الكثير منا يستخدم برامج مضادات الفيروسات .. والأغلب يعتمد على برنامج نورتون أنتي فيروس .. لذلك رأيت كتابة دراسة شاملة عن هذا البرنامج في إصدارته الاحترافية ..

وسوف تكون الدراسة عبارة عن سلسلة من عدة دروس ..

ولنبدأ الآن **درسنا الأول** ..

Norton Antivirus Professional Edition

برنامج نورتون مضاد الفيروسات الإصدار المتخصص

حول البرنامج :

برنامج نورتون مضاد الفيروسات يمدك بإمكانيات منع الفيروسات والتعرف عليها وإزالة برامجها من جهازك. ويعمل تلقائيا على الوصول إلى الملفات المصابة ثم إصلاحها للحفاظ على بياناتك سليمة والعمل على حمايتها.
كما أن خدمة التحديث لتعريفات الفيروسات عبر الانترنت بسهولة تحافظ على أن يكون نورتون مضاد الفيروسات مستعد دائما لمواجهة كافة التهديدات .

خصائص هذا البرنامج :

البرنامج ليس مجرد واقي من الفيروسات .. بل يتعدى ذلك إلى إمكانيات ضخمة وهائلة قلّما تجدها في أمثاله من هذه البرامج .. وأهم خصائصه هي :

P مانع الديدان Worm Blocking

يوفر برنامج نورتون أنتي فيروس عملية مسح لمرفقات الرسائل الالكترونية Email

Attachments التي ترسلها للبحث عن ملفات الديدان Worms وينبهك قبل إرسال أي ملف مصاب. فيقوم البرنامج بمنع هذه الديدان ويوصي بالإجراء الذي يجب اتخاذه، حتى لا يتم إرسال تلك الملفات بالبريد الالكتروني.

P اختبارات وتدعيم فوري للرسائل

تتيح الإصدارة الجديدة من نورتون عمل مسح للرسائل المستلمة بواسطة America Online ، و Yahoo ، و MSN وهي مواقع توفر الرسائل الفورية. فيمكنك الاختيار بين مسح للرسائل المستلمة بواسطة احد أو جميع تلك المواقع . ويمكن لبرنامج نورتون إصلاح أو حجر الملفات التي يجدها مصابة

P التوسع في إصلاح الملفات والإلغاء

أيضا الإصدارة الجديدة من نورتون مضاد الفيروسات يمكنها الآن إصلاح جميع الملفات القابلة للإصلاح Repairable Files تلقائياً بدون أي تدخل منك. بالإضافة إلى الإلغاء التلقائي للملفات التي يجدها البرنامج تحتوي على ديدان Worm أو حصان طروادة Trojan Horse وهي مصطلحات لبعض أنواع من الفيروسات.

P كلمة سر الحمايةPassword Protection

يوفر برنامج نورتون الآن إمكانية أن تقوم بإعداد أو تغيير وإعادة إعداد كلمة سر Password للتحكم في إعداد اختياراتك ، حتى لا يمكن للمستخدم الغير مرخص له التأثير على حماية ملفاتك ضد الفيروسات.

P عارض سجل الدخول Log Viewer

ينظم نورتون معلومات عن تحذيرات الفيروس Virus Alerts ، وأنشطة التطبيقات Aplication Ativities ، و الأخطاء .Erors ويمكنك تحديد عدد الأنشطة التي تريد تسجيلها.

بالإضافة الى الكثير من الامكانيات التي سنتعرف عليها من خلال الفقرات القادمة ..

كيف يعمل نورتون أنتي فيروس .. ؟؟

يراقب نورتون جهاز الكمبيوتر للفيروسات المعروفة وغير المعروفة ، الفيروسات المعروفة هي تلك التي يشعر بها نورتون ويتعرف عليها بالاسم.، والفيروس الغير معروف هو ذلك الذي لا يملك له نورتون أي تعريف. يراقب نورتون جهازك لحمايته من كل من النوعين ، فيستخدم تعريف الفيروس Virus Definitions ليشعر بالفيروسات المعروفة ، ويستخدم تكنولوجيا Bloodhound ، و Script Blocking ، و Worm Blocking ليشعر بالفيروسات غير المعروفة.
تعريفات الفيروس، وتكنولوجيا Bloodhound ، و Script Blocking ، ومسح البريد الالكتروني والرسائل السريعة يستخدمون جميعاً أثناء مواعيد المسح المحددة مسبقاً، وأيضا أثناء المسح اليدوي كما يستخدمون بالحماية التلقائية لاستمرارية مراقبة الكمبيوتر .

P خدمة تعريف الفيروس توقف الفيروسات المعروفة

تتكون خدمة تعريف الفيروس من ملفات يستخدمها برنامج نورتون مضاد الفيروسات في التعرف على الفيروسات ويوقف نشاطها. يمكنك إيقاف أسماء الفيروسات من نورتون مضاد الفيروسات الإصدارة المتخصصة ثم تدخل إلى موسوعة توصيف الفيروسات في موقع Symantec على الانترنت.

P تكنولوجيا Bloodhound توقف الفيروسات غير المعروفة

Bloodhound هي تكنولوجيا خاصة بإصدارة نورتون مضاد الفيروسات المتخصصة لمسح الفيروسات للتعرف على الفيروسات الجديدة وغير المعروفة .وهي تشعر بالفيروسات عن طريق تحليل تركيب الملفات، وسلوكها، والتعرف على خواص أخرى مثل المنطق البرمجي، وتعليمات الكمبيوتر وأي بيانات أخرى موجودة في الملف. وهي أيضاً تهيئ محاكاة البيئة التي يتم فيها تحميل المستند وتختبر فيروسات الماكرو.

P تكنولوجيا مانع النص Script Blocking توقف الفيروسات المبنية على النص

Script هو برنامج مكتوب بلغة النصوص مثل النص المكتوب بلغة Visual Basic أو لغة JavaScript ويمكن التخلص منها دون تدخل من المستخدم. وهذا النص يمكن فتحه عن طريق برامج تحرير النصوص Text Editor أو معالجة الكلمة Word Processing لذلك فتغييره في غاية السهولة.
النصوص يمكن استخدامها عند الدخول إلى الانترنت أو فحص البريد الالكتروني. إعادة تشغيل الكمبيوتر يتضمن استخدام النصوص التي تخبر الكمبيوتر أي البرامج يقوم بتحميلها وتشغيلها. ويمكن كتابة النص أيضاً لعرض الأنشطة الماكرة إذا تم تشغيلها. يمكنك دون أن تدري

استقبال نصوص ماكرة عند فتح مستند أو ملحقات بريد الكتروني ، او عند استعراض رسائل بريد HTML مصابة، أو زيارة مواقع انترنت مصابة .
مانع النصوص Script Blocking يشعر بفيروسات نصوص لغة Visual Basic ، ولغة JavaScript بدون الحاجة إلى تعريفات الفيروسات. فهو يراقب أنشطة النصوص المشابهة للفيروسات ثم ينبهك إذا وجدها.

P مانع الديدان Worm Blocking يوقف الديدان قبل انتشارها

الديدان Worms تختبئ في الملفات ولا تكون نشطة أو خطرة حتى يتم فتح الملفات المصابة، ويمكن دون أن تدري نسخ أو إرسال الملف المصاب بالبريد الالكتروني. الملف المصاب بالديدان لا يمكن إصلاحه، فيجب مسحه. وتقوم خاصية مانع الديدان Worm Blockingبمسح كل رسائل البريد الالكتروني المرسلة وتنبهك إذا وجدت الديدان. بمجرد الوصول إلى أحد الديدان يقوم نورتون بإيقافها ويقترح الأجراء المفضل اتخاذه، لذلك يتم منع ارساله بالبريد الالكتروني.

P الحماية التلقائية Auto-Protect تؤمن الكمبيوتر

يتم تحميل الحماية التلقائية لبرنامج نورتون مضاد الفيروسات الإصدارة المتخصصة في الذاكرة عند بدء تشغيل ويندوز، مما يمدك بحماية ثابتة أثناء العمل.
باستخدام الحماية التلقائية Auto-Protect فان نورتون يقوم تلقائياً بالأعمال الآتية :

× التخلص من الفيروساتViruses ، والديدانWorms ، وحصان طروادة Trojan horses ، ويشمل ذلك فيروسات الماكرو ، وإصلاح الملفات المصابة.

× الفحص ضد الفيروسات كلما تقوم باستخدام البرامج في الكمبيوتر، أو عند إدخال الأقراص المرنة أو أي وسائط أخرى ، كذلك عند استخدامك المستندات التي تتسلمها أو تقوم بإنشائها بنفسك.

× مراقبة جهازك ضد أي من الأعراض غير الطبيعية التي يمكن أن تكون ناتجة عن وجود فيروس نشط.

× حماية جهازك ضد الفيروسات التي تنتج عن طريق الانترنت.

