Think Intelligent About Artificial Intelligence

Artificial intelligence, including so-called “large language models” like ChatGPT, has rapidly become a major talking point in the press, amongst governments, and maybe even at your college! While AI has been a subject in the background for decades, everyday web users can now engage with AI like never before.

But whenever there is a sea change in technology, it is always smart to think about the security issues. This is how you can stay safe online over the years.

Should I use ChatGPT or other AI platforms?

With any shiny new technology, you should consider security and privacy risks before diving in. When it comes to AI-powered language models and other services, there are a few major factors to consider when loading up AI for help at work, school, or for fun:

Don’t Hand Over Your Crown Jewels!

AI models partly “learn” from what users input into the system. Therefore, you shouldn’t put any information into an AI model you want to keep private, from your company’s proprietary computer code to sensitive information about your family.

Prompting isn’t the Same as Creating

When it comes to your child’s homework or perhaps your own work endeavors, know that putting a query to AI and then copy/pasting the results isn’t the same as doing the work yourself. Also, if you are asking a fact-based question to an AI model (like “what atoms are in a water molecule?”) you need to fact check everything, because these models have become infamous for giving very confident but very wrong information in many situations. Other times, people have noted that AI models produced bizarre – and sometimes creepy – responses suggesting that the model had a mind of its own, which have been deemed “hallucinations.” We say it’s best to look at AI models as tools: they can help you get the work done, but we think you’re more talented than a machine!

Privacy Concerns

There are many concerns over how AI models scrape the web, from how these programs utilize the creations of artists and writers to what sort of personal information they know about us. Many experts are worried that it is collecting data on children, for example, and how these services can alert people about sharing their data remains an open question. In many cases, your chats with an AI are not private – the company can see what you input, even if it is anonymized. Carefully read the privacy notices of any AI service you use and ensure that you are okay with sharing the data it collects.

Bad Guys Also Use AI

Another trend is the rise of cybercriminals using AI to get better at their crimes. There is evidence that bad actors are using AI to craft more deceptive phishing emails and help develop malware. When there is any big disruption in tech, take it as a good time to review your cybersecurity basics: use strong passwords, take advantage of password managers, and enable MFA for all accounts that allow it.

- *National Cybersecurity Alliance*