مهارات الحاسب الالي

computer skills



الفصل السادس
فيروسات الحاسب

أهداف الفصل

الأهداف الرئيسية :

- التعرف على أنواع المخاطر التي تهدد الحاسب والبيانات .
- التعرف على الفيروسات من حيث آلية العمل وكيفية الإصابة بها والتعامل معها
- التعرف على طرق حماية البيانات .

تعريف فيروس الحاسب :

- هو برنامج له القدرة على الانتشار بين أجهزة الحاسبات المختلفة بإخفاء نفسه في ملف أو برنامج تطبيقي ، ويهدف إلى إصابة الحاسب بأضرار محددة غير مرغوب فيها .

أنواع المخاطر التي تهدد الحاسب والبيانات:

الاختراق :

- هو إمكانية الدخول إلى معلومات ما داخل الحاسب بطريقة غير شرعية والسبب الرئيسي للاختراق هو استخدام الانترنت ، مع وجود ثغرات في نظام الحماية بالجهاز

دوافع الاختراق :

- الحصول على المال من خلال سرقة المعلومات البنكية .
- الحصول على معلومات شخصية بهدف الابتزاز .
- الحصول على الرموز السرية للبريد الإلكتروني للتجسس على الرسائل الشخصية .
- الحصول على كلمة السر لأحد المواقع بغرض تدميره أو تغيير محتواه .

أنواع الاختراق :

- تنقسم أنواع الاختراق من حيث الطريقة المستخدمة إلى ثلاثة أنواع :

١- اختراق الخادمات للشركات أو الجهات الحكومية .

٢- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات .

٣- التعرض للبيانات أثناء انتقالها والتعرف على شيفرتها إن كانت مشفرة ، وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية .

برامج التجسس :

- هي برامج تهدف لجمع معلومات شخصية عن فرد أو مؤسسة دون علمهم ، والتي قد تتسبب في سرقة البيانات ، وبطء في الحاسب ، ويمكن أن تكون البيانات المسروقة كلمات سر مثلاً .

طرق الإصابة بملفات التجسس :

- يمكن عبر جلسات المحادثة الإلكترونية .
- يمكن عبر البريد الإلكتروني .
- يمكن من خلال تنزيل برامج أو ملفات من مواقع غير موثوقة .
- عبر استخدام وحدات تخزين مصابة .

الهاكرز:

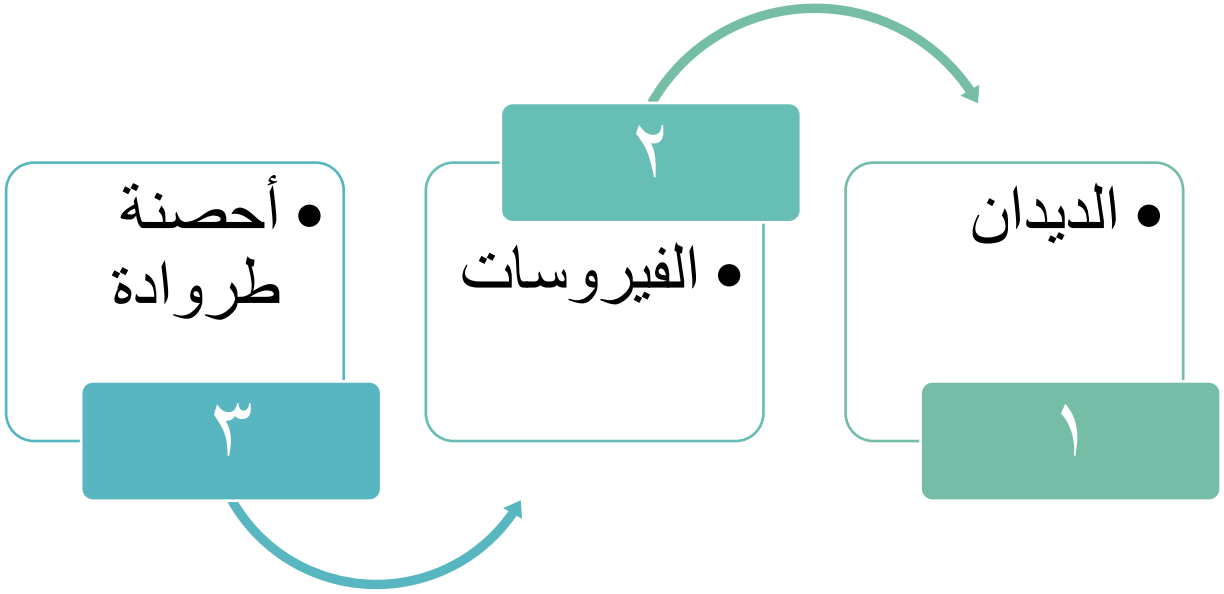
- هم أشخاص خبراء باختراق الحاسب لكي يصلوا إلى المعلومات المخزنة ، وهم متطفلون يتحدون أمن نظم الشبكات ولكن لا تتوافر لدى الغالبية العظمى منهم دوافع تخريبية .

الكراكرز:

- هم أشخاص متخصصون أو خبراء في مجال الحاسب ولكنهم يقومون بأنشطة غير شرعية أو قانونية ، مثل عمل برنامج لغرض الشرقة ، أو عمل برنامج للحصول على المعلومات بطرق غير قانونية .

برامج الحاسب الخبيثة :

- هي برمجية صغيرة يتم إدراجها في نظام الحاسب لإلحاق الضرر به أو تدميره ومن الممكن أن يكون الخطر بسيطاً يؤدي إلى خلل لا يمكن إصلاحه إلا بمسح بيانات الحاسب
- وهي عدة أنواع :