P التراجع عن الإلغاء UnErase يستعيد الملفات المفقودة

التراجع عن الإلغاء يساعدك على استعادة المفات التي نقلتها إلى سلة مهملات نورتون. لأن سلة مهملات نورتون المحمية تساعد على تحسين أداء سلة مهملات ويندوز بحماية الملفات من الإلغاء النهائي. فمعالج التراجع عن الإلغاء UnEraseWizard يتيح لك استعادة تلك الملفات المحمية .

P المسح النهائي للملفات بواسطة Wipe Info

لحماية معلوماتك الخاصة يتم المسح أو إزالة محتويات الملفات نهائياً بواسطة.Wipe Info فعن طريق Wipe Info يمكنك مسح ملف معين أو مجلد بالكامل بطريقتين Fast Wipe أو Government Wipeللحماية النهائية.

✦ كيفية صيانة الحماية

عندما تنزل برنامج نورتون مضاد الفيروسات الإصدارة المتخصصة فقد أكملت الحماية ضد الفيروسات. ومع ذلك فهناك الجديد من الفيروسات التي يتم صنعها دائماً. فالفيروسات يمكن أن تنتشر عندما تبدأ تشغيل جهاز الكمبيوتر من خلال قرص مصاب أو برنامج مصاب. وهناك العديد من الأشياء يمكنك عملها لتفادي الفيروسات أو للشفاء السريع عند التعرض لهجوم فيروسي.

✦ تفادي الفيروسات

من الأهمية أن تقوم يعمل صيانة دورية للملفات مع العمل على التحديث الدائم لبرنامج نورتون مضاد الفيروسات، ولتفادي الفيروسات:

× اعمل دائما للحصول على المعلومات الخاصة بالفيروسات بالدخول إلى موقع Symantec Security Response على الانترنت في العنوان :

http://securityresponse.symantec.com/

حيث تحصل على الجديد من المعلومات الشاملة والحديثة عن الفيروسات والحماية ضد الفيروسات.

× اعمل على التشغيل المنتظم لميزة التحديث الدائم LiveUpdate للتحديث المستمر لملفات تعريفات الفيروسات، وللحصول على تحديثات البرنامج.

× اعمل على التشغيل الدائم للحماية التلقائية Auto-Protect في جميع الأوقات لمنع الفيروسات من إصابة جهاز الكمبيوتر.

× إذا لم تكن الحماية التلقائية مشغلة فيجب عمل مسح للوسائط الخارجية قبل تشغيلها.

× اعمل على تشغيل جدول للمسح الدوري تلقائياً.

× احذر رسائل البريد الالكتروني مجهولة المصدر، ولا تفتح الملحقات المجهولة.

× اعمل على التشغيل الدائم لمانع الديدان Worm Blocking لتفادي إرسال ملحقات بريد الكتروني مصابة.

× اعمل على التشغيل الدائم لمانع النص Script Blocking لملاحظة أي سلوك مشابه للنشاط الفيروسي.

× اعمل على تشغيل أقصى إعدادات حماية موصى بها.

⌖ أقراص الطوارئ ... Rescue Disks كن مستعدا !

تستخدم أقراص الطوارئ في إعادة بدء تشغيل جهاز الكمبيوتر والمسح للفيروسات في حالة وجود مشاكل بالجهاز .
إذا كان بإمكان جهاز الكمبيوتر إعادة البدء من القرص المضغوط CD ، فيمكنك استخدام القرص المضغوط الخاص ببرنامج نورتون بدلاً من أقراص الطوارئ ولا تحتاج لعمل أقراص الطوارئ Emergency Disks .
تتكون مجموعة أقراص الإنقاذ Rescue Disks من قرص مرن للتشغيل Bootable Floppy Disk ، وقرص مرن لبرنامج نورتون مضاد الفيروسات ، وثلاث أقراص مرنة لتعريفات الفيروسات..
وباستخدام مجموعة أقراص الإنقاذ يمكنك بدء تشغيل جهاز الكمبيوتر في نمط DOS ثم استخدام برنامج نورتون مضاد الفيروسات للتخلص من المشاكل المتعلقة بالفيروسات.
تحتوي أقراص الإنقاذ على معلومات خاصة بجهاز الكمبيوتر الذي تم صنعها عليه . فإذا استخدمت أقراص الإنقاذ في الإنقاذ Recovery ، فيجب أن تستخدم أقراص الإنقاذ التي تم صنعها على نفس جهاز الكمبيوتر. أما إذا كنت تستخدمها لعمل مسح للفيروسات فيمكنك استخدام أي أقراص مخاطرة تم صنعها لأجهزة كمبيوتر أخرى.
إذا لم تستطع إعادة بدء جهاز الكمبيوتر، يمكنك إتباع التعليمات الآتية لصناعة أقراص الطوارئ على جهاز كمبيوتر آخر أو الذهاب إلى العنوان التالي على الانترنت لتحميل برنامج أقراص الطوارئ:

http://www.symantec.com/techsupp/ebd.html

كما بمكنك صناعة الأقراص بنفسك من خلال مجلد Support folder ستجد بداخله مجلد EDISK وداخله الأداة NED.exe انقر عليها واتبع التعليمات .. في حال لم تصنعها من خلال البرنامج قبل انهيار النظام .. ويمكنك صناعتها أيضا من خلال البرنامج باستخدام معالج أقراص الطوارئ Rescue Disks .

تحياتي .. محمد قطان ..

نكمل ما بدأنا به من شرح برنامج النورتون أنتي فيروس .. والآن مع **الدرس الثاني** ..

أدوات البرنامج

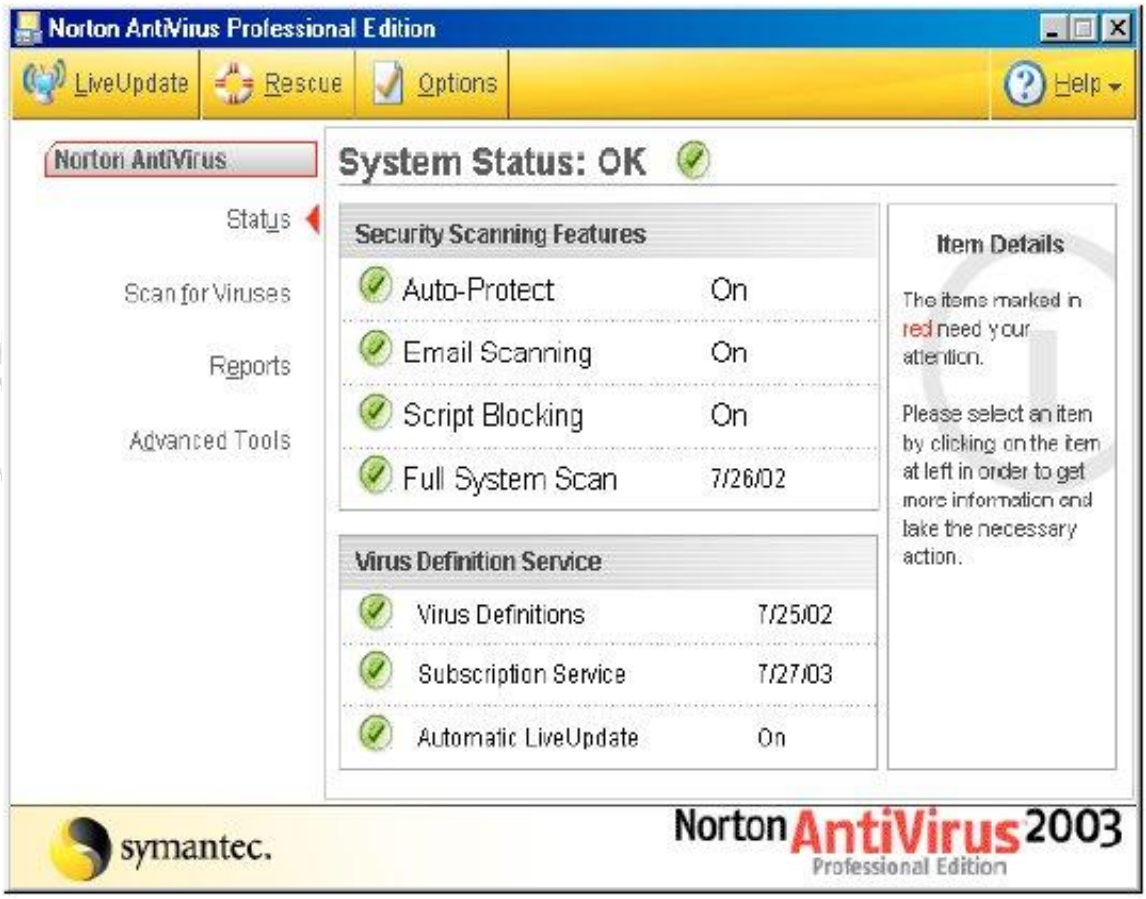
تظهر في الواجهة الرئيسية للبرنامج الأدوات التالية :

- تقرير الحالة Status Reporting
- خيارات المسح Scanning Options
- خيارات الجدولة Scheduling Options
- تقرير الأنشطة Activity Reporting
- إنقاذ الملفات و الإلغاء النهائي للملفات
- خيارات تشكيل جهاز الكمبيوتر

فحص حالة النظام System Status

إذا كان برنامج نورتون يعمل بطريقة غير طبيعية، أو إذا كنت غير متأكد من عمل مسح لجهازك ضد الفيروسات فيمكنك عمل اختبار لحالة النظام لديك.
في لوحة الحالة من النافذة الرئيسية لبرنامج نورتون تظهر علامة اختبار Check Mark تبين أن حالة النظام جيدة OK أو يظهر مثلث يبين أن حالة النظام تحتاج إلى عناية .
إذا رأيت المثلث راجع الخصائص Features والخدمات Servicesلمعرفة ما يحتاج إلى العناية.
إذا أردت ضبط أي من الإعدادات استخدم الاختيارات Options .

