

الفصل السادس عشر

نظام الأمان في Windows Vista

يهتم هذا الفصل بشرح الطرق المختلفة لتأمين الحماية لجهازك وأطفالك وتوفير المراقبة الأبوية لاستخدام أبنائك لجهاز الكمبيوتر ، كما يشرح هذا الفصل طرق حماية الجهاز من تعرضه للهجوم من أي شخص أو أي موقع . بانتهاء هذا الفصل ستتعرف علي :

- استخدام المراقبة الأبوية Parental Control
- استخدام "Windows Fire Wall جدار حماية ويندوز"
- استخدام "Windows Defender مدافع ويندوز"
- التعرف علي طرق إضافية لحماية البيانات والجهاز

يتمتع نظام Windows Vista بنظام عالٍ من الأمان. بعض نظم الأمان كانت موجودة في الإصدارات السابقة والبعض جديد في Windows Vista. تتعدد سبل الحماية والأمان الموجودة في Windows Vista ابتداءً بتقييد الدخول إلى النظام باستخدام نظام حساب المستخدمين User Accounts وكلمات المرور Passwords للحد من استخدام الكمبيوتر والبرامج والانترنت، مروراً باستخدام المراقبة الأبوية للحد من استخدام أطفالك للكمبيوتر وتقييد المواقع الهدامة. وحماية نفسك من مواقع الصيد، وانتهاءً باستخدام برامج الحماية والدفء مثل "Windows Firewall" والمدافع "Windows Defender"، يشكل النسخ الاحتياطي للملفات Backup and Restore الذي شرحناه في الفصل السابق نوعاً آخر من نظام الأمان في Windows Vista. في هذا الفصل ستتعرف علي أشهر وأفضل سبل الأمان لحماية نفسك وملفاتك وأطفالك. فكن معي أعزك الله.

المراقبة الأبوية Parental Control

آه من الانترنت... آه من ثورة الاتصالات الحديثة. إنها بقدر ما تنفع، فمن الممكن أن تكون هدامة ومضیعة للوقت وللأطفال لأنها تضيع بين أيديهم كل شيء الضار قبل النافع. من منا لا يخاف على أولاده من التجوال في المواقع الهدامة أو الإباحية أو التي تستخدم لغة بذيئة أو تحض على العنف والرذيلة ويتمنى لو تحجب عنهم.. من منا لا يخشى على أطفاله من المدة الزمنية التي يقضونها أمام الكمبيوتر في التجول على مواقع الويب أو التسلي بالألعاب مهملين واجباتهم المدرسية ويتمنى لو يضع حدوداً زمنية لاستعمالهم الكمبيوتر.

والسؤال الأخير هو هل يمكن حماية أطفالنا من بعض مواقع الانترنت أو تقييد دخولهم إلى الكمبيوتر؟

هذا السؤال محير دائماً! ولقد أجابني أحد الأصدقاء ذات مرة، أفضل وسيلة لحماية أطفالنا من مواقع الانترنت الغير مرغوبة، أن تمنع الانترنت من الدخول إلى منازلنا. قلت

عجباً. أليس هناك وسيلة أخرى نتمكن بها من الاستفادة من الانترنت والاستفادة من ثورة الاتصالات والمعلومات التي نعيشها ، وفي نفس الوقت نحمي أطفالنا من بعض المواقع وليس كلها؟ أو تقييد دخولهم علي الكمبيوتر واستعماله.

