

الذكاء الاصطناعي قد يجعل التهديدات السيبرانية أكثر تطوراً

الذكاء الاصطناعي في أيدي المهاجمين: سرعة أكبر وتخفي أذكي

قد لا يغير الذكاء الاصطناعي الهدف الأساسي من الهجوم، لكنه يمنح المهاجمين قدرات متقدمة لتطوير أساليبهم وجعلها أكثر تعقيداً وفعالية. فهو يسهل جمع المعلومات، وصياغة رسائل خداع دقيقة، وتخصيصها لاستهداف الضحية بشكل مباشر. وتتجلى أبرز هذه القدرات في عدة صور، منها:

تعديل أساليب الهجوم لتبدو مختلفة في كل مرة لتفادي الاكتشاف.



البحث عن ثغرات أو نقاط ضعف في الأنظمة والخدمات بشكل أسرع.



تحليل كميات كبيرة من المعلومات بسرعة لاختيار أهداف أكثر دقة.



التلاعب بتعليمات أدوات الذكاء الاصطناعي من خلال حقن الأوامر لتغيير استجابتها وإنتاج مخرجات مضللة أو غير آمنة.



ولا تقتصر هذه التهديدات على فئة محددة، فقد تستهدف أي شخص مرتبط بالمؤسسة، سواء كان موظفاً، مديراً، مسؤولاً في قسم معين، أو مزود خدمة من طرف ثالث. فالهدف غالباً هو استغلال الثقة أو الاستعجال لدفع الشخص إلى اتخاذ إجراء قد يعرض بياناته أو بيانات المؤسسة للخطر.

مع تطور استخدامات الذكاء الاصطناعي في بيئات العمل، أصبحت التهديدات السيبرانية أكثر اعتماداً على استغلال سلوك الموظف وثقته عند التعامل مع الرسائل والروابط والطلبات الإلكترونية. فالمخاطر لم تعد تعتمد فقط على الأنظمة أو الأدوات التقنية، بل قد تبدأ من قرار بسيط يتخذه المستخدم عند قراءة رسالة أو فتح رابط أو مشاركة ملف أو تنفيذ طلب يبدو مألوفاً. لذلك، يساعد الوعي بهذه الأساليب على فهم طبيعة التهديدات الحديثة، والتمييز بين الطلبات الاعتيادية وتلك التي قد تحمل مؤشرات خطر، خاصة عندما تستخدم تقنيات الذكاء الاصطناعي لجعل الهجمات أكثر إقناعاً وصعوبة في الاكتشاف.

هو أحد أساليب التلاعب بتطبيقات الذكاء الاصطناعي، ويحدث عندما تتعامل الأداة مع تعليمات مضللة موجودة ضمن نص، رسالة، ملف، رابط، أو صفحة ويب، بهدف التأثير على استجابتها أو تغيير الغرض الأصلي من الطلب. وتكمن الخطورة في أن الأداة قد تتعامل مع هذه التعليمات وكأنها جزء من الطلب، مما قد يؤدي إلى مخرجات غير دقيقة أو توصيات غير آمنة، خاصة إذا كانت الأداة مرتبطة بأنظمة العمل مثل البريد الإلكتروني، الملفات، أو التقويم.

ثقافة سيبرانية:



هل تعلم ما المقصود بحقن الأوامر (Prompt Injection)؟

كيف يطور الذكاء الاصطناعي التهديدات السيبرانية؟

مع تطور تقنيات الذكاء الاصطناعي، لم تعد المخاطر السيبرانية مرتبطة فقط بالرسائل الاحتيالية التقليدية أو محاولات الخداع الواضحة، بل أصبحت أكثر تنوعًا وقدرة على استغلال الثقة والاستعجال في بيئة العمل.

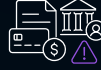
نوع التهديد	الفكرة الأساسية	كيف قد يتطور باستخدام الذكاء الاصطناعي	كيف قد يظهر للموظف؟
 التصيد الاحتيالي	استهداف الموظف للحصول على بيانات الدخول أو دفعه لتنفيذ إجراء غير آمن.	إنشاء رسائل مخصصة واحترافية تحاكي أسلوب التواصل المؤسسي وتخلو من المؤشرات التقليدية للاحتيال.	بريد إلكتروني يطلب فتح رابط تسجيل دخول مزيف، مرفق مشبوه، أو طلب تحديث كلمة المرور.
 الهندسة الاجتماعية المدعومة بالذكاء الاصطناعي	التأثير على قرار الموظف من خلال استغلال الثقة أو الاستعجال.	قد تُستخدم معلومات متاحة عن الموظف أو المؤسسة لصياغة طلب يبدو منطقيًا ومرتبًا بسياق العمل.	طلب يبدو طبيعيًا من جهة معروفة، مثل مشاركة ملف، تأكيد معلومة، أو تنفيذ إجراء إداري بشكل عاجل.
 انتحال الهوية والتزييف العميق	إظهار التواصل وكأنه صادر من جهة موثوقة.	تقليد أسلوب الكتابة أو الصوت، أو إنشاء تسجيل صوتي أو مقطع فيديو مزيف يبدو وكأنه صادر من مدير أو زميل أو جهة رسمية.	رسالة، مكالمة صوتية، أو مقطع مرئي يبدو صادرًا من شخص معروف ويطلب إجراءً سريعًا أو معلومات حساسة.
 اختراق البريد الإلكتروني التجاري BEC	استهداف الإجراءات المالية أو الإدارية داخل بيئة العمل.	صياغة طلبات دقيقة مرتبطة بالفواتير، الموردين، الحسابات البنكية، أو أليات الاعتماد الداخلي.	طلب تحويل مالي، تغيير بيانات حساب بنكي للمورد، اعتماد فاتورة، أو إرسال مستندات رسمية.

انتبه لهذه الإشارات قبل اتخاذ أي إجراء

طلبات عاجلة أو ملحة تتجاوز الإجراءات المعتادة أو تقلل من أهمية التحقق.



طلب مشاركة معلومات حساسة، تنفيذ إجراء مالي أو إداري، أو تعديل بيانات مثل الحسابات البنكية أو معلومات الموردين.



وجود روابط أو مرفقات غير متوقعة أو اختلافات بسيطة في البريد الإلكتروني أو الروابط قد تكون مؤشرًا على محاولة احتيال.



حتى لو بدا الطلب رسميًا أو صادرًا من جهة معروفة، توقف وراجع الطلب إذا لاحظت أيًا من الإشارات التالية:

تذكر دائمًا:

مع تطور التهديدات المدعومة بالذكاء الاصطناعي، لا يكفي أن تبدو الرسالة رسمية أو أن يكون الصوت مألوفًا. في بيئة العمل، قد يكون الخطر في طبيعة الطلب نفسه، خاصة إذا كان يتضمن مشاركة معلومات حساسة، تغيير بيانات دفع، فتح مرفق غير متوقع، أو تنفيذ إجراء مالي أو إداري عاجل. لذلك، تأكد من مصدر الطلب عبر قناة رسمية أخرى، وبلغ عند الاشتباه.



لمواجهة التهديدات السيبرانية المدعومة بالذكاء الاصطناعي

توقف
قبل أي إجراء



تحقق
من المصدر عبر قناة أخرى



بلغ
عند الاشتباه