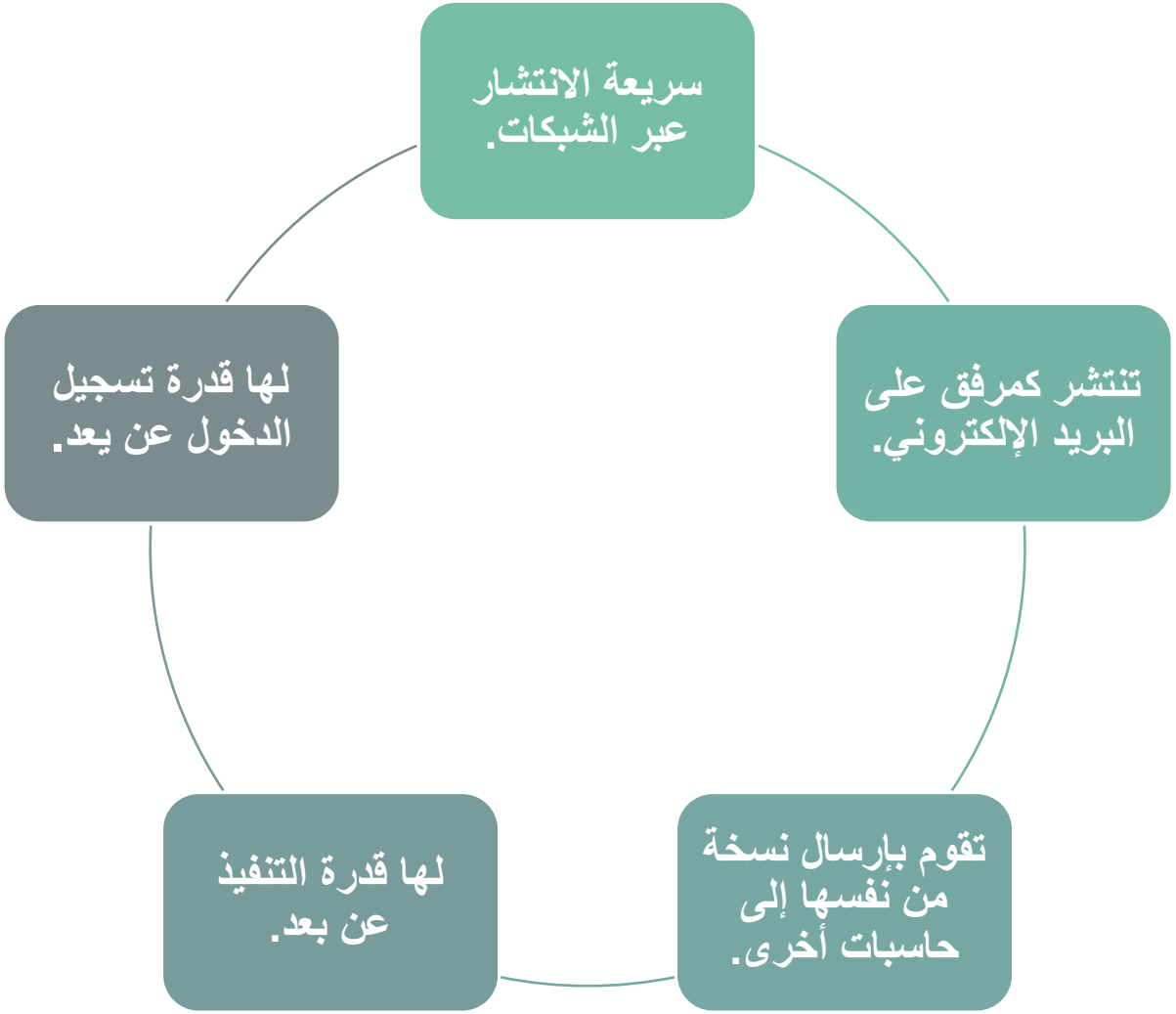


الديدان (Worms)

- هي برامج تعيد إنتاج نفسها لكن لا تلوث برامج أخرى، وصُنعت لغرض تخريبي أو سرقة بيانات من أجهزة الحاسب أثناء الاتصال بالإنترنت ، وهي سريعة الانتشار ويصعب التخلّص منها ، ومن أنواعها :

ديدان البريد	ديدان برامج مشاركة الملفات	ديدان الانترنت
• وتكون مرفقة في محتوى الرسالة وأغلب الأنواع من هذه الديدان تتطلب من المستخدم أن يقوم بفتح الملف المرفق لكي تصيب الجهاز	• وتنتشر عن طريق وضع نفسها في مجلدات المشاركة حتى تنتشر بين الحاسبات الأخرى	• وتقوم بالانتقال عن طريق بروتوكول TCP/IP

خصائص الديدان :



الفيروسات (Virus)

- الفيروس هو عبارة عن برنامج صغير تتم برمجته بغرض إلحاق الضرر بجهاز الحاسب. والانتقال من جهاز حاسب إلى آخر وأيضاً يقوم بنسخ نفسه داخل الجهاز

ويتداخل مع نظام التشغيل الخاص بالحاسب. وتتم برمجتها بواسطة مبرمجين محترفين لإلحاق الخراب والضرر بأجهزة الحواسيب ، أو لتحقيق مكاسب مالية.

حصان طروادة (Trojan Horse)

- هو جزء من برنامج مخفي عن قصد داخل مقطع برنامج مرغوب فيه وعندما يشغل المستخدم أحد هذه البرامج ينشط حصان طروادة ويقوم بعمل معين هو مصمم من أجله

تشترك أحصنة طروادة في الخصائص التالية :

- لديها القدرة على الاختفاء .
- يعمل على بُعد لسرقة البيانات .
- لديها احتيالات قوية ومهارة غير معلنة للاحتيال .
- الاتصال التلقائي لأجهزة الحاسب عبر الشبكة .
- لديه القدرة على الإصلاح الذاتي .

عناصر أمن المعلومات :

السرية

تعني ضمان وصول المعلومات على نظام الحاسب للمستخدمين المصرح

التكاملية وسلامة المحتوى

تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله

استمرارية توافر المعلومات

تعني توافر النظام المعلوماتي للمستخدمين المصرح لهم

حماية أجهزة الحاسبات وشبكات الحاسب

حماية الحاسب :

حماية الحاسب هي :
مجموعة من الإجراءات لحماية بيانات الحاسب والمعدات ، وتشمل الحماية:

- استخدام كلمة مرور قوية
- استخدام الجدار الناري.
- استخدام برامج الحماية من الفيروسات.
- تثبيت برامج مكافحة الفيروسات.
- تحديث برنامج مكافحة الفيروسات بشكل يومي.
- تشغيل برنامج مكافحة الفيروسات بشكل يومي.
- يجب العمل على تحديث نظام التشغيل باستمرار.
- يجب أخذ نسخة احتياطية من الملفات .

حماية شبكة الانترنت :

حماية شبكة الإنترنت: مجموعة من الإجراءات لحماية بيانات داخل شبكة الإنترنت وتشمل:

- استخدام الشبكات الآمنة.
- استخدام المواقع الموثوقة.
- تأمين الشبكة: يجب التأكد من أن كلمة المرور قوية .
- تجنب المواقع الإلكترونية التي توفر المواد المقرصنة.

