

الأمن السيبراني» يحذر من التسول الإلكتروني وجمع التبرعات الاحتيالية» عبر الإنترنت

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



أبوظبي/ وام

دعا مجلس الأمن السيبراني لحكومة الإمارات أفراد المجتمع إلى أخذ الحيطة والحذر من التسول الإلكتروني وحملات جمع التبرعات الاحتيالية عبر الإنترنت ومواقع التواصل الاجتماعي خاصة خلال شهر رمضان الفضيل. وأكد مجلس الأمن السيبراني أهمية التوعية السيبرانية حول الأعمال الخيرية كالمساعدات والتبرعات والصدقات والزكاة وذلك بهدف حفظ أموال المتبرعين وتسهيل توصيلها لمستحقيها بالطرق الآمنة والموثوقة. وأوضح مجلس الأمن السيبراني أنه لضمان وصول التبرعات لمستحقيها وحماية أموال المتبرعين تجنب الاستجابة لطلبات التبرع التي ترد إليك عبر منصات التواصل الاجتماعي إضافة إلى التبرع فقط من خلال الجهات المختصة والمرخصة لها من الجهات المعنية في الدولة، فضلاً عن عدم مشاركة أرقام البطاقة الائتمانية أو البنكية مع أي جهة عبر الإنترنت إلا بعد التأكد من شرعيتها ومصداقيتها. وقال مجلس الأمن السيبراني إنه مع ازدياد مخاطر الهجمات السيبرانية خاصة هجمات التصيد الاحتيالي بات تعزيز

الوعي السيبراني أمراً مهماً لجميع أفراد المجتمع لحماية أنفسهم من مخاطر هجمات التصيد الإلكتروني المحتملة ومعرفة وكيفية تجنب الوقوع ضحية لها.



وحدد المجلس 5 نصائح لتفادي رسائل التصيد الاحتيالية وكيفية التعرف على هجمات التصيد الإلكتروني والتي من شأنها أن تعزز الأمن الرقمي لأفراد المجتمع وحماية معلوماتهم الشخصية من السرقة ومواجهة الأخطار السيبرانية. وتتضمن النصائح أهمية التحقق من قنوات التواصل الاجتماعي الرسمية للشركة أو الجهة المختصة والحذر من العروض المبالغ فيها، مثل الصفقات الخيالية أو الأسعار المستحيلة، والانتباه لعناصر العلامة التجارية، فالشعارات أو الصور غير الواضحة قد تشير إلى عملية احتيالية، والتأكد من أن البنوك لا ولن تطلب المعلومات الائتمانية والشخصية عبر البريد الإلكتروني أو الرسائل النصية، وأخيراً التأكد من هوية المتصلين قبل الرد على المكالمات حيث يشترط في الإمارات وجود معرف المتصل الخاص بالشركات.

وأشار مجلس الأمن السيبراني إلى أنه مع التقدم التكنولوجي المتسارع وانتشار استخدام البريد الإلكتروني في مختلف جوانب الحياة اليومية تتزايد المخاوف من مخاطر الرسائل الاحتيالية التي تستهدف سرقة البيانات الحساسة. لذا من الضروري إدراك هذه المخاطر وفهمها جيداً من أجل الحماية الشخصية والوقوع ضحية للاحتيال الإلكتروني. واستعرض المجلس سيناريو لرسائل التصيد الاحتيالي الإلكتروني التي يصل عددها إلى 3.4 مليار رسالة بريد غير مرغوب بها تُرسل يومياً على مستوى العالم، موضحاً أن رسائل التصيد قد تظهر للضحية محتالين يدعون أنهم شركة شحن مع طلب تحديث العنوان لتسليم الطرد وتحمل علامة «حدث الآن» إضافة إلى طلب إعادة تفعيل الحساب على منصات التواصل الاجتماعي قبل إيقافه وتحمل علامة «أعد التفعيل الآن» إضافة إلى طلب تأكيد بيانات الحساب البنكي بشكل عاجل لاستكمال الخدمة وتحمل علامة «أدخل بياناتك»، فضلاً عن طلب المعلومات الشخصية ورقم البطاقة البنكية وتحمل علامة «إرسال» والتي من شأنها أن تسهم في تسهيل اختراق الحساب الشخصي والوقوع ضحية للاحتيال الإلكتروني.

وحدد مجلس الأمن السيبراني مجموعة من العوامل لكيفية كشف رسائل التصيد الاحتيالي وهي كالتالي «ضرورة تفحص عنوان البريد الإلكتروني للمرسل بعناية إضافة إلى التواصل مباشرة مع الشركات عبر وسائل اتصال موثوقة». «والحذر من الرسائل المُلحة وتجنب الضغط على الروابط المشبوهة