



Procedure to Report Phishing and Spam Emails

Procedure to Report Phishing and Spam Emails

Phishing and spam emails are deceptive messages designed to steal personal information or compromise security. Reporting them promptly helps protect yourself and others. Below is a step-by-step procedure based on the provided sources:

Step 1: Identify the Email Type

- **Phishing Email:** Attempts to steal personal or financial information, impersonates trusted entities (e.g., banks, coworkers).
- **Spam Email:** Unsolicited messages, often promotional or irrelevant.

Key Differences

Aspect	Phishing	Spam
Intent	Steal sensitive information	Promote products/services
Sophistication	Highly targeted and deceptive	Generic and poorly targeted
Urgency	Creates a sense of urgency	Often lacks urgency
Appearance	Mimics legitimate organizations	May appear unprofessional

Step 2: Avoid Interaction

- Do not click on links, download attachments, or respond to requests for personal information.
- If the email contains warnings or urgent calls to action, proceed cautiously.



Procedure to Report Phishing and Spam Emails

Step 3: Use Built-in Reporting Tools

Use the Phish Alert Button (PAB) in short to report phishing email as follow :

Phish Alert Button (PAB) for Microsoft 365 Guide

The Phish Alert Button (PAB) is a tool that allows you to report potentially malicious emails, such as phishing emails. When you use the PAB to report a potentially malicious email, you can help keep your organization safe from cyberattacks.

When Should I Use the PAB?

You should use the PAB to report any suspicious emails or potential phishing emails. When you use the PAB to report an email, the email will be automatically deleted from your inbox and forwarded to the OIT security team.

You should not use the PAB to report spam or marketing emails. You can delete these types of emails or add the sender or sender's email domain to a block list.

⚠ Important: If you need help adding a sender to a block list, contact infosec@athens.edu

How Do I Use the PAB?


The steps for reporting an email using the PAB may vary based on the app that you're using. When you report an email using the PAB, the reported email will be automatically forwarded to your OIT team regardless of the app that you're using.

Click the links below to learn how to use the PAB for the apps that you're using:

- [Using the PAB in Microsoft 365](#)
- [Using the PAB in the Microsoft Outlook Mobile App for Android](#)
- [Using the PAB in the Microsoft Outlook Mobile App for Apple iOS](#)

If you report an email in error, you can retrieve the email from your Trash or Deleted Items folders.

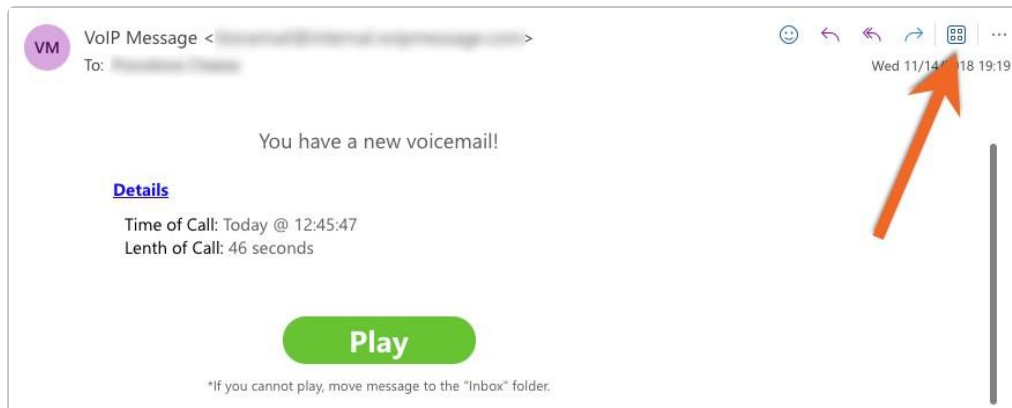
Procedure to Report Phishing and Spam Emails

 **Note:** The PAB is only compatible on mobile devices with public instances of Microsoft. Due to the permissions required, the PAB cannot be used on mobile devices with Microsoft 365 GCC High.

