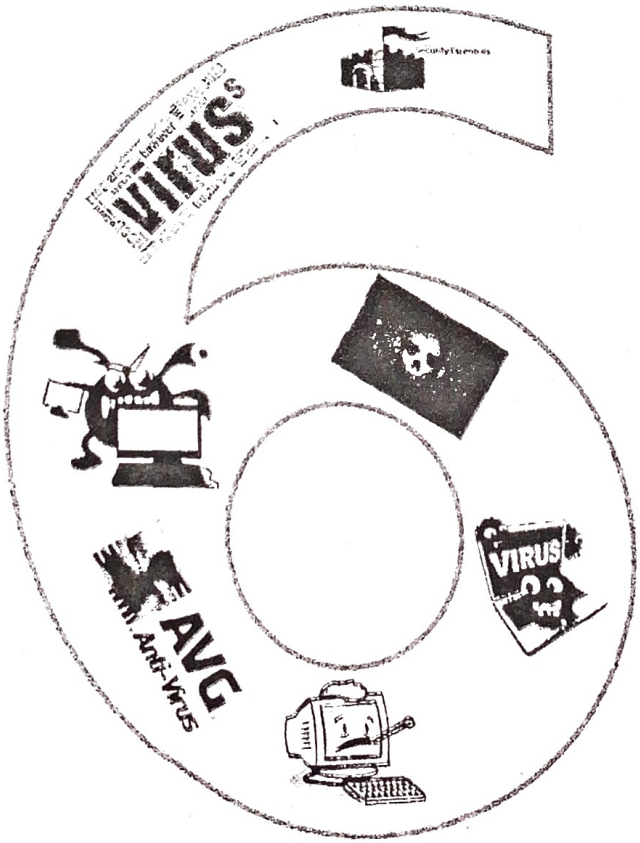
الفصل السادس

فيروسات الحاسب



فيروسات الحاسب

الأهداف

- **الأهداف الرئيسية:**

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

- **الأهداف الفرعية:**

يتوقع من الطالب بعد دراسة هذا الفصل أن يتقن المعارف والمهارات التالية:

- يتعرف على أنواع المخاطر المختلفة التي تهدد الحاسب والبيانات
- يتعرف على فيروسات الحاسب ويُعدِّد أنواعها.
- يتعرف على طرق حماية البيانات على الحاسب والشبكات.
- يتعرف على آليات عمل الفيروسات.
- يصنف أنواع الفيروسات المختلفة.
- يتعرف على طرق الإصابة بالفيروسات.
- يتعرف على أشهر الفيروسات.
- يتعرف على طرق الوقاية من الفيروسات وكيفية التخلص منها.
- يتعرف على أخلاقيات استخدام الحاسب لحماية البيانات.

فيروسات الحاسب	Computer Viruses
الاختراق	Penetration
المخترقون	Hackers
برامج الحاسب الخبيثة	Malware
الكراكرز	Crackers
الديدان	Worms
حصان طروادة	Trojan Horse
برامج التجسس	Spyware
البرامج المضادة للفيروسات	Antivirus
أساسيات الأمان من مايكروسفت	Microsoft Security Essentials
مدافع ويندوز	Windows Defender
حماية البيانات	Data Security
جدار الحماية	Firewall
الفحص السريع	Quick Scan
الفحص الكامل	Full Scan
الفحص المخصص	Custom Scan

6-1 مقدمة في فيروسات الحاسب

في الآونة الأخيرة مع تطور الحاسبات والشبكات كثرت المخاطر التي تهدد الحاسب. ومن أنواع تلك المخاطر البرامج الخبيثة وفيروسات الحاسب (Computer Viruses). والفيروس هو برنامج تم تطويره من قبل مبرمجين، والغرض منه إلحاق الضرر بالحاسب أو السيطرة عليه. وتتنوع الأضرار التي تصيب الحاسب؛ فمنها ما يدمر الحاسب بإلحاق الضرر بالقرص الصلب، ومنها ما يتلف جزءاً من 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.

وسمي فيروسات الحاسب بهذا الاسم لأنها تشبه الفيروسات الحيوية، وهي الكائنات الدقيقة التي تنقل الأمراض للإنسان، في صفات منها:

- فيروسات دائماً تختفي خلف ملف آخر، وعندما يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس.
- الفيروسات توجد في مكان أساسي في الحاسب مثل قطاع تشغيل القرص والذاكرة، وتصيب أي ملف يُشغَّل في أثناء وجودها بالقرص الصلب أو الذاكرة مما يزيد عدد الملفات المصابة.
- في بعض الأحيان يقوم الفيروس الحيوي وفيروس الحاسب بتغيير شكليهما حتى يصعب اكتشافهما والتغلب عليهما.

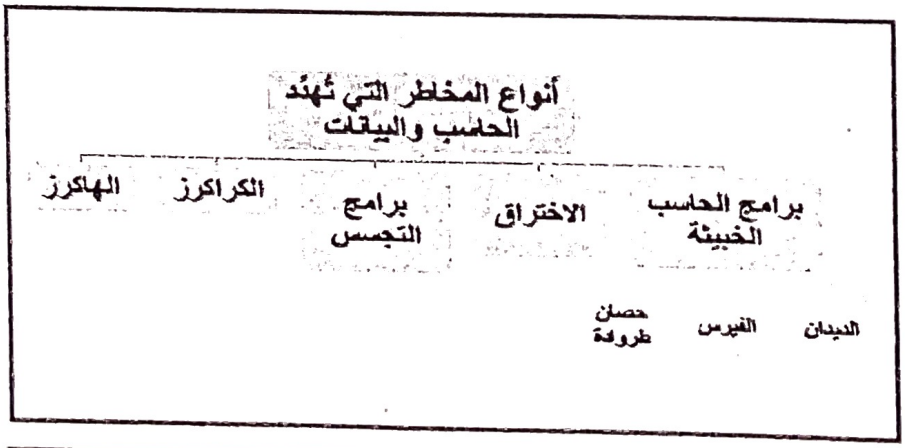
مهارة 6- 1

- **التعرف على أنواع المخاطر التي تهدد الحاسب والبيانات.**

6-2 أنواع المخاطر التي تهدد الحاسب والبيانات

يكاد لا يخلو حاسب على شبكة الإنترنت من التهديدات والمخاطر التي يتعرض لها، ومن تلك المخاطر الاختراق، برامج التجسس، الهاكرز والكراكرز، والبرامج الخبيثة.

