احتيال جديد يستهدف مستخدمي آيفون بهذه الطريقة

نخيل نيوز ـ متابعة

رغم أن تقنيات الذكاء الاصطناعي جعلت عمليات الاحتيال الإلكتروني أكثر تطوراً من خلال التزييف العميق واستنساخ الأصوات وإنشاء رسائل مزيفة يصعب تمييزها، فإن بعض أساليب الخداع التقليدية لا تزال تحصد ضحايا جدد.

وبعد سنوات من انتحال المحتالين صفة موظفي الدعم الفني لشركة مايكروسوفت، يبدو أن مستخدمي "أبل" أصبحوا الهدف المفضل الجديد.

وتشير تقارير حديثة إلى تزايد انتشار رسائل احتيالية تحمل اسم "□□□□□ □□□□ □□□□□"، تزعم أن جهاز آيفون أو حساب "آي كلود" أو معرف □□ □□□□□ تعرض للاختراق أو نشاط مشبوه.

ويعتمد المحتالون على إثارة الذعر لدى المستخدمين ودفعهم إلى اتخاذ قرارات سريعة قبل التحقق من صحة التحذيرات، بحسب تقرير نشره موقع "□□□□□□□□□□□□□□".

تظهر هذه التنبيهات المزيفة بعدة أشكال، منها النوافذ المنبثقة داخل المتصفح، والرسائل النصية، ورسائل البريد الإلكتروني، وحتى المكالمات الهاتفية التي يدّعي أصحابها أنهم من فريق دعم "أبل".

وغالباً ما تتضمن الرسائل تحذيرات من عمليات شراء غير مصرح بها أو محاولات تسجيل دخول مشبوهة أو إيقاف الحساب بسبب خرق أمني مزعوم.

بعد ذلك يُطلب من الضحية الضغط على رابط معين أو الاتصال برقم هاتف أو تنزيل برنامج لحماية الجهاز.

وبمجرد الاستجابة، يحاول المحتالون الحصول على كلمات مرور □□ □□□□□ أو رموز التحقق الثنائية أو بيانات البطاقات المصرفية وبطاقات الائتمان.

وفي بعض الحالات الأكثر خطورة، يتم إقناع الضحية بتثبيت برامج تتيح الوصول عن بُعد إلى الجهاز، ما يمنح المهاجمين سيطرة شبه كاملة على الهاتف أو الحاسوب.

تكمن خطورة هذه الهجمات في أن حسابات "أبل" تحتوي على كم هائل من البيانات الشخصية، بما في ذلك الصور وجهات الاتصال وبيانات الدفع وكلمات المرور والنسخ الاحتياطية للأجهزة.

لذلك فإن تلقي رسالة تدّعي فقدان الوصول إلى الحساب قد يدفع الكثير من المستخدمين إلى التصرف بدافع الخوف.

كما يعتمد المحتالون أحياناً على بطاقات الهدايا كوسيلة لتحصيل الأموال، نظراً لصعوبة تتبعها أو استرداد قيمتها بعد

استخدامها.

وكانت شركة □□□□□ قد أعلنت مؤخراً وقف بيع بطاقات هدايا □□□□□ المادية في بعض الأسواق بعد استغلالها بشكل متكرر في عمليات الاحتيال، وهو الأسلوب نفسه الذي قد يُستخدم في عمليات الاحتيال المرتبطة بعلامة "أبل".

كيف تحمي نفسك؟

تؤكد "أبل" أن على المستخدمين توخي الحذر من أي رسالة أو مكالمة أو نافذة منبثقة غير متوقعة تدّعي وجود مشكلة عاجلة في الحساب.

كما تشدد الشركة على أنها لا تطلب من المستخدمين مشاركة كلمات المرور أو رموز التحقق أو أرقام بطاقات الهدايا لمعالجة المشكلات الأمنية.

وينصح الخبراء بعدم الضغط على الروابط أو الاتصال بالأرقام الواردة في الرسائل غير المتوقعة.

وبدلاً من ذلك، يجب التحقق من حالة الحساب مباشرة عبر إعدادات الجهاز أو من خلال الموقع الرسمي لشركة أبل.

ومع استمرار تطور أساليب الاحتيال الإلكتروني، تبقى القاعدة الأهم هي عدم التفاعل مع أي رسالة تثير الذعر أو تطلب معلومات حساسة بشكل عاجل، قبل التأكد من مصدرها الحقيقي.