TeamLogicIT®
Your Technology Advisor

TIP SHEET

AI Security

6 Tips for Helping Organizations Stay Secure

Like many emerging technologies, artificial intelligence (AI) has already established itself as an innovation that is here to stay. Organizations of all types are exploring their potential and risks, even while adoption is rapidly accelerating. Some large enterprises are already building or buying apps for data analytics, decision support, accounting, insurance claims processing, legal research and numerous other business use cases.

But the emergence of AI has raised a variety of security and privacy concerns, as it opens the door for bad actors to exploit its capabilities. As AI systems become more advanced and integrated into daily operations, ensuring the safety and security of individuals and organizations must be a top priority for IT teams and business leaders.

At TeamLogic IT we believe in taking a security-first approach to technology. Therefore, we offer the following tips to help you minimize AI risks in your organization.

1. Hackers and scammers are busy trying to exploit AI through targeted spear-phishing attacks, malware and ransomware, and even fake websites and apps that impersonate popular generative AI platforms (i.e., "deep fakes"). **Train your staff to identify these outside threats.**

2. **Develop formalized policies and guidelines** for using AI platforms in your company. Have staff attest and acknowledge acceptable use policies on at least an annual basis. Train them to identify sensitive information and know how to protect it—e.g., personal identifiable information (PII) and intellectual property (IP).

3. **Maximize the use of technologies that blunt the negative impact of AI**, such as applications for data loss prevention, endpoint/antivirus protection, safe web browser filtering, identify access management and data encryption.

4. **AI tools cannot always distinguish between fact and fiction** and can often provide inaccurate information. Train your staff to closely review all AI responses and feedback to ensure the outcome aligns with and relates to your specific request or situation.

5. As there is no guarantee that information shared with a large language model remains private, **demand that your employees only use protected, enterprise versions of products** such as Microsoft Copilot, ChatGPT, etc.

6. **Consider these questions when evaluating the reliability and validity of AI-generated text and media:** Does it matter if the output is true? Do you have the expertise to verify that the output is accurate? Are you willing to take full responsibility for inaccuracies? Your answers to these questions can guide your use or nonuse of generative AI.

Move forward with **The Color of Confidence®.**

TeamLogicIT.com