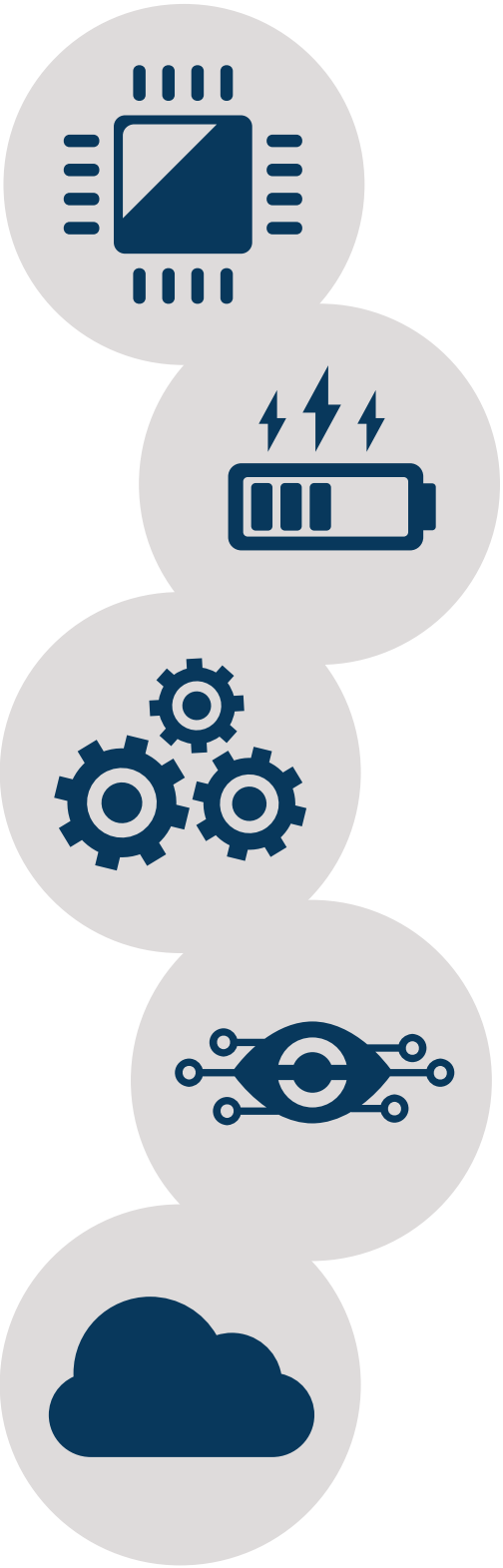
AI-Powered Attacks



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.