بمساعدة الذكاء الاصطناعي... محتالون يخدعون محاسب مالي و يسرقون "25" مليون دولار

افادت وسائل إعلام صينية بأن "محتالين تمكنوا من خداع محاسب مالي في إحدى الشركات وسرقة مبلغ 25 مليون دولار باستخدام تقنية التزييف العميق".

وذكرت وسائل الإعلام أن "المحتلين استخدموا الذكاء الاصطناعي التوليدي مع موظف مالي في مدينة هونغ كونغ، الواقعة على ساحل الصين الجنوبي، حيث تنكروا بهيئة زملاء الموظف، عبر مكالمة فيديو".

والتزييف العميق هو مقطع فيديو أو صوت أو صورة لشخص حقيقي تم تعديله والتلاعب به رقمياً، غالباً من خلال الذكاء الاصطناعي، للاحتيال بشكل مقنع.

وفي التفاصيل، حضر الموظف المالي مكالمة الفيديو مع أشخاص يُعتقد أنهم المدير المالي للشركة وموظفون آخرون، الذين طلبوا منه إجراء تحويل أموال، في حين كان بقية الحاضرين في الاجتماع عبارة عن تزييف عميق تمت إعادة إنشائهم رقمياً.

وأكدت شركة "أروب" استخدام "أصوات وصور مزيفة" في الحادث، مضيفةً أن: "عدد وتعقيد هذه الهجمات ارتفع بشكل حاد في الأشهر الأخيرة".

وأكدت شركة الهندسة البريطانية "Arup" لشبكة "CNBC" الإخبارية أنها "الشركة المسؤولة عن القضية، لكنها لم تُدلِ بتفاصيل؛ بسبب استمرار التحقيق في القضية"؟

وقال كبير مسؤولي المعلومات والأمن في شركة "Netskope" للأمن السيبراني، ديفيد فيرمان، إن: "مثل هذه التهديدات تزايدت نتيجة تعميم "ChatGPT" من "AI Open"، الذي تم إطلاقه في عام 2022".

وأضاف: "إن إمكانية الوصول العام إلى هذه الخدمات خفضت حاجز الدخول أمام مجرمي الإنترنت، ولم يعودوا بحاجة إلى مهارات تكنولوجية خاصة"، مبيناً أن حجم وتعقيد عمليات الاحتيال اتسع مع استمرار تطور تكنولوجيا الذكاء الاصطناعي".

وأشار فيرمان إلى أنه "بسبب مخاطر الاحتيال الرقمي، بدأ بعض المديرين التنفيذيين في محو وجودهم على الإنترنت، أو الحد منه؛ خوفا من أن يستخدمه مجرمو الإنترنت كمادة خام للتزييف العميق".

ويمكن استخدام العديد من خدمات الذكاء الاصطناعي التوليدية لإنشاء محتوى نصي وصوري وفيديو يشبه الإنسان، إذ يمكن أن تكون بمثابة أدوات قوية للجهات الفاعلة غير المشروعة التي تحاول التلاعب رقمياً.

وتحدثت وسائل الإعلام الحكومية الصينية عن حالة مماثلة في مقاطعة شانشي وقعت خلال العام الحالي، تتعلق بموظفة مالية، تم خداعها لتحويل "1.86" مليون يوان؛ ما يُعادل "262" ألف دولار، إلى حساب محتال بعد مكالمة فيديو مع رئيسها في العمل.