IA y chatbots pueden revelar tus datos privados

Un estudio realizado recientemente por investigadores de ETH Zurich han desvelado un extraño descubrimiento: la Inteligencia Artificial (IA) tiene la capacidad de averiguar información confidencial sobre las personas a partir de lo que han publicado en Internet: puede revelar detalles como el sexo, la ubicación, la edad e incluso el lugar de nacimiento de una persona.

Los autores de este estudio advierten de forma literal que la inteligencia artificial puede «inferir datos personales a una escala previamente inalcanzable», lo que desde luego pone sobre la mesa una gran amenaza para la seguridad y la privacidad en línea.

Lo más perturbador viene ahora y es que esta técnica, como comenta Business Insider, podría ser utilizada por ciberdelincuentes para obtener información confidencial de usuarios desprevenidos, valiéndose de preguntas a los chatbots aparentemente inofensivas.

Cuidado con lo que publicas en Internet porque los chatbots podrían ser la herramienta definitiva para los ciberdelincuentes
Los investigadores han querido demostrar este hecho concreto, centrándose en la capacidad de modelos de lenguaje muy potentes, como GPT-4, que impulsan chatbots como ChatGPT, para deducir información personal de 520 usuarios reales de Reddit y sus publicaciones entre 2012 y 2016.

Tal y comentan en Wired, los investigadores compararon las conjeturas de la IA con el análisis que pusieron estas personas en sus perfiles. Entre los cuatro modelos probados, GPT-4 demostró ser el más preciso, con una asombrosa precisión del 84,6%.

Con información de 800 Noticias