والخطر هو تهديد للمعلومات داخل الحاسب بوجود ثغرة أمنية. والشكل 6-1 يوضح أنواع المخاطر التي تهدد الحاسب والبيانات، وسوف نتناول بشيء من التفصيل هذه الأنواع.



شكل 6-1: أنواع المخاطر التي تُهدِّد الحاسب والبيانات

6-2-1 الاختراق

الاختراق (Penetration) هو إمكانية الدخول إلى معلومات ما داخل الحاسب بطريقة غير شرعية. والسبب الرئيسي للاختراق هو استخدام الإنترنت، مع وجود ثغرات في نظام الحماية بالجهاز.

ومن أهم دوافع الاختراق:

- الحصول على المال من خلال سرقة المعلومات البنكية.
- الحصول على معلومات شخصية بغرض 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:

- اختراق الخادمات للشركات أو الجهات الحكومية، وذلك باختراق الجدران النارية التي عادة ما توضع لحمايتها.
- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات.
- التعرض للبيانات أثناء انتقالها والتعرف على شيفرتها إن كانت مشفرة. وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية ATM.

6-2-2 برامج التجسس

برامج التجسس (Spyware) 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.

6-2-3 الهاكرز

الهاكرز (Hackers) هم أشخاص خبراء باختراق الحاسب لكي يصلوا إلى المعلومات المخزنة، وهم متطفلون يتحدَّون أمن نظم الشبكات ولكن لا تتوافر لدى الغالبية العظمى منهم دوافع تخريبية.

6-2-4 الكراكرز

الكراكرز (Crackers) هم أشخاص متخصصون أو خبراء في مجال الحاسب ولكنهم يقومون بأنشطة غير شرعية أو قانونية، مثل عمل برنامج لغرض السرقة، أو عمل برنامج للحصول على المعلومات بطرق غير قانونية.

مهارة 6- 2

- **التعرف على أنواع البرامج الخبيثة وخصائصها.**

6-2-5 برامج الحاسب الخبيثة

برامج الحاسب الخبيثة (Malware) 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 عده أنواع، منها: الفيروسات، والديدان، وأحصنة طراودة. والشكل 6-1 يوضح تلك الأنواع الخبيثة من حيث أنواع البرمجيات الضارة.

1. **الديدان (Worms):** هي برامج تعيد إنتاج نفسها لكن لا تلوث برامج أخرى، وصنعت لغرض تخريبي أو سرقة بيانات من أجهزة الحاسب أثناء الاتصال بالإنترنت، وهي سريعة الانتشار ويصعب التخلص منها.

ومن أنواع الديدان:

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

ومن خصائصها:

- سريعة الانتشار عبر الشبكات.
- تنتشر كمرفق على البريد الإلكتروني.
- تقوم بإرسال نسخة من نفسها إلى حاسبات أخرى.
- لها قدرة التنفيذ عن بعد.
- لها قدرة تسجيل الدخول عن بعد.

2. **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.

3. **حصان طروادة (Trojan Horse):** هو جزء من برنامج مخفي عن قصد داخل مقطع برنامج مرغوب فيه، وعندما يشغل المستخدم أحد هذه البرامج ينشط حصان طرواده ويقوم بعمل معين هو مصمم من أجله ويمكن أن يقوم حصان طروادة بأفعال خبيثة أو حميدة.

وتشترك معظم أحصنة طروادة في الخصائص التالية:

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

مهارة 6- 3

- **التعرف على حماية البيانات (Data Security) والنصائح التي يجب مراعاتها.**

3-6 حماية البيانات

أدى الانتشار السريع للحاسب والإنترنت إلى ظهور الكثير من المشاكل المتعلقة بكيفية حماية البيانات وتأمين الأمن اللازم لها من الفيروسات والبرامج الضارة والمخترقين وغيرها.

والجدير بالذكر أن امتلاك أحدث تقنيات الأمن وحده لا يكفي لتأمين الحماية الشاملة للبرامج والأجهزة والبيانات، بل هنالك مجموعة من الإجراءات الوقائية والأمور التي ينبغي على كل مستخدمي الحاسب معرفتها كي يسلم من الفيروسات والمخترقين.

6-3-1 عناصر أمن المعلومات

المبادئ الأساسية لأمن المعلومات يعتمد أمن المعلومات وحمايتها على مجموعةٍ من المبادئ الأساسية التي لا بد من الالتفات إليها خلال اتخاذ الإجراءات والتدابير اللازمة لحماية المعلومات، وتتمثل عناصر أمن المعلومات في الآتي:

1. **السرية (Secrecy):** تعني ضمان وصول المعلومات على نظام الحاسب للمستخدمين المصرح لهم فقط.
2. **التكاملية وسلامة المحتوى (Integrity):** تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله.
3. **استمرارية توافر المعلومات أو الخدمة (Availability):** تعني توافر النظام المعلوماتي للمستخدمين المصرَّح لهم.
4. **حماية أجهزة الحاسبات وحماية شبكات الحاسبات من المخاطر المحتملة.**

6-3-2 حماية الحاسب

حماية الحاسب هى مجموعة من الإجراءات لحماية بيانات الحاسب والمعدات، وتشمل حماية:

- 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: حفظ نسخة احتياطية من البيانات المهمة إلى قرص خارجي.

6-3-3 حماية شبكة الإنترنت

عندما يتصل الحاسب بالإنترنت، فإنه معرض للخطر. والخطر يشمل سرقة معلومة أو نشر معلومة أو أي كان الضرر. وتنقسم الحماية الشخصية على شبكة الإنترنت إلى قسمين هما:

- السلامة.
- الأمن.

