OUCH! May 2023

SANS SECURITY AWARENESS

Artificial Intelligence: What to Know

What is It and Why Should I Care?

Artificial Intelligence (AI) describes systems programmed to think and respond like humans. In fact, we asked the AI solution ChatGPT that very question and got this response.

What is Artificial Intelligence?

Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. It involves the development of algorithms and computer programs that can perform tasks that typically require human intelligence, such as recognizing speech, understanding natural language, making decisions, and playing games. There are several types of AI, including rule-based AI, expert systems, and machine learning.

What makes AI so powerful is it can simulate the intelligence and reasoning capability of the human mind, but it can analyze exponentially far more information than any human and do it exponentially faster.

The concept of AI is not new. Originally covered in science fiction novels, AI is something that has been in development for decades. The reason you are hearing so much about it now is that for the first time, anyone has the opportunity to interact with and see the true functionality of AI.

ChatGPT, an online-powered AI chat bot, is one of the first publicly available solutions that is able to respond like a real human, passing something called the Turing Test. This test determines a machine's ability to exhibit intelligent behavior by having a real human interact with the machine through a text-based chat channel. If the human could not tell whether they were interacting with a machine or person, the machine is said to have passed the test. AI solutions today are the first publicly available that do just that.

However, online conversations are just the beginning of what AI can do. There are now AI solutions that can create a video of a person teaching a class in any language, analyze health records and quickly determine who most likely has cancer, create news articles or essays on the topic of your choice, generate images for children's books, or create code for new computer programs. While AI is not necessarily something to be feared, there are some dangers of which to be aware.

Dangers of Artificial Intelligence

1. **Recreating You**: AI solutions can take a recording of a person's voice – your voice – and then use it to create real-time audio that sounds just like you, saying whatever it wants to impersonate you. So, a cyber attacker could record a phone voice message that sounds like you, tricking your coworkers, your bank, or a family member into thinking you called and asked them to take an action. AI can also do this with pictures or video. Sometimes called Deep Fakes, an AI solution can take an existing picture or video of you and use it to recreate entirely new pictures or videos (including your voice) appearing to show you doing things that you never did.

2. **Wrong Answers**: As for the data or answers AI provides, the solutions can be wrong. AI often uses public information from the Internet, and its answers can be influenced by the biases of its developers. While typical search engines are designed to provide you the "best" or most correct answer to your queries, solutions like AI may be designed to give you the most human-like answer. Which is better depends on what you are attempting to achieve.

3. **Not All Equal**: With AI becoming the latest hot technology, there are literally hundreds of startup companies now offering different AI services. Many of these want your information or credit card for a trial. Be careful - not all AI services are trustworthy. Do your research before signing up and using an AI service.

4. **Your Privacy:** Whenever using or interacting with an AI system, such as when chatting online with ChatGPT, be aware that any information you enter into the system can not only be processed by it but also retained and used to give answers to others. This means if you enter any personal information about yourself or any confidential information from work, that information will be stored and potentially shared with or sold to others. Do not share or enter any information that you consider sensitive, personal, or is confidential at work.

The Future of AI

Artificial Intelligence is still very much in its infancy, similar to where the Internet was twenty to thirty years ago. While we can expect rapid evolution and adoption of AI, it's very difficult to predict what its impact will be. Just be aware that these capabilities are out there, and when using AI, be very careful what information you enter and share.

Resources

ChatGPT: https://chat.openai.com/chat
Turing Test: https://en.wikipedia.org/wiki/Turing_test