الفصل الثالث

الآداب العامة و الأمان في الأنترنت

General ethics and safety

يوضح هذا الفصل الآداب العامة التي يجب عليك معرفتها أثناء تعاملك مع الانترنت وكيفية تحقيق الأمان اللازم لحماية نفسك.

بانتهاء هذا الفصل ستتعرف علي :

- إرساء القواعد العامة للأمان .
- استخدام اسم المستخدم وكلمة المرور والشهادات الرقمية.
- برامج مضادات الفيروسات.
- مفاهيم عامة للوقاية من الفيروسات وحماية خصوصياتك.
- مخاطر التجارة الالكترونية والتسوق المباشر.
- جدران النار.
- التشفير.
- تهديدات السرية من مواقع الويب المختلفة.
- التحكم في المحتوي المثير للاعتراض.
- المراقبة الأبوية .

1 إرساء القواعد العامة للأمان
General rools

كثيراً ما نقرأ في الصحف عن أناس يتنصتون على المكالمات الهاتفية وآخرون يعتدون على الممتلكات الخاصة والعامة إما بالنهب أو التخريب، فهل تسلم الإنترنت من ذلك ؟

بداية، فان الإنترنت أو الشبكة العالمية للمعلومات، عبارة عن عالم منفتح من المعلومات بلا حدود، وإذا كنت متصلا بأحد مواقع الإنترنت فان ذلك يعني أن هناك اتصالا بين نقطتين أو موقعين فلا تتعجب إذا وجدت أن أحد الأشخاص قد اخترق الاتصال بين النقطتين وبدأ في الحصول على بياناتك بطريقة آمنة أو غير آمنة، كما أن أي شخص لديه إلمام بسيط بالكمبيوتر يستطيع أن يحصل على أي معلومة من أي صفحة، يطلع عليها أو يعدل فيها بنفسه، كما أن هناك مواقع تتضمن برامج تقوم بتشغيلها دون أن تعرف صاحب هذا البرنامج ولا تسمع عنه شيئا.

الاعتبارات الأمنية Security Consideration

انتشرت فى الآونة الأخيرة محاولات السطو على المواقع واختراق الشبكات بواسطة مخربين يقال عنهم "هاكرز". يستطيع الهاكرز نسخ محتويات الموقع وإساءة استخدام هذه المحتويات، بل يستطيعون أكثر من ذلك تحميل الموقع بأكمله على أجهزتهم باستخدام برامج خاصة لديهم. على سبيل المثال فهم يستخدمون برامج تجسس **(Spyware)** لتسجيل معلومات عن بطاقات الائتمان وتسجيل أساليب الاستعراض المعتادة.

هناك الكثير من اجراءات التأمين التى يمكن باتباعها التغلب على كثير من مشاكل اختراق الشبكات ومواقع الويب مثل تأمين موقع الويب وتأمين بطاقات الائتمان واتباع أساليب التشفير والتخزين المؤقت.

وقد تضمن **Windows 7** ومستعرض الإنترنت **Internet Explorer** عدداً من أدوات (الحماية) أو الأمان والعديد من الاختيارات لاستخدامها في التعامل مع الإنترنت، ولكن قبل أن تقوم بتهيئة واستخدام أيا من هذه الخيارات يجب أن تفكر جديا في إرساء القواعد العامة (للحماية) أو الأمان، والتي تتماشى مع طبيعة عملك وأسلوب التعامل مع الإنترنت، والبيانات

المتوفرة لديك والمتوفرة على مزود الخدمة الذي تتعامل معه.

وبصفة عامة يجب أن تضع في الاعتبار عناصر الأمان التالية:

استخدام اسم للمستخدم وكلمة مرور User Name & Password

في حين أنه يمكن الوصول إلي القسم الأكبر من الانترنت بحرية ، فإن العديد من مواقع الانترنت تحتوي علي معلومات سرية أو قيّمة تجارياً ، وبالتالي فإن الوصول إلي مواقع الانترنت هذه يخضع لرقابة صارمة . الطريقة الأكثر شيوعاً لتحقيق هذه الرقابة هي الطلب من المستخدم تسجيل إسمه في موقع انترنت قبل منحه وصولاً إلي محتوياته. هذا يعني عادة أنه يجب أن يملأ نموذجاً في صفحة انترنت، ويزود موقع الانترنت بتفاصيل أساسية عنه كإسمه وعنوان بريده الإلكتروني وبلده. مقابل هذه المعلومات ، يُعطي المستخدم **Username** "إسماً" و **Password** "كلمة مرور" يتيحان له تسجيل الدخول إلي موقع الانترنت المحظور .

إن مواقع الانترنت المحمية ليست أمراً غريباً عند إجراء أي أعمال تجارة إلكترونية أو معاملات مالية علي الانترنت ، ومن السهل نوعاً ما أن يبني المستخدم نطاقاً كاملاً من الأسماء وكلمات المرور المختلفة المطلوبة للوصول إلي مواقع الانترنت المحمية.

الشهادات الرقمية Digital Certificates

بالإضافة إلي استعمال إجراءات تسجيل الدخول للتحكم بالوصول إلي بعض مواقع الانترنت ، يستعمل العديد من الأنظمة التي تتعامل مع التجارة الالكترونية والتسوق المباشر **(Online)** شهادات رقمية لتزويد أمان إضافي عند إجراء أعمال تجارية أومعاملات مالية.

إن الحاجة للتحقق من صحة المستخدم هي مسألة حاسمة لحماية الاتصالات . مبدئياً ، يجب أن يكون المستخدمون قادرين علي إثبات هويتهم للأشخاص الذين يتصلون بهم وأن يتحققوا من هوية الآخرين . التحقق من صحة الهوية علي الشبكة هو أمر معقّد ، لأن طرفي الاتصال لا يلتقيان وجهاً لوجه عندما يتصلون ببعضهما . هذا يمكن أن يتيح لشخص غير أخلاقي اعتراض سبيل الرسائل أو انتحال شخصية شخص أو كيان آخر .

Digital Certificate "الشهادة الرقمية" هي ورقة ثبوتية شائعة تزود وسيلة لإثبات هوية الشخص . تقوم مؤسسة موثوق بها كبنك مثلاً بإصدار شهادة لفرد أو لكيان. الفرد أو الكيان

الذي صدرت له الشهادة يسمي حامل(**Subject**) الشهادة.

عندما تزور موقع انترنت آمن (يبدأ عنوانه بـ **https**) ،يرسل لك الموقع شهادته تلقائياً .

Digital Signature "التوقيع الرقمي" التابع للشهادة الأمنية هو بطاقة هويتك الإلكترونية. التوقيع الرقمي يبلِّغ المستلم أن المعلومات جاءت منك حقاً وأنها ليست مزيَّفة أو لم يتم العبث بها.

يمكن لاستعمال الشهادات الرقمية أن يحمي أمانك عند التعامل مع معاملات شخصية أو مالية علي الانترنت ، لأنها تربط هوية مالك الشهادة بزوج مفاتيح إلكترونية (عمومية وخصوصية) يمكن استعمالها لتشفير المعلومات وتوقيعها رقمياً. تضمن الأوراق الثبوتية الإلكترونية أن المفاتيح تخص حقاً الشخص (أو المؤسسة) المحدده.

تحديد برامج مضادات الفيروسات *Determine Antivirus software*

تثبيت برامج مضادات الفيروسات يحفظ الكمبيوتر من مخاطر انتقال فيروسات جديدة أو فيروسات تكون انتقلت اليها عن طريق شخص اخر اذا كان يستعمل كمبيوترك.

مخاطر التجارة الالكترونية والتسوق المباشر

Risks associated with online activity

لقد ذكرنا التجارة الإلكترونية والتسوق المباشر **(Online)** بإيجاز ، وهما استعمالان شعبيان للانترنت . تسعي مواقع الانترنت الآمنة وميزة التحقق من الصحة إلي ضمان أن المعلومات المُرسلة عبر الانترنت آمنة نسبياً .

لكن معظم أنظمة التسوّق المباشر **(Online)** تتطلب أن يستعمل المستخدم بطاقة إئتمان من أجل تسديد ثمن البضائع التي يشتريها . هذا يفتح المجال أمام خطر أمني آخر .

خلافاً للشراء العادي وجهاً لوجه بواسطة بطاقة الإئتمان في المتاجر ، الشراء المباشر **(Online)** يجري عن بُعد ، مما يعني أن البائع والشاري يمكن أن يتواجدا في أي مكان في العالم . هذا بالطبع يسبّب بعض المشاكل . مثلاً ،بصفتك الشاري لا يمكنك أن تتأكد أن البائع هو الصانع الأصلي للبضاعة ، وقد تدفع ثمن شئ ولا تتلقي البضائع أبداً . نفس الشئ يصحّ للبائع أيضاً ، حيث لا يمكنه أن يكون متأكداً أن بطاقة الإئتمان الجاري استخدامها غير مسروقة أو منسوخة . لكن

تلك الأخطار موجودة أيضاً مع التسوّق عبر البريد أو الهاتف ، لذا فالانترنت ليست فريدة في هذا المضمار .

كما هو الحال مع أي معاملة أخري حساسة أو سرية ، لا يجب أن يشكل التسوق المباشر علي الانترنت خطراً أمنياً كبيراً إذا أخذت التدابير الوقائية التالية :

- اشتر دائماً من الشركات الحسنة السمعة وتأكد أن أي موقع تسوق علي الانترنت يزوّد تفاصيل اتصال شاملة عن الشركة التي تتعامل معها كأرقام الهاتف ، والعنوان المهني المسجَّل ، والعضوية بأي منظمات تجارية معروفة .
- تعامل فقط مع الشركات التي تستعمل مواقع انترنت آمنة للتسوق علي المباشر **(Online)** ، بمعني آخر ، مواقع الانترنت التي تستعمل البروتوكولات **HTTPS** للمعاملات .
- لا ترسل تفاصيل بطاقة إئتمانك بالبريد الإلكتروني كنص عادي (غير مشفر) أبداً . إذا تم اعتراض سبيل رسالة بريد إلكتروني ، يمكن قراءة تفاصيل بطاقة إئتمانك بسهولة فائقة.
- لا تفصح عن بياناتك الشخصية بطريقة غير مقصودة ، لأن هذا قد يعرضك لأعمال البلطجة أو التحرش والاستهداف من الأشخاص المتربصين وغير الأسوياء .

جدران النار Firewall

من المهم أن نفهم ما معني المصطلح **Firewall** "جدار النار" ولماذا تُستعمل جدران النار عند زيارة الانترنت ، تمرّ كمية كبيرة من حركة مرور البيانات المختلفة جيئة وذهاباً بين كمبيوترك ومزودك . معظم حركة المرور تلك غير ضارة نوعاً ما ولا تسبب تهديداً أمنياً لجهازك . لكنه من المحتمل تماماً أن يتمكن شخص مجهول بالنسبة لك من اكتساب وصول غير مرخّص له إلي البيانات . يستعمل العديد من المؤسسات وبعض الأفراد جهازاً معروفاً كـــ جدار نار يصدّ بفاعلية أي محاولة للوصول إلي البيانات الخصوصية .

هناك عادة نوعان من جدران النار : جهاز خاص يوضع بين الكمبيوتر والاتصال بالانترنت أو برنامج يشتغل علي الكمبيوتر نفسه . هذان النوعان مصممان ليفحصا البيانات الصادرة والواردة

ويصدان أي رسائل لا تستوفي متطلبات أمان محدَّدة . مثلاً أي طلبات لإرسال ملف من كمبيوترك إلي شخص آخر علي الانترنت لم تأمر كمبيوترك أن يفعل ذلك بصراحة سيوقفها جهاز أو برنامج جدار النار .

جدران النار مهمة جداً عندما يكون الكمبيوتر متصلاً بالانترنت بشكل دائم ، كما هو الحال مع معظم الاتصالات العريضة النطاق **Broadband** . الكمبيوتر الذي يُترك غير مراقب لفترات طويلة بينما يظل متصلاً بالانترنت سيكون غير محصّن كثيراً ، ولذا يجب حمايته دائماً بجهاز أو برنامج جدار النار .

التشفير Encryption

جميع البيانات التى يتم انتقالها من جهازك إلى الخادم السرى (الآمن) يتم تشفيرها. أى تحويلها إلى تنسيق لايمكن قراءته لتأمين سلامتها، حتى لايستطيع أحد من قراصنة الكمبيوتر مهاجمة هذه البيانات والإطلاع عليها واستغلالها.

فى عملية التشفير، يتم تشفير البيانات قبل إرسالها، ويتم حل هذه الشفرة بعد الوصول للجهة المطلوبة. يستخدم التشفير فى حماية الكود بالمستخدم ورسائل البريد الالكترونى والمعاملات التجارية التى تتم عبر الانترنت.

يبدو هذا معقداً جداً ، لحسن الحظ إن مهمة تشفير وفك تشفير النص المشفَّر ، ينفذها مستعرضك عادة تلقائياً .

تهديدات السرية من مواقع الويب المختلفة

Security threats from web sites

الانترنت مجال رحب لكي يمارس المخربون و الهاكرز هوايتهم الدنيئة في إيذاء الناس ولذلك فإن وسائلهم في تخريب بياناتك أو تعطيل كمبيوترك كثيرة ويجب الانتباه إليها . من ذلك مثلاً

- الفيروسات **Viruses** وقد تناولناها بالتفصيل وتحدثنا عن ضرورة تثبيت برامج مضادات الفيروسات لتجنب مخاطر الفيروس.
- الديدان وحصان طروادة **Worms & Trojan horses**
- برامج التجسس والبرامج الخبيثة **Spyware & malware programs**

الحماية من الفيروسات وحصان طروادة

Protection against virus& Trojan

- قم بتركيب برنامج مكافحة الفيروس من شركة معروفة ومشهورة وتحديثه واستعماله بإنتظام. تظهر فيروسات جديدة كل يوم، ولاتوفر برامج مكافحة الفيروس التي لا يتم تحديثها لعدة أسابيع الحماية الكفاية ضد الفروسات الحالية.
- إستخدام برنامج مكافحة الفيروس الذي يقوم بالمسح عند الدخول. وهذا سيحمي نظامك من خلال التحقق من الفيروسات في كل مرة يدخل فيروس إليك إلي ملف قابل للتنفيذ أو عندما يقوم بتنزيل بريد إلكتروني.
- قم بمسح أي ملف أو قرص جديد قبل فتحه بغض النظر عن مصدره. فإن الأقراص مرنة والأقراص المدمجة وسيلة سهلة لنشر الفيروسات.
- لا تقم بفتح أي رسائل إلكترونية أو مرفقات ملف بريد إلكتروني لم تكن تتوقع إستلامه. بإمكان بعض الفيروسات أن ترسل نفسها عبر البريد الإلكتروني وتظهر أيضاً في رسالة تبدو كأنها من شخص تعرفه. ببساطة، قم بحذف الرسالة وتفريغ سلة مهملات البريد الإلكتروني.

2 مفاهيم عامة للوقاية من الفيروسات وحماية و خصوصياتك
Safety and Security

نشرح هي هذا الجزء مفاهيم عامة تهمك لتأمين التعامل مع الكمبيوتر تشمل

سياسة الاستخدام القانوني للانترنت
Policy of the lawful use of the Internet

كثيراً ما ستصادف سياسات خاصة باستخدام الإنترنت بطريقة مناسبة . فعلي سبيل المثال قد تعمل الشركة التي تعمل بها علي وضع سياسات خاصة باستخدام خدمات الإنترنت أثناء العمل، حتي مجموعات الأخبار قد تفرض بعض السياسات لعمليات المراسلة داخلها (ما يتعلق باستخدام الألفاظ السيئة) ، وقد يعمل مزودو خدمة الإنترنت علي تحديد حجم البيانات أو المواد التي يتم تنزيلها أو إرسالها إلي الإنترنت وذلك لضمان سمعتها ولضمان عدم استخدام الألفاظ السيئة و المخادعة .

يتم وضع هذه السياسات من أجل حماية المنظمات من عمليات الاستخدام الخاطئ لخدمات الإنترنت (وذلك لعدم وجود وسائل فنية تقوم بضبط هذه الممارسات) . إذا قمت باستخدام خدمة الإنترنت فإنه يجب أن تقرأ وتستجيب لمثل هذه السياسات .

الخصوصية والأمان في البريد الالكتروني Privacy and Security in e-mail

يعتبر البريد الالكتروني وسيلة فعالة في إرسال الرسائل والبيانات بطريقة سريعة ، ومع ذلك فيجب الانتباه والحيطة عند استخدام البريد الالكتروني . ومن القواعد المهمة عند استخدام البريد الالكتروني .

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.

الفيروسات ومضادات الفيروسات Viruses & Antivirus

تسبب فيروسات الكمبيوتر مشكلة أمنية كبيرة لمستخدمي الانترنت . كلما تم تلقي رسالة بريد إلكتروني تحتوي علي ملف مُرفق أو كلما تم تحميل ملف من موقع انترنت ، هناك احتمال أن يُصاب كمبيوترك بعدوي فيروس .

Virus "الفيروس" هو برنامج أو قطعة من الشيفرة يتم تحميله في كمبيوترك من دون أن تعرف ذلك ويشتغل رغماً عنك . في حين أن العديد من الفيروسات غير مؤذية ، إلا أن جزءاً كبيراً منها مصمم ليتسبب بعرقلة خطيرة لأنظمة الكمبيوتر إما بحذفه أو تشويهه الملفات الموجودة علي القرص الصلب . بإمكان الفيروسات أن تستنسخ نفسها أيضاً ، لذا يُنشئ الفيروس نسخة عن نفسه مراراً وتكراراً وبالتالي ينتشر من حاسب آلي إلي آخر من خلال الانترنت .

هناك طريقتان مهمتان يمكنك بهما حماية نفسك من التلوث بفيروس عند استعمال الانترنت:

- تأكد أنك تحمّل الملفات فقط من مواقع الانترنت الحسنة السمعة ، وكن حذراً من أي رسائل بريد إلكتروني توسّلية تحتوي علي ملفات مرفقة مُرسلة من أشخاص لا تعرفهم شخصياً .
- تأكد أن هناك برنامج مضاد للفيروسات ملائم مثّبت في جهازك وأنه يتم تحديثه دائماً.

برامج مكافحة الفيروسات Antivirus software

يعج الإنترنت بالبرمجيات التي تساعد في تحسين أداء الإنترنت، ولكنها قد تحمل في طياتها الخطر

المحدق والذي يتمثل في العديد من الفيروسات، كما أن هناك عددا لا بأس به من البرمجيات التي قد تسبب تعارض أثناء التشغيل، ولهذا فان الشبكة التي يتصل بها جهازك قد يتم تدمير ما تحتوي من معلومات وبرامج وتصبح قاصرة عن أداء الأعمال أو تتوقف، لذا يجب أن يقوم مدير الشبكة بالتحكم في نوعية البرامج التي يمكن تحميلها من الإنترنت .

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). ويجب الاهتمام بتحديث برامج مكافحة الفيروسات .

تحديث برامج مضادات الفيروسات *Update anti-virus software*

المخربون أو الهاكرز لا يتوقفون عن تحديث وانتاج برامج التجسس **Spyware** والبرامج الخبيثة **malware** التي من الممكن أن تدمر بياناتك ، وعند تشغيل برنامج مكافحة فيروسات منتجٌ قبل برنامج الفيروس فقد لا يتعرف عليه ، لهذا وجب الانتباه إلي استخدام أحدث نسخة من برنامج مكافحة الفيروسات الذي تستخدمه . إن استخدام أحدث إصدارات من برنامج مكافحة الفيروسات **(anti-virus)** يجنبك الكثير من مخاطر فقد بياناتك .