الحافظ على المعلومات الشخصية آمنة.

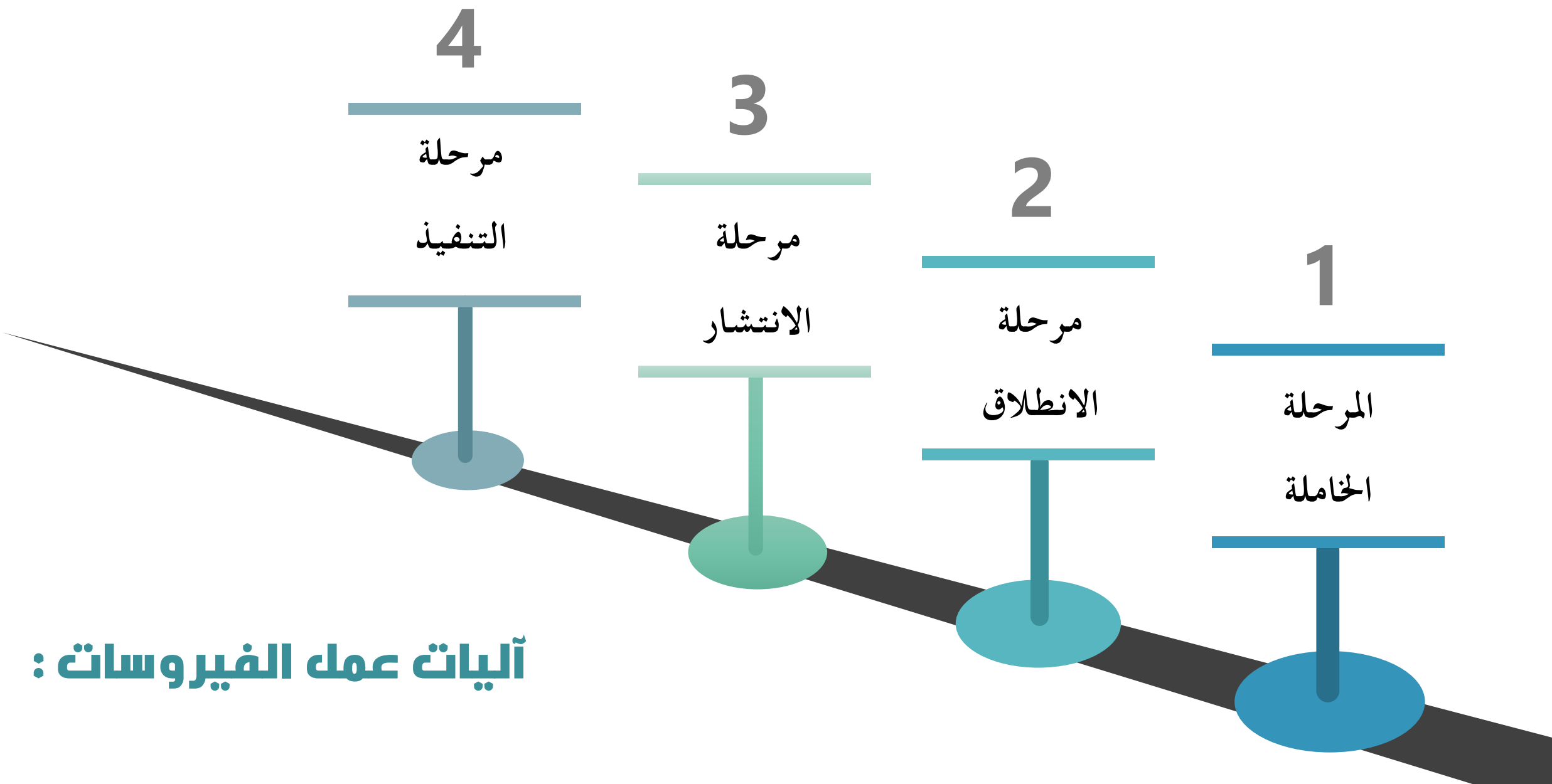
- عدم استخدام شبكة (Wi-Fi) مفتوحة: لا تستخدم شبكة واي فاي مفتوحة يمكن لشخص ضار الدخول إلى بيانات عبر الجهاز.

تنقسم الحماية الشخصية على شبكة الانترنت إلى قسمين

السلامة

الأمن

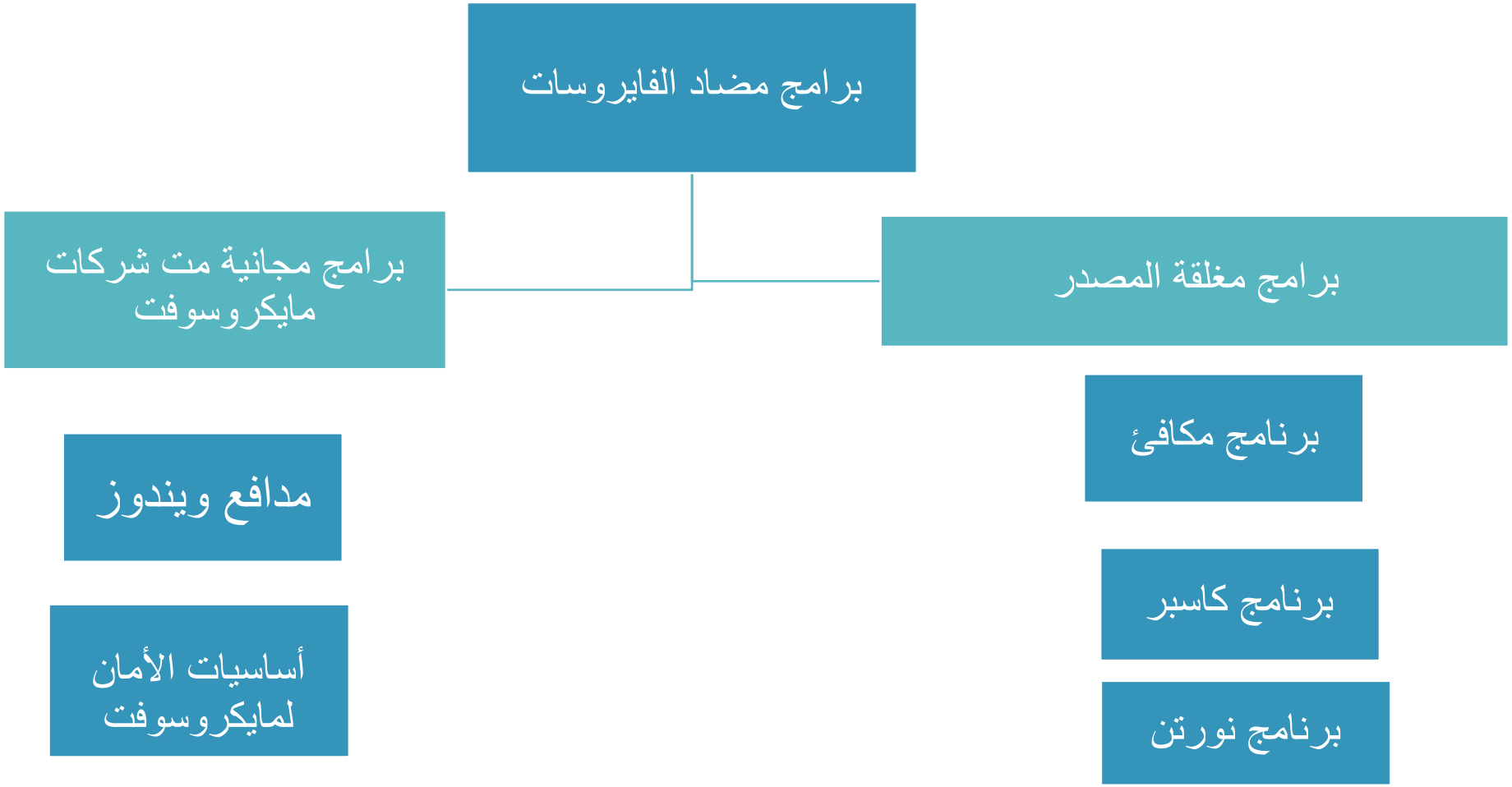
آليات عمل الفيروسات :



