

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

في هذا العدد..

- النسخ الاحتياطي: ماهو - متى وكيف
- الإستعادة
- تبييات هامة

OUCH!

النسخ الاحتياطي و الإستعادة

مقدمة

اذا كنت تستخدم جهاز حاسوب او هاتف محمول، عاجلاً ام آجلاً سوف يحدث خطأ يتسبب في فقدان ملفاتك الشخصية او مستنداتك او صورك. على سبيل المثال من الممكن ان تحذف ملف عن طريق الخطأ او يحدث فشل في نظام التشغيل أو تفقد جهازك الخاص او من الممكن اصابته بملفات ضارة مثل برمجيات طلب الفدية Ransomware. في مثل هذه الحالات يكون النسخ الاحتياطي هو الطريقة الوحيدة لاسترجاع ملفاتك و«حياتك» الرقمية. في هذه

النشرة سوف نوضح ماهو النسخ الاحتياطي وكيفيه عمل نسخ احتياطي للملفات الخاصة بك وكيف نضع استراتيجية بسيطة لذلك.

المحرر الضيف

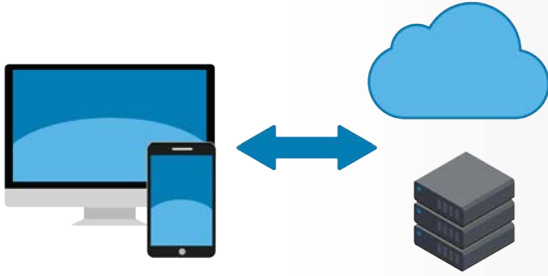
كيث بالمجرين يعمل في مجال أمن المعلومات منذ أكثر من 30 عاماً. مدرس مرخص من سانز SANS لمقرر SEC 301 مقدمة في أمن المعلومات، كيث يعمل أيضاً في مجال استشارات أمن المعلومات، تابعه علي تويتر [@kpalmgren](https://twitter.com/kpalmgren)

النسخ الاحتياطي .. ماهو ؟ متى ؟ وكيف؟

النسخ الاحتياطي هو نسخ المعلومات المخزنة على أحد الاجهزة (الكمبيوتر او الجوال مثلاً) في مكان آخر. الهدف من ذلك الرجوع الى تلك النسخ في حال حدث فقد لبعض تلك المعلومات. للأسف الكثير من الناس يفشلون في عمل نسخ احتياطية منتظمة على الرغم من انها عملية بسيطة وغير مكلفة. هناك عدة خيارات عليك تحديدها لتقوم بعملية النسخ الإحتياطي نسردها فيما يلي. الخيار الأول هو تحديد ما تريد نسخه : 1 - نسخ بعض البيانات التي تحدها وعمل نسخة احتياطية لها فقط. 2 - نسخ جميع محتويات الجهاز بما في ذلك نظام التشغيل والبرامج المثبتة على الجهاز. اغلب حلول النسخ الاحتياطي يتم تكوينها بشكل افتراضي لاستخدام النهج الاول حيث انها تقوم بعمل نسخ احتياطي للمعلومات الموجودة بالملفات الاكثر استخداماً، وفي الكثير من الاحيان هذا كل ماتحتاجه. ولكن اذا كنت غير متأكد من عملية النسخ الاحتياطي وتريد ان تكون اكثر حذراً بإمكانك عمل نسخ احتياطي لكل شيء.

الخيار الثاني هو تحديد مدى تكرار عملية النسخ الاحتياطي لمعلوماتك . توجد برامج عديدة للنسخ الاحتياطي مخصصة للحواسيب الشخصية مثل: Apple's Time Machine or Microsoft Window's Backup and Restore. هذه البرامج تتيح لك انشاء جدول للنسخ الاحتياطي يتضمن خيارات النسخ مثل كل ساعة او بشكل يومي او اسبوعي. هناك حلول اخرى توفر لك حماية دائمة عن طريق عمل نسخ من الملف في كل مرة تقوم بالتعديل عليه وحفظه. نحن نوصي بعمل نسخ احتياطي يومي على الاقل.

النسخ الاحتياطي و الإستعادة



التخزين الاحتياطي المؤتمت والموثوق هو خط الدفاع الأخير للحفاظ على بياناتك.

الخيار الثالث هو تحديد مكان تخزين النسخ الاحتياطي : اجهزة تخزين البيانات التقليدية او التخزين السحابي .ولكلٍ منهما مميزاته وعيوبه ..اذا كنت مختاراً أي منهما أفضل بالنسبة لك فيمكن التخزين بكلا الطريقتين في نفس الوقت. الوسائط المادية عبارة عن اجهزة يمكنك التحكم بها مثل أجهزة USB المحمولة . من مميزات هذه الطريقة انها تسمح لك بنسخ واسترجاع كم كبير من البيانات بسرعة كبيرة ايضا .اما عيوبها هو انه اذا اصاب الجهاز باحد البرامج الضارة من الممكن ان تنتقل العدوى لملفات النسخ الاحتياطي اذا تم توصيل جهاز التخزين بالجهاز.ايضا عند تعرض الجهاز للتلف (بحريق او غرق مثلاً) او للسرقة فانك ستفقد الجهاز ووحدات التخزين القريبة منه والتي قد تحتوي النسخ الاحتياطي. لذلك ننصح باستخدام جهاز تخزين خارجي لحفظ النسخ الاحتياطي والاحتفاظ به في مكان آمن و بعيداً عن الجهاز.

