الفصـــــل الخـــامس

مكافحات الفيروسات وبرامج الحماية

في هذا الفصل سوف نتعرف مكافحات الفيروسات وأهميتها في حماية الحاسوب حيث أصبحت ضرورة لا غنى عنها وبدونها فجهازك بكل تأكيد معرض لأضرار هذه الفيروسات وبالتالي تعطله على الدوام ، لذا لا استغناء عن برامج مكافحات الفيروسات .

ما هو الفايروس؟

الفيروس (virus) يمكن تشبيهه بمرض معدي يصيب الإنسان ويحتاج للمضاد الحيوي للقضاء عليه وهذا المضاد الحيوي هو عبارة عن برامج مكافحه الفيروسات المنتشرة ومن أشهرها افيرا و الكاسبر سكاي و الأفاست والبتديفاندر والتي تقوم بالحد من انتشار الفيروس و تزيد من مناعة الجهاز في وجه البرامج والفيروسات الضارة .في العادة معظم الفيروسات تأتي على شكل ملف تنفيذي exe منتقلة من جهاز إلى جهاز آخر ، فهذا الفيروس يربط نفسه ببرنامج تطبيقي في الأغلب وأحيانا كثيرة بالصور وملفات الفيديو المشبوهة وعند تحميلها على الجهاز فهي لن تعمل إلا إذا قمت أنت بتشغيلها فأنت بذلك تعطيها الأمر لبداية عملها من حيث لا تعلم ويتفاوت ضرر كل فيروس عن الآخر حسب قوته وحجمه والغرض الذي أنشي من اجله فبعضها يدمر الهاردوير وبعضها يدمر بعض المهام الرئيسية البسيطة في الجهاز وبعضها يدمر الملفات والمستندات المهمة وبعضها يتلف الكروت .mother board والأخطر انهيار نظام التشغيل بالكامل وعدم عمل الجهاز بالكامل.

فللفيروس الحاسوبي Computer Virus بمعنى أدق عبارة عن برنامج Software مخفي لا يمكن رؤيته من خلال برامج الاستعراض كتب بعناية ليكون قادرا على الدخول إلى نظامك الحاسوبي بشكل سري Surreptitiously وقد يُصيبُ بعض ملفاتكَ بالأذى والتخريب أو قد يكتفي بعرض رسالة ما تلبث أن تذهب. عموما يمكن القول أن أي برنامج يهدف إلى إلحاق الأذى بأنظمة وملفات الغير يسمى فيروسا.

مراحل الإصابة:

مرحلة الكمون : حيث يختبأ الفيروس في الجهاز لفترة ..

مرحلة الانتشار : و يبدأ الفيروس في نسخ نفسه و الانتشار في البرامج وإصابتها و ووضع علامته فيها ..

مرحلة الأضرار : و يتم فيها تخريب الجهاز ..

أنواع الفيروسات:

أذا الفيروس ينتقل هنا بواسطة الإنسان من جهاز إلى جهاز آخر ويعمل بمجرد تشغيلها وأفضل بيئة لانتقال الفيروس هي البريد الالكتروني والمواقع الإباحية او المشبوهة.

فيروسات قطاع التشغيل Boot Sector Virus

وهو الذي ينشط في منطقة نظام التشغيل وهو من اخطر أنواع الفيروسات حيث انه يمنعك من تشغيل الجهاز .

فيروسات الماكرو Macro Virus

وهي من أكثر الفيروسات انتشارا حيث أنها تضرب برامج الأوفيس و كما أنها تكتب بالورد او Notepad

فيروسات الملفات File Virus

وهي تنتشر في الملفات وعند فتح أي ملف يزيد انتشارها ..

الفيروسات المخفية Steath Virus

وهي التي تحاول آن تختبئ من البرامج المضادة للفيروسات و لكن سهل الإمساك بها .

الفيروسات المتحولة Polymorphic virus

وهي الأصعب على برامج المقاومة حيث انه صعب الإمساك بها وتتغير من جهاز إلي آخر في أوامرها .. ولكن مكتوبة بمستوى غير تقني فيسهل إزالتها .

فيروسات متعددة الملفات Multipartite Virus

تصيب ملفات قطاع التشغيل و سريعة الانتشار ..