تصنيف الفيروسات :

- على حسب الهدف
  - على حسب استراتيجية الإخفاء
  - من حيث حجم الضرر
- من حيث سرعة الانتشار
  - من حيث توقيت النشاط
  - من حيث مكان الإصابة

أنواع الفيروسات :



تصنيف الفايروسات حسب الهدف :

تُصنف الفيروسات حسب الهدف إلى ثلاثة أنواع :

١- فيروسات تصيب الملفات التنفيذية :

هو فايروس يقوم بإلحاق نفسه كملف في أي برنامج تنفيذي ، وينتشر عبر الأقراص أو عبر الشبكة .

٢- فيروسات قطاع التشغيل :

هي فايروسات تصيب برنامج الإقلاع الأساسي على القرص وإتلاف محتوياته

٣-فيروسات الماكرو :

هي فايروسات تصيب البرامج التطبيقية مثل ماكرو معالجة النصوص وماكرو اكسل .

هجمات حجب الخدمة :

هجمات الحرمان من الخدمة هي كأسلوب ليست حديثة ، ولكن الإنترنت جعلتها فتاكة ، وهي تعني أن مجموعة من أجهزة الحاسب تقوم بمهاجمة خادم واحد بمجموعة كبيرة جداً من الأوامر التي تفوق قدرة الجهاز الخادم على المعالجة بهدف حجب الخدمة عنه .

وللحماية من هجمات الحرمان من الخدمة استخدام نظام (Dos.deny) هو نظام مخصص لاكتشاف هجمات الحرمان من الخدمة DDOS والتصدي لها ومنعها من التأثير على أداء الخادمات أو المواقع التي تستعمل هذا النظام .

تصنيف الفايروسات حسب استراتيجية الإخفاء :

١- الفيروسات المشفرة (Encrypted Virus): فيروس يستخدم التشفير لإخفاء نفسه من برامج مضاد الفيروسات. وتعمل الفيروسات المشفرة على إنشاء مفتاح تشفير عشوائي ليصعب الكشف عنه عن طريق برنامج مكافحة الفيروسات .

٢- الفيروسات الخفية (Stealth Virus): هي مصممة لإخفاء نفسها من برامج مكافحة الفيروسات وتعمل على استراتيجية لإخفاء نفسها في الملفات حيث تعرض نسخة نظيفة عند فحص الملفات وتعمل على تغيير خصائص الملف المخفى.

٣- الفيروسات المتعددة الأشكال (Polymorpic Virus): هو فيروس يصعب الكشف عنه بسبب تحوله مع كل إصابة ، ويعمل على استراتيجية استخدام التشفير للحفاظ على نفسه .

٤-الفيروسات المتحولة (Metamorphic Virus): يتحول ويقوم بإعادة كتابة نفسه عند كل عملية تكرار؛ مما يزيد من صعوبة الكشف عنه ويعمل على استراتيجية تعمل على تغيير برمجته وإعادة تجميع نفسه في شكل قابل للتنفيذ .

طرق انتقال الفيروسات وأعراض الإصابة بها :

١- فيروس العدوى المباشر (Direct Infector):
عندما يتم تنفيذ برنامج أو ملف مصاب بفيروس من هذا النوع ، فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه ، وعندما يصاب أحد الملفات بالعدوى فإنه يقوم بتحميله إلى الذاكرة وتشغيله .

٢- فيروس العدوى غير المباشر (Indirect Infector): عندما يتم تنفيذ برنامج مصاب أو ملف بفيروس من هذا النوع ، فإن ذلك الفيروس سينتقل إلى ذاكرة الحاسوب ويستقر فيها ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله إلى الذاكرة بعد ذلك إلى أن يتم قطع التيار الكهربي عن الحاسوب وإعادة تشغيله.

من أهم طرق الاصابة بالفيروسات:

- فتح المرفقات من رسائل البريد الإلكتروني غير المعروفة والمصابة بالفيروس.
- تحميل البرامج المجانية من المواقع الضارة.
- الإعلانات المجهولة عبر الإنترنت.
- استخدام وحدات التخزين المتنقلة: تنقل وحدات التخزين مثل القرص المتنقل والأقراص الضوئية الفيروسات إذا أدخلت في جهاز مصاب .

