SECURITY CONCERNS REGARDING ARTIFICIAL INTELLIGENCE

What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) simulates human learning, comprehension, problem solving, decision making, creativity, and autonomy by utilizing or enables computers, machines, and technology. AI has the ability to learn human behavior specifically to users and provide best recommendations and details of specific topics or applications.

Types of Artificial Intelligence (AI):

- **ANI - Artificial Narrow Intelligence**
Everyday use of technologies fall under Artificial Narrow Intelligence (ANI). These technologies are great for one or a few closely related tasks. However, ANI has a limited range of abilities, specifically designed for a narrow use as it is only capable to reach a level of performance of a human, or better. Nonetheless, ANI does have limitations because it is not self-learning. As of today, ANI is the only form of Artificial Intelligence that we have been able to develop. (Examples: Siri, Face ID, Google Assistant)

- **AGI - Artificial General Intelligence**
Evaluation progress with technology as well. Artificial General Intelligence (AGI), the next generation that developers are trying to create.
AGI are technology that will be more advance similar to human intelligence and self-learning. Think about a device that would have a human mind and what developers are theorizing that AGI should be able to think and function like a human mind. The capabilities would be able to intellectually content, and problem solving by make decisions on its own. AGI is extremely complex, and developers are having difficulty to achieve it today, however, developers will create AGI and be attained in the near future.

- **ASI - Artificial Super Intelligence**
Once developers have successfully achieved AGI, computers will have the ability to learn independently and at a very fast rate, and more cognizant independently without human intervention or assistance. Developers theorize that they have achieved Artificial Super Intelligence (ASI). This is the final step where computers, devices and technology will be capable of "thinking" outperforming people in every job field, and more. Developers are saying that ASI would be able to "improve" itself.

In the 1993 movie Jurassic Park, Jeff Goldblum's character Ian Malcolm says, *"Your scientists were so preoccupied with whether or not they could, they didn't stop to think if they should."*

Now that you have been exposed to the different types of Artificial Intelligence (AI), you should know the security concerns and how AI will affect you. Fortunately, we are nowhere near AGI and ASI, however, that does not mean that you should take AI out of context. There are still AI forms that are being used today such as ChatGPT and other open AI sources. While these sources offer benefits like quick responses, sample writings and writing code, these applications also have heightened interest in consumers on a

broader scale audience. Therefore, people should take into consideration the cyber security threats, risks and vulnerabilities and take the necessary precondition for the safety, resilience, privacy, fairness, efficacy and reliability of all AI systems. It's also important to remember that the content produced by AI is only as good as the data they are trained on.

Evolution is inevitable. Whether it is humans or technology, everything evolves to a greater good or worse, to exploit and control information. Remember that information is power. Those that control information can control the minds of the vast majority of populations. There are some great benefits to a business by incorporating AI like an improvement in productivity, and cost efficiency. However, AI is a tool that should remain unbiased with the information that it provides. It is then up to you to understand the information you are looking at and be able to distinguish what is true and what manipulated.

Take time to read the articles below at your leisure:

- National Cyber Security Centre . (2024, February 13). AI and cyber security: what you need to know Understanding the risks - and benefits - of using AI tools. **https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know**
- Fox-Sowell , S. (2024, January 11). NIST researchers warn of top AI security threats. **https://statescoop.com/nist-security-threats-ai-state-local/**

References:

- Stryker, C., & Kavlakoglu, E. (2024, August 16). What is artificial intelligence (AI)? **https://www.ibm.com/topics/artificial-intelligence**
- youevolve.net. (n.d.). Ani, agi and asi - what do they mean?. ANI, AGI and ASI - what do they mean? **https://youevolve.net/ani-agi-and-asi-what-do-they-mean/**
- National Cyber Security Centre . (2024, February 13). AI and cyber security: what you need to know Understanding the risks - and benefits - of using AI tools. **https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know**