Using the PAB in Microsoft 365

If you use Microsoft 365, follow the steps below to report an email with the PAB:

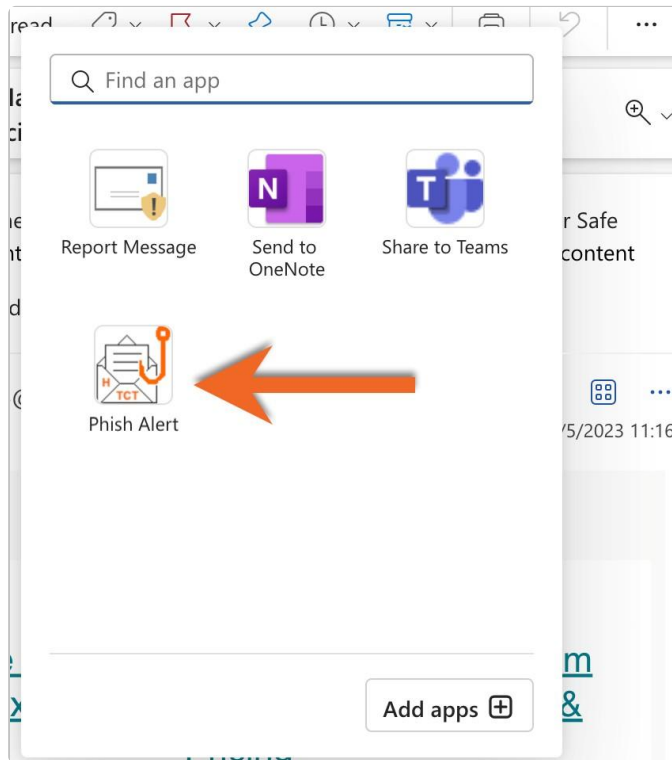
- 1 Open the email that you would like to report.
- 2 Click the **Apps** icon in the top-right corner of the email to open the Apps launcher. Or, click the **ellipsis** icon (...) and select **Apps**.



- 3 From the Apps launcher that opens, click the **Phish Alert** add-in.

Note: If the PAB add-in is not displayed in the Apps launcher, click **Add apps**. Then, locate and add the PAB add-in. You can also pin the PAB add-in to the toolbar at the top of an open email. To pin the add-in, click the **ellipsis** icon and select **Customize actions**. Or, navigate to **Settings > Mail > Customize actions**. Then, select the **Phish Alert** add-in and click **Save**. For more information about managing add-ins in Microsoft Office, visit Microsoft's [Get an Office Add-in for Outlook](#) article.

Procedure to Report Phishing and Spam Emails




- 4 In the prompt that opens, click **Phish Alert** again to report the email.

Note: If your admin has enabled the Comments and Dispositions setting for the PAB, you can select a disposition from the Email Classification section. The Unknown option is selected by default. You can also enter a comment about the email you are reporting. Then, click **Phish Alert**.



ATHENS
STATE
UNIVERSITY

Procedure to Report Phishing and Spam Emails

 Phish Alert ×

M365


KnowBe4

Are you sure you want to report this as a phishing email?

Subject:
New Voice Mail!

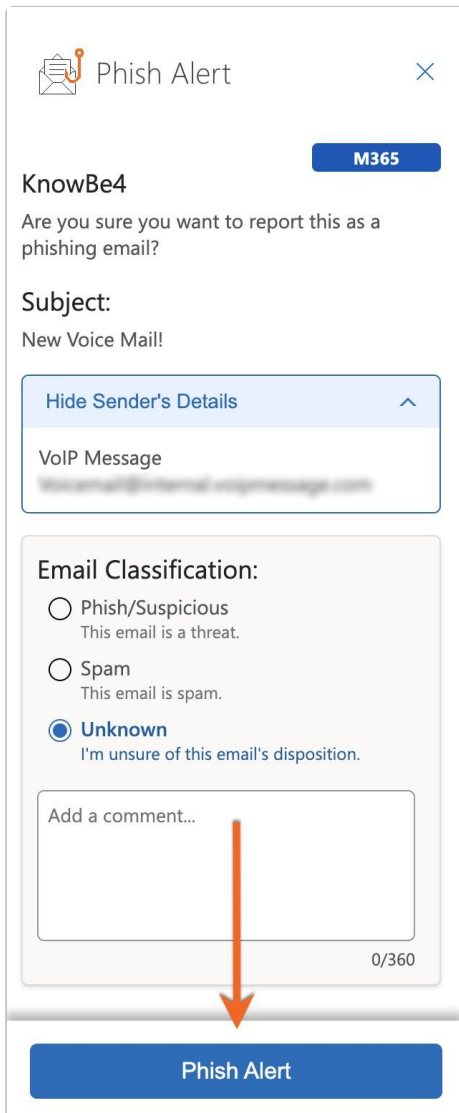
From:

