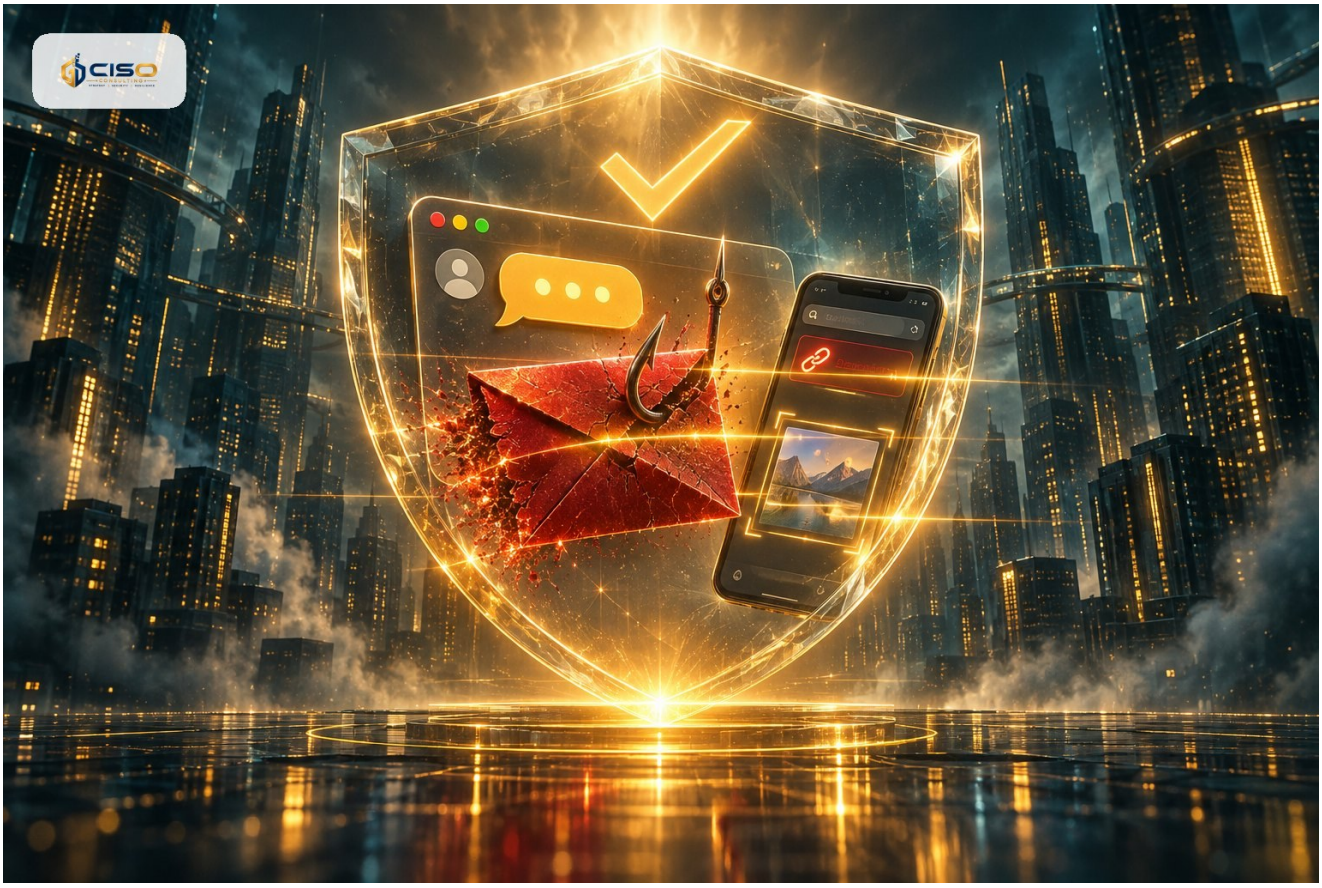
موصل Norton يتيح فحص الاحتيال بالذكاء الاصطناعي داخل محادثات Claude



يتيح موصل Norton لمستخدمي Claude فحص الرسائل والبريد والصور والروابط المشبوهة مع شرح للنتيجة وتوصيات. وأظهر اختبار Help Net Security نتائج واضحة للاحتيال والتصيد والعرض المشروع.