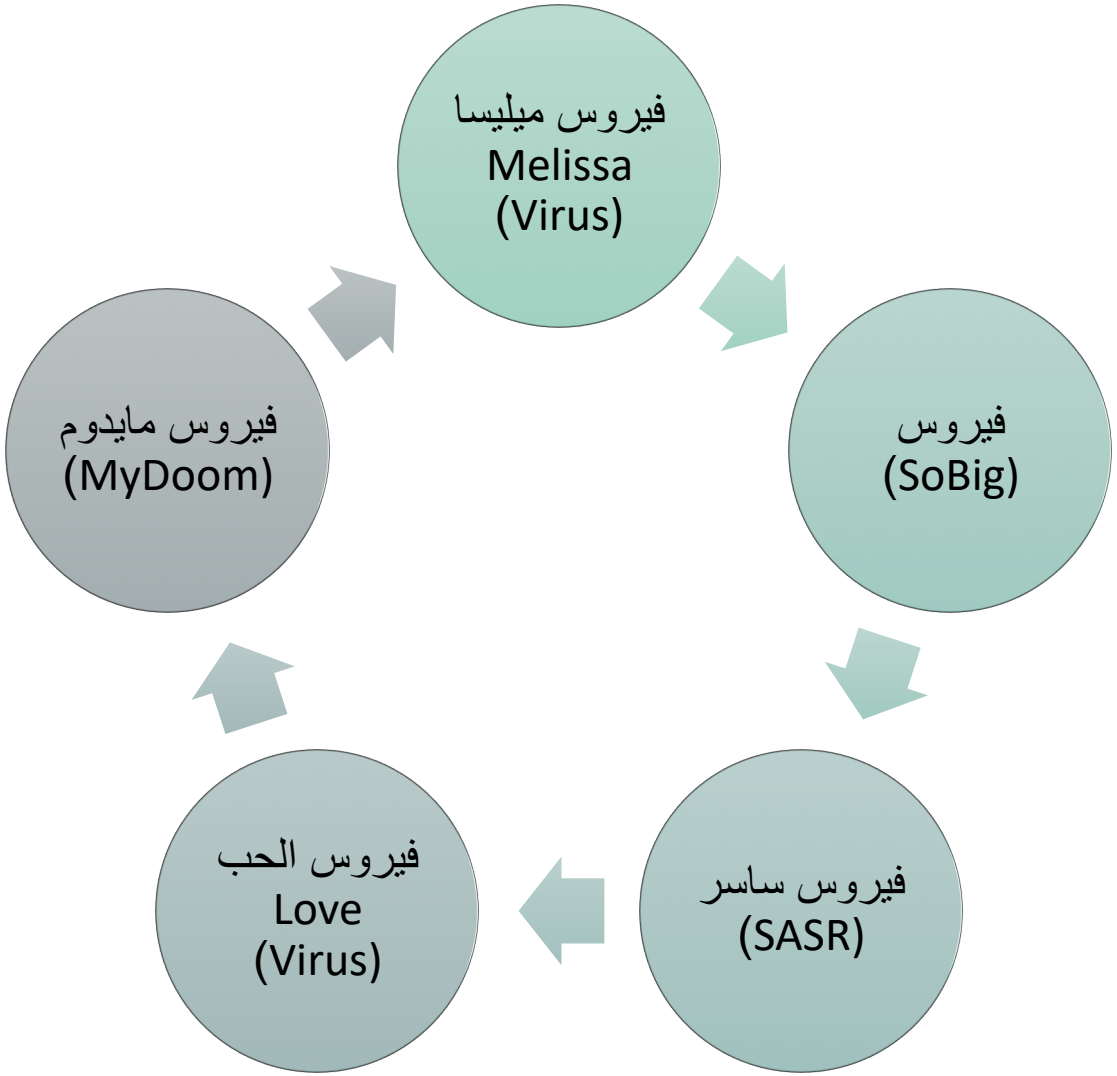
أعراض الإصابة بالفيروسات :

- يبطئ جهاز الحاسب دون أي سبب.
- احتواء نظام الحاسب على ذاكرة متوافرة أقل مما ينبغي .
- إنشاء برامج أو ملفات غير معروفة.
- تتعرض بعص البرامج أو الملفات للفقد.
- تتعرض بعض الملفات للتلف.
- إعادة تشغيل الحاسب بطرق غير معتادة .
- لا تعمل بعض الملفات أو البرامج بشكل صحيح تلقائياً .
- عرض رسائل غريبة وموسيقى أو أصوات .
- تغيير اسم القرص الصلب أو اسم وحدة التخزين .
- عدم القدرة على التعامل مع بعض الوحدات الطرفية .

طرق الوقاية من الفيروسات :

- تثبيت برامج مكافحة الفيروسات.
- الحفاظ على برنامج مكافحة الفيروسات محدثاً بشكل يومي.
- يجب إجراء فحوصات مجدولة بانتظام باستخدام برنامج مكافحة الفيروسات.
- عمل نسخة احتياطية للبيانات المهمة بشكل دوري للاستفادة منها عند إصابة الحاسب وإمكان استرجاعها .
- العمل على تحديث نظام التشغيل .
- عدم استخدام ذاكرة فلاش مصابة .
- استخدام شبكة الإنترنت بشكل مقنن.

أشهر الفيروسات :



آليات عمل مضاد الفيروسات :

- يتم إنشاء فيروس وإطلاقه.
- الفيروس يصيب عدداً قليلاً من أجهزة الحاسبات ، ويتم إرساله إلى شركة مكافحة الفيروسات .
- تقوم شركة مكافحة الفيروسات بتسجيل توقيع من الفيروس .
- تضمن الشركة التوقيع الجديد في قاعدة بياناتها .
- عند إجراء مسح بمضاد الفيروس يكتشف الفيروس ، ويتم تقليل خطر الفيروس .

البرامج المضادة للفيروسات من مايكروسوفت :

هي برامج مجانية من شركة مايكروسوفت وتوفر الحماية للحاسب من الفيروسات وبرامج التجسس والملفات الضارة وتشمل برنامجين :

- أساسيات الأمان لمايكروسوفت الذي يعمل مع إصدار ويندوز فيستا وويندوز 7
- نظام مدافع ويندوز والذي يعمل مع إصدار ويندوز 8 وما فوقه .

أساسيات الأمان لمايكروسوفت :

هو برنامج مضاد للفيروسات مجاناً للأجهزة التي تعمل على نظام تشغيل ويندوز وهو من إنتاج شركة مايكروسوفت ، مهمته حماية جهاز الحاسب من مخاطر الفيروسات والبرمجيات الخبيثة وهجمات الهاكرز.

