

الجمهورية اليمنية

وزارة التعليم العالي

جامعة سبا

بسم الله الرحمن الرحيم

**الفيروسات**

**الفيروسات في الكمبيوتر**

**بحث شامل وكامل عن الفيروسات**

**2014**

اعداد الطالب/هشام محمد قايد العنسي

اشراف الدكتور/عبد الماجد الخليدي

[علمي](http://www.brooonzyah.net/vb/t76359.html) عن [الفيروسات](http://www.brooonzyah.net/vb/t76359.html) [جاهز](http://www.brooonzyah.net/vb/t76359.html) و [كامل](http://www.brooonzyah.net/vb/t76359.html) ، بحث علمي عن الفيروسات جاهز و كامل ، بحث علمي عن الفيروسات جاهز و كامل ، بحث علمي عن الفيروسات جاهز و كامل بحث علمي عن الفيروسات **جاهز و كامل عن الفيروسات بحث**

**تعريف الفيروس  
  
فيروس الكمبيوتر هو برنامج صغير تم تجهيزه وإعداده من قبل أحد مستخدمي الكمبيوتر غير الأسوياء، وذلك لإرضاء متعته المريضة بنشر الفوضى والدمار في الكمبيوترات الأخرى. وتختلف أنواع الفيروسات من ناحية الحجم والنوع وطريقة التشغيل ومستوى الدمار الذي تحدثه.  
  
أنواع الفيروسات  
يمكن تقسيم الفيروسات إلى ثلاثة أنوع:**  
 **1-فيروسات بدء التشغيل  
يحتاج الكمبيوتر عند تشغيله إلى تعليمات خاصة داخلية لمعرفة مكونات الجهاز وحجم ومكان وجودها، 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**[.](http://www.brooonzyah.net/vb/)  
 **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**[.](http://www.brooonzyah.net/vb/)  
 **كيف تنتقل الفيروسات؟  
توجد طرق متعددة ومختلفة للإصابة بالفيروسات والملفات من مواقع مختلفة غير موثوقة.**  
 **2- تبادل الملفات من خلال استخدام البريد الإلكتروني (خصوصاً الملفات المرفقة.**  
 **3- المشاركة في استخدام القرص المرن بين الكمبيوترات المختلفة ، وتشمل:**  
 **1- انتقال الفيروسات من خلال الإنترنت خصوصاً عند عملية إنزال البرامج.**  
**طرق الوقاية من الفيروسات**  
**للمحافظة على سلامة وصحة جهازك يجب إتباع النقاط الأربع التالية:**  
 **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- من الضروري أيضاً، من 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.**  
 **3- تشغيل برامج مستكشف الفيروسات، وتفحّص 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.**  
 **4- 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.  
  
