الفصل الرابع عشر
حماية الأطفال وتأمين الكمبيوتر

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 ومفاهيم عامة للوقاية من الفيروسات وحماية خصوصياتك كتعيين كلمة مرور وتأمين البريد الالكتروني والتعامل مع برامج مكافحة الفيرسات.

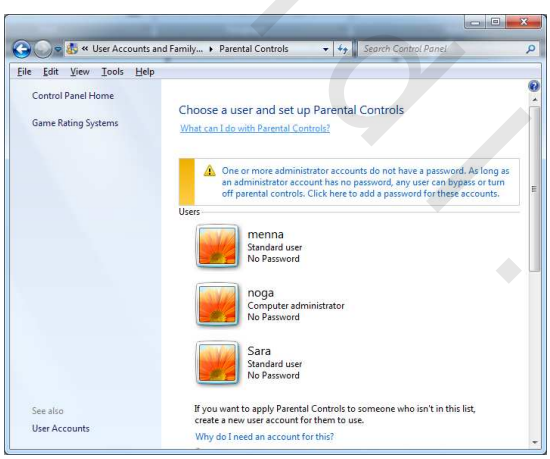
لحماية الأطفال وتأمين الكمبيوتر تتعدد سبل الحماية والأمان الموجودة في Windows ابتداء بتقييد الدخول إلي النظام باستخدام نظام حساب المستخدمين User Accounts وكلمات المرور Passwords للحد من استخدام الكمبيوتر والبرامج والانترنت، مرورا باستخدام المراقبة الأبوية للحد من استخدام أطفالك للكمبيوتر وتقييد المواقع الهدامة. وحماية نفسك من مواقع الصيد ، وانتهاء باستخدام برامج الحماية والدفاع مثل Windows Firewall "جدار حماية ويندوز" وWindows Defender "المدافع". في هذا الفصل ستتعرف علي أشهر وأفضل سبل الأمان لحماية نفسك وملفاتك وأطفالك. فكن معي أعزك الله .

المراقبة الأبوية Parental control

توفر المراقبة الأبوية مزايا هائلة منها تقييد الوصول إلي أو حجب المواقع الإباحية ومواقع العنف، والحصول علي تقرير يوفر لك المواقع التي زارها أطفالك ، وما هي المواقع التي حاولوا الدخول عليها ولكنهم لم يتمكنوا من ذلك، وكذلك حجب الألعاب العنيفة عن الأطفال والبرامج التي لا يصح أن يستخدموها. ايضاً بإمكانك أن تحدد الوقت المسموح لأطفالك أن يستخدموا فيه الكمبيوتر وما هي المدة المسموحة لهم بالبقاء أمام الكمبيوتر، بالإضافة إلي ذلك يمكنك أيضاً أن تحجب الوصول إلي بعض الأفلام المثيرة للاعتراض

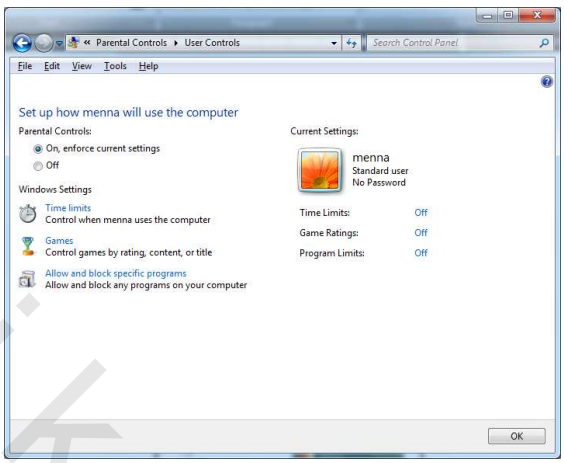
التي تعرض علي التليفزيون بواسطة Windows media center .
لتحديد الوقت الذي يستخدمه أطفالك (أو أي مستخدم آخر في جهازك) ومعاينة تقرير النشاط لما تم على الجهاز وللتحكم فى الوصول إلى الألعاب، والسماح ببرامج محددة أو حظرها اتبع الآتي:

١. افتح Control panel "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 Users Account Controls "التحكم في حساب المستخدم" إذا كنت مسجلاً دخولك كمسئول انقر زر Continue "متابعة" ، وإلا اكتب كلمة مرور المسئول ثم انقر OK "موافق. تظهر نافذة Parental Control "المراقبة الأبوية" كما فى شكل ١٤-١ .