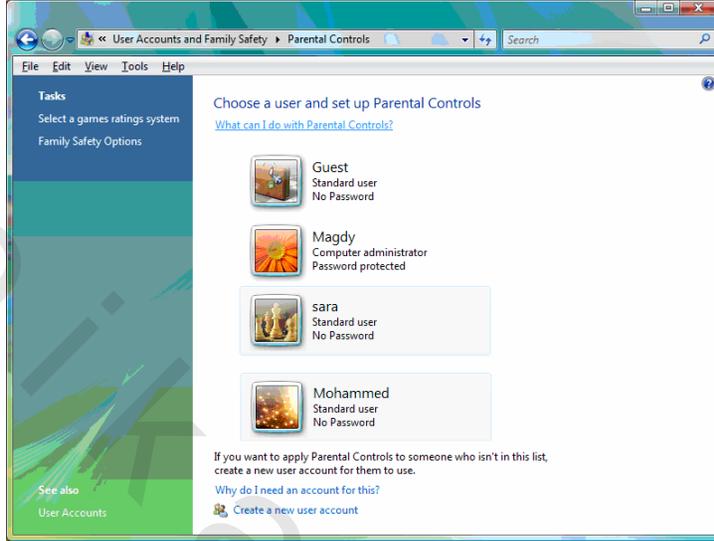
واحدة من المزايا الجديدة في Windows Vista هي ميزة المراقبة الأبوية "Parental Controls" توفر لك المراقبة الأبوية إمكانية تقييد وقت الجلوس أمام الكمبيوتر، وتقييد المواقع الإباحية ومواقع العنف والذيلة. والحصول على تقرير يوفر لك معلومات وافية عن المواقع التي زارها أطفالك. وماذا وجدوا بها. وما هي المواقع التي حاولوا الدخول عليها ولكنهم لم يتمكنوا من ذلك. بل أكثر من ذلك مراقبة الألعاب لحجب الألعاب العنيفة عن الأطفال والبرامج التي لا يصح أن يستخدموها.

لكي تستخدم المراقبة الأبوية يجب أن يكون حسابك مسجلاً كمستول. وأن يكون محمياً بكلمة مرور. حتى لا يستطيع أي شخص لديه حساب مستول أن يزيل المراقبة الأبوية التي تضبطها.



لتحديد الوقت الذي يستخدمه أطفالك (أو أي مستخدم آخر في جهازك) ومعاينة تقرير النشاط لما تم على الجهاز اتبع الآتي:

١. افتح لوحة التحكم.
٢. توجه إلى الخاصية **Uses Account And Family safety** "حسابات المستخدمين وأمان العائلة". وانقر المهمة **Set up Parental Controls for Any user** "إعداد المراقبة الأبوية لأي مستخدم"، وعندما يظهر مربع **Uses Account Controls** "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمستول انقر زر **Continue** "متابعة"، وإلا اكتب كلمة مرور المستول ثم انقر **OK** "موافق". تظهر نافذة **Parents Control** "المراقبة الأبوية" (شكل ١٦-١).



شكل ١٦-١ نافذة Parents Control "المراقبة الأبوية"

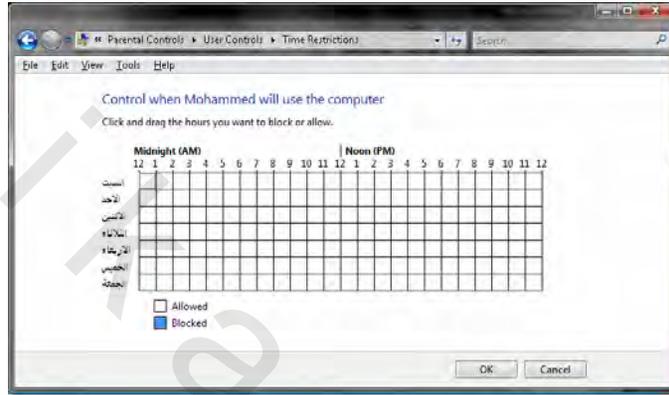
٣. انقر المستخدم الذي تريد تقييد وقت استخدامه للجهاز تظهر نافذة User Control "عناصر تحكم المستخدم" (شكل ١٦-٢).



شكل ١٦-٢ نافذة User Control "عناصر تحكم المستخدم"

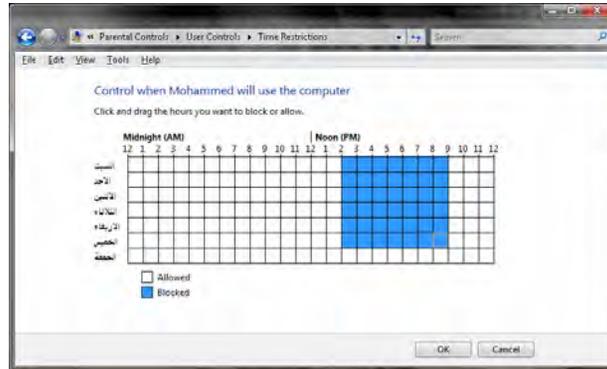
٤. تحت Parental Control "المراقبة الأبوية". انقر الخيار On, Enforce Current Setting "قيد التشغيل، فرض الإعدادات الحالية" لتنشيطه.

