Artificial Intelligence, Security, and You

As artificial intelligence (AI) becomes a larger part of everyone's lives, it's important to understand the threat it poses to security. Let's review what AI is, how it can be used for malicious purposes, and what it means for security.

AI Defined

The concept of AI refers to computers and machines that perform tasks normally requiring human intelligence. AI systems work by being trained on large amounts of data that is then analyzed and used to make decisions. There are many forms and functions of AI. Generative AI, for example, can generate content such as text, images, audio, and video.

AI-Powered Attacks

As AI evolves, so too will AI-powered attacks. A few examples of how criminals use AI include:

- ***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.
- ***Voice Phishing***
  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***
  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.

AI, Security, and You

Cybercriminals and scammers are already using AI to their advantage. Here's what you can do to identify and avoid AI-powered attacks 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.