المركز الوطني للمتميزين
NATIONAL CENTER FOR THE DISTINGUISHED
/NCDSyria

فيروسات الحاسب

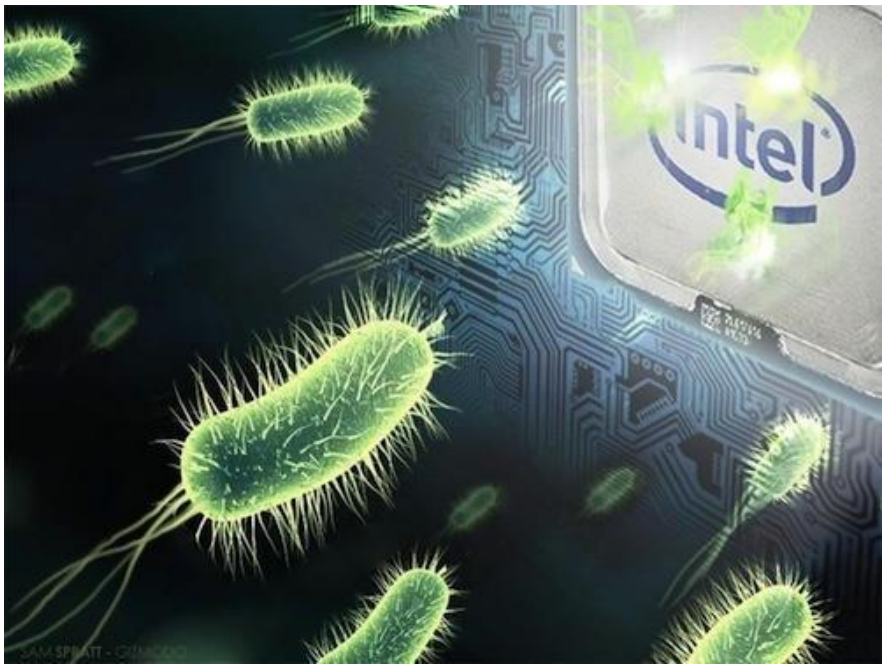
PC Viruses

تقديم الطالب: محمد زياد القباقيبي

الصف: الأول الثانوي

تاريخ: 15/1/2015

إشراف: الآنسة ميس درويش



مقدمة

كثيراً ما نسمع بكلمة فايروس وتعني هذه الكلمة بشكل عام الكائن الصغير الذي يتطفل ويستمد حاجاته من المضيف محدثاً له الأضرار ليبقى على قيد الحياة وهناك العديد من الفيروسات منها ما يصيب الإنسان وتحدث له الأمراض وتضر بجسمه ومنها أيضاً فيروسات الحاسب التي غالباً ما نسمع بها ونعتبرها وباءً على حواسبنا.....

لكن يا ترى ألم تسأل نفسك ما هو فيروس الحاسب؟ وما مبدأ عمله؟ ومن أين يأتي؟ ولماذا هو موجود أصلاً؟ وكيف أتخلص منه؟ وما هو مكافح الفيروس وما مبدأ عمله؟

وطبعاً الكثير منا يعاني من مشكلة الفيروسات التي تعد حالياً من أهم أسباب عطل الحواسب وفقدان الملفات في أيامنا هذه وفي هذه الحلقة سنناقش أيضاً ما الحلول النهائية التي تحمي حواسبنا من هذه الأوبئة لنحصل على حواسب نظيفة وأفضل....

فهرس الصور:

شكل 1 _____ *قاعدة بيانات فيها كلمة فايروس*

شكل 2 _____ *صورة كرتونية لفيروسات*

شكل 3 _____ *حاسوب مصاب*

شكل 4 _____ *أضرار الفيروسات*

شكل 5 _____ *أنواع الفيروسات*

شكل 6 _____ *مكافحة الفيروسات*

شكل 7 _____ *Bitdefender 13 AVP*

شكل 8 _____ *مكافحات الفيروسات*

شكل 9 _____ *إحصائيات AV-Test*

شكل 10 _____ *معالجة الحاسب*

شكل 11 _____ *الكمبيوتر المحمي السليم*

شكل 12 _____ *جدار الحماية*

الفهرس الرئيسي:

