الذكاء الاصطناعي التوليدي يمحو المؤشرات السلوكية التي اعتمدت عليها فلاتر البريد، بحسب Proofpoint



تفيد Proofpoint بأن الذكاء الاصطناعي التوليدي جعل الرسائل الخبيثة سليمة اللغة ومخصصة وفريدة، ما يضعف الكشف المعتمد على المؤشرات السلوكية وحدها. وعرضت أمثلة في مؤتمر Protect 2026.

- كانت الرسائل الخبيثة تكشف نفسها سابقاً عبر ركاكة الصياغة وعمومية الذرائع وتكرار القوالب.
- يُنتج الذكاء الاصطناعي التوليدي اليوم رسائل سليمة اللغة ومخصصة وفريدة لكل مستلم.
- المؤشرات السلوكية التي اعتمدت عليها فلاتر البريد لسنوات آخذة في التلاشي.
- عرضت Proofpoint أمثلة عدة على هذا التحول في مؤتمر Protect 2026.

ما الذي تغيّر

تفيد Proofpoint بأن الذكاء الاصطناعي التوليدي غيّر شكل الرسالة الخبيثة. فالرسائل التي كانت تفضح نفسها بركاكة الصياغة وعمومية الذرائع وتكرار القوالب أصبحت تصل اليوم بلغة سليمة، ومخصصة، وفريدة لكل مستلم.

أثر ذلك على الكشف

اعتمدت فلاتر البريد طويلًا على مؤشرات سلوكية، مثل أنماط تتكرر عادةً عبر حملات الهجوم. ووفق التقرير، فإن هذه المؤشرات تتلاشى مع إزالة الذكاء الاصطناعي لتلك العلامات. ومن ثم يصبح الكشف المعتمد على السلوك وحده أضعف مما كان. وقد عرضت Proofpoint أمثلة عدة على هذا التحول في مؤتمر Protect 2026.

ولا يذكر المصدر أرقاماً أو حملات مسماة أو ضحايا محددين، لذا فالقراءة العملية اتجاهية: العلامات الظاهرة التي تعلّم الموظفون والفلاتر رصدها باتت أقل موثوقية.

الخطوة التالية

على الجهات المنظمة أن تعدّ هذا الخبر دافعاً للمراجعة لا للتسرع في ردة الفعل. راجعوا مدى اعتماد حماية البريد والتوعية بالتصيد على رصد اللغة الضعيفة أو القوالب المتكررة، وقيّموا هل تتحمل طبقات أخرى، مثل ضوابط الهوية والتحقق من الطلبات الحساسة، عبئاً كافياً.

ما يجب فعله الآن

1. راجعوا ضوابط حماية البريد والتوعية التي تعتمد على رصد اللغة الضعيفة أو القوالب المتكررة.
2. اسألوا مزود حماية البريد عن آلية الكشف بما يتجاوز المؤشرات السلوكية وحدها.
3. حدّثوا محتوى التوعية بالتصيد ليركز على التحقق من الطلب لا على الحكم بجودة الصياغة.
4. اشترطوا التحقق عبر قناة مستقلة لطلبات الدفع وبيانات الدخول والوصول إلى البيانات الواردة بالبريد.
5. عززوا ضوابط الهوية مثل المصادقة متعددة العوامل للحد من الضرر إذا نجحت رسالة مقنعة.