فيروسات الدودة Worm

وهو عبارة عن برنامج ينسخ نفسه على الأجهزة و يأتي من خلال الشبكة و ينسخ نفسه بالجهاز عدة مرات حتى يبطئ الجهاز وهو مصمم لإبطاء الشبكات و الأجهزة و بعض الناس تقول أن هذا النوع لا يعتبر فيروس حيث انه مصمم للإبطاء لا لأزاله الملفات و تخريبها ..

الباتشات Trojans

وهو أيضا عبارة عن برنامج صغير قد يكون مدمج مع ملف آخر للتخفي عندما ينزله شخص و يفتحه يصيب ال Registryو يفتح عندك منافذ مما يجعل جهازك قابل للاختراق بسهوله و هو يعتبر من أذكى البرامج فمثلا عند عمل scan هناك بعض التورجن يفك نفسه على هيئة ملفات غير محدده فيمر عليها scan دون التعرف علية ومن ثم يجمع نفسه مره ثاني

ما أعراض الإصابة بالفيروسات ؟

١. ظهور رسائل غريبة على شاشة حاسبك، او أصوات غريبة أو موسيقى صاخبة تنبعث من جهازك في أوقات متفرقة .

٢. كثرة ظهور رسائل انتهاء الذاكرة Run Out of Memory أو المساحة التخزينية لديك Low System Resources. ، تغيير اسم الجهاز التابع لك .

٣. عدم وجود تطبيقات كانت في السابق تعمل بجهازك .

٤. بطء الحاسب الآلي عن السرعة المعتادة، أو حدوث أخطاء غير معتادة عند تنفيذ البرنامج
٥. بطء الحاسب في أداء بعض المهمات البسيطة كان يأخذ وقتا طويلا في عملية حفظ وثيقة عبارة عن سطرين أو ثلاثة.
٦. زيادة حجم الملفات ، أو زيادة زمن تحميلها إلى الذاكرة.
٧. حدوث خلل في أداء لوحة المفاتيح كأن تظهر رموز مختلفة عن المفاتيح التي تم ضغطها كما في فيروس Haloechon أو حدوث قفل للوحة المفاتيح كما في فيروس .Edv
٨. نقص في مساحة الذاكرة المتوفرة كما في فيروس Ripper الذي يحتل 2 كيلو بايت من أعلى الذاكرة الرئيسة .
٩. ظهور رسالة ذاكرة غير كافية لتحميل برنامج كأن يعمل سابقاً بشكل عادي
١٠. ظهور مساحات صغيرة على القرص كمناطق سيئة لا تصلح للتخزين كما في فيروس Italan وفيروس Ping Pong اللذين يشكلان قطاعات غير صالحة للتخزين مساحاتها كيلوبايت واحد
١١. تعطيل النظام بتخريب قطاع الإقلاعBOOT SECTOR
١٢. إتلاف ملفات البيانات مثل ملفات وورد واكسل ..... وغيرها.

كيف تنتقل أو تصيب الأجهزة:

- تشغيل الجهاز بواسطة اسطوانة مرنه مصابه.
- تنفيذ برنامج في اسطوانة مصابه.
- نسخ برنامج من اسطوانة مصابة بالفيروس إلى الجهاز.
- تحميل الملفات أو البرامج من الشبكات أو الإنترنت
- تبادل البريد الإلكتروني المحتوي على الفيروسات.(attachments)
- فلاشات الميموري .

الإجراءات الواجبة عند اكتشاف الإصابة بالفيروسات:

١. تصرف بهدوء وبدون استعجال لئلا تزيد الأمر سوءاً ولا تبدأ بحذف الملفات المصابة أو تهيئة الأقراص.
٢. لا تباشر القيام بأي عمل قبل أعداد وتدقيق خطة العمل التي تبين ما ستقوم به بشكل منظم أعد إقلاع جهازك من قرص نظام مأمون ومحمي وشغل أحد البرامج المضادة للفيروسات التي تعمل من نظام دوس ومن فلاشة ولا تشغل أي برنامج من قرصك الصلب.
٣. أفحص جميع الأقراص ببرنامج مكافح الفيروسات لعلاجها .
٤. في حالة عدم نجاحك في القضاء على الفايروس واستعادة النظام فعليك بخيارين وهما استعادة النظام باستخدام برامج ال باك أب أو الفرمتة والتحميل من جديد .

