أمن المعلومات
INFORMATION SECURITY

نظري L 5

1. مقدمة:

ساهم الحاسوب في رفع سوية الحياة التي نعيشها باختصاره للوقت والجهد، وأصبحت الكثير من الأمور لا تتم إلا بمساعدة الحاسوب (مثلاً المعاملات المالية وتنظيم رحلات الطائرات وتشغيل الكثير من الأجهزة الطبية والصناعية).

بعد ذلك ظهر الانترنت، حيث أصبح استخدام المعلومات في أجهزة الحواسيب وتناقلها عبر الشبكة الداخلية أو الشبكة العنكبوتية من الأمور الروتينية في وقتنا الحالي وأصبح من الصعب الاستغناء عنها كونها سهلت متطلبات العمل اليومية، ولكنها سلاح ذو حدين إذ أن هذه التقنية معرضة للاختراق والضرر الناتج إما عن سوء الاستخدام أو الاستهداف عن قصد.

إن أمن المعلومات مرتبط ارتباطاً مباشراً بأمن الحواسيب، فيجب أن تحدّد إجراءات وقائية ودفاعية وحسب الامكانيات المتوفرة.

2. مفهوم أمن المعلومات:

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.

أنت بالتأكيد لا ترغب أن يكون للآخرين مدخلاً لمعلوماتك الخاصة، ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات. فعلى سبيل المثال، يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي.

ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الإنترنت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام الكمبيوتر لديك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

أمن المعلومات:

مجموعة من الإجراءات الوقائية للحفاظ على المعلومات من مخاطر الاستخدام الغير صحيح سواء كان متعمّد أو عن غير قصد

توصف هذه الاجراءات بأنها عمليات مستمرة تتطلب استمرارية في التطوير ومتابعة للمستجدات ، واستمرار في مراقبة وافتراض المخاطر وابتكار الحلول لها

لهذا المنظمات لا توصف بأن لها نظام معلوماتي أمني حقيقي وفعال حتى تحقق نظام تطويري مستمر للعمليات الأمنية والبشرية والتقنية من أجل تقليل واحتواء المخاطر المفترضة أو المتوقعة.

3. مكونات أمن المعلومات:

قد يتبادر إلى أذهاننا أن أمن المعلومات وجرائم الحاسوب هو عبارة عن كشف معلومات سرية ولكن في الحقيقة أن الحفاظ على سرية المعلومات هو مكون واحد من أصل ثلاثة مكونات أساسية تعتبر على درجة واحدة من الأهمية وهذه المكونات هي:

1) سرية المعلومات Data Confidentiality:

يشمل هذا الجانب كل التدابير اللازمة لمنع اطلاع الأشخاص الغير مصرح بهم على المعلومات السرية، ومن أمثلة المعلومات التي يحرص على سريتها: المعلومات الشخصية لوزارة معينة.

2) سلامة محتوى البيانات Data Integrity:

يشمل هذا الجانب التدابير اللازمة لحماية المعلومة من التلاعب (التغيير) من قبل أشخاص مخولين أو أشخاص يوهمون النظام بأنهم مخولين.

مثال على ذلك: التلاعب بقواعد البيانات لوزارة معينة.

3) ضمان الوصول إلى المعلومات Data Availability:

إن المعلومات تصبح بلا قيمة في حالة عدم إمكانية الوصول إليها من قبل الأشخاص المخولين إليها.

وينفذ المخربون وسائل عدة لمنع الأشخاص المخولين من الوصول إلى المعلومة، مثلاً استهداف بناية تحوي على قاعدة بيانات مهمة.

لتحقيق هذه الأمور، نحتاج لاستخدام مجموعة من المقاييس، حيث تدرج هذه المقاييس تحت ثلاثة أمور رئيسية لفهم أمن الشبكات وأمن الوصول للبيانات، وتستخدم هذه الأمور بشكل يومي في حماية البيانات الخاصة وحماية الأنظمة من التخريب المتعمد والغير متعمد ، وهي:

- ✓ التحكم بالوصول (Access Control):

ممكن أن تعرف كسياسة للتحكم بمكونات البرامج أو مكونات الأجهزة من حيث المنع أو السماح للوصول إلى مصادر الشبكة ويمكن تمثيلها بالبطاقات الذكية أو أجهزة البصمة ويمكن أن تكون أجهزة الاتصال الشبكي مثل الراوترات أو نقاط الوصول للأجهزة اللاسلكية فيجب تخصيص صلاحيات على الملفات الشخصية لمستخدمي الكمبيوتر.

