From:	Strategic Communications
To:	Unified_Gov Users
Subject:	DOTS: Keeping Our Data and Systems SAFE! and Update on Health Building Access/Construction
Date:	Wednesday, May 8, 2024 2:13:31 PM
Attachments:	Using the Phish Alert Button Outlook.pdf image001.png Using the Phish Alert Button Office 365.pdf iOS KB4 PAB.pdf KB4 PAB- Android.pdf image002.png

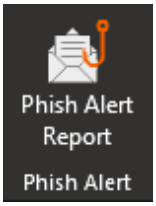
---

From the Department of Technology Services (DOTS):

This is to inform you of an important update regarding our cybersecurity training and awareness program. The UG will be transitioning to a new provider, KnowBe4, to help us with simulating phishing exercises (don't click that link!) and overall training on how to keep our systems safe. They have a great reputation and should be an important part of our overall cybersecurity efforts.

What does this mean for you?

Moving forward, you will start using the Phish Alert Button to report suspicious emails. Look for this icon:



Stay alert and be sure to report any suspicious emails. We are ALL on the front lines of our cybersecurity! Please see the attached instructions to help you find this new reporting tool using Outlook and Office 365. Stay tuned for instructions on how to report phishing emails via mobile phone.

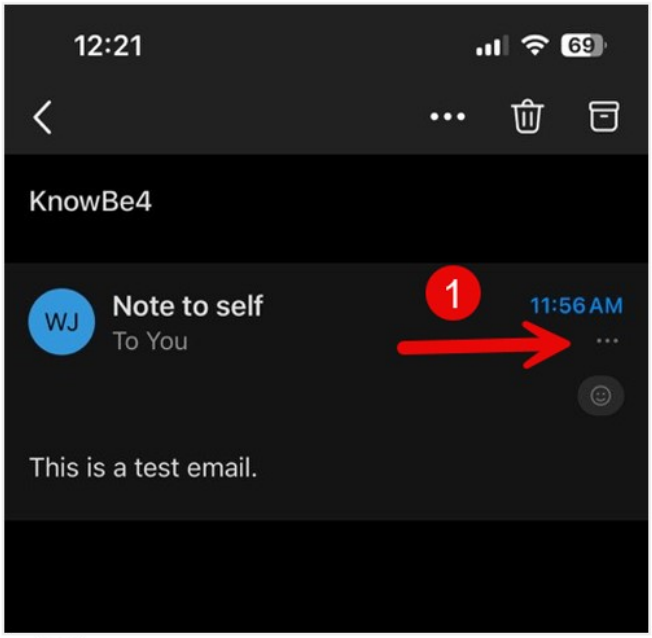
Update on Health Department Building Area Construction

Work around the Health Department Building has begun this week, impacting access from the north side of the building. Foot and vehicle traffic from Ann Avenue will need to use the driveway entrance into Lot E. Starting May 13 and running for about a week, the sidewalk will be opened and the driveway entrance will be closed to all foot and vehicular traffic. During this time, please use the South Entrance to Lot E.

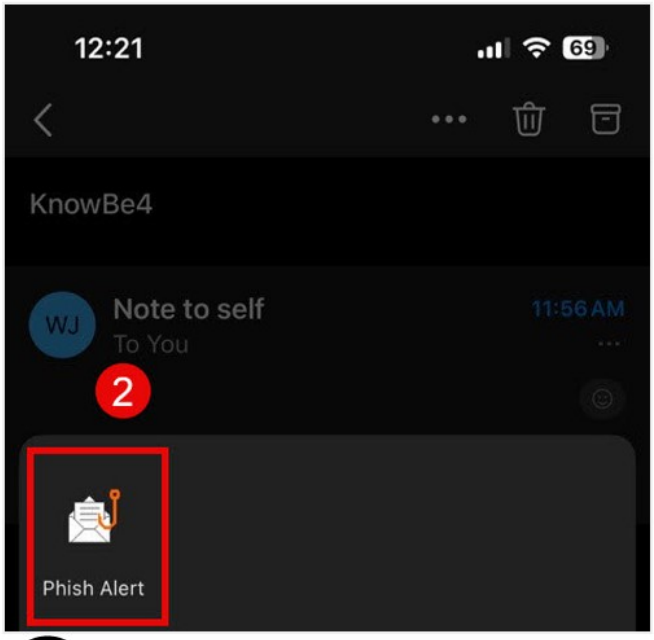
The main doors to the Health Department Building will remain open during regular business hours throughout the project. If you have any questions, please contact Buildings & Logistics (business hours) at 913-573-5330 or Security (after hours) at 913-573-6330. Thanks for your understanding as we make these improvements!


