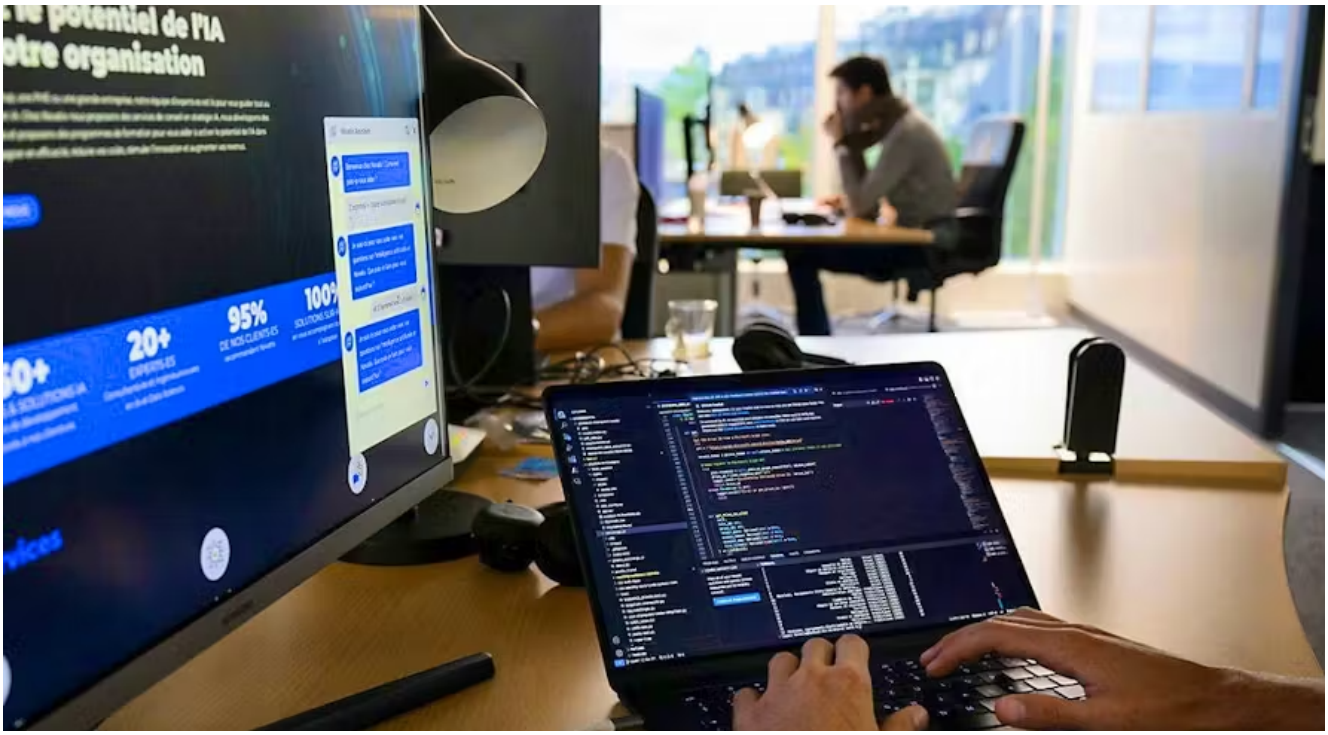
الذكاء الاصطناعي يجعل عمليات الاحتيالٍ عبر الإنترنت أكثر تعقيدا

11 فبراير، 2025



يشرح خبراء في الأمن السيبراني أنّ أدوات الذكاء الاصطناعي التي أصبحت قادرة راهنا على إنتاج نصوص وصور ومقاطع فيديو بشكل فوري تجعل عمليات الاحتيال معقدة أكثر، داعين مستخدمي الإنترنت إلى توخي الحذر.

من عملية الاحتيال التي حظيت بتغطية إعلامية كبيرة لامرأة فرنسية دفعت 830 ألف يورو لشخص ادعى أنه براد بيت، وصولا إلى مجموعات تبرعات وهمية لضحايا حرائق لوس أنجليس، أظهرت الأسابيع الأخيرة أننا جميعا "أفرادا وشركات نشكل أهدافا للهجمات الإلكترونية"، بحسب أرنود لومير من شركة "اف 5" الأميركية المتخصصة بالأمن السيبراني.

