KnowBe4

AI vs. AI

Combating Cybercriminals with an AI-Powered Security Awareness Training Program

AI vs. AI: Combating Cybercriminals with an AI-Powered Security Awareness Training Program

✦ Table of Contents

INTRODUCTION

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 the ways bad actors are using AI for their own devices and what a robust security awareness training (SAT) and simulated phishing program with AI at its core can bring to a comprehensive cybersecurity initiative.

THE EVOLVING AI CYBER THREAT LANDSCAPE

Unless you've been using DALLE-3 to generate images of rocks to hide under, you've read news stories of the myriad ways cybercriminals are using generative AI and associated tools to cause problems.

AI is already being used to facilitate disinformation and misinformation campaigns, enhance social engineering attacks and automate multi-layered and multifaceted attacks at scale — even by attackers with little technical know-how.

Infosec leaders are definitely paying attention. A recent report from threat-detection firm Netacea found that 93% of security professionals they surveyed believe they will face daily AI attacks within the next six months. Just more than two-thirds (65%) believe offensive AI will become the norm.

✦ How AI Supercharges Phishing Attacks and Social Engineering

➔ Automated Content Generation

- AI, particularly natural language processing models, can generate convincing phishing emails that are grammatically correct and contextually relevant. This makes it difficult for traditional spam filters to detect them as malicious.
- Research indicates that AI-generated phishing emails have higher success rates compared to those crafted manually. For example, a study by the European Union Agency for Cybersecurity (ENISA) found that AI can generate highly personalized phishing messages at scale, targeting specific individuals by mimicking their writing style

➔ Spear Phishing Personalization

- AI algorithms can analyze vast amounts of data from social media and other online sources to gather personal information about targets. This allows cybercriminals to craft personalized and convincing spear phishing emails that are more likely to deceive recipients.
- Verizon's Data Breach Investigations Report highlights how AI-driven social engineering attacks can utilize detailed information about an individual's interests, connections and behavior to increase the success rate of these attacks.

➔ Phishing Site Automation

- AI can automate the creation of fake websites that mimic legitimate ones. These sites can adapt in real-time to evade detection and appear more authentic, thereby increasing the chances of users entering their credentials.
- According to a study published in the journal Computers & Security, AI-powered phishing sites can dynamically change their appearance and behavior based on user interactions and threat intelligence data to remain undetected longer.

➔ Deepfake Technology

- AI-generated deepfakes can create realistic audio and video imitations of individuals. Cybercriminals use these to impersonate executives or trusted individuals, convincing targets to divulge sensitive information or authorize transactions.
- The Cybersecurity and Infrastructure Security Agency (CISA) has issued warnings about the potential for deepfakes to be used in social engineering attacks, noting their increasing sophistication and the challenges they pose for detection.

AI may be the hot new thing, but it does not represent a completely new attack vector. Attackers will still use AI-generated phishing to elicit emotional responses (just lots more of them). Scared victims will make mistakes by wiring money or introducing malware into systems. Ultimately, defense will be the same — that is, watch for the usual signs of a social engineering ploy.

With these fundamental tactical similarities in how attacks are still happening, the power of AI is proving vital in defending against them.

AI FOR GOOD: THE ROBOTS ON OUR SIDE

While threat actors increasingly wield AI for malicious purposes, cybersecurity tools are adapting to harness the power of AI.

One key area is intelligent email security. Legacy email filters rely heavily on analyzing attachments and scanning for known malware signatures. AI-powered email security goes beyond this. It can parse the actual content of emails, analyzing subtle patterns and semantics to identify sophisticated social engineering attempts

AI and machine learning also play a major role in monitoring, analyzing and detecting cyber threats in real time across an organization. AI algorithms can continuously ingest and correlate vast amounts of data from network traffic, endpoints, cloud services and more. This means AI detection can spot the early signs of threats and provide alerts in real-time, expediting incident response.

But the technical side is just one aspect of the fight against cyber crime. AI should be, and can be, brought to bear to fortify your human attack surface.

AI MEETS HUMANS: BUILDING SMARTER SECURITY AWARENESS TRAINING

Despite AI advances, 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.

AI-enhanced SAT has the potential to dramatically streamline a training administrator's job.

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.

Generative AI tools can be incorporated into phishing template creation itself to ensure template variety and the ability to scale across your entire organization.

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.

LEARN MORE → **Explore KnowBe4's Approach to AI-Driven Security Awareness**

Additional Resources

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

Free Training Preview
See our full library of security awareness content; browse, search by title, category, language or content

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

About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

For more information, please visit www.KnowBe4.com

KnowBe4

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

01E06K01