Everyone should now have access to the Phish Alert button in their Outlook email client. This will appear different ways on different devices such as phones but the concept and icon will be the same. Below are detailed directions and screenshots for using the Phish Alert Button.

> Note: if you believe the email is merely spam, undesired marketing emails and not malicious, please just move them to your Junk folder.

Desktop Outlook Client:

Look for the "Phish Alert" button on the right-hand side of the Home or Message tabs ribbon.
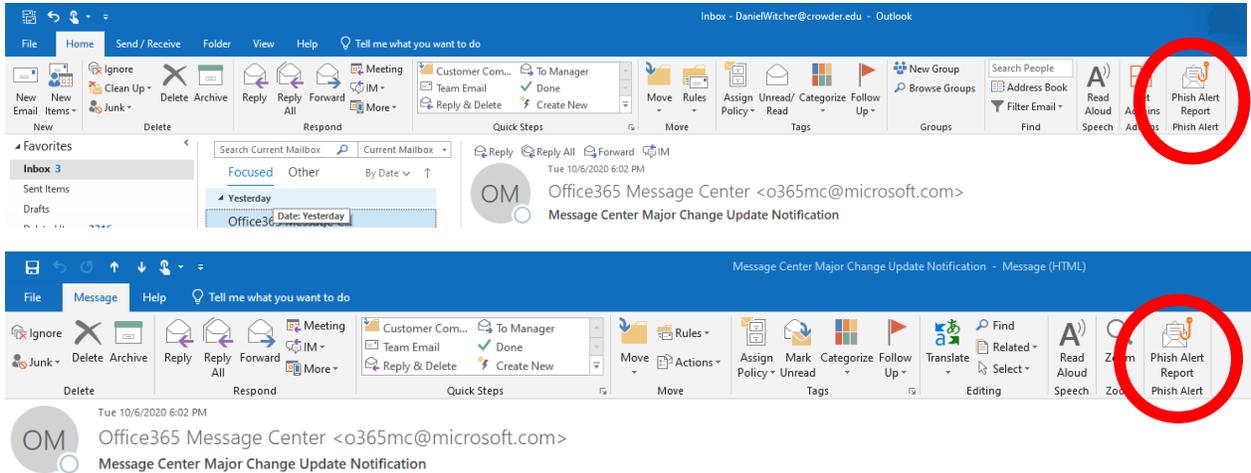
Browser (Chrome, Edge, Firefox, Safari, etc) Email:

The "Phish Alert" button can be accessed by clicking the three little dots in the upper right hand corner of the email and then selecting the button in the drop down menu that opens.
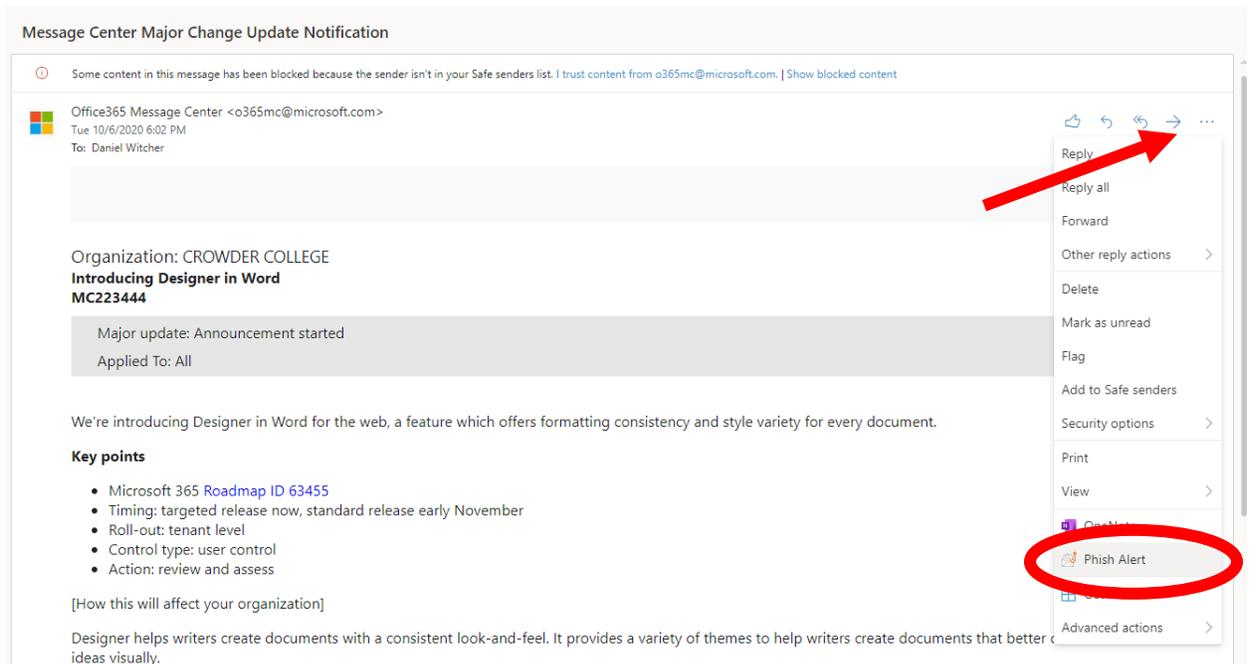
Outlook mobile app (Android):