VoIP Message
Voicemail@internal.voipmessage.com

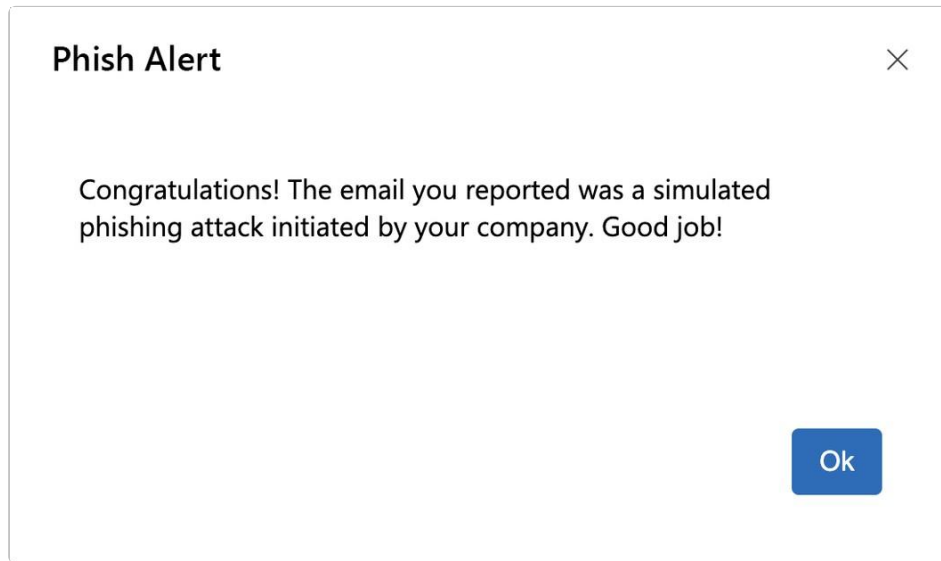


Phish Alert

Procedure to Report Phishing and Spam Emails



- 5 After you click **Phish Alert** again, a message will display to confirm that you reported the email. This message will tell you if the email you reported was a simulated phishing attack or if the email will need to be reviewed by the OIT team. To close this message, click **Ok**.

