Stronger Together:

KnowBe4's Phish Alert Button Paired with PhishER Plus and KnowBe4 Defend

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

CR-0706 0426

Introduction

“Stronger together” is not just a motivational slogan. It’s a critical concept in cybersecurity, where all your organization’s people play a role in keeping bad actors out of networks and systems.

As phishing emails get harder to spot, all your users need to know the steps to take when confronted with one. This means your users being able to report phishing emails is not just a nice-to-have, but a core component of your cybersecurity strategy.

Reporting phishing emails empowers your users to be part of the team. Plus, it gives your infosec team essential insight into the threats your technical defenses are missing.

KnowBe4’s Phish Alert Button (PAB) provides your users a safe way to report email threats to the security team for analysis, and automatically deletes the email from the user’s inbox to prevent further exposure. The PAB becomes even more valuable when combined with PhishER Plus, KnowBe4’s lightweight incident response and orchestration platform, and KnowBe4 Defend advanced inbound threat defense. Together these tools combine user engagement and AI-enhanced threat detection.

Read on to explore five ways these tools working together help your organization become more secure and reduce human risk.

1 Make Users Part of the Team

The cornerstone of your defense against phishing and social engineering threats is your users. Their ability to identify and report cyber threats is the foundation for your organization's protection against phishing attacks and the risks they present.

Before your users get a chance to inspect an individual email, KnowBe4 Defend has their back. The AI-powered Defend uses color-coded banners and tags to flag emails-of-interest, keeping users sharp and allowing them to provide the final human vetting and continue to report through the PAB. This turns your workforce into an active security sensor rather than a passive target. Your users need to feel like part of the team (because they are). Their presence on the frontlines of most cyber attacks — the email inbox — makes their awareness of and input on suspicious emails something you need to pay attention to and encourage.

Defend helps give your knowledge they need to make the most secure decisions when it comes to email. The PAB teamed with PhishER Plus makes the most of user input in three ways:

1. If your users are seeing real phishing emails, it means they slipped past your technical defenses. The PAB allows them to report potential phishing attempts, providing a continuous stream of real-world intelligence. This input will prove vital to enhancing the detection capabilities of PhishER Plus and your whole infosec team.

2. Your users need to know the importance of reporting, even if they "PAB" (we coined that verb) an email that turns out to be harmless. PhishER Plus includes automated email response templates to allow your infosec team to quickly communicate back to employees about emails they've reported. This ability gives your user instant feedback after reporting a phishing email with the goal of keeping them engaged with protecting your organization.

3. Users engaged with reporting suspicious emails helps you make the most out of KnowBe4 Security Awareness Training and its massive library of training content. Training lessons are reinforced every time they click the PAB. Every PAB'ed email becomes a stone in a fortified wall against cyber attacks.

The PAB's integration with Microsoft's Outlook email client makes it even easier for your users to report emails. The Microsoft Ribbon PAB allows your users to easily report suspicious emails and help protect your organization from cyberattacks. When you integrate the PAB with Microsoft's integrated spam-reporting feature, the PAB will appear in the Outlook ribbon. When your users click the PAB to report an email, they can provide your IT team with an early warning about potential threats. You can receive reported emails in the Microsoft 365 Defender platform and the KnowBe4 console. This integration delivers a uniform experience across most Outlook versions including the new Outlook for Windows, Outlook for Mac and the web. KnowBe4 has also extended the PAB into Microsoft Teams, extending your defense where the bulk of internal communication lives today.

Your users are a powerful line of defense. By empowering them and integrating them into your security strategy with the PAB, PhishER Plus and Defend, you unlock a formidable force multiplier that harnesses human insight alongside technological capabilities.

2 Use Missed Threats to Your Advantage

The only email threats that make it to the PhishER Plus platform are the ones that made it through every other prior protective control you have. Your users would have helped identify these threats.

While a scary prospect, these missed threats can be used to your advantage with the combination of the PAB and PhishER Plus. User-reported emails sent to the PhishER Plus platform become valuable data that can be used to reduce cybersecurity risk.

PhishER Plus's data is of high importance and low noise. Most other detective controls (e.g., firewalls, intrusion detection, etc.) are "high noise," meaning that they get many false-positive warnings for every real-world threat that should be mitigated. Anyone who has ever reviewed a firewall log understands noisy logs.

PhishER Plus is the opposite. PhishER Plus helps you to figure out "residual risk" from all your other controls and does it in real-time. Finding out what all your other preventative and detective controls are missing is incredibly valuable. It allows the organization to assess why threats are being missed and figure out further mitigations.

Additionally, the PhishRIP feature of PhishER Plus allows similar threats to be automatically pulled from user inboxes before they see them. Once a particular threat is identified, a PhishER Plus administrator can construct a PhishRIP query and ensure that all similar threats are immediately removed so they cannot further harm the environment.

But wait there's more! The PhishFlip feature (also baked into PhishER Plus) lets you "de-fang" (remove the bad stuff) any reported phishing email and sends a safe, simulated copy of it to users through the KnowBe4 simulated phishing platform. So what started as a user-reported email via the PAB can be used for good; to test and engage other users throughout your organization. We'll bet the bad actors who sent the phish in the first place never imagined it'd be used to teach!

3 Augment Human Knowledge with AI

Not even the largest, most well-resourced infosec teams can possibly stay ahead of the phishing/social engineering threat landscape. The threats are too diverse, constantly evolving and increasingly sophisticated. AI has empowered cybercriminals to create new phishing emails capable of evading traditional email security filters.