السلامة: هي توفير الحماية لضمان سلامة المستخدم نفسه من الاستغلال أو الابتزاز أو الانتهاك أو الإساءة. أما الأمن فهو توفير الحماية لضمان أمن المعلومات والبيانات والخصوصية الشخصية. وهي بذلك تشمل حماية الملفات والعتاد.

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

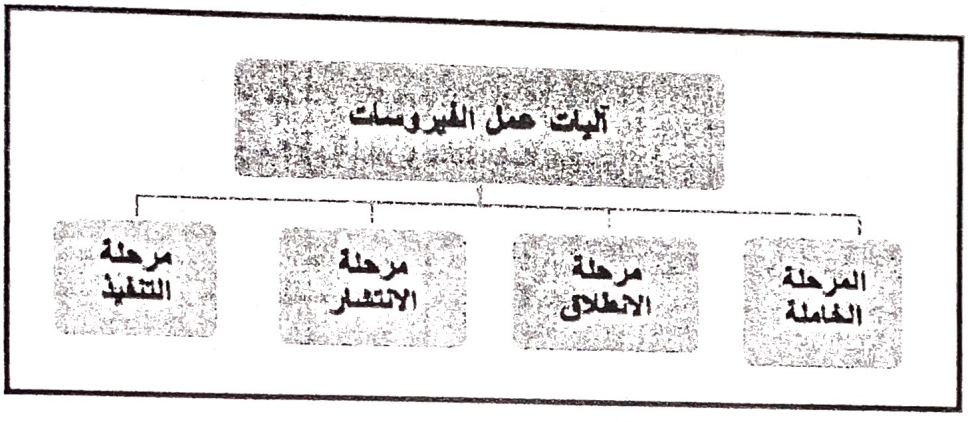
- استخدام الشبكات الآمنة.
- استخدام المواقع الموثوقة.
- تأمين الشبكة: يجب التأكد من أن كلمة المرور قوية.
- تجنب المواقع الإلكترونية التي توفر المواد المقرصنة.
- الحافظ على المعلومات الشخصية آمنة.
- عدم استخدام شبكة (Wi-Fi) مفتوحة: لا تستخدم شبكة واي فاي مفتوحة يمكن لشخص ضار الدخول إلى بيانات عبر الجهاز.

مهارة 6- 4

- **التعرف على آليات عمل الفيروسات.**

4-6 آليات عمل الفيروسات

تقسم آلية عمل الفيروسات إلى أربع مراحل أساسية هي: المرحلة الخاملة، ومرحلة الانطلاق، ومرحلة الانتشار، ومرحلة التنفيذ. والشكل 6-2 يوضح آليات عمل الفيروسات تلك.



شكل 6-2: آليات عمل الفيروسات

بعد أن يتمكن برنامج الفيروس من إصابة جهازٍ ما فإنه يدخل في المرحلة الخاملة (dormant phase) التي يكون فيها الفيروس خاملاً، ولكن ليس كل الفيروسات لديها هذه المرحلة.

ثم إذا توافرت شروط محددة مثل زمن محدد أو تشغيل تطبيق محدد يبدأ الفيروس في مرحلة الانطلاق (triggering phase) حيث يقوم الفيروس مختفياً في برنامج آخر وينشط معه، لأداء الوظيفة التي صنع من أجلها.

معظم الفيروسات تمر بمرحلة كُمون بعد العدوى مباشرة؛ بحيث لا يظهر التلف على البرامج التي تمت إصابتها جديداً؛ مما يتيح للفيروس الوقت اللازم لنسخ نفسه دون ملاحظته.

ثم تأتي مرحلة الانتشار (propagation phase) حيث ينطلق الفيروس ويضيف شفرته إلى البرنامج الأصلي ويعدل تعليماته بحيث ينتقل التنفيذ إلى شفرة الفيروس عند تشغيل الملف التنفيذي المصاب، وعند هذه المرحلة يكون الفيروس نشطاً والجهاز مصاباً. يصبح البرنامج المصاب مصدراً للعدوى ويصيب بدوره غيره من البرامج.

في مرحلة التنفيذ (execution phase) يتم انتشار الفيروس عبر ملفات ونظام الحاسب.

مهارة 6-5

- **تصنيف الفيروسات على حسب الهدف أو استراتيجية الاخفاء.**

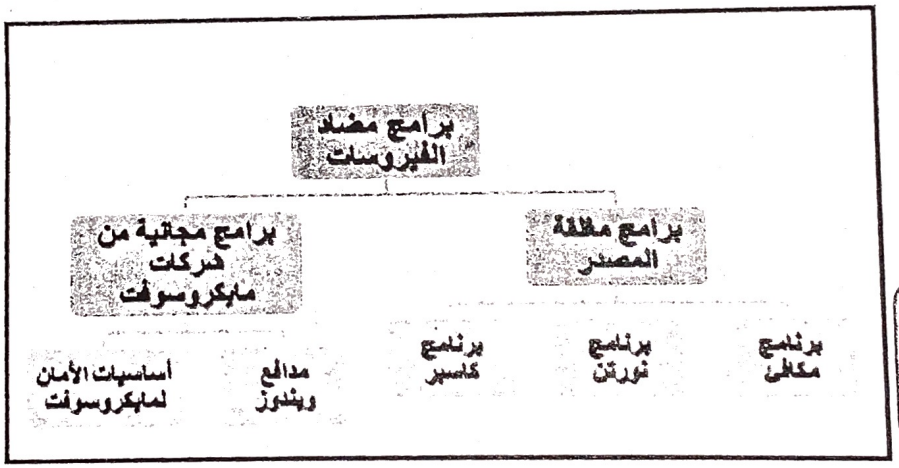
5-6 تصنيف الفيروسات

تصنف الفيروسات إلى عدة تصنيفات، منها:

- من حيث سرعة الانتشار: هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار.

