الـــفـــيـــروســـات

حسر 101

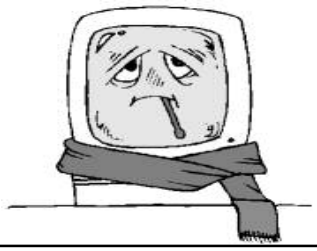
إعداد: أ. خـلـيـفـة الـجـدع
كلية المجتمع بالمجمعة

ما هي فيروسات الحاسوب؟

- إن فيروس الحاسوب عبارة عن برنامج صغير يختفي في موضع ما على الأقراص الخاصة بك (الأقراص المرنة والقرص الصلب). وإذا لم تكن تستخدم برنامج لاكتشاف الفيروسات، فستعرف بوجود فيروس بالحاسوب عندما ينشط. ويتم تنشيط الفيروسات المختلفة بطرق مختلفة. فعلى سبيل المثال، هناك فيروس شهير ينشط فقط عندما يكون يوم الجمعة هو اليوم الثالث عشر في الشهر. فاحذر لأن الفيروسات يمكنها تدمير كل البيانات الخاصة بك.

كيف يصيب الفيروس الحاسوب؟

- تختفي الفيروسات على أي قرص وعندما تستخدم القرص (إما قرص مرن أو قرص صلب آخر عبر شبكة)، يبدأ الفيروس في العمل ويصيب الحاسوب الذي تعمل عليه. وأسوأ شيء في الفيروسات هو أنها يمكن أن تنتشر من حاسوب لآخر أو عبر شبكة من الحواسيب.



يتبع...

- تسمح لك شبكة الإنترنت بالوصول إلى الملفات من جميع أنحاء العالم ويجب عليك ألا تتصل بالإنترنت إذا لم تكن قد قمت بتثبيت برنامج مضاد للفيروسات على الحاسوب الذي تعمل عليه.
- من المهم أن تقوم بتحديث البرنامج المضاد للفيروسات بشكل دائم. فالكثير من البرمجيات مثل "نورتون أنتي فيرس" تسمح لك بتحديثها حتى يمكنها تحديد الفيروسات المكتشفة حديثًا.

كيف يمكن حماية الحاسوب من الفيروسات؟

- هناك عدد كبير من البرمجيات المضادة للفيروسات. وأغلبها أفضل من البرمجيات القديمة نسبيًا والمتاحة مع أنظمة التشغيل دوس وويندوز، ولكنها ليست مجانية بالطبع! وأهم شيء بالنسبة للبرنامج الذي ستستخدمه هو أن تقوم بتحديثه بشكل دائم. وتقدم الكثير من الشركات أقراص تحديث بشكل منتظم أو تتيح لك الحصول على نسخة محدثة من خلال لوحة إعلانات إلكترونية أو عبر الإنترنت.

أشهر برامج الحماية من الفيروسات

- Macfee anti-virus software: http://www.macfee.com
- Norton Anti-virus software: http://www.symantec.com/avcenter
- DR Solomon anti-virus Software: http://www.drsolomon.com
- Kaspersky Anti-virus
- http://www.kaspersky.com

أنواع الفيروسات

- هناك ثلاثة انواع رئيسية للفيروسات:
  - فيروسات القنابل الموقوتة Time Bombs:

وهي الفيروسات التي تنشط و تفعل في وقت محدد أو بعد تنفيذه عدة مرات.

  - فيروسات أحصنة طروادة Trojan Hours:

هذا النوع من الفيروسات لا ينسخ نفسه، فقط عندما يتم تثبيته يقوم بعمل معين كأن يقوم بسرقة ملفات وأرقام سرية من جهازك إلى مكان ما على الإنترنت وهو الأكثر استخداماً لدى الهاكرز لسرقة المعلومات.

يتبع...

- الفيروسات الدودية Warms:

برامج تنسخ نفسها من جهاز إلى جهاز عن طريق الشبكات ولا تحتاج لأي نسخ منك فهي تنتقل عن طريق الشبكات لوحدها.

تصنيف الفيروسات حسب الخطورة

- العادي لا يفعل هذا النوع من الفيروسات شيئا سوى التكاثر ويمكن ان لا يشعرنا بوجوده لأنه لا يحدث ضررا أو تخزينا للمعلومات وحالما يتم تشخيصه واكتشافه فكل ما يلزم عليك عمله هو حذف هذا النوع م الفيروسات .

- كما في فيروس Stupid الذي لايفعل شيء سوى البحث عن ملف نظيف واصابته .