لعمل فحص لحالة النظام :
١. ابدأ تشغيل برنامج نورتون ..



٢. في نافذة الحالة Status window راجع الحالة على يسار كل خاصية Feature
٣. للحصول على مزيد من المعلومات لكل خاصية انقر فوقها. تعرض اللوحة اليمنى المزيد من المعلومات والارتباط الخاص بالخاصية.

تخصيص برنامج نورتون

إذا كنت تستخدم ويندوز ٢٠٠٠ أو XP وكنت أنت المدير Administrator فيمكنك تغيير خيارات نورتون وليكن في اعتبارك أن التغييرات التي تجريها سوف يتم تطبيقها على جميع مستخدمي الجهاز أما أن لم تكن المدير وليس لديك إمكانية الدخول كمدير فلن يمكنك تغيير اختيارات نورتون.

الإعدادات الافتراضية لبرنامج نورتون تمدك بالحماية الكاملة ضد الفيروسات . ومع ذلك يمكن أن تحتاج إلى ضبط تلك الخيارات لتحسين عرض النظام أو إلغاء بعض الاختيارات التي لا تريد تشغيلها.

كما يمدك نورتون بحماية الإعدادات التي تقوم بضبطها عن طريق كلمة مرور . Password ويمكنك إتاحة استخدام كلمة المرور كما يمكنك تغييرها حتى لا يمكن لأحد العبث بإعداداتك.

جميع الإعدادات الخاصة بخيارات نورتون يتم ترتيبها تحت ثلاث مجموعات رئيسية كما يلي :

١. النظام System وبه الاختيارات :

- Auto-Protect ×
- Bloodhound o
- Advanced o
- Exclusions o
- Script Blocking ×
- Manual Scan ×
- Bloodhound o
- Exclusions o

٢. الإنترنت Internet وبه الخيارات:

- Email ×
- Advanced ×
- Instant Messenger ×
- LiveUpdate ×

٣. خيارات أخرى :

- (Windows 98/98SE/Me) Inoculation ×
- Miscellaneous ×
- Advanced Tools ×

هذا الجزء لا يصف كيفية تغيير الاختيارات المنفردة ، ولكن يوضح بدقة ما تفعله الاختيارات وكيف تجدهم .

خيارات النظام

تتحكم خيارات النظام في المسح Scanning ومراقبة Monitoring جهاز الكمبيوتر. ويمكنك أن تستخدم خيارات النظام لتحديد ما الذي تريد مسحه ضد الفيروسات ، و ما الذي تبحث عنه بعملية المسح ، وما الذي تريد عمله عند الوصول إلى الفيروس أو إلى النشاط الفيروسي .

بعد تحميلك برنامج نورتون يمكن أن تريد ضبط الحماية إلى المستوي الأدنى أو إلغاء تشغيل تلك الخيارات التي لا تحتاج إليها .

١. الاختيار : الحماية التلقائيةAuto-Protect : وهذا الخيار يحدد ما إذا كانت الحماية التلقائية تبدأ مع بدء تشغيل جهاز الكمبيوتر، وما الذي يتم البحث عنه أثناء مراقبة جهاز الكمبيوتر وما الذي يجب عمله عند الوصول إلى الفيروس.

وتكنولوجيا المسح Bloodhound تحمي ضد الفيروسات الغير معروفة . استخدم تلك الخيارات لضبط مستوى حساسيتها في الحماية التلقائية .

والخيارات المتقدمة Advanced options تحدد الأنشطة التي يتم مراقبتها عند المسح ضد الأنشطة التي تشبه الفيروسات وعند مسح الاسطوانات المرنة .

والاستثناءات Exclusion تحدد الملفات التي لن يتم مسحها وذلك عن طريق امتدادات اسم الملف Extension أو عن طريق اسم ملف محدد. وتأكد من عدم استثناء أنواع الملفات التي يمكن إصابتها بالفيروسات مثل الملفات التي لها ماكرو أو الملفات التنفيذية.

٢. الاختيار : مانع النصوص Script Blocking : وهو يتيح تشغيل مانع النصوص ويضبط ما يفعله نورتون عندما يجد نصاً ماكراً . إذا كنت من مطوري أو مصححي النصوص يمكنك إغلاق مانع النصوص وإلا فان تلك الخاصية سوف تمنع النصوص التي تقوم بإعدادها .
٣. الاختيار المسح اليدوي Manual Scan : وهو يحدد ما يتم مسحه والذي يحدث عند وجود فيروس خلال المسح الذي تطلبه، ويتضمن المسح اليدوي أيضاً الأقسام Bloodhound و Exclusions .

خيارات الانترنت:

تحدد خيارات الانترنت ما يحدث عند اتصال جهازك بالانترنت .ومن خلال استخدامها تعرف كيف يقوم نورتون بعمل مسح للبريد الالكتروني Email وارتباطات المرسل الفوري Instant Messenger Attachments، ويتيح مانع الديدان Worm Blocking ويحدد كيفية تطبيق التحديث الدائم LiveUpdates .

١. البريد الالكتروني : EMAIL وهو يتيح عمل مسح فيروسي للبريد الالكتروني ، ومانع الديدان Worm Blocking ، ويحدد كيفية تصرف نورتون عند عمل مسح فيروسي لرسائل البريد الالكتروني. المسح الفيروسي للرسائل القادمة يحمي جهاز الكمبيوتر ضد الفيروسات المرسلة . المسح الفيروسي للرسائل الصادرة يمنع النقل غير المقصود للفيروسات أو الديدان إلى الآخرين. يمكنك الاختيار للمسح الفيروسي للرسائل الصادرة أو الواردة بالبريد الالكتروني أو كلاهما وان تختار عرض الرمز Icon أو مؤشر التقدم Progress Indicator أثناء المسح الفيروسي. يمكنك ضبط الخيارات لعمل أصلاح تلقائي أو عمل حجر Quarantine أو إلغاء Delete للرسائل المصابة بتدخل أو بدون تدخل منك. الخيارات المتقدمة تحدد تصرف البرنامج عند عمل مسح فيروسي لرسائل البريد الالكتروني.

٢. المرسل الفوري Instant Messenger : وهو يحدد ما يدعمه المرسل الفوري، وكيفية عرض مرسل جديد وما يحدث عند وجود فيروس خلال دورة مرسل فيروس.

٣. التحديث الدائم LiveUpdate : وهو يتيح لك التحديث الدائم تلقائياً ويحدد كيفية تطبيق التحديث. التحديث الدائم التلقائي يبحث عن التعريفات المحدثة للفيروسات وتحديثات البرنامج تلقائياً عند الاتصال بالانترنت .

خيارات أخرى:

وهـي تتضـمن إعـدادات التطعـيم Inoculation settings فـي ويـندوز ٩٨ ، و SE ٩٨ ، و ME ، و الإعـدادات المتنوعـة .Miscellaneous settings يمكنـك إتاحـة التطعـيم Inoculation ، وعمـل تحذير عند حدوث أي تغيير في أحد ملفـات النظـام ، وضـبط العديـد مـن الاختيـارات المتنوعـة . Miscellaneous Options

١. التطعيم Inoculation : وهو يتيح التطعيم للملفات ، وإذا تم تغيير ملـف مـن ملفـات النظـام أختـر تحـديث لقطـة التطعـيم Inoculation Snapshot أو إصـلاح الملـف بإعـادة تخزينـه بـالقيم الأصلية. خيارات التطعيم تكون متاحة فقط في ويندوز ٩٨ ، و SE ٩٨ ، و ME .

٢. التنـوع Miscellaneous : يصـنع نسـخة احتياطيـة Back up مـن الملـف فـي الحجـر Quarantine قبل محاولة إصلاحه. (هذا الاختيار يضبط تلقائياً على وضع التشـغيل. On) ومـن خلاله يمكن عمل تنبيه إذا أصبحت الحماية ضد الفيروسات تحتاج إلـى تحـديث. وكـذلك عمـل مسح فيروسـي للملفات أثناء تشـغيل النظـام (فـي ويـندوز ٩٨ ، و SE ٩٨ فقـط) ، كمـا يتـيح الحماية بكلمة مرور للخيارات .

٣. الأدوات المتقدمـة Advanced Tools : تخصـص السـلوك والاسـم لرمـز سـطح المكتـب Desktop Icon لسـلة مهملات نورتون. يتيح أو يمنع تخصيص حماية نورتون للملفـات الملغيـة Deleted files .