٥. تحت Windows Settings "إعدادات ويندوز" انقر Time limits "حدود الوقت". تظهر نافذة بعنوان Time Restrictions "قيود الوقت" (شكل ١٦-٣).



شكل ١٦-٣ نافذة Time Restrictions

تظهر في شكل ١٦-٣ شبكة بالأربع وعشرون ساعة خلال أيام الأسبوع السبعة. انقر كل ساعة في الشبكة تريد منع المستخدم (أو الأولاد) من العمل على الكمبيوتر فيها. يفرض أنك لا تريد لأولادك (أو للمستخدم) باستخدام الكمبيوتر خلال الفترة من الساعة الثانية بعد الظهر إلى الساعة التاسعة مساءً كل أيام الأسبوع ما عدا يوم الجمعة انقر الساعات التي تشير إلى ذلك (شكل ١٦-٤).

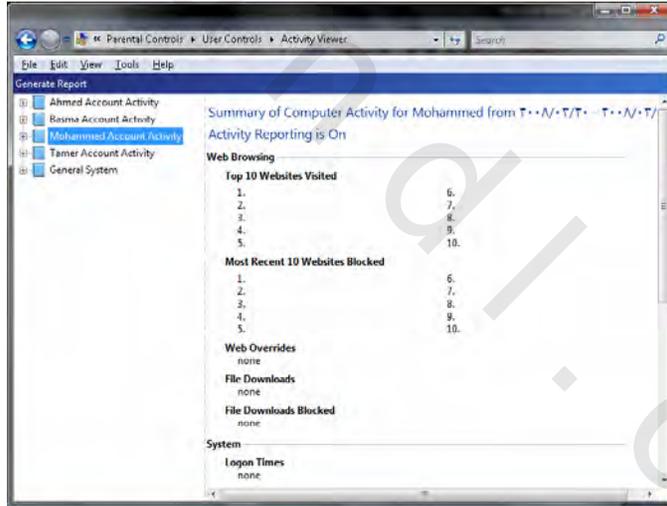


شكل ١٦-٤ تحديد الساعات المحددة للمستخدم لاستخدام الجهاز

خلال الفترات الزمنية التي حددتها، إذا حاول المستخدم تسجيل الدخول إلى حسابه لن يسمح له Windows وسيظهر له رسالة تفيد أن حسابه محظور في ذلك الوقت.
٧. انقر OK "موافق" للعودة إلى النافذة السابقة.

يجب أن تترك فترة زمنية للمستخدم ليحرب استخدام الكمبيوتر في الأوقات المسموحة والأوقات الممنوعة. تابع الخطوات الآتية:

١. افتح نافذة User Control "عناصر تحكم المستخدم" إذا كنت أغلقتها (راجع شكل ١٦-٢) تأكد من تنشيط الخيار ON, Collect Information about Computer Usage "قيود التشغيل، جمع معلومات حول استخدام الكمبيوتر".
٢. انقر View Activity Report "عرض تقارير النشاط" يظهر لك تقرير بالأنشطة داخل نافذة Activity Viewer "عارض الأنشطة". كما في شكل ١٦-٥



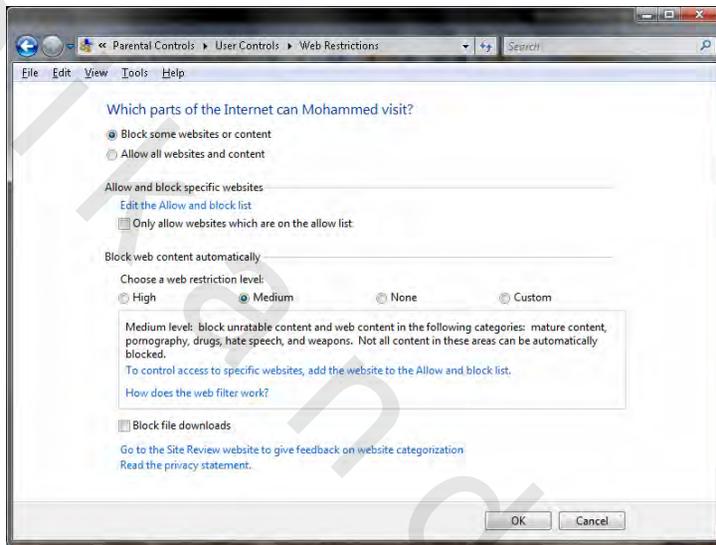
شكل ١٦-٥ نافذة Activity Viewer "عارض الأنشطة"

استخدم شريط التمرير الرأسي لقراءة باقي التقرير والتعرف على النشاطات التي يتعقبها.

