How to Report Phishing Using the Phish Alert Button (PAB)

David Raco - 2025-01-10 - Comments (0) - Security

Phishing is a type of cybercrime where attackers send fraudulent emails or messages that appear to be from reputable sources in order to trick individuals into revealing sensitive information, such as passwords, credit card numbers, and personal data. The goal is to use this information for malicious purposes, such as identity theft or financial gain.

Some common signs of phishing include:

- **Suspicious email addresses or URLs:** Phishing emails often come from email addresses that look similar to legitimate ones but have slight differences, such as misspellings or extra characters. Similarly, links in the email may lead to websites that mimic the appearance of trusted sites but have different domain names. E.g. soupresident@soou[.]net (email address is not part of the sou.edu domain) and https://souokta[.]com/login (URL is not part of the sou.edu domain)
- **Urgent or threatening language:** Phishing emails often create a sense of urgency or panic, using phrases like "Act now!" or "Your account will be suspended." This is done to pressure recipients into acting quickly without thinking.
- **Requests for sensitive information:** Legitimate organizations will never ask for sensitive information, such as passwords or credit card numbers, through email. If an email requests this information, it's likely a phishing attempt.
- **Poor grammar and spelling:** Many phishing emails contain spelling and grammatical errors, which can be a sign that the email is not from a professional source. However, you cannot rely on presentation alone to recognize a phishing email. Clever criminals can make their phishing attacks look very convincing.
- **Unsolicited attachments:** Phishing emails may contain attachments that, when opened, can install malware on the recipient's device. Be cautious of any unsolicited attachments, especially those with file extensions like .exe or .zip.
- **Odd or unexpected content:** If an email contains content that seems out of character for the sender or is unexpected, especially if it comes from an email address you don’t recognize for the sender, it could be a phishing attempt.

Remember, these are just some of the common signs of phishing, and attackers are constantly evolving their tactics. It's important to always double-check the legitimacy of any suspicious emails or messages you receive.

How to Report Phishing Emails

Warning

Students are not configured to have the Phish Alert Button described below. **Students** needing to report a phishing email should instead forward a copy of the email to infosec@sou.edu.

Generic email accounts (e.g. admissions@sou.edu) are not configured to have the Phish Alert Button. If you encounter a phishing email in one of those accounts, please forward a copy of the email to infosec@sou.edu.

Note

Employees are encouraged to report phishing emails using the Phish Alert Button according to the instructions below because it streamlines our automated phishing exercises. If you report a simulated phishing email, you will get immediate feedback and our training system will automatically record that you passed the phishing test.

You can find the vendor's instructions for this feature at https://support.knowbe4.com/hc/en-us/articles/4404150738067-Gmail-Add-on-Phish-Alert-Button-PAB-Guide

Report in Web-based GMail

Question

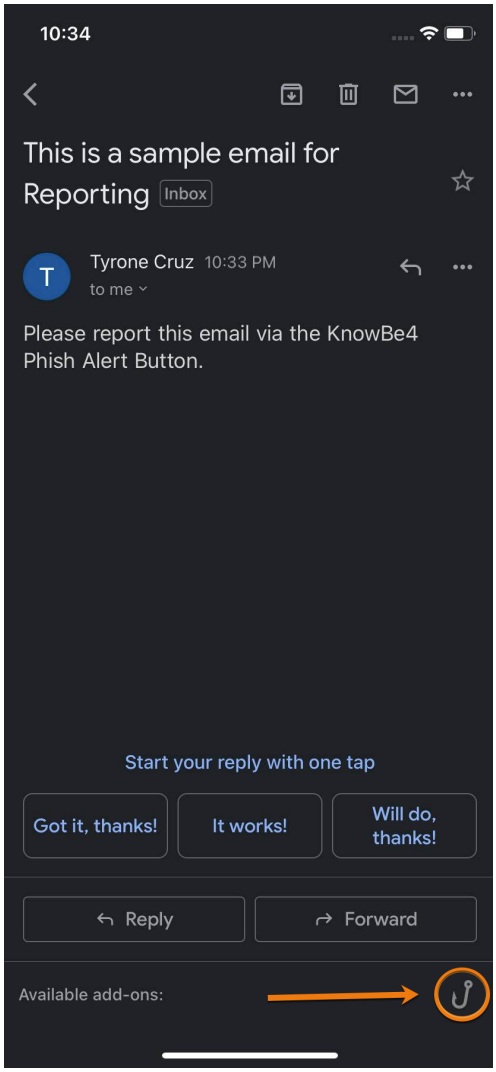
The Phish Alert Button requires you to open the email message to report it. That is safe in GMail. The old advice used to be never open suspicious emails, but that advice applies to antiquated local email clients that could be exploited just by opening a message. GMail's modern web-based interface is not vulnerable to those types of attacks, and many times you need to read the email to decide whether it's really phishing.