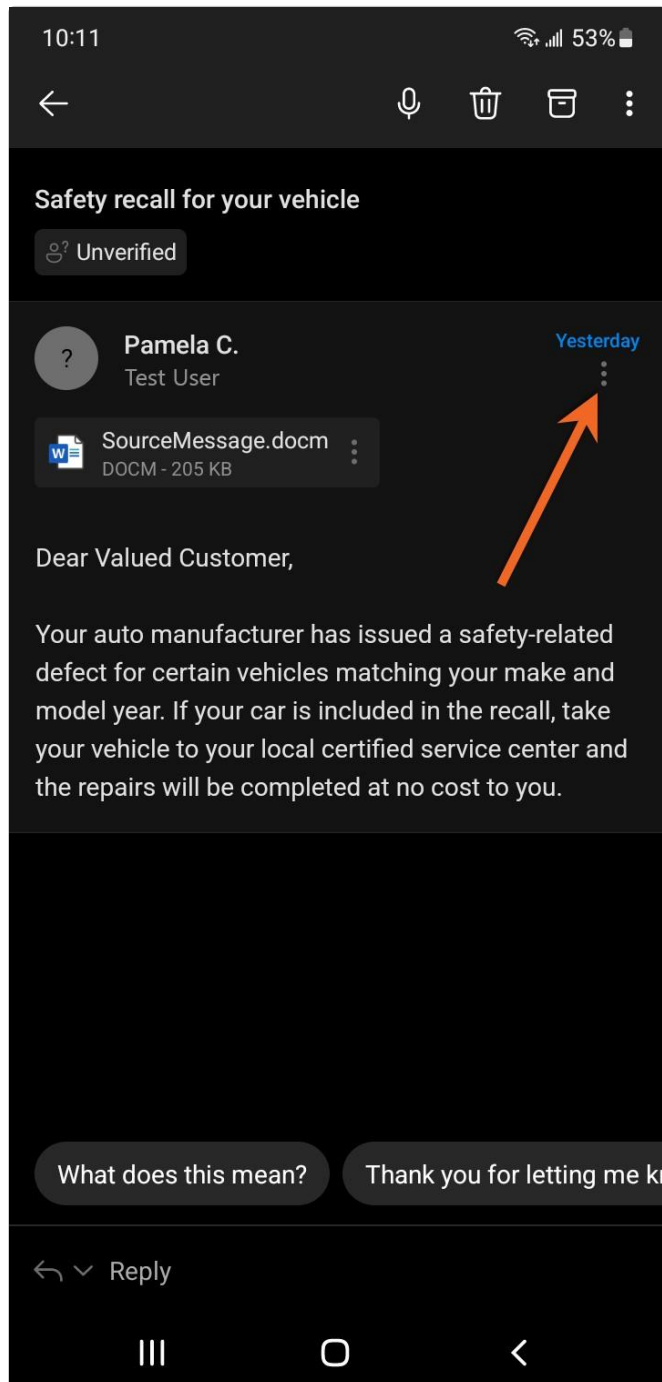


Using the PAB in the Microsoft Outlook Mobile App for Android

If you use the Microsoft Outlook app for Android, follow the steps below to report an email:

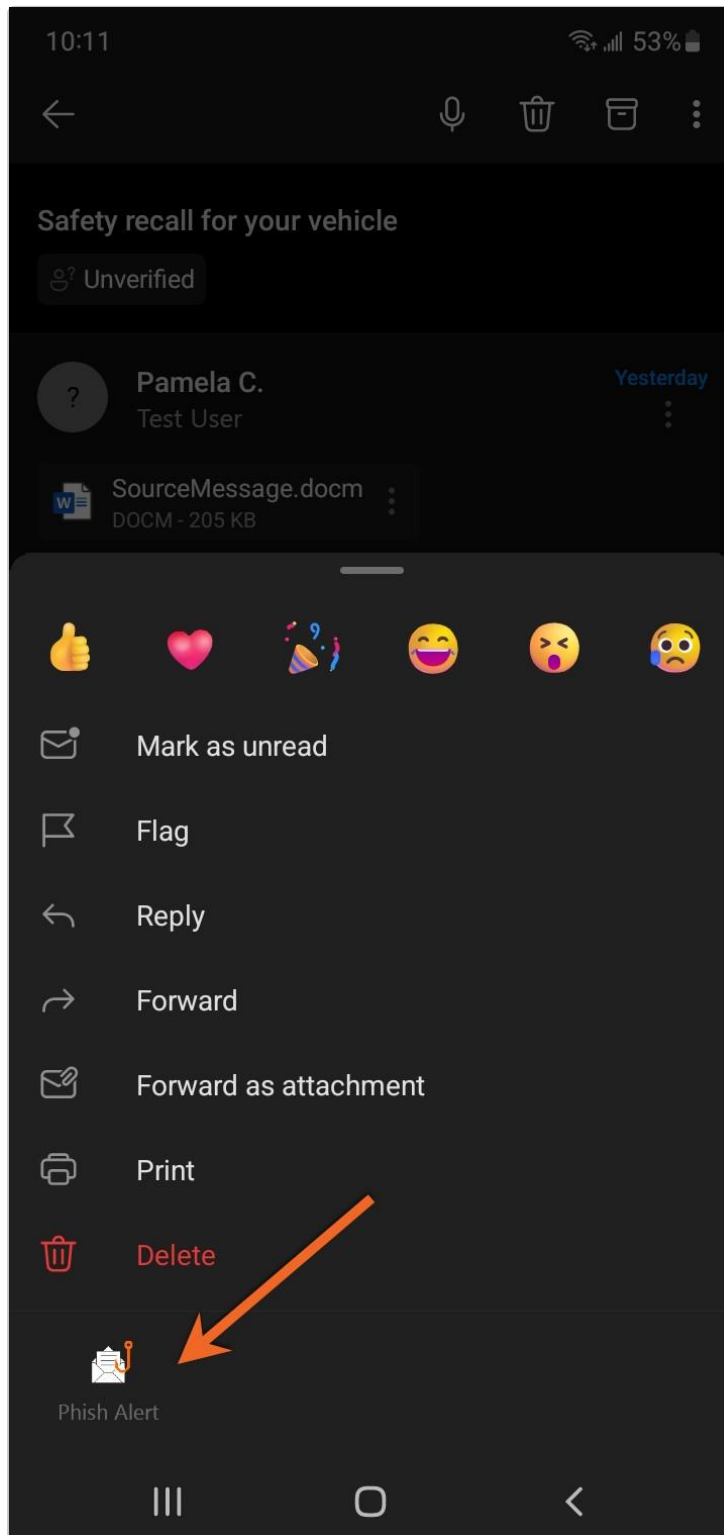
- 1 Open the email that you would like to report.
- 2 Click the vertical **ellipsis** icon (...) at the upper right corner of the email. Check the rest of the screen if you do not see the button in this location.

