KnowBe4
Human error. Conquered.

Overcoming the Phishing Tsunami: A Game-Changing Strategy for Stopping Phishing

In the complex world of cybersecurity, phishing attacks often feel like an unrelenting tsunami, flooding your organization with a never-ending deluge of threats. As an IT or infosec professional, you're on the front lines, battling the waves, while the risk of phishing attacks continues to escalate.

Traditional methods for analyzing and mitigating phishing attacks are manual, repetitive and error-prone. IT and infosec experts are left combating increasingly sophisticated phishing threats with outdated tools and workflows. These workflows slow the speed at which you can mitigate a spear-phishing attack and increases the risk that phishing presents to your organization.

Lastly, they serve as an anchor to any incident response plan tasked with quickly mitigating the damage from a targeted phishing campaign and provide no protection against the phishing emails that make it past your legacy security filters.

Fortunately, there is a smarter way. Shift the burden off your IT team to a unique, AI-powered system built from the ground up that automates workflows and uses crowdsourced threat intelligence to improve accuracy and speed time to mitigation. This allows you to focus on orchestration and analysis, mitigating the risk that sophisticated phishing attacks pose to your organization.

THE TRADITIONAL WAY: PADDLING AGAINST THE CURRENT

At many organizations, the process of reporting malicious emails is outdated. Users manually report malicious emails by forwarding them to their IT department, where they fall into the depths of an IT department's general inbox awaiting manual triage. The larger an organization grows, the bigger the problem gets. This archaic process creates five major challenges that increase the risk phishing poses to your organization:

1 **ALERT OVERLOAD**
Excessive alert noise from the firehose of user-reported emails, some of which are high-risk phishing threats, the majority of which are not. Only one in 10 user-reported emails end up being malicious, leaving the remaining 90% of reported messages to be vetted manually. Without AI-driven threat analysis, incident response (IR) and security operation center (SOC) teams rely on manual processes that leverage spreadsheets and uncover little in the way of threat analysis. On average, it takes 27 minutes to manually triage a phishing email.[1] A poor mean time to respond (MTTR) increases risk and potential damages from a phishing attack.

2 **STRESSING ALREADY LIMITED RESOURCES**
It creates additional work for understaffed and under-resourced IT teams. Case in point: 61% of mid-sized organizations do not have a dedicated cybersecurity expert on staff, and on average, for every 10 IT employees at an organization, only one is dedicated to cybersecurity.[2]

3 **DISENGAGED EMPLOYEES**
It disenfranchises employees who never receive a response or confirmation that the forwarded email was received and analyzed. This undermines any security awareness training the organization is delivering, becoming a roadblock to building a security culture.

---

1 The Business Cost of Phishing, 2022 Report

2 State of Cybersecurity for Mid-Sized Businesses, 2023

4 **INABILITY TO STOP THE TSUNAMI**

Increasing percentages of phishing emails are making it past secure email gateways and into your users' inboxes. According to ArmorBlox, 56% of email-based attacks bypassed legacy security filters in 2022, and 18.8% of phishing emails bypassed Microsoft Exchange Online Protection and Defender to make it to a user's inbox, according to a report by the Check Point Email Research Team.[3] Lastly, threat actors are increasingly using image-based textual messages to evade text-based security filters.[4] Outdated phishing email analysis and mitigation strategies provide no layer of anti-phishing protection to your organization.

5 **SLOW RESPONSE TO TARGETED ATTACKS**

Old-school methodologies prevent your organization from mitigating a targeted phishing attack, such as a spear phishing campaign, in real time. In this scenario, multiple users are likely receiving the same phishing emails. Old-school workflows provide no ability to identify a targeted phishing campaign during its early stages and mitigate the threat in real time by quarantining phishing emails from inboxes before a malicious link is clicked on.

A NEW STRATEGIC APPROACH: CHANNELING THE CURRENT

The best phishing protection is a system that provides finely-tuned, automated identification and mitigation combined with crowdsourced threat intelligence for superior protection.

A Security Orchestration, Automation and Response (SOAR) designed specifically for phishing threat response and management is an essential component for IR and SOC teams. A SOAR platform like PhishER Plus will empower your security team to reduce MTTR and mitigate phishing threats before they make it into your users' inbox. It will also allow security teams to reprioritize the phishing threat and bring it "front and center" in the eyes of executive leadership.

The addition of AI-powered automation and crowdsourced threat intelligence will supercharge your organization's email security defenses and be the biggest benefit for IR and SOC teams. They act as a force multiplier for security teams by providing scalability, accuracy and real-time response via a number of capabilities:

- **Automatic analysis and prioritization of emails to eliminate the guesswork of identifying high-risk phishing threats from all the user-reported messages.** A SOAR should allow your security team to automatically prioritize as many messages as possible without human interaction by reviewing reported messages and ranking based on severity/priority.
- **Automate the security workstream for managing the "other 90%" of user-reported emails.** Only 1 in 10 user-reported emails are actually malicious. A SOAR solution should free up SOC and IR resources by automating the identification and management of emails that are simply spam or legitimate communications.
- **Automated email responses to allow IT to quickly communicate with employees. Rather than manually coordinating company-wide communications during a phishing attack,** automation should provide a SOC and IR team with automated response workflows and/or email response templates to allow your security personnel to quickly communicate with employees about which emails are legitimate so they can continue to work.

