أفاست! الحزمة الأمنية المتكاملة ٦.٠

دليل البدء السريع

أهلاً بكم بأفاست! الحزمة الأمنية المتكاملة ٦.٠

بني أفاست! مضاد الفيروسات ٦.٠ على منتجات الإصدار ٥.٠ التي أثبتت نجاحها ولكنه يحتوي الآن على عدد من الميزات والتحسينات الجديدة ، مثل أفاست! صندوق الاختبارات – التلقائي، ودعم كل من أنظمة التشغيل ٣٢ و ٦٤ بت. أفاست! الحزمة الأمنية المتكاملة مصمم للإستخدام في المكاتب المنزلية/ الصغيرة والشركات الصغيرة. أما بالنسبة للأعمال و الشركات الأكبر حجماً ، فنوصيكم بإستخدم منتجاتنا التي يمكن إدارتها و التحكم بها مركزياً ، يمكن الحصول على مزيد من المعلومات من موقع أفاست!.

إستناداً إلى الجوائز المتعددة التي حصل عليها محرك مضاد الفيروسات أفاست !، فإن برنامج أفاست! الحزمة الأمنية المتكاملة يتضمن تقنيات مضاد– برامج التجسس ، مصادق عليها من قبل مختبرات الساحل الغربي لعملية تدقيق العلامة ، وكذلك مضاد للجذور الخفية و حماية ذاتية قوية ، ولكنه ما يزال إلى الآن يقدم فحصاً أسرع مع تحسن بقدرات الكشف. كما يأتي الإصدار ٦.٠ الآن مع واجهة مستخدم تم إعادة تصميمها بشكل كامل لتأدية الفحص بسهولة.

إضافة إلى ذلك فإن أفاست! الحزمة الأمنية المتكاملة ٦.٠ يتضمن ما يلي :

- أفاست! المنطقة الآمنة – بيئة خاصة آمنة غير مرئية من بقية نظام التشغيل لديك يمكنك من خلالها إدارة معاملاتك الحساسة (كالمعاملات المصرفية) في بيئة آمنة و نظيفة.
- فاحص خط–موجه الأوامر – يسمح لكم بتشغيل الفحص حتى قبل بدء نظام التشغيل الخاص بجهازكم الحاسب.
- جدار الحماية – يوفر حماية إضافية ضد القراصنة/المتسللين.
- مصفي ضد البريد المزعج – يمنحكم المزيد من التحكم على بريدكم الإلكتروني.

مثل كل منتجات أفاست! مضاد الفيروسات ٦.٠ ، فإن أفاست! الحزمة الأمنية المتكاملة ٦.٠ يحتوي على عدة دروع بالوقت– الحقيقي التي ترصد باستمرار بريدكم الالكتروني و إتصالكم بالإنترنت و تتحقق من الملفات على جهازكم الحاسب كلما تم فتحها أو إغلاقها. بمجرد تركيبه ، فإن أفاست يقوم بعمله بشكل صامت لحماية جهازكم بإستمرار ضد تهديدات الفيروسات والبرمجيات الخبيثة الأخرى. إذا سار كل شيء على ما يرام ، فإنك لن تلاحظ أن أفاست! شغال – فقط ركب و إنسى !

مساعدة إضافية

يهدف دليل البدء السريع هذا الى إعطاءكم مجرد لمحة موجزة عن البرنامج وسماته الرئيسية. إنه ليس دليل شامل عن البرنامج. لمزيد من المعلومات التفصيلية حول البرنامج و إعداداته ، يرجى الرجوع إلى مركز التعليمات التي يمكن الوصول إليها من خلال واجهة البرنامج ، أو يمكنكم الضغط على مفتاح F1 لمشاهدة المعلومات المطلوبة عن الشاشة المفتوحة الآن.

إذا كنتم تواجهون أي صعوبة في إستخدام البرنامج ، و كنتم غير قادرين على حلها بعد قراءة هذا الدليل ، أو بمركز التعليمات بالبرنامج نفسه ، فقد تجدون الإجابة في مركز الدعم بأفاست!

- في قسم كنز المعرفة ، يمكنكم العثور على إجابات لبعض الأسئلة الأكثر شيوعاً (الأسئلة الشائعة).
- بدلاً عن ذلك ، يمكنكم الاستفادة من أفاست! منتدى الدعم .هنا يمكنكم التفاعل مع غيركم من مستخدمي أفاست! الذين قد تعرضوا لنفس المشكلة ، و إكتشفوا حلها بشكل فعلي . مع العلم أنكم ستحتاجون إلى التسجيل لإستخدام هذا المنتدى ، ولكن عملية التسجيل هذه سريعة وبسيطة للغاية. إذا رغبتم بالتسجيل لإستخدام هذا المنتدى ، انتقل إلى التسجيل بمنتدى أفاست!

وأخيراً ، إذا كنتم غير قادرين على حل مشكلتكم فبإمكانكم " إحالة بطاقة " إلى فريق الدعم التقني لدينا . مرة أخرى فإنكم بحاجة إلى التسجيل للقيام بإحالة هذه البطاقة ، و يرجى عند مراسلتنا كتابة أكبر قدر ممكن من المعلومات (عنوان البريد الإلكتروني المستخدم وقت التسجيل / الإشتراك ، تكوينات جهازكم و نظام التشغيل، هل ظهرت أية رسائل خطأ ، ماهي ، لقطة شاشة عن المشكلة ... إلخ).

كيفية تركيب أفاست! الحزمة الأمنية المتكاملة ٦.٠

تقدم لكم الصفحات التالية شرحاً عن كيفية تحميل و تركيب أفاست! الحزمة الأمنية المتكاملة ٦.٠ على جهاز كم الحاسب وكيفية البدء في استخدام البرنامج بعد إكتمال التحميل و التركيب. يمكن تحميل و تركيب و إستخدام البرنامج أفاست مجاناً لمدة ٣٠ يوما كفترة تجريبية . إذا قررتم الإستمرار في استخدام البرنامج بعد انقضاء هذه الفترة التجريبية ، فستحتاجون إلى شراء الترخيص و بعد ذلك إدخال ملف الترخيص في البرنامج. لقطات الشاشة المبينة في الصفحات التالية مأخوذة من نظام التشغيل ويندوز إكس بي و قد تختلف قليلاً عن الإصدارات الأخرى من مايكروسوفت ويندوز .

فيما يلي الحد الأدنى لمتطلبات النظام الموصى بها لتركيب وتشغيل برنامج أفاست! الحزمة الأمنية المتكاملة ٦.٠ :

- مايكروسوفت ويندوز ٢٠٠٠ المحترف حزمة الخدمة ٤، أو مايكروسوفت ويندوز إكس بي حزمة الخدمة ٢ أو أعلى (أي إصدار، ٣٢ أو ٦٤ بت) ، أو مايكروسوفت ويندوز فيستا (أي إصدار، ٣٢ أو ٦٤ بت) أو مايكروسوفت ويندوز ٧ (أي إصدار، ٣٢ أو ٦٤ بت).
- نظام تشغيل ويندوز متوافق تماماً مع معالج انتل بنتيوم ٣ أو أعلى (معتمداً في ذلك على متطلبات إصدار نظام التشغيل المستخدم وغيرها من برامج الطرف الثالث التي تم تركيبها في الجهاز الحاسب).
- ٢٥٦ ميغابايت من ذاكرة الوصول العشوائي أو أعلى (معتمداً في ذلك على متطلبات إصدار نظام التشغيل المستخدم وغيرها من برامج الطرف الثالث التي تم تركيبها في الجهاز الحاسب).
- ٢٥٠ ميغابايت مساحة حرة على القرص الثابت (للتحميل و للتركيب) أو ٣٠٠ ميغابايت إذا اخترت تركيب متصفح جوجل كروم في نفس الوقت أيضاً
- توفر اتصال بالإنترنت (لتحميل و تسجيل المنتج ، و إجراء التحديثات التلقائية للبرنامج وقاعدة بيانات الفيروسات).
- دقة الشاشة المثلى يجب ألا تقل عن ١٠٢٤ x ٧٦٨ بيكسل.

يرجى ملاحظة أن هذا المنتج لا يمكن تركيبه على نظام تشغيل المخدم (ويندوز المخدم نت / ٢٠٠٠ / ٢٠٠٣) .

الخطوة ١. تحميل أفاست! الحزمة الأمنية المتكاملة ٦.٠ من www.avast.com

من المستحسن أن تكون جميع برامج ويندوز الأخرى مغلقة قبل بدء التحميل .

اضغط على "التحميل " و من ثم قم باختيار " البرامج" وبعد ذلك حدد أفاست! الحزمة الأمنية المتكاملة.

إذا كنتم تستخدمون إنترنت إكسبلورر كمتصفح للإنترنت ، سيظهر لكم المربع المبين أدناه:

بعد ذلك ستبدأ تحميل ملف التركيب إلى جهازكم الحاسب إما بالنقر على "تشغيل – **Run**" أو "حفظ – **Save**".

إذا كنتم ترغبون بأن يتم تركيب أفاست! الحزمة الأمنية المتكاملة ٦.٠ بشكل فوري على الجهاز الحاسب بعد أن يكون قد تم التحميل بشكل تام ، انقر فقط على " تشغيل – **Run** " .

في متصفحات المواقع الأخرى، يمكنكم فقط اختيار " حفظ – **Save** " الملف. انقر على " حفظ – **Save** " لتحميل البرنامج إلى جهازكم الحاسب و لكن أفاست! لن يتم تركيبه في هذا الوقت. لإكمال عملية التركيب سيكون من الضروري تشغيل ملف التركيب فيما بعد ، لذلك لو سمحت تذكر أين قمت بحفظ هذا الملف !

الخطوة ٢. تركيب أفاست! الحزمة الأمنية المتكاملة ٦.٠ على جهازكم الحاسب

لتركيب أفاست! الحزمة الأمنية المتكاملة ٦.٠ على جهازكم الحاسب ، فستحتاجون إلى تشغيل ملف التركيب. عند تشغيل ملف التركيب (بالنقر فوق "تشغيل" كما هو موضح أعلاه ، أو بالنقر المزدوج على الملف المحفوظ على جهازكم الحاسب) فسيتم عرض لقطة الشاشة التالية:

بالنقر على "تشغيل – **Run**" مرة أخرى سيأخذكم إلى لقطة شاشة إعداد أفاست! التالية:

من القائمة المنسدلة ، حدد لغة التركيب المطلوبة ، ثم انقر فوق " التالي" للمتابعة. على لقطة الشاشة التالية ، يمكنكم التأكيد فيما إذا كنتم لا ترغبوا أو ترغبون بالمشاركة في أفاست! المجتمع.