1. With the message open in your inbox, click on the **Phish Alert Icon**. Look for it in the column of icons on the right-hand side of the email message, called the side panel. The Phish Alert icon looks like an **orange fish hook**. If you do not see the icons in the side panel, you may need to expand the side panel. Look for a small left-arrow tag in the bottom-right corner of your Gmail window. When you hover your mouse pointer over it, it should say "show side panel." That same tag functions as a toggle that you can use to hide the show or hide the side panel according to your preferences. You will need to show the side panel in order to access the Phish Alert icon.

2. Click the blue Phish Alert button in the side screen that opens to report the email as

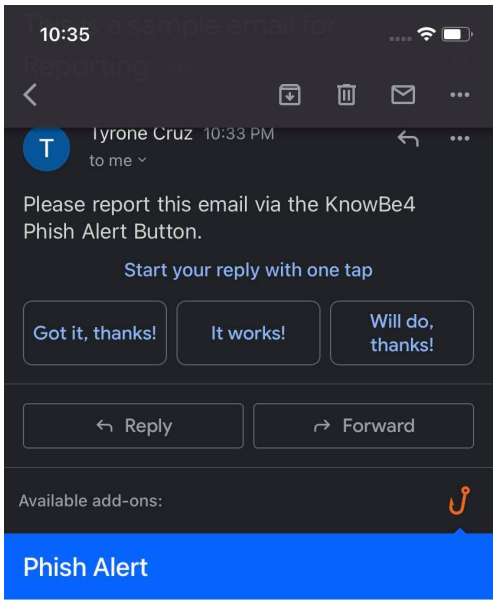
phishing.

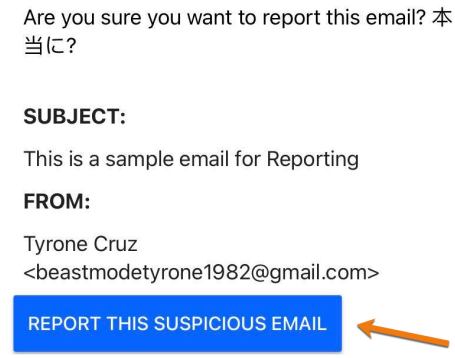
Report in GMail Phone App

1. Open the email that you would like to report.
2. Scroll to the bottom of the screen and locate the available add-ons section.
3. 

4. From the add-ons section, click the **fish hook** icon and scroll down to the bottom of the screen to access the Phish Alert Button.

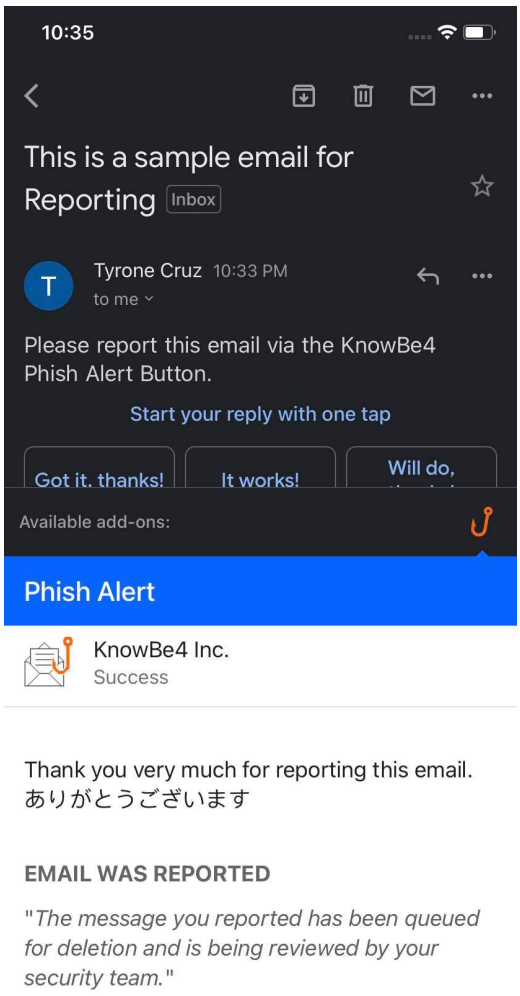
5. Click the blue **Report This Suspicious Email** button to report the email.





6.

7. If enabled, you will see a confirmation message and the email will be moved to your Trash folder.



8. ---

9. Click the back arrow to return to your inbox.