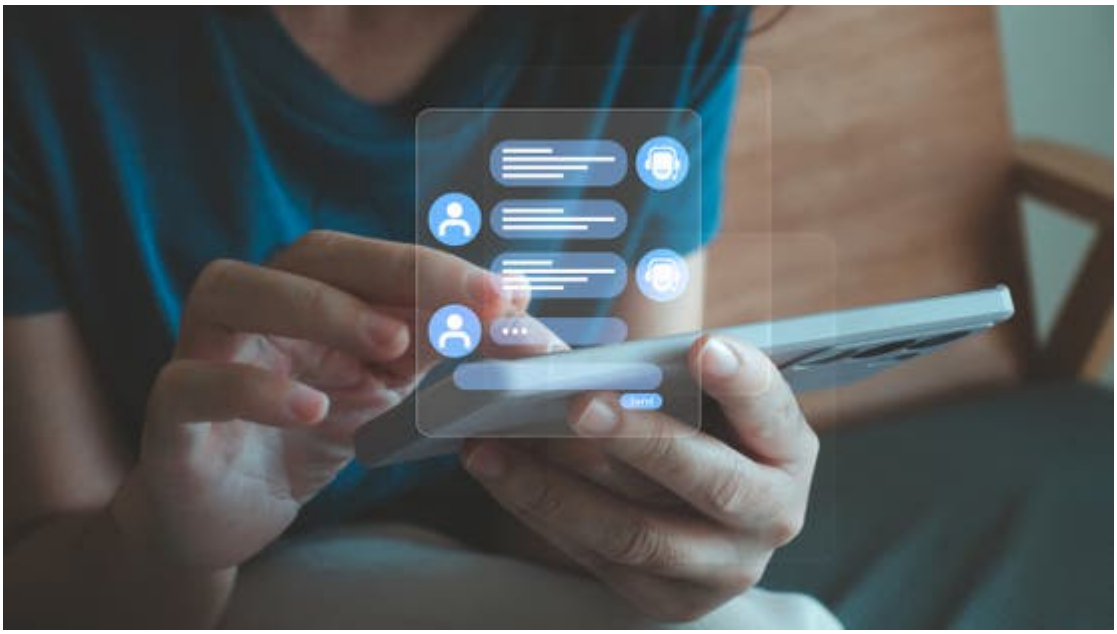
6 نصائح لحماية أمانك عند استخدام روبوتات الدردشة بالذكاء الاصطناعي

20 ديسمبر، 2025



مع تزايد الاعتماد على روبوتات الدردشة المدعومة بالذكاء الاصطناعي في الحياة اليومية، حذّر خبراء أمن سيبراني وتقنيون من مخاطر مشاركة المعلومات الشخصية بشكل مفرط، مؤكدين أن هذه المنصات لا توفّر الخصوصية ذاتها التي تمنحها الاستشارات البشرية.

ووفق تقرير لموقع CNET، فإن ثقة المستخدمين المتزايدة بالذكاء الاصطناعي تدفعهم إلى مشاركة بيانات حساسة قد تُستغل لاحقًا تجاريًا أو أمنيًا. وفي هذا الإطار، قُدّمت مجموعة نصائح أساسية لتعزيز الأمان الرقمي عند استخدام روبوتات المحادثة، أبرزها:

اعتبار روبوتات الدردشة بيئات عامة وليست محادثات خاصة، وتجنّب إدخال أي معلومات تعريفية شخصية كالعنوان أو البيانات المالية أو الصحية.

عدم الإفراط في مشاركة الحالة النفسية أو المشكلات الشخصية، إذ يمكن تحليل هذه البيانات لبناء ملفات دقيقة عن نقاط الضعف.

تقليل ما يفصح عنه المستخدم للروبوت، مع تعطيل ميزات الذاكرة والتخصيص واستخدام بريد إلكتروني ثانوي، إضافة إلى إلغاء

المشاركة في تدريب النماذج على البيانات المدخلة.

تصدير البيانات بشكل دوري للاطلاع على ما تم تخزينه من معلومات شخصية.

التحقق من صحة المعلومات التي يقدمها الذكاء الاصطناعي وعدم التعامل معها كمصادر مؤكدة، بسبب احتمالات الخطأ أو "الهلوسة".

الحذر من عمليات الاحتيال، خصوصًا الروابط المزيفة أو صفحات تسجيل الدخول الوهمية، مع تفعيل المصادقة الثنائية ومراقبة أي نشاط مشبوه على الحسابات.

وأكد الخبراء أن الذكاء الاصطناعي أداة مفيدة، لكن التعامل معها بوعي وحذر بات ضرورة لحماية الخصوصية في عالم رقمي سريع التطور.