المقدمة _____ 1

الفهرس _____ 2

الفصل الأول: الفيروسات: _____ 3-8

الباب 1: التعريف بالفيروسات _____ 3

الباب 2: مبدأ وأجزاء الفيروس _____ 4

الباب 4: العدوى بالفيروسات وتأثيرها _____ 4-6

الباب 5: أنواع الفيروسات _____ 7-8

الفصل الثاني: الحماية من الفيروسات: _____ 9-12

الباب 1: التعريف بمكافح الفيروسات _____ 9

الباب 2: أنواع المكافحات _____ 10

الباب 2: ما الأفضل؟ _____ 11

الفصل الثالث: حماية الحاسب: _____ 12

الباب 1: إجراءات حماية الحاسب _____ 13

الفصل الأول: الفيروسات

1) ما هو فايروس الحاسب؟[1]

هو عبارة عن برنامج صغير مكون من شيفرة وبالأغلب هذه الشيفرة تكرر نفسها للقيام بأضرار أكبر و تتم برمجته بغرض الحاق الضرر بجهاز الكمبيوتر والانتقال من جهاز كمبيوتر الى اخر، وايضاً يقوم بنسخ نفسه داخل جهازك، ويتداخل مع نظام التشغيل الخاص بالكمبيوتر، وسمي بهذا الاسم لأنه يشبه الكائنات المتطفلة في صفتين:

- اولاً: الفيروسات تستتر دائماً خلف ملف آخر ولكنها تأخذ زمام السيطرة على البرنامج المصاب بحيث أنه حين يتم تشغيل البرنامج المصاب يتم تشغيل الفيروس أيضاً.
- ثانياً: تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة رام مثلاً وتصيب أي ملف يشغَّل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة كلما طال وقت اكتشاف الفيروس.
- تستخدم عادة لغة التجميع (الأسمبلي)لكتابة كود الفايروس أو بلغات برمجة شهيرة كالـ c++ و #cأو على برنامج notepad++.

شكل 1

2) لماذا صنعت الفيروسات؟[2]

- تكون مصممة لأهداف مختلفة .معظمها تندرج تحت الفئات التالية :

- للسيطرة على جهاز الكمبيوتر واستخدامه لأداء مهام محددة
- لتوليد المال
- لسرقة معلومات حساسة (أرقام بطاقات الائتمان وكلمات السر وتفاصيل الشخصية، والبيانات وغيرها)
- لإثبات المهارة أو لأغراض الانتقام
- لتعطل جهاز كمبيوتر أو شبكة
- أهداف تجارية كبعض شركات مكافح الفيروسات التي تصنع الفيروسات مما يضطر المستخدمين لشراء المكافح من عندها للتخلص منها.

3) ما مبدأ عمل الفيروس؟وممَّ يتكون؟

[1] university of Hawaii An Introduction to Computer Viruses GEN008 بتصرف

[2] http://www.technibble.com/why-do-people-create-computer-viruses/

بما أن الفايروس برنامج فهو مجموعة من التعليمات أو شيفرة والبعض منها تكرر نفسها لتملأ الحاسب وتلحق الضرر به وبعضها تدخل نفسها داخل رسائل البريد الإلكتروني لتنتقل عبر الإنترنت او تنسخ نفسها إلى وسائط التخزين من مستخدم على آخر.

4) يتجلى عمل الفيروس من خلال أربع آليات:[3]

- آلية التناسخ: وهو الجزء الذي يسمح للفيروس بأن ينسخ نفسه.
- آلية التخفي: وهو الجزء الذي يخفي الفايروس من أن يُكتشف.
- آلية التنشيط: وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف المستخدم بوجوده كاستخدام توقيت الساعة في الحاسب.
- آلية التنفيذ: وهو الجزء الذي ينفذ الفايروس عندما يتم تنشيطه.