مميزات برنامج الحماية أساسيات الأمان لمايكروسفت :

- هو برنامج مجاني يتم تحميله من مايكروسوفت مباشرة: سهل الاستخدام ويعمل بكفاءة عالية على نظام التشغيل ويندوز دون توقف؛ للمحافظة على حماية النظام من أي تهديد.
- يوفر فحصاً سريعا لجهاز الحاسب.
- يوفر فحصاً كاملاً لجميع الملفات والبرامج.
- يوفر فحصاً مخصصاً يتضمن الجزء المراد فحصه.
- سريع ويقدم تقارير فورية في حالة وجود خطر على الجهاز.
- تتم عملية التحديث بطريقة تلقائية.

فحص النظام :

يوفر برنامج أساسيات النظام لمايكروسوفت خيارات فحص للحاسب وهي :

الفحص السريع
Quick Scan

- يقوم الفحص السريع بالبحث في الأماكن الموجودة على القرص الصلب بالحاسب والتي تصاب بواسطة البرامج الضارة على الأرجح

الفحص الكامل للجهاز
Full Scan

- يقوم الفحص الكامل بالبحث في جميع الملفات الموجودة على القرص الصلب وفي جميع البرامج المشغلة حالياً. ولكنه قد يتسبب في بطء تشغيل جهاز الحاسب حتى يكتمل الفحص .

الفحص المخصص
Custom Scan

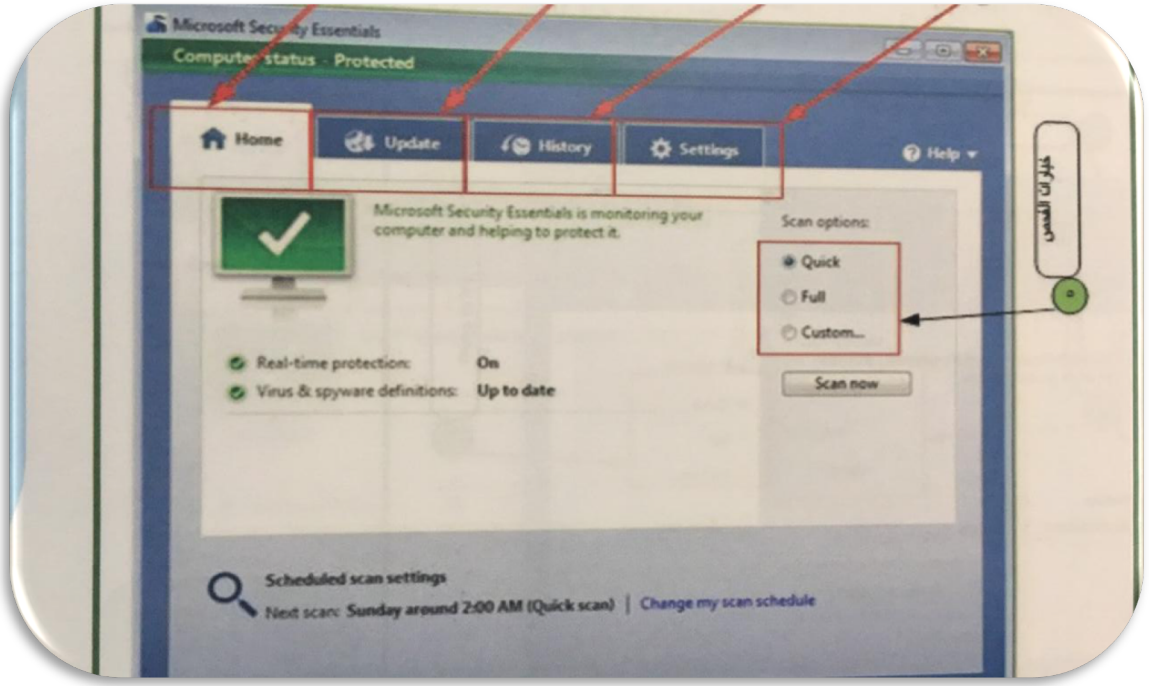
- ويمكننا من خلاله اختيار الجزء من البيانات المطلوب فحصها.

الصفحة الرئيسية في برنامج أساسيات الأمان لمايكروسفت :

تحتوي على رمز الإعدادات للنظام ورمز يوضح تاريخ عمليات الفحص التي أجريت للنظام ، وتحتوي على خيارات البحث وهي بحث سريع أو كامل أو مخصص ، تحتوي على رموز تعرض حالة أمان جهاز الحاسب على شكل رمزاً إما أخضر أو أصفر أو أحمر

الرمز الأخضر :

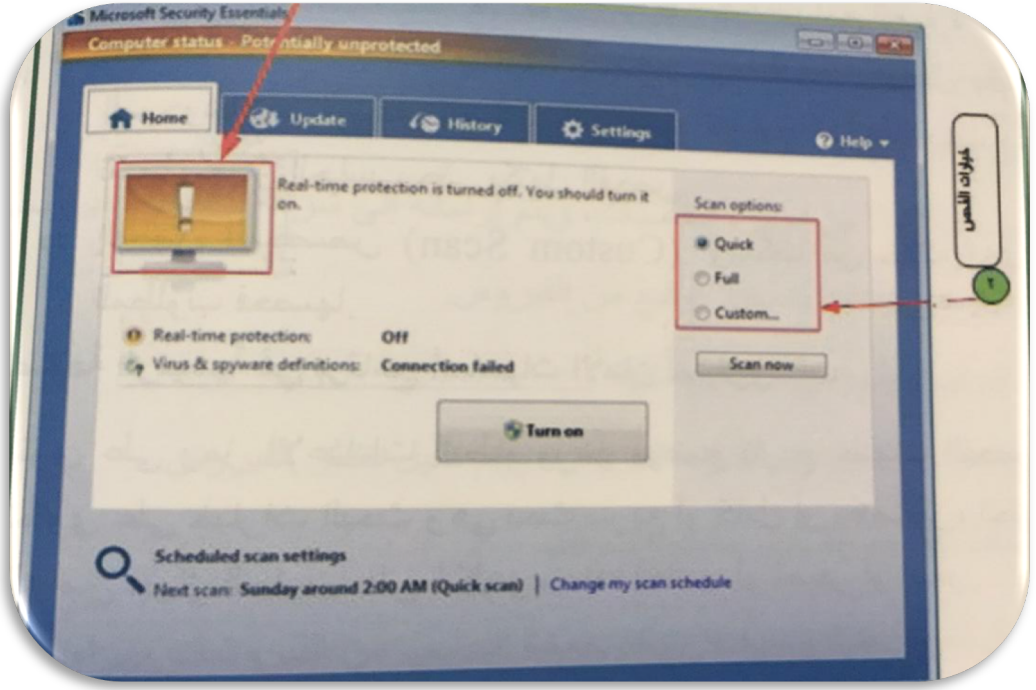
يعني أن حالة أمان الحاسب جيدة ،عندما يواجهِ جهاز الحاسب تهديداً أقل فيتحول من اللون الأخضر إلى اللون الأصفر الشكل 5–6 يوضح أن الرمز الأخضر يعنى أن حالات الأمان جيدة



