KnowBe4
Human error. Conquered.

The Power of the PhishER Blocklist

Leveraging Your Last Line of Defense To Protect Your Entire Organization

INTRODUCTION

You hear the phrase “blocklist” and you likely think, “Yeah, I know how important blocklist email filtering is already.”

Great. We’re not here to convince you how important email filtering tools are.

Like the 98% of CISOs surveyed in a recent email security report, you likely either have a tool in place to monitor and protect against email-borne threats, or you’re planning to roll one out. Blocklisting is vital to keeping phishing emails out of your users’ inboxes before they get a chance to click.

Even with tools in place, maintaining and monitoring a blocklist can mean a great deal of work for already-busy Security Operations Centers (SOC). This is where the explosion of artificial intelligence (AI) and machine learning has come in. In the same report referenced above, nearly half of respondents (49%) said they were using some combination of AI and machine learning to make their SOC’s job easier.

But even the smartest AI-based platforms miss sometimes. Phishing emails still get past email filters and blocklists, making your users the last line of defense against potentially devastating cyber attacks. Users need to become part of, not a hurdle to, a robust and efficient email security strategy.

The unique and powerful combination of user-reported phishing emails and machine learning is the foundation of KnowBe4’s PhishER platform. PhishER is a lightweight security orchestration, automation and response (SOAR) tool that helps your InfoSec and SOC team cut through the inbox noise and respond to the most dangerous threats more quickly.

In this whitepaper, you’ll learn how the blocklist feature built into PhishER helps make the most of its machine-learning capabilities through user input. See how you can improve your Microsoft 365 email filters using reported messages to keep similar phishing emails from reaching the rest of your user base.

RELIEVING AN OVERWORKED SOC

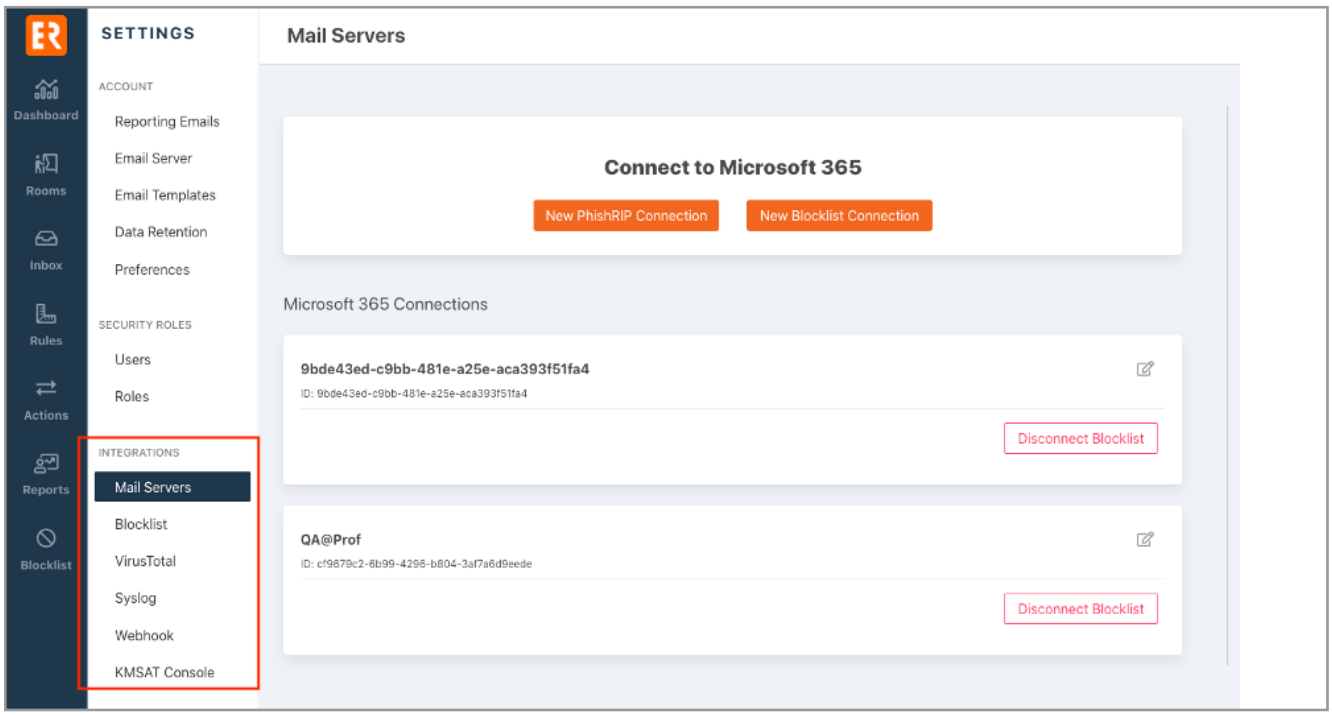
SOC team members are unsung heroes. “Hackers” seem to get an unfair share of the limelight in Hollywood blockbusters, even if they are shown working from the ubiquitous poorly-lit basement.