5) كيف تنتقل الفيروسات؟

كما ذكرت أن الفايروس ينسخ نفسه إلى رسائل البريد الإلكتروني أو وسائط ووحدات التخزين فإنه عندما تفتح رسالة مصابة بالبريد الإلكتروني أو تضع وحدة تخزين مصابة في الحاسب فإنه سينسخ نفسه إلى الحاسب ويصبح حاسبك مصاباً وبشكل عام الفيروسات تصيب الملفات المشفرة غير النصية او الملفات ذاتية التنفيذ التي يكون امتدادها .exe، com في أنظمة الويندوز والدوز، وفي أنظمة اللينوكس. Elf وقد تصيب ملفات الأوفيس وورد والإكسل وملفات القراءة المحمولة pdf والملفات المضغوطة rar, zip.

ونميز نوعين للفيروسات من حيث آلية العدوى:

– (Direct Infector) فيروس العدوى المباشر: عندما يتم تنفيذ برنامج مصاب بهذا النوع من الفيروسات, فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه وعندما تصاب أحد الملفات بالعدوى فإنه يقوم بتحميله على الذاكرة وتشغيله ولكن هذا النوع قليل الانتشار.

–(Indirect Infector) فيروس العدوى غير المباشر :عندما يتم تنفيذ برنامج ما مصاب بفيروسات بهذا النوع فإن ذلك الفيروس سينتقل إلى ذاكرة الحاسوب ويستقر فيها ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس كل برنامج يتم تحميله إلى الذاكرة بعد ذلك, إلى أن يتم قطع التغذية الكهربائية عن الحاسب أو إعادة تشغيله.

---

3 http://www.F-Secure.com/ Computer Viruses – From an Annoyance to a Serious Threat White Paper September 2001 بتصرف

6)كيف أعرف إن كان الحاسوب مصاباً بالفيروسات؟(ما أعراض إصابة الحاسب بالفيروسات؟)[4]

حسناً بما أنه واقعاً لكل للأمراض أعراض وعندما يصاب الحاسب بالفيروسات أيضاً فتظهر عليه اعراض ومنها:

شكل 2

- ✓ تغير في حجم وعدد الملفات
- ✓ عرض رسائل فجائية ومتكرر.
- ✓ تغير في وظائف لوحة المفاتيح
- ✓ اقلاع بعض البرامج بصورة تلقائية.
- ✓ تثبيط عمل بعض البرامج التطبيقية.
- ✓ اختفاء ملفات وظهور أخرى غريبة.
- ✓ إعادة تشغيل الحاسب بصورة الزامية
- ✓ فقدان تعريفات بعض الاجهزة الموصولة بالحاسب.
- ✓ بطء في اقلاع نظام التشغيل وعند تشغيل البرامج التطبيقية.
- ✓ تكرر رسائل الخطأ عند إقلاع نظام التشغيل وعند تشغيل البرامج التطبيقية.

[4] http://www.almajd.ps/?ac=showdetail&did=4623
3/1/2015

7) ما تأثير الفيروسات عل كل من الحاسب والمستخدم؟

شكل 3

طبعاً للفيروسات أنواع وكل نوع يقوم بأضرار معينة ولكن بشكل عام

تؤثر اغلب الفيروسات في الحاسب تأثيراص ملحوظاً ونلاحظ ما يلي:[5]

- ✓ نقص شديد في الذاكرة :بعد أن يبدأ الفيروس في العمل يلاحظ نقص شديد في الذاكرة. وذلك لأن الفيروس في هذه الحالة يبدأ في تدمير الذاكرة وكذلك ملفات التبادل Swap Files عن طريق إزالة البيانات المخزنة، مما ينتج عنه توقف البرنامج العامل في الوقت ذاته لعدم وجود أي بيانات في الذاكرة، وإنما يستبدلها الفيروس بمجموعة من الأصفار في مكان تعليمات التشغيل.
- ✓ بطء تشغيل النظام بصورة مبالغ فيها.
- ✓ عرض رسائل الخطأ بدون أسباب حقيقية.
- ✓ تغيير في عدد ومكان الملفات وكذلك حجمها بدون أي أسباب منطقية.
- ✓ الخطأ في استخدام لوحة المفاتيح عن طريق إظهار أحرف غريبة أو خاطئة عند النقر على حرف معين.
- ✓ توقف النظام بلا سبب.
- ✓ استخدام القرص الصلب بطريقة عشوائية. وتستطيع أن تلاحظ ذلك من إضاءة لمبة القرص الصلب حتى وإن كان لا يعمل.
- ✓ اختلاط أدلة القرص أو رفض النظام العمل منذ البداية.

