PhishER: Why is it a Must Have?

The Problem

Phishing remains the most widely used cyber attack vector. Organizations that have trained their users through simulated phishing tests and security awareness training, and have armed them with the Phish Alert Button can run into 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.

Many of those emails are reported by users to your security response team - and they have to handle them as quickly as possibel . The sheer volume of potential malicious email reported by your users can get overwhelming. Since each message requires some level of analysis and possibly human intervention to prioritize,organizations with limited Incident Response staff need a simple and effective way to respond to and mitigate these reported messages.

With only approximately 1 in 10 user-reported emails being verified as actually malicious in some form, how do you not only handle the phishing attacks and threats—and just as importantly—effectively manage the other 90% of user-reported messages accurately and efficiently?

Specific Problems that IT Admins Face:

- *Training your users is paying off, but training creates cautious users and an influx of potentially thousands of user-reported messages that must be analyzed and prioritized.*
- *Your team has operational SLAs to analyze potentially malicious messages within a certain amount of time, how do you filter through the IR-inbox noise quickly and efficiently?*
- *90% of messages reported to your security response team are not phishing or malicious but need to be handled fast so the important messages get back to your users.*

Managing the Problem

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.

Identify and respond to email threats faster with PhishER.

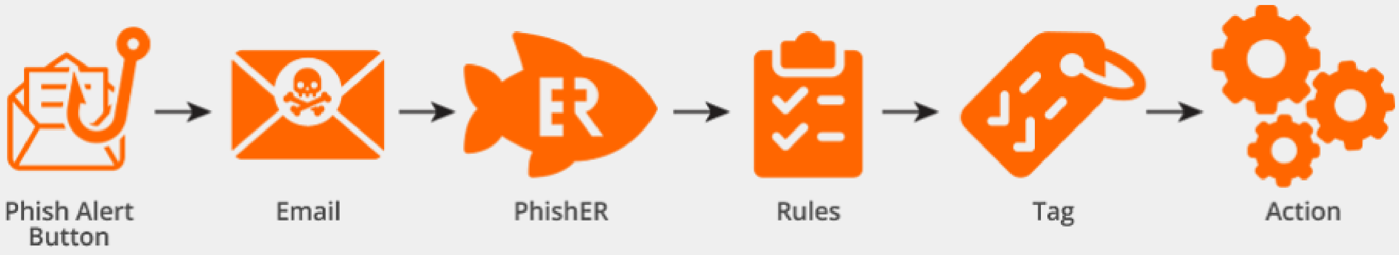
PhishER is a simple and lightweight SOAR platform with critical functionality that serves as your email emergency room to identify and respond to user-reported messages. PhishER helps you analyze and prioritize what messages are legitimate and what messages are not - quickly.

PhishER reviews message attributes of reported messages from KnowBe4's Phish Alert Button and stack ranks the most critical messages based on severity. By identifying similarities between user-reported threats, PhishER helps you see clusters or groups of messages based on patterns that can help you determine real phishing attacks against your organization. Using built-in YARA-based system rules, PhishER helps you analyze messages faster with recommended focal points (Emergency Rooms) where you have the opportunity to review and take the actions you desire.

With automatic identification of emails that are not threats, PhishER helps your InfoSec and security operations teams cut through the IR-inbox noise. With PhishER, you are able to identify the most dangerous threats more quickly by helping you automate the prioritization of the 90% of reported emails that are not threats.

With PhishER, your team can analyze, prioritize and manage threats. With data enrichment services and an intelligent engine technology process, PhishER helps you analyze 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 priority status and take the actions you desire.

How PhishER Works



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. PhishER reviews attributes of reported messages and stack ranks the most critical messages based on priority.

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.

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. The overview of the Emergency Rooms allows you to immediately prioritize which room contains the most messages and is in need of attention.

Best of all, you can define criteria to create your own room and highlight what means the most to your organization. Interested in how many messages are spoofing your executives or how many legitimate HR notices are being reported by your users? How about finding out if there is a widespread generic phish campaign that many users are reporting? Emergency Rooms will give you all that and more.

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.