قوة أفاست! قائمة على الجمع بين الخبرات التي تواجه أكثر من ١٥٠ مليون مستخدم حول العالم. فيرجى إن رغبتم في مساعدتنا على مواصلة تقديم أفضل حماية ممكنة لكافة عملائنا من خلال المشاركة في أفاست! المجتمع.

إذا كنتم توافقون على المشاركة ، فأن أفاست! سيجمع المعلومات المتعلقة بالتهديدات الجديدة وقت إكتشافها بشكل تلقائي ، و يقوم بإرسال هذه المعلومات بإستمرار إلى شركة أفاست للبرمجيات.

المعلومات الوحيدة التي سيتم جمعها هي المعلومات المتعلقة بالفيروسات الجديدة والملفات التي تظهر نوعاً من السلوك المشكوك بأمره. بعد ذلك فإن المعلومات التي تم جمعها ستحلل ، و تستخدم لتحسين الحماية التي يوفرها أفاست! لجميع المستخدمين في جميع أنحاء العالم.

ستكون جميع المعلومات المرسلة إلى أفاست للبرمجيات مجهولة الهوية – أي لن يتم جمع أي معلومات شخصية . إذا لم ترغب في المشاركة ، ببساطة قم بإلغاء تحديد هذا الخيار ، و بذلك لن يتم إرسال أي معلومات من جهازكم .

للمزيد من المعلومات، يرجى قراءة "نهج الخصوصية" من خلال النقر على الوصلة التي تظهر على لقطة الشاشة.
على هذه الشاشة يمكنكم أيضاً تخصيص التركيب ، ولكن ، للمضي قدماً في التركيب النموذجي (مستحسن) يرجى ترك هذا الإختيار بدون إشارة ، و من ثم انقر فوق التالي.

في الخطوة التالية، لديك الخيار باستخدام البرنامج في الوضع التجريبي ، أو بإدخال ملف ترخيص ساري المفعول :

- إذا كنت ترغب باستخدام البرنامج في الوضع التجريبي، فستحتاج بأن تكون متصلاً بالإنترنت، حيث سيتم تحميل الترخيص التجريبي تلقائياً أثناء التركيب. و بذلك ستكون قادراً على استخدام البرنامج لفترة تجريبية مدتها ٣٠ يوماً ، ومع ذلك فستحتاج لإدخال ترخيص كامل ساري المفعول بعد هذه الفترة تجريبية إذا كنت ترغب بالاستمرار في استخدام هذا البرنامج – انظر الصفحة التالية.

- إذا قمت بشراء الترخيص بشكل فعلي، فيرجى حفظه على جهازك الحاسب ، و من ثم استخدم زر "استعراض – **Browse** " لتحديد المكان الذي قمت بحفظ ملف الترخيص على جهازك الحاسب . اضغط عليه لتحديده ومن ثم انقر فوق "فتح – **Open** " بذلك سيتم إدراج ملف الترخيص الخاص بك تلقائياً. يمكنك الآن استخدام البرنامج حسب مدة الاشتراك الذي اشتريته.

- إذا اشتريت مضاد الفيروسات أفاست مع رمز التفعيل، فيمكنك إدخاله هنا لتفعيل الترخيص الخاص بك.

- إذا كان لديك مفتاح ترخيص لبرنامج أفاست! الإصدار المحترف (X).٤، فيمكنك إدراجه هنا، وسيتم تحويله إلى ترخيص جديد للنسخة ٦.٠

ثم انقر فوق زر "التالي– **Next** " للمتابعة.

عند اكتمال التركيب سيقوم أفاست بإجراء فحص سريع لجهازك الحاسب للتأكد من أن كل شيء على ما يرام.

يجب أن تؤكد لقطة الشاشة النهائية على أن تركيب أفاست! قد تم بنجاح. انقر فوق "إنهاء – Finish ".

يرجى إعادة تشغيل جهازك الحاسب، بعد عملية إعادة التشغيل سيطلب منك التأكيد على وضع جدار الحماية الذي ينبغي أن يستخدم على شبكة الاتصال لديك:

تحدد الإعدادات الثلاثة المتاحة ما هي الاتصالات بين الشبكة والشبكات الخارجية الأخرى المسموحة. الوضع الافتراضي هو " منطقة متوسطة المخاطر/عمل – Work/Medium Risk Zone "و هذا يعني أن أفاست سيقرر ما هي الاتصالات الخارجية التي سيسمح بها. الإعداد الأكثر أمانا هو " منطقة عالية المخاطر/عامة – Public/high risk zone" التي من شأنها عرقلة كافة الاتصالات الواردة، أو يمكنك اختيار " منطقة منخفضة المخاطر/محلية – Home/low risk zone " التي تسمح لجميع الاتصالات، يوصى بها فقط إذا كنت تستخدم جهازك الحاسب على شبكة محلية مع عدم وجود اتصالات الخارجية على سبيل المثال على الإنترنت. لقد تم شرح هذه الإعدادات الثلاثة في هذا الدليل في مقطع "جدار حماية".

سترى أيقونة أفاست! البرتقالية الموجودة أعلاه على سطح المكتب و كرة أفاست! البرتقالية التي يتوسطها حرف " a" في شريط المهام (بالقرب من الساعة).

إذا كنت تستخدم ويندوز فيستا أو أعلى ، سترى مع خيار الشريط الجانبي أيضاً رمز الشريط الجانبي لأفاست. هذا يخبرك عن الوضع الحالي لبرنامج أفاست ويمكنك كخيار سحب وإسقاط أي ملف على رمز أفاست في حالة أنك تريد فحصه.

الابتداء

يمكن إستخدام هذا البرنامج مجاناً لمدة ٣٠ يوماً كفترة تجريبية ، ولكن إذا قررتم الإستمرار في إستخدام البرنامج بعد انقضاء هذه الفترة التجريبية ، فستحتاجون إلى شراء الترخيص و بعد ذلك إدخال ملف الترخيص في البرنامج.

يمكنكم شراء تراخيص أفاست! الحزمة الأمنية المتكاملة لمدة ١ أو ٢ أو ٣ سنوات و لعدد يبدأ من ٣ إلى ٦ إلى ١٠ أجهزة حاسب في منزلكم أو في شبكة منزلكم/ مكتبكم.

لمستخدمي الشبكات و الشركات الكبيرة ، نوصيكم بإستخدام المنتجات التي توفر لكم إدارة مركزية لجميع أجهزة الكمبيوتر على الشبكة. يمكن الحصول على المزيد من المعلومات حول منتجاتنا التي تدار مركزياً من صفحات موقعنا الإلكتروني www.avast.com

يمكنكم شراء ترخيص بعد الإنتقال إلى www.avast.com و النقر على "الشراء – **Purchase**" في أعلى الشاشة. ثم انقر على "حلول الحاسوب " ويكفي أن تدخل عدد و إسم ومدة الترخيص الذي ترغب بشراءه.

بعد تلقي ملف الترخيص الخاص بكم ، فإنكم بحاجة فقط إلى النقر–مرتين/مزدوج على هذا الملف لفتحه و بهذه الطريقة سيتم إدخال ملف الترخيص في البرنامج بشكل تلقائي. بدلاً عن ذلك ، هنالك طريقة أخرى لإدخال الترخيص حيث يمكنكم حفظ ملف الترخيص في الجهاز الحاسب ، و بعد ذلك فتح واجهة المستخدم بأفاست! و النقر على علامة التبويب " الصيانة – **Maintenance** " ، ثم إنقر فوق " الإشتراك – **Subscription** " ثم على "إدخال ملف الترخيص – **Insert license file** " .

ستفتح نافذة جديدة حيث يمكنكم استعراض جهازكم الحاسب لتحديد الموقع الذي اخترته سابقاً لتخزين ملف الترخيص .

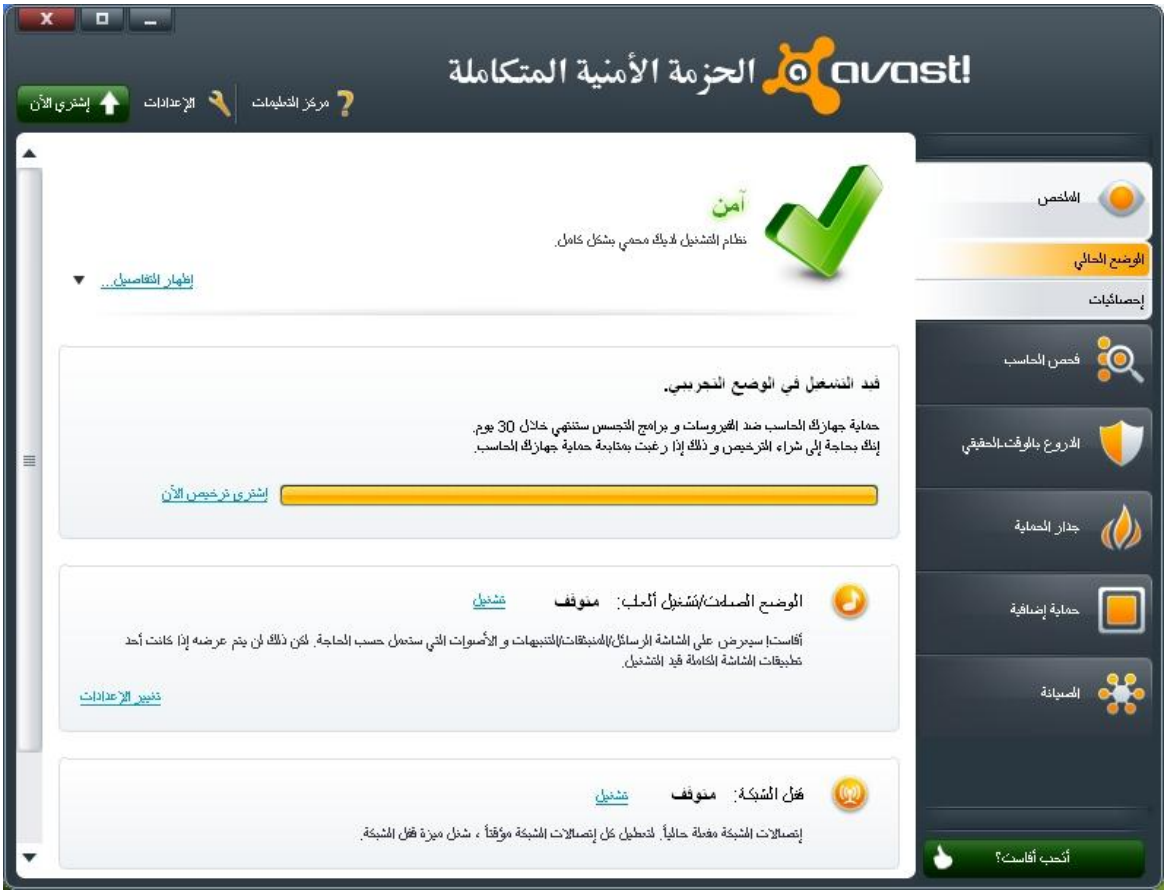
بعد تحديد مكانه، إنقر مرتين عليه ، و بذلك سيتم إدخاله بشكل تلقائي في البرنامج.