الوقاية من الإصابة بالفيروسات:

فحص جميع الأقراص الغريبة أو التي استخدمت في أجهزة أخرى قبل استعمالها.
عدم تنفيذ أي برنامج مأخوذ من الشبكات العامة مثل إنترنت قبل فحصه.
عدم إقلاع الكمبيوتر من أي قرص قبل التأكد من خلوه من الفيروسات.
عدم ترك الفلاشات في السواقة عند ما يكون الجهاز متوقفا عن العمل.
عدم تشغيل برامج الألعاب على الجهاز ذاته الذي يتضمن البيانات والبرامج الهامة.
استخدام برامج أصلية أو مرخصة.
استخدام كلمة سر لمنع الآخرين من العبث بالكمبيوتر في غيابك.
الاحتفاظ بنسخ احتياطية متعددة من جميع ملفاتك قبل تجريب البرامج الجديدة.
تجهيز الكمبيوتر ببرنامج مضاد للفيروسات واستخدامه بشكل دوري
تحديث البرامج المضادة للفيروسات بشكل دائم لضمان كشف الفيروسات الجديدة.
الاحتفاظ بنسخة DOS نظيفة من الفيروسات ومحمية ضد الكتابة لاستخدامها عند الإصابة.
الانتباه للفلاشات الواردة من المعاهد والكليات (الأماكن التقليدية للفيروسات).

أنواع المكافحات:

برنامج مكافح الفيروسات (Anti Virus)

وهو برنامج يحتوي على محرك بحث عن الفيروسات أو البرامج الخبيثة ويقوم بكشفها ومنعها من دخول الحاسب ثم حذفها بشكل نهائي مثل الديدان أو أحصنة طروادة أو برامج التجسس وغيرها من البرامج الخبيثة والمضرة بالنظام . اغلب برامج مكافحة الفيروسات تكون مزودة فقط بأدوات كشف وحذف الفيروسات وتفتقر لكثير من تقنيات الحماية ، بمعنى أن عملها محدود أو يقتصر على مهام محددة في عملية الحماية وينقصها بعض ألتقنيات ، وهي مناسبة لأصحاب الأجهزة ذات المواصفات البسيطة لخفتها على النظام .

برنامج حماية الانترنت (Internet Security)

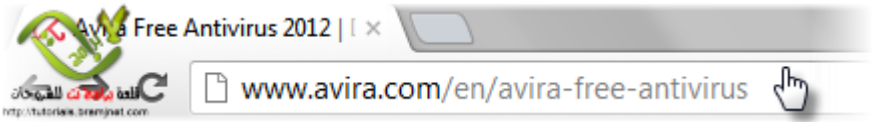
وهو برنامج يحتوي على جميع أدوات وتقنيات الحماية مثل مكافح فيروسات وجدار ناري وحامي مواقع الويب ويحتوي على بعض أدوات إصلاح النظام وأدوات النسخ الاحتياطي للنظام والتحكم في تشغيل التطبيقات ووضع صلاحيات عليها وغيرها من الأدوات الهامة ,
مما يجعله يحتاج إلى جهاز ذو مواصفات عالية لكي يعمل بكفاءة دون أن يؤثر على عمل المستخدم.

تحميل المكافحات وتشغيلها:

برامج الفيروسات كثيرة ومتنوعة تبعاً لكل شركة منتجة له وأشهر المكافحات :
Kaspersky , Avira , Avast , Nod , Norton , Bitdefender