ويمكن التعديل بسـهولة في هذه الخيارات من خلال نافذة الخيارات Options Window ..

حماية الاختيارات Options بكلمة مرور Password

يمكنك اختيار الحماية أو إلغاء الحماية من إعدادات الخيارات الخاصة بك باستخدام كلمة مرور Password إذا خصصت كلمة مرور سوف تسأل لإدخالها كلما فتحت نافذة الاختيارات Options window، أو كلما أتحت أو منعت الحماية التلقائية Auto-Protect .

إذا نسيت كلمة المرور يمكنك إعادة ضبطها عن طريق زر المساعدة Help button من النافذة الرئيسية لبرنامج نورتون .

لتخصيص أو إلغاء كلمة المرور :

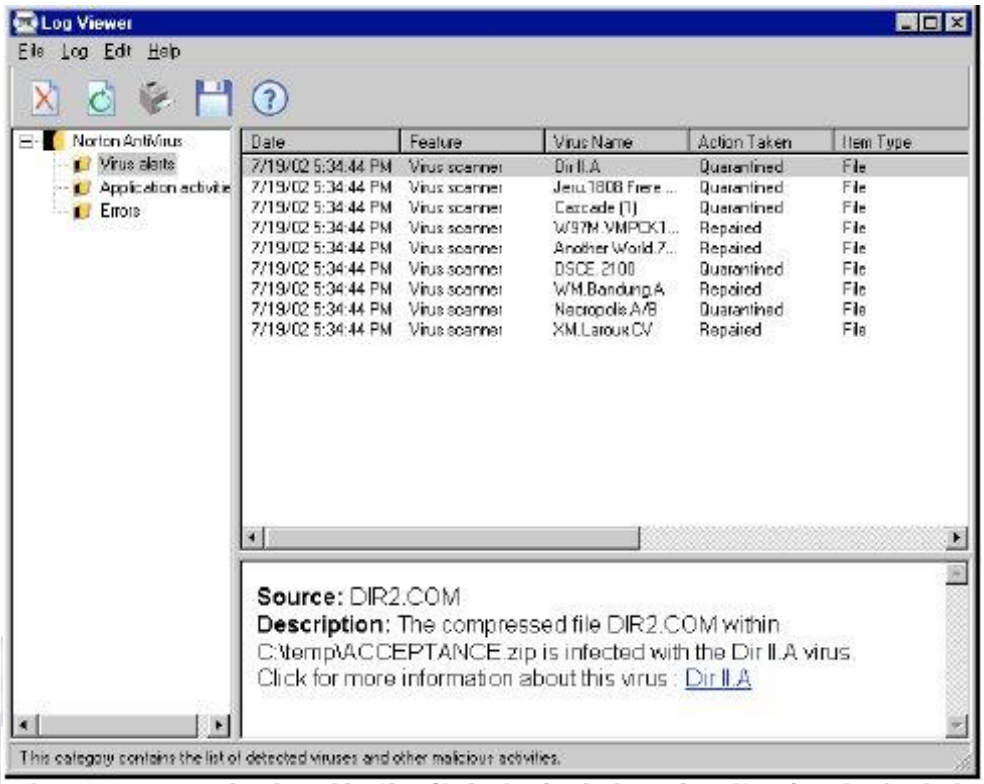
١. ابدأ تشغيل برنامج نورتون
٢. من نافذة البرنامج الرئيسية انقر فوق الخيارات Option
٣. من نافذة الاختياراتOptions window تحت الاختيارات الأخرى Other انقر المتنوعاتMiscellaneous .
٤. حدد أو قم بإلغاء التحديد من الاختيار إتاحة حماية الاختيارات بكلمة مرور Enable password protection for options
٥. قم بإدخال كلمة المرور في صندوق حوار كلمة المرور ثم زر الموافقة ..

مراقبة أنشطة نورتون

سوف تحتاج في بعض الأحيان إلى مراجعة الأنشطة السابقة لنورتون مضاد الفيروسات، مثلا معرفة متى تم عمل آخر مسح فيروسي للنظام ، أو كم عدد الفيروسات التي وجدت في الأسبوع الماضي. يعرض برنامج نورتون مضاد الفيروسات تقريراً عن الفيروسات التي وجدها، والتطبيقات ، الأخطاء في الأنشطة عارض سجل الأداء Log Viewer .
قم بمراجعة سجل الأنشطة Activity Log لمعرفة المهام التي أتمها برنامج نورتون مضاد الفيروسات ونتائج تنفيذ تلك المهام للتأكد من أن إعدادات الاختيارات Options settings تم ضبطها جيداً لمواجهة احتياجاتك بدقة.

لمراجعة الأنشطة :

١. ابدأ تشغيل برنامج نورتون مضاد الفيروسات
٢. من نافذة البرنامج الرئيسيةMain Window انقر فوق تقارير Reports
٣. من لوحة التقارير Reports pane في خط سجل الأنشطة انقر عرض التقارير View Report



٤. من اللوحة اليسرى انقر السجل الذي ترغب في مراجعته

كلما تنقر كل سجل يتم عرض معلومات خاصة به في اللوحة اليمنى. تظهر أحدث الأنشطة أعلى قائمة كل سجل.

مازال للحديث بقية .. في درس قادم بإذن الله ..
أرحب بمناقشاتكم حول الموضوع ..

تحياتي ..
محمد قطان ..

فيما يلي **الدرس الثالث** من دروس الدورة الخاصة ببرنامج نورتون أنتي فيروس ..

بسم الله نبدأ ..

حماية الجهاز والبيانات من الفيروسات

يتطلب الاحتفاظ بجهاز الكمبيوتر في حالة حماية ضد الفيروسات انتظام المراقبة عن طريق الحماية التلقائية Auto-Protect ، و مانع النصوص Script Blocking ، و مانع الديدان Worm Blocking، والمسح الفيروسي لملحقات رسائل البريد الالكتروني والملفات المنقولة بواسطة المرسل الفوري Instant Messenger ، والمسح الفيروسي المتكرر للنظام. وكل تلك المهام يمكن ضبطها لتتم تلقائياً .
للحماية الإضافية من نورتون في ويندوز ٩٨ ، و ٩٨ SE ، و ME ، يمكنك إتاحة التطعيم Inoculation لينبهك عند حدوث أي تغيير في ملف من ملفات النظام.

التأكد من تشغيل كافة إعدادات الحماية

تم إعداد برنامج نورتون ليوفر الحماية المتكاملة ضد الفيروسات . ومن المستبعد أن تحتاج إلى تغيير أي من تلك الإعدادات. ومع ذلك للوصول إلى الدرجة القصوى من الحماية يجب أن تتأكد من تشغيل جميع أشكال الحماية .

ويمكن استعراض جميع أشكال الحماية المتاحة في برنامج نورتون كما يلي :

- **P** الحماية التلقائيةAuto-Protect

ويمكن الوصول إلى الإعداد الخاص بها عن طريق النافذة الرئيسية للبرنامج و التأكد من أنها متاحة Enable وتم ضبطها على وضع التشغيل On

- **P** المسح الفيروسي للبريد الالكترونيEmail scanning

ويمكن الوصول إلى الإعداد الخاص بها عن طريق الاختيارات Options ثم اختيار البريد الالكتروني Email وأقصى حماية لهذا الاختيار هو ضبطه على المسح الفيروسي للبريد الإلكتروني الصادر والوارد ، وإذا كان برنامج البريد الإلكتروني يستخدم أحد بروتوكولات الاتصال المدعمة يتم اختيار كلا النوعين افتراضياً .

P الحماية ضد نفاذ الوقتTimeout protection

ويمكـن الوصـول إليهـا عـن طريـق الاختيـارات Options ثـم البريـد الإلكترونـي Email وأقصـى إعـدادات الحمايـة لهـذا الاختيـار هـو تحديـد الاختيـار حمايـة ضـد نفـاذ الوقـت عنـد المسـح الفيروسـي للبريد الإلكترونـي Protect against timeouts when scanning Email لمنـع انتهـاء وقت الاتصال أثناء استلام كمية كبيرة من الملحقات Attachments

P المسح الفيروسي للمرسل الفوري Instant messenger scanning

ويمكن الوصول إليها عن طريق الاختيارات Options ثم المرسـل الفـوري Instant messenger وأقصى إعدادات الحماية لهذا الاختيار هو تحديد المرسل الفوري الذي تريد حمايته .

P مانع الديدان Worm Blocking

ويمكـن الوصـول إليهـا عـن طريـق الاختيـارات Options ثـم البريـد الإلكترونـي Email وأقصـى إعدادات الحماية لهذا الاختيار هو تحديد الاختيار إتاحة مانع الديـدان Enable Worm Blocking و الاختيـار التنبيـه عنـد المسـح الفيروسـي لملحقـات البريـد الالكترونـي Alert me when scanning email attachments.