إن اتباع طرق الوقاية السابقة، واعتمادها كنظام يومي دائم في التعامل مع جهازك، يضمن المحافظة على صحة كمبيوترك ووقايته من الإصابة بالفيروسات.**  
**فيروس تشير نوبل**  
**ما هو فيروس تشير نوبل؟**  
**هو أحد الفيروسات المدمرة الموقوته، ينشط يوم 26 من كل شهر ميلادي، وتزداد تدميرا يوم 26 من شهر إبريل.**  
**ما هو تأثيره على الجهاز؟**  
**هناك عدة أنواع من تشير نوبل، ولكن يظهر لن انوعان رئيسين وهما:**  
**1. النوع الأول: يدمر البيانات الموجودة في ال BIOS، ويدمر أيضا جدول التقسيمات (Partition Table) للقرص الصلب (Hard Disk).**  
**2. النوع الثاني: يدمر Partition Table للقرص الصلب فقط.**  
**فبخصوص ال BIOS وهو عبارة عن رقاقة (CHIP) موجودة على لوحة الأم (Mother Board) داخل جهازك إذا دمرت البيانات الموجودة فيه فلن تظهر لك الشاشة أبدا، فعند تشغيل الجهاز لن يظهر لك أى شئ على شاشة وترى أن الشاشة في وضع آمن (StandBy).**  
**وإذا دمر Partition Table في القرص الصلب وهو الذي يتعرف على الأقراص الصلبة الموجودة في جهازك وتقسيمات كل قرص، فسيوهمك بأنه لغى محتويات القرص الصلب بأكمله وتطر إلى إعادة تقسيم القرص الصلب من جديد وعمل تهيئة للقرص الصلب (Format).**  
**طرق الوقاية منه؟**  
**· تحديث برنامج مضاد الفيروسات الذي في جهازك دائما من الإنترنت.**  
**· عمل Rescue Disk الذي يأتي مع برنامج مضاد الفيروسات، وذلكل لضمان إذا تعطل جهازك أو أصابك تشير نوبل يمكنك إصلاحه.**  
**· كما يمكنك عمل تعديل بسيط في Jumper في لوحة الأم داخل جهازك لعدم السماح بالكتابة على ال BIOSولعمل ذلك أقرا الكتاب المرفق مع لوحة الأم.**  
**كيفية معالجته إذا أصاب جهازك؟**  
**سأدلك على طريقة معالجة ال Hard Disk وال BIOS:**  
**· Hard Disk: لإرجاع ال Partition Table يمكنك عمل عدة أشياء ،ومنها:**  
**o وضع Rescue Disk في السواقة (Driver) عند بدء التشغيل ثم تتبع الخطوات.**  
**o أو سحب أحد البرامج التالية بمجرد الضغط عليها، وذلك حسب مواصفات القرص الصلب لديك، ثم تتبع الخطوات من الملف المرفق معها Readme.txt:**  
**§ إذا كان القرص الصلب Fat 16 bit.**  
**§ إذا كان القرص الصلب Fat 32 bit وأقل من 8 جيجابايت.**  
**§ إذا كان القرص الصلب Fat 32 bit وأكثر من 8 جيجابايت.**  
**· BIOS: لإرجاع البيانات الأصلية فعليك نسخ البيانات من BIOS مصلح إلى ال BIOS التي يصعب إيجادها،**  
 **بعض الإعتقادات الخاطئة عن الفيروسات  
  
الفيروسات لا تنتشر باستخدام ملفات البيانات.  
قراءة البريد الإلكتروني لا يمكن أن تسبب إصابة الجهاز بفيروس.  
الفيروسات لا يمكن أن تسبب تلفاً في قطع الحاسب.  
فيروسات البرامج التحميلية هي الأكثر خطراً.  
الفيروسات لا تعمل جيداً في بيئة وندوز.**  
**ما هي الإختراقات؟  
هي محاولة الدخول على جهاز أو شبكة حاسب آلي من قبل شخص غيرمصرح له بالدخول إلى الجهاز أو الشبكة وذلك بغرض الإطلاع / السرقة / التخريب / التعطيل .**  
 **ماهي مصادر أخطار الإختراقات؟  
1. أخطار متعمدة : ويكون مصدرها جهات خارجية تحاول الدخول إلى الجهاز بصورة غير مشروعة بغرض قد يختلف حسب الجهاز المستهدف. هناك عدة جهات تصنف تحت هذا النوع :  
1- محبي الاختراقات هاكرز  
2- جهات منافسة  
3- أعداء خارجيين  
4- مجرمين محترفين  
2. أخطار غير متعمدة وهي تنشأ بسبب ثغرات موجودة في برمجيات الكمبيوتر والتي قد تؤدي إلى تعريض الجهاز إلى نفس المشاكل التي تنتج عن الأخطار المتعمدة .**  
 **من يقوم بهذه الإختراقات ؟  
1. محترفين : وهم يتميزون بمعرفة دقيقة ببرامج النظم والثغرات فيها والقدرة العالية في البرمجة .  
2. هواة : وهم ذوي خبرة محدودة في البرمجة نسبياً وغالباً يبحثون عن برامج جاهزة لاستخدامها في عملية الاختراق .**  
 **لماذا لا تقوم شركات تقديم خدمة الإنترنتب حماية أجهزة المستخدمين من عمليات الاختراقات ؟.  
  
- إنالو㳣ائل الفنية المتبعة في الحد من المخاطر الأمنية على أنظمة وشبكات الحاسب الآلي عادة ما تحد أيضا من استخدام بعض تطبيقات وخدمات الإنترنت. فمثلاً لزيادة التحصين الأمني قد ُتعطل بعض برامج الحوارات أو الاتصال الهاتفي عن طريق الإنترنت. ولهذافإنه غالباً ما يترك للمستخدم تحديد المستوى الأمني الذي يرغب في توفره لأنظمت هو بالتالي توفير الوسائل الفنية الأمنية المناسبة. ولكن مع كثرة المخاطر الأمنية على شبكة الإنترنت من ناحية ، واتساع عدد المستخدمين وقلة خبرة الكثير منهم في المخاطر الأمنية وأساليب الحد منها من ناحية أخرى ، بدأ بعض مقدمي خدمة الإنترنت في الولايات المتحدة الأمريكية بتقديم خدمات إضافية لمشتر كيهم سواء عن طريق الاتصال الثابت (Leased Lines) أو حتى الاتصال الهاتفي (Dial-up) ، تتمثل في توفير وسائل حماية أمنية لأجهزة هؤلاء المشتركين.**  
 **لماذا لم تصمم شبكة الإنترنت بشكل آمن يحد من المخاطر الأمنية ؟.  
  