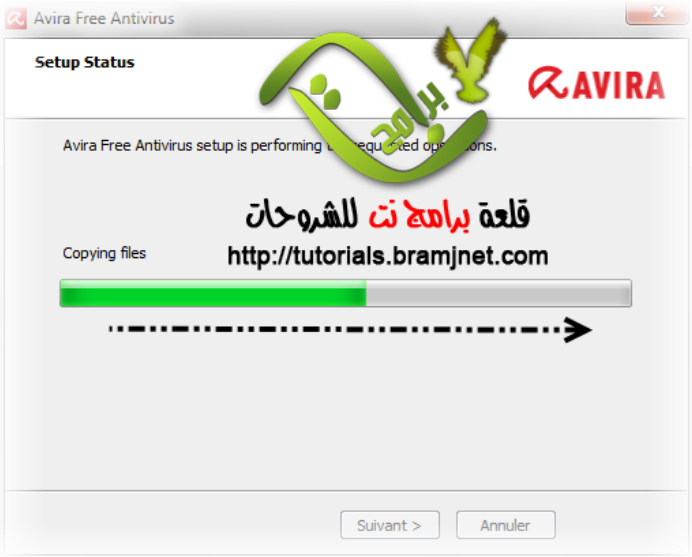
شرح برنامج Avira Free Antivirus المجاني

يمكنك تحميل البرنامج من أي أسطوانة شاملة البرامج أو من موقع الشركة كما هو موضح :



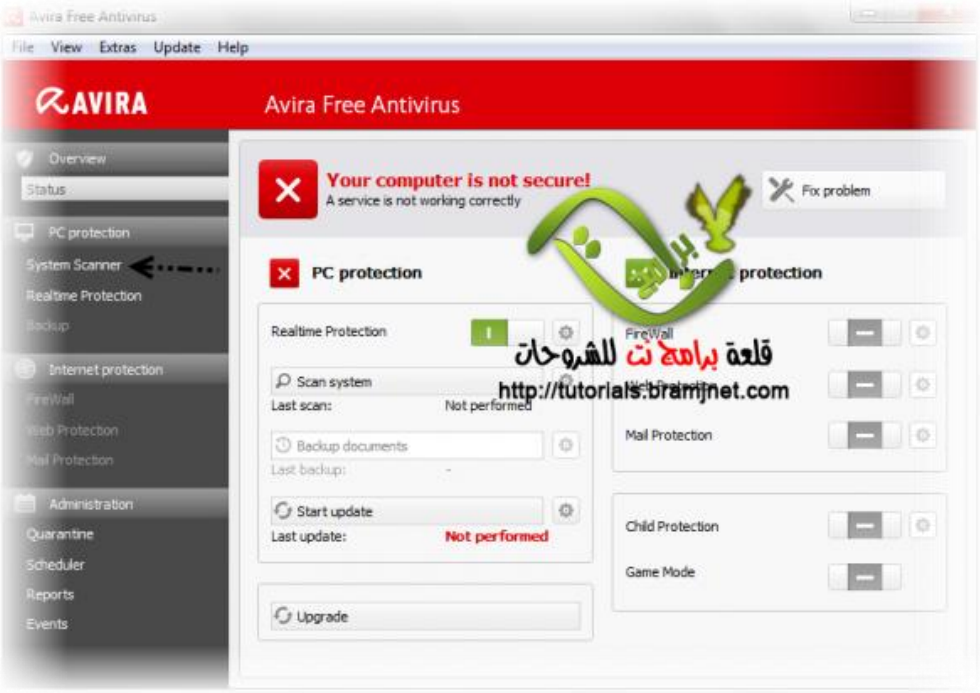
بعد تحميل البرنامج Avira free antivirus ونقله إلى سطح المكتب ، اضغط على أيقونة البرنامج مرتين لبدء التثبيت

طريقة التثبيت عادي قم بقراءة التعليمات واضغط Next …Next… Next



بعد تثبيت البرنامج ستظهر أيقونة صغيرة للبرنامج جنب الساعة اضغط عليها مرتين ليفتح البرنامج

واجهة البرنامج Avira Free Antivirus ، اضغط على System Scanner من القائمة الفرعية لفحص الجهاز من الفيروسات. كما يمكنك عمل التحديثات بالنقر على start update لكن عليك التأكد من توفر خط النت للاتصال وتنزيل التحديثات



كما ترى بدأت عملية فحص الجهاز كما هو مبين أدناه:

عند انتهاء الفحص اضغط على End لرؤية النتائج وعرضها تبين النتائج ما إذا تم القضاء على الفيروسات أو عمل حجر لها Quarantine .