P مانع النصوص Script Blocking

ويمكـن الوصـول إليـه عـن طريـق الاختيـارات Options ثـم الاختيـار Script Blocking وأقصـى إعدادات الحماية لهذا الاختيار هو تحديد الاختيار Enable Script Blocking

P التطعيم Inoculation

ويمكن الوصول إليه عـن طريـق الاختيـارات Options ثـم اختيـار التطعـيم Inoculation وأقصـى إعدادات الحماية لهذا الاختيار هو تحديد Inoculate Boot Records

والنقاط السابقة هي خيارات لأقصى إعدادات الحماية في النورتون ..

الاستمرار مع التحديث الدائم LiveUpdate

تعتمد منتجات شركة Symantec على المعلومات الحديثة في حماية جهازك من التهديدات المكتشفة حديثاً. وتكون هذه المعلومات متاحة لك عن طريق التحديث الدائم LiveUpdate. ويتم التحديث الدائم عن طريق استخدام اتصال الانترنت حيث يتم الحصول على تحديثات البرنامج وتحديثات الحماية لجهازك .

تحديثات البرنامج Program Updates

تحديثات البرنامج هي تحسينات طفيفة على البرنامج الذي قمت بتحميله. ويختلف ذلك عن ترقية البرنامج ، حيث تكون الترقية هي إصدارة جديدة من نفس المنتج. تحديثات البرنامج التي لها صفة التحميل الذاتي Self-installers لتحل محل المعلومات الحالية في البرنامج تسمى الحزم Patches .

والحزم Patches عادة يتم عملها لتكون امتداد لنظام التشغيل أو لتوافق الأجهزة Hardware ، و أيضا لضبط قضية العرض Performance Issue ، ولإصلاح الأعطال .

تتيح عملية التحديث الدائم LiveUpdate الحصول التلقائي على البرامج وتحميل التحديثات. فهي تحدد موقع الملفات ثم تحصل عليها من موقع الانترنت، ثم تقوم بتحميلها، ثم بعد ذلك تقوم بإزالة الملفات المتبقية من جهاز الكمبيوتر.

تحديثات الحماية Protection Updates

هي ملفات متاحة من الشركة المنتجةSymantec ، عن طريق الاشتراك Subscription ، الذي يجعل منتجات Symantec لديك محدثة دائماً بأحدث تكنولوجيا مواجهة التهديدات. وتعتمد تحديثات الحماية التي تتسلمها على نوع المنتج الذي تستخدمه. ونوضح ذلك كما يلي:

× أعمال نظام نورتون

مستخدمي نورتون ، وأعمال نظام نورتون يتسلمون خدمات تحديث تعريفات الفيروسات ، والتي تمد بإمكانية الدخول إلى خدمة Latest Virus Signatures وخدمات تكنولوجية أخرى من شركة Symantec

✣ حماية الإنترنت في نورتون

بالإضافة إلى خدمة تعريفات الفيروسات ، فان مستخدمي حماية الانترنت في نورتون يتسلمون أيضاً تحديثات الحماية لخدمة ترشيحات الويب Web filtering ، وخدمة كشف الاقتحام Intrusion Detection ، وخدمة التنبيه Spam Alert .

× خدمة تحديث ترشيحات الانترنت Web filtering تمدك بأحدث القوائم لعناوين مواقع الانترنت ومجموعات مواقع الانترنت التي تستخدم في التعرف على محتويات الانترنت غير المناسبة.

× وخدمة تحديث كشف الاقتحام Intrusion Detection تمدك بأحدث قواعد حوائط النيران Firewallالمعرفة مسبقاً وقوائم محدثة للتطبيقات التي تدخل إلى الانترنت. تلك القوائم تستخدم في التعرف على محاولات الدخول غير المسموح به إلى جهازك.

× خدمة تحديث التنبيهات Spam Alert وهي تمدك بأحدث تعريفات Spam والقوائم المحدثة من خصائص البريد الالكتروني Spamوتستخدم تلك القوائم في التعرف على برسائل البريد غير المطلوبة .

× حوائط النيران الشخصية من نورتونNorton Personal Firewall

مستخدمي هذا النوع من الحماية يتسلمون خدمة تحديث كشف الاقتحام Intrusion Detection لأحدث قواعد حوائط النيران المعرفة مسبقاً التي تدخل إلى الانترنت .

✣ الاشتراك Subscription :

المنتج الذي لديك من Symantec يتضمن اشتراك مجاني لفترة محدودة في تحديثات الحماية Protection Updates لخدمات الاشتراك التي تستخدم بالمنتج الذي حصلت عليه من الشركة. عندما يقترب موعد انتهاء الاشتراك الخاص بك يتم التنبيه عليك بضرورة تحديثه .
إذا لم تقم بتحديث الاشتراك يمكنك الاستمرار في استخدام التحديث الدائم LiveUpdate للحصول على تحديثات البرنامج. ومع ذلك لا يمكنك الحصول على تحديثات الحماية Protection Updates ولن يكون لديك حماية ضد التهديدات المكتشفة حديثاً .

عندما تقوم بالتحديث
قم بتشغيل التحديث الدائم LiveUpdate فور الانتهاء من تحميل البرنامج. وبمجرد الحصول على تحديثات ملفاتك تأكد من تشغيل التحديث الدائم LiveUpdate بانتظام للحصول على التحديثات .

طلب تنبيه التحديث

للتاكد من سريان تحديثات الحماية ، يمكنك طلب استلام بريد الكتروني تنبيهي وقتما تنشب مستويات عليا من الفيروسات أو أي تهديدات امنية أخرى على الإنترنت . البريد الإلكتروني التنبيهي يصف التهديدات الامنية ويمدك بتعليمات التعرف والازالة، كما يشمل نصائح للحفاظ على أمن جهاز الكمبيوتر . ويجب بالطبع تشغيل التحديث الدائم LiveUpdate عند استلام مثل ذلك البريد التنبيهي .

ويمكن طلب تنبيه التحديث كما يلي :

١. انتقل من خلال مستعرض الإنترنت الخاص بك إلى العنوان التالي على الإنترنت securityresponse.symantec.com/avcenter

٢. من صفحة الإنترنت Security Response انتقل إلى أسفل الصفحة ثم انقر على الاختيار Symantec security response Free subscription

٣. من صفحة الإنترنت Security Alert Subscription املأ نموذج الاشتراك Subscription Form

٤. انقر الاختيار Send me FREE Security Alerts

تشغيل التحديث الدائم على شبكة داخلية

يمكنك تشغيل التحديث الدائم LiveUpdate على جهاز كمبويتر متصل بشبكة توجد خلف حائط ناري Firewall خاص بالشركة ، ويجب أن يقوم مدير هذه الشبكة بتحديد خادم خاص بالتحديث الدائم LiveUpdate على هذه الشبكة وسوف يصل التحديث الدائم إلى هذا الخادم تلقائياً .

إذا كنت لا تستطيع استخدام التحديث الدائم:

عند وجود تحديثات متاحة تقوم شركة Symantec بارسالها الى موقع الانترنت الخاص بها ، فاذا كنت لا تستطيع تشغيل التحديث الدائم LiveUpdate فيمكنك الحصول على تلك التحديثات من موقع شركة Symantec على الإنترنت ، وفي هذه الحالة يجب أن يكون اشتراكك ساري لكي تستطيع الحصول على تلك التحديثات من موقع شركة Symantec على الإنترنت. وللحصول على التحديثات من موقع الشركة على الإنترنت اتبع الخطوات الاتية :

١. وجهة مستعرض الويب الخاص بك إلى موقع شركة سيمانتك على الإنترنت وهو securityresponse.symantec.com

٢. اتبع الروابط للوصول إلى نوع التحديثات التي تريدها .

إعداد نمط التحديث الدائم LiveUpdate

يعمل التحديث الدائم تحت النمط التفاعلي Interactive أو النمط السريع . Express mode في النمط التفاعلي (وهو النمط الافتراضي) يقوم التحديث الدائم بتنزيل قائمة من التحديثات المتاحة لمنتجاتك الموجودة من شركة سيمانتك والتي تدعمها تكنولوجيا التحديث الدائم LiveUpdate، وعند ذلك يمكنك اختيار أي التحديثات تريد تحميلها. أما في النمط السريعة Express mode يقوم التحديث الدائم تلقائياً بتنزيل جميع التحديثات المتاحة لجميع منتجات سيمانتك الموجودة على جهازك .

تشغيل التحديث الدائم تلقائياً

يمكنك ضبط التحديث الدائم للبحث عن تحديثات الحماية تلقائياً بضبط الجدولة واتاحة العمل التلقائي للتحديث الدائم. ويجب أن تستمر في التشغيل اليدوي للتحديث الدائم لاستلام تحديثات المنتج .

