Phish Alert Button
Employees report phishing attacks with one click
Do your users know what to do when they receive a suspicious email?

Should they call the help desk, or forward it? Should they forward to IT including all headers? Delete and not report it, forfeiting a possible early warning?

KnowBe4’s Phish Alert add-in button gives your users a safe way to forward email threats to the security team for analysis and deletes the email from the user’s inbox to prevent future exposure. All with just one click!

When the user clicks the Phish Alert button on a phishing email, the email will be directly forwarded to your Incident Response team.

Has fully customizable button text and user dialog boxes.

Clients supported: Outlook 2010, 2013, 2016 & Outlook for Office 365, Exchange 2013 & 2016, Outlook on the web (Outlook.com), the Outlook Mobile App (iOS and Android), Chrome 54 and later (Linux, OS X, and Windows)
Phish Alert Benefits

- Reinforces your organization’s security culture, users can report suspicious emails with one click.
- Your employee gets instant feedback, which reinforces their training.
- Incident Response gets early phishing alerts from users, creating a network of “sensors”. You can change the receiving email address and add a prefix.
- You can change the user dialog box text regularly to coordinate with your security awareness program. When your user opens email client, the add-in pulls in your updated messaging.
- Easy deployment via MSI file for Outlook, G Suite deployment for Gmail (Chrome).
When the User Clicks the PAB on a Phishing Security Test

Congratulations! The email you reported was a simulated phishing attack initiated by your company. Good job!

When the User Clicks the PAB on a Non-Simulated Phishing Email

Thank you for reporting this email to your security team. Because of people like you, our company is more secure!
Phish Alert: How it Works

A new email arrives in an inbox. The user thinks it’s a phishing attack.

They click on the Phish Alert button.

System determines if email is from KnowBe4.

Yes

Our simulated phishing security tests come with a special SMTP header.

The add-in contacts KnowBe4 servers to record the action of the user in your Admin Console.

The user gets acknowledged for having security top of mind.

The email gets deleted from the user’s inbox.

No

The email could be a legit email, could be spam or a real phish.

The email is sent directly from the user’s email client to your Incident Response Team.

Your IR Team receives a copy of the email with an attachment containing all SMTP headers.
Continue to push down your user’s Phish-prone percentage.

- Reporting of both simulated and real phishing emails involves users even more.
- Your Incident Response Team can act faster on possible real phishing attacks.

Further Enhance Your Management of Social Engineering Threats

![Graph showing a decrease in Phish-prone percentage over time.](image)

- Initial Baseline Phish-prone Percentage: AVG 30%
- 3 Months Later: AVG 15%
- 12 Months Later: AVG 2%

Based on 9 Million Users
Phish Alert

Phish Alert Support Portal
support.knowbe4.com

Questions?
Email support@knowbe4.com
Phone: 888-815-9494

To Learn More

Sales@KnowBe4.com

www.KnowBe4.com

855-566-9234