إذا إشتريتم عدة تراخيص لحماية العديد من أجهزة الحاسب ، فستحتاجون لتنفيذ نفس العملية على كل جهاز حاسب قمتم بتركيب أفاست! عليه فعلى سبيل المثال يمكنكم إرسال بريد إلكتروني مع المرفقات " ملف الترخيص " لكل مستخدم ، أو عن طريق حفظ ملف الترخيص على محرك أقراص مشترك ، ذاكرة وميضية ... إلخ.

بمجرد أن يتم إدخال الترخيص فسيتم تفعيل البرنامج و يؤدي إلى إستمراركم في تلقي التحديثات التلقائية لكلاً من البرنامج و قاعدة تعريفات الفيروسات الأمر الذي يبقي جهازكم الحاسب محمي ضد آخر التهديدات المحتملة.

أساسيات إستخدام البرنامج

عند فتح النافذة الرئيسية للبرنامج ، ستشاهدون الوضع الأمني الراهن لجهازكم الحاسب. عادة ، يجب أن تظهر النافذة كما هو مبين أدناه.



بالنقر على "إظهار التفاصيل – Show details " فيمكنكم الكشف عن المزيد من المعلومات حول الوضع الحالي للبرنامج و قاعدة تعريفات الفيروسات.

الدروع بالوقت–الحقيقي

كما يوحي إسمها ، فإن الدروع في الوقت–الحقيقي تقوم بحماية جهازكم الحاسب ضد التهديدات في الوقت الحقيقي أي في اللحظة التي يتم الكشف عنها ، لذلك عادة ما ينبغي أن تكون الحالة على "شغال – On ". إذا تم إيقاف أي من الدروع ، فستظهر الحالة "متوقف – Off ". لتشغيلهم مرة أخرى ، انقر فوق "تشغيل – Turn On ".

جدار الحماية

جدار الحماية يراقب كل الإتصالات بين جهازكم الحاسب والعالم الخارجي و يقوم بحجب الاتصالات الغير المرخص بها. عادة ما ينبغي أن تكون الحالة على "شغال – On ".

إصدار قاعدة تعريفات الفيروسات

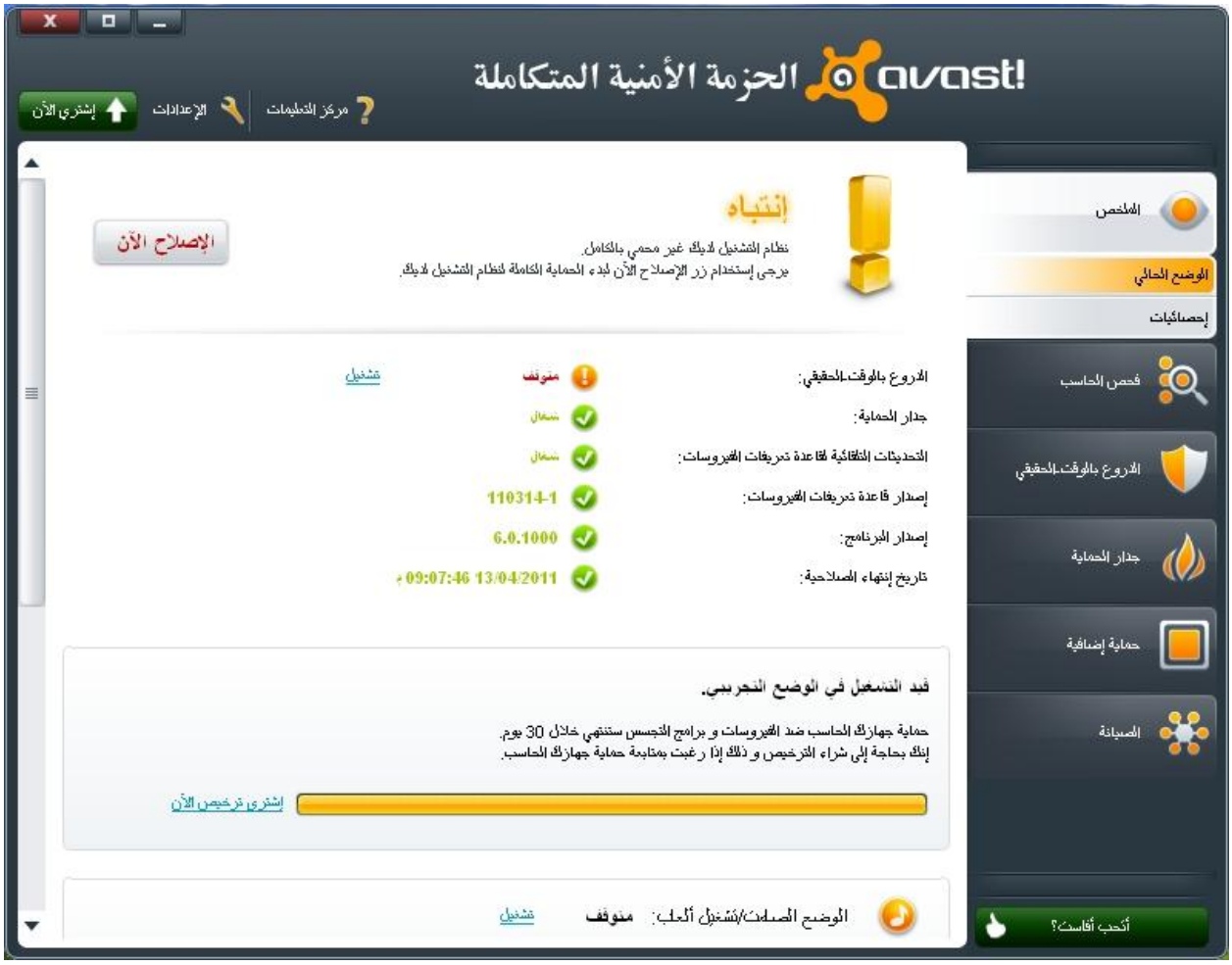
ستشاهدون في هذا السطر الإصدار الحالي من قاعدة تعريفات الفيروسات . هذه يتم تحديثها تلقائياً بشكل افتراضي ، ولكن للتأكد من أن لديكم أحدث قاعدة لتعريفات الفيروسات ، انقر فوق "تحديث– Update " وبعد ذلك يمكنكم إختيار فيما إذا كنتم ترغبون بتحديث المحرك و قاعدة تعريفات الفيروسات ، أو البرنامج أيضاً.

إصدار البرنامج

يخبركم هذا السطر عن الإصدار الحالي للبرنامج. لضمان حصولكم على كافة التحديثات الأخيرة ، إنقر على "تحديث– Update "

التحديثات التلقائية لقاعدة تعريفات الفيروسات

عادة ما ينبغي أن تكون الحالة على "شغال – On ". بهذا ستضمن أن قاعدة تعريفات الفيروسات محدثة تلقائياً كلما تم الإتصال بالإنترنت . لتشغيل هذه الميزة أو إيقافها ، انقر فوق "تغيير – Change ". من المستحسن أن يتم تغيير الخيار للمحرك و قاعدة تعريفات الفيروسات على "تحديثات تلقائية – automatic update ". إذا ظهر في النافذة الرئيسية كما هو مبين أدناه ، فإن ذلك يعني أن برنامج الحماية من الفيروسات قد لا يكون محدثا أو أن أحد أو أكثر الدروع بالوقت – الحقيقي قد تم إيقافها . يمكنكم حل هذا بالنقر على زر "الإصلاح الآن –Fix Now ".



"غير آمن – Unsecured " يعني أن كل الدروع بالوقت– الحقيقي متوقفة. استخدام زر "الإصلاح الآن –Fix Now " لتشغيلهم و بذلك يتم توفير حماية كاملة لجهازكم الحاسب ، أو استخدام السهم أسفل الجانب الأيمن أو الأيسر من الشاشة (حسب لغة إصدار البرنامج المستخدم) لتشغيل الدروع واحداً تلو الآخر .

الوضع الصامت /تشغيل ألعاب

من النافذة الرئيسية ، يمكنكم أيضاً الوصول إلى إعدادات الوضع الصامت/تشغيل ألعاب . إفتراضياً ، يتم عرض الحالة على "متوقف – Off " ولكن رسائل الشاشة لن يتم عرضها فيما إذا كان أحد تطبيقات كامل الشاشة قيد التشغيل . يمكنكم بالنقر على "تغيير الإعدادات – Change settings " تحديد أن رسائل الشاشة لن يتم عرضها نهائياً (الوضع الصامت "شغال") أو يمكنكم إيقاف الوضع الصامت/تشغيل ألعاب بشكل كامل.

قفل الشبكة

يمكنكم قفل الشبكة من تعطيل مؤقت لكافة إتصالات الشبكة. يمكن أن يكون هذا مفيداً إذا كنت تعمل على بيانات حساسة ، وتريد أن تكون على يقين من أنه لا يمكن الوصول إليها من قبل أي شخص آخر ، أو إذا كان لديكم أي سبب للإعتقاد بأن جهازكم الحاسب قد تعرض لهجمة من مصدر خارجي. بتشغيل قفل الشبكة ، فلن يتمكن جهازكم الحاسب من الوصول بشكل تام إلى بقية الشبكة.

المزيد من المعلومات عن الدروع بالوقت –الحقيقي

الدروع بالوقت–الحقيقي هي أهم جزء بالبرنامج ، لأنها تعمل بشكل دائم لمنع جهازكم الحاسب من الإصابة بالعدوى. إنهم يراقبون كل الأنشطة التي تتم بجهازكم الحاسب ، و التحقق من جميع البرامج والملفات في الوقت –الحقيقي - أي في لحظة تشغيل البرنامج أو كلما تم فتح أو إغلاق ملف.