يتبع..

- الثانوي أخطر قليلا يسبب هذا النوع من الفيروسات تغييرا أو مسحا لواحد أو أكثر من الملفات القابلة للتنفيذ EXE, COM,BAT بحيث أنه يحذف الملفات التنفيذية لكنه غير خطر لأنه هذه الملفات موجوده على Disk وأعيد تنزيله مرة أخرى بما أن هذه الملفات أخذت أساسا من الاقراص الاصلية المقدمة من قبل منتجي البرامج فإنه اعادة تركيبها على الجهاز بعد إزالة الفيروس هي عملية بسيطة نسبيا مثل فيروس AIDS الذي يصيب الملفات من نوع COM .

يتبع...

- المعتدل يمكن لهذا النوع من الفيروسات تدمير جميع الملفات الموجودة على القرص الصلب وذلك عن طريق Format أو استبدال معلومات بمعلومات أخرى كما في فيروس Disk Killer (قاتل ال Disk) الذي يسبب إعادة تهيئة القرص الصلب عندما يبلغ عدد الاقراص المرنة التي تمت إصابتها عددا محددا أو كمافي فيروس كولومبوس الذي يفعل الشيء ذاته اذا تم تنفيذ ملف من نوع .com مصاب بتاريخ octobar/12 وبالرغم من ان الكثيرين قد يرون ان هذه المشكلة الخطيرة إلا أنه مسح جميع الملفات لا يشكل ضررا حقيقيا طالما أن النسخ احتياطي تتم بانتظام .

يتبع...

- الرئيسي يؤدي هذا النوع إلى تخريب المعلومات بشكل تدريجي وبطيء عبر فترة من الزمن كنسخ رسالة معينة او بشكل عشوائي كما في فيروس Ripper الذي يتسبب في واحدة كل 1000 عملية كتابة على القرص بشكل خاطيء مما يؤدي إلى تخريب تدريجي للنظام .

يتبع...

- الشديد يتمكن هذا النوع من احداث تغييرات ذكية وبارعة للبيانات دون ترك اي اثر يشير الى التغيير الحاصل كأن يقوم بشكل عشوائي بمبادلة كتل من المعلومات المتاثلة في الطول بين بعض الملفات وإن تأخر اكتشاف الاصابة به اكثر من بضعة ايام فإن هذا النوع من الضرر يستحيل ازالته لان المعلومات الاصلية لن تكون موجودة في ذلك الوقت وقد يصبب الضرر النسخ الاحتياطية ايضا كما في فيروس 1 2/1 .

يتبع...

- اللامحدود يستهدف هذا النوع شبكات الكمبيوتر ويمضي أكثر الوقت في معرفة كلمة السر للمستخدمين الاكثر فعالية(supervisers,Administrator) وعندما يتمكن من الحصول عليها فإنه يمررها الىواحدة او أكثر من مستخدمي الشبكة على أمل أن تستخدم لأغراض سيئة .

تصنيف الفيروسات حسب منطقة الإصابة

- فيروسات قطاع بدء التشغيل
  يمكن لهذا النوع ان يسبب العدوى اذا تم بدء التشغيل من قرص مصاب ولما كانت المساحة التي يحتلها برنامج بدء التشغيل صغيرة فإن الفيروس يعمل الى نقله الى مكان آخر على القرص ويحله محل ليضمن لنفسه أولية التنفيذ كما في فيروس Stoned

يتبع...

- **فيروسات البرامج**
  هذا النوع يصيب البرامج التنفيذية والغير تنفيذية يتميز بسرعة العدوى .
  هنا سوف نستعرض أهم وأخطر أنواع الفيروسات إلى وقتنا الحالي :

1) buddylst.exe
2) calcu18r.exe
3) deathpr.exe
4) einstein.exe
5) happ.exe
6) girls.exe
7) happy99.exe
8) japanese.exe
9) keypress.exe

طرق انتشار الفيروسات

- القرص المرن Floppy Disk حيث يحدث دوما أن تقوم بنقل ملف او برنامج صغير من جهاز إلى جهاز آخر.
- القرص المضغوط CD-ROM و خصوصاً الأنواع المنسوخة منها والغير أصلية.
- القرص الصلب Hard Disk بعض مستخدمي الحاسبات المتقدمين نوعاً ما يقومون بنقل المعلومات من قرص صلب لآخر.

يتبع..

