

Why AI is Your New Best Friend... and Worst Enemy in the Battle Against Phishing Scams

Opinions expressed by Entrepreneur contributors are their own.

Artificial Intelligence is a double-edged sword. While it opens a plethora of use cases for making our work and daily lives more efficient, it also empowers cybercriminals to execute more effective attacks.

Phishing, already the most prevalent form of cyberattack with almost 3.4 billion emails sent per day, is now being fueled with AI, enhancing sophistication and maximizing the likelihood of these attacks succeeding.

A recent study reveals a 60% increase in AI-driven phishing, with higher success rates compared to messages created by human experts. This highlights that AI is not merely a tool but a catalyst in transforming the way these attacks are carried out, underscoring the need to stay ahead of their rapid evolution.

Related: [Fraud Alert! Watch Out for These 5 Sneaky Scams Targeting Small Businesses and How to Avoid Them](#)

Is it really your CEO? Think Twice

In the GenAI era, the lines between phishing and authentic messages are blurred, making them almost impossible to detect. C-level executives fall as one of the prime targets in

cyberattacks due to the amount of sensitive information and authority they wield within an organization. Attackers have elevated phishing to a whole new level with the help of AI tools, engaging in what is known as “whale phishing.”

This method involves leveraging deep fake AIs to impersonate top executives of a company, mimicking their appearance, voice and mannerisms to persuade employees to transfer funds or gain system access, leading to financial and reputational loss.

A stark example would be the attack on an advertising firm where hackers used the CEO’s image to create a fake WhatsApp profile to set up a Microsoft Teams meeting with him and another senior executive. During the call, the attackers used AI voice cloning and YouTube footage to trick the employees into disclosing personal details and transferring money under the guise of setting up a new business. Fortunately, the attempt was a failure due to the vigilance of the company executive.

The sophistication of such attacks reminds us that we no longer can afford to blindly believe someone is who they claim to be simply because they have their image and name on their profile. More than 95% of IT professionals find it challenging to identify phishing attacks crafted with large language models (LLM) like ChatGPT, Gemini and WormGPT. The strategy lies in playing with human psychology and personal information available on the internet to create the most convincing message. These messages often pose as trusted colleagues, incite fear about a potential security breach, or spark curiosity with a “too-good-to-be-true” offer related to a recent purchase, prompting users to click.

Gone are the days when phishing attacks could be spotted with their misspellings, incorrect information and clumsy execution. Today’s AI-powered phishing campaigns correct such errors, making it effortless for bad actors to generate a campaign with only five prompts and five seconds, which could

traditionally take a scammer almost 16 hours.

In this landscape, it is crucial to remain vigilant and question the authenticity of every message. The stakes are high, and the need for rigorous verification processes has never been more critical.

Related: Viral TikTok Warns Small Business Owners About Package Scam

How can we outsmart these attacks?

Paradoxically, the defense against these AI-powered attacks is utilizing AI itself. Businesses should consider investing in AI-driven security measures, with Extended Detection and Response (XDR) playing a crucial role in this strategy. XDR constantly monitors the mailbox, scanning for any indicators of compromise (IOC) such as URLs, domains, IP addresses, file hashes, and more.

Additionally, XDR's behavior analytics establishes a baseline of typical user behavior and email traffic patterns. When deviations from this baseline are detected, such as unusual login times, unexpected email attachments, or strange communication patterns, the system flags these anomalies, proactively mitigating phishing attempts within an organization.

Complementing XDR is the role of a Unified Endpoint Management (UEM) solution. Beyond being a repository from which XDRs can leverage endpoint data, UEMs are also essential in the realm of patch management, enforcing password policies and access management. By enabling timely patch deployment, UEM keeps all systems up to date, reducing vulnerabilities that phishing campaigns often exploit. Moreover, consistent password policies across all endpoints, including password complexity, multi-factor authentication, and access controls, protect the major perishable factor – passwords. So, an integration

between XDR and UEM creates a comprehensive defense against phishing threats. XDR detects and responds to attacks, while UEM helps lay the first line of defensive protocols in place. If a breach does occur, UEMs can also remotely wipe compromised devices to contain the damage.

Ultimately, the end goal should always be to transition towards a zero-trust architecture. While UEMs and XDRs are essential in this journey, they are not the entire picture. By adopting role-based access controls and rigorously validating every account before it gains any data handling privileges, administrators can fully embrace the tenet – trust none, always verify. This approach helps prevent unauthorized access in the event of a breach and greatly limits potential damage by restricting lateral movement.

Finally, it boils down to human vigilance

Even with the most advanced security measures, they are completely ineffective if employees are unaware of the latest phishing techniques and the critical details they must watch out for. Business leaders must invest in effective training programs that are not monotonous for the employees and often include the usual markers like bad grammar and failed personalization. It needs to go further by conducting AI-simulated phishing drills that create awareness on validating the sources of the emails, verifying the URL and domain names against the actual company and developing a sense of skepticism to evaluate and respond to highly convincing phishing scenarios critically.

In addition, the basic practices of enforcing strong, unique passwords for each account coupled with multi-factor authentication (MFA) are timeless measures that will always remain essential.

<https://www.entrepreneur.com/leadership/how-to-outsmart-ai-powered-phishing-scams/479422>