Few movies tend to focus on the “light” side of cybersecurity in which dozens of overworked IT professionals sift through reams of log files and network status reports, diligently keeping a secure but fragile status quo.

Email filtering and analysis has become an increasingly vital part of this work, as bad actors focus on social engineering to infiltrate and compromise networks and systems. Cybercriminals often target multiple users with the same attack over time. These malicious emails can still reach other users in your organization unless they are added to your blocklist.

Our own PhishER data illustrates how prevalent email attacks are. In just one month, PhishER’s automated PhishRIP feature removed 4.5 million malicious messages from user inboxes. All these emails likely made it past some form of email management tool or another.

With the PhishER Blocklist feature, malicious emails just like these can be used to craft blocklists for your Microsoft 365 email filters directly from the PhishER platform. An analyst on your SOC team using PhishER can all-at-once see what sort of emails are making it through your tech stack (Secure Email Gateway, firewall, anti-virus software, spam filters, etc.) and better align your blocklist to filter them out.



Build blocklists for your Microsoft 365 email filters directly from the PhishER platform.

In this way, PhishER and its blocklist feature become a force multiplier for your SOC team, allowing time-strapped analysts to focus more time on higher priorities. A blocklist informed in-part by user input (more on that later) will help prevent future malicious email with the same sender, URL or attachment from reaching other users without additional direct analyst input.

Your SOC team is already full of low-key superheroes. PhishER gives them the tools to make the most of their superpowers.

MAKING YOUR USERS PART OF THE TEAM

Your SOC team's many responsibilities have made automation and machine learning critical, but a robust tech stack or single tool can only do so much on its own. You should be willing to trust in your users to do the right thing and equip them with the knowledge, training and tools that will help them be part of the larger infosec team.

Think of it this way: That 4.5 million figure from earlier means users helped turn away close to that many emails by reporting them. Your users really are your last line of defense!

We're sure you won't be surprised when we mention how a robust security awareness training program makes PhishER and the blocklist feature even more powerful. New-school security awareness training leads to behavior change, which means less risk for your organization.

But what does training have to do with the blocklist feature? We're glad you asked!

KnowBe4's new-school training combined with our no-charge Phish Alert Button (PAB) allows users to take action immediately on any email they think is suspicious. Once installed in your email client, the PAB gives users a one-click option to report phishy emails to a pre-designated IT inbox or directly to the PhishER platform.

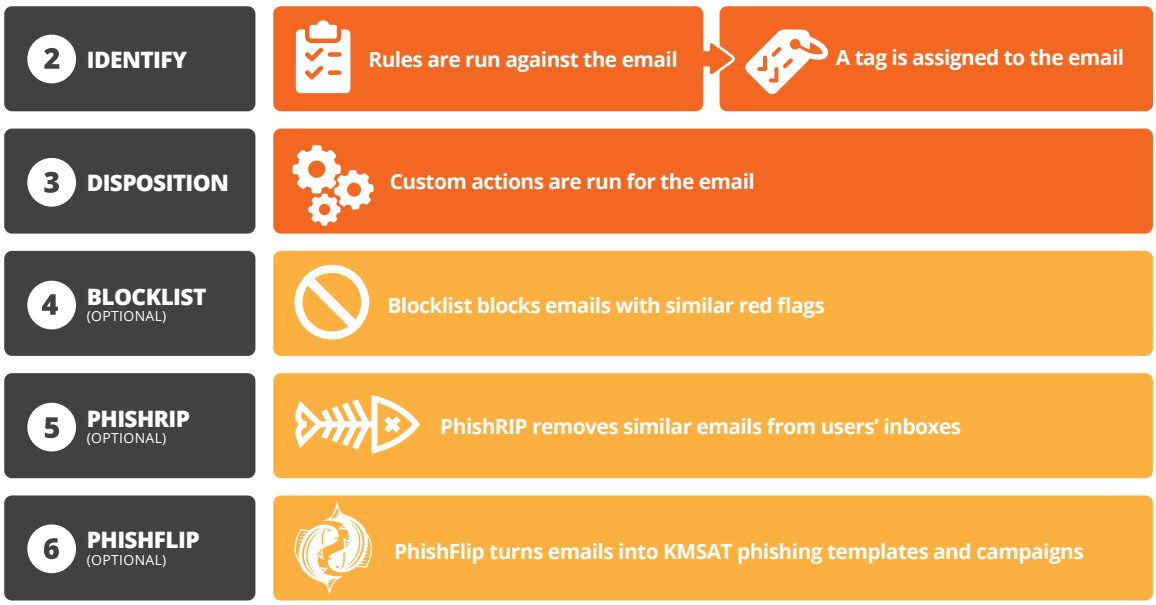
Once in PhishER, your SOC team can quickly create rules that remove emails similar to the reported messages (using PhishER's PhishRIP feature) and adjust your Microsoft 365 blocklist to dramatically improve your Microsoft 365 email filters without ever leaving the PhishER console. In this way, the blocklist feature helps turn your users' efforts into information that can help your entire organization.