شرح برنامج avast 2014 free edition المجاني حماية عالية

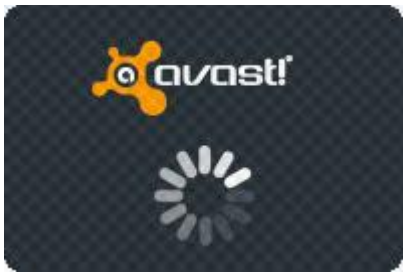
مميزات البرنامج

١. يحجز الفيروسات وبرامج التجسس .
٢. يسمح بالمساعدة من صديق ذو خبرة.
٣. يؤمن الخدمات المصرفية و التسوق.
٤. تشغيل البرامج الخطرة بأمان.
٥. يمنع هجمات القراصنة.
٦. يؤمن البيانات الشخصية .
٧. يوقف البريد المزعج .
٨. يمنع حيل التصيد .

طريقة التحميل

دبل كليك نضغط عليها .. التحميل هذه إيقونة البرنامج بعد

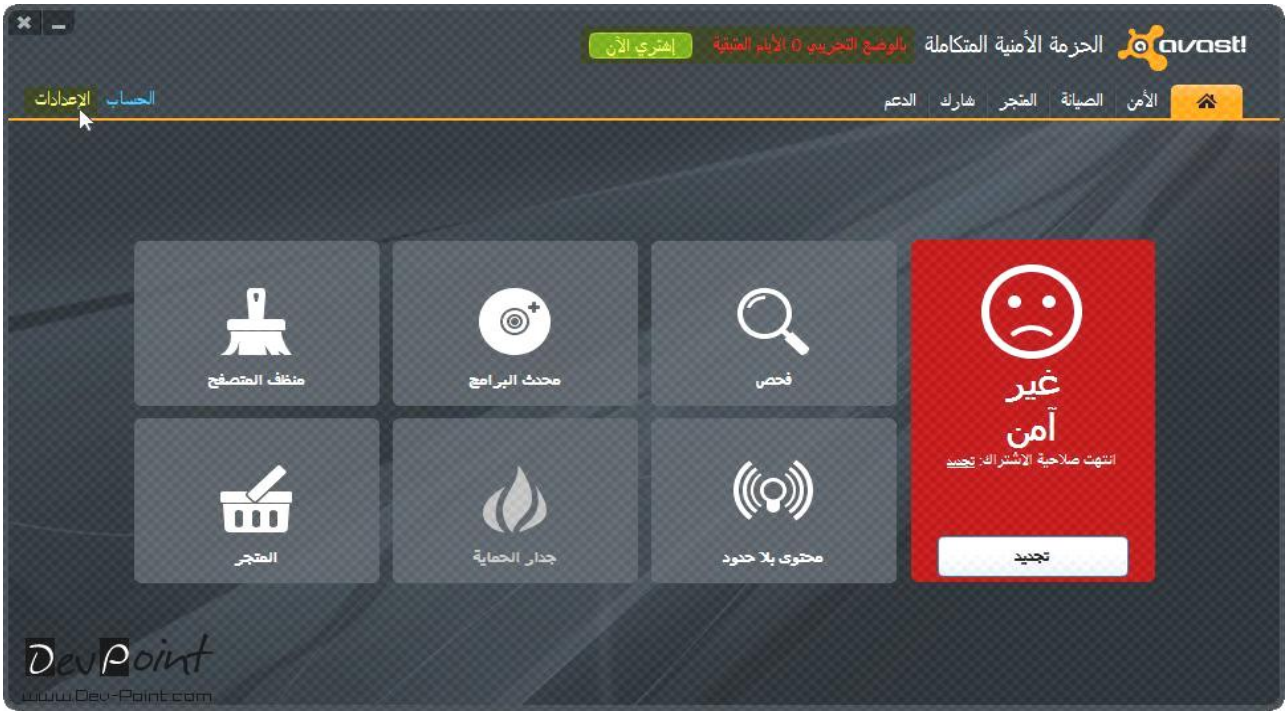
ننتظر شوي



نضغط على تركيب سريع وننتظر ، يجري التركيب

هذه واجهة البرنامج وتم تثبيته % 100 شغال بعد الانتهاء من التحميل وإعادة التشغيل تظهر رسالة نجاح التحميل لكن المشكلة أن البرنامج صالح لمدة 30 يوم فقط وهو تجريبي