٣. انقر زر Back (الخلف). ترجع إلى نافذة User Controls "عناصر تحكم المستخدم".

تتيح لك الخيارات الموجودة تحت **Windows Settings** إعدادات ويندوز " مزيداً من المراقبة الأبوية على النحو التالي:

١. انقر **Windows Vista Web Filter** "عامل تصفية ويب لويندوز" تظهر نافذة بعنوان **Web Restricting** "تقييدات الويب" (شكل ١٦-٦).



شكل ١٦-٦ نافذة **Web Restricting** "تقييدات الويب"

يمكنك اختيار القيود التي تراها على استخدام الويب مثل:

- منع بعض مواقع ويب أو منع بعض المحتويات " **Block Some Websites or Content**.
- لاختيار مواقع معينة للسماح بزيارتها انقر الارتباط **Edit the Allow and Blocks List** "تحرير قائمة السماح والمنع"، وعندما يظهر تظهر نافذة **Blocker Web Pages** "السماح/حظر صفحات ويب" حدد عناوين مواقع الويب المسموحة وتلك الممنوعة ثم انقر **OK** "موافق". للعودة إلى نافذة **Web Restricting** "تقييدات الويب".

- اختيار مستوى قيود أعلى للويب **Choose Web Restriction Level** "اختر مستوى تقييد ويب".
 - إغلاق تنزيل الملفات **Block File Download** "منع تنزيل الملفات".
- بعد الانتهاء من تحديد قيود الويب انقر **OK** "موافق" لإغلاق نافذة **User Control** "عناصر تحكم المستخدم" والعودة إلى نافذة **User Control** "عناصر تحكم المستخدم".
٢. تحت **Windows Setting** "إعدادات ويندوز" انقر **Games** "الألعاب" ثم حدد المراقبة للألعاب التي ترغب أن يلعبها الابن (أو المستخدمين) من نافذة **Game Controls** "عناصر تحكم الألعاب" لمنع الألعاب العنيفة أو التي تعلم أشياء ضارة. بعد الانتهاء انقر **OK** "موافق" لإغلاق نافذة **Game Control** "عناصر تحكم الألعاب" والعودة إلى نافذة **User Control** "عناصر تحكم المستخدم".
٣. تحت **Windows Settings** "إعدادات ويندوز" انقر **Allow and Block Specific Programs** "السماح ببرامج محددة وحظرها" ثم عدل المراقبة الأبوية مثلما تريد من نافذة **Application Restrictions** "قيود التطبيق" لمنع استعمال بعض البرامج.

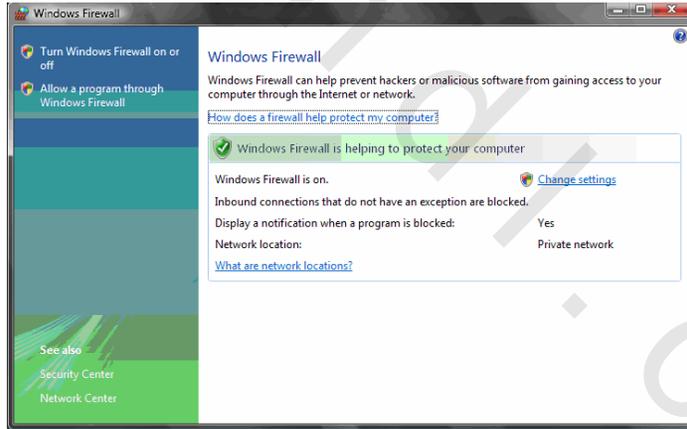
Windows Fire Wall "جدار حماية ويندوز"

يشتمل **Windows Vista** على برنامج أمان رائع يسمى **Windows Fire Wall** ومعناها "جدار الحماية" أو "جدار نار ويندوز" يشكل جدار الحماية المثبت في **Windows Vista** عنصر أمان فعال بين شبكة الإنترنت وبين جهازك في حالة اتصالك بالإنترنت مباشرة. يتم تثبيت جدار الحماية في الكمبيوتر الذي تستخدمه في منزلك ليتحكم في الاتصالات بين شبكة منزلك وبين شبكة الإنترنت.