- ✓ إثبات الصلاحيات (Authentication):

هي عملية التحقق من صلاحيات المستخدمين على مصادر الشبكة ويتم تحديد المستخدم من خلال استخدام اسم المستخدم وكلمة السر أو البطاقات الذكية ويتم بعد ذلك إعطاءه الصلاحيات بناء على هويته.
وهذه الصلاحيات يتم تحديدها من قبل مدير الشبكة.

- ✓ التدقيق (Auditing):

هي عبارة عن عمليات التدقيق وتتبع الصلاحيات عن طريق مراقبة الموارد والشبكة وتعتبر من أهم الأمور في مجال أمن الشبكة حيث يتم التعرف على المخترقين ومعرفة الطرق والأدوات التي تم استخدامها للوصول إلى الشبكة.

4. الوعي الأمني للمعلومات:

أن مخاطر غياب مفهوم أمن المعلومات لدى معظم المستخدمين مشكلة حقيقية، فكثير من المخاطر الواقعة على أمن المعلومات صادرة من داخل مكان العمل، بعضها بسبب الجهل وبعضها بسبب الخطا أو الإهمال.
فبعضهم يتساهل في تداول وسائل التخزين المختلفة دون التأكد من خلوها من البرامج الضارة، وبالتالي يعرض البيانات إلى خطر التلف أو السرقة والعبث.
وقد يتسبب الجهل بنوع الخطر وطريقة معالجته بخطر آخر لا يقل عن سابقه في الخطورة.
ومن الأمور التي تعتبر غاية في الأهمية هو التصنيف الأمني للمعلومات، فلا بد من تحديد القيمة الفعلية للبيانات والتعريف بدرجات سريتها وحساسيتها ومن ثم تعريف إجراءات الحماية المناسبة لكل معلومة بحسب أهميتها ، فليس كل البيانات بنفس القدر من الأهمية، ولهذا يجب التفاضل أيضاً بينها في درجة الحماية.
وأيضاً لابد من الفحص الدوري للمعلومات والتاكد من صحة بقائها في المستوى المناسب لأهميتها، فأهمية المعلومات والبيانات تتغير من حين لآخر، ومن ثم تحتاج إلى إعادة تصنيف من جديد.

5. مخاطر الشبكة المختلفة:

تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة.
وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل بطء حركة التصفح وانقطاعه على فترات منتظمة، ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.
وفي حالة وجود أخطاء برمجية أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق

للنظام، كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم من تعديل النظام ،وبالتالي تعطل الجهاز مؤقتاً.
إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.
كل ذلك يحدث باستخدام برامج ضارة والتي سنتعرف عليها التفصيل .

❖ **البرامج الضارة (الخبيثة) (Malware):**

تعرّف بأنها أي برنامج يكون كل مهامه أو أحدها عمل ضرر ما في النظام من تجسس، تخريب أو استنزاف لموارد النظام (الوقت،المعالج،الذاكرة،وحدة التخزين،موارد الشبكة،...الخ).
ومن الدوافع الشائعة لتطوير مثل هذه البرامج:

1) أن يثبت الشخص لنفسه أو لغيره مقدرته على تطوير برامج تستطيع الاختراق أو التجسس ، وغالباً ما ينتشر هذا النوع بين صغار السن والمبتدئين.
2) للتجسس الصريح وسرقة المعلومات، سواء على مستوى الأفراد أو الشركات أو الوزارة.
3) الانتقام من أفراد أو شركات أو وزارة أو دولة.
4) التسويق التجاري، غالباً ما تكون الإعلانات التجارية غير مرغوب بها وإجبارية وتستنزف موارد النظام من معالج وذاكرة ووحدة تخزين وسعة نقل الشبكة.