شكل 4

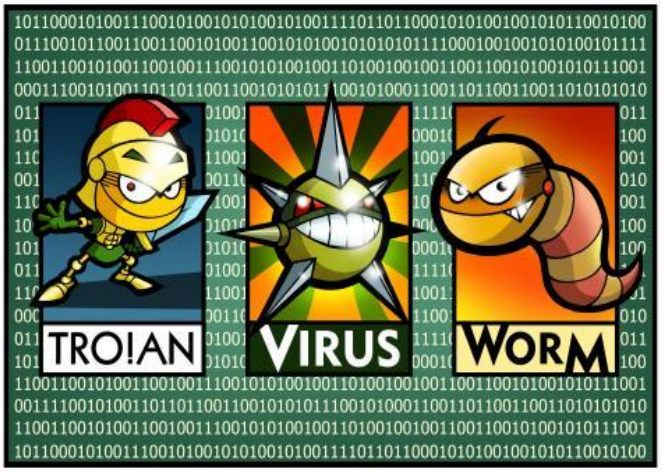
8) ما أنواع الفيروسات؟

طبعاً يجب أن ننوه إلى أنه لكل نظام تشغيل فيروسات تختلف عن الآخر قد يكون لها نفس طريقة العمل لكن لا يوجد فايروس مثلا يعمل على اللينوكس والويندوز في آن واحد والجدير بالذكر أن نظام التشغيل ويندوز هو النظام الذي تعمل عليه أغلب الفيروسات لانتشاره أكثر من باقي الأنظمة على مستوى العالم، بالنسبة لنظام التشغيل لينوكس يوجد 60 نوع تقريباً من الفيروسات ولا تتسبب بأضرار كبيرة كالفيروسات التي على نظام ويندوز التي تعد بالآلاف.

بعض أنواع الفيروسات على نظام التشغيل ويندوز:

[5] dkordy/tags/6108/posts#http://kenanaonline.com/users/ahmedkordy/posts/323682
3/1/2015

1. **الديدان (Worms)**: وهي عبارة عن برامج تكتب لكي تقوم بتخريب بيانات ومعلومات معينة وتوجد الكثير من برامج الديدان المنتشرة وتلك الأنواع من الديدان ليست لها القدرة على الانقسام.