1. Open an email, tap the three dots at the top-right of the screen.
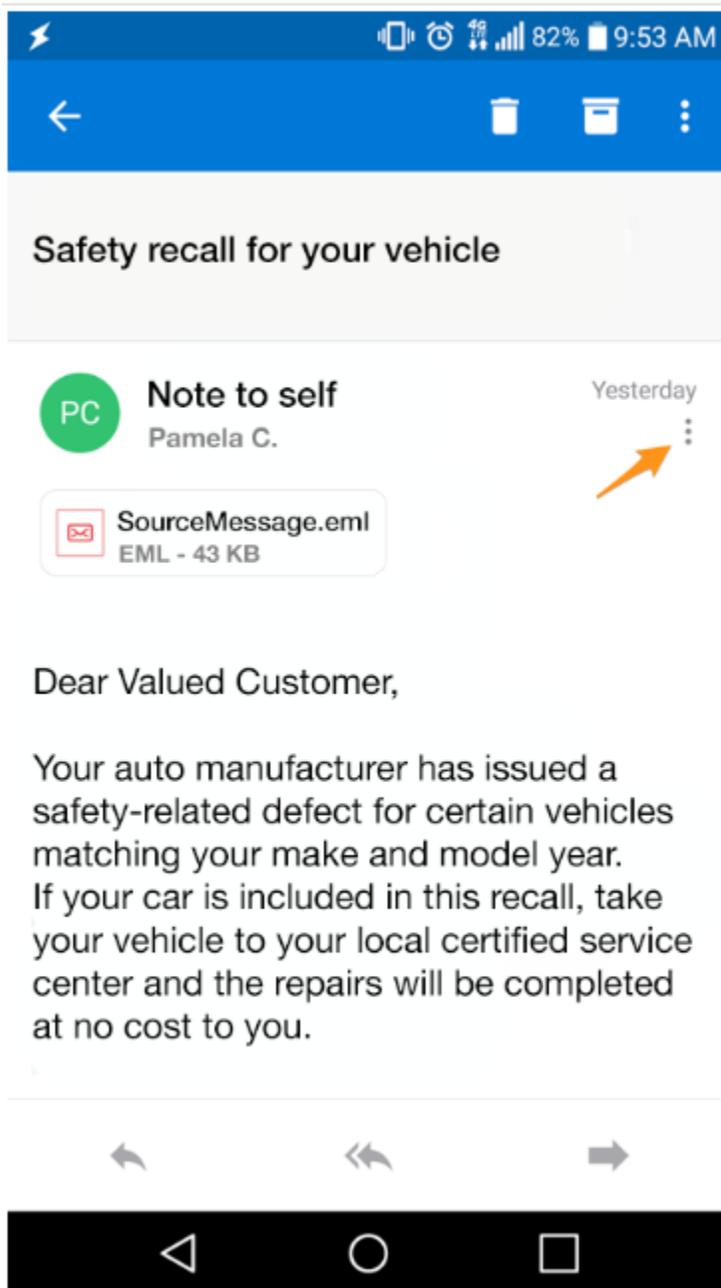