عادة ، الدروع بالوقت– الحقيقي تبدأ العمل تلقائياً عند بدء تشغيل جهازكم الحاسب. وجود الأيقونة البرتقالية لأفاست! في الركن الأيمن أو الأيسر السفلي لشاشة الجهاز الحاسب (ذلك يعتمد على لغة نظام التشغيل لديكم) يخبركم بأن الدروع بالوقت–الحقيقي تعمل بشكل جيد. كما يمكن إيقاف أي درع في أي وقت ،

ولكن هذا الأمر غير موصى به حيث أن القيام بذلك قد يخفض مستوى الحماية الخاص بجهازكم. إذا كان أي من الدروع متوقف ، فسوف ترى رسالة تحذير عند فتح واجهة المستخدم تخبرك أن جهازكم الحاسب ليس محمياً بالكامل (إذا كان أحد أو أكثر الدروع متوقفة) أو "غير آمن" (إذا كان كل الدروع متوقفاً).

يحتوي أفاست! مضاد الفيروسات ٦.٠ على الدروع بالوقت–الحقيقي التالية:

درع ملف النظام – يقوم بالتحقق من أي برامج في لحظة بدء التشغيل و غيرها من الملفات في اللحظة التي يتم فيها فتحها أو إغلاقها. إذا تم إكتشاف أي شيء مريب ، سيقوم درع ملف النظام بمنع بدء تشغيل البرنامج أو من أن يتم فتح هذا الملف لمنع أي ضرر محتمل قد يلحق بالجهاز الحاسب أو البيانات الموجودة فيه.

درع البريد – يقوم بالتحقق من رسائل البريد الإلكترونية الصادرة والواردة ، و يعمل على إيقاف أي رسالة قد تحتوي على عدوى فيروس محتملة من الممكن أن يتم قبولها أو إرسالها.

درع ويب – يحمي جهازكم من الفيروسات في وقت إستخدام الإنترنت (التصفح وتحميل الملفات ، إلخ). و سيعمل على كشف ومنع التهديدات المحتملة أو القادمة من الشبكة العنكبوتية و تحديداً صفحات الإنترنت المخترقة (المحتملة أو الفعلية) المصابة بالبرامج النصية الخبيثة. إذا تم إكتشاف فيروس أثناء تحميل ملف من الإنترنت ، فسوف يتم إيقاف هذا التحميل لمنع هذه العدوى من الوصول إلى جهازكم الحاسب.

درع الند للند – يتحقق من الملفات التي يتم تحميلها عند إستخدام أحد برامج الند للند (تبادل الملفات).

درع المراسلة الفورية – يتحقق من الملفات التي يتم تحميلها من قبل برامج المراسلة الفورية أو "الدردشة."

درع الشبكة – يراقب كل أنشطة الشبكة و يقوم بحجز أي تهديد يتم إكتشافه على الشبكة. كما أنه يمنع الوصول إلى المواقع الضارة المعروفة و ذلك إستناداً إلى قاعدة بيانات عناوين المواقع المصابة الموجودة بأفاست.!

درع السلوك – يراقب كل الأنشطة على جهازكم الحاسب ، ويكشف و يحجز أي نشاط غير عادي قد يدل على وجود أي من البرامج الضارة. و يتم ذلك من خلال الرصد المتواصل لنقاط الدخول بجهازكم الحاسب مستخدماً مجسات خاصة لتحديد أي شيء مريب أو مشبوه.

درع البرامج النصية المنبثقة – يراقب كل البرامج النصية التي تحاول تشغيل نفسها على جهازك الحاسب، فيما إذا كان هذا البرنامج النصي متحكماً به عن بعد على سبيل المثال أثناء تصفح الإنترنت، أو محلياً من خلال فتح ملف على جهاز ك الحاسب.

العملية الاختبارية (صندوق الاختبارات)

يتيح صندوق الاختبارات بأفاست! تصفح مواقع الإنترنت ، أو تشغيل أي تطبيق آخر ضمن بيئة آمنة تماماً. هذه الميزة مفيدة جداً و خاصة عند زيارة مواقع عالية المخاطر على الشبكة العنكبوتية ، سواء عن قصد أو غير قصد ، حيث أن المتصفح أو أي عمل آخر سيتم ضمن صندوق الإختبارات هذا ، الأمر الذي يمنع أي ضرر على جهازكم الحاسب.

يمكن استخدام صندوق الاختبارات أيضاً لتشغيل أي من التطبيقات الأخرى التي تعتقد أنه يمكن أن تكون مشتبهاً بها – يمكنكم تشغيل البرنامج داخل صندوق الاختبارات لتحديد ما إذا كان آمناً أو غير آمنٍ في حين تبقى الحماية كاملة ضد أي إجراء أو محاولة قد تقوم به أي من البرمجيات الخبيثة.

لتشغيل تطبيق أو لتصفح مواقع الإنترنت باستخدام صندوق الإختبارات ، إضغط فقط على "تشغيل العملية الإختبارية – Run a virtualized process " ثم استعرض الملفات الموجودة على جهازكم الحاسب للعثور على التطبيق أو البرنامج المطلوب ، على سبيل المثال متصفح الإنترنت . سيفتح المتصفح أو أي تطبيق آخر ضمن نافذة خاصة محددة باللون الأحمر ، ذلك يشير إلى أن هذا المتصفح أو التطبيق يجري تشغيله داخل صندوق الإختبارات.

في إعدادات الخبراء ، يمكنكم كذلك تحديد التطبيقات التي ينبغي أن يتم تشغيلها دائماً في الوضعية الإختبارية ، و التطبيقات الموثوقة التي لا يجب أبداً القيام بإختبارها.

إذا اكتشف أفاست عن أي شيء مريب عند محاولة بدء تشغيل تطبيق ما، فسترى رسالة تسألك فيما إذا كنت تريد تشغيل التطبيق في صندوق الاختبارات :

يمكنكم أيضا تشغيل تطبيق في صندوق الإختبارات من دون إستخدام واجهة مستخدم أفاست! . يتم ذلك بالنقر بالزر الأيمن على هذا التطبيق الأمر الذي يؤدي إلى فتح قائمة السياق المنسدلة.

لتشغيل التطبيق داخل صندوق الإختبارات قم بإختيار "تشغيل إختباري – **Run virtualized** " من قائمة السياق و بذلك سيبدأ التطبيق ضمن خاصة محددة باللون الأحمر .إذا كان هنالك تطبيق ما ينبغي أن يكون دائماً مشغلاً في صندوق الإختبارات في كل مرة يتم تشغيله فيه ، حدد "دائماً التشغيل في صندوق الإختبارات – **Always run in sandbox** " بذلك فإن التطبيق سيضاف الى قائمة التطبيقات على شاشة إعدادات الخبراء التي ينبغي أن يتم تشغيلها بشكل إختباري دائماً. في كل مرة يتم تشغيل هذا التطبيق ، فسيظهر داخل الحدود الحمراء مشيراً إلى أنه يجري تشغيله حالياً داخل صندوق الإختبارات.

النقر بالزر الأيمن للفأرة على التطبيق المشغل فعلياً ضمن صندوق الإختبارات ، سيتم فتح قائمة سياق منسدلة جديدة لتمكين تشغيل هذا التطبيق مرة واحدة

خارج صندوق الإختبارات ، أو بدلاً عن ذلك ، يمكن حذفه من صندوق الإختبارات بشكل نهائي بحيث أن تشغيل هذه التطبيق سيتم في البيئة الطبيعية من جديد في كل مرة يتم فيها تشغيله.

العملية الاختبارية (المنطقة الآمنة)

أفاست! المنطقة الآمنة هي ميزة أمنية إضافية تسمح لك بتصفح مواقع الإنترنت في بيئة خاصة آمنة، وغير مرئية من بقية نظام التشغيل لديك. على سبيل المثال، للتسوق أو الخدمات المصرفية عبر الإنترنت، أو غيرها من المعاملات الحساسة أمنياً ، يمكنك أن تتأكد من أنه لا يمكن رصد أو مراقبة بياناتك الشخصية من قبل برامج التجسس أو راصدي لوحة المفاتيح .

خلافاً لصندوق الاختبارات بأفاست! ، الذي يهدف إلى إبقاء على كل شيء يعمل بداخله بحيث لا يمكنها أن تضر ببقية نظام التشغيل لديك ، تم تصميم أفاست! المنطقة الآمنة لإبقاء كل شيء آخر يعمل بالخارج.

لفتح المنطقة الآمنة ، يمكنك الذهاب إلى علامة التبويب "حماية إضافية – **Additional Protection** " ، ثم فتح علامة التبويب "المنطقة الآمنة – **SafeZone** " و النقر على "تحويل إلى المنطقة الآمنة – **Switch to SafeZone** "

عند التحويل إلى المنطقة الآمنة، متصفح الويب بالمنطقة الآمنة سيبدأ بالفتح تلقائياً. متصفح المنطقة الآمنة هو متصفح خاص دون أي مكونات إضافية مثل "برامج الإضافية" التي غالباً ما تستخدم لتوزيع برامج التجسس.

عند الانتهاء ، انقر على قائمة ابدأ ، وحدد "إيقاف" لإغلاق المتصفح والعودة إلى جهاز الحاسب العادي. إعدادات متصفحك وأية ملفات قمت بتحميلها سيتم حفظها تلقائياً وستكون

هناك في المرة القادمة عند فتح المنطقة الآمنة. إذا كنت لا تريد أن يتم حفظ أي شيء، انقر فوق زر "إعادة تعيين المنطقة الآمنة – **Reset SafeZone**" و سيتم حذف كل شيء. سيتم إعادة تعيين محتويات المنطقة الآمنة ، بما في ذلك جميع إعدادات المتصفح ، إلى حالتها الأصلية.

بدلا من ذلك ، يمكنك فقط النقر على زر "عودة – **Switch back** " الموجود في شريط المهام (بجانب الساعة) الذي سيعيد لك جهازك الحاسب العادية دون إنهاء متصفح ويب ، بحيث يمكنك العودة إليها في وقت لاحق.

أفاست! سمعة الموقع

ميزة أفاست! سمعة الموقع يتم تركيبها اختيارياً أثناء تركيب مضاد الفيروسات أفاست!. بدلاً من ذلك يمكن تركيبه في وقت لاحق عن طريق فتح واجهة المستخدم بأفاست! ، ثم الذهاب إلى علامة التبويب "حماية إضافية" ، ثم حدد سمعة الموقع ومن ثم انقر فوق فقط "تركيب". هنا يمكنك أن ترى أيضا فيما إذا كان متصفح الإنترنت لديك مدعوم، و ذلك قبل محاولة تركيبه.