- من حيث توقيت النشاط: هناك فيروسات تنشط في أوقات محدّدة وفيروسات دائمة النشاط.
- من حيث مكان الإصابة: فيروسات تصيب جزءاً معيناً من الحاسب مثل فيروس قطاع التشغيل.
- من حيث حجم الضرر: هناك الفيروسات المدمرة للأجهزة مثل أن يؤذي الفيروس ذاكرة الوصول العشوائي في الحاسب.
- وهناك فيروسات عديمة الضرر وهي التي لا تقوم بأي عمل مؤذٍ.
- أو على حسب الهدف: وهي مجموعة متنوعة من الفيروسات لكل منها خصائص وسمات محددة، مثل فيروسات الماكرو التي تختص بإصابة المستندات في حزمة مايكروسوفت أوفيس.
- أو على حسب استراتيجية الاخفاء: مثل الفيروسات المشفرة.
- وتصنف أيضا بشكل عام إلى صنفين على حسب الهدف أو استراتيجية الإخفاء: إلى مجموعة متنوعة من الفيروسات لكل منها خصائص وسمات محددة.

والشكل 6-3 يوضح تلك الأنواع.



شكل 6-3 : أنواع الفيروسات

6-5-1 تصنيف الفيروسات حسب الهدف

تُصنَّف حسب الهدف إلى ثلاثة أنواع.

1. **فيروسات تصيب الملفات التنفيذية (File infector viruses):** هذا النوع من الفيروسات يلحق نفسه كملف في أي برنامج تنفيذي، يصيب الملف التنفيذي بوحدة التخزين وهو يقوم بإدراج التعليمة البرمجية المصابة في ملف قابل للتنفيذ، وتنتشر عبر الأقراص أو عبر الشبكة.
2. **فيروسات قطاع التشغيل (Boot sector viruses):** هي فيروسات تصيب برنامج الإقلاع الأساسي على القرص (Boot Sector) وإتلاف محتوياته، مما يؤدّي إلى عدم قدرة الحاسب على الإقلاع أو التشغيل، ويعتبر من أخطر الأنواع حيث إنه يؤدى إلى توقف الحاسب عن العمل.
3. **فيروسات الماكرو (Macro viruses):** هي سريعة الانتشار بين المستخدمين خاصة أنه قادر على الانتشار بكل الطرق كالأقراص المتنقلة والمدمجة والبريد الإلكتروني والبرامج المجانية، وهي فيروسات تصيب البرامج التطبيقية مثل ماكرو معالجة النصوص وماكرو الكسل، ويتصف بأشكال عديدة ليتوافق مع كافة الملفات.

4. **هجمات حجب الخدمة (Denial of Service Attacks(DDOS)):** 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.

ومن أنواع هجمات الحرمان من الخدمة:

- الهجمات التي تستغل خطأً برمجياً Bug في بناء TCP/IP
- الهجمات التي تستغل تقصيراً في مواصفات TCP/IP
- الهجمات التي تعيق المرور في شبكتك حتى لا تستطيع أي بيانات أن تصل إليها أو تغادرها.

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.

2-5-6 تصنيف الفيروسات على حسب استراتيجية الإخفاء:

1. **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.
2. **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 المخفي.
3. **الفيروسات المتعددة الأشكال (Polymorphic Virus):** هو فيروس يصعب الكشف عنه بسبب تحوُّله مع كل إصابة، ويعمل على استراتيجية استخدام التشفير للحفاظ على نفسه.
4. **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 برمجيته، وإعادة تجميع نفسه في شكل قابل للتنفيذ.

مهارة 6-6

- **التعرف على طرق انتقال الفيروسات وأعراض الإصابة بها.**

6-6 طرق انتقال الفيروسات وأعراض الإصابة بها

أكثر الفيروسات اليوم تنتقل باستخدام الإنترنت ما لم يتم استخدام أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات، وثانياً وسائط التخزين مثل الأقراص الضوئية والذاكرة المتنقلة وثالثاً ضمن رسائل البريد.

وينتقل فيروس الحاسب وفقاً لطريقة الانتشار إلى نوعين هما: فيروس العدوى المباشر، وفيروس العدوى غير المباشر.

1. **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.
2. **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.

ومن أهم طرق الإصابة 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.

مهارة 6-7

- **تعداد أعراض الإصابة بالفيروسات.**

6-7 أعراض الإصابة بالفيروسات

عند تشغيل البرنامج المصاب بالفيروسات فإنه قد يصيب باقي الملفات الموجودة معه في جهاز الحاسب، ويحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر، بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من القرص المتنقل أو الإقراص المدمجة أو عبر البريد الإلكتروني أو الإنترنت.

الأعراض الأكثر شيوعاً للإصابة بفيروس الحاسب هي:

- يبطئ جهاز الحاسب دون أي سبب.
- احتواء نظام الحاسب على ذاكرة متوافرة أقل مما ينبغي.
- إنشاء برامج أو ملفات غير معروفة.
- تتعرض بعض 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 مثل مشغل الأقراص والطابعات.

- انهيار النظام بالكامل وعدم قدرة الجهاز على العمل.

مهارة 6-8

- **التعرف على طرق الوقاية من الفيروسات.**

6-8 طرق الوقاية من الفيروسات

لوقاية الحاسب من خطر الإصابة بالفيروسات يجب اتباع الخطوات التالية:

1. تثبيت برامج مكافحة الفيروسات.
2. الحفاظ على برنامج مكافحة الفيروسات محدَّثاً بشكل يومي.
3. يجب إجراء فحوصات مُجدْوَلة بانتظام باستخدام برنامج مكافحة الفيروسات.
4. عمل نسخة احتياطية للبيانات المهمة بشكل دوري للاستفادة منها عند إصابة الحاسب وإمكان استرجاعها.
5. العمل على تحديث نظام التشغيل.
6. عدم استخدام ذاكرة فلاش مصابة.
7. استخدام شبكة الإنترنت بشكل مقنن.

6-9 أشهر الفيروسات

بدأ ظهور الفيروسات في منتصف الثمانينات من القرن الماضي، ومنذ ذلك الوقت تطورت وبدأت الانتشار بكثرة. وفى نهاية عقد التسعينيات وصل عدد الفيروسات الشهيرة منها إلى آلاف الفيروسات وهي في ازدياد كل يوم، ومن أشهر الفيروسات التي انتشرت بسرعة:

1. **فيروس ميليسا (Melissa Virus)**

هو أول فيرس ينتقل عبر البريد الإلكتروني، وكان هذا الأمر مخيفاً جداً؛ حيث كان الاعتقاد السائد في ذلك الوقت بأن الفيروسات لا يمكنها التأثير على الجهاز إلا إذا قام مستخدمه بفتح أحد الملفات التي تحمل الفيروس والملحقة برسالة على البريد الإلكتروني.

