SecurityAwarenessNews
the security awareness newsletter for security aware people

The Rise of Artificial Intelligence

Chatting with ChatGPT

AI-Powered Attacks

Human Intelligence and Security

Chatting with ChatGPT

Artificial Intelligence (AI) refers to smart machines capable of performing tasks that typically require human intelligence. Generative AI is one of the most commonly used forms today. It generates content such as text, audio, and video. You might already be familiar with one such type of Generative AI: ChatGPT.

ChatGPT is a chatbot where the "GPT" stands for "Generative Pre-training Transformer." What this means is that it was, and continues to be, trained on massive data sets. It uses that knowledge to generate text based on the prompts it has been given.

For example, imagine you want to learn about William Shakespeare. Prompt: "Who is William Shakespeare?" ChatGPT will explain, in great detail, that Shakespeare was an English playwright who is widely regarded as one of the greatest writers in the English language.

That might not sound any different than asking an internet search engine the same question. So, let's explore this idea further to showcase ChatGPT's capabilities. Prompt: "Explain what AI is and how it works." ChatGPT will, again, generate a detailed response. Now, change the prompt to "Explain AI in the style of William Shakespeare," and you might get something like this:

> ***"In realms of wire and lines, where metal mind do dwell,***
>
> ***Lies artificial intelligence, a tale I now shall tell."***

This example demonstrates that Generative AI, like ChatGPT, is a powerful tool that can be tailored to your specific needs. You could use it to generate complex spreadsheet functions, edit emails to sound professional, or even write code for software development.

It can also be used for malicious purposes. Attackers already use AI chatbots to write personalized emails designed to steal information or convince people to click on malicious links. This is why it's crucial for everyone to understand the power of AI and what it means to the future of productivity and security.

So stay alert and informed, and remember that human intelligence remains the best defense against modern attack methods.

AI-Powered Attacks

The rise of AI offers several benefits to society at large. It also ushers in concerns regarding security. Social engineers are already using Generative AI to create sophisticated phishing campaigns. As a quick refresher, social engineering is the art of misleading people via psychological manipulation.

It's not hard to imagine how social engineers could use AI to power their attacks. Here are a few examples:

Impersonation

Given that 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 actually aren't. This is known as a deepfake — a dangerous tool used to deceive the public.

Voice Phishing

Another form of impersonation is voice phishing, where attackers attempt to scam people over the phone. With AI, this 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 with someone they know.

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.

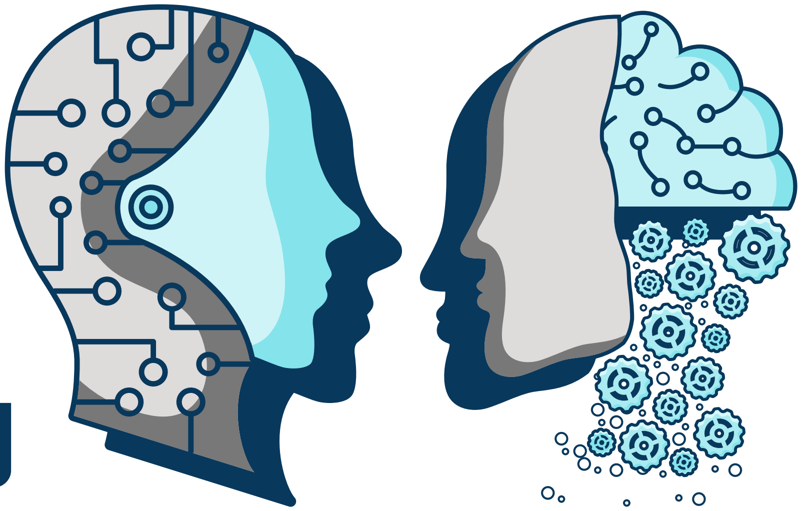
Reconnaissance

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.

Those examples of AI-powered attacks barely cover the scope of how social engineers use modern technology to leverage classic scams. Avoiding those scams requires everyone to maintain a heightened sense of awareness, especially when prompted to provide money or confidential information.

When you encounter anything suspicious, trust your instincts and remain skeptical. When at work, report it immediately.

Human Intelligence and Security



AI will continue to evolve and be a common fixture in everyday life. To get a better understanding of what the future holds, here's an overview of three basic types of AI worth knowing about:

Narrow AI	Also known as Weak AI, it can focus on one narrow task at a time. It has no emotions or conscience and is the only type of AI that currently exists. ChatGPT is an example of Narrow AI.
General AI	Also known as Strong AI, it can do almost anything humans can do. It doesn't yet exist, but there have been massive investments by tech companies to create it.
Super AI	Mostly found in science fiction, Super AI refers to technology that surpasses human intelligence and can perform tasks better than us. It'll have emotions, needs, beliefs, and desires, just like humans do.

With the three types of AI established, let's shift our focus back to security. There is reasonable concern that it will be more difficult than ever to identify AI-powered attacks. Enter the last line of defense: human intelligence. Here's what you can do to stay safe both at work and home:

Remain Skeptical and Thorough

The power of AI means that everyone needs to take extra precautions as a part of their daily routines. For example, when handling emails, thoroughly inspect the entire message and never open random links or attachments.

Follow the Signs

Even if AI helps attackers hide their intentions, there will still be warning signs. Stay alert for common indicators of scams, such as threatening language, urgent messages, and suspicious requests.

Utilize Zero Trust

The zero trust model assumes everything is untrustworthy until proven otherwise — a great approach to all things security. At a basic level, never assume someone is who they claim, regardless of how they engage with you.

Follow Policies

Always following policy is a simple, effective way to maintain security. If you're allowed to use AI tools for work, be sure you understand your organization's guidelines for doing so.