تستند سمعة الموقع على المعلومات الواردة من مجتمع مستخدمي أفاست! في أنحاء العالم المتعلقة بمحتوى وأمن المواقع التي تمت زيارتها ، للمساعدة في تحسين تجربة التصفح لجميع المستخدمين. يمكنك المساهمة بملاحظاتك الخاصة عن طريق "التصويت" على المحتوى وأمن المواقع التي تزورها .
عند زيارة الموقع ، سوف ترى سلسلة من ثلاثة أشرطة (الأحمر ، و الأصفر ، أو الأخضر) والتي تخبرك كيف كان تقييم هذا الموقع ، أو عند القيام بالبحث باستخدام أحد محركات البحث الشعبية ، فسترى نفس مؤشر ترميز–اللون بجوار كل من النتائج المذكورة.

يخبرك لون المؤشر فيما إذا كان قد تم تقييم الموقع بأنه "جيد" (الأخضر)، "متوسط" (الأصفر)، أو "سيئ" (الأحمر). عدد من الأشرطة تشير إلى إبراز قوة التقييمات. شريط واحد أو اثنين أو ثلاثة أشرطة تمثل عدد صغير ، محدود ، أو كبير من الأصوات.

بالنقر على المؤشر الملون سيفتح مربع يمكنك من أن ترى المزيد من المعلومات حول كيف تم تقييم الموقع و المكان الذي يمكن أن تقدم فيه أيضاً تصويتك الخاص.

على الجانب الأيسر ، يمكنك أن ترى التقييم العام. تحت التقييم ، يمكنك ان ترى أصغر الرموز التي تمثل الفئات الذي ينتمي إليها هذا الموقع أو ذاك.

على الجانب الأيمن ، يمكنك تقدم تصويتك الخاص . هنا يمكنك ان ترى شريط واحدة مقسمة إلى خمسة قطاعات ملونة يمكنك استخدامها لتعيين تقييم بطريقة أكثر تفصيلاً عن مجال موقع ما . تحت هذا الشريط يمكن أن تجد رموز الفئة. انقر على أحد هذه الرموز لوضع مجال موقع ما إلى الفئات ذات الصلة ، ثم أخيرا انقر على "التصويت" لتقديم تقييمك.

فاحص خط–موجه الأوامر

يمكنك فاحص خط–موجه الأوامر من تشغيل الفحص يدوياً بجهازكم الحاسب دون الحاجة إلى فتح واجهة المستخدم بأفاست! و ذلك يتم حتى قبل أن يكون قد بدأ نظام التشغيل لديك . يستخدم البرنامج (ashCmd) نفس محرك الفحص الموجود بأفاست! للكشف عن عدوى البرامج الضارة المحتملة لذلك فإن النتائج ستكون نفسها تماماً كما لو أن الفحص تم إجراءه من خلال واجهة البرنامج العادي. إن أفاست! فاحص خط –موجه الأوامر ، ashCmd.exe، مركب بالعادة على مسار الدليل التالي (C:\program files\AVAST Software\Avast) .

الفحص يتم تشغيله من موجه الأوامر باستخدام تحويلات و معايير متعددة. حتى تتمكن من مشاهدة وصف لهذه المعايير ، حدد موقع الملف (ashCmd) وإنقر مرتين عليه. بهذه الطريقة ستفتح نافذة جديدة تعرض معايير متعددة. يمكن الحصول على قائمة بكافة هذه المعايير و التحويلات من مركز التعليمات بالبرنامج نفسه و ذلك بالنقر على F1 و قراءة الصفحة "معايير و تحويلات ".

جدار الحماية

يتضمن أفاست! الحزمة الأمنية المتكاملة جدار حماية مدمج بشكل تام حيث يمكن ضبطه مباشرة من واجهة المستخدم بأفاست. !
جدار الحماية يراقب كل الإتصالات بين جهازكم الحاسب والعالم الخارجي و يقوم بحجب الاتصالات الغير المرخص بها على أساس عدد من قواعد "سماح" و "حجب". بهذه الطريقة ، يمكن لجدار الحماية منع البيانات الحساسة من مغادرة جهازكم الحاسب كما يمكنه أيضاً عرقلة محاولات الاقتحام الغير مشروعة من قبل المتسللين/ القراصنة.

على هذه الصفحة ، يمكنكم ضبط إعدادات جدار الحماية الأمنية للحد من الاتصالات الخارجية وفقاً للبيئة التي يجري إستخدام الجهاز الحاسب فيها.

ثلاثة مستويات من الأمان تم تعريفها:

• منطقة منخفضة المخاطر/محلية – هذا المستوى مناسب عند إستخدام جهازكم الحاسب كجزء من شبكة عمل محلية / منزلية. إذا كان هذا الإعداد محدداً ، فإن جدار الحماية سيسمح لجميع الإتصالات مع هذه الشبكة.

• منطقة متوسطة المخاطر/عمل – هذا المستوى مناسب عندما يكون جهازكم الحاسب متصلاً بشبكة إتصال عامة أوسع ، بما في ذلك الاتصالات المباشرة على الإنترنت. هذا هو الإعداد الافتراضي ، فإذا تم إختياره ، فإن جدار الحماية لن يتيح لأي من الإتصالات الصادرة و الواردة إلا إذا كانت مسموحة ضمن " قواعد التطبيق –Application Rules ". إذا لم يتم إنشاء قاعدة ، فسوف يطلب التأكيد فيما إذا كنتم تريدون السماح بالإتصال مع تطبيق معين أو لا.

• منطقة عالية المخاطر/عامة – هذا المستوى مناسب عند إستخدامكم الجهاز الحاسب للاتصال بشبكة عامة ، حيث تريد ضمان أعلى مستوى من الأمن. هذا الإعداد هو الأكثر أمناً إذا تم إختياره ، فلن يسمح بأن تكون أي من الإتصالات الواردة ، مما يجعل جهازكم الحاسب غير مرئي تماماً للآخرين.

يمكنكم ضبط مستوى الأمان إما عن طريق النقر على الأيقونة ذات الصلة ، أو عن طريق النقر على المنزلقة البرتقالية و نقلها إلى اليسار أو اليمين أثناء الضغط على زر الفأرة بإستمرار.

على هذه الصفحة ، يمكنكم أيضاً إيقاف جدار الحماية تماماً ، إما بصفة دائمة أو لفترة محددة من الوقت عن طريق النقر على زر إيقاف وتحديد الخيار المطلوب.

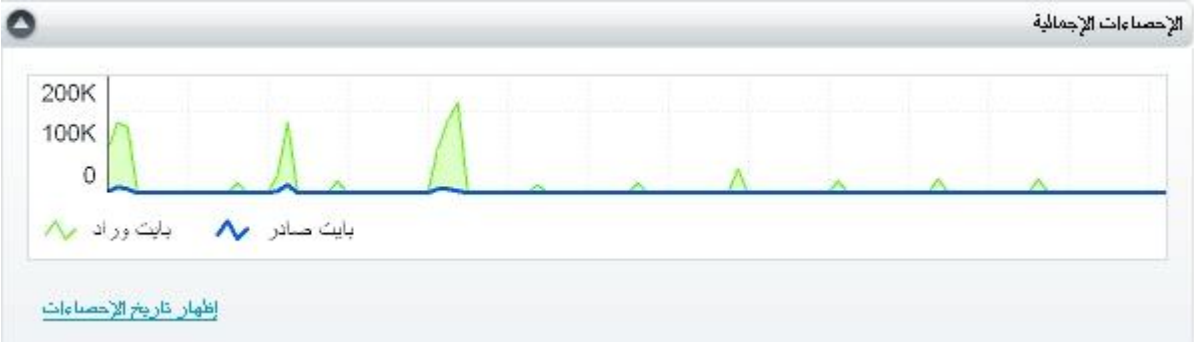
إنقر فوق بدء لتشغيله مرةً أخرى.

شاشة مماثلة لهذه الشاشة ستظهر لكم أيضاً كلما تم الكشف عن شبكة اتصال جديدة. وعندها يمكنكم تحديد مستوى الأمن لهذه الشبكة الجديدة ، ويمكنكم

تحديد أن هذا الأمر يجب القيام به دائماً و ذلك حتى لا يطلب نفس الأمر لمرة أخرى في المرة التالية التي يتم الكشف فيها عن نفس الشبكة.

إحصائيات جدار الحماية

يمكنكم مشاهدة الرسم البياني في أسفل الصفحة ، ممثلاً في الوقت– الحقيقي لكمية البيانات الواردة والصادرة.

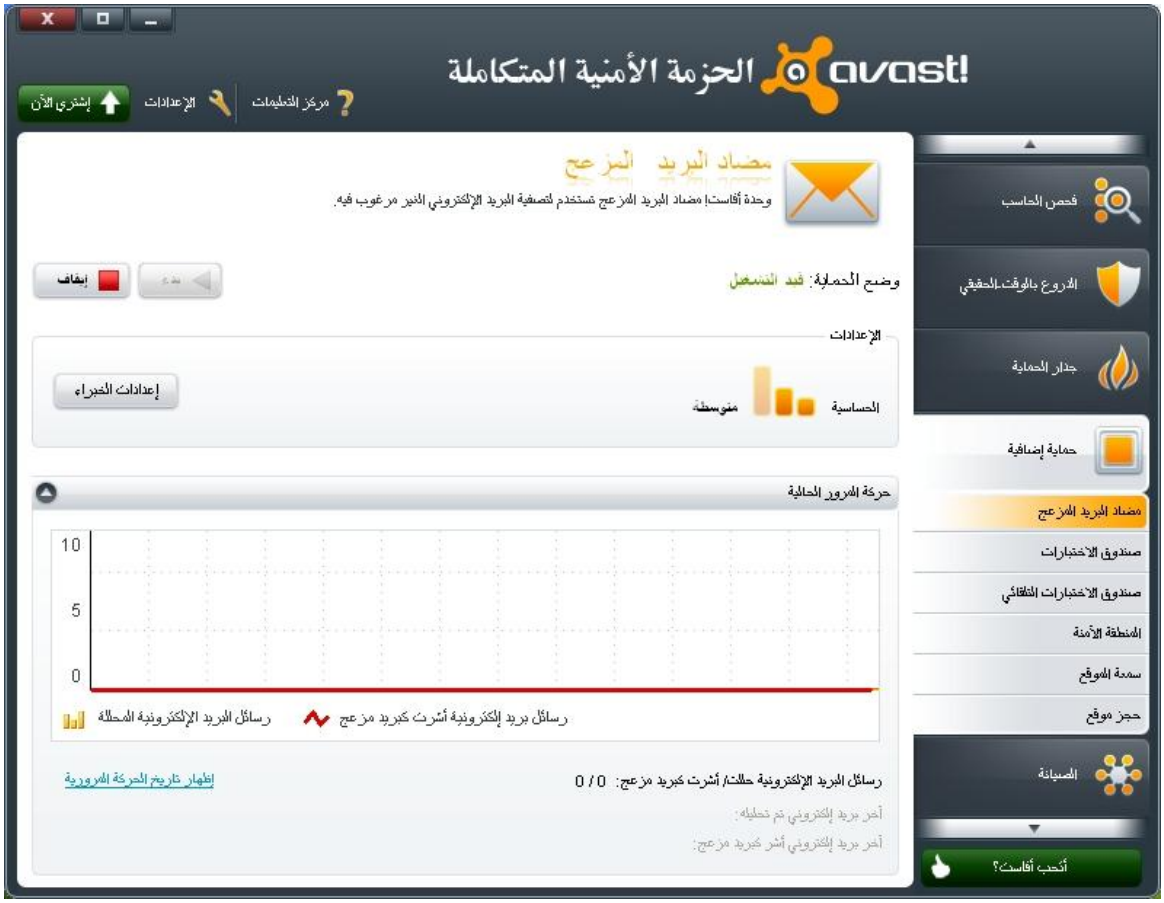


لمشاهدة الموضوع بتفصيلٍ أكثر ، انقر على "إظهار تاريخ الإحصاءات – Show Statistics History ". على شاشة الإحصاء ، يمكنكم عرض بيانات جدار الحماية ، و مصفي مضاد البريد المزعج ، أو أي درع من دروع الوقت –الحقيقي خلال فترة محددة. لتغيير حجم أي جزء من الرسم البياني ، إنقر على الخط العمودي واسحبه إلى اليمين. للعودة الى العرض السابق ، إنقر فقط على "إظهار الكل – Show all " و بذلك سيتم إستعادة العرض السابق.

على الجانب الأيسر أو الأيمن من الشاشة (حسب إصدار لغة البرنامج المستخدم) ، يمكنكم مشاهدة خيارات جدار الحماية الأخرى التي ورد وصفها في تعليمات البرنامج.

مصفي مضاد البريد المزعج

تحلل وحدة أفاست! مصفي البريد المزعج جميع رسائل البريد الإلكتروني الواردة إستناداً إلى معايير مختلفة لتحديد ما إذا كان هذا البريد مشروعاً أو بريداً مزعجاً. سيتم وضع إشارة على رسائل البريد الذي تم تحديدها على أنها بريد مزعج قبل أن يتم تسليمها الى صندوق البريد الوارد. إذا كنتم من مستخدمي مايكروسوفت أوتلوك ، يمكنكم تحديد المجلد البديل للبريد الإلكتروني غير المرغوب فيه الذي ينبغي أن تنقل إليه الرسالة اذا ما تأكد على أنها بريد مزعج – راجع المقطع التالي.



بشكل افتراضي ، إن أفاست! سيفحص جميع رسائل البريد الإلكترونية الواردة و يطابقها مع القاعدة العالمية لبيانات رسائل البريد المزعج و ذلك قبل إجراء أي عمليات فحص أو تحليل إرشادي إضافية لتحديد رسائل البريد المزعج المحتملة الأخرى . سيتم إدراج رسالة أو عبارة على هذه الرسائل للتعرف على أنها رسائل بريد مزعجة و ذلك قبل أن يتم تسليمها لصندوق البريد الوارد.

يمكنكم ضبط حساسية تدقيق الإرشادي و ذلك بالنقر على الشريط البرتقالي.

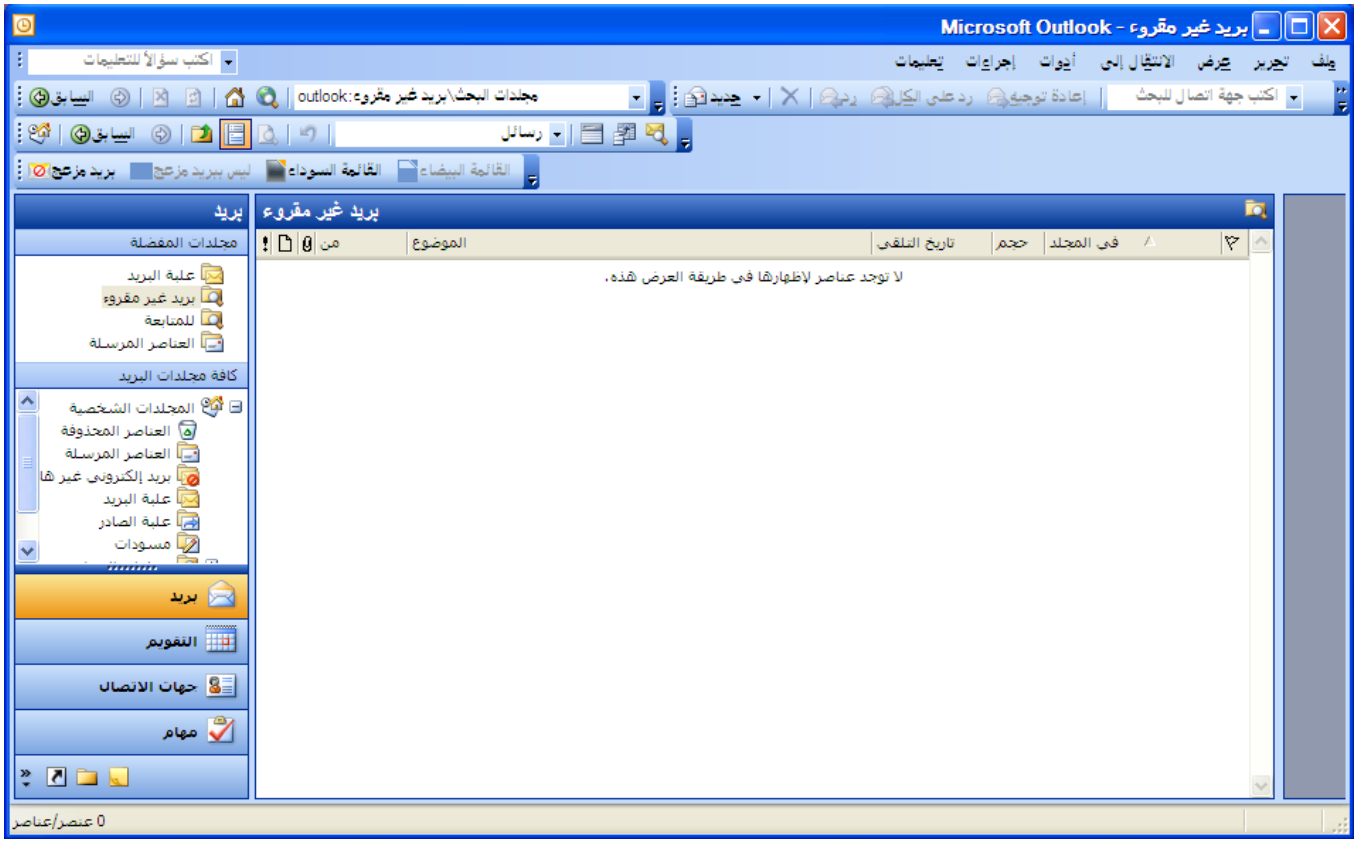
إن زيادة الحساسية ستزيد من احتمالات الكشف ، ولكن ذلك سيزيد أيضاً من إحتمال عرض الإيجابيات الزائفة – إذا وجدتم أن بعض حسابات البريد الالكتروني المعروفة لديكم يتم وضع إشارة عليها على أنها بريد مزعج ، فإن الحد أو التقليل من الحساسية من شأنه أن يساعدكم بحل هذه المسألة.

يمكن إضافة عناوين البريد الإلكترونية الموثوقة أو المعروفة لديكم إلى " القائمة البيضاء" الموجودة بمضاد البريد المزعج. بذلك فإن كل عناوين البريد الإلكتروني الموجودة بالقائمة البيضاء لن تعتبر بأنها بريد مزعج على الإطلاق و سيتم تسليمها لصندوق البريد الوارد . بدلاً عن ذلك ، فإن إضافة أي عنوان بريد إلكتروني إلى "القائمة السوداء " سيضمن لكم أن رسائل البريد الإلكتروني من مرسل معين سيتم إعتبارها دائماً على أنها بريد مزعج. تتم هذه العملية بالنقر على "إعدادات الخبراء" ثم "القائمة البيضاء" أو "القائمة السوداء" و إدخال عنوان البريد الإلكتروني ذي الصلة.

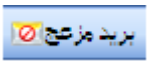
أخيراً ، يمكنكم على الصفحة الرئيسية للإعدادات تحديد كيفية عرض رسائل البريد المزعجة و ما هي الإشارة التي يجب وضعها عليها ، على سبيل المثال *** بريد مزعج – Spam ***. يمكن استخدام هذا الأمر لإنشاء قاعدة في عميل بريدكم الإلكتروني ، على سبيل المثال لنقل رسائل البريد الإلكتروني التي لها إشارة معينة بشكل تلقائي إلى مجلد آخر.

مايكروسوفت أوتلوك

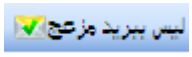
مصفي مضاد البريد المزعج بأفاست! يعمل كجزء من مكونات مايكروسوفت أوتلوك ، مما يعني أنك تستطيع ضبط بعض الميزات مباشرة من خلال برنامج أوتلوك.



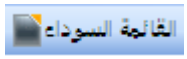
عند فتح مايكروسوفت أوتلوك بعد تركيب أفاست! الحزمة الأمنية المتكاملة ، ستلاحظ بعض الخيارات الإضافية في شريط الأدوات بأوتلوك :



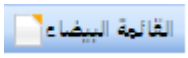
" بريد مزعج "– هي الرسالة تم نقلها إلى مجلد البريد الغير مرغوب فيه "Junk folder " و ذلك إستناداً على إعدادات مضاد البريد المزعج بإفاست!. بشكل إفتراضي فإن المجلد يدعى " avast! Junk " .



" ليس ببريد مزعج "– هي الرسالة التي تم إخراجها من مجلد " avast! Junk " .