- أنواع البرامج الضارة (Malware):

هناك أنواع عديدة للبرامج الضارة، منها الخبيث الصريح ومنها ما يكون من ضمن أعمالها تأثير سلبي غير معلوم للمستخدم، مثل: استخدام مصادر الحاسوب (الذاكرة والمعالج) ، والتجسس التجاري، وبهذا التقسيم يمكننا إدراج برامج الإعلانات Adware، وبرامج متابعة تصرفات المستخدم أو التجسس البسيط Spyware تحت البرامج الضارة، لأنها إما أن تستهلك موارد الحاسوب والشبكة، أو تتابع تحركاتك دون علمك، وهذا بحد ذاته عمل ضار، وفيما يلي بعض أنواع البرامج الضارة.

- الفيروسات Viruses.
- الديدان Worms.
- الخدع أو البلاغ الكاذب Hoax.
- الأحصنة الطروادية Trojan Horses.
- رسائل الاصطياد الخادعة Phishing Scam.
- برنامج تجسسي Spyware.
- برنامج إعلاني Adware.
- صفحات فقاعية أو انبثاقية Popup.
- برنامج تسجيل نقرات لوحة المفاتيح Keystroke Logger.

- طرق الإصابة بها:

1) وسائط التخزين المختلفة:

تنتقل البرامج الضارة من حاسوب مصاب إلى آخر سليم بواسطة وسائط التخزين المتنقلة، ومن أمثلة الوسائط: وحدة التخزين Flash memory و كرت الذاكرة Memory card، والقرص المدمج CD/DVD، والقرص الصلب الخارجي External hard.

2) عن طريق البريد الالكتروني:

أصبح البريد الالكتروني من أهم وسائل نقل البرامج الضارة وذلك لانتشاره الواسع بدون قيود أو حدود.

هناك عدة وسائل لانتقال البرامج الضارة عن طريق البريد الالكتروني:

- عن طريق المرفقات Attachments: يمكن إرسال رسالة تحتوي على مرفق لبرنامج يدعى فائدته وعند فتحه يصاب نظامك بالملف الضار، وقد ينتحل الهاجم البريد الالكتروني الخاص بأصدقائك لإضفاء قدر من المصداقية لكي لا يساورك الشك بأن صديقك سيرسل لك برنامجاً ضاراً.
- عن طريق رابط في الرسالة: تحتوي بعض الرسائل البريدية على رابط يحثك على الضغط عليه، كأن يدعي بأنه رابط لصورة أو تحديث لسد ثغرة أمنية، ....الخ.

3) تصفح المواقع المشبوهة:

يحتوي متصفح الانترنت على العديد من الثغرات الأمنية التي غالباً ما يتجاهل المستخدم سدها أو إصلاحها، وبعض المواقع المشبوهة تستغل تلك الثغرات لاختراق النظام وأنصح بعدم استخدام متصفح Internet Explorer الموجود في نظام التشغيل Windows وتحميل إحدى المتصفحين إما Firefox او Google Chrome.

4) المراسلة الآنية:

وهي برامج للتخاطب وتناقل الملفات بشكل مباشر مع الأصدقاء أو الغرباء، وهنالك مشكلتين رئيسيتين لهذه البرامج: أنك لاتستطيع التأكد بأن من يخاطيك هو صديقك فعلاً لأن يمكن للشخص المهاجم انتحال شخصيته، والمشكلة الثانية هي الثغرات الأمنية لبرامج المراسلة الآنية.

يجب مراعاة استخدام آخر إصدار لبرامج المخاطبة لأنها تحتوي آخر التحديثات الخاصة بسد الثغرات الأمنية الخاصة بالبرنامج.

5) المنافذ المفتوحة:

عندما يتصل النظام بالشبكة فإنه يتخاطب من خلال منافذ معينة، فمثلاً عندما نتصفح الانترنت فإننا نمر من خلال منفذ رقم 80، وعندما نريد إرسال بريد الكتروني نستخدم منفذ رقم 25.

يستطيع المهاجم من خلال ثغرات أمنية على بعض التطبيقات المعتمدة على بعض المنافذ تمرير برامج ضارة إلى نظامك دون علمك.

