دراسة تحذر: الذكاء الاصطناعي قادر على سرقة كلمة المرور الخاصة بك

دراسة مقلقة تظهر كيف يسرق الذكاء الاصطناعي كلمات المرور بدقة 95%

حذر تقرير جديد من أن "القراصنة" يمكنهم استخدام أدوات "الذكاء الاصطناعي" لسرقة كلمات مرور المستخدمين بدقة شبه مثالية من خلال الاستماع إلى ضربات لوحة المفاتيح.

وقامت مجموعة من علماء الكمبيوتر في المملكة المتحدة بتدريب نموذج ذكاء اصطناعي لتحديد الأصوات الناتجة عن ضغطات المفاتيح على إصدار 2021 من "ماك بوك برو"، الموصوف بأنه "كمبيوتر محمول شائع جاهز للاستخدام".

وعندما تم تمكين برنامج الذكاء الاصطناعي على هاتف ذكي قريب، كان قادرا على إعادة إنتاج كلمة المرور المكتوبة بدقة هائلة تصل إلى 95%، وفقا لنتائج الدراسة التي نشرتها جامعة كورنيل.

وكانت أداة الذكاء الاصطناعي "الصديقة للقراصنة" أيضا دقيقة للغاية أثناء الاستماع إلى الكتابة من

خلال ميكروفون الكمبيوتر المحمول أثناء مؤتمر فيديو عبر تطبيق "زوم".

وقال الباحثون إن: "الذكاء الاصطناعي أعاد إنتاج ضغطات المفاتيح بدقة 93%، وهو رقم قياسي للوسيط".

وحذر الباحثون من أن العديد من المستخدمين غير مدركين لخطر قيام الجهات السيئة بمراقبة كتابتهم لخرق الحسابات، وهو نوع من الهجمات الإلكترونية أطلقوا عليه اسم "هجوم القناة الجانبية الصوتية".

ولقياس الدقة، ضغط الباحثون على "36" مفتاحا من مفاتيح الكمبيوتر المحمول بما مجموعه 25 مرة لكل مفتاح، مع كون كل ضغطة "متفاوتة في الضغط ومختلفة الإصبع".

وكان البرنامج قادرا على الاستماع وتحديد عناصر كل ضغطة مفتاح، مثل أطوال موجات الصوت. وتم وضع الهاتف الذكي "آيفون 13 ميني" على بعد 17 سم من لوحة المفاتيح.

وأجرى البحث جوشوا هاريسون من جامعة دورهام، وإحسان توريني من جامعة ساري، ومريم مهرنجاد من جامعة رويال هولواي في لندن.

وقال الفريق: "إن إمكانية مساعدة أدوات الذكاء الاصطناعي للمتسللين هي مجرد عامل خطر آخر للتكنولوجيا الناشئة".