2. The Phish-Alert button will appear. Tap the Phish-Alert button.
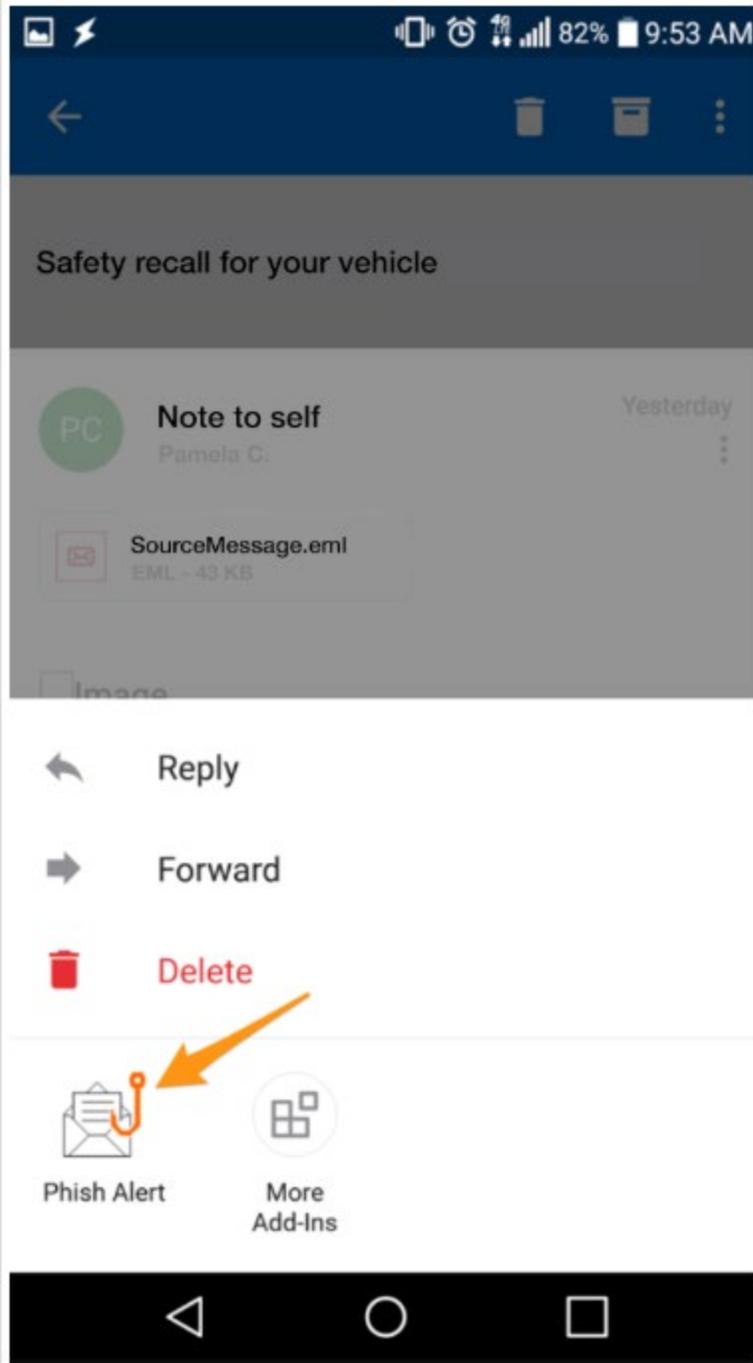
Outlook mobile app (iOS; Apple)