Ann Ave
Ann Ave
Ann Ave
Drive
Sidewalk
UMB Bank ATM

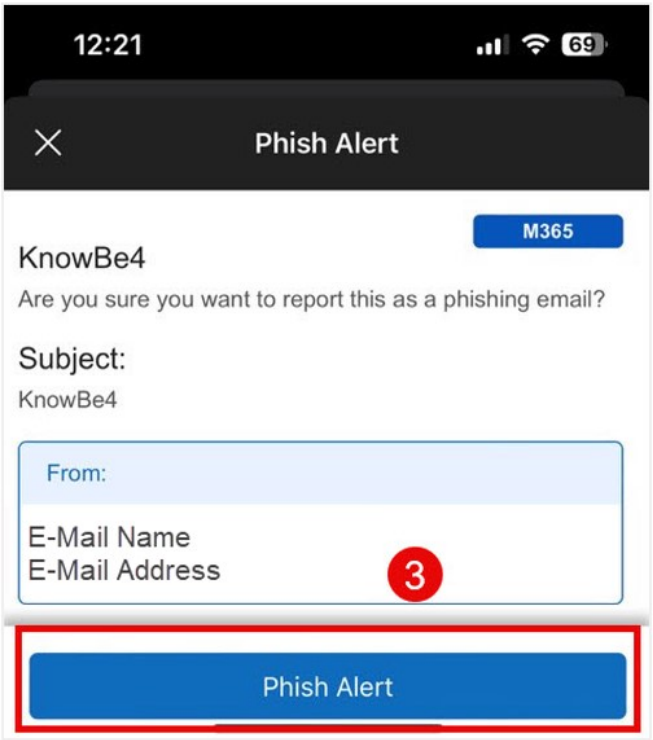
iOS KnowBe4 Phish Alert Button (PAB)



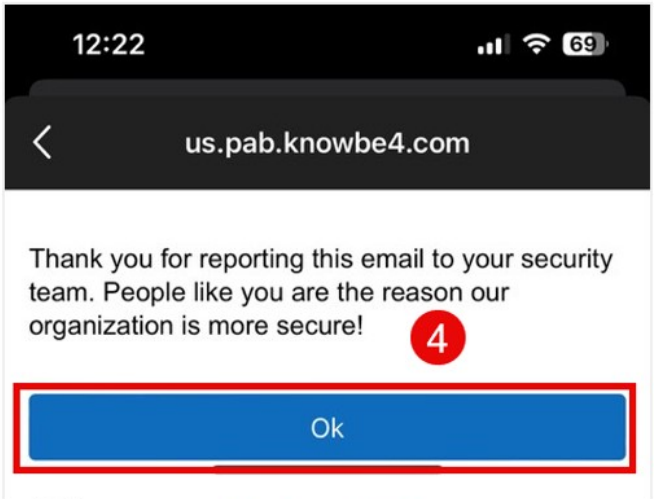
1 **Open the email that you want to report. Select the three dots. (...)**



