KnowBe4
Human error. Conquered.

The Future of Phishing Defense: AI Meets Crowdsourcing

As an infosec professional, you face the stealthiest troublemakers in cyber space on a daily basis, sneaking into the inbox of your users at the riskiest times. You and your comrades in arms are doing their best, but your team is stretched thin. What's more, those budgets aren't getting any bigger.

Legacy security layers such as secure email gateways (SEGs), aren't enough anymore in the face of sophisticated attacks. They're like rusty padlocks trying to keep out a red team of expert lock pickers. The truth is, they're just not cutting it against these slick, well-orchestrated attacks.

To keep cybercriminals at bay, organizations need a more proactive approach to phishing mitigation. This approach should leverage both the power of artificial intelligence (AI) as well as the collective strength of crowdsourced intelligence.

This whitepaper explores the limitations of legacy SEGs and presents a groundbreaking approach that combines the power of AI with the wisdom of crowdsourcing to mitigate phishing threats. Learn why you should drop the rusty, old-school approaches for something that combines the genius of AI with the strength of human insight.

WHY TRADITIONAL APPROACHES DON'T CUT IT

Historical trends and current metrics repeatedly attest to the ineffectiveness of relying solely upon legacy email defense platforms. The statistics are alarming:

- 78% of phishing attacks in 2022 used sophisticated techniques to bypass email security tools
- 56% of phishing attacks bypassed legacy security filters
- 18.8% of phishing emails bypassed Microsoft Exchange Online Protection and Defender to make it to a user's inbox

Meanwhile, threat actors are increasingly using image-based textual messages to evade text-based security filters. The traditional approaches of native email security tools (i.e. DMARC) and SEGs are important to network security but have their limitations in accurately detecting sophisticated phishing attacks.

This makes the human element imperative to the "big picture" of phishing mitigation. AI and crowdsourced threat intelligence is now imperative to enhancing phishing mitigation strategies.

Seeing The Malicious Emails That All Other Filters Miss

Crowdsourcing should not be reduced to a buzzword; it has real-world impacts on your organization, and it's more common already than you might think. The crowdsourcing intelligence we're referring to here is the highly trained, security-minded end user that flags a suspicious email. Which is followed by the seasoned security operations center (SOC) personnel reviewing that reported email to validate the threat. Now, multiply that by 10 million trained and vigilant users across tens of thousands of organizations from around the world. Crowdsourcing in that context is remarkably powerful.

In short: using the collective knowledge and insights of a diverse community on a global scale to uncover, report and collate problems and threats. The result is seeing what digital eyes can miss.

Cyber threat reporting, prioritization and analysis is vital for defense and proactive response. The more eyes and minds you have on the lookout, the better you are at detecting, reporting and blocking threats.

Crowdsourcing Meets Phishing Mitigation

Phishing mitigation needs to be proactive. This is the best way to meet cybercriminals head on; and you shouldn't have to do it alone. Your users want to help in this cybersecurity battle, and we have tools to enable them to proactively defend your environment.

> *Crowdsourcing helps make AI smarter by allowing users and security teams to identify, vet and gather data (in this case, suspicious vs malicious emails) in vast quantities.*

Crowdsourcing enables users to report these phishing campaigns faster than conventional methods. A 2021 study by ETH Zurich found that "crowd-sourcing" allows fast detection of new phishing campaigns, the operational load for the organization is acceptable, and the employees remain active over long periods of time."

Consider the typical phishing email reporting procedure:

1. A suspicious email makes it through your SEGs, endpoint, or network security provider (not if, but when)
2. In organizations with a strong security culture, highly trained security-minded users then report these suspicious emails
3. Once reported, the organization's security team analyzes and determines which emails are threats
4. From there, those phishing emails are added to their corporate blocklist

Now consider this process, but on a global scale.

Imagine tens of thousands of organizations just like yours sharing this sort of information. Imagine a blocklist where not just your users' reported phishing emails end up, but millions from all over the world.

Why not use the collective strength of highly trained end users to create blocklist data to proactively protect your organization and its end users from verified threats before they reach their inboxes? By harnessing the power of human intelligence in phishing mitigation, users can potentially contribute to an active, never-ending global threat feed.

AI + Crowdsourcing: The Way Forward

AI (and machine learning) are changing the world as we speak. In the world of cybersecurity, AI has become integral to infosec professionals to help process the massive amount of information networks generate every day. AI helps spot patterns in the massive digital noise and can instantaneously enable proactive threat detection.

Crowdsourcing helps make AI smarter by allowing users and security teams to identify, vet and gather data (in this case, suspicious vs malicious emails) in vast quantities. Also, collecting this large corpus of information from a diverse, global user base will ensure far more accurate and unbiased reporting.