1. Open an email, tap the three dots at the top-right of the screen.

Doris K.
To You

12:40 PM

Dear Valued Customer,

Your auto manufacturer has issued a safety-related defect for certain vehicles matching your make and model year. If your car is included in this recall, take your vehicle to your local certified service center and the repairs will be completed at no cost to you.

Please click here to see if your vehicle qualifies under this program.

Thank you,

NHTSA
National Highway Traffic Safety Administration

Reply to All

2.   The Phish-Alert button will appear. Tap the Phish-Alert button.
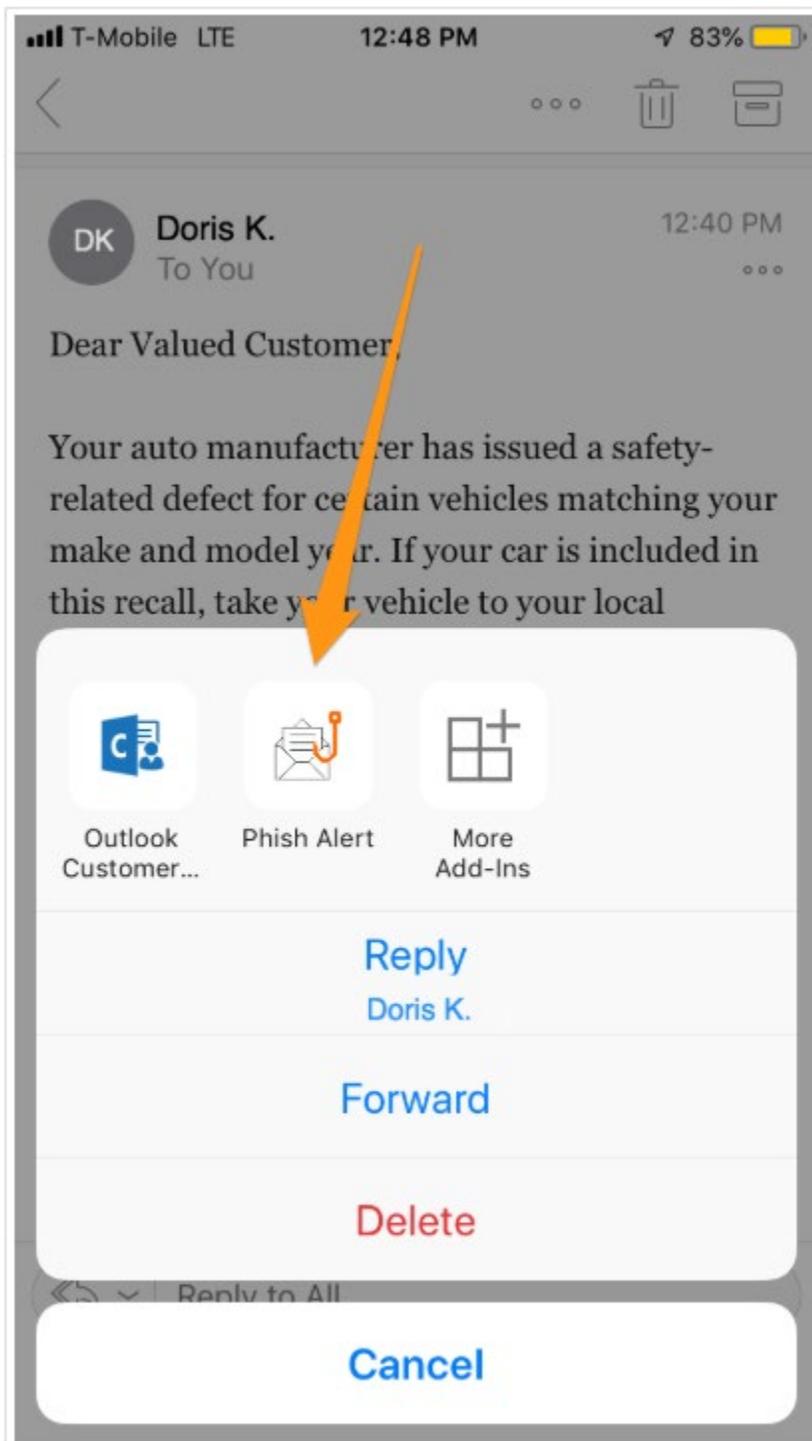
Finish reporting the email as phishing