يوفر لك جدار حماية ويندوز طريقة آمنة بحيث لا تتم أي اتصالات خارجية إلى جهازك بخلاف التي تقبلها أو تجربها أنت. وهذا البرنامج نشط تلقائياً لجميع المستخدمين.

أما إذا كنت تعمل في ميدان (Domain) فإن جدار الحماية سيشكل جسراً آمناً بين شبكة الإنترنت العالمية وشبكة الإنترنت التي تستخدمها في شركتك، والمتصل بها جهازك. للتعرف على إعدادات جدار حماية ويندوز وتعديلها تابع الخطوات التالية:

١. افتح لوحة التحكم Control Panel.
٢. انقر Security "الأمان".
٣. من نافذة Security "الأمان" انقر Security Center "مركز الأمان"، تظهر نافذة Windows Security center "مركز أمان ويندوز".
٤. من الجزء الأيسر لنافذة Windows Security center (أو الأيمن في حالة اتجاه الشاشة من اليمين لليساار) انقر الارتباط Windows Firewall "جدار حماية Windows". تظهر نافذة Windows Firewall "جدار حماية ويندوز" (شكل ٧-١٦)

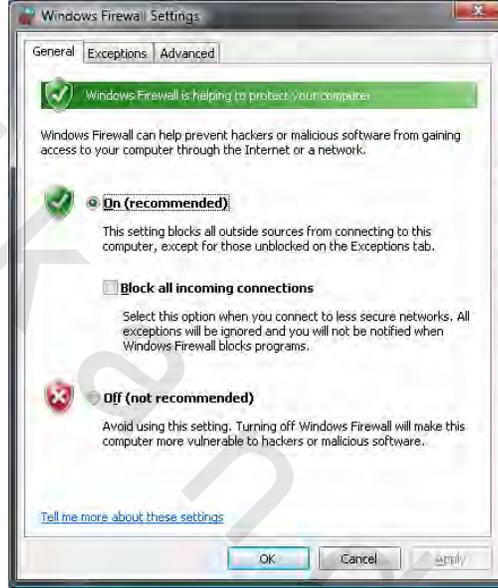


شكل ٧-١٦ نافذة Windows Firewall "جدار حماية Windows"

تشتمل النافذة على معلومات عن حالة جدار حماية ويندوز.

٥. انقر Change Settings "تغيير الإعدادات" عندما يظهر مربع User Account Central "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمستول انقر زر Continue "متابعة" وإلا اكتب كلمة مرور المستول ثم انقر OK "موافق". يظهر

مربع حوار Windows Firewall settings "إعدادات جدار حماية Windows
"إعدادات جدار حماية ويندوز"، وتظهر علامة التبويب General "عام" هي النشطة
(شكل ١٦-٨)



شكل ١٦-٨ نافذة Window Firewall Settings "إعدادات جدار حماية ويندوز"

يشتمل مربع الحوار على ثلاثة خيارات

- On (Recommend) "تشغيل مستحسن".
 - Block all incoming connections "منع كافة الاتصالات الواردة".
 - Off (not recommended) "إيقاف التشغيل (غير مستحسن)".
- ابق الخيار الأول نشطاً لحظر اتصال كافة المصادر الخارجية باستثناء المصادر غير المخطورة. نشط الخيار Block all Incoming Connections "منع كافة الاتصالات الواردة" إذا كنت تتصل بالإنترنت من جهة غير موثوقة ليتم تجاهل جميع الاستثناءات وستحظر جميع الاتصالات. للحصول على المزيد من المعلومات حول إعدادات جدار النار انقر الارتباط Tell me more about those settings "معرفة المزيد حول هذه الإعدادات" الموجود في أسفل المربع الحوار.

٦. انقر علامة التبويب **Exceptions** "استثناءات" لتنشيطها. تظهر قائمة بأنواع الاستثناءات تحت عنوان **Program or Port** "برنامج أو منفذ". تعرف على الاستثناءات المختارة بظهور علامة ✓ أمامها. استخدم شريط التمرير الرأسي للاطلاع على باقي الاستثناءات. انقر زر **All program** "إضافة برنامج" أو زر **Add Port** "إضافة منفذ" لإضافة برنامج أو المنفذ الذى يستعمله إلى القائمة.
٧. انقر علامة التبويب **Advanced** "خيارات متقدمة" تظهر قائمة بالاتصالات الشبكية المحمية بواسطة جدار النار.
٨. انقر **OK** "موافق" ، يغلق مربع حوار **Windows Firewall Settings** "إعدادات جدار حماية Windows".
٩. أغلق نافذة جدار حماية ويندوز.

