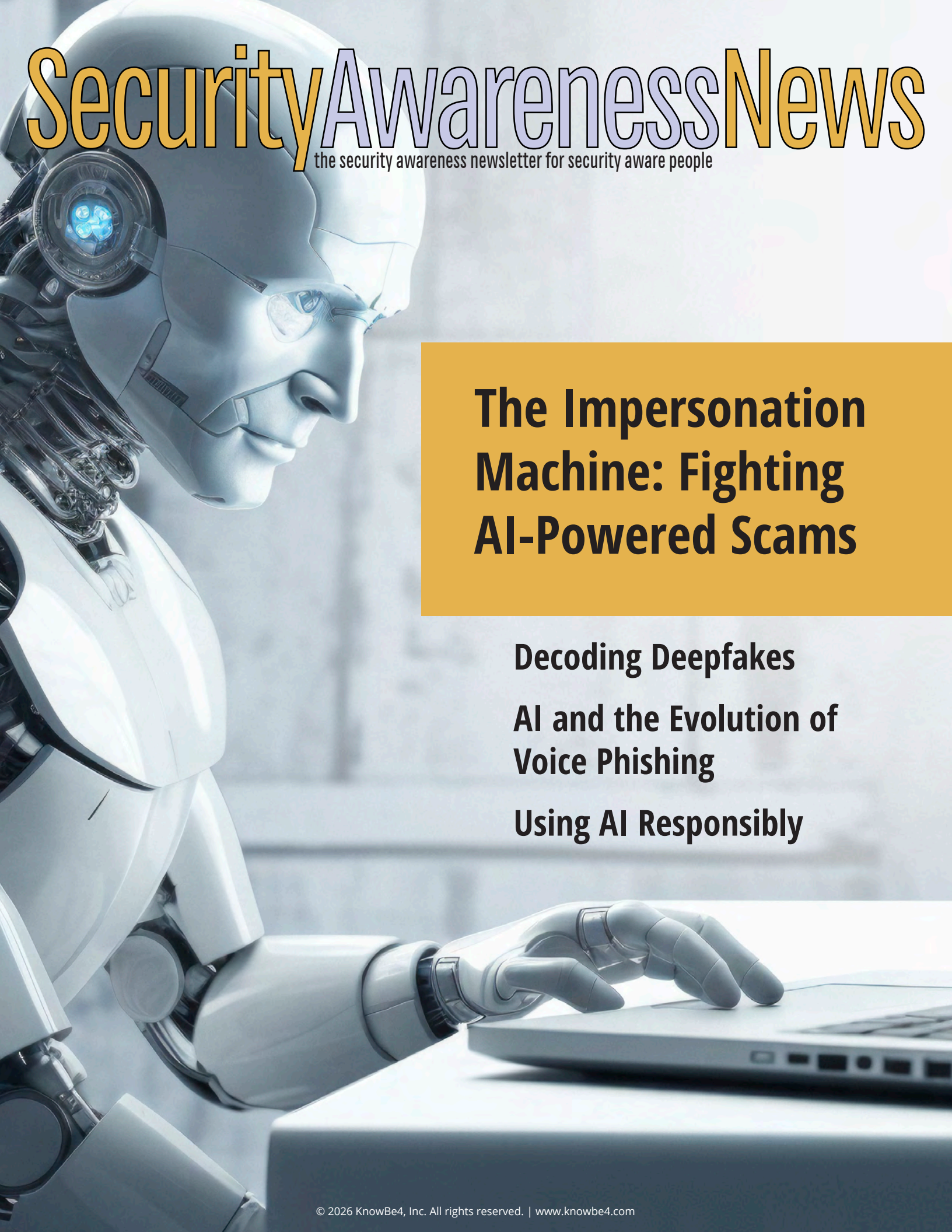
SecurityAwarenessNews

the security awareness newsletter for security aware people



The Impersonation Machine: Fighting AI-Powered Scams

Decoding Deepfakes

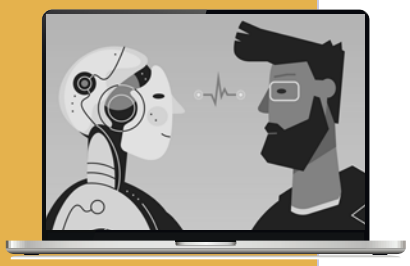
AI and the Evolution of Voice Phishing

Using AI Responsibly

Decoding Deepfakes

Unless you avoid the internet (and people) completely, it's impossible to not encounter artificial intelligence (AI) almost everywhere. As a quick reminder, AI refers to computer systems or models designed to simulate human intelligence.

While it's a powerful tool, it can be used for malicious purposes, such as creating deepfakes. Here's what everyone needs to know about the dangers of these AI-powered forms of media.



What exactly are deepfakes?

