

5 أشياء احذر مشاركتها مع منصات الذكاء الاصطناعي



الجمعة 26 ديسمبر 2025 05:00 م

أصبح منصات الذكاء الاصطناعي، وأبرزها روبوت الدردشة (تشات جي بي تي) الوجهة المفضلة للكثيرين، للحصول على المساعدة والمعلومات في مختلف المجالات، فهي قادرة على إجراء المحادثات والإجابة على الأسئلة وتقديم معلومات قيّمة

وعلى الرغم من فائدها الكبيرة، إلا أن خبراء الأمن السيبراني يحذرون من مشاركة بعض المعلومات معه، وتحديدًا خمسة أمور بالغة الأهمية يجب عدم مشاركتها معه مطلقًا

1. المعلومات الشخصية القابلة للتعريف

تشمل المعلومات الشخصية القابلة للتعريف مجموعة واسعة من البيانات الشخصية، بدءًا من التفاصيل الأساسية كالاسم الكامل وتاريخ الميلاد، وصولًا إلى معلومات أكثر حساسية كأرقام الحساب البنكي والعناوين وأرقام الهواتف وعناوين البريد الإلكتروني. إذ يحذر الخبراء من خطورة مشاركة هذه المعلومات مع "تشات جي بي تي".

فبينما قد لا تقوم منصات الذكاء الاصطناعي بتخزين هذه المعلومات أو الاحتفاظ بها عمدًا، إلا أن قابليتها للاختراق تجعلها عرضة لسرقة البيانات. ويمكن أن تكون عواقب هذه الاختراقات وخيمة، وتؤدي إلى سرقة الهوية والاحتيال المالي، بل وحتى التلاعب بالمُحتل بالسجلات الشخصية.

قد يستغل الهاكرز هذه البيانات لانتحال شخصيات الأفراد، أو اختراق حساباتهم، أو التصيد الاحتيالي. لذا، كمستخدمين، يجب علينا توخي الحذر الشديد عند مشاركة أي شكل من أشكال المعلومات الشخصية القابلة للتعريف مع الأنظمة التي تعمل بالذكاء الاصطناعي، وذلك لحماية هوياتنا وسلامتنا المالية.

2. المعلومات المالية والمصرفية

يُعدّ مجال المعلومات المالية والمصرفية بالغ الحساسية، ويجب عدم إفشائه مطلقًا لمنصات الذكاء الاصطناعي. تشمل هذه البيانات أرقام بطاقات الائتمان، وبيانات الحسابات المصرفية، وغيرها من التفاصيل المالية. ولضمان أعلى مستويات الأمان، من الضروري استخدام قنوات مشفرة وآمنة عند إجراء أي معاملات مالية عبر الإنترنت.

ويحذر الخبراء من العواقب المحتملة لاختراق المعلومات المالية، بدءًا من المعاملات الاحتيالية وسحب الأموال من الحسابات المصرفية وصولًا إلى فقدان الاستقرار المالي بالكامل. لذا، يجب على المستخدمين توخي الحذر دائمًا والالتزام ببروتوكولات أمنية صارمة لحماية بياناتهم المالية.

3. كلمات المرور وبيانات تسجيل الدخول

تُعدّ كلمات المرور وبيانات تسجيل الدخول بمثابة المفاتيح الرقمية لهوياتنا الإلكترونية ومعلوماتنا الشخصية. ويُشكّل مشاركة هذه البيانات الحساسة مع "تشات جي بي تي" أو أي نظام ذكاء اصطناعي آخر خطرًا كبيرًا. فمشاركة هذا النوع من البيانات السرية تُتيح الوصول غير المصرح به من قبل جهات خبيثة.

لذا، يجب أن تكون كلمات المرور فريدة وقوية لكل حساب إلكتروني، ما يُصعّب على مجرمي الإنترنت استغلالها من الضروري الامتناع عن مشاركة كلمات المرور مع أي شخص، بما في ذلك أنظمة الذكاء الاصطناعي، وتفعيل إجراءات أمنية إضافية مثل المصادقة الثنائية لتوفير طبقة حماية إضافية وبهذه الطريقة، يُمكننا الحدّ من خطر الوصول غير المصرح به والحفاظ على سلامة هوياتنا الإلكترونية

4. المعلومات الخاصة أو السرية

قد تترتب على مشاركة المعلومات الخاصة أو السرية مع أنظمة الذكاء الاصطناعي عواقب وخيمة، على الصعيدين الشخصي والمهني، فهي تفتقر إلى الفهم السياقي الذي يمتلكه البشر، مما يجعلها أكثر عرضة للكشف غير المقصود عن محتوى حساس

والكشف عن الأسرار الشخصية أو التفاصيل الحميمية أو المعلومات السرية المتعلقة بالعمل لأنظمة الذكاء الاصطناعي قد يؤدي إلى كشف غير مقصود، مما يضر بخصوصيتنا وسمعتنا

في بيئات العمل، قد يؤدي إفشاء معلومات العمل الحساسة إلى خرق الثقة، ومشاكل قانونية محتملة، والإضرار بالميزة التنافسية للمؤسسة

من الضروري توخي الحذر والتأكد من أن المعلومات التي تتم مشاركتها مع أنظمة الذكاء الاصطناعي تقتصر على ما هو ضروري ومناسب للغرض المقصود

5. الملكية الفكرية أو الملكية الخاصة

قد تنطوي مشاركة المعلومات الخاصة بالملكية الفكرية، بما فيها المعلومات السرية، والأفكار الحاصلة على براءات اختراع، والمواد المحمية بحقوق الطبع والنشر، والأسرار التجارية مع أنظمة الذكاء الاصطناعي، على مخاطر جسيمة، بما فيها احتمال السرقة أو الاستخدام غير المصرح به

تُعد حماية الملكية الفكرية أمراً بالغ الأهمية للحفاظ على حقوق الملكية والقيمة التجارية

وقد يؤدي النشر غير المصرح به للأفكار المبتكرة أو المعرفة السرية إلى نزاعات قانونية، وفقدان الميزة التنافسية، وعواقب مالية وخيمة

يجب على المستخدمين توخي الحذر والامتناع عن الكشف عن أي شكل من أشكال الملكية الفكرية لأنظمة الذكاء الاصطناعي، لضمان بقاء أعمالهم الإبداعية وابتكاراتهم آمنة ومحمية

أهمية أمن البيانات

في ظل التطور التكنولوجي، أصبحت خروقات البيانات مصدر قلق متزايد إذ يسعى مجرمو الإنترنت باستمرار إلى استغلال الثغرات الأمنية في الأنظمة للوصول غير المصرح به إلى المعلومات الحساسة

وقد سُجلت حالات استُهدفت فيها منصات مدعومة بالذكاء الاصطناعي مثل تشات جي بي تي وفي الفترة من يونيو 2022 إلى مايو 2023، تم اختراق بيانات اعتماد أكثر من 100 ألف حساب مستخدم مدفوع على منصة شات جي بي تي وبيعها في أسواق الإنترنت المظلم

لذا، فإن حماية خصوصيتنا وأمننا أمر بالغ الأهمية، والوعي بالبيانات التي نقدمها لأنظمة الذكاء الاصطناعي ضروري في هذا المسعى من خلال فهم هذه القيود واستخدام الذكاء الاصطناعي بمسؤولية، بما يُمكننا من الاستفادة الكاملة من مزاياه مع الحفاظ على حياتنا الرقمية