الخليج

اقتصاد, تقنية وسيارات

6 أبريل 2024  23:36 مساء

# قادرون على كشف التزييف العميق للصورة المولدة اصطناعياً 51%


يُعد التزييف العميق أحد مصادر التهديد بأدوات جديدة متطورة لتنفيذ الهجمات، والتي تتزايد مع تطور تقنيات الذكاء الاصطناعي، إذ يقلد البشر، ويتضمن كلاماً، أو صوراً، أو فيديو مولداً، يصعب تمييزه من الحقيقي. وبينما تستهلك هذه الهجمات وقتاً وجهداً أكبر من «مكافآتها» المحتملة، تحذّر «كاسبرسكي»، شركة الأبحاث المختصة بالأمن الإلكتروني، من وجوب إدراك الشركات والمستهلكين، لكون عمليات التزييف ستصبح مصدر قلق أكبر في المستقبل.

وكشفت أبحاث «كاسبرسكي» وجود أدوات وخدمات صنع التزييف العميق في أسواق الشبكة المظلمة، وتوفر هذه الخدمات مقاطع فيديو مصنوعة بالذكاء الاصطناعي التوليدي ومخصصة لمجموعة متنوعة من الأغراض، بما في ذلك الاحتيال والابتزاز، وسرقة البيانات السرية. كما تشير تقديرات خبراء الشركة إلى إمكانية شراء دقيقة واحدة من فيديوهات التزييف العميق، مقابل أقل من 300 دولار.

وهناك مخاوف حول الفجوة الكبيرة في المعرفة الرقمية بين مستخدمي الإنترنت. حيث أشار استطلاع رأي رقمنة الأعمال، الذي أجرته الشركة مؤخراً، إلى أن 51% من الموظفين الذين شملهم الاستطلاع في منطقة الشرق الأوسط

وتركيا وإفريقيا، قالوا إنهم يستطيعون التمييز بين الصورة المُولدة بتقنية التزييف العميق والصورة الحقيقية؛ لكن ولدى إجراء الاختبار حقاً، لم يتمكن سوى 25% منهم تمييز الصورة الحقيقية عن تلك المولدة بالذكاء الاصطناعي. ويعرّض ذلك المؤسسات للخطر، حيث غالباً ما يكون الموظفون هم الأهداف الأساسية للتصيد الاحتيالي، وهجمات الهندسة الاجتماعية الأخرى.

ويمكن للمجرمين السيبرانيين إنشاء مقطع فيديو مزيف لرئيس تنفيذي يطلب تحويلاً مصرفياً، أو يمنح الإذن لعملية دفع، ما يسمح لهم بسرقة أموال الشركة. كما يمكنهم توليد مقاطع فيديو، أو صور مزيفة للأفراد واستخدامها لابتزازهم مقابل المال، أو المعلومات.

وقال فلاديسلاف توشكانوف، من «كاسبرسكي»: «على الرغم من عدم توافر التقنية اللازمة، لإنشاء التزييف العميق عالي الجودة على نطاق واسع حتى الآن، سيكون توليد أصوات لانتحال شخصية أكثر الاستخدامات الممكنة للتقنية».

وللحماية من التهديدات المختلفة التي يشكلها التزييف، توصي الشركة الأشخاص والشركات باتخاذ الإجراءات التالية:

1. انتبه للمكالمات المشبوهة:
2. انتبه إلى الميزات الأوضح لفيديوهات التزييف:
3. لا تتخذ قرارات بناءً على المشاعر أبداً، ولا تشارك التفاصيل مع أي شخص:
4. تحقق من ممارسات الأمن السيبراني للمؤسسة وقم بتحديثها.