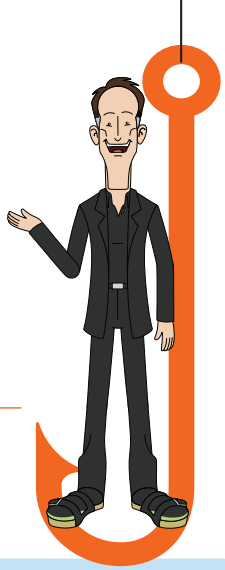
BE A HERO!

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?

You should only report messages you suspect are malicious, like **phishing** or **spear phishing** emails. Reporting annoying messages, like **spam**, to IT will waste their time and resources.

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!

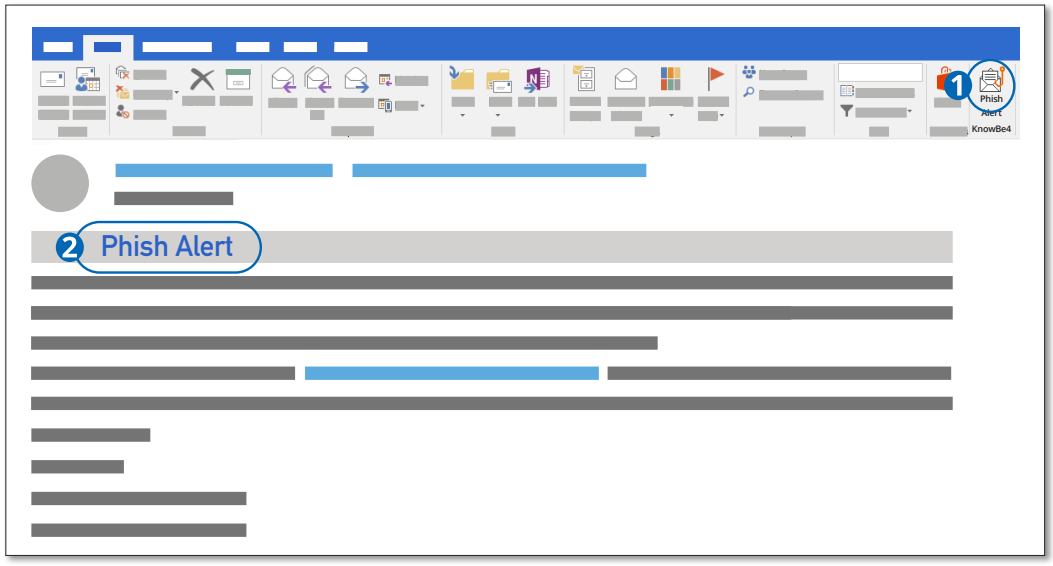
Where do I find the PAB in Outlook?

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."

or

❷ You will also see the words "Phish Alert" in a text link toward the top of an open email.

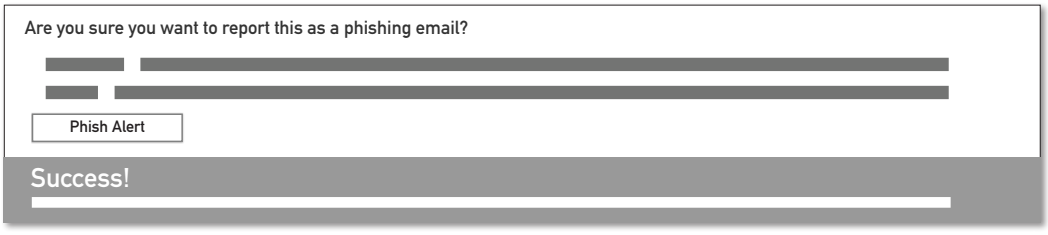


Report:

Report suspected phishing emails by clicking the Phish Alert in the ribbon *or* in the text link at top of the email.

Confirm:

Once you click to report, using either method, 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.