



نخيل نيوز - متابعة

كشف باحثون في مجال الخصوصية عن إمكانية الوصول إلى أكثر من 6 آلاف محادثة جرى مشاركتها عبر مساعد الذكاء الاصطناعي التابع لشركة "ميتا"، تضمنت معلومات شخصية ومالية حساسة، من بينها بيانات عن قروض الشركات الصغيرة، وأجزاء من أرقام حسابات مصرفية، وأسماء موظفين، وتقارير داخلية عن الإيرادات.

وبحسب تقرير نشره موقع "بي سي وورلد" المتخصص في التكنولوجيا، تعود المشكلة إلى الطريقة التي اعتمدتها "ميتا" لإنشاء روابط مشاركة المحادثات، إذ أدرجت عناوين الدردشات ضمن روابط الإنترنت، ما أتاح للباحثين اكتشافها من خلال البحث في سجلات نظام أسماء النطاقات، المعروف اختصاراً باسم "دي إن إس"، دون الحاجة إلى اختراق حسابات المستخدمين أو أنظمة الشركة.

وأعاد الحادث تسليط الضوء على المخاطر المرتبطة بمشاركة محادثات الذكاء الاصطناعي عبر روابط عامة، خصوصاً أن حوادث مشابهة طالت خدمات أخرى، من بينها "تشات جي بي تي" و"كلود"، بعدما ظهرت محادثات مستخدميها في نتائج محركات البحث.

وتتيح ميزة مشاركة المحادثات للمستخدم إرسال رابط إلى صديق أو زميل للاطلاع على جلسة سابقة مع مساعد الذكاء الاصطناعي، بما يشمل الإجابات والعروض التقديمية والرسوم البيانية والملفات التي أنشأها النموذج. لكن هذه الميزة قد تتحول إلى مصدر خطر عندما تحتوي المحادثة على معلومات خاصة أو عندما يُعاد تداول الرابط خارج نطاق المشاركة الأصلي.

وتضمنت المحادثات معلومات حساسة، مثل طلبات الحصول على قروض للشركات الصغيرة، وأجزاء من أرقام حسابات مصرفية، وقوائم بأسماء موظفين، وتقارير أعمال داخلية احتوت على بيانات تعريف شخصية وأرقام فعلية للإيرادات. وتبين أن تضمين عناوين المحادثات داخل روابط الإنترنت سهّل العثور على الروابط المشتركة من خلال البحث في سجلات نظام أسماء النطاقات، وهي سجلات يمكن أن تكشف معلومات عن أسماء النطاقات والروابط المرتبطة بها. وعقب إبلاغ الباحثين الشركة بالمشكلة، أوقفت "ميتا" ميزة مشاركة المحادثات في "ميوز"، وأشارت إلى أنها ستجري تعديلات على طريقة اكتشاف الروابط.

ولا تقتصر مخاطر تسرب المحادثات على خدمات "ميتا"، إذ واجه مستخدمو مساعد "كلود" التابع لشركة "أنثروبيك" مشكلة ظهور محادثاتهم المشتركة ضمن نتائج بحث "غوغل"، في واقعة أعادت إلى الأذهان حادثة مشابهة سُجلت في وقت سابق.

نخيل نيوز

كما اكتشف مستخدمون لـ "تشات جي بي تي" أن محادثات شاركوها عبر روابط عامة أصبحت قابلة للعثور عليها من خلال محرك بحث "غوغل"، قبل إزالة المحادثات المتأثرة من نتائج البحث.

وتختلف التفاصيل التقنية بين هذه الحوادث، ففي حالة "ميتا"، أمكن اكتشاف الروابط من خلال البحث في سجلات نظام أسماء النطاقات، بينما زحف محرك "غوغل" إلى المحادثات المشتركة في حالتي "تشات جي بي تي" و"كلود".

لكن الوقائع الثلاث تشترك في مشكلة أساسية، تتمثل في الاعتماد على روابط عامة تتيح الوصول إلى المحادثات لأي شخص يمتلك الرابط، ما يجعل تداولها خارج نطاقها الأصلي أمراً ممكناً.

وينطبق هذا الأمر أيضاً على روابط مشاركة المحادثات في مساعدات ذكاء اصطناعي أخرى، من بينها "جيميني"، إذ لا يعني إنشاء رابط للمشاركة أن المحتوى سيظل محصوراً بالشخص الذي أرسل إليه.

واتخذت شركات الذكاء الاصطناعي إجراءات للحد من ظهور المحادثات المشتركة في نتائج البحث، فيما يُتوقع أن تعمل "ميتا" على منع اكتشاف روابطها من خلال عمليات البحث في سجلات نظام أسماء النطاقات.

كما أتاحت "كلود" للمستخدمين إمكانية دعوة أشخاص محددين لمشاركة المحادثات معهم، بدلاً من الاكتفاء بإنشاء روابط عامة يمكن لأي شخص يمتلكها فتحها.

لكن هذه الإجراءات لا تلغي المخاطر بالكامل؛ فحتى إذا لم تظهر الروابط في نتائج "غوغل"، يستطيع الشخص الذي يتلقى رابط المحادثة إعادة إرساله إلى آخرين عبر البريد الإلكتروني أو نشره على منصات التواصل الاجتماعي.

وبذلك، لا ترتبط المشكلة فقط بإمكانية العثور على الروابط عبر محركات البحث، بل بطبيعة الرابط العام نفسه، الذي يمكن تداوله خارج نطاق المشاركة الأصلي.

وتوفر خدمات الذكاء الاصطناعي الكبرى، بما فيها "تشات جي بي تي" و"كلود"، أدوات لمراجعة المحادثات التي سبق للمستخدم مشاركتها وإلغاء مشاركة الروابط عند الحاجة.

وتبقى القاعدة الأهم هي التعامل مع رابط المحادثة العامة كما لو أن محتواها قد أصبح متاحاً على نطاق واسع. فإذا لم تكن مستعداً لنشر المحادثة كاملة في مكان عام، فمن الأفضل عدم مشاركتها عبر رابط يستطيع أي شخص يمتلكه الوصول إليه.