Procedure to Report Phishing and Spam Emails



- 3 Click the **Phish Alert** icon.

Procedure to Report Phishing and Spam Emails

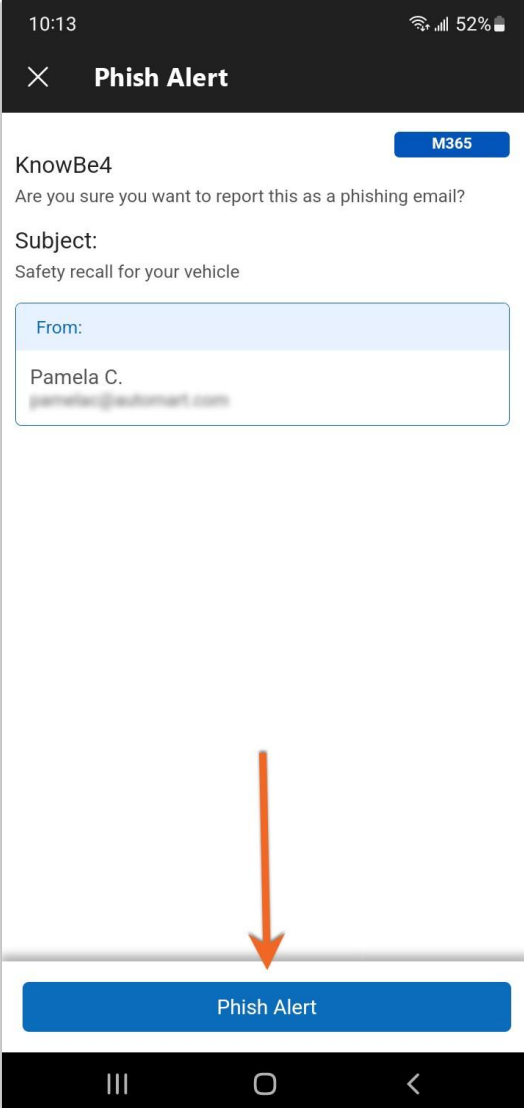


- 4 In the pop-up window that opens, click **Phish Alert** to report the email.

Note: If your admin has enabled the Comments and

Procedure to Report Phishing and Spam Emails

Dispositions setting for the PAB, you can select a disposition from the Email Classification section. The Unknown option is selected by default. You can also enter a comment about the email you are reporting. Then, click **Phish Alert**.