شكل 5

2. **أحصنة طروادة (Trojan Horses)**[6]:يعتقد كثير من المستخدمين أنه برنامج مثل الفيروس والديدان، ولكنه اعتقاد خاطئ، ذلك أن هذه النوعية من البرامج لا تنقسم ولا تعمل نسخاً أخرى لنفسها وهي تشابه القصة اليونانية (حروب طروادة)، وهذه البرامج تقوم بجذب انتباه المستخدم وهي عادة تحوي على عدة رسوم بيانية وهي تستخدم للقيام بعمل ما في الحاسب محدد من قبل ويكون مختبأً في لعبة أو برنامج ما.
3. **التروجان المخبئ/الخلفي(Backdoor Trojan)**:هذا النوع من الفيروسات ليش كفيروس حصان طرواده بل يعتبر أداة تجسس يستخدمها الهاكرز للسيطرة على الحاسب عن بعد من حواسيبهم باستخدام البروتوكولات في الشبكة ويتيح هذا الفيروس للمخترق أن يتحكم بالملفات أو يستلم قيادة الحاسب أو يسحب كلمات السر او يعدل بإعدادات النظام أي أنه يستخدم لاختراق الحواسيب وهناك برنامج NetBus مثلاً الذي يقوم بصناعة هذا النوع من الفيروسات وعندما فتح هذا الفيروس يتيح للمخترق التحكم بالضحية عن طريق بعض الخيارات في البرنامج.
4. **فيروسات الكتابة فوق :(Write on Viruses)** تقوم هذه الفيروسات بإصابة الملفات والكتابة والتعديل عليها وتخريبها والحل في هذه الحالة حذف الملفات المصابة أيضاً مع الفيروس عند التخلص منه وهذا طبعاً يؤدي على فقداننا للملفات الاصلية.
5. **فيروسات الماكرو(Macro viruses)** : فيروسات تستخدم لغة برمجة ماكرو خاصة بتطبيق لتوزيع نفسها . وحدات الماكرو هذه لديها القدرة على إلحاق الضرر للمستند أو للبرامج الأخرى على الكمبيوتر .يمكن أن تصيب هذه الفيروسات ملفات Word بالإضافة إلى أي تطبيق آخر يستخدم لغة الماكرو.
6. **فيروسات الإقلاع :(Boot Viruses)** هذا الفيروس يصيب محرك الأقراص المرنة والقرص الثابت وهذا من شأنه جعل الكمبيوتر غير قادر على الإقلاع، يمكن تجنب هذه الفيروسات عن طريق ضمان أن الأقراص المرنة والقرص الصلب محمية بشكل جيد وبدء تشغيل جهاز الكمبيوتر باستخدام محرك الأقراص غير معروف أو قرص مرن.

---

[6] Computer Viruses – from an Annoyance to a Serious Threat
F-Secure Corporationبتصرف.

7. **الفيروسات الخفية :(Stealth Viruses)** تعتمد هذه الفيروسات على تقنيات عدة لتجنب اكتشافها من قبل برامج الحماية من الفيروسات، مثل توجيه رؤوس القراءة في القرص الصلب إلى منطقة أخرى لقراءتها بدلا من قراءة القطاع الذي يحتوي على الفيروس من القرص الصلب.
8. **فيروس الأوتورن(Auto run virus)** : يعد هذا النوع أكثر أنواع الفيروسات تسبباً بالأضرار حيث أنه يعتمد على خاصية التشغيل التلقائي في الويندوز ليقوم بإخفاء الملفات أو إغلاق وفتح نوافذ وغالباً يصيب هذا الفايروس وسائط التخزين والأقراص على الحاسب.
9. **فيروس الخدعة(Hoax Virus)** : يقوم هذا النوع من الفيروسات بعد أن يصيب الحاسب بإعطاء رسائل الأخطاء في النظام وأن الكمبيوتر معطل أو به خطب أو مشكلة ما، هذا الفيروس ليس خطيراً بل هو فقط يوجد لإزعاج المستخدم وقد نسأل لماذا تم عدُّهُ من الفيروسات؟ وهذا بسبب كما ذكرنا سابقنا أنه يعطيك إنذارات مزعجة وليس لها سبب.
10. **فيروس المزحة(Joke virus)** : يتم تصميم هذا الفيروس من أجل القيام بأشياء يعتبرها مبرمج الفيروس مضحكة أو مسليّة وليس له أضرار على النظام ولكن الهدف منه التسلية وإزعاج المستخدم.
11. **فيروس استقرار الذاكرة(Memory resident virus)** : يستقر هذا الفيروس في الرام ما دام الكمبيوتر يعمل وهذا يوصله إلى البرامج الخلفي التي تعمل وإحداث الاضرار فيها.
12. **الفيروسات متعددة الأجزاء (Multipartite Viruses)**: سمي هذا النوع من الفيروسات بهذا الاسم لأنه يقوم بمهام عدة في نفس الوقت أي يمكننا اعتبار هذا النوع وأنه نوعان في واحد فتقوم هذه الفيروسات بإحداث الضرر لكل من قطاعات الإقلاع في الحاسب والبرامج من نوع 16 بت.
13. **الفيروس المخفي (Polymorphic Virus)**: هذا النوع من الفيروسات يقوم بالتعديل على شيفرته لكي لا يكتشفه المكافح ويبقى مخفياً وغير معروف بوجوده.