الشكل 5–6

الرمز الأصفر :

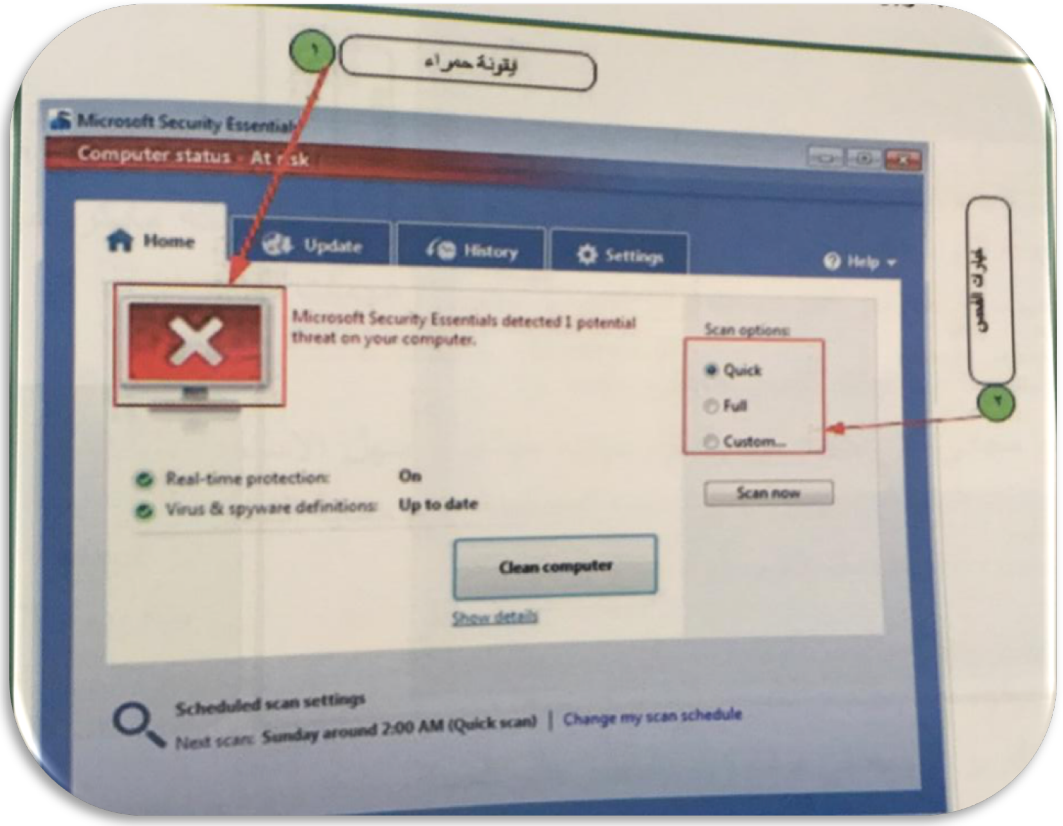
يعني أن الحالة غير محمية وأنه يجب تشغيل الحماية في الوقت الحقيقي أو إجراء فحص النظام سواءٍ سريعاً أو كاملاً أو مخصصاً والشكل 6-6 يوضح الرمز الأصفر ويجب على المستخدم إجراء الفحص عن الفيروسات وإزالتها .



الشكل 6-6

الرمز االأحمر :

يعني أن اجهاز الحاسب في مرحلة خطورة كبيرة وأنه يجب تشغيل البرنامج لإزالة الخطر .



الشكل 6-7

تعريف واستخدام برنامج مدافع ويندوز :

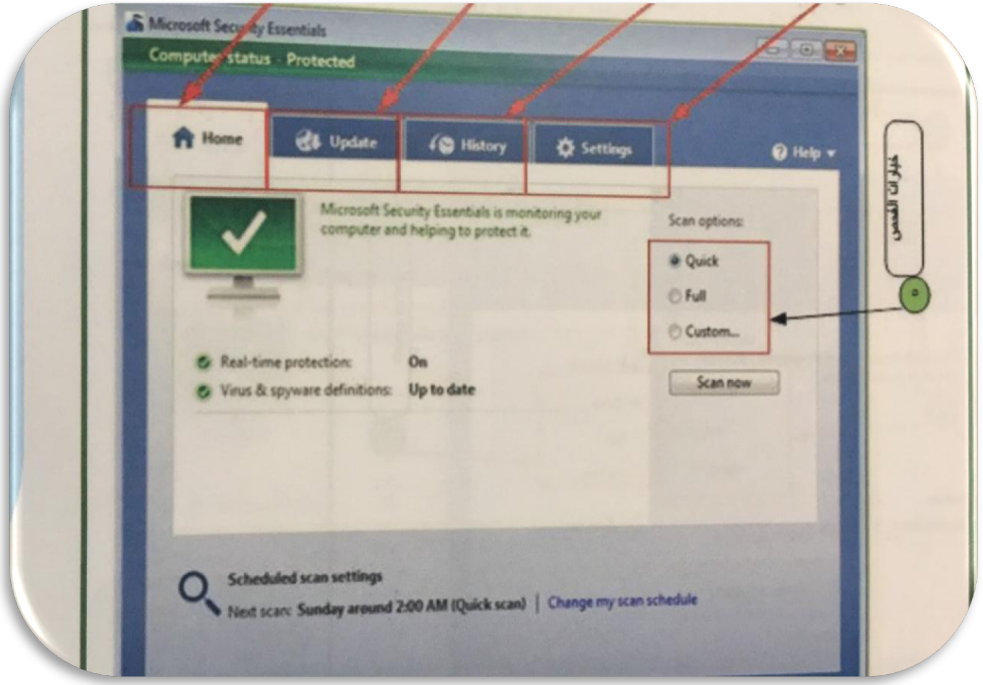
هو بديل لبرنامج أساسيات الأمان لمايكروسفت ويعمل لتحقيق الحماية لأجهزة الحاسب التي تعمل بنظام ويندوز أحدث من ويندوز8؛ فهو يعتبر من البرامج الضرورية والمهمة والذي بدوره يقوم بحماية الملفات والتخلص من البرامج الضارة

مميزات برنامج مدافع ويندوز :

- يوفر تحديثات دورية.
- يوفر حماية كاملة للحاسب من الفيروسات والتجسس.
- يعمل على تنظيف الحاسب من البرامج الضارة والملفات العديمة الفائدة.
- حماية فعالة أثناء تصفح الانترنت .
- واجهة مستخدم سهلة الاستخدام.
- واجهة المستخدم تدعم عدة لغات .
- يتوافق مع جميع إصدارات نظام ويندوز الحديثة من ويندوز 8 وأعلى.
- البرنامج مجاني ومتاح لجميع مستخدمي ويندوز .