- الإنترنت Internet: و هي تعتبر من أكثر المصادر نشراً للفيروسات حيث تقوم بالإبحار داخل العديد من المواقع المنتشرة والتي تحوي في داخلها برامج الفيروس و خصوصاً في المواقع التي تقدم البرامج المساعدة المجانية والتجريبية.
- البريد الإلكتروني E-mail: ويتم من خلاله ارسال الفيروس على شكل ملف مرفق مع رسالة فإذا تم تنزيل هذا الملف انتقل الفيروس للجهاز.

أعراض إصابة الجهاز بالفيروس

- نقص شديد في الذاكرة:

حيث تكون الذاكرة طبيعية قبل دخول الفيروس اما بعد دخول الفيروس فإنه يلاحظ نقص شديد في الذاكرة.

- بطء تشغيل النظام بصورة مبالغ فيها.
- كثرة ظهور رسائل الخطأ
- توقف النظام بلا سبب
- تغير في عدد و مكان الملفات و كذلك حجمها بدون اسباب مقنعة.

يتبع...

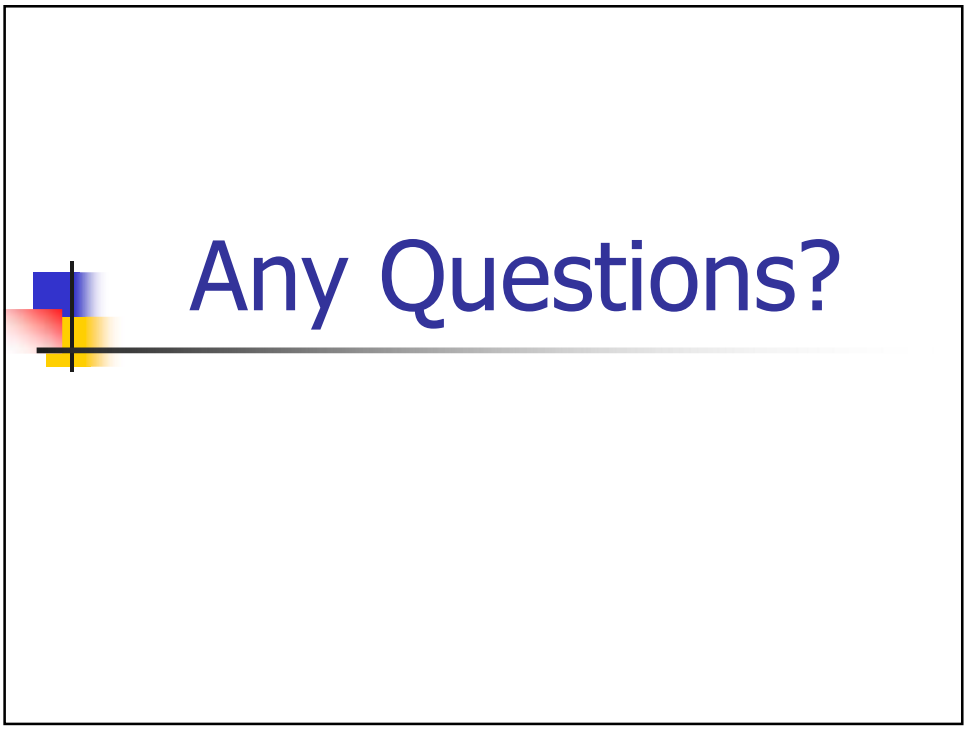
- ظهور أحرف ورموز غريبة على الشاشة عند محاولة الكتابة باستخدام لوحة المفاتيح.
- اختلاط أدلة القرص أو رفض النظام العمل منذ البداية.

طرق الحماية من الفيروسات

- تجنب طرق الإنتشار السابقة.
- شراء النسخ الأصلية و تجنب النسخ التجريبية من البرامج.
- الإحتفاظ بنسخ دورية من البيانات و عمل نسخ احتياطية منها باستمرار وبشكل دوري Backup.
- استخدام أحدث وأفضل برامج مكافحة الفيروسات Anti Virus Program والذي يقوم بما يلي:

يتبع...

- التأكد من عدم وجود الفيروسات على جهاز الحاسوب.
- فحص كافة الملفات التي تقوم بتحميلها سواء م القرص المرن أو الصلب أو المضغوط و التأكد من عدم وجود فيروسات بها قبل التحميل.
- فحص كافة الملفات التي تقوم بتحميلها من الإنترنت.
- فحص الرسائل الواردة إليك من البريد الإلكتروني.


Any Questions?