الفصل الثاني: الحماية من الفيروسات

شكل 6

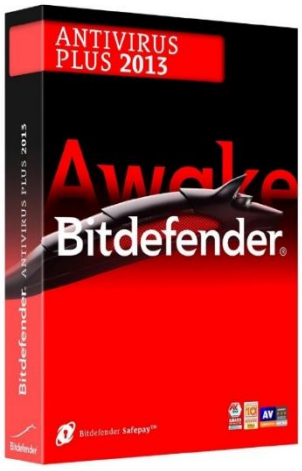
حسنا بعد قراءتنا لمخاطر الفيروسات وانواعها سيخطر ببالنا ما الحل لهذه الأخطار التي تصيب الحاسب؟

كما يُقال لكل داء دواء وبما أن الفيروسات داء للحواسب فيوجد لدينا الدواء أيضاً ألا وهو مكافح الفيروسات.

1) ما هو مكافح الفيروسات؟

[7]هو برنامج يقوم بالقضاء على الفيروسات وتعطيل أعمالها المُضرَّة بالحاسب.تقوم هذه البرامج بعمل مسح للملفات على الحاسب والعثور على الفيروس إن وجد من خلال مطابقة اسمه أو شيفرته مع الاسماء الموجودة في قاعدة البيانات الخاصة بالمكافح وتعطيل عمل الفيروس من خلال ثغرة موجودة داخل شيفرة الفايروس أو من خلال مسحه نهائياً دون رجعة لضمان عمل الحاسب دون أعطال فيروسية.

يمكننا الحصول على المكافح من خلال شرائه إذا كان مدفوعاً أو يمكننا تحميله من الإنترنت إذا كان مجانياً.



شكل 7

2) بعض مكافحات الفيروس:

- Kaspersky:وهو مكافح فيروسات روسي صنع من قبل أوجين كاسبرسكي ويعد من أفضل المكافحات وهو لشركة كاسبرسكي لاب.
- Bitdefender: مكافح فيروسات روماني الأصل شعاره تنين.
- Avira:مكافح فيروسات ألماني شعاره مظلة
- Symantec
- ESET
- Avast: مكافح فايروس ألماني توفر منه نسخة مجانية وأخرى مدفوعة.
- Microsoft Security Essentials:مكافح فيروس من شركة مايكروسوفت
- MC Afee

شكل 8

3) من المؤكد أنه بعدما رأيت كل هذه المكافحات ستسأل ما الأفضل أو ما تقييم كل مكافح؟[8]

---

[7] 9/1/2015
http://www.microsoft.com/en-gb/security/resources/antivirus-whatis.aspx

[8] http://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software
9/1/2015

هذا السؤال المتداول في أيامنا وخصوصاً من يصاب حاسبه كثيراً بالفيروسات ويخسر ملفات ويقوم بعمل فورمات وما إلى ذلك المهم أنه يلجأ إلى مكافح الفيروس هذه خطوة صحيحة لكن لها شروطها فيسأل من حوله ما المكافح الأفضل؟، في الحقيقة لا أحد يعلم ما المكافح الأفضل لأنه كل سنة تنزل نسخة جديدة وبالتالي كل سنة من الممكن أن يتفوق مكافح على آخر مع أن ذاك الآخر كان أفضل من ذاك السنة التي قبلها ويعود ذلك أيضاً إلى أن كل مكافح يجدد قاعدة بياناته التي تحوي أسماء الفيروسات كل فترة معينة ومع التحديث فإنك مكافحك يحصل على الأسماء الجديدة للفيروسات , لكن لا تقلق فهناك شركات ومواقع تقوم باختبار المكافحات وتقييمها من عدة جوانب كتأثيرها على سرعة وأداء الحاسب وشموليتها للفيروسات و... إلخ.