10:13 52%

× **Phish Alert**

KnowBe4 **M365**

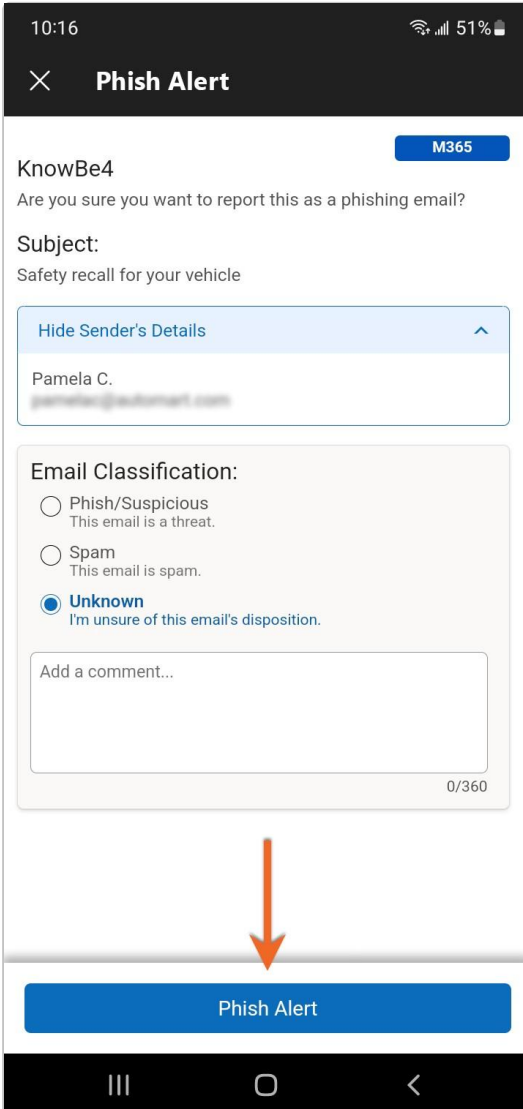
Are you sure you want to report this as a phishing email?

Subject:
Safety recall for your vehicle

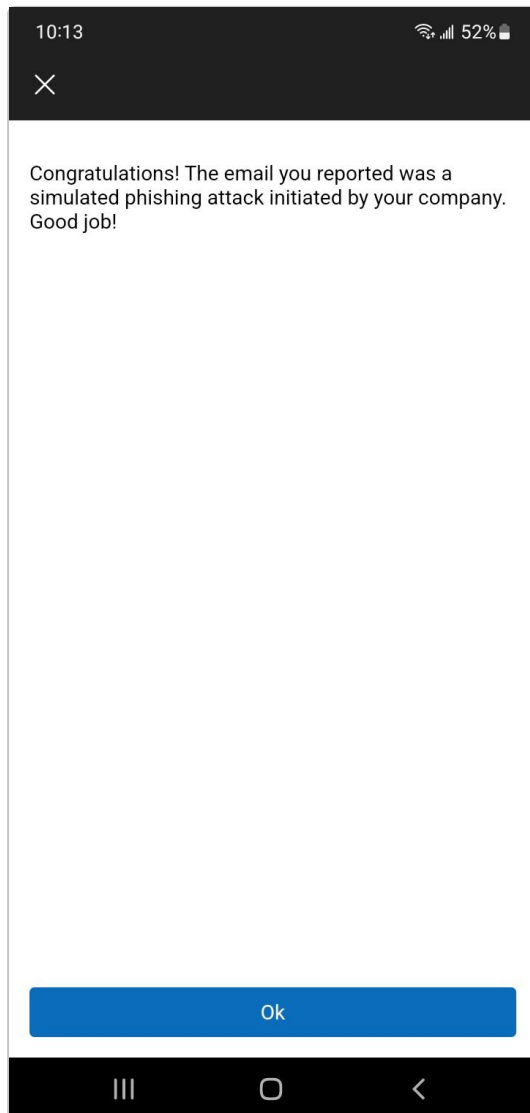
From:
Pamela C.
pamela@autismart.com

Phish Alert

Procedure to Report Phishing and Spam Emails



- 5 After you click **Phish Alert** again, a message will display to confirm that you reported the email. This message will tell you if the email you reported was a simulated phishing attack or if the email will need to be reviewed by the OIT security team. To close this message, click **Ok**.