2 **Select the Phish Alert Button (PAB).**

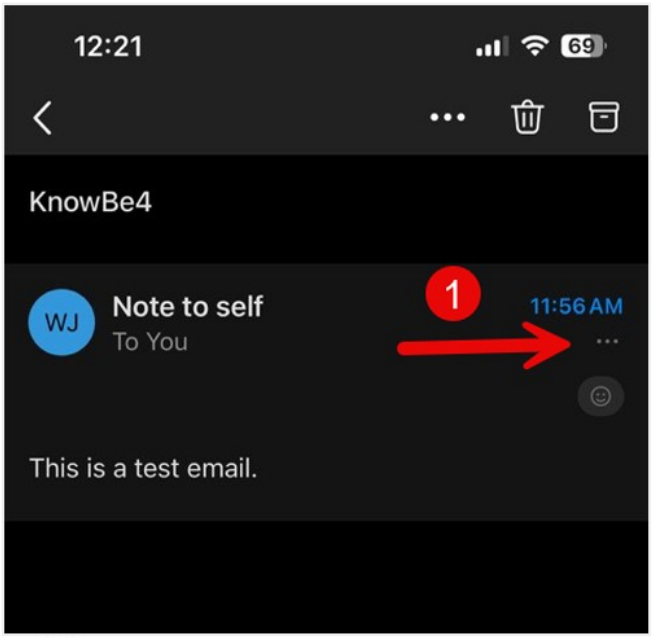


3 **Select the Phish Alert Button (PAB).**

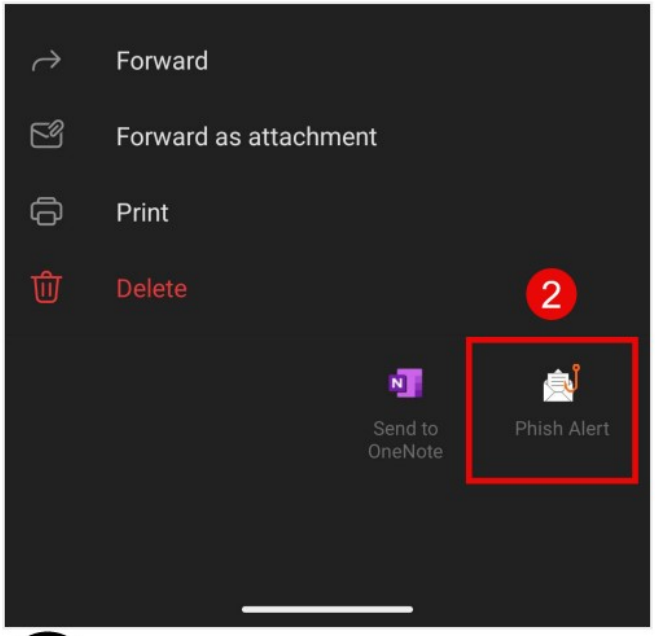


4 **Select Ok.**

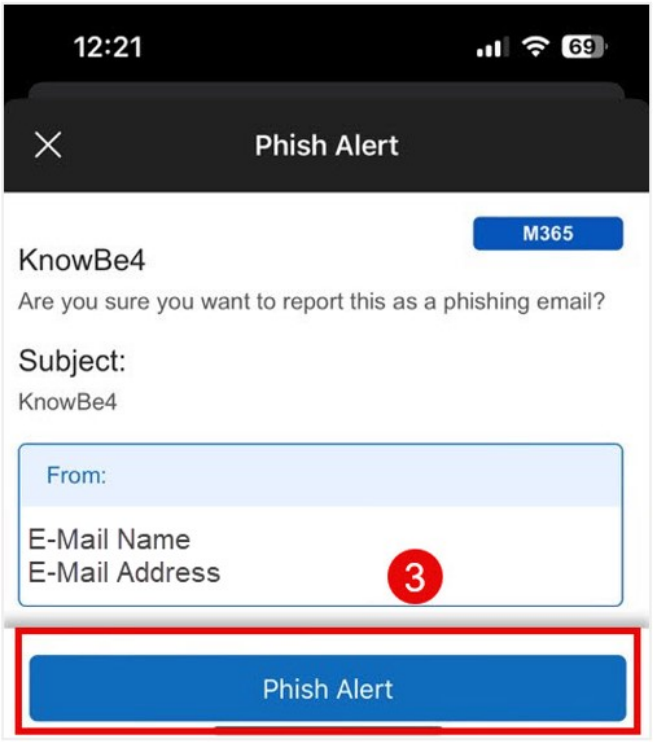
Android KnowBe4 Phish Alert Button (PAB)



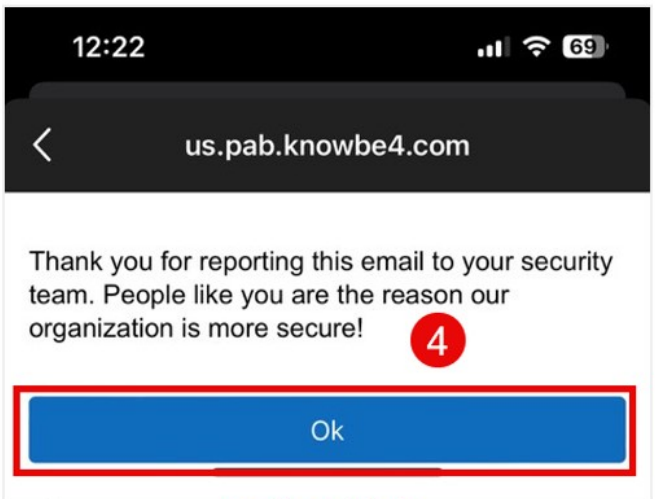
1 **Open the email that you want to report. Select the three dots. (...)**



2 **Swipe up. Select the Phish Alert Button (PAB).**



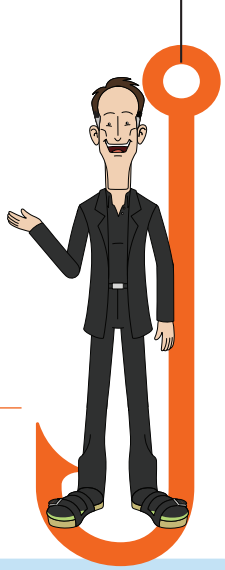
3 **Select the Phish Alert Button (PAB).**



4 **Select Ok.**

BE A HERO!