التحديث الدائم الذي يعمل تلقائياً يبحث عن اتصال بالانترنت كل خمس دقائق حتى يصل إلى الاتصال ، وبعد ذلك كل اربعة ساعات . إذا كان لديك قناة اتصال ISDN تم ضبطها للاتصال التلقائي بالانترنت ، فسوف يتم عمل عدة اتصالات ، وفي هذه الحالة تزيد تكلفة الاتصالات كثيراً . ولكن يمكنك ضبط قناة التصال ISDN لكي لا تعمل تلقائياً ، او يمكن ضبط التحديث الدائم ايضاً لكي لا يعمل تلقائياً

لإتاحة التحديث الدائم من Option اضغط على Enable Automatic LiveUpdate

ثم اختر Apply updates without interrupting me

آمل أن يكون الدرس مفيداً وسهلاً للجميع ...

تحياتي ..
محمد قطان ..

اليـوم **سـنختتم السلسـلة** التـي بـدأنا بهـا بـدروس احترافيـة حـول برنـامج الانتـي فيـروس ..

وهذا السلسلة اذا ما قرأتها بعناية فسوف تتكون لديك خلفية جيـدة جـدا عـن حمايـة جهـازك من الفيروسات ..

وأما الحماية من الاختراق وهو الشق الثاني مـن الحمايـة فهـذه لهـا دورة قريبـا بـإذن الله مـع دراسـة شـاملة حول برنامج zone alarm

والآن لنبدأ درسنا ..

ماذا يفعل النورتون إذا وجد ملفا مصابا بفيروس ؟

إذا وجد برنامج نورتون فيروس في جهازك يكون هنـاك ثـلاث حلـول ممكنـة لهـذه المشـكلة :

P Repair إصلاح الملف

ويعنى ذلك إزالة الفيـروس مـن الملـف أمـا إذا كـان التهديـد عبـارة عـن دودة Worm أو حصـان طروادة Trojan horse فيتم إزالة الملف ..

P Quarantine أي وضع الملف في الحجر

ويعنـي ذلـك أن يكـون الملـف غيـر قابـل للفـتح باسـتخدام اي برنـامج آخـر غيـر نورتـون مضـاد الفيروسات .حتى لا يمكنك فتح الملف بدون قصد مما يؤدي إلى انتشار الفيروسات .

P Delete إزالة الملف

ويعني ذلك إزالة الفيروس من جهازك عن طريق إزالة الملـف الـذي يحتـوي علـى الفيـروس أو الدودة أو حصان طروادة . ويتم استخدام هـذا الحـل فقـط عنـد عـدم إمكانيـة إصـلاح الملـف أو وضعه في الحجر Quarantine .

يمكن اكتشاف التهديدات الماكرة خلال مسح فيروسـي دوري أو عن طريـق الحمايـة التلقائيـة عند محاولـة العمـل مـع أحـد الملفـات المصـابة. ويمكـن أيضـاً أن تظهـر التهديـدات خـلال دورة المرسـل الفوري Instant Messenger أو عنـد إرسـال بريـد الكترونـي . Email وتختلـف طريقـة التعامل مع التهديد بحسب طريقة التوصل إلى ذلك التهديد هل عن طريق الحماية التلقائية أو عن طريق المسح الفيروسي.

اكتشاف الفيروس أثناء المسح

إذا وجد نورتون فيروس ، أو حصان طروادة أو دودة خلال عملية المسح الفيروسي أو من خلال دورة مرسل فوري ، فإما أن تتسلم ملخص عن الإصلاح التلقائي أو نتائج الإزالة ، أو يجب عليك أن تستخدم معالج الإصلاح Repair Wizard .

مراجعة تفاصيل الإصلاح

إذا كنت أعددت اختيارات المسح اليدوي ليقوم نورتون بإصلاح الملفات تلقائياً ، وجميع الملفات يمكن أن يتم إصلاحها، فان ملخص المسح الفيروسي يقدم قائمة بعدد الملفات المصابة التي تم إصلاحها. ويتم تقديم هذه المعلومات في أغراض الحالة Status Purposes فقط ، ولا تحتاج إلى اتخاذ إجراءات إضافية لحماية جهازك. إذا كنت تريد معرفة المزيد يمكنك مراجعة تفاصيل الإصلاح لكي تعرف أي الملفات كانت مصابة وماهية التهديد الذي أصابها .

استخدام معالج الإصلاح Repair Wizard

إذا كانت هناك ملفات لم يمكن إصلاحها ، أو إذا كنت أعددت اختيارات المسح اليدوي ليسألك نورتون ماذا يفعل عندما يجد فيروس ، يتم فتح معالج الإصلاح . إذا لم يكن نورتون قد حاول الإصلاح ، يتم فتح معالج الإصلاح على لوحة الإصلاح Repair pane ، وإلا فانه يفتح على نافذة الحجر Quarantine window .

لاستخدام معالج الإصلاح اتبع الخطوات الآتية :

١. إذا فتح معالج الإصلاح على لوحة الإصلاح ، قم بإلغاء التحديد عن الملفات التي لا ترغب أن يقوم نورتون بإصلاحها. جميع الملفات محددة افتراضياً وهو الإجراء المفضل .

٢. انقر إصلاح Fix

يتم فتح نافذة الحجر إذا لم تتمكن من إصلاح أو إزالة بعض الملفات . وجميع الملفات تكون محددة لتضاف إلى الحجر افتراضياً وهو الإجراء المفضل .

٣. من نافذة الحجر قم بإلغاء التحديد عن الملفات التي لا ترغب في إضافتها إلى الحجر .

٤. انقر فوق الحجر Quarantine

إذا لم تتمكن من وضع أي من الملفات في الحجر يتم فتح لوحة الإزالة . Delete pane إذا لم تقم بإزالة الملفات المصابة يستمر الفيروس على جهازك ويمكن أن يتسبب في خسائر أو ينتقل إلى مواقع أخرى .

٥. قم بإلغاء التحديد التي لا ترغب في إزالتها.

٦. انقر إزالة Delete

بمجرد انتهاء الملفات إما بالإصلاح أو بالحجر أو بالإزالة يتم فتح لوحة الملخص Summary pane لنافذة المسح .

٧. بعد الانتهاء من مراجعة الملخص يمكنك نقر الانتهاء Finished

إذا تم اكتشاف الفيروس عن طريق الحماية التلقائية Auto-Protect
تقوم الحماية التقائية بعمل مسح فيروسي للملفات ضد مختلف التهديدات عند محاولة التعامل مع تلك الملفات ، مثل تحريكهم ، أو نسخهم ، أو فتحهم . اذا تم اكتشاف أي أنشطة فيروسية ، فانك في أغلب الأحوال تتسلم تنبيه يخبرك باكتشاف وإصلاح فيروس . ويعتمد الاستمرار على نوعية نظام التشغيل الذي تستخدمه ..

P إذا كنت تستخدم ويندوز ٩٨/ ٩٨ SE / Me

إذا تم اكتشاف وإصلاح الفيروس عن طريق الحماية التلقائية فسوف تتسلم تنبيه يخبرك باسم الملف الذي تم إصلاحه أو إزالته . ولإغلاق التنبيه انقر فوق الانتهاء Finish

إذا كنت قد أعددت الحماية التلقائية لتسألك عن التصرف الذي ترغب فيه عن اكتشاف الفيروس فان التنبيه يسألك لاختيار احد الأعمال ، والتصرف المفضل يكون محددا افتراضياً.وتكون الاختيارات كما يلي :

١. إصلاح الملف المصاب
يتم هنا التخلص من الفيروس أو الدودة أو حصان طروادة وإصلاح أو إزالة الملف المصاب . عند اكتشاف الفيروس فان الإصلاح هو دائماً أفضل الاختيارات.

٢. حجر الملف المصاب
يتم هنا عزل الملف المصاب ولكن ذلك لا يزيل التهديد. اختر الحجر إذا كنت تشك في أن سبب التهديد عير معروف وتريد تسليمه إلى سيمانتك ليتم تحليله .

٣. إزالة الملف المصاب
ويتم هنا التخلص من كل من التهديد والملف المصاب . اختر الإزالة إذا لم تفلح في إصلاح الملف . استبدل الملف المزال بنسخة أخرى من البرنامج الأصلي أو من النسخ الاحتياطي Backup Copy، فإذا تم اكتشاف التهديد مرة أخرى فان النسخة الأصلية تكون مصابة.

٤. لا تتعامل مع الملف المصاب واتركه
ويتم هنا إيقاف العملية الحالية بالتعامل مع الملف المصاب لمنع استخدام الملف المصاب . ولكن هذا الفعل لا يحل المشكلة . وسوف تتسلم تنبيه عند محاولة التعامل مع الملف في المرة القادمة .

٥. تجاهل المشكلة ولا تقم بمسح فيروسي لهذا الملف مستقبلاً

وهنا يتم إضافة الملف المشكوك في إصابته إلى قائمة الاستبعاد . Exclusions list عند إضافة الملف إلى قائمة الاستبعاد يتم استثناءه من أي مسح فيروسي مستقبلاً ، إلا إذا قمت بإزالته من القائمة . نفذ هذا الاختيار فقط إذا كنت تعلم أن الملف لا يحتوي على فيروس

٦. تجاهل المشكلة واستمر مع الملف المصاب

ويتم العمل مع هذا الاختيار فقط إذا كنت متأكداً من أن الفيروس ، أو الدودة ، أو حصان طروادة لا يعمل . وسوف تتسلم التنبيه مرة أخرى . إذا كنت غير واثق من الإجراء اختر عدم فتح الملف واترك المشكلة. Do not open the file, but leave the problem alone

إذا كان الملف لا يمكن إصلاحه تتسلم رسالة تفيد أن الإصلاح لم يتم ويفضل وضع الملف في الحجر .Quarantine سوف يكون لديك الاختيارات التي تم توضيحها في النقاط السابقة باستثناء إصلاح الملف.

