

الكمبيوتر والإنترنت

الفيروسات Viruses

• ماهي 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.

• تقسيم 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) :

وهذه 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

الكمبيوتر والإنترنت

الفيروسات Viruses

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.

الكمبيوتر والإنترنت

الفيروسات Viruses

. من خصائص الفيروسات

1- الإنتشار :

يتميز الفيروس أيضاً بقدرة هائلة على الإنتشار .. وقد سبق وأن قدمت العوامل التي تساعده في ذلك ..

2- القدرة على التخفي :

للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الإرتباط ببرامج أخرى كما تم أيضاً تزويد الفيروسات بخاصية التوميه والتشبه حيث أن الفيروس يرتبط ببرنامج يقوم بأعمال لطيفة أو له قدرة عرض أشياء مثيرة، وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه.

وللفيروسات عدة وسائل للتخفي منها ارتباطه بالبرامج المحببة إلى المستخدمين .. 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 الحاسب 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 وسرية (فيروسات تدري من أين تأكل الكتف) ..

3- القدرة التدميرية :

تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين (كفيروس تشرنوبل).

الكمبيوتر والإنترنت

الفيروسات Viruses

• أفضل برامج الحماية من الفيروسات

توجد العديد من برامج الحماية من الفيروسات لكن أفضلها وأشهرها على الإطلاق هما هذان البرنامجان

ظهر مؤخراً فيروس جديد خطير من نوع الدودة Worm



يحمل هذا الفيروس الاسم " بنتاغون Pentagon " ، ولعل أخطر ما في هذا الفيروس هو سرعة انتشاره عبر الإنترنت ، وذلك عن طريق برنامج مايكروسوفت أوتلوك ونظام إرسال الرسائل آي سي كيو، ما أدى إلى إصابة الآلاف من أجهزة الكمبيوتر حتى الآن.

ويصيب فيروس البنتاغون برنامج مكافحة الفيروسات بالعجز، ومن ثم يرسل نفسه بصورة تلقائية إلى جميع عناوين البريد الإلكتروني وعناوين الرسائل المستعجلة الموجودة ضمن الكمبيوترات المصابة.

والملف المصاب هو عبارة عن ملف من المفترض أنه تطبيق لحفظ الشاشة **Screen Saver** ، أما الرسالة فتأتي معنونة بعبارة " هاي " ويتضمن نصها عبارة: كيف حالك؟ إنني في عجلة من أمري أعد بأنك ستحبها".

ويقول أحد خبراء مركز أبحاث الفيروسات لدى شركة مكافي أن الفيروس الجديد ينتشر بسرعة كبيرة جداً، وقد ألحق بالشركات والأفراد من مستخدمي الكمبيوتر أضراراً جسيمة نظراً للفترة الزمنية القصيرة التي ينتقل خلالها من مكان لآخر.

الكمبيوتر والإنترنت

الفيروسات Viruses

يذكر أن آخر الفيروسات التي انتشرت بسرعة هائلة كانت فيروس خطاب الغرام الذي أصاب الملايين من أجهزة الكمبيوتر العام الماضي.

وفيروس جديد ينتشر ضمن ملفات أدوبي أكروبات ..

"استطاع قسم مكافي المتخصص في أبحاث الفيروسات لدى شركة نيتورك أسوسيتس، التعرف على فيروس جديد يحمل اسم بيتشي **Peachy**، وهو يعتمد على مستندات بي دي إف للتنقل والانتشار"، حسب ما ذكره فينسينت غولوتو، مدير مجموعة مكافي لمكافحة الفيروسات.

ولكن لحسن الحظ، فإن أولئك الذين يقومون فقط بتصفح هذا النوع من الملفات لن يكونوا عرضة لمخاطر فيروس بريتشي، فالفيروس ينتشر فقط عن طريق برنامج أدوبي أكروبات، البرنامج الذي يقوم بإنشاء مستندات بي دي إف، وليس من خلال برنامج أكروبات ريدر الجاني الذي تنحصر مهمته فقط في استعراض هذا النوع من المستندات.

يستغل هذا الفيروس خاصية متوفرة في برنامج أدوبي أكروبات تسمح للمستخدم بدمج ملفات أخرى ضمن ملحقات بي دي إف والتي لا يمكن لأحد فتحها إلا إذا كان لديه برنامج أكروبات. (يمكننا القول بأن خطورة هذا الفيروس قليلة إلى حد ما، حيث لم يردنا إلى الآن أي تقرير عن وجوده لدى أحد من عملائنا) و يضيف غولوتو : ولكن مما لا شك فيه أن فيروس بريتشي هذا سيثير قلقاً عارماً بين أوساط مستخدمي الكمبيوتر والإنترنت، فظهوره يعني إمكانية أن تتحول مستندات بي دي إف ذات الانتشار الواسع بين مستخدمي البريد الإلكتروني والإنترنت إلى قناة جديدة لتسرب الفيروسات وانتشارها.

يرتبط اسم هذا الفيروس الجديد بلعبة صغيرة موجودة ضمن مستندات بي دي إف تدور فكرتها حول البحث عن الخوخ **Peach** ، وذلك حسب ما جاء على لسان شخص اسمه زولو يدعي أنه هو الذي صمم هذا الفيروس.

الكمبيوتر والإنترنت

الفيروسات Viruses

وفي حال قامت شركة أدوبي مستقبلاً بتعديل إصداراتها الجديدة من أكروبات ريدير بحيث تغدو قادرة على قراءة الملفات المرفقة داخل مستندات من نوع بي دي إف، فإن هذا البرنامج سيصبح عرضة لفيروس بريتشي أيضاً.

ولدى وصول الفيروس إلى جهاز ما، فإنه يقوم تلقائياً بإرسال نفسه إلى الآخرين بعد أن يجمع كافة العناوين البريدية من برنامج آوتلوك وعقب عقد اتفاقية مع شركة أدوبي في يونيو/ حزيران الماضي، أصبح برنامج مكافحة الفيروسات مكافى قادراً على إجراء مسح وقائي على مستندات بي دي إف، ولكن ومع ذلك فإن هذه العملية لن توفر الحماية الشاملة من أنواع أخرى مماثلة من الفيروسات، سيما أن البرنامج لا يستطيع التعرف على الفيروسات وإثبات نشاطها ما لم يتم تحديث بياناته باستمرار غير أن التحديث الأخير الذي تم إجراؤه على برنامج مكافى لمكافحة الفيروسات سيجعل البرنامج قادراً على كشف الفيروس بريتشي في حال وجوده ..