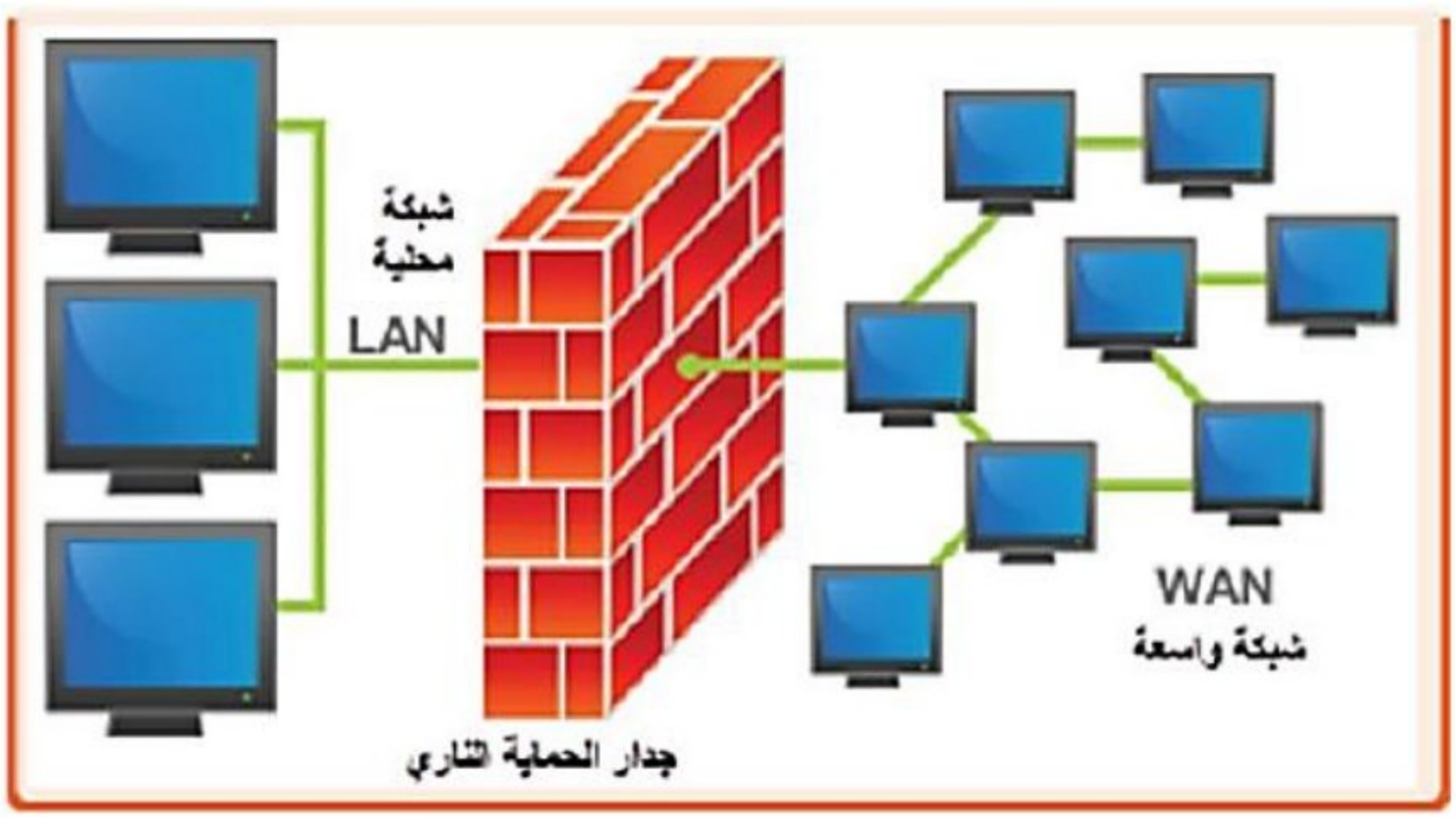
6) تحميل برامج من الانترنت:
قد تحوي البرامج التي تخزن من الانترنت على برامج ضارة فيجب التحميل فقط من المواقع الموثوقة.