BLOCKLIST USE CASE

Let's walk through a PhishER blocklist use case (presuming PhishER is installed and in use):

1. Using the Phish Alert Button, or other means, a user reports a suspicious email
2. PhishER ingests this email and applies machine-learning based rules to the email to mark it as Clean, Threat or Spam
3. Depending on how the email is tagged, PhishER can run a variety of actions on the email based on what your SOC team wants to do with it
4. With PhishER's machine-learning feature PhishML enabled, you can use PhishML tags to help you prioritize messages with attributes that you want to add to the blocklist
5. The blocklist feature allows your SOC team to review the email and set up a blocklist entry that will block future emails like it from getting to your users
6. PhishER will automatically sync with your Microsoft 365 email server to add new blocklist entries

PhishER Workflow



CONCLUSION

No blocklist is perfect. No email filtering tool is perfect. Your SOC team likely has dozens of fires to put out at any given time. Phishing emails making it through your existing tech stack aren't doing them any favors.

The only email threats that make it to KnowBe4's PhishER platform are the ones that made it through every other prior protective control you have. Your users would have helped catch these threats.

The PhishER blocklist feature helps your SOC make the most of user efforts, saving themselves time, and your organization money. Leverage the intelligence of your users reporting real threats to create another layer of security that further strengthens your human firewall.

Learn What PhishER Can Do for You

The blocklist feature is not the only benefit of PhishER that helps SOC teams identify and respond to email threats faster. Learn more about PhishER and see how it can:

- Automate prioritization of email messages by rules you set that categorize messages as Clean, Spam, or Threat
- Augment your analysis and prioritization of messages with PhishML, a PhishER's machine-learning module
- Search, find and remove email threats with PhishRIP, PhishER's email quarantine feature for Microsoft 365 and Google Workspace
- Automatically flip active phishing attacks into safe simulated phishing campaigns with PhishFlip. You can even replace active phishing emails with safe look-alikes in your user's inbox.
- Easily integrate with KnowBe4's email add-in button, Phish Alert, or forward reported emails to a dedicated mailbox

LEARN MORE

Additional Resources

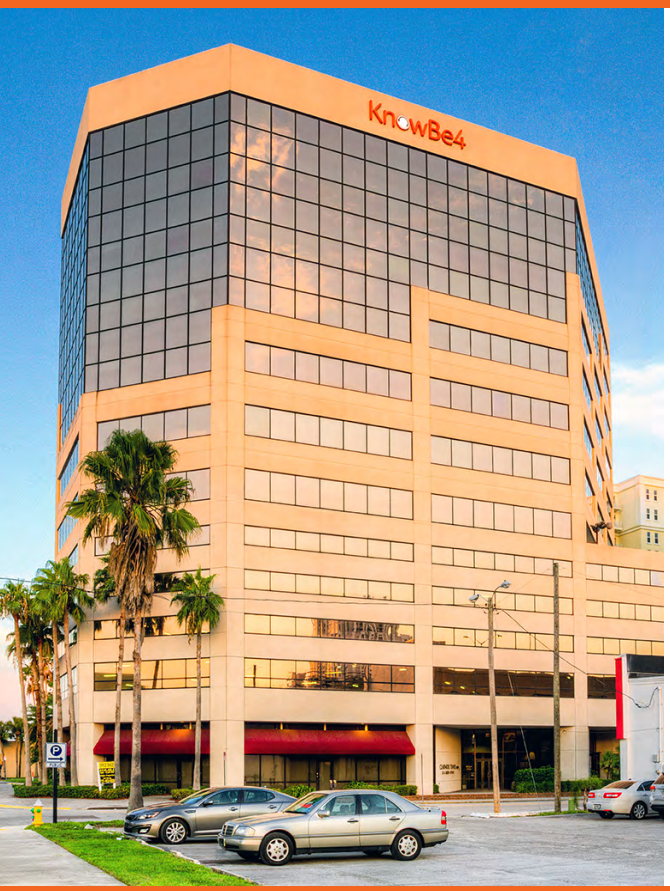
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

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

01D05K01