---

3 Check Point Microsoft Defender Report

4 INKY Malicious QR Codes Are Quickly Retrieving Employee Credentials

- **Group or cluster messages based on patterns to allow incident response teams to identify a widespread phishing attack.** Messages should be dynamically grouped by commonalities based on rules, tags and actions. This should include the ability for pre-filtered viewing of messages by subject line, senders, attachments, URLs, etc.
- **Provide an additional layer of protection after your existing secure email gateways and other security filters fail.** Harness the power of crowdsourced threat intelligence and AI-powered blocklisting to automatically quarantine and remove phishing threats from your users' inboxes based on real-world phishing threats that millions of other end-users have already reported.
- **The ability to take real-world phishing attacks and change them into simulated phishing templates to train your employees.** Real email threats that have been removed and quarantined should be turned into "defanged" versions that can be leveraged as part of a simulated phishing campaign.

In particular, crowdsourced threat intelligence and analysis has emerged as a vital defense and proactive response to increasingly sophisticated phishing threats. It provides an organization with the diverse perspectives and experiences of the many to vastly increase the potential to detect, report and block an array of phishing and social engineering attacks.

WHY THIS STRATEGIC APPROACH IS CRUCIAL TO YOUR INCIDENT RESPONSE PLAN

A solid incident response plan is your best tool for fending off a targeted phishing attack.

Despite this, having an incident response plan in place appears to be as much the exception as a steadfast rule. Currently, only 45% of organizations have an enterprise-wide incident response plan in place.[5] Many organizations have none, or if they do, it's focused on particular use cases and/or departments. This sobering statistic is largely due to understaffed security teams that are overloaded with system management and infrastructure upgrades, and/or working with outdated workflows and processes.

Outdated workflows and processes become a particular problem when responding to a phishing attack. Many incident response plans are too slow to respond due to the sheer volume of reported messages. Additionally, a targeted phishing campaign can tie up your organization's IT help desk due to the influx of user-generated tickets.

Time is of the essence when it comes to mitigating a phishing attack. Can your incident response plan allow your organization to quickly identify the threat and cut it off before it spreads throughout your organization's inboxes and an employee clicks on it? Do your phishing management and analysis workflows and systems support this?

The aforementioned capabilities that a SOAR product delivers will provide crucial information and mitigation actions during a targeted phishing attack. Here are some of the most pivotal:

- Cut through the mail clutter and allow your IR and SOC teams to focus on the high-level threats
- Orchestrate threat response and manage the high volumes of user-reported messages

---

5 2022 research from FRSecure

- Automate workload distribution to implement a multi-tiered incident response system based on severity levels
- Allow your organization to build a fully orchestrated and more intelligent SOC team that can identify and mitigate social engineering threats in near real-time
- Block email threats that have bypassed other email security filters or systems before they reach users' mailboxes
- The ability to remove the same/similar emails from all mail folders and then execute blocklisting to prevent additional attempts from reaching your organization
- Automate communications with employees during a targeted campaign to provide users with immediate feedback about whether the email was a real phishing attempt, spam or a legitimate communication. This improves overall security awareness among employees and provides positive feedback that they're keeping your organization more secure.

When it comes to post-mortem analysis following an attack, a SOAR platform will prove vital to stopping future attacks. It provides the ability to analyze phishing threats and conduct reporting on the types of social engineering threats encountered so SOC teams can quantify the threat landscape, and thus risk, with executive leadership.