التخزين السحابي هي خدمة تقدمها عدة جهات على الانترنت من خلال تطبيقات معينة يمكنك من تخزين نسخ احتياطي من ملفاتك

حسب جدول تحدده او بشكل آلي حين تقوم بتعديل الملفات. من مميزات استخدام التخزين السحابي ، سهولة إجراء النسخ الاحتياطي لانه يعمل بشكل تلقائي بالإضافة لسهولة الوصول الي ملفاتك من اي مكان عبر الانترنت. ايضا المعلومات المحفوظة عن طريق السحابة تكون في مأمن عن الحوادث المنزلية مثل الحريق والسرقة. من عيوب استخدام هذه الالية انها تحتاج لوقت طويل حيث يتم رفع جميع البيانات الى شبكة الانترنت. وايضاً هناك خطورة على خصوصية البيانات في حال تعرض مزود الخدمة للاختراق. لذا فعليك التأكد من أن مزود الخدمة يوفر ضوابط امنية قوية مثل تشفير البيانات والمصادقة.

بالنسبة لاجهزة الجوال الذكية والاجهزة اللوحية توفر الشركات المصنعة مثل google و Apple خدمة تخزين بيانات المستخدمين المسجلة على تلك الأجهزة على تخزين سحابي خاص بها. هذه الخدمة لا تقوم بتخزين كل ما يحتويه الجهاز فعليك التأكد من إعدادات هذه الخدمة أو استخدام تطبيقات إضافية لعمل نسخ احتياطي لجميع ما يحتويه الجهاز من بيانات. هذا الاجراء لا يساعدك فقط على استعادة هذه البيانات عند فقدانها ولكن يسهل عملية نقلها إلى جهاز آخر عند رغبتك باستبدال الجهاز الحالي.

الاستعادة

لا يعتبر النسخ الاحتياطي للبيانات ذا فائدة إن لم يتم التأكد من امكانية استعادة تلك البيانات. تحقق بشكل دوري من ان ملفات النسخ الاحتياطي تعمل بشكل صحيح بحيث يتم استعادة البيانات والتأكد من صحتها. ايضا تأكد من اجراء نسخ كامل للنظام عند اجراء اصلاح رئيسي مثل استبدال القرص الصلب أو تحديث للنظام وتحقق من امكانية إستعادة البيانات قبل البدء بالإصلاح.

النسخ الاحتياطي و الإستعادة

تنبهات هامة

- من الضروري اختبار النسخ الاحتياطية بشكل دوري للتأكد من أن عملية النسخ تتم بشكل صحيح.
- عند إعادة بناء النظام لجهاز معين من النسخ الاحتياطي، قد لا تكون آخر اعدادات النظام أو التحديثات ضمن ذلك النسخ. تأكد من تطبيق اخر التحديثات الامنية قبل استخدام الجهاز.
- يجب اطلاق جميع النسخ الاحتياطية التي لم تعد بحاجة اليها لمنع الوصول لها من قبل الآخرين.
- قبل استخدام التخزين السحابي الالكتروني عليك التأكد من سمعة مقدم الخدمة والتأكد من أن معايير أمن المعلومات التي يعتمدها تفي بمتطلباتك. على سبيل المثال هل يتم تشفير البيانات المخزنة على السحابة؟ من هم الاشخاص الذين يمكنهم الوصول للنسخ الاحتياطية؟ هل تتم المصادقة بشكل جيد وقوي (التحقق بخطوتين مثلاً)؟

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة

[.securingthehuman.sans.org/ouch/archives](https://securingthehuman.sans.org/ouch/archives)

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_aa.pdf

https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_aa.pdf

https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201611_aa.pdf

https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_aa.pdf

<https://securingthehuman.sans.org/ouch/2016#august2016>

عدد أوتش حول عبارات المُرور:

عدد أوتش حول التحقق باستخدام خطوتين:

عدد أوتش حول استخدام الحوسبة السحابية بأمان:

عدد أوتش حول التشفير:

عدد أوتش حول برمجيات طلب الفدية (باللغة الانجليزية):

أوتش! تنشر من قبل برنامج «سانس» لحماية الإنسان ويتم توزيعها بموجب الرخصة [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو استخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الإتصال على: ouch@securingthehuman.org

مجلس التحرير: والت سكرينغ، فيل هوفمان، كاتي كليك، شيريل كوني

ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman.org)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus