

OUCH!

O boletim mensal de conscientização de segurança para você

Inteligência Artificial: o que saber

O que é e por que devo me importar?

A Inteligência Artificial (IA) descreve sistemas programados para pensar e responder como humanos. Na verdade, fizemos essa mesma pergunta à solução de IA do ChatGPT e obtivemos essa resposta.

O que é Inteligência Artificial?

A inteligência artificial (IA) refere-se à simulação da inteligência humana em máquinas programadas para pensar e aprender como humanos. Envolve o desenvolvimento de algoritmos e programas de computador que podem executar tarefas que normalmente requerem inteligência humana, como reconhecer a fala, entender a linguagem natural, tomar decisões e jogar. Há vários tipos de IA, incluindo IA baseada em regras, sistemas especializados e aprendizagem de máquinas.

O que torna a IA tão poderosa é que ela pode simular a inteligência e a capacidade de raciocínio da mente humana, mas pode analisar exponencialmente muito mais informações do que qualquer ser humano e fazê-lo exponencialmente mais rápido.

O conceito de IA não é novo. Originalmente abordada em romances de ficção científica, a IA é algo que está em desenvolvimento há décadas. A razão pela qual você está escutando tanto sobre isso agora é que, pela primeira vez, qualquer pessoa tem a oportunidade de interagir com e ver a verdadeira funcionalidade da IA.

ChatGPT, um robô de bate-papo/chat de IA com tecnologia online, é uma das primeiras soluções disponíveis publicamente que é capaz de responder como um verdadeiro humano, passando por algo chamado Teste de Turing. Esse teste estabelece a capacidade de uma máquina demonstrar comportamento inteligente ao ter um humano real interagindo com a máquina por meio de um canal de chat baseado em texto. Se o humano não pudesse dizer se estava interagindo com uma máquina ou pessoa, diz-se que a máquina passou no teste. As soluções de IA hoje são as primeiras disponíveis publicamente que fazem exatamente isso.

No entanto, as conversas online são só o começo do que a IA pode fazer. Agora existem soluções de IA que podem criar um vídeo de uma pessoa dando uma aula em qualquer idioma, analisar registros de saúde e determinar rapidamente quem tem mais probabilidade de ter câncer, criar artigos de notícias ou ensaios sobre o tema de sua escolha, gerar imagens para livros infantis, ou criar código para novos programas de computador. Embora a IA não seja necessariamente algo a ser temido, há alguns perigos dos quais devemos estar atentos.

Perigos da Inteligência Artificial

1. **Recriando você:** 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. Portanto, um atacante cibernético pode gravar uma mensagem de voz telefônica que soe como você, enganando seus colegas de trabalho, seu banco ou um membro da família, fazendo-os pensar que você ligou e pediu que eles tomassem uma ação. A IA também pode fazer isso com fotos ou vídeos. Às vezes chamada de Deep Fakes, uma solução de IA pode tirar uma foto ou vídeo existente sua e usá-la para recriar fotos ou vídeos totalmente novos (incluindo sua voz) que parecem mostrar você fazendo coisas que nunca fez.
2. **Respostas erradas:** Quanto aos dados ou respostas que a IA fornece, as soluções podem estar erradas. A IA normalmente usa informações públicas da Internet e suas respostas podem ser influenciadas pelos preconceitos de seus desenvolvedores. Embora os mecanismos de pesquisa típicos sejam projetados para fornecer a “melhor” ou mais correta resposta às suas perguntas, soluções como IA podem ser projetadas para fornecer a resposta mais humana. O que é melhor depende do que você está tentando alcançar.
3. **Nem todas iguais:** Com a IA se tornando a mais recente tecnologia quente, existem literalmente centenas de empresas iniciantes que agora oferecem diferentes serviços de IA. Muitos deles querem suas informações ou cartão de crédito para um teste. Tenha cuidado- nem todos os serviços de IA são confiáveis. Faça sua pesquisa antes de se inscrever e usar um serviço de IA.
4. **Sua privacidade:** Sempre que usar ou interagir com um sistema de IA, como ao conversar online com o ChatGPT, esteja ciente de que qualquer informação que você inserir no sistema pode não apenas ser processada por ele, mas também retida e usada para dar respostas a outras pessoas. Isso significa que se você inserir qualquer informação pessoal sua ou qualquer informação confidencial do trabalho, essa informação será armazenada e potencialmente compartilhada ou vendida a outros. Não compartilhe ou insira qualquer informação que considere sensível, pessoal ou confidencial no trabalho.

O futuro da IA

A Inteligência Artificial ainda está engatinhando, semelhante a onde a Internet estava há vinte ou trinta anos. Embora possamos esperar uma rápida evolução e adoção da IA, é muito difícil prever qual será seu impacto. Esteja ciente de que esses recursos estão disponíveis e, ao usar a IA, tenha muito cuidado com as informações que você insere e compartilha.

Recursos

ChatGPT: <https://chat.openai.com/chat>

Teste de Turing: https://pt.wikipedia.org/wiki/Teste_de_Turing

Traduzido para a Comunidade por: David Boldrin

OUCH! É publicado pela SANS Security Awareness e distribuído sob a licença [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Você é livre para compartilhar ou distribuir este boletim, desde que não o venda ou modifique. Conselho Editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.