الخليج

أخبار الدار, حوادث وقضايا

6 أبريل 2026 00:28 صباحا

من الهجمات السيبرانية تبدأ برسائل تصيّد إلكتروني % 75

حذر مجلس الأمن السيبراني لحكومة دولة الإمارات من المخاطر السيبرانية المرتبطة بالاحتيال عبر البريد الإلكتروني، مؤكداً أهمية توخي الحيطة من الرسائل الإلكترونية الخادعة أو المزيفة التي يستخدمها المحتالون لاختراق الحسابات الإلكترونية بما في ذلك الحسابات الشخصية وسرقة البيانات المالية، الأمر الذي قد يعرّض الأفراد والمؤسسات لمخاطر الاختراق وسرقة البيانات.

وأوضح المجلس لوكالة أنباء الإمارات «وام»، أن أكثر من 75% من حالات الاختراق الإلكتروني تبدأ برسائل تصيد عبر البريد الإلكتروني أو رسائل مزيفة قد تحتوي على برمجيات خبيثة أو تهدف إلى سرقة بيانات الدخول أو تمهد لعمليات انتحال الشخصية محذراً من خطورة هذه الرسائل وتداعياتها، مشيراً إلى انتشار هذا النوع من الاحتيال الذي يعتمد على استغلال نقص الوعي والسلوكيات الرقمية السليمة لدى بعض المستخدمين.

وأشار المجلس إلى أن أكثر من 3.4 مليار رسالة تصيد يتم إرسالها يومياً لاستهداف أعداد كبيرة من الأفراد على مستوى العالم بهدف سرقة معلوماتهم وبياناتهم الشخصية والمالية، إضافة إلى المعلومات الحساسة والتي قد تُستخدم لاحقاً في تنفيذ هجمات سيبرانية أو عمليات ابتزاز وطلب فدية.

وأكد المجلس ضرورة التركيز على حماية البيانات الشخصية، لافتاً إلى وجود عدد من العلامات التي يمكن من خلالها اكتشاف رسائل التصيد ومن أبرزها الرسائل التي تتضمن طلبات بدفع مبالغ مالية مقدماً، أو تلك التي تمارس ضغطاً على المتلقي لاتخاذ إجراء سريع دون تفكير، أو التي تطلب بيانات شخصية دون مبرر واضح، وكذلك الرسائل التي تقدم عروضاً مغرية بشكل مبالغ فيه يثير الشك.

وأوضح المجلس أن الرسائل التي تحتوي على أخطاء كتابية ولغوية تعد من العلامات الشائعة على رسائل التصيد التي قد تُستخدم لاختراق حسابات الأفراد وسرقة بياناتهم.

ونصح المجلس المواطنين والمقيمين باتباع مجموعة من الإرشادات لحماية أنفسهم من الرسائل الاحتيالية من بينها تجنب النقر على الروابط المشبوهة أو غير المعروفة، وعدم مسح رموز الاستجابة السريعة في الأماكن العامة أو غير الموثوقة.

وشدد المجلس على ضرورة تأمين الحسابات الشخصية سواء البريد الإلكتروني أو حسابات وسائل التواصل الاجتماعي والتي قد تحتوي على معلومات مهمة من خلال تفعيل خاصية المصادقة متعددة العوامل والحرص على تحديث الأنظمة والتطبيقات بشكل دوري.