

الفيروسات

تعريف الفيروسات

فيروس الكمبيوتر هو برنامج صغير يتم إدخاله على الحاسب الآلي من غير علم المستخدم بغرض تدمير بعض أو جميع البرامج والأجهزة المكونة للحاسب الآلي .

أنواع الفيروسات

1. فيروسات تعمل عند بدء التشغيل: يحتاج الكمبيوتر عند تشغيله إلى تعليمات خاصة داخلية لمعرفة مكونات الجهاز، وهي توجد عادة في ملفات تدعى ملفات النظام (System Files) التي تحتوي على البرامج الخاصة ببدء التشغيل . ويقوم هذا النوع من الفيروسات بالتسلل إلى القطاع الخاص ببرنامج الإقلاع على القرص (Boot Sector) وإتلاف محتوياته والعبث بها، ما يؤدي إلى تعطل عملية الإقلاع .
2. فيروس الملفات: يهاجم هذا النوع نظام التشغيل، وأي برامج أخرى موجودة على الكمبيوتر، كالتطبيقات المكتبية والألعاب وغيرها، ويعمل على العبث بمحتويات الملفات التي تنتهي بامتداد bin, com sys, exe, وتدميرها .
3. فيروسات الماكرو : تصيب هذه الفيروسات برامج التطبيقات المكتبية مثل مايكروسوفت وورد أو أكسل. وهي من أكثر أنواع الفيروسات انتشاراً واستخداماً في عمليات التسلل إلى كمبيوترك عبر التطبيقات .
4. الفيروسات المتعددة الملفات : تنسخ هذه الفيروسات نفسها في صيغة أولية ثم تتحول إلى صيغ أخرى لتصيب ملفات أخرى.
5. الفيروسات الخفية (الأشباح) : وهي فيروسات مخادعة. إذ أنها تختبئ في الذاكرة ثم تتصدى لطلب تشخيص وفحص قطاع التشغيل، ثم ترسل تقرير مزيف إلى السجل بأن القطاع غير مصاب
6. الفيروسات متعددة القدرة التحويلية : وهذه الفيروسات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الانتقال من ملف إلى آخر، لكي يصعب اكتشافها

كيفية حماية الحاسوب

1. من الضروري تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز. إن هذا يتيح لهذه البرامج البحث عن الفيروسات وتدميرها سواء كان أسبوعياً أو يومياً أو عند التشغيل
2. عدم فتح أي ملف مرفق ضمن أي رسالة بريد إلكتروني أو أي برنامج آخر كالماسنجر، مهما كان مصدرها، إلا بعد أن تفحصها باستخدام برنامج مضاد للفيروسات، بشرط أن يكون مصدر الرسالة معروفاً، و أن تكون تتوقع وصول هذا الملف لأن بعض الفيروسات ترسل نفسها بأسماء أشخاص آخرين عن طريق دفتر العناوين. لذا احذر من ذلك .
3. متابعة أخبار الفيروسات وطرق تغريبها بالمستخدم، عبر مواقع الأخبار التقنية أو الصحف اليومية أو النشرات الإخبارية بهدف أخذ الاحتياطات اللازمة وعدم الوقوع في فخ هذا الفيروس الجديد

4.التأكد من مصدر أي برنامج تقوم بإنزاله عبر إنترنت وفحصه بواسطة برنامج مضاد الفيروسات الذي تستخدمه قبل تثبيته في جهازك

5.تعطيل خاصية تحميل الجهاز من مشغل الأقراص المرنة (Floppy drive)

6. من الضروري أيضاً تحديث برامج مستكشف الفيروسات بصورة دورية، من خلال الحصول عليها من الشركة المنتجة، أو من مواقع إنترنت المختلفة، كي تضمن حصولك على آخر المعلومات والأعراض الخاصة بالفيروسات الجديدة، وطريقة الوقاية منها .

7. تشغيل برامج مستكشف الفيروسات، وتفحص أي ملفات أو برامج جديدة تصلك عبر البريد الإلكتروني، والإنترنت، والأقراص المرنة، وعدم السماح بإدخال وتشغيل أي ملفات أو برامج مجهولة المصدر وبدون الفحص مسبقاً .

8. الانتباه إلى عدم تشغيل أو إعادة تشغيل الكمبيوتر بوجود القرص المرن في موقعه، حيث أن بعض هذه الفيروسات تختبئ داخل القرص المرن حتى تجد الفرصة الملائمة للتشغيل عندها .

9.تحميل البرامج عن طريق المواقع الموثوق فيها .

خصائص الفيروسات

1.الانتشار: يتميز الفيروس بقدرته على التناسخ والانتشار

2.القدرة على التخفي : للفيروسات قدرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى كما تم أيضاً تزويد الفيروسات بخاصية التمويه والتشبه حيث أن الفيروس يرتبط ببرنامج موجود في الحاسبة وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه ومنها ما يدخل النظام على شكل ملفات مخفية بحيث لا تستطيع ملاحظة وجوده عن طريق عرض ملفات البرنامج. وبعض الفيروسات تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسبة وتنتظر وقت التنفيذ. كما أن بعضها تقوم بإخفاء أي أثر لها حتى أن بعض مضادات الفيروسات لا تستطيع ملاحظة وجودها ثم تقوم بنسخ نفسها إلى البرامج بخفة

3.القدرة التدميرية : تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين (فايروس تشرنوبل)