Windows Defender "مدافع ويندوز"

كثيرة هي البرامج التي تسبب لك إزعاجاً وتفرض تهديداً محتملاً على بياناتك وكمبيوترك، بعضها برامج خبيثة (Malware) وبعضها تجسس (Spyware) لهذه البرامج قدرة على تثبيت نفسها فى جهازك والقدرة على تدمير المعلومات أو سرقتها إما فوراً، أو بعد مدة زمنية. يتولى **Windows Defender** "مدافع ويندوز" منع هذه البرامج الخبيثة والتجسس من إلحاق الضرر ببياناتك أو سرقتها.

وعموماً يقدم **Windows Defender** أنواع الحماية الآتية :

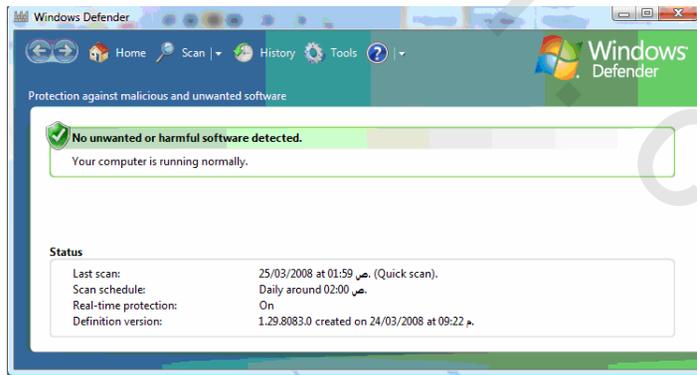
- يلاحظ **Windows Defender** باستمرار كمبيوترك، ويلاحظ جميع البرامج التي تقوم بتشغيلها وإعدادات النظام التي تجريها، ويتأكد من خلو البرامج أو الملفات من برامج التجسس، وينبهك إذا كان من المحتمل حدوث تخريب للبرامج التي يتم تثبيتها أو الإعدادات التي تتم.
- يمكنك أن تطلب في أي وقت أن يقوم **Windows Defender** بفحص شامل لجميع ملفاتك، أو أن تضع جدولاً دورياً للقيام بهذا الفحص لجميع الملفات.

• يفحص Windows Defender كل عملية تثبيت تتم، ليعرف هل تم التثبيت بواسطة، أم تم من خلال الانترنت، أو عن طريق ارتباط، أو نقر زر في رسائل البريد الإلكتروني الوارد، وينظر للشكل أو الهيكل المألوف للبرامج، فإذا وجد من شكل أو هيكل البرنامج أنه ينطوي على غير المألوف، وبالتالي يحتمل أن يسبب مشكلة، فإنه يقوم بتنبيهك.

يجب أن تقوم بتحديث Windows Defender بانتظام من موقع ميكروسوفت على الانترنت، أو باستخدام ميزة تحديث ويندوز (Windows Update)، شأنه في ذلك شأن أي برنامج من برامج مضادات الفيروسات التي تحتاج لتحديثها باستمرار ليتم تحديث قاعدة البيانات التي يستخدمها.

للتعرف على خيارات Windows Defender "مدافع ويندوز" وتعديلها تابع الخطوات الآتية:

1. افتح لوحة التحكم، اختر Security "الأمان" ثم اختر Windows Defender "مدافع ويندوز" (أو كإجراء بديل انقر زر Start "ابدأ" ثم أر إلى All programs "كافة البرامج" ثم انقر Windows Defender "مدافع ويندوز" تظهر نافذة Windows Defender "مدافع ويندوز" شكل ١٦-٩