شكل ١٤-١ نافذة Parents Control "المراقبة الأبوية"

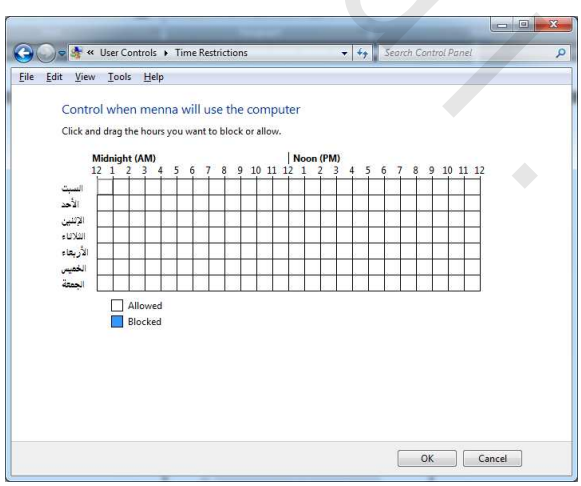
٣. انقر المستخدم الذي تريد تقييد وقت استخدامه للجهاز تظهر نافذة User Control "عناصر تحكم المستخدم" (انظر شكل ١٤-٢).



شكل ١٤–٢ نافذة User Control "عناصر تحكم المستخدم"

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

٥. تحت Windows Settings "إعدادات ويندوز" انقر Time limits "حدود الوقت". تظهر نافذة بعنوان Time Restrictions "قيود الوقت" كما فى شكل ١٤–٣.

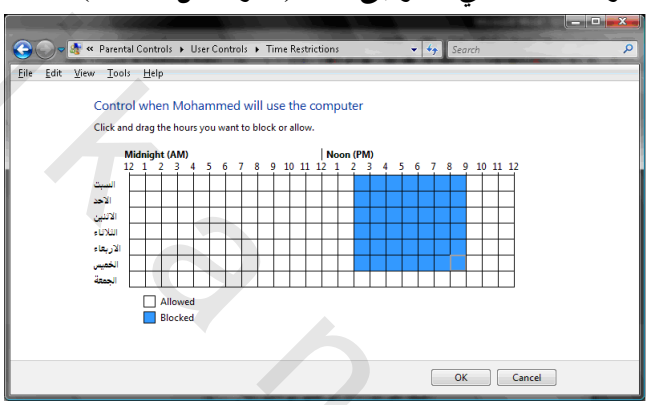


شكل ١٤–٣ نافذة Time Restrictions

تظهر في الشكل السابق شبكية بالأربع وعشرون ساعة خلال أيام الأسبوع السبعة.

٦. 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 إلي الساعة التاسعة مساءً كل أيام الأسبوع ما عدا يوم الجمعة انقر الساعات التي تشير إلى ذلك (انظر شكل ١٤-٤).



شكل ١٤-٤ تحديد الساعات المحددة للمستخدم لاستخدام الجهاز

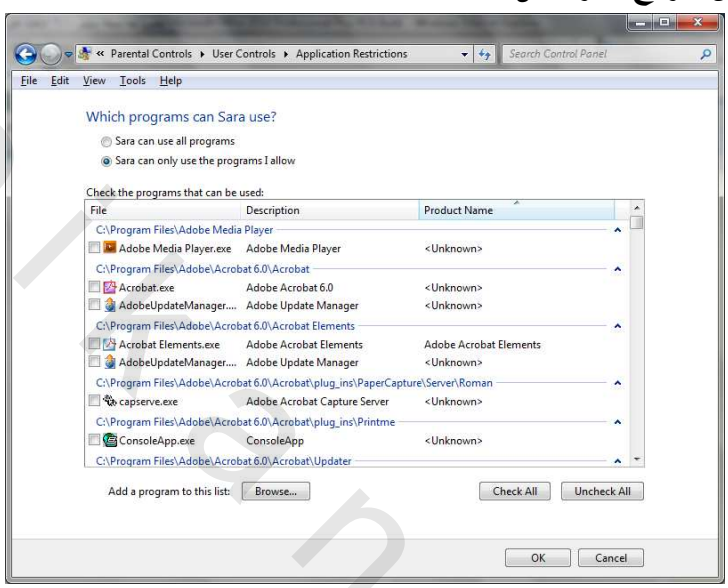
خلال الفترات الزمنية التي حددتها، إذا حاول المستخدم تسجيل الدخول إلى حسابه لن يسمح له Windows وسيظهر له رسالة تفيد أن حسابه محظور في ذلك الوقت.

٧. انقر OK "موافق" للعودة إلى النافذة السابقة.

٨. 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 Controls "عناصر تحكم الألعاب" والعودة إلي نافذة User Controls "عناصر تحكم المستخدم" .

٩. 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 انظر شكل ١٤–٥ .



شكل ١٤–٥ تحديد البرامج التى يمكن للأطفال استخدامها كنوع من المراقبة الأبوية

جدار حماية "ويندوز" Windows Firewall

جدار حماية "ويندوز" أو جدار نار "ويندوز" **Windows Firewall** يوفر طريقة آمنه بحيث لا تتم أي اتصالات خارجية إلي جهازك بخلاف التي تقبلها أو تجريها أنت وبهذا تحمي جهازك من القراصنة والبرامج الخبيثة.

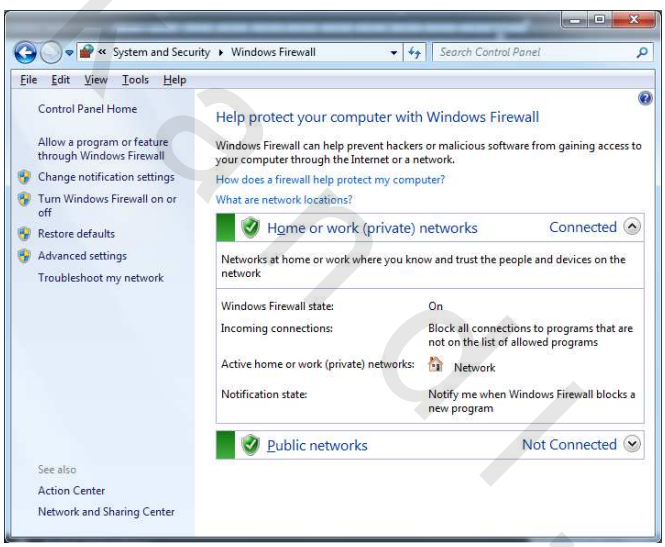
يعد جدار الحماية أحد البرامج أو الأجهزة التي تتولى فحص المعلومات الواردة من إنترنت أو من إحدى الشبكات، ثم تقوم إما باستبعادها، أو السماح لها بإمكانية المرور إلى الكمبيوتر، وذلك استنادًا إلى إعدادات جدار الحماية.

يمكن لجدار الحماية أن يساعد في منع المتطفلين أو البرامج الضارة (مثل الفيروسات المتنقلة) من الحصول على حق الوصول إلى الكمبيوتر من خلال إحدى الشبكات أو إنترنت. يمكن لجدار الحماية أيضًا أن يساعد في إيقاف الكمبيوتر عن إرسال برامج ضارة إلى أجهزة الكمبيوتر الأخرى.

تشغيل "جدار حماية Windows"

يتم تشغيل "*جدار حماية* **Windows**" بشكلٍ افتراضي في هذا الإصدار من **Windows**. للتأكد من إيقاف تشغيله، اتبع الخطوات التالية:

١. انقر زر **Start** "ابدأ" ثم انقر فوق **Control Panel** "لوحة التحكم" ثم اختر **System and security** "النظام والأمان" ثم انقر فوق **Windows Firewall** "جدار حماية **Windows**" تظهر نافذة **Windows Firewall** كما فى شكل ١٤-٦.



شكل ١٤-٦ نافذة **Windows Firewall**

٢. في الجزء الأيسر (أو الأيمن فى حالة تغيير اتجاه الشاشة)، انقر فوق **Turn windows Firewall on or off** "تشغيل جدار حماية **Windows**" أو إيقاف تشغيله. إذا تمت مطالبتك بإدخال كلمة مرور مسؤول أو تأكيدها، اكتب كلمة المرور أو قم بتأكيدها. تظهر نافذة جديدة بعنوان **Customize settings**.

٣. أسفل كل نوع موقع شبكة، انقر فوق **Turn on windows firewall** "تشغيل جدار حماية **Windows**"، ثم فوق **OK** "موافق".

نوصي بتشغيل جدار الحماية لكافة أنواع مواقع الشبكات.

مدافع ويندوز Windows Defender

يتولى مدافع ويندوز **Windows Defender** منع البرامج الخبيثة **Malware** والتجسسية **Spyware** من إلحاق الضرر ببياناتك أو سرقتها.

فى **Windows 7** يشتمل مدافع **Windows** على رسائل بسيطة وإمكانيات متقدمة لمسح البرامج الخبيثة الموجودة على الكمبيوتر بتأثير قليل على أداء الكمبيوتر.

استخدام Windows Defender

عند استخدام **Windows Defender** "مدافع ويندوز"، فإنه من المهم جداً توفر تعريفات محدثة. تُعد التعريفات بمثابة ملفات تعمل كموسوعة تنمو باستمرار حول التهديدات المُحتملة للبرامج. يستخدم **Windows Defender** "مدافع ويندوز" التعريفات لتنبيهك حول المخاطر المحتملة في حالة تحديد ما إذا كانت البرامج التي يكتشفها برامج تجسس أو غيرها من البرامج غير المرغوب فيها.

- لفتح **Windows Defender** "مدافع ويندوز" اتبع الآتي:

١. من نافذة سطح المكتب في نظام **Windows 7** انقر فوق الزر **Start** "ابدأ" .

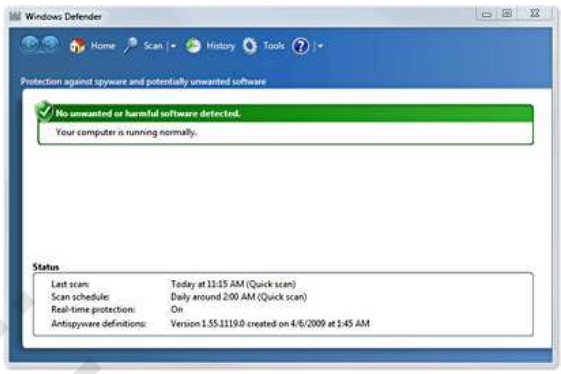
٢. في مربع البحث، اكتب **Defender**

٣. في قائمة النتائج، انقر فوق **Windows Defender** "مدافع ويندوز". (شكل ١٤-٧) تظهر نافذة **Windows Defender** ومنها تستطيع الفحص بحثاً عن برامج التخسيس وغيرها من البرامج المحتملة غير المرغوب فيها على النحو التالى:

- لفحص المناطق الموجودة على الكمبيوتر التي من المرجح أن تصيبها برامج التجسس (فحص سريع)

١. افتح **Windows Defender** "مدافع ويندوز" تظهر نافذة **Windows Defender** "مدافع ويندوز".