وهي من أسرع الفيروسات التي انتشرت في عام 1999 وهي من نوع ماكر وفيروس متخصص في إصابة البريد الإلكتروني، وهي تنتشر عن طريق الالتصاق في برامج النصوص كملحق في رسالة البريد الإلكتروني، وبمجرد أن يقوم المستخدم بفتح الملف الملحق بالرسالة يبدأ الفيروس بالعمل؛ حيث يستطيع الوصول إلى قائمة المراسلة الخاصة بالمستخدم ليقوم بإرسال نفس الرسالة إلى أول خمسين عنواناً دون علمك، وتستمر في الانتشار.

2. **فيروس (SoBig)**

عبارة عن رسالة إلكترونية مجهولة المصدر تعطل أجهزة الحاسوب عند فتحها. وقد عطَّل هذا الفيروس مجلة نيوزويك حين ظهوره عام 2003.

3. **فيروس ساسر (SASR)**

أصاب الفيروس ساسر في مايو 2004 أجهزة الحاسوب في العالم بنسبة 3.17% التي تعمل بنظام تشغيل ويندوز، وذلك من خلال الإنترنت. ويسبب هذا الفيروس تأخيراً في تنفيذ الأوامر التي تعطى للجهاز، كما يعمد إلى إغلاق الجهاز وإعادة فتحه.

4. **فيروس الحب (Love Virus)**

دودة حاسوبية مدمّرة سريعة الانتشار ضربت أجهزة الحاسوب في عام 2000 مستغلة ثغرة في نظام ويندوز وضعف نظام البريد الإلكتروني. ولكنه متخصص في إصابة برنامج مايكروسوفت أوت لوك لإدارة البريد الإلكتروني، ويُعرف بسرعة انتشاره.

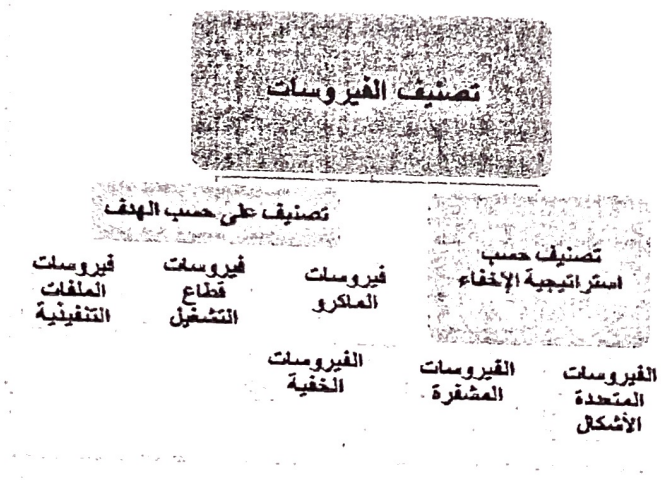
5. **فيروس مايدوم (MyDoom)**

نوع من الفيروس الذي يلحق برسالة البريد الإلكتروني كملف نصي، ويقوم بإعادة إرسال نفسه لعناوين إلكترونية أخرى، كما ينتشر من خلال ملفات الموسيقى والأفلام والألعاب عبر الإنترنت.

ويقوم الفيروس بإدخال برنامج يسمح للهاكرز المتطفلين والقراصنة بالدخول إلى جهاز الحاسب وتسجيل كل ما تمت طباعته ابتداء من كلمة السر إلى أرقام بطاقات الائتمان، وقد أصاب هذا الفيروس ملايين أجهزة الحاسب عند ظهوره عام 2004.

10-6 برامج مضاد الفيروسات

يوجد العديد من برامج مضاد أو مكافحة الفيروسات، التي يمكن استخدامها لمكافحة الفيروسات والبرمجيات الضارة والدودة وأحصنة طروادة؛ حيث يقوم برنامج مضاد الفيروسات بفحص جهاز الحاسب لمعرفة الفيروسات الجديدة التي أصيب بها، ومن ثم تنظيف هذه الفيروسات بما يكفل عدم إلحاق المزيد من الأذى بالحاسب، وتكون عديمة الفائدة في مواجهة الفيروسات الجديدة إلا إذا تم تحديث البرنامج من موقع الشركة المنتجة له. وتنقسم برامج مكافحة الفيروسات إلى برامج مجانية من شركة مايكروسوفت مثل أساسيات الأمان لمايكروسفت وأمان مايكروسفت، وبرامج مغلقة المصدر (غير مجانية) مثل كاسبر ونورتن ومكافي. وسوف نتطرق إلى البرامج المضادة للفيروسات من مايكروسوفت، الشكل 6-4 يوضح تصنيف تلك البرامج.



شكل 6-4: برامج مضاد الفيروسات

6-10-1 آليات عمل مضاد الفيروسات:

الخطوات التالية توضح آليات عمل مضاد الفيروسات وكيفية التخلص من الفيروسات:

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

6-10-2 البرامج المضادة لفيروسات من مايكروسوفت

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

- أساسيات الأمان لمايكروسفت الذي يعمل مع الإصدار ويندوز فيستا وويندوز7.
- نظام مدافع ويندوز والذي يعمل مع إصدار ويندوز8 وما فوقه.

مهارة 6- 9

- **تعريف واستخدام برنامج Microsoft Security Essentials.**

أولاً: أساسيات الأمان لمايكروسفت

أساسيات الأمان لمايكروسفت (Microsoft Security Essentials) 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.

1. 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 سريعاً لجهاز الحاسب.
- يوفر فحصاً كاملاً لجميع الملفات والبرامج.
- يوفر فحصاً مخصصاً يتضمن الجزء المراد فحصة.
- سريع ويقدم تقارير فورية في حالة وجود خطر على الجهاز.
- تتم عملية التحديث بطريقة تلقائية.

