

برامج مكافحة فيروسات الحاسوب

مهمة هذه البرامج

تختلف التفاصيل الدقيقة لمهام برامج مكافحة فيروسات الحاسوب باختلاف البرامج نفسها، فكل شركة منتجة لهذه البرمجيات تحاول أن تضيف مهاماً جديدة حتى تنجح عملية التسويق لها، و لكن بشكل عام فإن المهمة الأساسية لهذه البرامج هي اجراء فحوصات للملفات وذاكرة الحاسوب بحثاً عن أي تشابه مع أنماط معينة يمكن أن تدل على وجود لفيروسات الحاسوب، قد تكون هذه الأنماط عبارة عن مجموعة من التراكيب الثابتة أو التواقيع (Signatures) مُخزنة في قاعدة بيانات بصيغة معينة وقد تكون عبارة عن أنشطة معينة تُستخدم عادةً لأغراض مشبوهة، و حيث أن مبرمجي فيروسات الحاسوب يعملون باستمرار على انتاج فيروسات جديدة و بأساليب برمجية مختلفة، لذلك فمن الضروري أن يتم دائماً الحصول على آخر تحديث لقواعد البيانات التي تشتمل على أنماط الفيروسات المختلفة وتثبيتها باستمرار.

عند تثبيت أي من برامج مكافحة فيروسات الحاسوب، يُفضل القيام باجراء فحص كامل للحاسوب وبشكل دوري، وهذه الفحوصات قد تكون آلية أو يدوية:

- **الفحص الآلي** - و هذا الخيار يعتمد على نوع برنامج مكافحة الفيروسات المستخدم، فقد يتيح البرنامج امكانية عمل إعدادات خاصة لكي يقوم البرنامج بفحص مجموعة من الملفات أو المجلدات بشكل آلي و خلال فترات زمنية يتم تحديدها أثناء الإعداد.
- **الفحص اليدوي** - و هي الطريقة التي تتوفر غالباً في كافة برامج مكافحة الفيروسات، و يفضل توظيف هذا الخيار باستمرار، فمثلاً يجب اجراء فحص يدوي للملفات التي يتم استقبالها من مصادر خارجية قبل تشغيلها و استخدامها، و هذه المصادر قد تكون:
 - الانترنت - أي من خلال برامج المحادثة أو البريد الالكتروني أو من خلال التحميل المباشر من مواقع المشاركة المختلفة.
 - وسائط البيانات - والتي تشمل أقراص الـ CD أو DVD أو ذواكر الـ Flash.

آلية التعامل مع الفيروسات المُكتشفة:

يختلف التعامل مرةً أخرى مع الفيروسات باختلاف البرنامج المُستخدم، كما يختلف التعامل إذا كان اكتشاف الفيروس تم خلال الفحص الآلي أو من خلال الفحص اليدوي، و في حالات كثيرة سيقوم البرنامج بإظهار صندوق نصي لإعلام المستخدم عن اكتشاف فيروس و أيضاً لسؤاله عن الاجراء الذي سيقوم به سواءً كان هذا الاجراء هو تنظيف (Clean) الملف و هذا الخيار يعني إزالة الفيروس و الاحتفاظ بالملف المُصاب و قد يقوم البرنامج بهذا الاجراء بشكل آلي، و عند نجاحه يقوم بإعلامك و أما عند عدم امكانية اجراء (Clean) يقوم بسؤال المستخدم عن بعض الاجراءات الأخرى، من المفيد دائماً أن يقوم المستخدم بالتعرف على كافة الميزات التي يُقدمها البرنامج حتى يمكن توظيفها بأفضل طريقة ممكنة؟

اختيار البرنامج المناسب

يوجد العديد من الشركات المتخصصة في انتاج برامج مكافحة الفيروسات، لهذا فقد يكون اختيار برنامج للحماية مهمة مُربكة إلى حدٍ ما، لأن كافة برامج مكافحة الفيروسات تقوم بشكل أساسي بنفس المهمة و هي الحماية و هي اكتشاف و حذف فيروسات الحاسوب و عليه فإن اختيار برنامج مُعين يكون عادةً من خلال توصيات المستخدم أو من خلال الميزات و المهام الاضافية الموجودة أو حتى من خلال سعر البرنامج نفسه.

يوجد العديد من مواقع الانترنت المتخصصة و التي تقوم بعمل تقييمات دورية لبرامج مكافحة الفيروسات المختلفة، و هذه المواقع تقوم عليها غالباً جمعيات غير ربحية تهدف إلى زيادة درجة التنافس بين منتجي هذه البرامج و من هذه المواقع:

- <http://www.av-comparatives.org/>
- <http://www.virusbtn.com/>

الحصول على التحديثات ومعلومات الفيروسات

تقدم كافة برامج مكافحة الفيروسات آليات لتحديث قواعد بيانات الحماية لديها، وهذه الآليات قد تكون يدوية أو قد تكون تلقائية - وهو الخيار المُقدم من أغلب برامج الحماية الحديثة. ولأن أغلب الفيروسات الشائعة المُكتشفة يتم إصدار تحديثات خاصة لتمكين برامج الحماية من اكتشافها، فمن المفيد تجاهل رسائل البريد الإلكتروني التي تدعي اكتشاف فيروسات خطيرة ستقوم بتدمير قرصك الصلب وغيرها من التحذيرات التي تبالغ بشكل كبير في وصف فيروسات قد تكون حقيقية ولكنها قديمة جداً، مثل هذه الرسائل غالباً تُصنف على أنها بريد مخادع، يمكن مراجعة النشرة الخاصة بالبريد المخادع للاطلاع على المزيد من المعلومات.

عند الشك باحتمال صدقية هذه الرسائل يمكن دائماً الرجوع إلى الشركة للمنتجة لبرنامج الحماية لديك والتي بدورها ستقوم غالباً بتوفير قاعدة معرفية عن كافة التساؤلات والاستفسارات والمعلومات عن مختلف الفيروسات المنتشرة وهذه المعلومات تكون حقيقية بخلاف ما يتم نشره عبر الرسائل الكاذبة.

أخيراً - فإن تثبيت واستخدام أحد برامج الحماية من الفيروسات والحفاظ عليه مُحدثاً باستمرار، سيوفر بالضرورة حماية كبيرة للحاسوب والملفات الشخصية ولكن ينبغي في نفس الوقت عدم الاكتفاء بهذه البرامج و اتخاذ اجراءات وقائية أخرى لضمان أفضل حماية متكاملة.

دائرة أمن المعلومات