PhishER

KnowBe4
Human error. Conquered.

Identify and respond to email threats faster with PhishER

Because phishing remains the most widely used cyberattack vector, most end users report a lot of email messages that they 'think' could be potentially malicious to your incident response team. Whether or not you take 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 organisation. **The increase of this email traffic can present a new problem!**

With the fire hose of spam and malicious emails that attack your network, some 7–10% 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 the key ingredient of an essential security workstream. It's 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 prioritisation of emails, PhishER helps your InfoSec and Security Operations teams cut through the inbox noise and respond to the most dangerous threats more quickly.

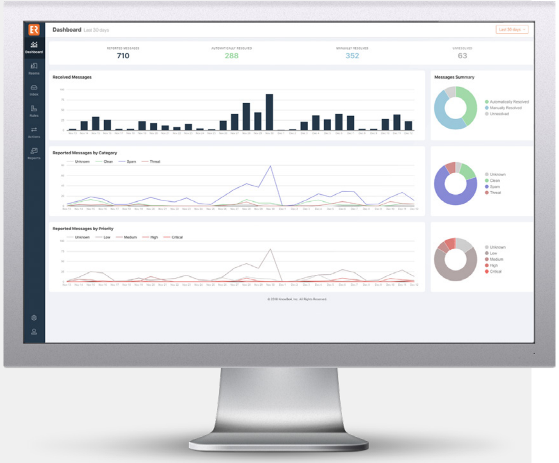
Additionally, with PhishER you are able to automate the workstream of the 90% of reported emails that are not threats. Incident Response (IR) orchestration can easily deliver immediate efficiencies to your security team, but the potential value is much greater than that. With the right strategy and planning,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

PhishER enables a critical workstream to help your IR teams work together to mitigate the phishing threat and is suited for any organisation that wants to automatically prioritise and manage potentially malicious messages - quickly and accurately! 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 workstream functionality that serves as your phishing emergency room to identify and respond to user-reported messages. PhishER helps you to prioritise and analyse what messages are legitimate and what messages are not - quickly.

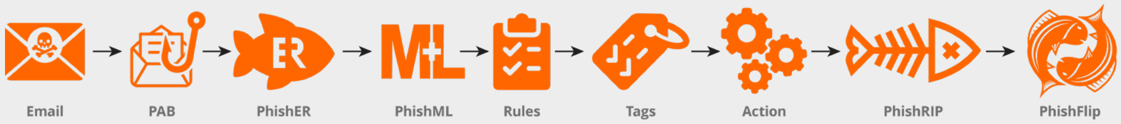
With PhishER, your team can prioritise, analyse and manage a large volume of email messages - fast! The goal is to help you and your team prioritise as many messages as possible automatically, with an opportunity to review PhishER's recommended focus points and take the actions you desire.



Key Benefits

- Full integration with KnowBe4's Phish Alert Button allows automatic prioritisation 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 organisation
- Meet critical SLAs within your organisation to process and prioritise 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
- Create custom workflows for tasks such as prioritisation and alerting so that the IR team can focus on the right messages

How PhishER Works



PhishER processes user-reported phishing and other suspicious emails by grouping and categorising emails based on rules, tags and actions. PhishML, the custom machine-learning module, analyses messages and generates confidence values which are used to tag messages. PhishRIP helps you to easily find and quarantine suspicious messages that are still sitting in inboxes across your entire organisation. PhishFlip automatically turns defanged phishing emails into training opportunities by flipping them into simulated phishing campaigns.

Automatic Message Prioritisation

PhishER helps you to prioritise every reported message into one of three categories: Clean, Spam or Threat. Using YARA rules, you assign what's most important to you and PhishER helps to develop a process to automatically prioritise as many messages as possible without human interaction.

PhishER helps your team respond to the most dangerous threats more quickly by reviewing the attributes of reported messages and ranking the most critical messages based on priority.

Emergency Rooms

Emergency Rooms help you to identify similar messages reported by your users. PhishER groups these messages by commonalities and includes pre-filtered views for messages by Top Subject Lines, Top Senders, Top Attachments and Top URLs.

Each Emergency Room is interactive, allowing you to drill down into filtered inbox views and take action across all related messages.

Integrations

With PhishER's API integration and support for multiple syslog destinations, you can connect PhishER with your existing security stack products to push data into popular email security, threat intelligence, ticketing and SIEM platforms. Additionally, you can send events from PhishER and add them to your users' timelines in your KnowBe4 platform. You can use these events to help tailor specific phishing and training campaigns that enable your users to better identify and report suspicious emails through the Phish Alert Button.

PhishER also integrates with external services such as VirusTotal to help analyse attachments and malicious domains.

Microsoft 365 Blocklist

With the PhishER Blocklist feature, it's easy to create your organisation's unique list of blocklist entries and dramatically improve your Microsoft 365 email filters without ever leaving the PhishER console. You can use reported messages to prevent future malicious emails with the same sender, URL or attachment from reaching other users.

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 prioritisation process. PhishML analyses every message coming into the PhishER platform and gives you the info to make your prioritisation 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 prioritised based upon PhishER categorisation, saving you even more time.

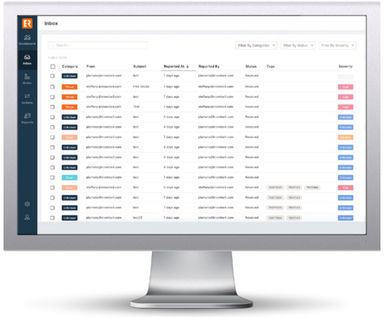
PhishRIP™

PhishRIP is an email quarantine feature that integrates with Microsoft 365 and Google Workspace so that your incident response team can quickly and easily remediate.

PhishRIP enables you to remove an identified threat from all user inboxes, inoculate unreported threats and protect from future threats by deleting, quarantining or restoring legitimate emails.

PhishFlip™

PhishFlip is a PhishER feature that automatically turns user-reported phishing attacks targeted at your organisation into safe simulated phishing campaigns in your KnowBe4 platform. With PhishFlip, you can now immediately 'flip' a dangerous attack into an instant real-world training opportunity for your users.



For more information visit: www.KnowBe4.com