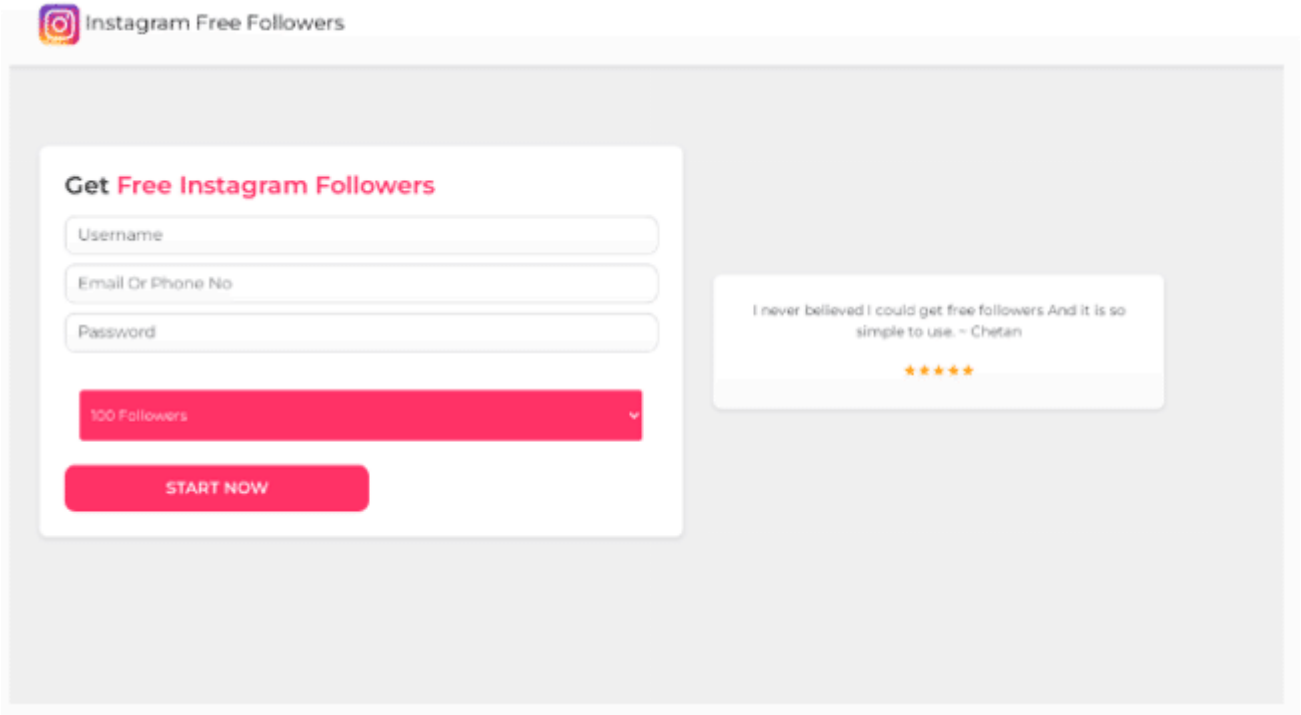
تحذير من تصاعد عمليات الاحتيال السيبراني عبر منصات التواصل الاجتماعي

4 يوليو، 2025



في يوم 30 يونيو من كل عام، يحتفل العالم باليوم العالمي لمنصات التواصل الاجتماعي؛ تلك المساحات التي أصبحت جزءًا لا يتجزأ من الحياة اليومية، لكنها في الوقت ذاته أصبحت ميدانًا واسعًا لعمليات احتيال رقمية تتطور باستمرار. ومع انتشار هذه المنصات مثل واتساب وفيسبوك وإنستجرام وإكس وتيليجرام وتيك توك، بدأ المحتالون في استغلال شعبيتها لتنفيذ هجمات سيبرانية تستهدف سرقة البيانات الشخصية والسيطرة على الحسابات.