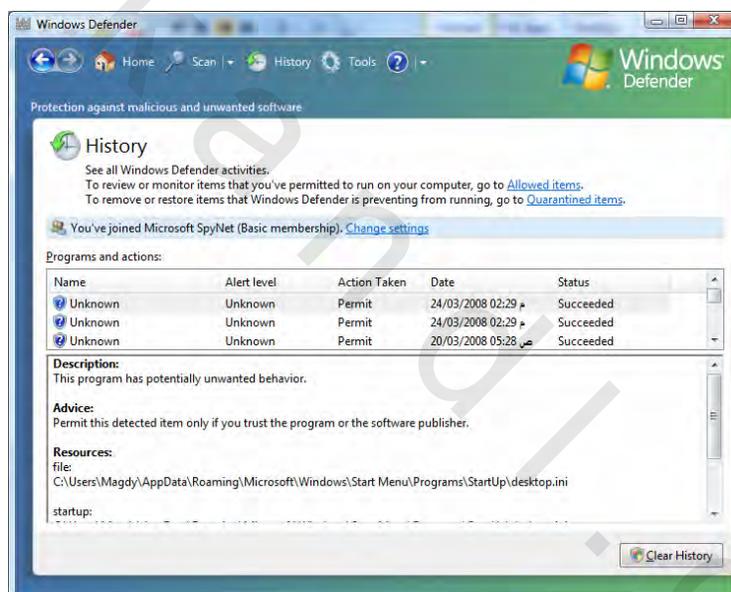


شكل ١٦-٩ نافذة Windows Defender

عندما تفتح نافذة Windows Defender، ستجد أن نظامك سليم كما يبدو في

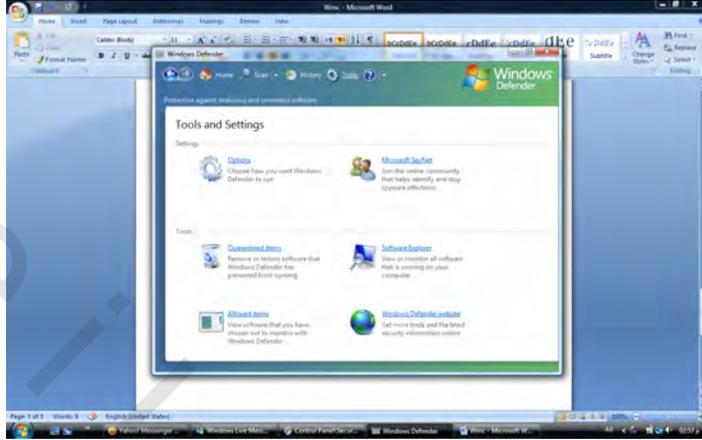
الشكل ١٦-٩ لأن Windows Defender يعمل دائماً في الخلفية لكي يتولى معالجة المشاكل الطارئة. ويظهر أسفل النافذة تقرير عن الحالة (Status).

٢. من شريط الأدوات انقر زر History "محفوفات" لتعرف متى قام Windows Defender بتسببها لعلاج مشكلة . يظهر في نافذة History "محفوفات" البرامج التي حاول Windows Defender منعها ومكانها ووصف لها والنصائح التي أعطاها لك Windows Defender عندما قمت بعمل شيء أو تثبيت برنامج من المحتمل أن يسبب لك مشكلة (شكل ١٦-١٠).



شكل ١٦-١٠ Windows Defender ينيهك لوجود مشكلة

٣. انقر زر Tools "الأدوات" تظهر شاشة تتيح لك تغيير إعدادات Windows Defender كالتالي (شكل ١٦-١١) .



شكل ١٦-١١ التحكم في إعدادات عمل Windows Defender

- نقر زر **Options** "الأدوات" يتيح لك جدولة **Windows Defender** ليقوم بفحص النظام بالكامل كل أسبوع.
 - نقر زر **Microsoft SpyNet** يتيح لك تحديث عضويتك في جمعية **Microsoft SpyNet**.
 - انقر زر **Quarantined Items** "العناصر المعزولة" لحذف أو استرجاع البرامج التي قام **Windows Defender** بمنعها من العمل على جهازك.
 - انقر زر **Allowed Items** "العناصر المسموح بها" لإظهار العناصر التي سمح **Windows Defender** بتشغيلها على جهازك.
- إذا سمحت لـ **Windows Defender** بتشغيل برنامج، ثم اكتشفت بعد ذلك أنك يجب ألا تشغله. بإمكانك إيقاف تشغيل البرنامج في المستقبل (بفرض أن البرنامج لم يحدث أي تخريب). من نافذة أدوات **Windows Defender** انقر **Allowed Items** "العناصر المسموح بها" تظهر نافذة **Windows Defender Tools** بالعناصر المسموحة. انقر البرنامج لاختياره ثم زر **Disable** "تعطيل" لمنع البرنامج من التشغيل حتى تسمح له بذلك ، أو انقر زر **Remove From List** "إزالة من القائمة" لإزالة البرنامج من جهازك.