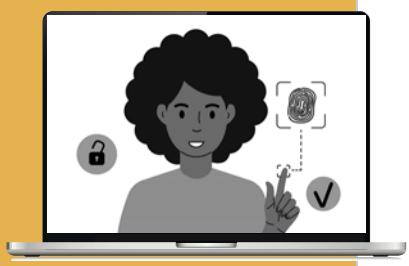
The term deepfake is a blend of "deep learning" and "fake." It refers to media, such as videos, images, or audio recordings, that have been digitally created or altered by AI tools. In many cases, the creation of deepfakes is done with malicious intentions, such as deceiving people to steal money, information, or generally cause civil unrest.

What makes them so dangerous?

Unfortunately, the rise of AI has eroded our ability to trust what we see, hear, or encounter. Deepfakes can now create alarmingly realistic content. This means attackers could, for example, create audio of a celebrity saying something they never actually said, but it would sound just like the real person. It's easy to imagine how much harm this could cause, especially when politics and other civil issues are involved.

How are deepfakes used in scams?

The celebrity example illustrates how deepfakes can cause personal harm to someone. Now imagine an attacker using similar techniques to target organizations. If a cybercriminal leverages AI to impersonate an executive, they could instruct employees to wire money to fraudulent accounts or reveal confidential information.



How can you avoid scams that use deepfakes?

Identifying deepfakes is not easy and will likely only become more challenging as AI continues to evolve. However, you can stay alert and use situational awareness to avoid scams related to these AI-powered attacks. Treat random requests for money or information with a healthy dose of skepticism. Always follow your organization's policies. When in doubt, make contact with all relevant parties in person wherever possible to confirm that a request is trustworthy.

AI and the Evolution of Voice Phishing

While deepfakes are a major concern, another dangerous AI attack is unfolding over the telephone: voice phishing. As you may know, phishing is a classic scam where a target is contacted by email, telephone, or text message and lured into providing sensitive data such as passwords or sending money.

AI voice cloning takes this to the next level by providing two distinct advantages for attackers:	**One: accuracy.** AI can clone an executive's, colleague's, or family member's voice with alarming accuracy, using minimal audio samples. Hearing a familiar voice helps reduce suspicion.
	Two: scalability. AI simplifies the process, allowing criminals to launch high volumes of personalized attacks quickly and cheaply.

Those two advantages are often featured in technical support scams, where the caller impersonates someone in IT and claims they need you to provide your password to run an important update. They may also impersonate your co-workers and even family members in an effort to steal money.

Here's what you can do to avoid falling for these scams:

Always Verify

If you receive an urgent call from someone claiming to be a bank, IT, or an executive, consider ending the call. You can then reconnect with them through known and trusted communication methods to verify their identity.

Never Share Confidential Information

Do not give out your password or other forms of confidential data over the phone call. This is especially true for any calls you receive at random.

Remain Skeptical

If you suspect a familiar voice on the phone may be cloned, ask a question only the real person would know the answer to.

Stay Alert for Warning Signs

Voice phishing and other attacks often feature common warning signs, such as urgent requests, threatening language, and unrealistic promises or offers. Stay alert for those signs, which can help you identify scams.

Using AI Responsibly

There's no question that AI dramatically enhances productivity and unlocks new possibilities for innovation, but it also introduces modern concerns regarding data privacy and security. Therefore, every member of an organization plays a crucial role in using AI tools responsibly. Let's explore a few key concepts of what this means for you.

Know the Expectations

Your responsibility begins with gaining a firm understanding of expectations and guidelines. For example: Do you know which AI tools have been approved for use within your organization? Do you fully understand what types of data you can and cannot input into these systems? Don't make assumptions. Instead, ask questions by reaching out to management or the relevant party at your organization.

Always Fact Check

It's important to verify the outputs of AI. While tools like ChatGPT and others are excellent resources for research, there's always a chance their outputs are factually incorrect or misleading. This is commonly known as AI hallucination, which happens when AI systems are trained on outdated or inaccurate data. It's your responsibility to independently verify what AI gives you by doing your own research.

Understand the Security and Privacy Concerns

Public AI systems are not secure vaults for confidential information. Any inputs — also known as prompts — entered into AI might be stored, analyzed, or used to improve these systems. This means that whatever information you use to prompt AI could eventually become part of their learning model. In general, never input the following information:

- Confidential and personal data, whether it's yours or someone else's
- Strategic business information such as marketing strategies, or details about unreleased products
- Intellectual property, like product designs and trade secrets

Always Follow Policy

Lastly, always adhere to your organization's policies regarding which AI tools you're allowed to use and how. These policies exist to protect data, assets, and people. By following them consistently, you help your organization avoid potential security and privacy concerns, while still harnessing the powerful benefits of artificial intelligence.