In this way, multiple layers of human-curated (human-reported, human-analyzed, and human-vetted) phishing threat intelligence supported by AI-based analysis is equipped to protect your organization from new phishing attacks. This method will help ensure a proactive and faster response time to the latest wave of phishing attacks against your organization.

HOW TO GET THERE: CONSIDERATIONS FOR IMPLEMENTATION

The foundation for any evolved phishing mitigation strategy should include human and cyber elements working together to achieve a security goal. The response to any malicious email campaign should include workflow processes as a baseline for what to do before, during and after a phishing campaign targets your organization.

There are a number of considerations when implementing AI-powered blocklisting and crowdsourcing:

- Training users to spot, detect, and report phishing attacks in real time
- Analyzing and reporting malicious activity by the SOC team
- Additional vetting and analysis by a third party
- Uploading threat data to a global blocklist

Unfortunately, many organizations have little to no standard operating procedures for a rapid response to malicious email attempts. If so, it's typically focused on use cases and/or departments. And unfortunately these responses often don't include end user security awareness training or unbiased, third-party threat evaluation.

First and foremost, end users must receive new-school security awareness training to spot, assess and alert security teams regarding malicious social engineering attempts. Users must also have access to (and know how to use) reporting mechanisms to inform the IT department and/or SOC of the suspicious email.

> *Train and encourage users to report suspicious email by fostering a security culture mindset that makes employees feel a part of the security team.*

The benefits of these reporting tools are two-fold. One, they help make your users feel like part of the team and drive home the point that cybersecurity is everyone's responsibility. Two, ongoing monitoring and analysis is critical to fine-tuning AI systems and threat intelligence so phishing emails can be better detected and removed before they hit users' inboxes.

Responsible personnel must then have the means and training to appropriately vet and confirm or deny whether an email is malicious. How does your team respond to this threat? For small to medium businesses with limited staff, a full-blown security operations center may not be an option. A software component that involves evaluation of threats powered by machine learning will alleviate the workload on your already stressed IT department.

Last but not least, use an unbiased third-party threat analysis team to confirm or deny the nature of the suspect email. An outside third party team of experts also removes any bias that can influence the determination of whether there's been a malicious attempt on your corporate environment.

The Upshot

Bad actors are innovating all the time. Defending against the threats they pose means staying one step ahead of them with new ideas of our own. This is why it’s critical that you embrace crowdsourced threat intelligence and AI-powered mitigation as essential tools in the fight against phishing threats. AI-powered blocklisting combined with crowdsourcing provides a “tip-of-the-spear,” proactive approach to mitigate real-world phishing attacks and targeted spear phishing campaigns.

Train and encourage users to report suspicious email by fostering a security culture mindset that makes employees feel a part of the security team. That sense of ownership will assist your organization in locating and containing malware before it harms your network. Add to this a third layer of defense with an unbiased, third party of security experts to vet, confirm and then share these threats via a globally crowdsourced blocklist.

With this triple-edged cybersecurity sword, your organization will create a proactive phishing mitigation model that leverages the best of human and artificial intelligence efforts to defend your networks against threat actors.

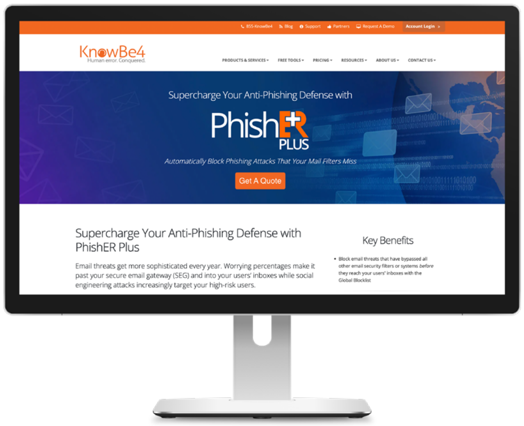
CROWDSOURCING MEETS AI WITH KNOWBE4’S PhishER PLUS

PhishER Plus is a lightweight Security Orchestration, Automation and Response (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.

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

LEARN MORE



Supercharge Your Anti-Phishing Defense with

Automatically Block Phishing Attacks That Your Mail Filters Miss

Supercharge Your Anti-Phishing Defense with PhishER Plus

Email threats get more sophisticated every year. Worrying percentages make it past your secure email gateway (SEG) and into your users’ inboxes while social engineering attacks increasingly target your high-risk users.

Key Benefits

- Block email threats that have bypassed all other email security filters or systems *before* they reach your users’ inboxes with the Global Blocklist

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 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