التحكم في المحتوي المثير للاعتراض

The Control of charged content to object

المحتوى المثير للاعتراض، هو المحتوى الذي يتعارض مع الخلق القويم وعادات المجتمع والشرع الحنيف. فكما يحلو لبعض الناس السير بعكس اتجاه الشارع أو إيقاف سياراتهم في أماكن ممنوعة وتعطيل حركة المرور، يحلو لبعض مستخدمي الانترنت أن يجرحوا مشاعر الآخرين واختراق خصوصياتهم بالصور الخليعة، أو اللغة المرفوضة التي تخدش الحياء، أو نشر الصور التي تثير الخوف والرعب والتي تسبب فزعاً للصغار والكبار. بل يتعدى الأمر أحيانا كل ذلك إلى تقديم وصف للتميز العنصري أو للمخدرات واستعمال الأسلحة وغيرها من الأمور التي تضر بالمجتمع كله.

لقد قامت مؤسسة مستقلة بتصنيف مواقع الويب حسب المحتوى الذي يمكن عرضه على الانترنت. هذه المؤسسة تسمى:

Internet Content Rating Association وتختصر هكذا **ICRA**. ويمكن ترجمتها

"جمعية تصنيف محتوى الانترنت".

ليضمن **IE** إعدادات تحمي مشاعرك من أن يجرحها منظر خليع أو كلمة سوقية، أو وصف يشجع على تصرفات غير مرضية. وذلك كله تماشيا مع التصنيف الذي وضعته "جمعية تصنيف محتوى الانترنت".

وتتحكم ميزة "مرشد المحتويات" **Content Advisor** في **IE** في كل فئة من فئات المحتوى الذي يمكن عرضه على الانترنت وطبقا للتصنيف السابق. بأربعة مستويات هي:

None "بلا" ، **Limited** "محدود" ، **Some** "بعض"، **Unrestricted** "غير مقيد".

إضافة مواقع الإنترنت الى منطقة أمان

Add sites to the area of Internet safety

عندما تتعامل مع مواقع إنترنت موثوقة مثل قاعدة بيانات أحد البنوك المعروفة، أو مواقع محترمة تثق في أن بياناتها لا تحتوي على فيروسات أو برامج لم يتم اختبارها، فمن الأفضل ألا تضع قيود أمان على استخدامها، فأنت تدرك أن أنظمة الأمان لابد ولاشك أن تؤثر بطريقة أو بأخرى على مستوى الأداء، وعدم استخدام هذه الأنظمة مع المواقع الموثوقة سوف يوفر لك الاستخدام الأمثل ومستوى الأداء المرتفع.

أما المواقع الخطرة أو الغير آمنة وخاصة عندما تدخل عليها من خلال شبكة محلية، فيجب عليك أن تضيفها إلى منطقة من مناطق الأمان وأن تحدد مستوى التعامل مع تلك المواقع .

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**

ملخص الفصل Summary

الدرس الأول : شرحنا القواعد العامة للأمان في الانترنت والتي تساعدك في التغلب علي مشاكل اختراق الشبكات ومواقع الويب مثل استخدام اسم للمستخدم وكلمة مرور والتأكد من سرية مواقع الويب عن طريق التشفير وجدران النار ومضادات الفيروسات والشهادات الرقمية .

الدرس الثاني : شرحنا مفاهيم عامة للوقاية من الفيروسات وحماية خصوصياتك مثل اتباع سياسة الاستخدام القانوني للانترنت واتباع قواعد الخصوصية والأمان في البريد الالكتروني ، واستخدام برامج مكافحة الفيروسات والتحكم في المحتوي المثير للاعتراض والمراقبة الأبوية .