في السنوات الأخيرة، شهد العالم تزايدًا ملحوظًا في استخدام أساليب الهندسة الاجتماعية والتصيد الاحتيالي. ينشئ المهاجمون صفحات إلكترونية مزيفة تحاكي الواجهات الرسمية لتطبيقات التواصل الاجتماعي، ويوهمون المستخدمين بعروض مغرية مثل توثيق الحسابات أو الحصول على متابعين مجانًا أو الاستفادة من خدمات حصرية. خلف هذه الوعود الكاذبة، يقف هدف واحد: اختراق الحسابات وسرقة بيانات الدخول.

ومن أبرز الحيل التي انتشرت مؤخرًا ما يُعرف بصفحات التوثيق المزيفة. يقاد المستخدمون عبر روابط وهمية إلى مواقع تشبه منصات مشهورة مثل واتساب، ويُطلب منهم إدخال رقم الهاتف ورمز التحقق الذي يصلهم برسالة نصية قصيرة. بمجرد تسليم هذه البيانات، تصبح الحسابات تحت سيطرة المهاجمين الذين قد يستخدمونها لانتحال هوية الضحية أو إرسال رسائل احتيالية أو حتى الاطلاع على بيانات خاصة.

في ممارسات أخرى، يلجأ المحتالون إلى استغلال رغبة المستخدمين في زيادة عدد متابعيهم على منصات مثل إنستجرام. يعدونهم بخدمات مجانية لرفع أعداد المتابعين مقابل تزويدهم بمعلومات الحساب، والتي يتم الاستيلاء عليها لاحقًا لاستخدامها في هجمات جديدة أو بيعها في الأسواق السوداء.

حتى تيك توك لم يسلم من هذه الهجمات، حيث استغل المهاجمون خاصية "المتجر" لإنشاء صفحات مزيفة تروج لمنتجات وهمية، مستهدفين بذلك البائعين الذين يتم خداعهم لسرقة بياناتهم.

الأمر لم يتوقف عند هذا الحد، بل أصبح المهاجمون يرسلون إشعارات أمنية مزيفة يدّعون فيها أنهم من فرق الحماية الرسمية لفيسبوك أو غيره من التطبيقات. تدفع هذه الرسائل الضحايا إلى الدخول على صفحات احتيالية لإعادة إدخال بياناتهم، مما يفتح الباب أمام فقدان الحسابات واستخدامها لاحقًا في عمليات ابتزاز أو نشر محتوى ضار.

ما يجعل هذه التهديدات أكثر خطورة أن الكثير من المستخدمين يقعون في الفخ نتيجة غياب الوعي الرقمي أو ضعف ممارسات الحماية. إلا أن الخبراء يؤكدون أن هناك خطوات بسيطة لكنها فعالة يمكنها تقليل احتمالية التعرض لمثل هذه المخاطر. من بين هذه الخطوات: توخي الحذر من الروابط المشبوهة، والحرص على عدم مشاركة معلومات شخصية قد تُستغل في الاختراق، واستخدام كلمات مرور قوية ومتنوعة لكل منصة، مع تفعيل المصادقة الثنائية.

كما ينصح بمراجعة إعدادات الخصوصية بانتظام، للتأكد من من يمكنه الوصول إلى الحسابات والبيانات الشخصية، إضافة إلى إلغاء أذونات التطبيقات غير المستخدمة. وتبقى الاستعانة ببرامج الحماية الموثوقة خطوة مهمة لتأمين الحسابات من محاولات التصيد أو اختراق البيانات.

في النهاية، يبدو أن العالم الرقمي يفرض على المستخدمين مسؤولية جديدة: أن يكونوا أكثر وعيًا وأكثر حرصًا في كيفية التعامل مع

منصات التواصل الاجتماعي التي باتت، كما هي نافذة للتواصل، بابًا واسعًا للتهديدات إذا أُسيء استخدامها.