نبدأ طريقة التفعيل:
أول خطوة ندخل إعدادات البرنامج من الاعلى تظهر نافذة بقوائم نختار منها آخر خيار (مستكشف الأخطاء)



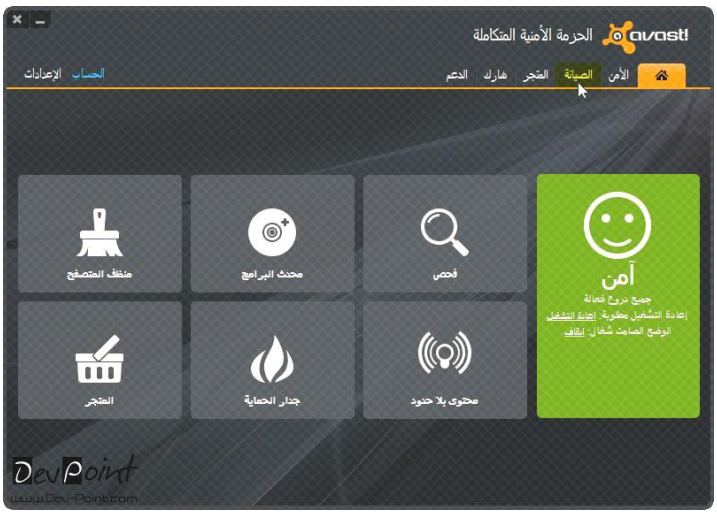
ونحذف التحديد عن الخيار الرابع والسابع .. الكل يتساءل لماذا ؟ .. الكراك هو عبارة عن ملف سرنسخه بمجلد تثبيت البرنامج وسيتفعل و الخاصية رقم7 + 4 لن تسمحلك بنسخ أي شيء او تستبدله بمجلد تثبيت البرنامج ..

الآن نقوم بتحميل الكراك

ندخل على ملف الكراك بعد فك ضغطه

سنلاحظ وجود ملفين .. أول ملف هو كراك للويندوز XP كل ماعليك فعله هو فتح الكراك ومتابعة تثبيته ... والملف الثاني هو كراك للويندوز 7 .. ننسخه ونروح لملف تثبيت البرنامج بـ C:\Program Files\AVAST Software\Avast ونعمله لصق

نقوم بعمل إعادة تشغيل ونرجع نفتح البرنامج من جنب الساعة ونرى إذا انضبط التفعيل.