- يضيف الموصل قدرات Norton Genie لكشف الاحتيال إلى Claude دون حاجة إلى حساب Norton أو تطبيق منفصل.
- يوفر ثلاث أدوات: فحص الاحتيال، وإرشادات التهديدات مع توصيات الاستجابة للحوادث، ودعم منتجات Norton، مع إمكانية ضبط صلاحيات كل أداة.
- في الاختبار صُنفت رسالة غرامة حكومية مزيفة كابتزاز بثقة عالية، وصُنف بريد ترويجي حقيقي على أنه آمن.
- صُنف إشعار تجديد اشتراك تخزين سحابي كتصيد، مع إقرار الأداة بتعذر تأكيد خبثه من المعلومات

المتاحة.

- كانت التوصية ثابتة: تجنب الروابط والتحقق عبر المواقع أو التطبيقات الرسمية.

أطلقت Norton موصلًا يدمج قدرات Genie لكشف الاحتيال بالذكاء الاصطناعي في روبوت المحادثة Claude. يمكن للمستخدم إرسال رسائل بريد ونصوص وصور شاشة وروابط مشبوهة للتحليل، كما يمكنه طرح أسئلة عامة عن الأمن السيبراني والخصوصية وحماية الهوية. ولا يتطلب ذلك حساب Norton ولا تطبيقاً منفصلًا.

ما الذي تقدمه الأداة

يوفر الموصل ثلاث أدوات: الأولى تفحص الروابط والرسائل والبريد وأرقام الهاتف بحثاً عن الاحتيال، والثانية تقدم إرشادات حول التهديدات وتوصيات للاستجابة للحوادث وتوعية بالسلامة، والثالثة تتعلق بدعم منتجات Norton. ويمكن ضبط صلاحيات كل أداة على حدة.

وتظهر النتيجة في بطاقة مخصصة تتضمن التصنيف ومستوى الثقة والتشخيص والشرح والتوصيات.

ما أظهره الاختبار

أجرى مراجع من Help Net Security الاختبار على iPhone. صُنفت رسالة نصية مزيفة تنتحل صفة وزارة حكومية بشأن غرامة سرعة غير مسددة على أنها ابتزاز بثقة عالية، استناداً إلى انتحال الجهة الرسمية واللغة الرسمية والإشارات القانونية وتصاعد الإلحاح. أما بريد ترويجي حقيقي بمناسبة Black Friday فصُنف آمناً، ومع ذلك نصحت الأداة بزيارة موقع الشركة بدل النقر على الأزرار داخل البريد.

وصُنف إشعار تجديد اشتراك تخزين سحابي على أنه تصيد بسبب العلامة التجارية العامة والضغط لتسوية الدفع ورقم اشتراك يتعذر التحقق منه. وفي هذه الحالة أقرت الأداة بأنها لا تستطيع تأكيد النية الخبيثة قطعياً، ونصحت بفتح تطبيق المزود أو موقعه الرسمي، وحذف الرسالة إن لم يوجد اشتراك مطابق.

الأهمية

تكمن فائدة الأداة لفرق الأمن في الشروحات المنظمة التي تساعد الموظفين على إدراك أنماط الاحتيال المتكررة. وتتناول المراجعة أداة موجهة للمستهلكين، ولا تقيّم استخدامها في المؤسسات أو معالجة البيانات أو دقتها خارج هذه الأمثلة.

ما يجب فعله الآن

1. ذكّروا الموظفين بأن أدوات فحص الاحتيال بالذكاء الاصطناعي مساندة فقط، وأن الرسائل المشبوهة يجب الإبلاغ عنها لفريق الأمن.
2. راجعوا البيانات والصلاحيات التي يطلبها أي موصل طرف ثالث قبل السماح به في مساعدات الذكاء الاصطناعي، وفق سياسات حماية البيانات وإدارة مخاطر الأطراف الخارجية.
3. حذّروا من لصق بيانات العملاء أو معلومات سرية في أدوات ذكاء اصطناعي خارجية عند فحص الرسائل.
4. عززوا في التوعية قاعدة عدم استخدام الروابط في إشعارات الدفع أو الغرامات غير المتوقعة، والتحقق عبر المواقع أو التطبيقات الرسمية.

5. استخدموا هذه الأمثلة (انتحال جهات حكومية وتصيد تجديد الاشتراكات) في محاكاة التصيد.