But AI should also be used for good. KnowBe4 leverages a separation of powers approach using two distinct data models to train the AI engines for maximum coverage on the attacks that native filters were never designed to see:

knowbe4 Defend™

Defend:

Behavioral AI that catches 37% of the threats that SEGs miss. Defend's color-coded banners and tags give users more context on what to be cautious of with incoming emails before they click.

knowbe4 PhishER Plus

PhishER Plus:

Takes those user reported threats and triggers SOC review or immediate remediation depending on how you want to configure your environment.

PhishML is the PhishER Plus machine-learning module that helps you identify and assess the suspicious messages that are reported by your users, at the beginning of your message prioritization process. PhishML analyzes every message coming into the PhishER Plus platform and gives you the info to make your prioritization process easier, faster and more accurate.

PhishER Plus complements Defend by providing thorough threat assessment capabilities, employing PhishML to analyze and categorize reported emails. This powerful combination of AI technologies ensures that both incoming and reported threats are subject to advanced analysis, significantly enhancing your organization's ability to identify and mitigate sophisticated phishing attacks.

PhishML is constantly learning based on the messages that are tagged, not only by you but also by other members of the PhishER Plus user community (more on this later). That means that the learning model is being fed new data to constantly improve its accuracy. More messages can be automatically prioritized based upon PhishER Plus categorization, saving you even more time.

The PAB adds the eyes and mouse-clicking fingers of your users to your defenses to augment Defend's and PhishER's AI-powered capabilities. The PAB allows you to crowdsource phishing defense across your entire organization. In this way new and emerging threats are even more likely to be caught; either by the fine-tuned PhishML capabilities or your properly-trained and vigilant users.

4 Enhance the Power of Your Blocklist

Another benefit of the Defend/PAB/PhishER Plus combination is the strength it brings to the Global Blocklist feature. PhishER Plus's Global Blocklist allows you to create your organization's unique list of blocklist entries and dramatically improve your Microsoft 365 email filters. Blocklist entries of validated threats crowdsourced from 10+ million trained users are leveraged to automatically block matching new incoming messages from reaching your users' inboxes.

Imagine 10+ million trained users across tens of thousands of organizations just like yours sharing information on phishing threats reported via the PAB. This means blocklists where not just your users' reported phishing emails end up, but millions from all over the world.

Let's walk through a step-by-step use case:

1	A user reports a suspicious email using the PAB, with Defend giving context on what makes the email risky
2	PhishER Plus ingests this email and applies machine-learning based rules to the email to mark it as Clean, Threat or Spam, helping you prioritize which messages to add to your blocklist
3	Depending on how the email is tagged, PhishER Plus can run a variety of actions on the email based on what your SOC team wants to do with it
4	The PhishER Plus Blocklist feature allows your infosec team to review the email and set up a blocklist entry that will block future emails like it from getting to your users plus share this information with the global community of PhishER Plus users
5	PhishER Plus will automatically sync with your Microsoft 365 email server to add new blocklist entries
6	With PhishER Plus's Global Blocklist feature, when other KnowBe4 customers report threats using these steps, and the threats are validated by KnowBe4's Threat Research Lab, you'll get the benefit of their contributions automatically

In short, the Global Blocklist plus the PAB lets you harness the power of human intelligence in phishing mitigation. This means your users, teamed with others from around the world, can contribute to an active, never-ending global threat feed. How cool is that?

5 Expert Intelligence Applied to Threats You're Facing

As powerful as AI tools have become, the power of humans is still a key focus for us at KnowBe4. The importance of the human element underpins all our training content and platform development. We see the user as the most important part of any cybersecurity strategy, and we think you should too.

This focus on the human is behind the final feature of PhishER Plus and its connection to the PAB. Once users report a suspicious email via the PAB, its entry into the Global Blocklist is determined by both machine learning and human validation.

Here's where KnowBe4's own human-powered expertise comes in. KnowBe4's Threat Research Lab team compiles data from all PhishER blocklists and other sources to create Global Blocklist entries. This combined power of the KnowBe4 Threat Research Lab and KnowBe4's end-user network around the world helps protect against new and evolving phishing and social engineering attacks.

In this way, multiple layers of human-curated (human-reported, human-analyzed, and human-vetted) phishing threat intelligence supported by AI-based analysis is equipped to protect your organization from new phishing attacks. This approach will help ensure a proactive and faster response time to the latest wave of phishing attacks against your organization.

PhishER Plus, Defend and the PAB: A Winning Combination

You need a layered separation-of-powers approach that uses two AI models to catch the intent-based threats that native filters were not designed to detect.

PhishER Plus combines robust machine learning-powered email analysis, prioritization, inoculation and blocklisting capabilities with the industry's most powerful global threat feed for proactive anti-phishing protection. PhishER Plus is powered by a triple-validated, global threat feed that automatically blocks phishing attacks before they reach your users' inboxes.

The machine-learning power behind Defend lets you move from reactive triage to proactive protection. This reduces your risk exposure while continuing to increase productivity across the organization.

Adding PAB to the mix lets you make the most out of the user engagement and awareness you've worked so hard to to build. The feedback loop these tools create together improves phishing detection, helps you prioritize real threats and reinforces your security culture.

Learn more about

Phish Alert Button

PhishER Plus

Defend

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before bad actors do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 empowers the human and AI workforce to make safer security decisions every day. Trusted by over 70,000 organizations worldwide, we help strengthen security culture and manage risk. Our comprehensive AI-driven HRM+ platform includes awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents, and more. As the only global security platform of its kind, KnowBe4 provides personalized content, tools, and techniques to keep the modern workforce safe from phishing, vishing, deepfakes, and emerging threats.

For more information, please visit www.KnowBe4.com.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com