

ما المخاطر الأمنية لتطبيقات الذكاء الاصطناعي؟ .. "شات جي بي تي" يجيب

30 نوفمبر، 2024



قد تثير تطبيقات مثل ChatGPT، التي تعتمد على الذكاء الاصطناعي، بعض المخاطر الأمنية إذا لم يتم استخدامها أو إدارتها بشكل صحيح.

ولذلك طلبنا من تطبيق "شات جي بي تي" نفسه، والذي طورته شركة "OpenAI" أن يرصد لنا المخاطر الأمنية للتطبيقات المعتمدة على الذكاء الاصطناعي.

وفي إجابته رد تطبيق "شات جي بي تي" أن التطبيقات المعتمدة على الذكاء الاصطناعي قد تثير بعض المخاوف الأمنية مثل، استخدامها في نشر المعلومات المضللة، عن طريق إنشاء محتوى مضلل أو أخبار كاذبة.

يعتقد "ChatGPT" أنه يمكن استخدامه في الهجمات السيبرانية عبر الهندسة الاجتماعية، وذلك من خلال صياغة رسائل بريد إلكتروني

احتمالية أو محاولات تصيد معقدة، مما يجعل هذه الهجمات أكثر إقناعاً.

يمكن للتطبيقات المعتمدة على الذكاء الاصطناعي تسريب البيانات الحساسة في حال تم إدخالها الى التطبيق عن طريق الدردشة معه، بحسب "شات جي بي تي".

ويرى تطبيق "شات جي بي تي" أن الإفراط في استخدام تطبيقات الذكاء الاصطناعي في المهام الفكرية أو التواصل، يضعف من مهارة المستخدم في القدرة على حل المشكلات.

تجنب مخاطر تطبيقات الذكاء الاصطناعي
تقييد وصول التطبيق إلى البيانات الحساسة أو الحساسة.

تدريب الأفراد على استخدام الأداة بشكل مسؤول وتجنب إدخال معلومات حساسة.

استخدام تقنيات إضافية لمنع إنشاء محتوى ضار.