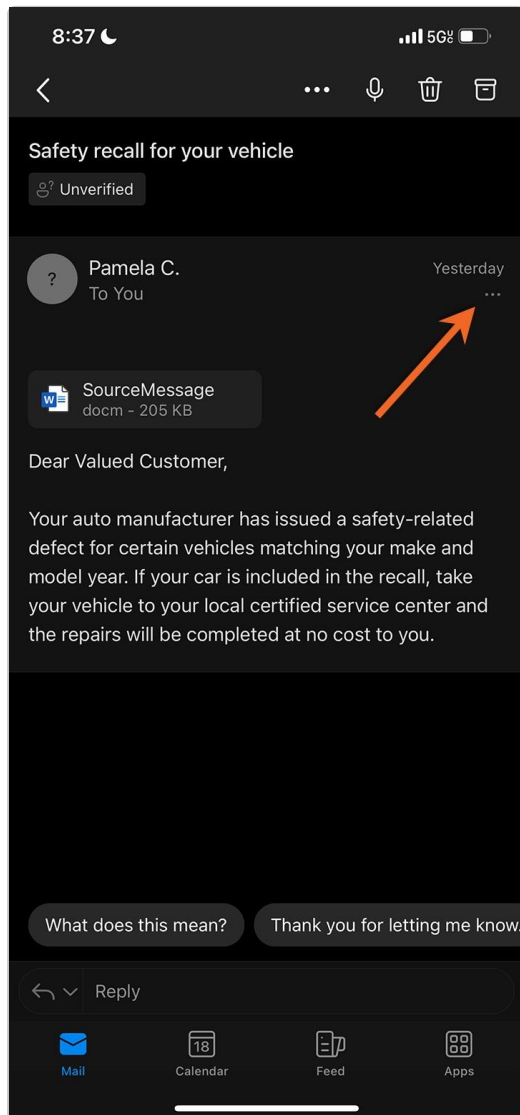


Using the PAB in the Microsoft Outlook Mobile App for Apple iOS

If you use the Microsoft Outlook app for Apple iOS, follow the steps below to report an email:

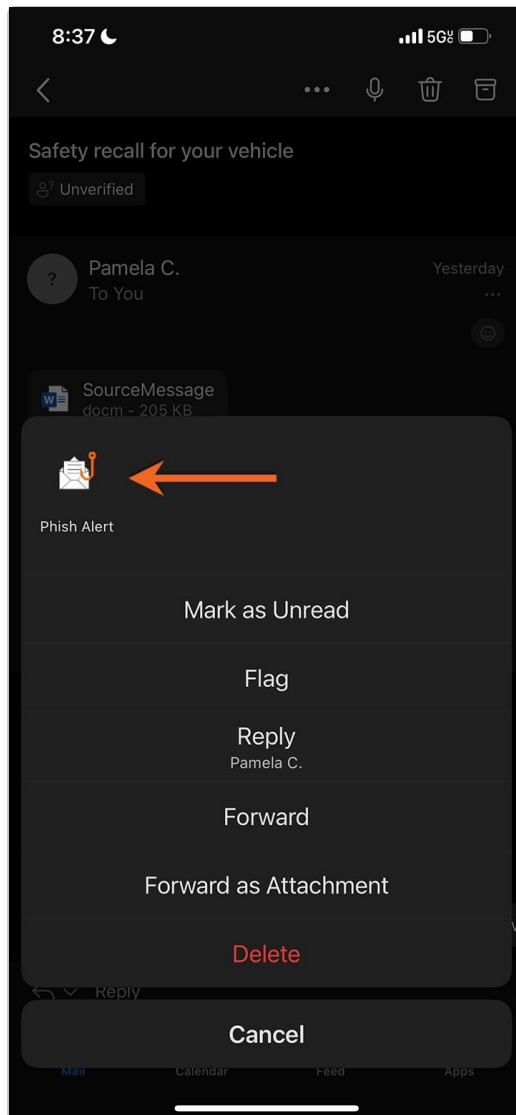
- 1 Open the email that you would like to report.
- 2 Click the **ellipsis** icon (...) at the upper right corner of the email.

Procedure to Report Phishing and Spam Emails



- 3 Click the **Phish Alert** icon.

Procedure to Report Phishing and Spam Emails



- 4 In the pop-up window that opens, click **Phish Alert** again to report the email.

Note: If your admin has enabled the Comments and Dispositions setting for the PAB, you can select a disposition from the Email Classification section. The **Unknown** option is selected by default. You can also enter a comment about the email you are reporting. Then, click **Phish Alert**.