- طرق الوقاية العامة من البرامج الضارة:

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

✓ الحصول على جدار حماية ناري: (Firewall)

جدار الحماية الناري من الإنترنت هو برنامج أو جهاز يقوم بفرز وتصفية الفيروسات والديدان والمتسللين والمعتدين الذين يحاولون الوصول إلى جهازك عبر الإنترنت. ويعتبر تركيب جدار حماية ناري أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية جهاز الكمبيوتر لديك هو القيام بتركيب جدار حماية ناري قبل الدخول إلى الإنترنت للمرة الأولى والإبقاء عليه عاملاً في كافة الأوقات.
تتمثل وظيفته بعزل شبكة الحاسوب أو جهاز الحاسوب عن غيره من الشبكات، من خلال مراقبة الاتصالات وتطبيق القواعد التي تمنع الاختراق والقرصنة، ويقوم جدار الحماية بتطبيق مجموعة من قواعد الأمن على هذه الاتصالات، بحيث يسمح للاتصالات التي تتوافق مع هذه القواعد بالمرور، ويمنع الاتصالات الأخرى، وعادة ما يتم وضع هذه القواعد من خلال مستخدم الجهاز ومن خلال مدير النظام للشبكات، ويوضح الشكل أدناه جدار حماية ناري وآلية عمله.



يمكنك الحصول على جدار حماية ناري لجهازك من محلات الكمبيوتر أو من خلال الإنترنت. علما أن بعض أنظمة التشغيل مثل ويندوز إكس بي مع الحزمة الخدمية/الإصدار-2 (Service Pack2) ونظام التشغيل ماكنتوش (MacOS X) يوجد من ضمنها جدار حماية ناري.

✓ الحصول على برنامج مكافحة فيروسات:

إضافة لبرنامج الحماية الناري(Firewall) ، فإن عليك الحصول على برنامج مكافحة فيروسات قبل الدخول إلى الإنترنت للمرة الأولى. حيث يقوم برنامج مكافحة الفيروسات بفحص جهازك لمعرفة الفيروسات الجديدة التي أصيب بها ومن ثم تنظيف هذه الفيروسات بما يكفل عدم إلحاق المزيد من الأذى بجهازك.

وكما هو الحال في جدار الحماية الناري، فإن عليك الإبقاء على برنامج مكافحة الفيروسات عاملاً في جميع الأوقات بحيث أنه بمجرد تشغيل جهازك يبدأ البرنامج بالعمل للكشف عن الفيروسات مما يضمن التعامل معها بأسرع ما يمكن. كما يقوم برنامج مكافحة الفيروسات بالكشف عن الفيروسات في الأقراص المدخلة في جهازك والبريد الإلكتروني الذي تستلمه والبرامج التي تقوم بتحميلها في جهازك من الإنترنت.

في حالة دخول فيروس إلى جهازك، فإن برنامج مكافحة الفيروسات سينبهك بذلك ومن ثم سيقوم بمحاولة إصلاح الملف المصاب، كما يقوم هذا البرنامج بعزل الفيروسات التي لا يستطيع إصلاحها مع محاولة إنقاذ وإصلاح أية ملفات مصابة يستطيع إصلاحها. هذا علماً بأن بعض برامج مكافحة الفيروسات تطلب منك إرسال الفيروس إلى شركة مكافحة الفيروسات، كي يتسنى لها إدخاله ضمن قاعدة بياناتها إذا كان من الفيروسات الجديدة.

يمكنك شراء برامج مكافحة الفيروسات عبر الإنترنت أو من محلات بيع البرمجيات، كما يستحسن التأكد فيما إذا كان مزود خدمات الإنترنت الذي تتعامل معه يزود مثل هذه البرمجيات. ومما تجدر ملاحظته، أنه في حالة كون جهازك مصاباً بالفيروسات، فمن الخطر شراء برنامج الحماية عبر الإنترنت لأنه يمكن لبرنامج التجسس التلصص على معلومات بطاقتك الائتمانية وسرقتها حتى ولو أدخلتها في صفحة ويب آمنة.

