العادات الأمنية الجيدة

هناك بعض العادات البسيطة التي يمكن في حال تبنيها واستخدامها بانتظام ، ان تقلل بشكل كبير جدا من احتمالات خسارة المعلومات الموجودة على حاسوبك أو إفسادها.

كيف يمكن تقليص وصول الآخرين إلى معلوماتك؟

قد يكون في مقدورك بسهولة تحديد الأشخاص الذين يمكنهم بشكل مشروع أو غير مشروع ، الوصول المادي (الفيزيائي) إلى حاسوبك– ومن هؤلاء أعضاء الأسرة ورفقاء السكن وزملاء العمل وأعضاء فرق التنظيف وربما غيرهم. ولكن أكثر صعوبة من ذلك تحديد الأشخاص الذين يمكنهم الوصول من بعيد لحاسوبك. طالما أن حاسوبك موصول بشبكة الانترنت فإنك معرض لأن يقوم شخص ما أو شيء آخر بالوصول الى معلوماتك أو افسادها. ولكن بإمكانك اتباع عادات تجعل ذلك أمرا صعباً و منها:

- **أغلق حاسوبك في حال عدم استخدامه:** حتى لو كنت بعيدا عن حاسوبك لبضع دقائق فإنها كافية لشخص ما لتدمير أو إفساد معلوماتك أو إدخال شيفرة من شأنها الحاق الضرر. إن إغلاق حاسوبك من شأنه منع شخص آخر من الجلوس ببساطة على حاسوبك والوصول إلى معلوماتك.

- **افصل حاسوبك عن الشبكة في حال عدم استخدامه:** لقد مكن تطوير بعض التقنيات مثل (أجهزة البث الالكتروني المتصلة بالخطوط الالكترونية والهاتفية DSL and Cable Modems) المستخدمين من البقاء على الخط طوال الوقت، ولكن لهذه الراحة ثمنها. إن احتمال استهداف حاسوبك من قبل المهاجمين والفيروسات التي تجوب الشبكات للوصول الى حاسوب تهاجمه أصبح أكبر بكثير عندما يكون الحاسوب موصولا على الدوام. واعتمادا على الطريقة التي تستخدمها للربط بالشبكة فإن الفصل يعني إنهاء الاتصال وإغلاق الحاسوب أو الموديم modem (جهاز البث الالكتروني) أو فصل الاسلاك .
- **قيّم المواقع الأمنية:** معظم البرامج بما في ذلك محركات البحث Browsers وبرامج البريد الالكتروني التي تتيح وفرة من الإمكانيات التي تمكنك من تلبية احتياجاتك ومتطلباتك. وإن تفعيل تلك الإمكانيات لزيادة الراحة والأداء قد يجعلك أكثر عرضة للهجوم. من المهم فحص المواقع خاصة الأمنية واختيار ما يلبي حاجاتك دون أن يجعلك عرضة لمزيد من الهجوم. إذا أدخلت نسخة جديدة من البرامج أو إذا سمعت عن شيء ما يمكن أن يؤثر على مواقعك أعد تقييم مواقعك لتتأكد من أنها لا زالت مناسبة.

ما الخطوات الأخرى التي يمكنك اتخاذها؟

أحيانا لا تأتي التهديدات لمعلوماتك من أشخاص آخرين بل من أسباب طبيعية أو تكنولوجية. رغم أنه لا توجد طريقة للحماية أو الوقاية من هذه المشكلات إلا أنه يمكنك الاستعداد لها ومحاولة تقليص أخطارها.

- **احمي حاسوبك من تذبذب الطاقة الكهربائية.** إضافة إلى توفير فتحات لتوصيل حاسوبك وجميع ملحقاته. هناك شرائط (strips) كهربائية يمكن أن تحمي حاسوبك من تذبذبات الطاقة. ويُعلن اليوم عن الكثير من التعويض ان لم تقم هذه الشرائط بحماية حاسوبك بفعالية. خلال عاصفة رعدية أو أعمال بناء من النوع الذي قد يؤدي إلى تذبذبات في الطاقة فكر في إغلاق حاسوبك ونزع التوصيلات الكهربائية من جميع مصادر الطاقة. الشرائط وحدها لن تحمي كوميوترك من التذبذبات ولكن هناك منتجات أخرى توفر إمدادا للطاقة لا ينقطع عندما يحصل انقطاع أو تذبذب في الطاقة.
- **احتفظ بنسخ أخرى لمعلوماتك.** سواء اتخذت أو لم تتخذ خطوات لحماية نفسك فهناك دائما إمكانية أن يحدث شيء ما يدمر معلوماتك. ربما يكون قد مررت بتجربة على الأقل من هذا النوع– خسارة ملف او أكثر بسبب مشكلة مع الأجهزة أو بسبب فيروس أو بسبب البرامج الخبيثة "دودة" . ولذلك فإن التخزين المنتظم لبياناتك على القرص المدمج CD أو الشبكة يقلل من التوتر والعواقب السلبية الأخرى التي تنجم عن خسارة المعلومات المهمة. ويعود تقرير مدى الانتظام في حماية معلوماتك على هذا النحو إلى قرارك الشخصي. إذا كنت تضيف أو تغير المعلومات باستمرار فيمكن أن يكون الحفظ الأسبوعي للمعلومات أفضل بديل. وإذا كان المحتوى قلما يتغير فقد لا تقوم باستمرار بعملية الاحتفاظ بنسخ أخرى. لا تحتاج إلى دعم البرامج التي تمتلكها على اقراص تخزين البيانات CD-ROM او اقراص تخزين البيانات المصورة DVD-ROM، يمكنك إعادة إدخال البرنامج من مصدره الأصلي عند الضرورة.

تأليف : مندي مكدول، وآلن هاوس هولدر

المؤلفون : ميندي مكدويل ، الين هاوسهولدر

إنتاج جامعة كارنيجي ميلون سنة .2007 تمت إعادة إنتاجه بواسطة كيوسيرت مع أخذ الترخيص

المؤلفون : ميندي مكدويل ، الين هاوسهولدر

إنتاج جامعة كارنيجي ميلون سنة 2007. تمت إعادة إنتاجه بواسطة كيوسيرت مع أخذ الترخيص