KnowBe4

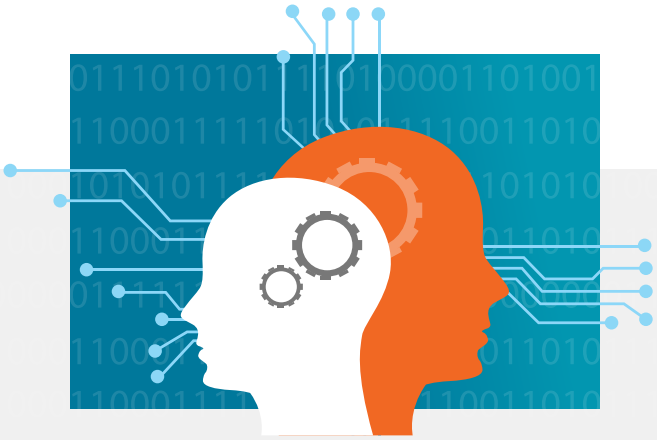
Fight AI with AI: 3 Ways AI-Powered Security Awareness Combats Cybercriminals

Cybercriminals are diving into AI to make the world more dangerous for the rest of us. From deepfakes to AI-generated phishing emails at scale, this emerging technology has become a powerful weapon in the arsenals of bad actors around the world.

Fortunately, infosec professionals like you can do something about it. You're likely already bringing the power of AI to bear across your tech stack. Why not leverage it to fortify your human firewall? Cybersecurity is not just about the security products you have in place, but the people using them.

When it comes to the vital human element of cybersecurity, the power of AI can be used to your advantage to engage users with relevant training and keep them informed against evolving cyber attacks.

Read on for an overview of what a robust security awareness training (SAT) and simulated phishing program with AI at its core can bring to a comprehensive cybersecurity initiative.



AI Meets Humans: Building Smarter Security Awareness Training

While threat actors increasingly wield AI for malicious purposes, cybersecurity tools are adapting to harness the power of artificial intelligence. Despite these advances, though, infosec challenges remain.

Rapid evolution of AI technology requires constant vigilance from users

Traditional security measures may be insufficient against AI-powered attacks, necessitating innovative defensive tactics

Time- and resource-strapped cybersecurity personnel exacerbates the challenge of staying abreast of emerging threats

Fortunately, emerging advances in security awareness and simulated phishing strategies offer hope.

Here are some key ways AI enhancement can bring existing SAT initiatives to the next level:

Automated Training and Reinforcement

AI-enhanced SAT has the potential to dramatically streamline a training administrator's job. Imagine an AI-driven adaptive learning system that automatically assigns training to individuals based on their entire learning history. This means the effectiveness of previous training modules, recent SAT exercise results, and personal learning preferences, such as content format (videos, quizzes, animations, games) and duration, are all taken into account to deliver a tailored experience for each user.

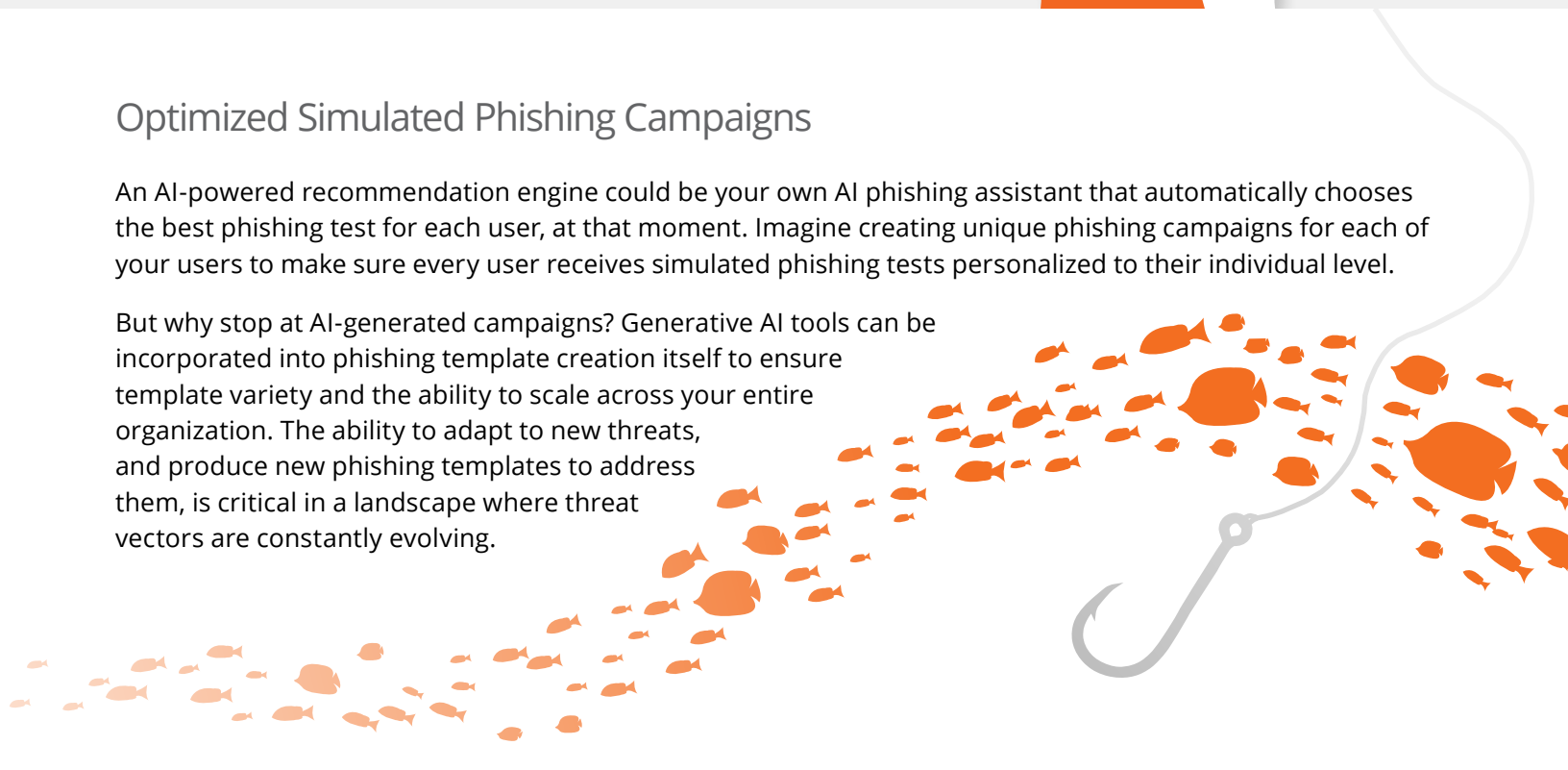
This approach would not only cut down on specific tasks for the admin. It would also increase training relevance for the user, upping the chances they will engage with the content and retain what they learn.

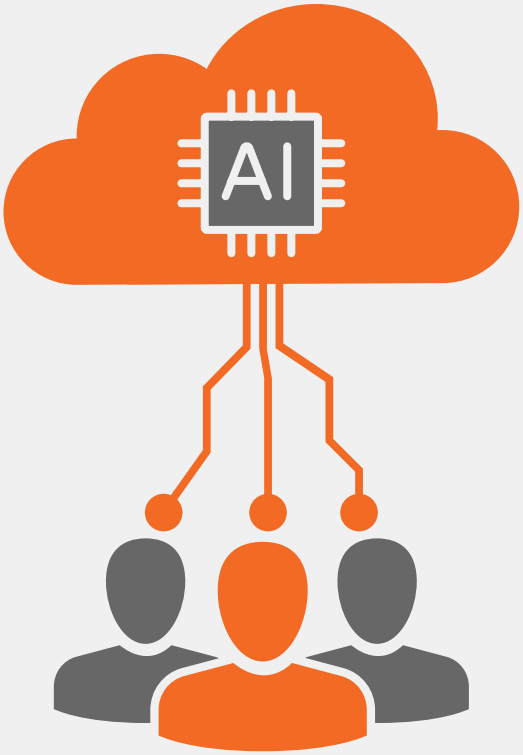
Once the primary training is delivered, AI can also be used to auto-generate training quizzes to help reinforce the content learned. Quizzes could be built from the training content itself or organizational policies, with generative AI doing much of the heavy lifting. The goal: Reiterate key takeaways and ensure that policy information is being taught to end users not just shown.

Optimized Simulated Phishing Campaigns

An AI-powered recommendation engine could be your own AI phishing assistant that automatically chooses the best phishing test for each user, at that moment. Imagine creating unique phishing campaigns for each of your users to make sure every user receives simulated phishing tests personalized to their individual level.

But why stop at AI-generated campaigns? Generative AI tools can be incorporated into phishing template creation itself to ensure template variety and the ability to scale across your entire organization. The ability to adapt to new threats, and produce new phishing templates to address them, is critical in a landscape where threat vectors are constantly evolving.





AI Teamed with Crowdsourced Intelligence

A key element of a robust SAT program is the ability for users to report both simulated phishing emails and real ones that make it to their inboxes. Your users want to help in this cybersecurity battle, and you should have the tools to enable them to proactively defend your environment.

This user-driven crowdsourcing enables users to report these phishing campaigns faster than conventional methods. Teamed with an AI-powered email security tool, 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.

In this way, 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.

The Upshot: AI Is Here

The impact of AI on society is no longer theoretical. It's happening right now. The choice is not *whether* to build it into your cybersecurity and SAT initiatives, but *when*.

Organizations must fight fire with fire. By harnessing the power of AI within security awareness training programs, businesses can manage their human risk and stay one step ahead of cybercriminals.

Ultimately, investing in AI-enhanced security awareness is an essential strategy for maintaining a strong security culture and safeguarding against the formidable cyber threats of today and tomorrow.

Explore KnowBe4's Approach to AI-Driven Security Awareness

Learn More

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