طرق أخرى للأمان في Windows Vista

يشتمل Windows Vista علي مزايا أخرى - بخلاف المراقبة الأبوية - تساعدك في حماية جهازك من التهديدات الخارجية التي شاعت ونفشت خصوصا من خلال الاتصال بالإنترنت، ولو لفترات قصيرة. يوفر Windows Vista حماية جهاز الكمبيوتر بطرق مختلفة نوضحها فيما يلي :

- **Windows Security Center** "مركز أمان ويندوز" : افحص مركز أمان ويندوز بشكل دوري لأنه يراقب أنواع الحماية الموجودة عندك لتتأكد أن كل أنظمة حاسبك مضبوطة للحماية الأمثل.
- **Windows Update** : يسألك Windows عادة عندما تقوم بتثبيته أول مرة هل تريد أن يحدث Windows نظامك تلقائيا كلما قامت الشركة المنتجة بعمل تحديثات في موقع تحديث Windows وطبعا تختار أنت إما التحديث التلقائي أو عدم التحديث التلقائي. طبعا التحديث التلقائي مريح جدا، وهو يضمن لك تحديث نظامك كلما أصبحت هناك تحديثات متوفرة على موقع تحديث ويندوز، ويعفيك من مسؤولية تذكر تحديث نظامك يدويا. المشكلة إذا كنت قد اخترت عدم التحديث تلقائيا أثناء تثبيت Windows Vista في هذه الحالة يمكنك أن تطلب من Windows أن يقوم بتزيل وتثبيت التحديثات تلقائياً.
- أو تطلب من Windows أن يبلغك عندما تكون هناك تحديثات متوفرة أو يقوم بتزيل التحديثات ويبلغك عندما تصبح جاهزة للتثبيت.
- **User Account Control** "التحكم بحساب المستخدم" : واحدة من سبل الأمان في Windows Vista نظام حسابات المستخدمين (User Accounts) وكلمات المرور (Passwords) التي تستخدمها عند بداية دخولك إلى النظام. حيث يخصص لكل مستخدم أو لكل فرد في العائلة حساب معين ، حتى لا يستطيع

الوصول إلى معلومات سرية أو غير مسموح له بها أو تغيير ملفات يجب الاحتفاظ بها، وبهذا يحتفظ كل فرد من أفراد العائلة (أو المؤسسة) بخصوصياته وملفاته وصوره. حيث يخصص لكل مستخدم مجلد شخصي يحتفظ فيه بمستنداته وصوره الخاصة رغم إمكانية استخدام المجلد العمومي المسموح به للجميع. ويتمتع مالك حساب المسؤول (Administrator) بصلاحيات أعلى لتنفيذ مهام لا يقدر عليها صاحب الحساب القياسي (Standard). كلما قمت بإجراء من شأنه أن يؤثر على استخدام كمبيوترك مثل تغيير الإعدادات، يطالبك Windows بإدخال كلمة مرور المسؤول للمتابعة .

راجع الشرح الذي تقدم عن إدارة حسابات المستخدمين في الفصل الأول



- تثبيت أحد برامج مضادات الفيروسات بحيث يعمل تلقائياً مع بداية تشغيل الحاسب.
- قم بتحديث برنامج مضاد الفيروسات وذلك بتنزيل النسخة المحدثة منه بواسطة الإنترنت.
- شراء البرامج الأصلية فقط لأن معظم البرامج المنسوخة تحتوي على فيروسات.
- تجنب بقدر المستطاع استخدام الأقراص المرنة لنقل البيانات لأنها مصدر جيد أيضاً لنقل الفيروسات.
- لا تفتح رسائل البريد الإلكتروني غير معروفة المصدر.
- إذا اضطررت لتنزيل برامج عبر الإنترنت، قم بفحص ملفات البرامج قبل تشغيلها.
- احتفظ دائماً بنسخة احتياطية من القرص الصلب الذي تستخدمه لاسترجاع ملفاتك إذا أصابها ضرر.