يجب أن يكون برنامج مكافحة الفيروسات مناسباً لجهاز الكمبيوتر لديك والبرامج التي لديك. وهناك العديد من أنواع البرامج المتوفرة التي تناسب مستخدمي أنظمة التشغيل ويندوز ولينكس وماكنتوش .(MacOS) علماً بأن أكثر برامج مكافحة الفيروسات استخداماً هي البرامج المزودة من ماكافي(McAfee) ، ونورتن (Norton Antivirus)من سيمانتك(Symantic) ، وأنظمة سيسكو (Cisco System)وميكروسوفت.(Microsoft)

✓ حافظ على تحديث برامج وجهازك:

نظراً لأن الفيروسات تتغير باستمرار، فمن الأهمية بمكان قيامك بالتحديث المستمر لنظام التشغيل الموجود في جهازك وبرنامج جدار الحماية الناري وبرنامج مكافحة

الفيروسات المركب في جهازك، بحيث يتم إدخال آخر تحديثات صدرت عن هذه البرامج. وسيقوم برنامج مكافحة الفيروسات بسؤالك تلقائياً بتحديث البرنامج وعليك التأكد من قيامك بالتحديث. علماً بأن الكثير من برامج مسح الفيروسات يمكن الحصول عليها مرة كل سنة، وننصحك بترقية البرنامج بعد ذلك حفاظاً على تضمين جهازك آخر التحديثات.

- ✓ لا تفتح رسائل البريد الإلكتروني المشكوك فيها:

تصل معظم الفيروسات إلى أجهزة الكمبيوتر عبر البريد الإلكتروني، لذا لا تفتح أي مرفقات بريد إلكتروني لا تعرف مصدره أو غير متأكد من محتوياته حتى ولو كنت تستخدم برنامج مكافحة فيروسات. مع ملاحظة أنه يمكن أن تصلك رسائل بريد إلكتروني مصابة بالفيروسات حتى من أصدقائك وزملائك والمسجلين لديك في قائمة البريد الإلكتروني. ولا يكون الفيروس خطيراً إلا إذا فتحت المرفقات المصابة. وتأكد من أن محتويات الرسالة تبدو منطقية قبل فتح المرفقات. كما يجدر بك ألا تقوم بتمرير أو إحالة أي مرفقات قبل أن تتأكد من أنها آمنة. وقم بحذف أية رسالة تعتقد أنها مصابة وقم كذلك بتفريغ الرسائل المحذوفة من المجلد الذي يحتوي عليها بشكل منتظم.

- ✓ الحذر عند إقفال النوافذ المنبثقة:

النوافذ المنبثقة هي النوافذ التي تقفز على شاشة الكمبيوتر لديك عند ذهابك إلى مواقع إلكترونية محددة. وبعض المواقع الإلكترونية تحاول خداعك لتنزيل برامج تجسس أو برامج دعاية في جهازك من خلال الضغط على موافق (OK) أو اقبل (Accept)الموجودة في النافذة المنبثقة. وعليك إتباع وسيلة آمنة لإقفال هذه النوافذ آلا وهي الإقفال من مربع العنوان (X) الموجود في أعلى النافذة.

- ✓ فكر ملياً قبل تنزيل ملفات من الإنترنت:

يمكن كذلك أن تُصاب بفيروسات وبرامج دعاية وبرامج تجسس من خلال تنزيل برامج وملفات أخرى من الإنترنت. فإذا كان البرنامج مجانياً ومزود من قبل مطور برمجيات مجهول، فهو من المرجح أن يحتوي على برمجيات إضافية وغير مرغوب فيها أكثر مما لو كانت قد تمت بتنزيل أو شراء برنامج من مطور برمجيات مشهور ومرموق.

- ✓ برامج مراقبة بيانات الشبكة:Packet Sniffers

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

- ✓ عمل نسخ احتياطية من ملفاتك:

لتفادي فقد ملفات العمل لديك في حالة تعرض كمبيوترك للإصابة بالفيروسات، عليك التأكد من عمل نسخ احتياطية لملفاتك المهمة. وإذا كنت تقوم بشكل منتظم بعمل نسخ

احتياطية للمعلومات الموجودة في جهازك على أقراص صلبة خارجية أو أقراص ضوئية قابلة للكتابة أو أقراص مرنة، فلا تضع أقراص النسخ الاحتياطية المساندة في جهاز الكمبيوتر لديك إذا كنت تعتقد أن لديك فيروساً، لأنه يمكن للفيروس الانتشار إلى تلك الأقراص.

✓ التحديثات:

حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه. وإذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

✓ التشفير:

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.