P إذا كنت تستخدم ويندوز ٢٠٠٠ / XP

إذا تم اكتشاف التهديد وتم إما الإصلاح التلقائي أو الإزالة عن طريق الحماية التلقائية Auto-Protect فسوف تتسلم تنبيه يخبرك باسم الملف المصاب الذي تم إصلاحه أو إزالته ونوع الفيروس ، أو حصان طروادة أو الدودة التي أصابت ذلك الملف. إذا كان لديك اتصال بالانترنت فان النقر على اسم الفيروس يؤدي إلى فتح صفحة سيمانتك على الإنترنت التي يكون فيها معلومات عن الفيروس .

إذا لم يمكن إصلاح الملف سوف تتسلم تنبيهين يخبرك أحدهما بان الحماية التلقائية لم تتمكن من إصلاح الملف والأخرى تخبرك أنه تم تجاهل فتح الملف.

يمكنك ضبط اختيارات الحماية التلقائية لمحاولة وضع الملفات التي لم تتمكن من إصلاحها في الحجر. إذا عملت ذلك سيتم إخبارك إذا تم وضع أي ملفات في الحجر.

لحل مشكلة الملفات التي لم يتم إصلاحها:

١. قم بتشغيل مسح فيروسي للنظام بالكامل للتأكد من عدم وجود ملفات مصابة أخرى.

٢. اتبع التعليمات المفضلة لمعالج الإصلاح Repair Wizard لحماية جهازك من الملفات المصابة.

P إذا تم اكتشاف فيروس عن طريق مانع النص Script Blocking

سيقوم مانع النص بمسح فيروسي لنصوص الفيجوال بيسك Visual Basic ، والجافا سكريبت JavaScript إذا اكتشف وجود فيروس أو أي نشاط فيروسي ففي أغلب الأحيان يظهر تنبيهه يخبرك باكتشاف وجود تهديدات.
ويجب أن تختار أحد الاختيارات لإزالة التهديد . والاختيار المفضل هو إيقاف تشغيل النص ويمكنك النقر على زر المساعدة في رسالة التنبيه للحصول على معلومات عن كيفية رد الفعل.

P إذا تم اكتشاف التهديد عن طريق مانع الديدان Worm Blocking

إذا حاول أحد البرامج أن يرسل نفسه عن طريق البريد الإلكتروني أو أن يرسل نسخه من نفسه فيمكن أن يكون أحد الديدان يحاول الانتشار عن طريق البريد الإلكتروني . ويمكن للدودة أن ترسل نفسها أو نسخة منها عن طريق رسالة بريد الكتروني دون أي تدخل منك .

يقوم مانع الديدان بعمل مسح فيروسي لملحقات البريد الإلكتروني وإذا تم اكتشاف أحد الديدان تتسلم رسالة تخبرك بوجود التهديد .

توجد اختيارات في رسالة التنبيه التي تصلك إذا لم تتم عملية إرسال البريد هذه المرة فمن الممكن أن تكون دودة ويجب عزل الملف في الحجر . إذا رغبت في معلومات إضافية عن كيفية رد الفعل يمكنك النقر على المساعدة في رسالة التنبيه.

بعد الانتهاء من التعامل مع التهديد أو إلغاء الملف فمن الممكن أن يكون مازال لديك نظام مصاب Infected System عند ذلك يمكنك تشغيل الحماية الدائمة LiveUpdate ، أو عمل مسح فيروسي للنظام ، كما يمكنك عند الضرورة الذهاب إلى صفحة سيمانتك على الإنترنت (securityresponse.symantec.com) للحصول على أحدث أدوات وتعريفات الفيروسات.

P إذا نبهك التطعيم Inoculation إلى وجود تغييرات في ملفات النظام

الحماية ضد التطعيم Inoculation protection متاحة فقط في أنظمة التشغيل ويندوز ٩٨، ٩٨ SE، و Me ، والتطعيم هو عبارة عن تغييرات تحدث في ملفات النظام.

ويمكن أن تحدث تغييرات في ملفات النظام للعديد من الأسباب . فمن الممكن أنك قد قمت بتحديث نظام التشغيل لديك ، أو قمت بإعادة تقسيم القرص الصلب ، أو يمكن أن يكون لديك فيروس . وينبهك نورتون مضاد الفيروسات عند حدوث تغييرات في ملفات النظام.

إذا جاءك تنبيه بحدوث تغييرات في ملفات النظام ، فلديك اختيارين . يمكنك تحديث لقطة التطعيم Inoculation Snapshot أو إصلاح الملف . قبل إصلاح الملف يجب التأكد من أن تعريفات الفيروسات تم تحديثها إلى آخر تحديث ثم قم بإجراء مسح فيروسي.

للاستجابة إلى تغييرات التطعيم:

× من نافذة التنبيه Alert window اختر الإجراء الذي تريده ، واختياراتك هي :

١. تحديث النسخة المحفوظة من سجلات التحميل الرئيسي
وهو يستخدم إذا ظهر التنبيه بعد تغييرات منطقية في ملفات النظام

٢. استعادة النسخة المحفوظة من سجل التحميل الرئيسي
وهو يستخدم عند التحقق من أن التغييرات التي حدثت لا ترجع إلى أسباب منطقية.

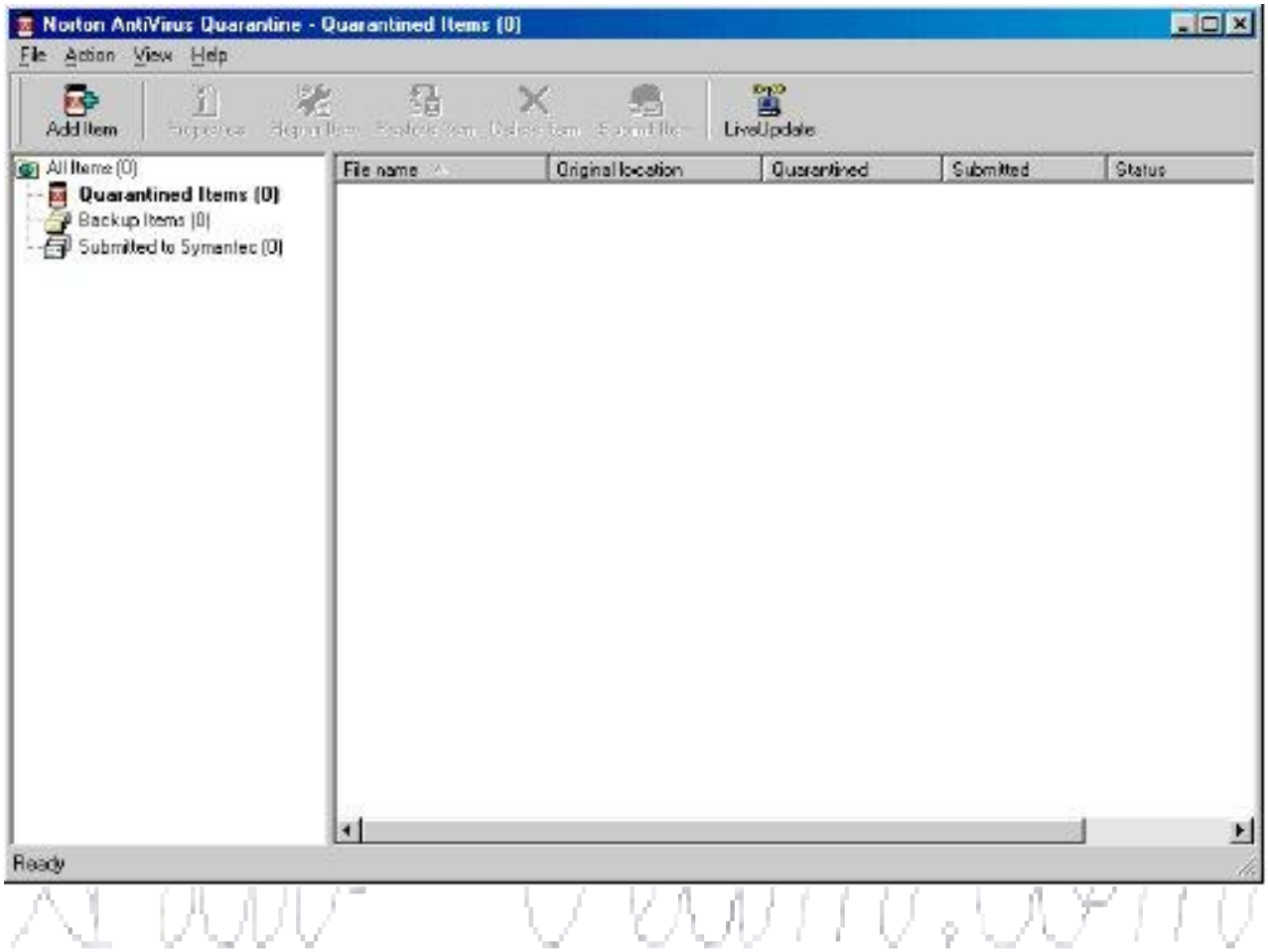
P إن كان لديك ملفات في الحجر Quarantine

بمجرد وضع ملف في الحجر Quarantine ، فلديك عدة اختيارات . جميع الإجراءات التي يمكن أن تتخذها للملفات في الحجر يجب أن تكون ظاهرة في نافذة الحجر Quarantine window