٢. انقر فوق **Scan** "فحص" من شريط الأدوات أعلى النافذة.



شكل ١٤–٧ يحمى مدافع ويندوز جهازك من برامج التجسس

- لفحص كافة المناطق الموجودة بالكمبيوتر (فحص كامل)

١. افتح **Windows Defender**.

٢. من نافذة **Windows Defender** انقر فوق السهم الموجود بجوار الزر فحص، ثم انقر فوق **Full Scan** "فحص كامل".

مفاهيم عامة للوقاية من الفيروسات وحماية خصوصياتك

نشرح هي هذا الجزء مفاهيم عامة تهمك لتأمين التعامل مع الكمبيوتر تشمل هذه المفاهيم تخصيص كلمة مرور لمنع الأخرين من الوصول إلي ملفاتك وتحمي خصوصياتك كما تشمل الوقاية من فيروسات البريد الالكتروني.

تعيين كلمة مرور

إذا كنت تتشارك في نفس الكمبيوتر مع شخص آخر، فإنه يستطيع بسهولة أن يقوم بتشغيل برنامج البريد الإلكتروني ويجعله يتحقق من وجود رسائل جديدة ثم يقرأ هذه الرسائل ويرد عليها باسمك. وأفضل طريقة لمنع هذا هو أن تقوم بإعداد حساب مستخدم خاص بك وتضع له كلمة مرور. وكبديل لهذا، تتيح لك معظم برامج البريد الإلكتروني تعيين كلمة مرور تمنع المستخدمين غير المصرح لهم من الوصول إلي بريدك.

لاتفتح الملفات المرفقة مجهولة المصدر

ليس هناك أي سبب يجعل شخص لا يعرفك يرسل لك ملفاً مرفقاً. فإذا تلقيت رسالة بها

ملف مرفق وكنت لاتعرف المرسل فلا تقم بفتح الملف المرفق أبداً. أما إذا أرسل لك صديق رسالة غير متوقعة وبها ملف مرفق، فلا تفترض أن صديقك هو الذي أرسل هذه الرسالة بالفعل ولا تفترض ان الملف المرفق آمن. من الممكن أن يكون كمبيوتر صديقك قد أصيب بعدوي وأن الفيروس الذي أصابه هو الذي ينسخ نفسه. في هذه الحالة، أرسل رسالة إلي صديقك اطلب منه تأكيداً بأنه هو من أرسل الرسالة المشكوك فيها.

أمن البريد الإلكتروني

العديد من برامج البريد الإلكتروني تحتوي علي خصائص لمكافحة الفيروسات. علي سبيل المثال، قد يأتي البرنامج بإعداد يمنع البرامج الأخري من إرسال بريد الكتروني باستخدام حسابك. عندما تنشط هذا الخيار، فإن الفيروس لن يتمكن من نسخ نفسه وإرسال نفسه في رسائل إلي معارفك وأصدقائك.

ومن إعدادات الأمن الأخري أن تمنع فتح أنواع الملفات التي تحتوي علي فيروسات في الغالب. وهذه الأنواع تتضمن ملفات الأوامر النصية، وملفات البرامج التنفيذية، وحتي شاشات التوقف، والتي يمكن أن تحتوي علي أوامر شريرة.

برامج مكافحة الفيروسات

من المهم أن تقوم بتثبيت برنامج جيد لمكافحة الفيروسات في جهازك، وأن تطلب منه فحص جميع رسائل البريد الإلكتروني الواردة إليك. جرب برنامج **Norton Anti Virus** (في الموقع www.symantec.com) أو **McAfee Virus Scan** في (الموقع www.mcafee.com).