- كانت الإنترنت في بدايتها محصورة في مجموعة قليلة من الأكاديميين والباحثين في عدد منال جامعات ومراكز الأبحاث الأمريكية ، ونظرا لمحدودية عدد المستخدمين و معرفة بعضهم لبعض لم يكن هناك قلق بشأن مخاطر أمنية على الشبكة. و لذلك لم تؤخذ هذه المخاطر فيال اعتبار عندما تم تصميم البروتوكول الأساسي لنقل المعلومات على شبكة الإنترنت (TCP/IP). ولكن مع مرور الوقت ودخول القطاع التجاري للشبكة وما يعنيه ذلك منال ازدياد المضطرد لعدد المستخدمين وتنوع خلفياتهم العلمية والعملية و اختلاف أعمارهم ، بدأت تظهر بعض التجاوزات الأمنية على الشبكة. فقد سجلت أول مشكلة أمنية على شبكة الإنترنت في عام 1988م (أي بعد مرور ما يقرب من عقدين على نشأت الشبكة). تتمثل هذه المشكلة في فيروس كتبه شخص يدعى موريس سمي الفيروس فيما بعد باسمه (Morris Virus). حيث استغل ثغرة في برنامج البريد الإلكتروني مكنت الفيروس من الانتشار في ما يقرب من 10% من أجهزة الحاسب الآلي المرتبطة بشبكة الإنترنت آنذاك و عددها 60 ألف جهاز تقريباً قبل أن يتم اكتشافه.**  
 **ما هي المخاطر الأمنية التي يمكن أن تتعرض لها أجهزة الحاسبات الشخصية عند ارتباطها بشبكة الإنترنت؟.  
  
شبكة الإنترنت تعج بالمخاطر الأمنية المتعددة والمتجددة ، و سنتطرق إلى أكثر تلك المخاطر الأمنية انتشاراً:  
  
1. الفيروسات: تنتقل الفيروسات إلى أجهزة الحاسب بطرق عدة ، ولكن كانت تاريخياً أكثر هذه الطرق انتشار هي استخدام أقراص ممغنطة ملوثة ، أما الآن وبعد ازدهار استخدام الإنترنت فقد أصبح البريد الإلكتروني أكثر طرق انتشار الفيروسات إلى أجهزة الحاسبات. وتختلف نوعية و حجم الأضرار التي قد تحدثه تلك الفيروسات على جهاز الحاسب. فمنها ما يقوم بمسح جميع المعلومات الموجودة على الجهاز أو إحداث أضرار على بعض مكونات الجهاز مثل الشاشة ، ومنها ما يقوم بإرسال نفسه بالبريد الإلكتروني إلى جميع من هم على قائمة المستقبلين مثل فيروس ميليسيا الذي ظهر عام 1999م ، ومن هذه الفيروسات ما هو أقل ضرر كأن يقوم بتعطيل برنامج معين على جهاز الحاسب.  
2. برامج الباب الخلفي: عادة ما تنتقل هذه البرامج إلى أجهزة الحاسب الآلي عن طريق ما يسمى ب "الترو جان"،والترو جان هو عبارة عن برنامجين ، الأول برنامج موثوق به يرغب المستخدم في تحميله على جهازه ، ولكن يلتصق في هذا البرنامج الموثوق برنامج آخر مثل برامج الباب الخلفي، لا يظهر للمستخدم حيث يقوم بتحميل نفسه تلقائياً متى ما قام المستخدم بتحميل البرنامج الأول. و عندما يتحمل برنامج الباب الخلفي في جهاز ما فإنه يفتح ثغرة فيذلك الجهاز تسمح لأي مستخدم على الإنترنت ، وباستخدام برنامج مرافق ، من التحكم الكامل بالجهاز حيث يمكن استرجاع أو حذف أو تغيير أي معلومة مخزنة على ذلك الجهاز ،كما يمكن أيضا سماع ورؤية ما يدور حول ذلك الجهاز المصاب إذا كان**  
**.وكاميرا يضم مايكروفون  
  
