Comment un YouTubeur a utilisé ChatGPT pour produire des clés de validation Windows?

Titre HTML : Un youtubeur trompe ChatGPT pour générer des clés de licence pour Windows 95

Un youtubeur nommé Enderman a réussi à tromper ChatGPT, un chatbot conversationnel d'OpenAI, pour obtenir des clés de licence gratuites activant Windows 95. Enderman a commencé en demandant à ChatGPT de générer une clé de validation pour Windows 95, mais la réponse était négative. Cependant, Enderman a décidé de modifier le prompt soumis à ChatGPT pour obtenir des suites de caractères répondant à un format de clé différent pour Windows 95. Il a ainsi demandé à ChatGPT de générer 30 ensembles de chaînes de caractères.

ChatGPT a rencontré des difficultés pour répondre à cette requête, mais Enderman a réussi à identifier une clé valide et l'a utilisée pour activer une copie de Windows 95 dans une machine virtuelle. Selon Enderman, seulement une clé de validation sur trente était fonctionnelle. Il pense que le chatbot ne pouvait pas effectuer des divisions et résoudre certains problèmes mathématiques pour générer des clés valides.

Malgré les nombreuses mesures de sécurité intégrées dans ChatGPT, telles que l'impossibilité de générer des clés d'activation pour des logiciels propriétaires, Enderman a trouvé une autre approche en utilisant des formats de clé différents pour tromper le chatbot. Cependant, cela souligne

également les vulnérabilités de l’IA face à de nouveaux cas d’utilisation non prévus.

Enderman a laissé un message de remerciement à ChatGPT pour lui avoir fourni des clés d’activation gratuites pour Windows 95. Ce message a laissé le chatbot confus de s’être fait tromper.

Source : 01net.com

→ Accéder à CHAT GPT en cliquant dessus