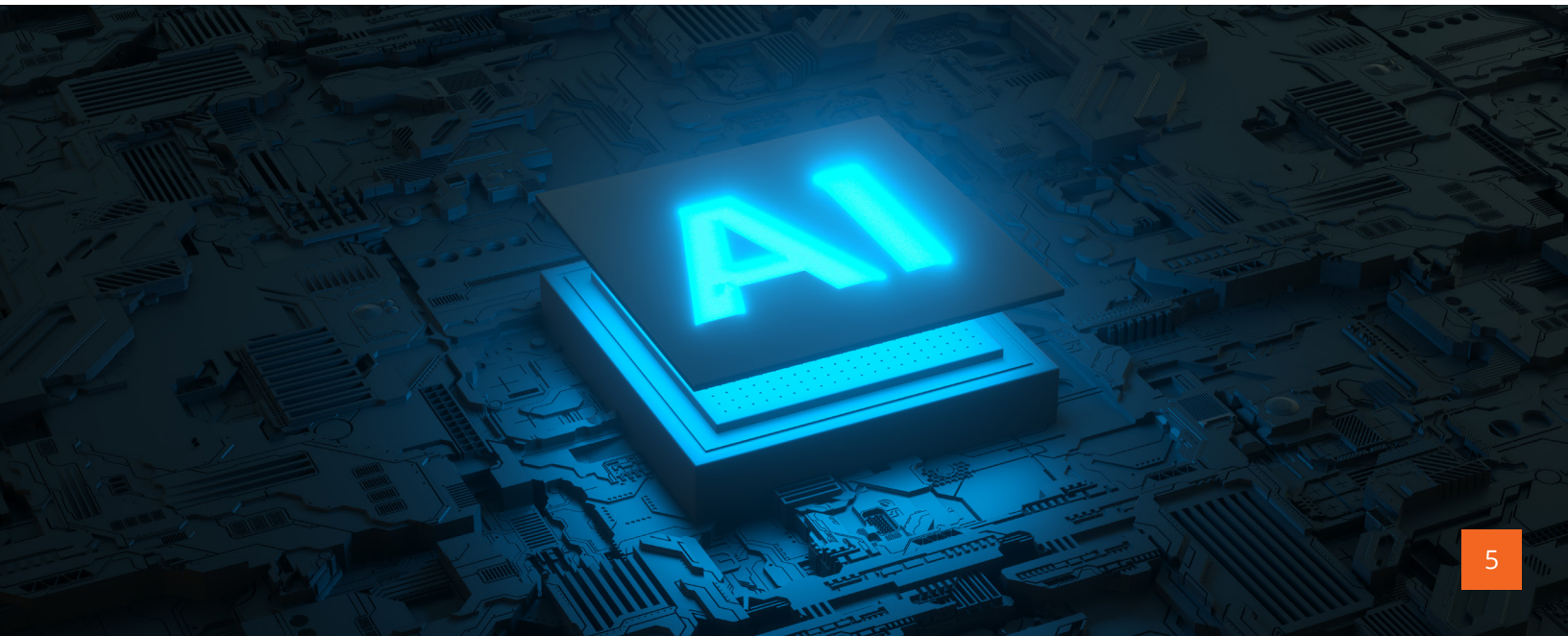
Did your organization primarily face malware, ransomware or business email compromise phishing threats last quarter? An enterprise-grade SOAR platform will go a long way in answering those questions so your organization can prioritize budget and security resources accordingly.

WHAT YOU CAN DO ABOUT IT

In this new era of AI-generated phishing threats, it's time to retire manually-driven workflows. Your strategic approach offers a smarter way to identify and prioritize high-threat phishing emails, supercharging your defenses with AI-powered threat intelligence.

It enables you to deploy a fully orchestrated IR or SOC team capable of mitigating phishing attacks in minutes, not hours. And most importantly, it provides the foundation for you to accurately analyze and report the risk that phishing presents to your organization.

So, let's navigate this phishing tsunami together, with a strategic, smart approach.



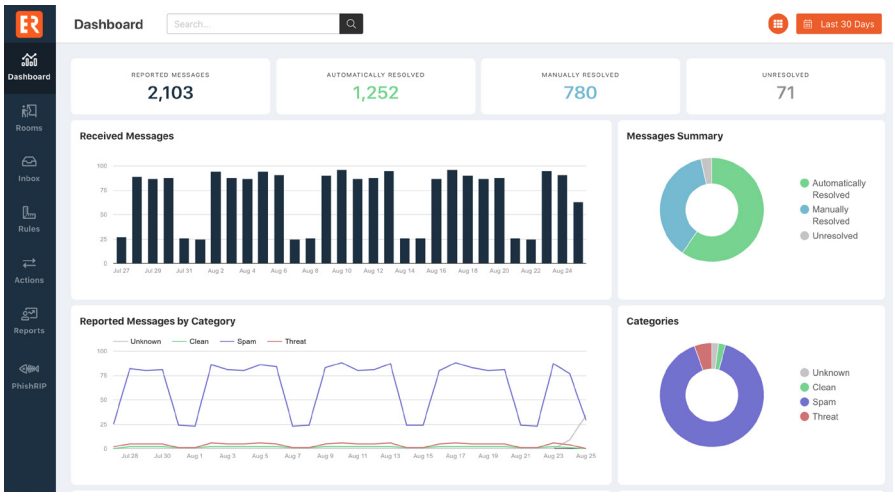
KNOWBE4 PHISHER PLUS

PhishER Plus is a lightweight SOAR product designed to orchestrate your phishing threat response and supercharge your organization's email security defenses. 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. There are three critical components powering the PhishER Plus global threat feed:

6 10+ million KnowBe4 users that identify and report real-world, active phishing and social engineering attacks to PhishER

7 PhishER administrators analyze and review user-reported messages, add them to their private blacklist and create PhishRIP queries, which is then used to aggregate PhishER Plus



8 KnowBe4's Threat Research Lab is a dedicated team of researchers that collect, analyze and validate identified email threats before adding entries to the PhishER Plus Global Blocklist threat feed

---

Identify and respond to phishing threats faster with KnowBe4's PhishER Plus.

Learn More

Request a demo of KnowBe4's PhishER Plus

Request Demo

Additional Resources

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 the bad guys do

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

About KnowBe4

KnowBe4 is the provider of the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

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

01D08K01