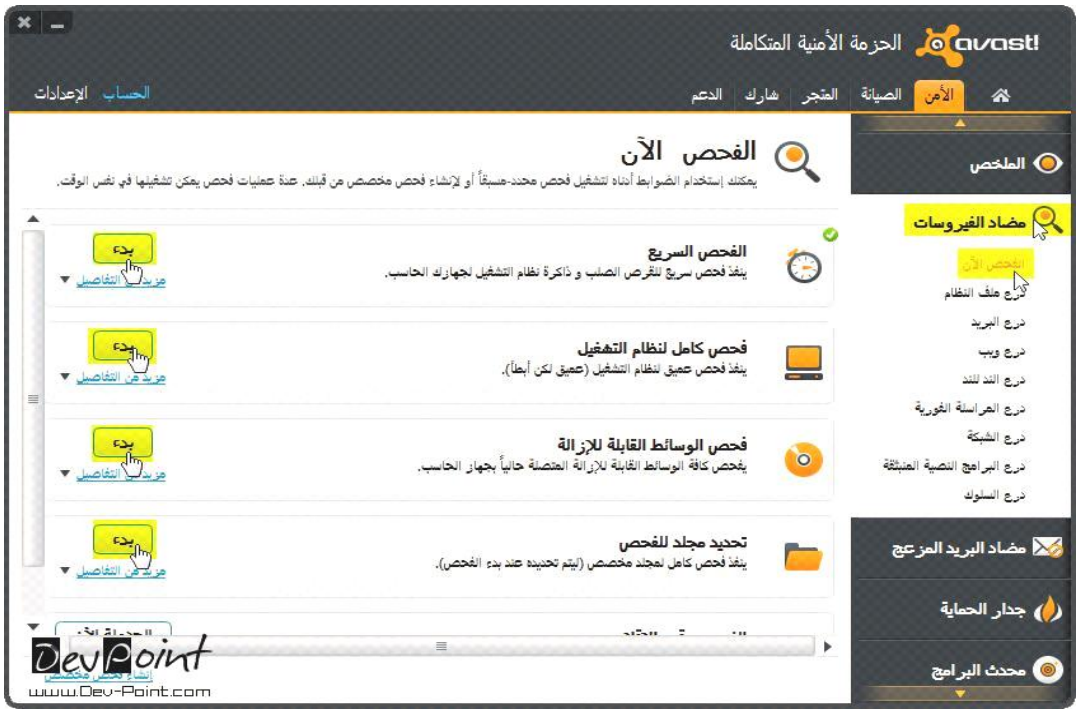


يمكننا أيضا معرفة مدة التفعيل / نختار صيانة / بعدين الاشتراك ونرى

بعد التأكد من أن كل شيء تمام ، نعود نفعل الخيارات التي عطلناها في مستكشف الأخطاء. سنلاحظ أن هناك عدة قوائم وهي (الأمن – الصيانة – المتجر – شارك – الدعم) نقوم بالنقر على قائمة (الأمن) الأولى سنلاحظ وجود عدة خيارات :

الخيار الأول الملخص : وفيه الإحصائيات العامة للفحص عن درع النظام ، درع الويب .... الخ.

الخيار الثاني مضاد الفيروسات: وفيه عمليات الفحص أول خيار ..هذا الخيار لفحص الكمبيوتر من الفيروسات / وموجود فحص سريع ليس شامل لكل شيء / وفحص بطيء شامل لكل شيء / وفحص للأقراص القابلة للإزالة) الفلاش ميموري (او ممكن نحدد مجلد ونفحصه / فقط للفحص نضغط على البدء)



كما توجد خيارات (درع ملف النظام – البريد – الويب – الشبكة ... الخ) ، يمكنك تفعيل الدرع وإيقافه من خلال الضغط على زر إيقاف / تشغيل في كل منها وهي الحماية الآنية. كما يمكنك الدخول إلى إعدادات أي منها والتحكم في أسلوب الفحص لكل درع.

الخيار الثالث (مضاد البريد المزعج) يستخدم لتصفية البريد المزعج والغير مرغوب فيه يمكن التحكم فيه وإيقافه وكذا الدخول بالإعدادات لتغييرها.

الخيار الرابع (جدار الحماية) يستخدم لحماية الجهاز من الاختراق ، يمكن التحكم فيه وإيقافه وكذا الدخول بالإعدادات لتغييرها.

الخيار الخامس (محدث البرامج) : توجد به خاصية تحديث البرامج يمكنك من خلاله تحديث البرامج المحتاجة لتحديثها كـ Adobe flash player وغيرها ، انقر على تبويب التحديثات واختر البرنامج الذي تود تحديثه بعدها انقر على تحديث.

ا

الخيار السادس(الاتصال الأمن) : لإنشاء اتصال في بي ان ويجعلك امن على الشبكة .. للاتصال نضغط على اتصال .

الخيار السا بع(الأدوات) : وفيها أدوات خدمية ممتازة كتنظيف المتصفح من الملفات غير الضرورية وكذا صندوق الاختبارات لاختبار وفحص أي ملف كما توجد به خاصية حجر المواقع لحظر أي موقع من الدخول إليه.

تحتوي قائمة (الصيانة) أيضا على عدة أوامر هامة وهي :

الخيار الأول التحديث : وهو مهم وتستخدمه من فترة إلى أخرى لتحديث البرنامج وتحميل الملفات الجديدة لإبقاء البرنامج مواكبا لتطورات الفيروسات .

كما توجد خيارات أخرى كمعلومات الاشتراك وسجلات الفحص التى قمت بها والفيروسات المحجورة ومعلومات كاملة عن برنامج أفاست.