في فرنسا، تم تسجيل أكثر من 130 ألف عملية احتيال عبر الإنترنت في العام 2023 بحسب بيانات وزارة الداخلية، التي تشير إلى زيادة بنسبة 8% سنويا في المتوسط بالجرائم "الرقمية" المتعلقة بجرائم الملكية منذ العام 2016.

أحد أكثر أشكال عمليات الاحتيال عبر الإنترنت شهرة هو "التصيد الاحتيالي"، أي إرسال رسائل بالبريد إلكتروني أو رسائل نصية قصيرة تحت ادعاءات كاذبة تحضّ المستخدمين على النقر على رابط احتيالي ومشاركة البيانات الشخصية.

تجعل روبوتات المحادثة المهاجمين يوفرون الوقت وتتيح لهم إعداد رسائلهم الكاذبة بشكل أفضل، وفق لومير.

إذا كان المحتال يجهل تفاصيل لغة معيّنة يستخدم الذكاء الاصطناعي التوليدي لكتابة بريده الإلكتروني، "فسيخفي تماما الأدلة" كالأخطاء الإملائية والنحوية، على قول الخبير.

رؤساء شركات مزيّفون

ليست برامج توليد النصوص سوى غيض من فيض, يمكن لنماذج الذكاء الاصطناعي "الاستفادة من كل البيانات التي سُرقت خلال السنوات الأخيرة لأتمتة إنشاء عمليات احتيال مخصصة جدا"، بحسب ستيف غروبمان، المدير الفني لشركة "مكافي" McAfee المتخصصة في برامج الأمان.

وبدل الاكتفاء بمكاسب صغيرة وسريعة، يسعى المهاجمون غالبا إلى كسب ثقة بعض الموظفين داخل الشركات المستهدفة.

إذا وقع موظف في الفخ، ينتظر المجرمون "حتى يصبح هذا الشخص مؤثرا جدا أو تسنح فرصة جيّدة لابتزازه من أجل الأموال" قبل استغلال هذا التواصل، على قول مارتن كريمر، من شركة "نوو بي 4" KnowBe4 الأميركية للتدريب على الأمن السيبراني.

وفي فبراير 2024، حصل محتالون على 26 مليون يورو من شركة متعددة الجنسية في هونغ كونغ.

وقالت السلطات إن أحد الموظفين الماليين اعتقد أنه كان في مكالمة جماعية عبر الفيديو مع الرئيس التنفيذي للشركة وموظفين آخرين، إلا أنّ هؤلاء كانوا صورا متحركة مفبركة بتقنية "التزييف العميق".

يحذر ستيف غروبمان الذي يؤكد أن باحثا في شركة "مكافي" تمكن من استبدال وجهه بوجه النجم الهوليوودي توم كروز بأقل من 5 يورو، أنّ "أحدث جيل من برامج التزييف العميق وصل إلى نقطة لا يستطيع فيها أحد تقريبا التمييز بين الصورة الفعلية والصورة المولّدة بواسطة الذكاء الاصطناعي".

كلمة مفتاح

يقول لومير إنّ التأكد من هوية المحاور عبر الإنترنت، "يحتاج نوعا ما إلى كلمة مفتاح".

وتتمثل إحدى النصائح الأخرى بالطلب من أحد المحاورين عبر الفيديو تحريك الكاميرا لإظهار محيطه، وهو ما يصعب على الذكاء الاصطناعي إنجازه راهنا.

أصبحت عمليات الاحتيال عبر الإنترنت مجالا مربحا، "فعلى غرار قطاعات أخرى، ثمة سلاسل توريد ونظام كامل لدعمها"، على ما يلاحظ الخبير في "مكافي".

على الرغم من أن عددا كبيرا من عمليات الشرطة قوضت شبكات معيّنة، مثل شبكة "لوكبيت"، وهي إحدى مجموعات الجرائم الالكترونية الرئيسية في العالم والتي تم تفكيكها في أوائل عام 2024، بات هذا النوع من الجرائم الإلكترونية منظما واحترافيا.

ولا يقلق تطوير أدوات الذكاء الاصطناعي الجديدة مارتن كريمر بشكل كبير.

ويقول "يمكننا استخدام الذكاء الاصطناعي في الهجوم كما في الدفاع".

وتبقى الحماية الأساسية لمستخدم الإنترنت ضد عمليات الاحتيال هذه تظل، يقظته.