إعداد: علاء عثمان
(خبير في تصميم المواقع)

لست في مأمن من الفيروسات

هناك بعض المفاهيم الخاطئة الشائعة بين مستخدمي الانترنت حول انتشار الفيروسات. وسأحاول من خلال هذه السطور توضيح بعضها مع ذكر أهم أساليب وأدوات حماية الحواسيب الشخصية من فيروسات الشبكة العالمية التي سنقتصر على ذكر أشهرها.

١ – هناك من يرى بما أنه لا يحتفظ بمعلومات مهمة في حاسوبه الشخصي لذلك لا يبالي بموضوع الأمن وحماية المعلومات!!."

منذ فترة ليست ببعيدة كان لهذه الفكرة شيء من الصحة. أما الآن فلا أساس لها حيث تلاحظ عزيزي القارئ وتسمع كل يوم عن الديدان والتهديدات المختلفة وعن فيروسات الحاسوب المنتشرة والمتجددة. التي نذكر منها: فيروس (Love Bug) الشهير. وفيروس (Nimda) وفيروس (Blaster).

وتنتشر هذه الفيروسات عبر شبكة الإنترنت، بشكل عشوائي دون تمييز، إلى آلاف بل إلى ملايين الحواسيب الشخصية في مختلف أنحاء العالم، خلال ساعات قليلة وبغض النظر عمن يملك الحاسوب، وماهية المعلومات المخزنة عليه، أو قيمتها.

فالهدف الأساسي لمثل هذه الاعتداءات غير المسؤولة هو إشاعة الفوضى. وحتى إن لم تتعرض للاعتداءات مباشرة فمن الممكن أن يُستعمل جهازك كوسيط للاعتداء على حواسيب أخرى من الشبكة، مما يسبب حجب الخدمة عنها أو إرسال الإعلانات المزعجة.

لذلك فمن مسؤولياتك المهنية والوطنية حماية حاسبك الشخصي حتى يسلم الآخرون.

٢– وهناك من يرى أنه سيتوقف عن استعمال الانترنت بغية حماية جهازه.

للأسف.. هذا غير صحيح أيضاً!!

وذلك لأنك عندما ولجت إلى شبكة الانترنت فإنك بطبيعة الحال كنت مستهدفاً، فمن الممكن أن يكون حاسوبك قد حُمل (دون معرفتك) أحد الفيروسات وقد لا ينشط إلا بعد عدة أيام عندما تقوم بقراءة بريدك الإلكتروني وأنت لست على اتصال بالشبكة (Off line). كما يمكن أن يصل الفيروس إلى جهازك من أحد ملفات الشبكة المحلية أو من قرص مرن (floppy disk) استعرته، أو من سواقة الذاكرة الوميضية (USB).

٣– وهناك من يرى أنه بعدم فتح ملحقات البريد الإلكتروني المشبوه فيها سيحمي جهازه من وبال الفيروسات.

مرة أخرى نقول إن هذا الكلام غير صحيح، فمن

الممكن أن يصاب جهازك بفيروس أتى من جهاز مديرك أو أعزّ أصدقائك في حال تعرض دفتر عناوين البريد الالكتروني الخاص بهم إلى اختراق من قبل أحد الفيروسات وبالتالي يتم إرسال الرسائل إليك باسم صديقك أو مديرك ويكون المحتوى عبارة عن نوع من أنواع الفيروسات..

فالفيروس المسمى نيمدا (Nimda) وبعض الديدان المشابهة له تستطيع الولوج عبر متصفح الانترنت Web Browser. ومن الممكن أن تنشط بعض أنواع الفيروسات، بكل بساطة، بقراءة الرسائل الالكترونية أو استعراضها. لذلك يجب أن يحوي جهازك برنامجا واحدا على الأقل مضادًا للفيروسات، وأن يكون هذا البرنامج قابلا للتحديث والتطوير باستمرار..

٤- وهناك من يرى أنه سيستعمل نظام التشغيل ماكنتوش أو نظام Linux، عوضا عن نظام Windows، لأن كلا النظامين غير مستهدفين بشكل عام!!!.."

والجواب: صحيح أن معظم الاعتداءات تستهدف الأجهزة التي تعتمد نظام التشغيل Windows، لكن عليك أن تعلم أن هناك اعتداءات تستهدف Mac Os و Linux تماما كما هو الحال بالنسبة لنظام Windows، ولكن بشكل أقل، ويتوقع بعض الخبراء أن مشكلة الفيروسات في Mac ستكون أسوأ ولن تكون هذه الأنظمة في معزل عن الهجمات، وذلك لأن نظام Mac Os X يستعمل شكلا من أشكال نظام Unix الأمر الذي يجعله عرضة للاعتداء على الرغم من الميزات الأمنية المفيدة التي يتمتع بها هذا النظام.

٥- كما أن هناك من يقول "إن الجهاز الذي استخدمه مزود ببرنامج حماية من الفيروسات، لذلك فأنا في مأمن من هجومها."

في الحقيقة هذا القول ليس دقيقاً تماماً، لأنه:

أولاً- إذا لم تنشّط الفحص الآلي في البرنامج المضاد للفيروسات لتفحص المراسلات والملفات الواردة فأنت غير محمي من هجوم فيروسات البريد الالكتروني ومتصفحات المواقع.

ثانيا- هناك أخطار وتهديدات جديدة تظهر يومياً، وبشكل دائم لذلك فإن مضاد الفيروسات الموجودة في حاسوبك، إذا لم يتم تحديثه، يصبح غير مؤهل للتصدي للأخطار الجديدة. لذلك عليك القيام بالتحديث التلقائي لهذا البرنامج ليكون على أتم استعداد لمواجهة آخر أنواع التهديدات.

ثالثاً- إن مضاد الفيروسات لا يمكنه وحده أن يؤمن لك الحماية من كل أنواع التهديدات، لذلك فأنت غالباً بحاجة إلى مجموعة من الحلول تشمل على الأقل: مضادًا للفيروسات وجدارً نارياً خاصاً بك مثل (Zone Labs, ZoneAlarm-Pro) وخطة من أجل الحفاظ على نظامك واستخدام التحديثات الأمنية التي تتوفر على مواقع الشركات والتي يمكنها أن تؤمن لك الحماية من الاختراقات المشؤومة.

كما ننصحك بمضاد التجسس وبرنامج لحجب الإعلانات غير المرغوب بها وإليك مثالٌ على ذلك: (Norton AntiSpam)

* ليس الغرض من ذكر برامج الكمبيوتر في المقال الإشهار بها أو بالشركات المنتجة لها.