3. قلة الخبرة في التعامل مع بعض البرامج: مع ازدياد استخدام الإنترنت من العامة غير المتخصصين ، يتم - وبشكل مستمر ومتسارع – تطوير برامج مختلفة على أنظمة النوافذ (Windows 95/98) تساعد على تفعيل استخدام الشبكة مثل تلك البرامج التي تهيئ جهاز الحاسب الشخصي كي يعمل كخادم (server) مثل خادم نقل الملفات (ftp Server) . إن استخدام مثل هذه البرامج قد يفتح ثغرة في جهاز الحاسب الآلي تمكن الغير من اختراق الجهاز.  
  
4. أخطاء في الإستخدام: مثل الإختيار سوء لكلمة السر أو كتابتها على ورقة يمكن للآخرين قراءتها ، فكلمة السر يجب ألا تكون سهلة يمكن تخمينها.**  
 **ما هي الوسائل التي يمكن إتباعها للحد من تلك المخاطر؟.  
  
1. استخدام برامج كشف ومسح الفيروسات (Virus Scanners) والعمل على تحديثها بشكل دوري حتى تشمل الفيروسات حديثة الاكتشاف. تقوم معظم هذه البرامج أيضا على كشف برامج الباب الخلفي.  
2. الحذر في استقبال البريد الإلكتروني والذي يحوي مرفقات (Attachment) فقد تكون تلك المرفقات عبارة عن برامج مؤذية كالفيروسات وبرامج الباب الخلفي ، علماً بأن معظم برامج كشف الفيروسات تقوم بكشف البريد الإلكتروني قبل تحميله.  
3. عندما يريد المستخدم أن يحمل برنامج على جهازه بإنزاله من موقع على شبكة الإنترنت ، فإن عليه التأكد من موثوقية ذلك الموقع حتى لا يكون البرنامج المراد تحميله عبارة عن تروجان يؤذي جهازه عند تحميله.  
4. عدم استخدام برامج ليس للمستخدم أي خبرة في تشغيلها.  
5. الاحتفاظ بنسخ احتياطية للمعلومات الحساسة في أقراص إضافية خارج الجهاز.**  
 **ما مدى كفاءة الأنظمة الأمنية المستخدمة حاليا في وسائل التجارة الإلكترونية؟.  
  
إن استخدام شبكة الإنترنت في عمليات البيع والشراء قد ينتج عنه تبعات أمنية مثل سرقة أرقام بطاقات الائتمان والتي تمثل الوسيلة الأكثر استخدام في الشراء عن طريق الإنترنت ، أو سرقة معلومات مالية أو تجارية حساسة خلال نقلها بين الشركات والمؤسسات المختلفة. ولهذا فقد تم تطوير عدة أنظمة أمنية تقوم على نقل المعلومات بطريقة آمنة تمنع الغير من الإطلاع عليها أثناء نقلها من خلال الشبكة ، ولذا فإن على جميع مقدمي خدمة الإنترنت الذين يسعون إلى استضافة مواقع للتجارة الإلكترونية توفير مثل هذه الأنظمة واستخدامها لتلك المواقع وبالتالي تقليل المخاطر الأمنية التي قد تحدث عليها. ومن الجدير ذكره أن هذه الأنظمة الأمنية تستخدم في معظم مواقع التجارة الإلكترونية ولا تكلف بالدولارات. آلاف من**  
**الوقاية خير من العلاج لحماية الشبكات من الاختراقات  
  