1. After having clicked the Phish Alert button, a prompt will ask you if you are sure you want to report the email as a phishing email. Tap the Phish Alert button to finish reporting the email.
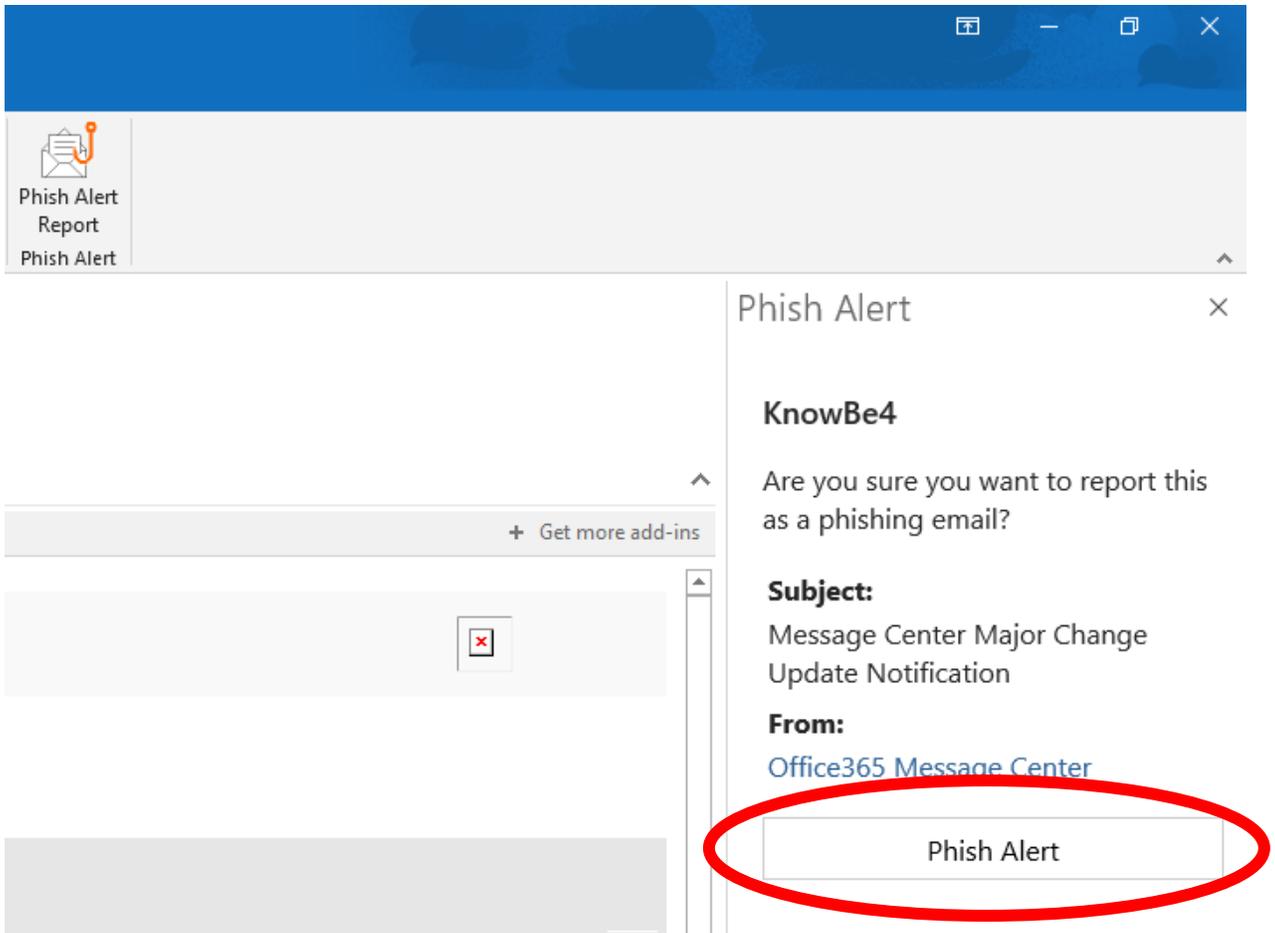
2. A final popup will occur thank you for reporting the phishing email.
   a. If the popup begins with the words "Congratulations …", the email being reported is one of the simulated phishing emails being sent as part of the phishing awareness campaigns.
   b. If the popup begins with the words "Thank you …", the email was not one of the simulated phishing emails sent as part of the phishing awareness campaigns.