الخليج

اقتصاد, تقنية وسيارات

25 يونيو 2024 14:21 مساء

إجراءات لسلامة مشاركة البيانات 4

حدد مجلس الأمن السيبراني لحكومة الإمارات، 4 إجراءات لسهولة وسلامة مشاركة البيانات وتأمينها عبر وسائط المصابة ببرمجيات خبيثة USB لتفادي أي هجمات سيبرانية بواسطة أقراص USB التخزين المحمولة.

وأوضح أن إجراءات تأمين وسائط التخزين المحمولة هي: «تعزيز كلمات المرور من خلال استخدام كلمات مرور قوية لنظام Bitlocker لحماية المعلومات المخزنة فيها، وتشفير البيانات عبر استخدام أدوات التشفير المدمجة مثل لحماية الملفات الخاصة، والاحتفاظ بنسخ احتياطية بشكل منتظم، وحفظ Mac لنظام Filevault أو windows وسائط التخزين عند عدم استخدامها وتخزينها في مكان آمن لمنع الوصول غير المصرح به أو السرقة».

ودعا المجلس الأفراد إلى الحرص على تشفير البيانات على أجهزة وسائط التخزين المحمولة، وفحص الملفات بواسطة برامج مكافحة الفيروسات قبل الاستخدام، وحذف البيانات الحساسة بعد عملية النقل، وتعطيل وظائف التشغيل التلقائي والآلي.

وأكد أهمية تجنب استخدام وسائط التخزين المحمولة مجهولة المصدر، وتجنب ترك وسائط التخزين المحمولة دون مراقبة، وتجنب أيضاً تخزين البيانات الحساسة دون تشفير، بالإضافة إلى تجنب استخدام وسائط التخزين المحمولة التي تجدها في الأماكن العامة.

وأشار المجلس إلى أن هناك دراسة حديثة كشفت عن حملة هجمات إلكترونية عالمية استهدفت منظمات في القطاعين العام والخاص، حيث استغل المجرمون الإلكترونيون أقراصًا محمولة USB ملوثة لشن هذه الهجمات.

وأضاف أن باحثون أبلغوا عن حملة استهدفت منظمات على مستوى العالم حيث استخدم المجرمون السيبرانيون مصابة ببرمجيات خبيثة، مشدداً على أن هذا التهديد يؤكد على أهمية أمن USB سلسلة هجمات بدأت بواسطة أقراص وسائط التخزين المحمولة من أجل حماية معلومات الشركة والعملاء من التسريب أو الوصول الغير مصرح إليها، وحماية وسائط التخزين المحملة من السرقة أو الفقدان، وتجنب الآثار القانونية أو المالية.