شكل 9

مثلاً الموقع المشهور في هذا المجال AV-Test

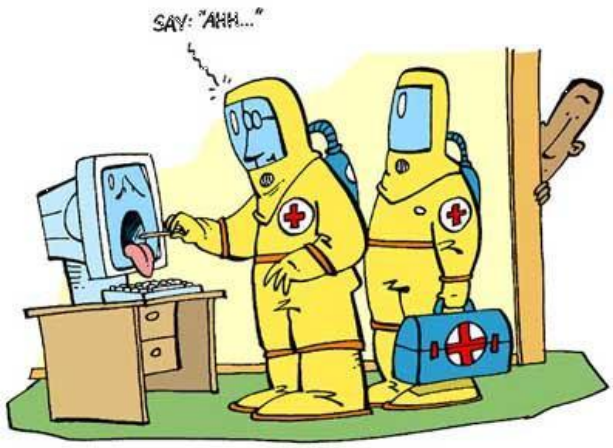
فمثلاً في الشكل المجاور 10 يصنف لنا الموقع أداء المكافحات مع الويندوز سيفن بعد تجريبها بشهر آب 2014 من حيث الحماية والأداء (ليست مرتبة) وعليك الانتباه على أنه ليس عليك التركيز على الحماية بل عليك التركيز أيضاً إن كان هذا المكافح كما يقولون ثقيلاً على الحاسب الذي تملكه حسب مواصفات حاسبك طبعاً لذا عليك أن تختار ما هو مناسب للحاسب وحسب ما إذا كنت تريده لحاسب العمل أو للمنزل وتكون حمايته قوية وأنصحك بالاطلاع على هذا الموقع قبل شرائك لمكافح الفيروسات.

الفصل الثالث: حماية الحاسب

طبعاً[9] الفيروسات كالبرامج تتطور وتصبح أقوى وكل فترة تزداد أنواع هذه الفيروسات وتعتبر مكافحات الفيروسات الجزء الأكبر من الحل ولكن مع ذلك علينا القيام ببعض الإجراءات التي تساهم في حمايتنا من الإصابة بها ومنها:

[9] http://windows.microsoft.com/en-us/windows/how-protect-computer-from-viruses#how-protect-computer-from-viruses=windows-7
http://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer

1. تثبيت مكافح فيروسات قوي ويفضل أن تكون النسخة أصلية ومدفوعة وتجنب المكافحات المجانية وكما ذكرت هذا هو الجزء الأكبر من الحل.
2. التحديث الدوري للمكافح وبرامج الأوفيس (لأنه كل يوم يعدل على الفيروسات وتبرمج أنواع جديدة ويمكن أن تلتصق بملفات الأوفيس)



شكل 10

3. عدم فتح الصفحات في المواقع غير معروفة أو غير الأخلاقية أو المنتديات التي يكثر فيها المتطفلون أو الروابط المباشرة أو الرسائل التي ترسل إلى البريد الإلكتروني من مصادر غريبة وغير معروفة من قبل أو غير موثوقة
4. نسخ الملفات إلى أكثر من مكان لتجنب فقدانها عند الإصابة بالفيروسات.عدم وضع الفلاشات أو الأقراص الليزرية غير الموثوقة في الحاسب وعند الضرورة عدم فتحها إلا بعد فحصها بمكافح الفيروسات.

شكل 11

5. التأكد من تشغيل جدار الحماية من لوحة التحكم لتجنب الفيروسات التي تأتي من الإنترنت والشبكات.
6. الفحص الدوري لملفات ومجلدات وأقراص الحاسب وخصوصاً القرص المتواجد عليه ملفات النظام للكشف عن إصابة الحاسب بالفيروس بوقت أقصر مما يجنب أن يصاب الحاسوب بأضرار كبيرة.

شكل 12

طبعاً هذه هي الإجراءات التي يمكننا القيام بها لنحمي حواسبنا ما أمكن من الفيروسات ومع تطور التكنولوجيا تتطور الفيروسات أيضاً يوماً بعد يوم ولكن لا تقلق فهناك شركات المكافحات الموجودة لرصد هذه الفيروسات وإيجاد الحلول للقضاء عليها.....،أتمنى أن أكون قد قدمت لكم الفائدة في هذه الحلقة لتعزيز أمان الحواسيب والقضاء على أبرز أسباب عطل الحواسيب.