



«چت جی پی تی سرچ» در خطر فریب خوردن است

گزارش‌ها حاکی از این هستند که «چت جی پی تی سرچ» در خطر فریب خوردن قرار دارد و ممکن است اطلاعات اشتباه را ارائه دهد.

گزارش‌ها حاکی از این هستند که «چت جی پی تی سرچ» در خطر فریب خوردن قرار دارد و ممکن است اطلاعات اشتباه را ارائه دهد.

به گزارش ایسنا، روزنامه بریتانیایی «گاردین» نوشت موتور جست‌وجوی «چت جی پی تی سرچ» (ChatGPT Search) مبتنی بر هوش مصنوعی که در ماه جاری میلادی راه اندازی شد، با مشکل فریب خوردن همراه است و متن‌های گمراه‌کننده را تولید می‌کند.

به نقل از تک کرانچ، هدف از ویژگی چت جی پی تی سرچ این است که با انجام دادن کارهایی مانند خلاصه کردن بررسی‌های صفحه وب، به مرور سرعت بدهد، اما گاردین خاطرنشان کرد که این قابلیت می‌تواند چت جی پی تی را ترغیب کند تا نظرات منفی را نادیده بگیرد و با درج متن پنهان در وب سایت‌هایی که ایجاد کرده، خلاصه‌های کاملاً مثبت را تولید کند. همچنین، چت جی پی تی سرچ با استفاده از این روش می‌تواند رمزهای مخرب را استخراج کند.

این گونه حملات متنی مخفی، یک خطر شناخته شده برای مدل‌های زبانی بزرگ هستند، اما به نظر می‌رسد این اولین بار است که در یک محصول جستجوی زنده با هوش مصنوعی نشان داده می‌شود. گاردین خاطرنشان کرد که موتور جست‌وجوی «گوگل»، تجربه بیشتری را در برخورد با مشکلات مشابه دارد.

شرکت «اوپن ای آی» (OpenAI) به تماس تک کرانچ درباره این اتفاق خاص اظهار نظر نکرد، اما گفت که از روش‌های گوناگونی برای مسدود کردن وب سایت‌های مخرب استفاده می‌کند و به طور مداوم در حال بهبود بخشیدن آن است.