AI-powered attacks are growing: Is your company ready?

AI-powered attacks are a significant concern for individuals and businesses. They use advanced methods to exploit vulnerabilities and breach security measures, making traditional defenses less effective. To help protect your business from AI-powered attacks, you need a baseline understanding of the threats and the resources to stand up to them. Not sure where to start? We're breaking it all down.

Types of AI-powered attacks.

The Security Awareness Company breaks down the most common AI-powered attacks into four buckets:

1. **Impersonation.** Because AI can create realistic video or audio recordings, attackers can use it to generate content that appears to come from a trusted individual saying or doing something they aren't. This is known as a deepfake — a dangerous tool used to deceive the public.
2. **Voice Phishing.** This is when attackers attempt to scam people over the phone. With AI, it becomes even easier. A small sample of someone's voice can be used to generate speech that sounds like a real person, which can trick people into believing they are talking to someone they know.
3. **Automation.** Time is money. Through AI automation, social engineers can cast a wide net and increase the volume of their attacks. This process requires less effort on the attacker's part and means they can target a greater number of people, increasing the chances of successfully scamming someone.
4. **Reconnaissance.** AI is especially effective at mining social media and other online platforms to gather detailed information on potential targets. In the past, it could take weeks or months

for a social engineer to perform that task. AI can do it in seconds.

How you can stay safe from AI-powered attacks.

- **Keep your guard up.** Like all online security measures, trust your gut. If something feels suspicious or fishy, it probably is. Verify sources and research senders before clicking attachments or opening links.
- **Utilize zero trust.** The Security Awareness Company recommends a zero-trust model. “Assume everything is untrustworthy until proven otherwise. At a basic level, never assume someone is who they claim, regardless of how they engage with you.”
- **Get to know the platforms.** Familiarize yourself with AI chatbots and image generators. Playing around with the platforms and learning their capabilities can help you better distinguish between human content and AI content.
- **Create company policies.** Establish rules surrounding the use of AI in the office and for company purposes. For example, maybe team members can use AI for thought starters or helpful assistants, but not to replace existing functions. Ensure team members don’t enter proprietary information into AI systems, as it can be used in the future AI learning process and knowledge base.
- **Consider cyber insurance.** Cyberattacks are the fastest-growing crime in the United States, which is why businesses today benefit from cyber insurance. Coverage can help you worry less about digital asset protection, loss of income, privacy breaches, and more.

When it comes to AI, knowing the basics and the types of scams out there can help you prevent AI-powered attacks. For added peace of mind, our experts are here. Talk to a local, independent agent about online and cyber safety today.