" القائمة السوداء " – إضافة عناوين مرسلين إلى القائمة السوداء.

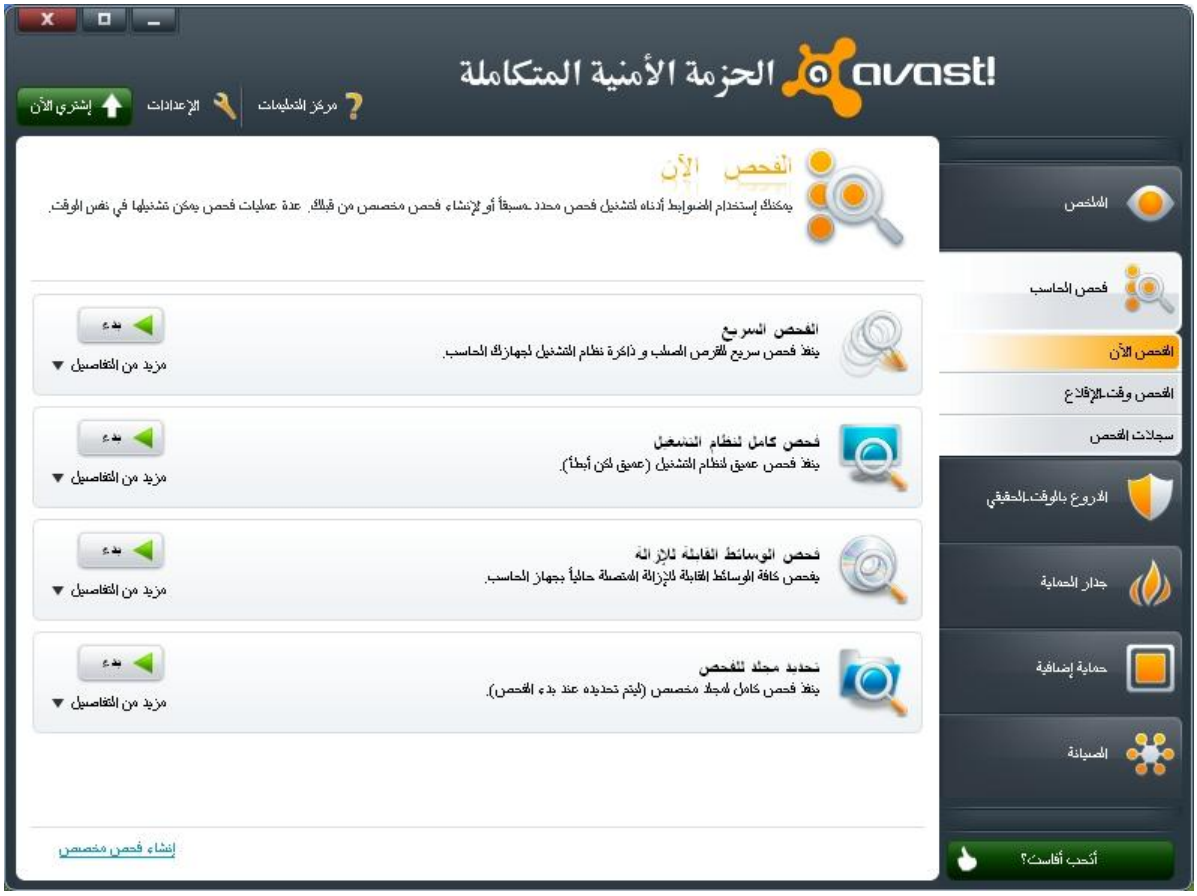


" القائمة البيضاء " – إضافة عناوين مرسلين إلى القائمة البيضاء.

علما أن الرسائل المؤشرة على أنها "بريد مزعج" لن يتم نقلها إلى مجلد " avast! Junk " تلقائياً. لنقل رسالة إلى مجلد البريد الغير مرغوب فيه "Junk folder " ، فمن الضروري تظليل الرسالة أولاً ، ثم النقر على "بريد مزعج – Spam " سيؤدي ذلك إلى نقل الرسالة . مجلد " avast! Junk " سيتم إنشاؤه تلقائياً عند الحاجة ، من ثم سيضاف إلى بنية مجلدات أوتلوك.

كيفية إجراء فحص يدوي لجهازكم الحاسب

لإجراء فحص يدوي لجهازكم الحاسب ، إفتح واجهة المستخدم و من ثم حدد علامة التبويب "فحص الحاسب – Scan computer ". هذا سيؤدي إلى فتح شاشة " فحص الآن – Scan Now " كما هو مبين أدناه.



يوفر أفاست!الحزمة الأمنية المتكاملة ٦.٠ عدد من عمليات الفحص المحددة–مسبقاً و ذلك بشكل إفتراضي.

الفحص السريع - هذا سينجز فحصاً سريعاً لقرص نظام تشغيل جهازكم الحاسب (عادة ما يكون محرك الأقراص " C:\ " على جهازكم الحاسب). بشكل إفتراضي ، فقط الملفات التي لها إمتدادات تندرج تحت درجة"خطيرة" سيتم فحصها ، على سبيل المثال الملفات ذات الإمتدادات مثل " exe " ، " com "، " bat "إلخ . فقط تلك الأجزاء في بداية ونهاية الملف ، حيث يتم عادة العثور على العدوى المحتملة ، سيتم إختبارها.

فحص كامل لنظام التشغيل – هذا سيؤدي إلى فحص أكثر تفصيلاً على كل الأقراص الصلبة على جهازكم الحاسب و بشكل إفتراضي ، كل الملفات سيتم فحصها وفقاً لمضمونها ، وبعبارة أخرى ، فإن أفاست! سينظر داخل كل ملف لتحديد نوعه ، و فيما إذا كان ينبغي أن يتم فحصه. يتم إختبار الملف بشكل كامل ، وليس فقط تلك الأجزاء في بداية أو نهاية الملف ، حيث يتم فيه عادةً العثور على العدوى.

فحص الوسائط القابلة للإزالة – هذا الخيار سيفحص الوسائط القابلة للإزالة أي في اللحظة التي يتم توصيلها بجهازكم الحاسب ،على سبيل المثال ذاكرة وميضية ، محرك أقراص صلب خارجي .. إلخ .ستفحص هذه الوسائط للكشف عن إحتمالية وجود البرامج ذات "التشغيل-التلقائي "التي قد تحاول تشغيل نفسها عندما تكون هذه الوسائط متصلة بالجهاز.

تحديد مجلد للفحص – هذا الخيار يتيح لكم فحص مجلد معين أو عدة مجلدات فقط.

لتشغيل أحد عمليات الفحص المحدد–مسبقاً الآن ، فقط إنقر فوق "بدء." . بدلاً عن ذلك ، يمكنكم جدولة الفحص ليتم تشغيله على أساس منتظم ، أو مرة واحدة فقط في وقت لاحق ، لمزيد من المعلومات يمكنكم مراجعة صفحة "الجدولة" في قسم "إعدادات الفحص." ، شاشة " الإعدادات " الأخرى يمكن إستخدمها أيضاً لإجراء فحص مخصص، أو عن طريق النقر على "إنشاء فحص مخصص" يمكنكم إنشاء فحص جديد مع كافة الإعدادات المطلوبة.

إنشاء فحص مخصص

بالنقر على زر " إنشاء فحص مخصص – Create Custom Scan " ، يمكنكم من تعريف عملية فحص جديدة متضمنةً معايير فحص خاصة بها. بعد ذلك ستفتح نافذة جديدة ، حيث يمكنكم إنشاء اسم لعملية الفحص الجديدة ، و تحديد أي جزء من أجزاء جهازكم الحاسب وأنواع الملفات التي يجب فحصها.

بشكل إفتراضي، المنطقة التي يراد فحصها تم إعدادها على "كافة الأقراص الصلبة". لتحديد منطقة جديدة تريد فحصها ، قم بفتح القائمة المنسدلة واختيار المنطقة الإضافية ليتم فحصها. لإزالة هذه المنطقة ، إنقر فوقها مرة واحدة ومن ثم انقر فوق "حذف ."يمكنكم أيضا تحديد كيفية تعرف أفاست! على الملفات المشبوهة التي يجب فحصها ، و ذلك إما عن طريق التدقيق بإمتدادات الملف أو عن طريق التدقيق بالمحتوى الفعلي:

المحتوى – إذا تم تحديده ، فإن أفاست! سينظر داخل كل ملف لتحديد نوع الملف ، و فيما إذا كان ينبغي أن يتم فحصه.