2. فحص النظام

يوفر برنامج أساسيات الأمان لمايكروسفت خيارات فحص للحاسب وهي: الفحص السريع، الفحص الكامل، الفحص المخصص. والشكل 6-6 يوضح خيارات الفحص.

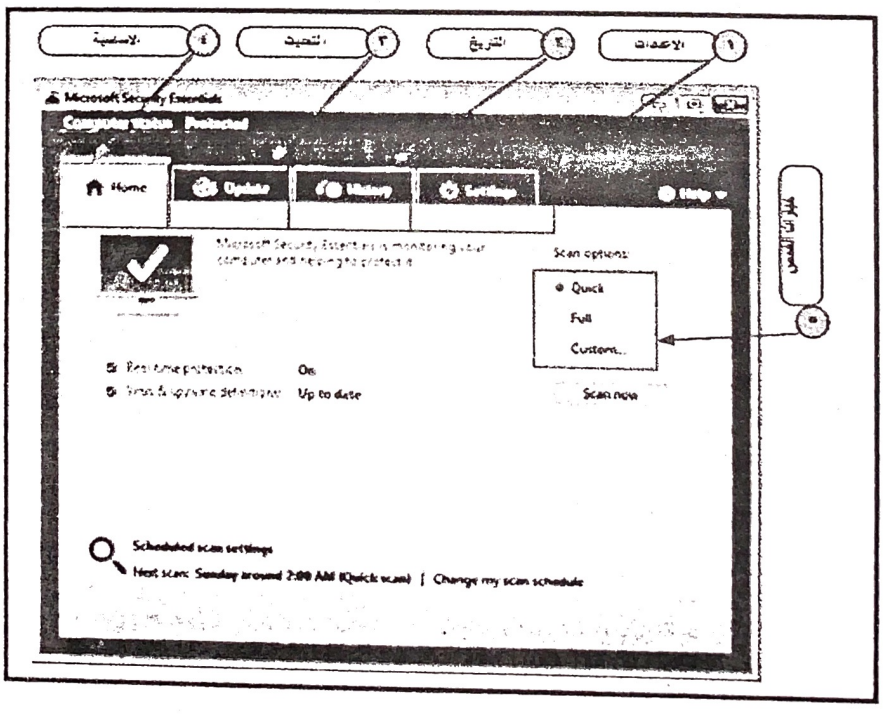
- الفحص السريع (Quick Scan): يقوم الفحص السريع بالبحث في الأماكن الموجودة على القرص الصلب بالحاسب والتي تصاب بواسطة البرامج الضارة على الأرجح.
- الفحص الكامل للجهاز (Full Scan): يقوم الفحص الكامل بالبحث في جميع الملفات الموجودة على القرص الصلب وفي جميع البرامج المشغلة حالياً، ولكنه قد يتسبب في بطء تشغيل جهاز الحاسب حتى يكتمل الفحص.
- الفحص المخصص (Custom Scan): ويمكننا من خلاله اختيار الجزء من البيانات المطلوب فحصها.

3. 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 رمز إما أخضر أو أصفر أو أحمر.

أ. الرمز الأخضر

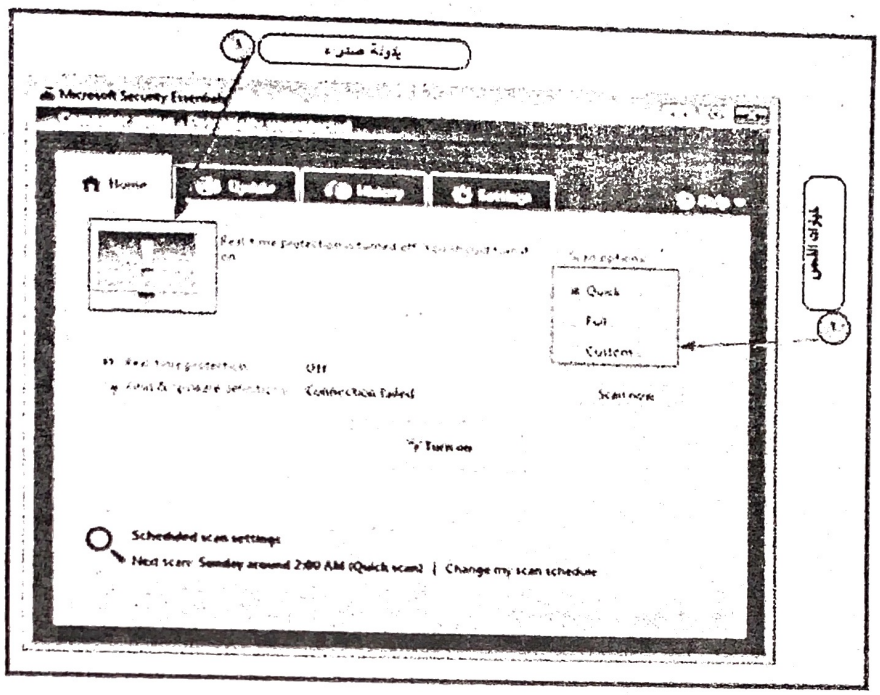
يعني أن حالة أمان الحاسب جيدة، عندما يواجه جهاز الحاسب تهديداً أقل فيتحول من اللون الأخضر إلى اللون الأصفر. الشكل 6-5 يوضح أن الرمز الأخضر يعنى أن حالات الأمان جيدة.