لفتح نافذة الحجر:

١. ابدأ تشغيل برنامج نورتون مضاد الفيروسات الإصدارة المتخصصة
٢. من نافذة البرنامج الرئيسية انقر تقارير Reports

٣. في لوحة التقارير على خط العناصر المحجورة Quarantined items انقر عرض التقارير View Report



يحتوي شريط الأدوات الموجود أعلى نافذة الحجر على كافة الإجراءات التي يمكن اتخاذها مع الملفات في الحجر وتظهر هذه الإجراءات كما يلي :

١. إضافة عنصرAdd Item
يضيف ملفات إلى الحجر .ويستخدم هذا الإجراء لحجر أحد الملفات الذي تشك في إصابته . وهذا الإجراء ليس له تأثير على الملفات الموجودة بالفعل في الحجر .

٢. الخصائص Properties
تمد بالمعلومات التفصيلية عن الملف المحدد والفيروس الذي أصابه.

٣. إصلاح العنصر Repair Item
يحاول إصلاح الملف المحدد Selected File ، يستخدم هذا الإجراء إذا تسلمت تعريفات جديدة للفيروسات منذ إضافة الملف إلى الحجر .

٤. استعادة العنصر Restore Item
يرجع الملف المحدد إلى موقعه الأصلي بدون إصلاحه

٥. إزالة العنصر Delete Item
يزيل الملف المحدد من جهاز الكمبيوتر

٦. تسليم العنصر Submit Item
يرسل الملف المحدد إلى شركة سيمانتك . ويستخدم هذا الإجراء إذا كنت تشك في إصابة الملف حتى إذا لم يشعر به نورتون مضاد الفيروسات.

٧. التحديث الدائم LiveUpdate
يعمل على تشغيل التحديث الدائم للحصول على الحماية الجديدة أو تحديثات البرنامج .
استخدم هذا الإجراء إذا لم تكن حدثت تعريفات الفيروسات لفترة ما ثم عند ذلك حاول إصلاح الملفات الموجودة في الحجر.

لاتخاذ إجراء مع أحد ملفات الحجر اتبع الخطوات الآتي :
١. حدد الملف الذي تريد اتخاذ إجراء معه
٢. من شريط الأدوات Toolbar اختر الإجراء الذي تريد اتخاذه

إذا لم يستطع نورتون مضاد الفيروسات إصلاح أحد الملفات

أحد أكثر الأسباب شيوعاً والذي يؤدي إلى عدم مقدرة نورتون على إصلاح أحد الملفات هو عدم وجود حماية محدثة ضد الفيروسات . فقم بتحديث الحماية الفيروسية Virus Protection ثم قم بالمسح الفيروسي مرة أخرى.

إذا لم يؤت ذلك نتيجة فاقرأ المعلومات الموجودة في نافذة التقرير Report window ثم اتخذ الإجراء المناسب

ونلخص ذلك كما يلي :
١. نوع الملف المصاب : إذا كان الملف المصاب له الامتداد,exe أو .doc, أو .dot,أو)xls أي ملف يمكن أن يصاب (فيكون الإجراء المناسب هو : استخدام معالج الإصلاح Repair Wizard كما سبق.

٢. نوع الملف المصاب : السجل الرئيسي للتحميل على القرص الصلب Hard disk master boot record، و ملفات النظام) System files مثل IO.SYS أو (MSDOS.SYS ، أو سجل

التحميل على القرص المرن Floppy disk boot record وملفات النظام فيكون الإجراء المناسب هو الاستبدال باستخدام أقراص الإنقاذ Rescue Disks أو أقراص نظام التشغيل Operating System Disks

الإطلاع على الفيروسات في موقع سيمانتك على الإنترنت

موقع شركة سيمانتك على الإنترنت يحتوي على قائمة بجميع الفيروسات المعروفة والأكواد الماكرة المتعلقة بها ، بالإضافة إلى وصف كامل لها. فيجب أن تتصل بالانترنت للإطلاع على كل ذلك كما يلي :

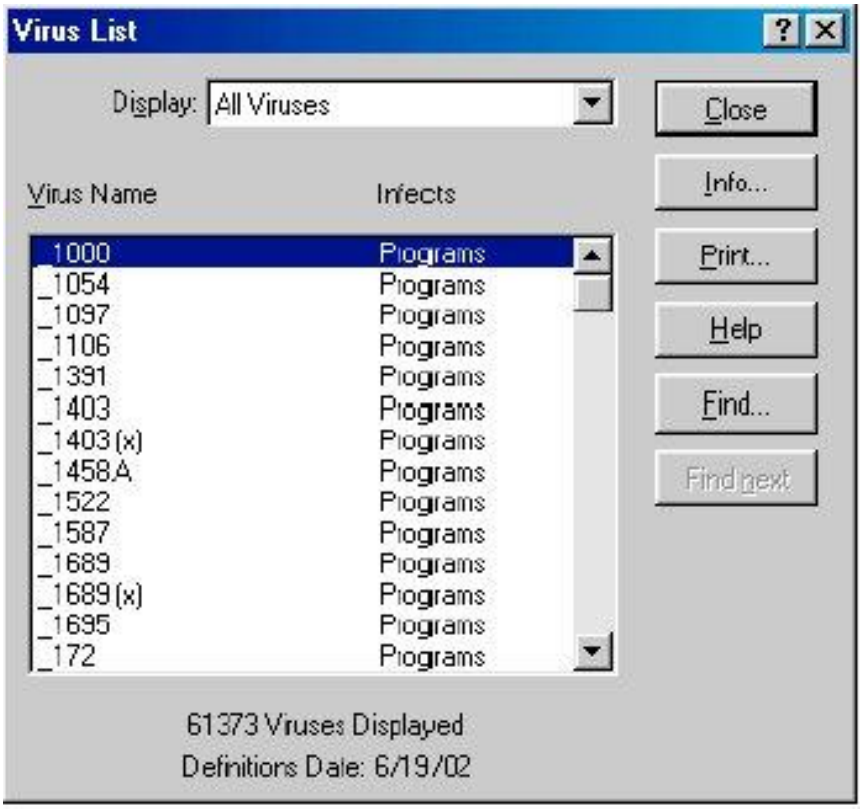
١. ابدأ تشغيل برنامج نورتون من النافذة الرئيسية للبرنامج انقر تقارير Reports

٢. من لوحة التقارير على خط موسوعة الفيروسات الفورية Online Virus Encyclopedia ، انقر عرض التقارير View Report يتم فتح موقع شركة سيمانتك في مستعرض الإنترنت الخاص بك.

٣. استخدم الروابط الموجودة بالموقع للوصول إلى معلومات الفيروسات التي تبحث عنها .

الإطلاع على الفيروسات في نورتون

إذا لم يكن لديك اتصال ساري بالانترنت ، يمكنك الإطلاع على أسماء الفيروسات من خلال نورتون الإصدارة المتخصصة . يوضح مربع حوار قائمة الفيروسات قائمة لملفات خدمة تعريفات الفيروسات السارية على جهازك. ونظراً لكمية الفيروسات الكبيرة لا تحتوي القائمة على وصف لكل فيروس .



للتأكد من أنك لديك أخر تحديثات تعريفات الفيروسات ، قم بتشغيل التحديث الدائم LiveUpdate .

للإطلاع على أسماء وتعريفات الفيروسات اتبع الخطوات الآتية :

١. ابدأ تشغيل برنامج نورتون من النافذة الرئيسية للبرنامج انقر تقارير Reports

٢. من لوحة التقارير على خط قائمة الفيروساتVirus List line ، انقر عرض التقارير View Report

للحصول على معلومات إضافية عن فيروس معين اتبع الخطوات الآتية :

من مربع حوار قائمة الفيروسات حدد الفيروس الذي ترغب في الحصول على معلومات إضافية له انقر على معلومات Info ..

من المفترض الآن بعد قراءة هذه السلسة انك قادر على حماية جهازك من عوارض الاصابة بالفيروسات بنسبة ٨٠ الى ٩٠ % .. وتذكر دائما ان الحماية الكاملة على النت شيء وهمي ولا وجود له ...

أتمنى أن تكون هذه السلسلة مفيدة للجميع ..

مع خالص تحياتي
محمد قطان