Use the Phish Alert Button



You receive an email asking you to take an action. Sounds suspicious, right? But don't worry. You can be a hero by taking the correct action–and giving your IT department the information they need to defend your organization against the effects of malicious email attacks. It's easy. Thanks to the **Phish Alert Button**, or **PAB** for short.

How do I know what to report?

Spam is unsolicited and unwanted email, typically sent to try to sell you something. While it is often annoying and misleading, it is rarely malicious.

Simply delete it!

Phishing messages are bulk emails, typically appearing to be from a reputable source, that ask you to take a specific action that can cause damage to you or your organization. These messages are malicious.

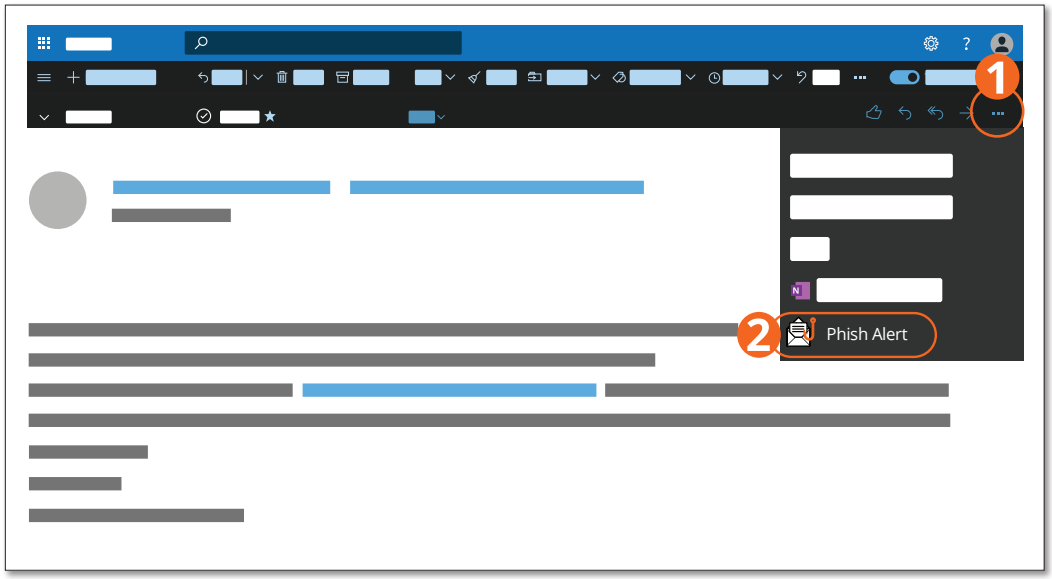
Spear phishing emails are targeted attacks on a person or organization, occurring after detailed research in order to make them seem especially real. These messages are extremely malicious and can lead to very damaging consequences.

Report it with the PAB!

Where do I find the PAB in Office 365?

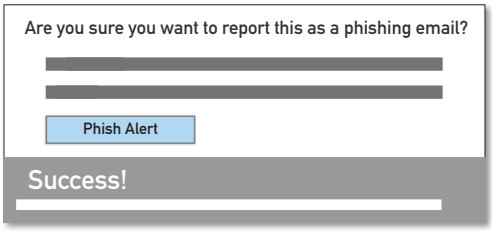
While viewing your email:

❶ You can find the Phish Alert Button by clicking the ellipses (or three dots) in the right side to open a menu. ❷ You can then click the Phish Alert Button at the bottom of the menu.



Confirm:

The pop-up box you see will prompt you to confirm your action. Once confirmed, the email in question will be immediately forwarded to your organization's IT team.