شكل 6-5: الصفحة الأساسية مايكروسوفت سكيورتي

ب. الرمز الأصفر

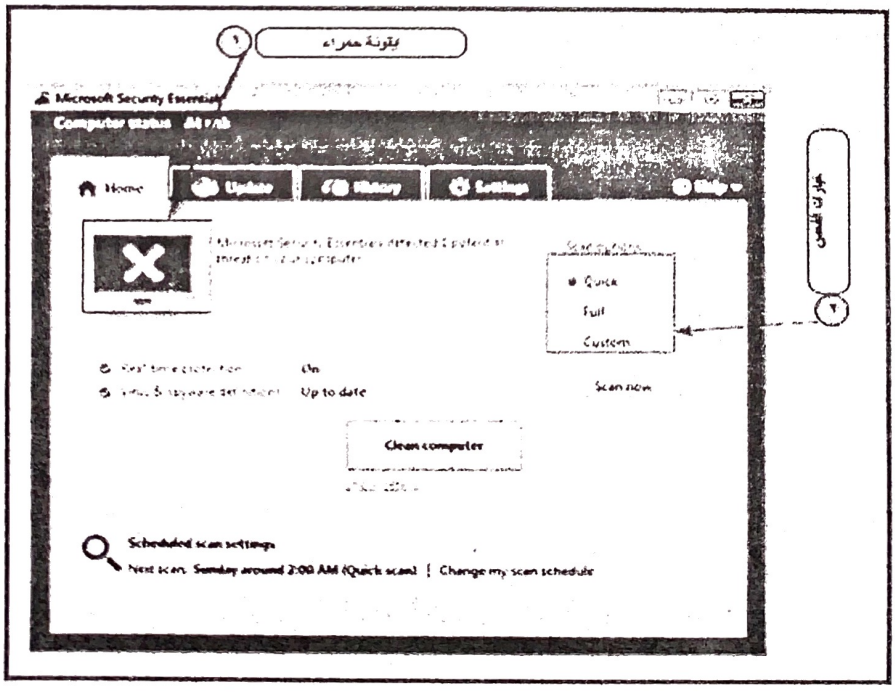
يعني أن الحالة غير محمية وأنه يجب تشغيل الحماية في الوقت الحقيقي أو إجراء فحص النظام سواء سريعاً أو كاملاً أو مخصصاً. والشكل 6-6 يوضح الرمز الأصفر ويجب على المستخدم إجراء الفحص عن الفيروسات وإزالتها.



شكل 6-6:
الحالة غير
محمية فى
مايكروسوفت
سكيورتي

ج. الرمز الأحمر

ظهور اللون الأحمر يعنى أن جهاز الحاسب في مرحلة خطورة كبيرة وأنه يجب تشغيل البرنامج لإزالة الخطر. والشكل 6-7 يوضح الرمز الأحمر يعنى أن الحاسب في خطر كبير ويجب فحص الحاسب وإزالة التهديد.



شكل 6-7:
الحالة في
خطر فى
مايكروسوفت
سكيورتي

مهارة 6- 10

- **تعريف واستخدام برنامج مدافع ويندوز (Windows Defender).**

ثانياً: برنامج مدافع ويندوز

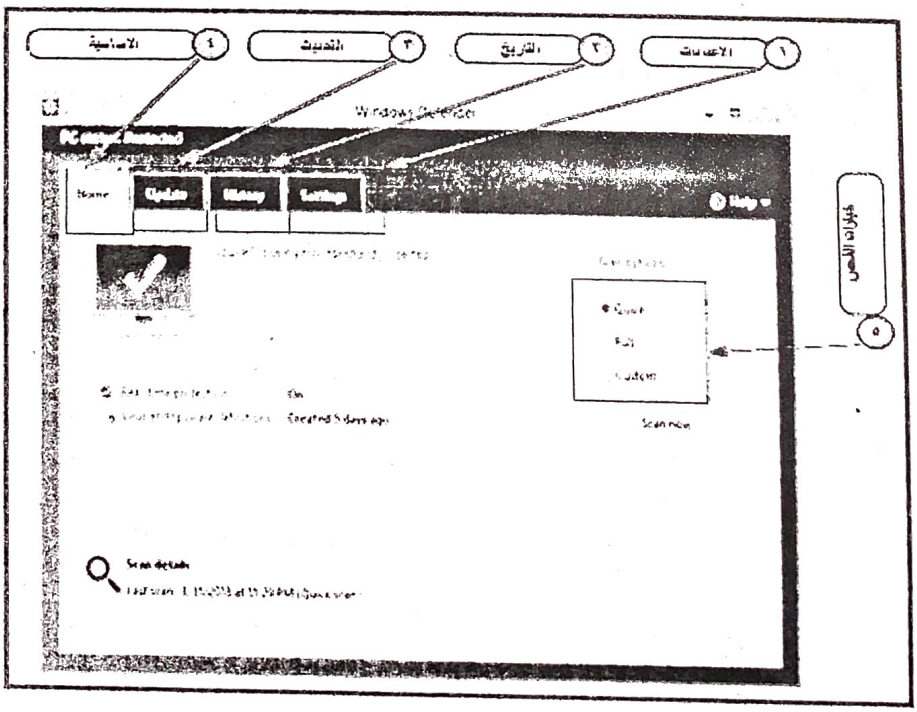
برنامج مدافع ويندوز (Windows Defender) هو بديل لبرنامج أساسيات الأمان لمايكروسفت ويعمل لتحقيق الحماية لأجهزة الحاسب التي تعمل بنظام ويندوز أحدث من ويندوز8، فهو يعتبر من البرامج الضرورية والمهمة والذي بدوره يقوم بحماية الملفات والتخلص من البرامج الضارة.

1. مميزات برنامج مدافع ويندوز

- يوفِّر تحديثات دورية.
- يوفِّر حماية كاملة للحاسب من الفيروسات والتجسس.
- يعمل على تنظيف الحاسب من البرامج الضارة والملفات العديمة الفائدة.
- حماية فعالة أثناء تصفح الإنترنت.
- 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.

2. الشاشة الرئيسة 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. والشكل 6-8 يوضح تلك العناصر.

