TAKE 5
SAFELY UTILIZING AI TOOLS
with Keenan & Associates and Firestorm Global

Safely Utilizing AI Tools

Long before the internet, we dreamed of technology so advanced it could think, create, and solve problems with us. Now, that reality is here in the form of Artificial Intelligence (AI). Whether analyzing data, crafting presentations, or exploring new ideas, AI has the potential to be one of the most impactful innovations of the last century, with the only limits being the extent of our imagination. However, just like learning to “Google,” harnessing AI safely requires strong security fundamentals. In this edition of Take 5, we’ll cover some key points to keep in mind as you explore AI in your organization.

Select AI Models Carefully

With the explosion of AI tools available, choosing the right model can be challenging. For instance, if you search for ChatGPT on the iOS App Store, you’ll see an endless list of copycat apps, with many offering free or improved access to ChatGPT. It’s highly recommended to only utilize official AI apps from trusted sources. For practical purposes, consider ChatGPT, Claude, Perplexity, Google Gemini, and Microsoft Copilot as examples of commonly accepted and respected models.

Foreign-Interest AI Models

Emerging platforms like DeepSeek have recently generated much discussion and controversy over connections to China. Security researchers have identified concerns related to potential data sharing with the Chinese government and military. As a best practice, consider avoiding controversial or poorly vetted models.

Treat Prompts Like Public Posts

Contrary to traditional search engines, AI models are uniquely equipped to interact with data, which can include photos, spreadsheets, and other file types. Caution should always be exercised when inputting sensitive information, particularly for protected data. Given the widespread history of data leaks and data breaches, users should generally assume that inputs into third-party AI models have the potential to be publicly exposed one day.

Third-Party AI Risk

Many technology vendors are in a competitive race to effectively incorporate AI into their product platforms as a basis for determining their enterprise market value. Due to the rapid pace of change, security can be a deferred function in product development cycles. It’s important to maintain strong data privacy agreements that govern AI use and auto-enabled features across all vendors.

Pro Tip: Assess AI Adoption

Partner with your Information Technology team to perform a network traffic analysis to determine AI trends across staff and network users. Contact Firestorm Global (support@firestormglobal.com) if you need further information.

Jessica Blushi | jblushi@keenan.com Tim Femister | tim@firestormglobal.com