

منها قاعدة 1-2-3.. نصائح الخبراء لنسخ ونقل بياناتك المهمة بسهولة وبشكل منتظم



السبت 25 يوليو 2020 04:07 م

كتب: -الجزيرة

يتعين على المستخدم إجراء عمليات النسخ الاحتياطي للبيانات المهمة بصورة منتظمة للحفاظ عليها من فقدان أو التعرض لهجمات التشفير وطلب الفدية، وهناك عدة تقنيات وقواعد يمكن للمستخدمين اتباعها لتأمين نسخ بياناتهم

قاعدة "1-2-3"

وينصح يان شوسلر، من مجلة التكنولوجيا سي تي (c't) -وفقا لوكالة الأنباء الألمانية- باتباع قاعدة "1-2-3"، التي تنص على أنه يتعين على المستخدم إنشاء ثلاث نسخ احتياطية من الملفات المهمة بما في ذلك الملفات الأصلية، وأن يتم تخزين بيانات النسخ الاحتياطية على اثنين من وسائط التخزين المختلفة على الأقل، مثل الأقراص الصلبة الخارجية وخدمات التخزين السحابية

وعلى يان شوسلر سبب ذلك قائلا "عند وجود اثنين من الأقراص الصلبة المتطابقة، فإنه كثيرا ما تحدث أعطال القرصين معا". ومن الأفضل أن يتم تخزين إحدى نسخ البيانات خارج المنزل أو المكتب لحماية البيانات من فقدان التام في حالة نشوب حريق أو تعرض المنزل أو المكتب للسرقة

نوعية وسيط التخزين

وترتبط نوعية وسيط التخزين، سواء كان خدمات التخزين السحابية أو الأقراص الصلبة أو وحدات الذاكرة الفلاشية يو أس بي (USB)، بما يرغب المستخدم في نسخه احتياطيا

وأضاف الخبير الألماني "إذا رغب المستخدم في حفظ بعض المستندات أو الصور فقط، فإن خدمات التخزين السحابية أو وحدات الذاكرة الفلاشية تعتبر الخيار المناسب".

ومن جانبه أضاف راينر شولت، من مجلة "كمبيوتر بيلد" الألمانية، أنه في حالة وجود عدد معين من الملفات، فإنه يمكن تنزيل هذه الملفات على الحاسوب أو الهاتف الذكي الجديد لاحقا من الذاكرة السحابية، ومن الأفضل الاعتماد على هذه الذاكرة أيضا عند الرغبة في نقل جهات الاتصال والعلامات المرجعية لمتصفح الإنترنت

مزايا التخزين السحابي

ومن ضمن مزايا خدمات التخزين السحابية عدم القلق بشأن أمان البيانات واستقرارها، على عكس الحالة التي يتم فيها تخزين بيانات النسخ الاحتياطي على الأقراص الصلبة، والتي قد تتعرض للفقدان أو التلف

ويتعين على المستخدم البحث عن الجهات الموثوقة فيها لتقديم خدمات التخزين السحابية ومن الأفضل الاعتماد على وظيفة التشفير من النهاية إلى النهاية لجميع البيانات، التي يتم رفعها على خدمات الذاكرة السحابية نظرا لأن مفتاح التشفير يكون بيد المستخدم فقط

برامج أنظمة التشغيل

وعند الرغبة في إجراء عمليات النسخ الاحتياطي لجميع البرامج والبيانات المخزنة على الحاسوب، ينصح الخبير الألماني راينر شولت بالاعتماد على برامج النسخ الاحتياطي الخاصة بنظام تشغيل ويندوز أو أجهزة الماك مثل برنامج تايم ماشين (Timemachine)، حتى يتم نقل جميع بيانات الحاسوب بالكامل على الجهاز الجديد

وينصح راينر شولت باستعمال برنامج النسخ الاحتياطي دبلكاتي (Duplicati) للحواسيب المزودة بنظام مايكروسوفت ويندوز، وأشار يان شوسلر إلى أن الإعدادات الافتراضية المضبوطة مسبقاً لا تتضمن تشفير بيانات النسخ الاحتياطي، وهنا يتعين على المستخدم تفعيل خيار تشفير كلمة المرور

وهناك العديد من البرامج الأخرى لإجراء عمليات النسخ الاحتياطي، حتى إن نظام تشغيل مايكروسوفت ويندوز نفسه يتضمن وظيفة النسخ الاحتياطي، إلا أن يان شوسلر ينصح بعدم استعمال هذه الوظيفة لأنه لم يجر تطويرها منذ إصدار ويندوز 7.

وبشكل عام ينصح يان شوسلر المستخدم بضرورة التحقق من ملفات النسخ الاحتياطي من وقت إلى آخر، والتحقق من أنها تعمل، وأنه يمكن استدعاء البيانات، وفي حالة توافر حاسوب آخر، فإنه يمكن استعمال للاختبار

وأوضح راينر شولت أنه يجب توافر كود التسجيل عند الرغبة في نقل البرامج المدفوعة، وعادة ما يكون كود التسجيل مرتبطاً بالحاسوب المثبت عليه البرنامج، ولذلك يتعين على المستخدم إلغاء ارتباط البرنامج بالحاسوب قبل أن يتم تثبيت البرنامج على حاسوب جديد والتسجيل مرة أخرى بواسطة كود التسجيل

رسائل البريد الإلكتروني

وأضاف راينر شولت أنه يمكن إجراء عمليات النسخ الاحتياطي لرسائل البريد الإلكتروني بسهولة، لأنه عادة ما يتم إرسال رسائل البريد الإلكتروني واستقبالها عن طريق بروتوكول آي ماب (IMAP)، الذي يتم معه تخزين النسخ الأصلية على سيرفر الشركة المقدمة للخدمة، وعند إعداد حساب البريد الإلكتروني على الحاسوب الجديد فستتم مزامنة جميع الرسائل والمجلدات تلقائياً على السيرفر وسيتم الاحتفاظ بكل البيانات

وتعد حسابات البريد الإلكتروني، التي تعتمد على بروتوكول بوب 3 (POP3) غير عملية، حيث يتم نقل الرسائل من السيرفر إلى الحاسوب، وبالتالي لا يتوافر منها نسخة على السيرفر، ولذلك يتعين على أصحاب حسابات البريد الإلكتروني أرشفة الرسائل الإلكترونية على قرص صلب خارجي، ثم استيراد الرسائل مرة أخرى على الحاسوب الجديد