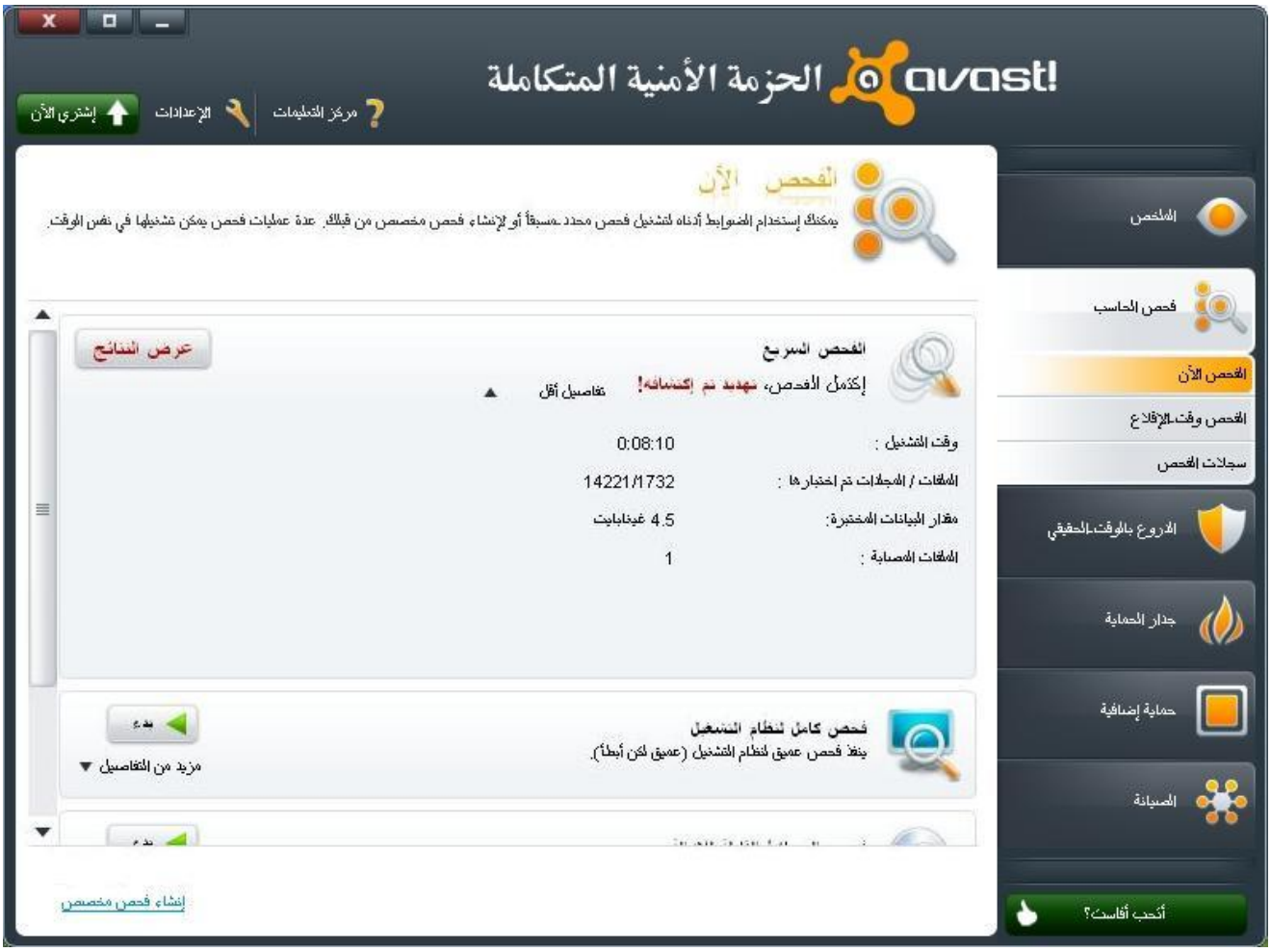
إسم الإمتداد – إذا تم تحديده ، بشكل إفتراضي ، فإن الملفات ذات الإمتدادات " exe "، " com "، " bat "إلخ سيتم فحصها فقط. يمكنكم إضافة إمتدادات الملفات الأخرى عن طريق النقر على "تحديد مناطق إضافية" وكتابة إمتدادات الملفات في مربع النص . من ثم انقر فوق "موافق". لإزالة إمتداد ملف ، انقر عليه مرة واحدة ومن ثم انقر فوق "حذف."

على هذه الصفحة ، يمكنكم أيضاً الوصول إلى إعدادات أخرى ، على سبيل المثال ، إذا كنت ترغب في تحديد موعد فحص منتظم أو لتشغيل فحص لمرة واحدة في وقت معين، وإذا كنت تريد إستثناء مجلدات أو ملفات معينة من عملية الفحص ، أو إذا كنت تريد أن تعرف ما هي الإجراءات التي ينبغي اتخاذها في حال تم الكشف عن فيروس على سبيل المثال حذف الملف ، أو نقله تلقائياً إلى حجز الفيروسات .

يمكنكم أيضاً إنشاء تقارير عن الملفات التي تم فحصها و عن الأخطاء التي وقعت خلال عملية الفحص. الإعدادات الأخرى يمكن إستخدامها لضبط سرعة وعمق الفحص .

ماذا تفعل إذا تم العثور على فيروس

في نهاية الفحص ، إذا كان البرنامج قد إكتشف ملفاً مشبوهاً ، فسيتم عرض الرسالة "تهديد تم إكتشافه – **Threat detected** " – أنظر أدناه.



لمعرفة مزيد من المعلومات حول الملفات المشبوهة والخيارات المتاحة ، انقر على "عرض النتائج – **Show Results** ".

وعندها يمكنكم مشاهدة قائمة الملفات التي إعتبرها أفاست! ملفات مشبوهة و بذلك ستكون قادراً على تحديد الإجراءات التي يمكن اتخاذها في ما يتعلق بهذه الملفات ، على سبيل المثال حذف ، نقل إلى الحجز .. إلخ وبمجرد الانتهاء من الإجراءات المحددة التي يتعين اتخاذها ، انقر فوق "تطبيق – **Apply** ".

الخيار الموصى به هو نقل الملف إلى حجز الفيروسات. حيث ستكون هذه الملفات المصابة أو المشبوهة في منطقة حجر مضمونة يمكنكم إستخدامها بأمان لتخزين مثل هذا النوع من الملفات حتى تقرر أنها آمنة و تقوم بإستعادتها إلى موقعها الأصلي. الملفات المخزنة هنا لا يمكن أن تتسبب بأيٍ من الاضرار لملفاتك الأخرى و يمكن أن يتم إصلاحها وربما قبل أن يتم نقلها مرة ثانية إلى موقعها الأصلي.

بشكل إفتراضي ، فإن الملفات المشبوهة التي يتم الكشف عنها بواسطة الدروع بالوقت–الحقيقي يتم نقلها إلى حجز الفيروسات تلقائياً.

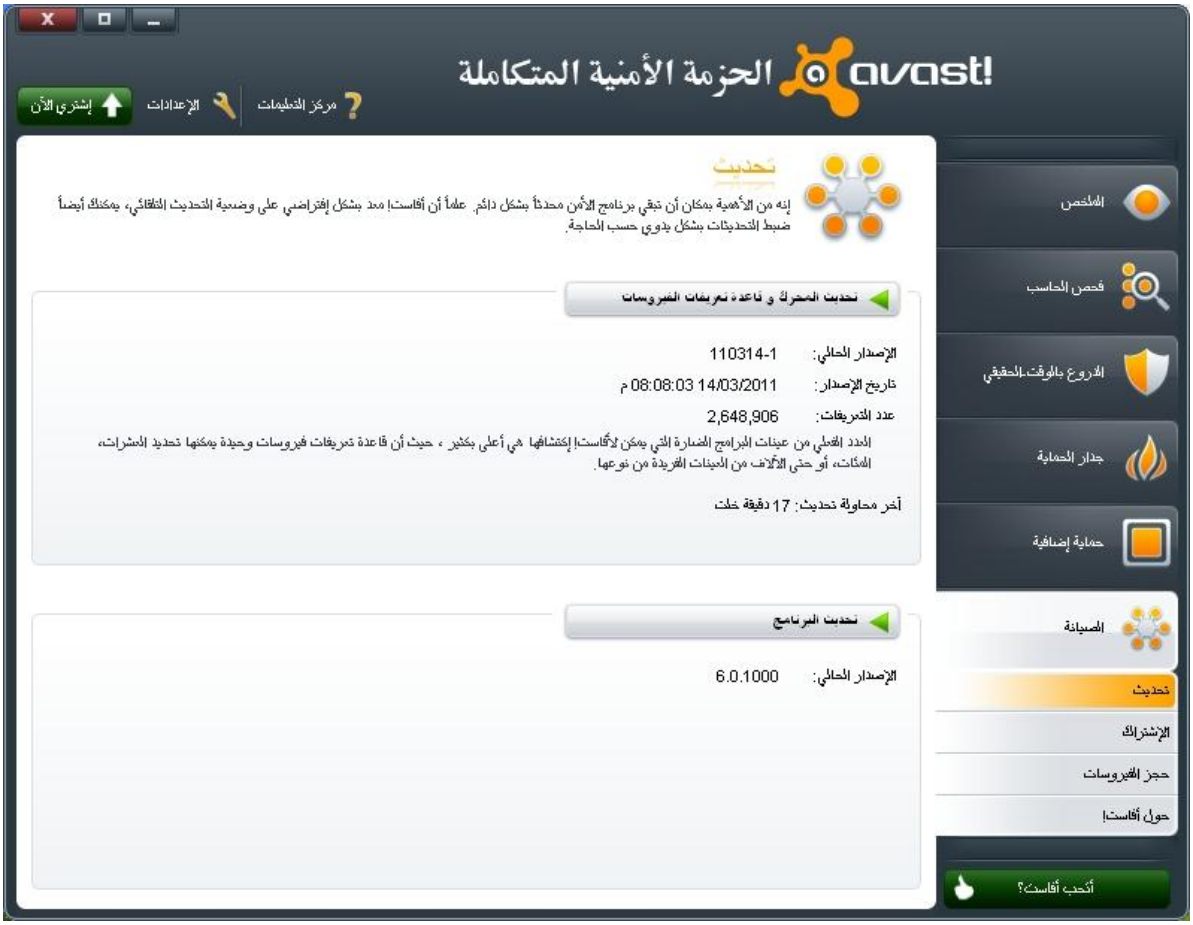
يمكنكم عرض نتائج الفحص مرة أخرى في أي وقت بالذهاب إلى قسم "سجلات الفحص – **Scan Logs** " ثم إختيار عملية الفحص التي ترغب في مشاهدتها.

كيفية إبقاء أفاست محدثاً

إن أهم ميزة ببرنامج مضاد الفيروسات هي تحديثاته المستمرة لكلاً من البرنامج و قاعدة تعريفات الفيروسات ، لهذا السبب فمن المهم أن يتم تحديث كلاً من البرنامج و قاعدة تعريفات الفيروسات بشكل منتظم.

بشكل إفتراضي ، فلقد تم إعداد أفاست! على أن يتم تحديث كل من المحرك و قاعدة تعريفات الفيروسات تلقائياً كلما توفر إصدار جديد. للتأكد من أن المحرك و قاعدة تعريفات الفيروسات معدة على "تحديثات تلقائية – Automatic update " ، انقر على "الإعدادات –Settings " ثم "التحديثات – Updates ".

في علامة التبويب الصيانة ، إذا قمتم بالنقر على "تحديث – Update " ، فيمكنكم التحقق من الإصدار الحالي لكل من "تحديث المحرك و قاعدة تعريفات الفيروسات – Update engine and virus definitions " و "البرنامج – Program ".



"المحرك" هو ذلك الجزء من البرنامج الذي يقوم بتفحص جهازكم الحاسب بحثاً عن التهديدات المحتملة مستنداً بذلك على قاعدة تعريفات الفيروسات.

"البرنامج" يعني ما تشاهدون أعلاه ممثلاً بواجهة المستخدم التي تستخدم لضبط ما يقوم به البرنامج.

يمكنكم التحديث يدوياً إما عن طريق النقر على السهم الأخضر. لاحظ أن النقر على "تحديث البرنامج –Update Program " يؤدي بشكل تلقائي إلى تحديث كلٍ من البرنامج ومحرك البرنامج و قاعدة تعريفات الفيروسات.

نشكركم على إختيار أفاست!