  
في كل مرة تعمد شركة ما الى وصل شبكتها الداخلية LAN بالانترنت تعرض نفسها لخطر كبير محتمل، فالشبكة العالمية مجال مفتوح لكل الجهات مهما كانت اهدافها ومصادرها وآراؤها. لذلك فان المنظمات والمؤسسات والشركات والمعاهد والوزارات وسواها اصبحت تواجه تهديدا جديا. ما هي الاجراءات المتبعة لمواجهتها؟ نسرد هنا امثلة عما يتبعه مديراي شبكة داخلية ووصلنا الى خلاصة تفيد ان الوقاية خير من العلاج. وطبعا الوقاية النسبية لأن كل شركة تريد في النهاية ان تتصلب الانترنت للاستفادة منها.  
وبهذا فان الفارق بين الاتصال بالانترنت او الانقطاع عنها تظلله الحكمة في الاستخدام. بمعنى اتخاذ الاجراءات.  
واذا كان فعلا رأس الحكمة معرفة الذات، فان جدار النار Fire Wall الحصن الاول هو للتأكد من كل ما يدخل الشبكة الداخلية من الانترنت، وطبعا ما يخرج من الداخل.  
المخترقون  
يستطيع الخبراء في شؤون الشبكات ان يخترقوها. ومن حيث المبدأ يمكنهم بعداتمام اي حالة اختراق ان يسببوا الاذى بطرق مختلفة تؤدي الى نتائج مختلفة .فما هي؟  
1 يستطيع ونبعد الاختراق ان يسرقوا معلومات مهمة في الشبكة او يدمروها.  
2 قد يصلون في اختراقهم الى حدود بلوغ اجهزة فردية خاصة بالموظفين.  
3 يمكن ان يقوموا بتخريبي ؤدي الى توقف الشبكة الداخلية كليا او جزئيا.  
4 يمكن ان يدخلوا بعد الاختراق الى قواعد معلومات محددة ويسعوا لاستعمالها لمصالح شركاتهم الخاصة او يبيعوه الشركات اخرى.  
5 يمكن ان يخترقوا مصادر الشبكة الخاصة بالمعلومات الحساسة والتنكر في شكل موظفين من الشركة المخترقة للقيام باتصالات توحي بأنهم يقومون بأعمال لصالح الشركة المخترقة.  
6 يمكن ان يخترقوا الشبكة الداخلية ولا يقوموا بأي شيء مؤذ. بل الانتظار مدة لإجراء أمر في المكان والزمان المناسبين.  
بناء الجدار  
طبعا الحل لن يكون في قطع اتصال الشبكة الداخلية بالانترنت لأن ذلك سيعرض اعمال الشركة للفشل في مسائل معينة كما سيعطل بريدها الالكتروني. وباختصار فان الهرب من المشكلة لن يحلها. بل سيؤدي في نهاية الامر الى تعزيز سيادة المخترقين على الانترنت. وفي المقابل يمكن للشركة ان تبدأ ببناء جدار الكتروني تحدد ثغراته المعروفة التي يحرسها خبراء الشركة. وعبر هذه الثغرات المحددة تتم عمليات الاتصال بالانترنت. واذا كان هذا الجدار الالكتروني يمنع عمل المخترقين او يعرقله فانه لا يمنع عمل موظفي الشركة ولا يقطع اتصالهم بالانترنت. ولذلك يعتبر الجدار الالكتروني Fire Wall اول حاجز يقف في وجه المخترقين لحماية شبكة داخلية من الاخطار.  
ما هو الجدار الالكتروني؟  
الجدار الالكتروني هو تركيبة من المعدات الالكترونية والبرامج الرقمية التي تبنى متضمنة خوادم Servers واجهزة كومبيوتر شخصية PCs وبرامج تطبيقية وApplications Routers ويتم تجميع كل هذه المعدات والبرامج لتكون الجدار فتقف بذل كفي الخندق المتقدم على «خط النار الشبكي». ويمكن للجدار ان يكون بسيطا جدا ومؤلفا من معدات وبرامج قديمة وقابلة للاختراق. او قد يكون معقدا ومتقدم او مؤلفا من احدث الاجهزة والبرامج العالمية الجديدة. ولا تقتصر كفاية الجدار على المعدات والبرامج بل تتعداها الى ما هو اهم من كل المواد: المدير. مدير الشبكة عادة هو خبير في شؤون الكومبيوتر والاتصالات والبرامج. وبهذه المعادلة التي يجمعها يستطيع ان يبني خبرة تصقل قدراته وتعززها. فاذا كان هناك جدار الكتروني ما في شركة كبرى يتمتع بتقدم لامثيل له. ولكن يشرف عليه مدير تنقصه المعلومات والخبرة والمتابعة. فان الجدار يكون غير ذي قيمة. ويشبه الامر وجود خندق على الحدود ممتلئ بالجنود والمعدات العسكرية. من سلاح بر وجو وبحر، ولكنه يفتقر الى قائد ذكي وخبير. وفي الحالتين تكون النتيجة خسارة الحرب.**

**تم البحث بحمد الله**