الشاشة الرئيسية في برنامج مدافع ويندوز :

- تحتوي الشاشة الرئيسية في برنامج مدافع ويندوز على مجموعة من الرموز توضح حالة أمان جهاز الحاسب على شكل رمز إما أخضر أو أصفر أو أحمر على حسب الحالة :



- يقوم البرنامج للتخلص من الفيروسات بالتالي :

- الخطوة الأولى: فحص الأجهزة (Scan) للكشف عن الفيروسات.

- الخطوة الثنية: إزالة الفيروس والتخلص منه وإذا تعذر ذلك نستخدم أمر إعادة تشكيل الجهاز Format

أمن المعلومات والأمن السيبراني :

- أمن الملومات :
Information Security

هو العلم الذي يبحث في نظريات وأساليب حماية المعلومات والبيانات الرقمية ويُعنى بوضع الإجراءات والتدابير الوقائية اللازمة لضمان سرية وحماية

البيانات والمعلومات من السرقة أو الاختراق.

- الأمن السيراني:

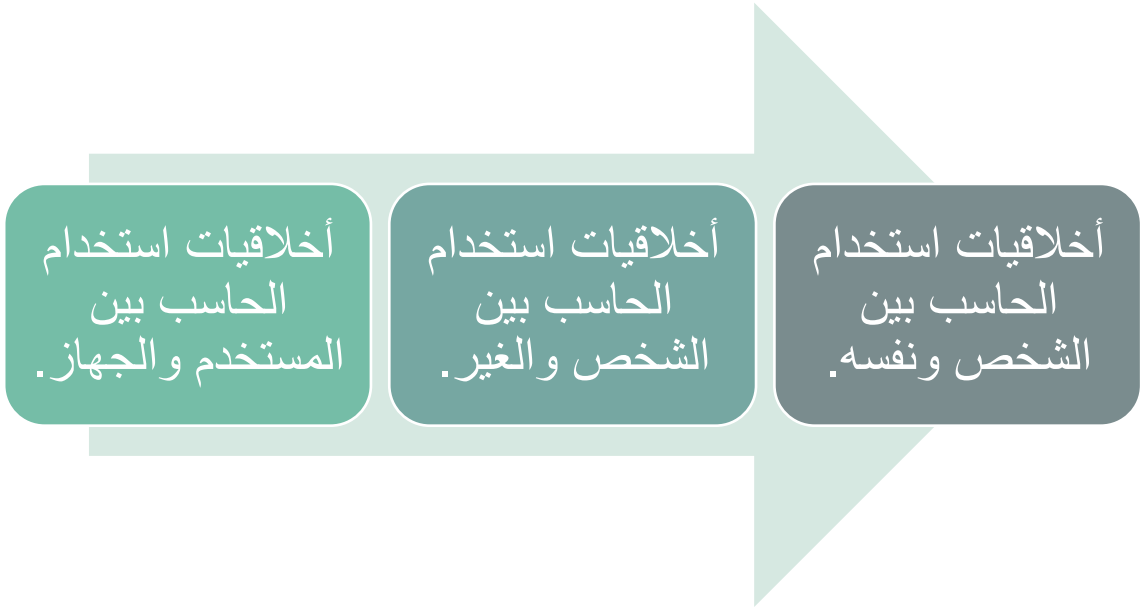
Cyber Security

- هو العلم الذي يُعنى بالفضاء المعلوماتي ، ويستخدم الوسائل التقنية والإدارية لمنع الاستخدام الغير مصرح به للبيانات الرقمية والمعلومات .

أخلاقيات استخدام الحاسب :

تعرف أخلاقيات الحاسب بأسلوب التعامل مع الحاسب وتهتم بالجانب الأخلاقي والقانوني. ويستخدم أخلاقيات الحاسب لوصف المبادئ الأخلاقية التي تنظم عملية استخدام الحاسب والتي تشمل القضايا الأخلاقية مثل حقوق الملكية الفكرية (حق المؤلف؛ وحق النسخ؛ براءة الاختراع) التي تواجه مجتمع اليوم القائم على الحاسب والمعلومات.

وأخلاقيات العمل على استخدام الحاسب عديدة ومتنوعة ، ويمكن ذكر ثلاثة أمور رئيسية يجب على مستخدم الحاسب معرفتها أثناء التعامل معه؛ ومنها:



الوصايا لأخلاقيات استخدام الحاسب والانترنت :

- هناك العديد من الأخلاقيات يجب على مستخدم الحاسب التحلي بها :
- لا يجوز استخدام جهاز الحاسب لإيذاء الآخرين.
- لا يجوز التجسس على بيانات الأشخاص الآخرين.
- لا يجوز استخدام جهاز الحاسب لتنفيذ عمليات للسرقة والاحتيال.
- لا يجوز استخدام جهاز الحاسب بغرض التزوير في الوثائق أو البيانات.
- لا يجوز استخدام موارد الحاسب الخاصة بالأشخاص الآخرين دون إذن أو ترخيص منهم.
- يجب استخدام جهاز الحاسب بطرق تظهر الاهتمام واحترام خصوصية الآخرين.
- الالتزام بالسرية والتعهدات والاتفاقيات وقوانين العمل.
- لا يجوز نسخ برمجيات الآخرين واستخدام ملفاتهم دون موافقة أو دون دفع ثمن هذه البرامج إلا إذا كانت مجانية.
- لا يجوز استخدام الإنترنت في إرسال الرسائل الملغومة لإيذاء الآخرين والتدخل في ملفاتهم وتعطيل أجهزتهم.