

Click the ellipsis located under the timestamp within the email.



Android Mobile Devices

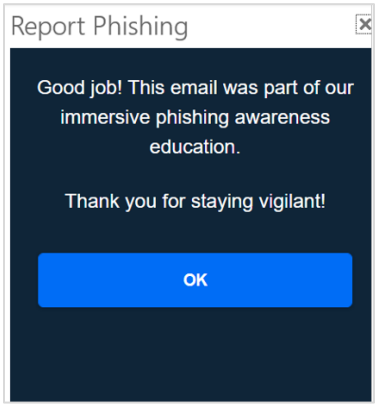
Click the add-in cubes.



What happens next?

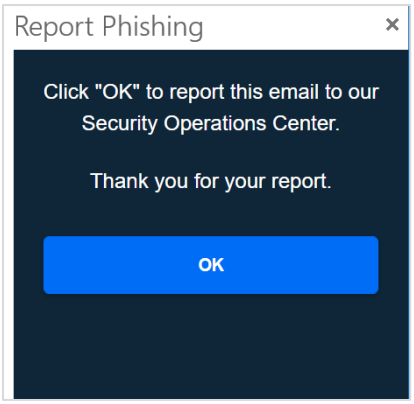
Once you submit an email using any of the methods above you will receive an immediate response/confirmation of your submission as detailed below.

If the email you submitted was related to a commonwealth phishing exercise a message like the one shown below will display notifying you that it was part of our immersive phishing awareness education. ***BONUS*** – this is automatically tabulated into exercise results to reflect your positive responsiveness to the exercise!



If the email you submitted was NOT recognized as one issued by the commonwealth as part of the phishing exercise program, it will be forwarded to our CWOPA Spam team for further analysis and you will receive a message indicating so like the one below.

> **NOTE:** Modifications made to the subject line of the email when reporting do affect its ability to determine whether or not an email is related to a commonwealth phishing exercise. Therefore, please do not modify the subject line when reporting.



After clicking **OK** on either notification message, the email will be removed from your inbox and sent to your Deleted Items folder. Should an item be accidentally reported, or later determined to be legitimate and needs to be retrieved you can obtain from this folder.

> **NOTE:** This process may take a moment, so please be patient and allow the system to process your request. You do not need to take any other actions on the email during this time.

A member of the CWOPA Spam team will respond if your submission requires further guidance or action.

Manual Forwarding to CWOPA Spam

There are some instances in which the manual forwarding of an email to CWOPA_Spam@pa.gov may still be required. These instances may include, but are not limited to:

- Error received while trying to submit email using button (*try restarting Outlook first*)
- Asking a specific question

In these instances, it is important that you *provide the actual suspicious email as an attachment*. Do not send screenshots, PDF's or Word documents with screenshots. These types of media do not provide the information needed by analysts to conduct a detailed review of the message.

Important Reminders

Do not modify the subject line text of email when submitting utilizing the button. This is one among many of the criteria being checked during the initial system analyzation. Changes to the subject line text will affect how the system analyzes your email.

Never forward a suspicious email to your co-workers or supervisor. IT Security or your IT Help Desk are trained in how to analyze and handle these emails. By forwarding a potentially malicious email to others not equipped to properly analyze these emails, you are increasing the potential that someone may expose our environment to malware or ransomware.

Only submit a suspicious email utilizing one method. If you are submitting your message utilizing the Report Phishing button and receive confirmation of its submission. There is no need to also manually forward to CWOPA Spam as the button has already done that step for you or vice versa.

Need Assistance?

If you are experiencing issues with your Report Phishing button, please contact CWOPA_Spam@pa.gov or submit an IT Help Desk ticket to be routed to the Enterprise Information Security Office.

If your preference is to notify via email, please ensure your email indicates in the subject line Reporter button issue so it can be quickly identified and routed for troubleshooting.