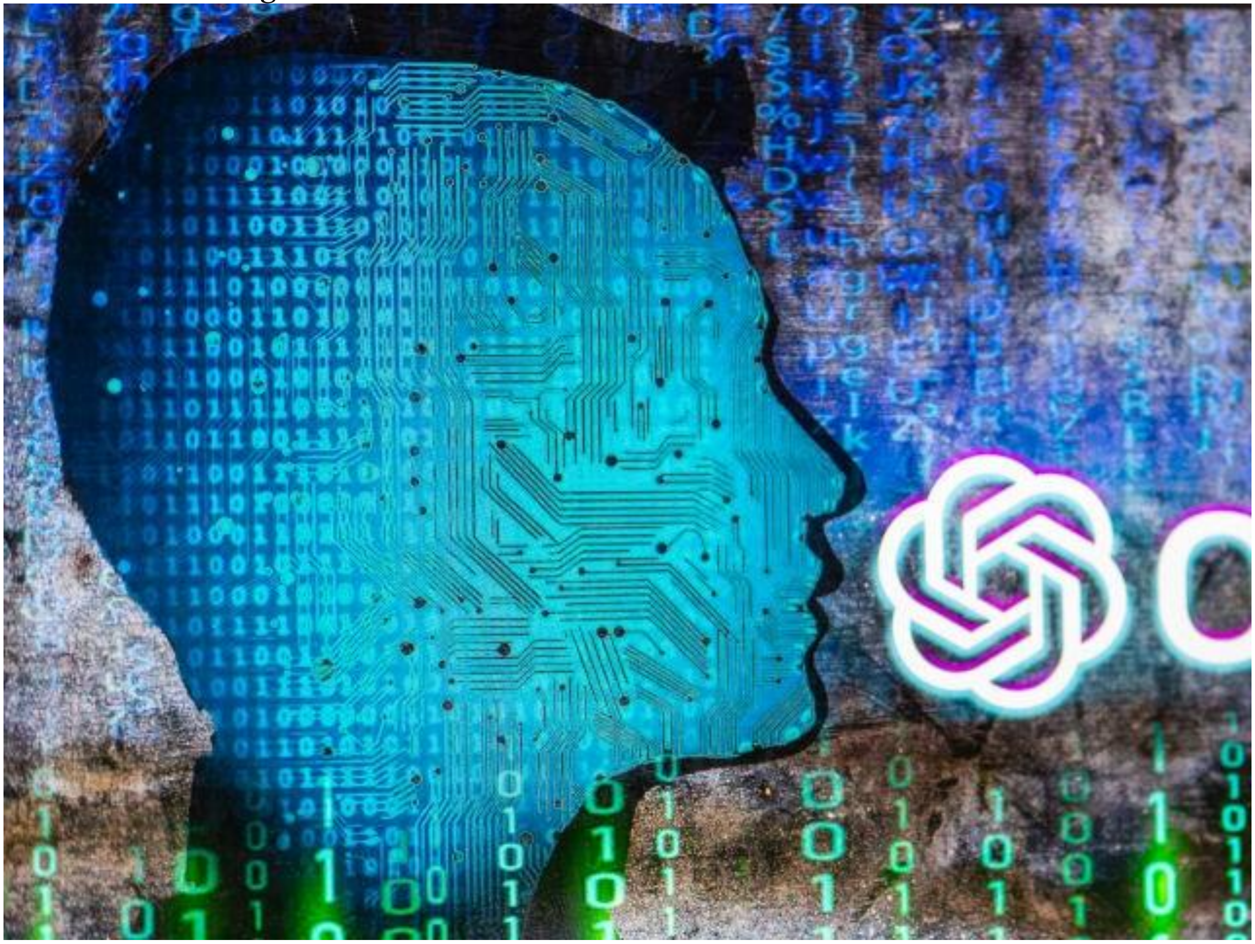
AI RUN AMOK: RESEARCHERS DISCOVER CHATGPT CAN FIGURE OUT EVERYTHING ABOUT YOU FROM SIMPLE CONVERSATIONS

By LUCAS NOLAN

Recent research has uncovered a worrying issue — AI chatbots, like ChatGPT, have the capability to discern sensitive personal information about individuals through casual conversations, like an evil cybernetic version of Sherlock Holmes.

Wired reports that AI chatbots have emerged as intelligent conversationalists, capable of engaging users in seemingly meaningful and humanlike interactions. However, beneath the surface of casual conversation lurks a concerning capability. New research spearheaded by computer science experts has revealed that chatbots, armed with sophisticated language models, can subtly extract a wealth of personal information from users, even in the midst of the most mundane conversations. In other words, AI can determine all sorts of sensitive facts about you based on simple conversations, which could then be used for intrusive advertising or even worse purposes if the information falls into the wrong hands.



OpenAI logo seen on screen with ChatGPT website displayed on mobile seen in this illustration in Brussels, Belgium, on December 12, 2022. (Photo by Jonathan Raa/NurPhoto via Getty Images)

Martin Vechev, a leading computer science professor at ETH Zurich, who championed the research, expressed his concerns, stating, “It’s not even clear how you fix this problem,” and further emphasized, “This is very, very problematic.” The study meticulously analyzed the operational mechanisms of large language models that empower these advanced chatbots, uncovering their alarming proficiency in deducing intimate details such as an individual’s race, location, and occupation.

The research illuminates the potential risks associated with the unsuspecting disclosure of sensitive information. Vechev explained the potential implications, suggesting that malicious actors could exploit chatbots as tools to harvest sensitive data from unsuspecting individuals.

Moreover, the study heralds a forewarning about the future landscape of advertising. It raises questions about a new era where companies could potentially utilize the information gleaned from chatbot interactions to craft detailed and highly personalized user profiles for advertising purposes. Vechev noted: “They could already be doing it.”

Retrieved January 6,2024 from AI Run Amok: Researchers Discover ChatGPT Can Figure Out Everything About You from Simple Conversations (breitbart.com)