Procedure to Report Phishing and Spam Emails

8:40 5G%

Phish Alert

KnowBe4 M365

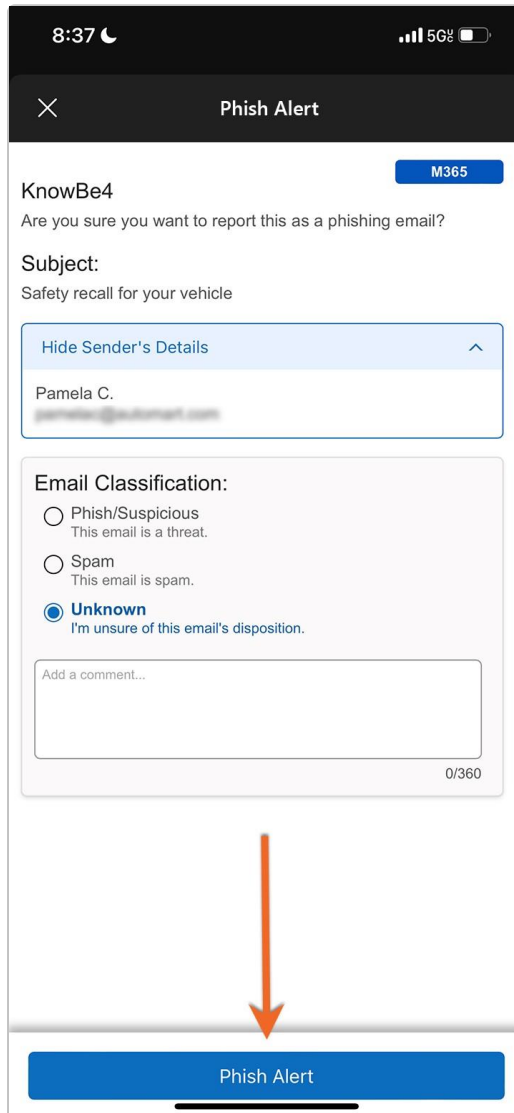
Are you sure you want to report this as a phishing email?

Subject:
Safety recall for your vehicle

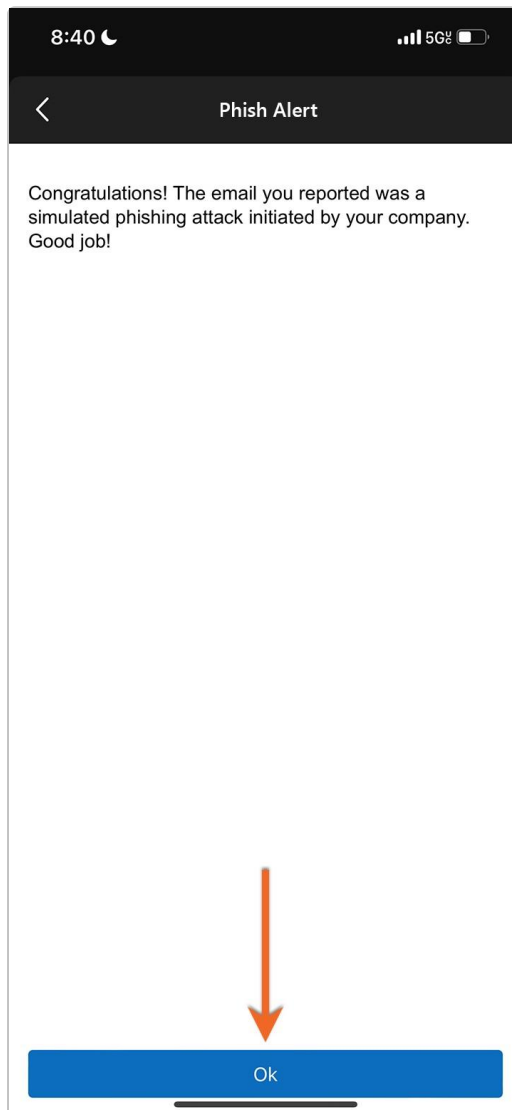
From:
Pamela C.
pamela.c@autismart.com

Phish Alert

Procedure to Report Phishing and Spam Emails



- 5 After you click **Phish Alert** again, a message will display to confirm that you reported the email. This message will tell you if the email you reported was a simulated phishing attack or if the email will need to be reviewed by the OIT security team. To close this message, click **Ok**.



Why Should I Use the PAB?

When you use the PAB to report suspicious emails, you can help keep your organization safe from security threats. The reported emails are sent to your organization for analysis, which will help keep the OIT security team informed about potential phishing emails that their employees receive. Once the OIT security team is aware of potential threats, they can help your organization stay safe from future attacks.