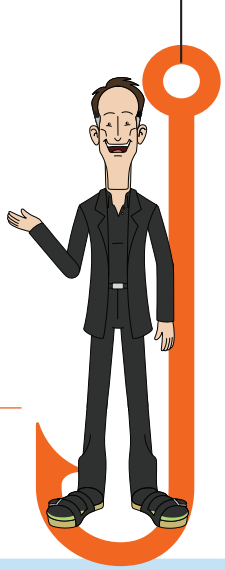
Stop. Look. Think. Report!

Remember, you are the last line of defense against email based criminal activity. Never click on a link or open an attachment in any unexpected or unsolicited email. If you are uncertain, follow your organization's security policy–or ask your IT team for advice.

KnowBe4
Human error. Conquered.

BE A HERO!

Use the Phish Alert Button



You receive an email asking you to take an action. Sounds suspicious, right? But don't worry. You can be a hero by taking the correct action–and giving your IT department the information they need to defend your organization against the effects of malicious email attacks. It's easy. Thanks to the **Phish Alert Button**, or **PAB** for short.

How do I know what to report?

Spam is unsolicited and unwanted email, typically sent to try to sell you something. While it is often annoying and misleading, it is rarely malicious.

Simply delete it!

Phishing messages are bulk emails, typically appearing to be from a reputable source, that ask you to take a specific action that can cause damage to you or your organization. These messages are malicious.

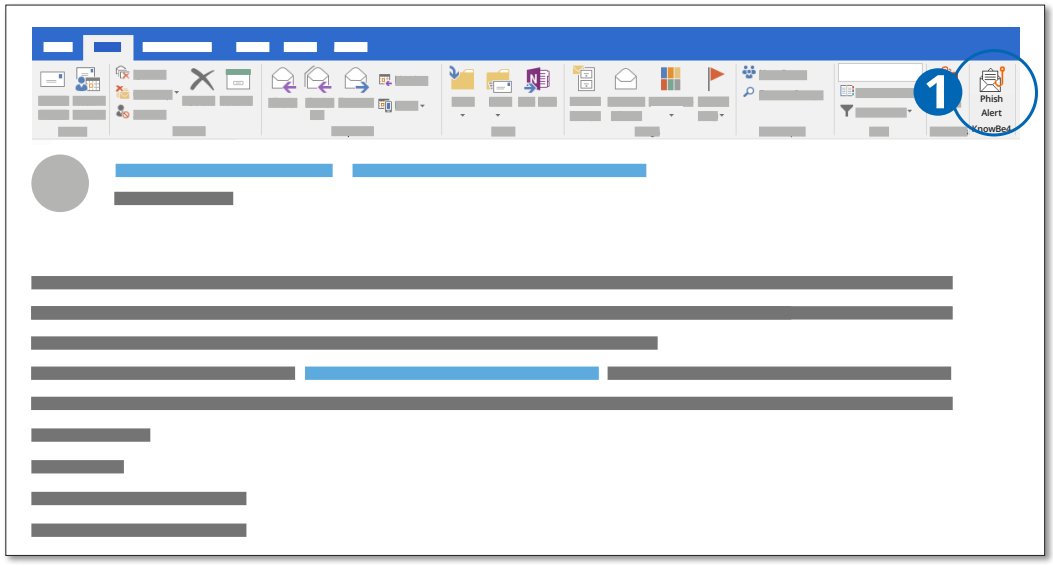
Spear phishing emails are targeted attacks on a person or organization, occurring after detailed research in order to make them seem especially real. These messages are extremely malicious and can lead to very damaging consequences.

Report it with the PAB!

Where do I find the PAB in Outlook?

While viewing your email:

❶ You can find the Phish Alert Button in the Outlook ribbon at the top of your screen. Locate the envelope icon with the orange "fish hook."

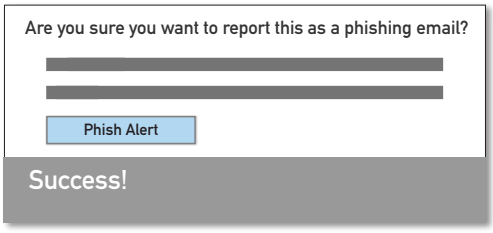


Report:

Report suspected phishing emails by clicking the Phish Alert in the ribbon.

Confirm:

Once you click to report, the pop-up will prompt you to confirm your action. Once confirmed, the suspicious email will be immediately forwarded to your IT team.



Stop. Look. Think. Report!

Remember, you are the last line of defense against email based criminal activity. Never click on a link or open an attachment in any unexpected or unsolicited email. If you are uncertain, follow your organization's security policy–or ask your IT team for advice.

KnowBe4
Human error. Conquered.