أدوات إزالة الفيروســـــات

هناك العديد من الأدوات الخفيفة التي تتميز بإزالة الفيروسات الشائعة كالأوترن وغيرها كما هناك أدوات تقوم بإصلاحات الريجستري وكذا إظهار الملفات المخفية ومن هذه الأدوات حماية الكمبيوتر من الفلاشات حاملة الفيروسات وهو برنامج USB Security 6 ويفضل تحميله مع مكافح الفيروسات ليعطي حماية مضاعفة لجهاز الحاسوب ، بعد تحميل البرنامج تظهر نافذة البرنامج ، الشرح مع الصور لكل تبويب من القائمة الجانبية كما يلي:


USB Disk Security
Your computer is protected
Help
Settings
Protection Status
USB Shield
USB Scan
Data Protection
System Tools
Quarantine
USB Shield
Monitor in real time and protect your computer against all threats that can take over your computer via USB drive.
Threat
State
ملاحظة مهمة :
اذا اخترت delette all يعني سيقوم بمسح الفيروسات كاملة مع بعضها
لكن ان وجدت بقرب فيروس delette failed أعد نفس العملية حتى يكتب
لك بجانب كل فيروس delette.
و قم باختيار كل فيروس بالضغط عليه عليه و ضغط بعدها delette فيروس
وضع العلامة يعني مسح أوتوماتيكي للفيروسات و هي خاصية ممتازة.
Delete threats automatically
مسح الفيروس
Delete
مسح كل الفيروسات
Delete All
Safe Open
Recommended way to open your USB drives. Safe Open lets you safely open your USB drives without running virus.
فتح usb دون الحاجة لفحصه، أو فتحه بالقوة في حالة لم تستطع فتحه


USB Disk Security
Your computer is protected
Help
Settings
Protection Status
USB Shield
USB Scan
Data Protection
System Tools
Quarantine
USB Scan
Scan your USB drives for the presence of threats.
Threat
State
فحص
أمر بالتوقف
مسح
مسح الكل
Scan
Stop
Delete
Delete All
USB Vaccine
تلقيح جهاز الكمبيوتر و ال usb. بالضغط عليها تجد :
Disable autorun feature on your PC and USB drives to avoid some malware infections.


vaccine : تعني ان البرنامج يقوم بانشاء autorun مخفي خاص به في جهاز الكمبيوتر و هو غير مؤذي دوره أنه يمنع الفيروس autorun الحقيقي من الدخول للجهاز واهما اياه أن الفيروس موجود من قبل داخل الجهاز.
Settings
Protection Status
USB Shield
USB Scan
Data Protection
System Tools
Quarantine
Computer Vaccination
Vaccinating your computer can prevent some malware from auto-executing on your computer from USB drives.
لمن يريد يقوم بالضغط هنا
Computer not vaccinated
Vaccinate Computer
USB Drive Vaccination
Vaccinating your USB drive can prevent you from inadvertently transmitting malware to/from other computers where you insert your USB drives.
لمن يريد يقوم بالضغط هنا لل usb
Remove Vaccine
Vaccinate USB
لمن لم يعجبه الأمر يمكنه نزعه عن طريق remove vaccine .
Scan
Stop
Delete
Delete All
USB Vaccine
Disable autorun feature on your PC and USB drives to avoid some malware infections.


USB Disk Security
Your computer is protected
Help
Settings
Protection Status
USB Shield
USB Scan
Data Protection
System Tools
Quarantine
Data Loss Prevention
Provide high level of protection against theft and accidental disclosure of confidential data.
USB Access Control
منع أي شخص غير مرخص له بأن يسرق معلوماتك
Prevent unauthorized persons from copying your data to USB drives.
Lock
USB Drive Control
منع أي شخص غير مرخص له لايصال usb بالكمبيوتر و توقيف مسح الفيروسات منه.
Prevent unauthorized persons from connecting USB drives to your computer, and stop any threats from USB drives.
Lock
بالضغط على الخاصيتين السابقتين تظهر لك أيقونة بكلمة سر و تأكيدها لتفعيل الخاصية لكن أنصحك لا تنسى كلمة السر. أو تجنب الخاصيتين.
Password Settings
Old password:
New password:
Confirm password:
OK
Cancel

أدوات الفيروسات كثيرة وقد تجد أداة مخصصة لفيروس معين ، ومن الأدوات الرائعة أيضا أداة Zeezoom زيـــــزوم للقضاء على الفيروسات الشائعة وإصلاح الويندوز استعن بمدرب الدورة لاطلاعك على أدوات الفيروسات الهامة في الوقت الحالي .