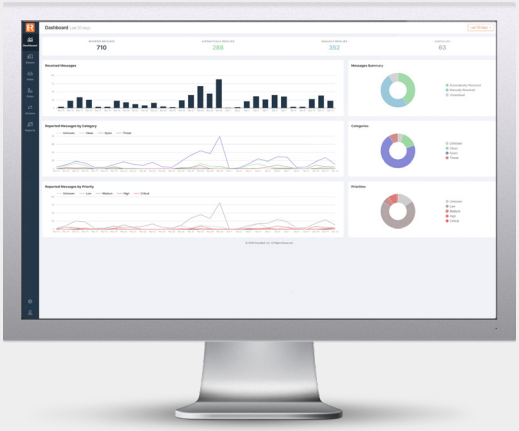
PhishER

KnowBe4
Human error. Conquered.



Key Benefits

- Full integration with KnowBe4's Phish Alert Button allows automatic prioritization of emails that are not threats
- Cut through the IR-inbox noise and respond to the most dangerous threats more quickly and efficiently
- Free up IR resources to identify and manage the 90% of messages that are either spam or legitimate email
- See clusters or groups of messages based on patterns that can help you identify a widespread phishing attack against your organization
- Meet critical SLAs within your organization to process and prioritize threats and legitimate emails
- Automated email response templates let you quickly communicate back to your employees about the emails they need in order to continue working
- You can create custom workflows for tasks such as prioritization and alerting so that the IR team can focus on the right messages

Identify and respond to email threats faster with PhishER

Because phishing remains the most widely used cyber attack vector, most end users report a lot of email messages they "think" could be potentially malicious to your incident response team. Whether or not you step employees through security awareness training doesn't change the fact that your users are likely already reporting potentially dangerous emails in some fashion within your organization. **The increase of this email traffic... can present a new problem!**

With the firehose of spam and malicious email that attack your network, some 10-15% of these make it past your filters. With only approximately 1 in 10 user-reported emails being verified as actually malicious, how do you not only handle the high-risk phishing attacks and threats, but also effectively manage the other 90% of user-reported messages accurately and efficiently? **PhishER™**.

What is PhishER?

PhishER is your lightweight SOAR platform to orchestrate your threat response and manage the high volume of potentially malicious email messages reported by your users. And, with automatic prioritization of emails, PhishER helps your InfoSec and Security Operations teams cut through the inbox noise and respond to the most dangerous threats more quickly.

Additionally, with PhishER you are able automate the management of the 90% of reported emails that are not threats. Incident Response (IR) orchestration can easily deliver immediate efficiencies to your security team, but the potential value is much greater than that. With the right strategy and planning, your organization can build a fully orchestrated and intelligent SOC that can contend with today's threats.

PhishER is a critical element to help your IR teams work together to mitigate the phishing threat and is suited for any organization that wants to automatically prioritize and manage potentially malicious messages—accurately and fast! PhishER is available as a stand-alone product or as an add-on option for KnowBe4 customers.

Why Choose PhishER?

PhishER is a simple and easy-to-use web-based platform with critical functionality that serves as your phishing emergency room to identify and respond to user-reported messages. PhishER helps you prioritize and analyze what messages are legitimate and what messages are not—*quickly*.

With PhishER, your team can prioritize, analyze, and manage a large volume of email messages—fast! The goal is to help you and your team prioritize as many messages as possible automatically, with an opportunity to review PhishER's recommended focus points and take the actions you desire.

How PhishER Works

PhishER processes user-reported phishing and other suspicious emails by grouping and categorizing emails based on rules, tags, and actions.

Automatic Message Prioritization

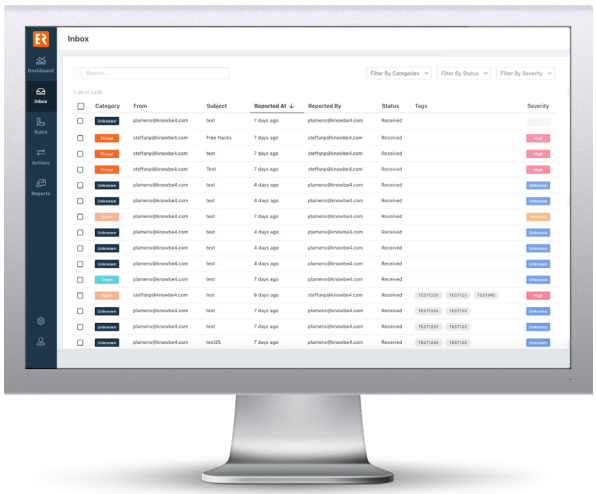
PhishER will help you prioritize every reported message into one of three categories: Clean, Spam, or Threat. Through rules you set, PhishER helps you develop your process to automatically prioritize as many messages as possible without human interaction.

With automatic prioritization of emails that are not threats, PhishER helps your team respond to the most dangerous threats more quickly. PhishER easily integrates with KnowBe4's email-add in button, Phish Alert and also works by forwarding to a dedicated mailbox.

Emergency Rooms

PhishER features "Emergency Rooms" to help you identify similar messages reported by your users. Emergency Rooms consist of pre-filtered views of your messages that are unresolved in your PhishER inbox. These messages are dynamically grouped by commonalities and include system pre-filtered views for messages by Top Subject Lines, Top Senders, Top Attachments, and Top URLs.

Each room is interactive, allowing you to drill down into filtered inbox views of the messages and take action across all associated messages at the same time.



PhishML™

PhishML is a PhishER 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 platform and gives you the info to make your prioritization process easier, faster, and more accurate.

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

Simple and Advanced Rule Creation

You can create custom rules, use the built-in YARA-based system rules, or edit existing YARA rules. You can use system rules to help simplify your rules requirements or copy and modify to customize rules depending on the proficiency of your incident response team.

Data Enrichment Intelligence

PhishER integrates with external services like VirusTotal to help analyze attachments and malicious domains. Using URL Unwinding, PhishER automatically expands shortened URLs to help see the potential threat level of the final destination.

SIEM Integrations

PhishER integrates into your organization by pushing data into popular SIEM platforms such as Splunk and QRadar. With support for multiple syslog destinations available it's also possible to push data into as many other systems as you like.

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

August 2019