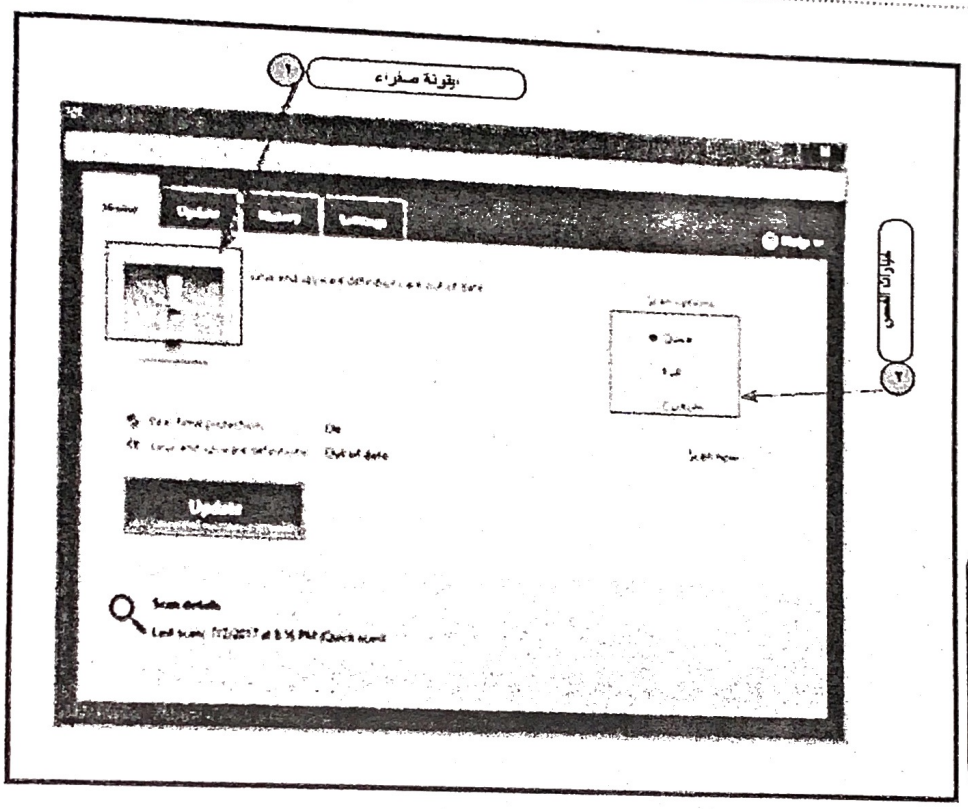


شكل6-8 للصفحة الأساسية ويندوز ديفندر

3. طريقة استخدام برنامج مُدافع ويندوز

هناك عدة أساليب فحص يوفرها برنامج مدافع ويندوز. والشكل 6-9 يوضح ذلك.

- الفحص الكامل، الفحص المخصص، الفحص السريع.



شكل 6-9: الحالة غير محمية فى ويندوز ديفندر

أ. **الرمز الأخضر:**

في الشكل 6-8 يعنى أن حالة أمان الحاسب جيدة محدثة وتعمل في الخلفية للمساعدة على حماية الحاسب من البرامج الضارة والتهديدات الضارة الأخرى.

ب. **الرمز الأصفر**

يعني أن الحالة غير محمية بشكل محتمل ويمكن اتخاذ بعض الإجراءات، مثل تشغيل الحماية في الوقت الحقيقي أو إجراء فحص النظام. كما في الشكل 6-9.

كيفية عمل برامج مايكروسوفت لإزالة الفيروسات

يقوم البرنامج بالآتي للتخلص من الفيروسات:

- الخطوة الأولى: فحص الأجهزة (Scan) للكشف عن الفيروسات.
- الخطوة الثانية: إزالة الفيروس والتخلص منه، وإذا تعذَّر ذلك نستخدم أمر إعادة تشكيل الجهاز (Format).

6-11 أمن المعلومات والأمن السيبرانى

أمن المعلومات (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.

بينما نجد أن الأمن السيبرانى (Cyber Security) هو العلم الذي يُعنى بالفضاء المعلوماتي، ويستخدم الوسائل التقنية والإدارية لمنع الإستخدام الغير مصرح به للبيانات الرقمية والمعلومات. ويهدف

الأمن السيبرانى الى ضمان توافر واستمرارية عمل نظم المعلومات الرقمية وتأمين وحماية سرية وخصوصية البيانات الشخصية لحماية المواطنين في ظل استخدام خدمات الحكومة الالكترونية، وغيرها من الخدمات الالكترونية الأخرى. والحقيقة أن أمن المعلومات أصبح جزءاً من الامن السيبرانى، حيث يشمل الأمن السيبرانى أمن المعلومات على الأجهزة وشبكات الحاسبات. ويعتبر الأمن السيبرانى حالياً من الركائز الأساسية في العديد من المؤسسات وحتى الدول لمواجهة الحروب الالكترونية. نجد ان هنالك العديد من الدول العربية ومنها على سبيل المثال المملكة العربية السعودية التي أصبحت تضع الامن السيبرانى في مقدمة اولوياتها في سياستها الدفاعية الوطنية، كما قامت بتخصيص اقسام خاصة بالحرب السيبرانية ضمن فرق الامن الوطني. عليه نجد ان صلاحية الامن السرياني الوطني تعتمد على عدة أشياء منها:

- إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات
- تطوير استراتيجية وطنية للأمن السيبرانى وحماية البنية التحتية للمعلومات الحساسة
- ردع الجريمة السيبرانية
- إيجاد الحافز لخلق قدرات وطنية لإدارة جرائم الحاسب الالي

مهارة 6- 10

- **التعرف على أخلاقيات استخدام الحاسب وأهم الوصايا لأخلاقيات الحاسب.**

6-12 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:

- أخلاقيات استخدام الحاسب بين الشخص ونفسه.

ومن الأخلاقيات التي يجب أن يتصف بها الفرد في هذه الحالة عدم القيام بأمور تنعكس سلباً عليه، كإضاعة الوقت، والاطلاع على خصوصيات الآخرين.

- أخلاقيات استخدام الحاسب بين الشخص والغير.

عند العمل على الحاسب والإنترنت يجب احترام الملكية الفردية وعدم سرقة أعمال الأشخاص الآخرين، والحفاظ على خصوصية وأسرار الآخرين وعدم إيذاء الآخرين.

- أخلاقيات استخدام الحاسب بين المستخدم والجهاز.

تعنى المحافظة على الحاسب والالتزام بالقوانين التي وضعت للاستفادة من استخدامه.

من الوصايا لأخلاقيات استخدام الحاسب والإنترنت

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.