سلسلة
الحوسبة و الذكاء الاصطناعي
و الأمـن السيبراني

المستوى التاسع
9



Grok Gemini Windows 10 Windows 11 deepseek

الفهرس

الشخصيات الرئيسة ١

الوحدة الأولى (أساسيات الحاسوب) -الفيروسات وأمن البيانات - ٢

الدرس الأول - مقدمة عن الفيروسات الإلكترونية - ٣
الدرس الثاني - أنواع الفيروسات الإلكترونية- ٥
الدرس الثالث - الحماية من الفيروسات- ٧

الوحدة الثانية (البرامج والتطبيقات) - برنامج الجداول الحسابية MS – Excel - ١٣

الدرس الأول - أساسيات برنامج اكسيل MS – Excel - ١٤
الدرس الثاني - التعامل مع الخلايا - تحديد الخلايا والنطاقات - ١٩
الدرس الثالث - إدخال البيانات إلى الخلايا - ٢٢
الدرس الرابع - تنسيق الخلايا - ٢٥

الوحدة الثالثة (البرامج والتطبيقات) - الجداول الحسابية وعملياتها في MS – Excel - ... ٣٢

الدرس الأول - إنشاء جدول البيانات - ٣٣
الدرس الثاني - فرز البيانات - ٣٦
الدرس الثالث - تصفية البيانات - ٣٨
الدرس الرابع - التعامل مع المصنفات - ٤٠

الوحدة الرابعة (الإنترنت) - تطبيقات الإنترنت الحديثة - ٤٧

الدرس الأول - الخدمات السحابية (Cloud Computing) - ٤٨
الدرس الثاني - التجارة الإلكترونية - ٤٩
الدرس الثالث - إنترنت الأشياء (IoT) - ٥٠
الدرس الرابع - التطبيقات الذكية - ٥٢
الدرس الخامسة - الثورة الرقمية - ٥٣

الوحدة الخامسة (الذكاء الاصطناعي) - الأنظمة الخبيرة Expert Systems - ٥٨

الدرس الأول - مفهوم الأنظمة الخبيرة ودورها - ٥٩
الدرس الثاني - مكونات الأنظمة الخبيرة - ٦١
الدرس الثالث - تصميم نظام خبير - ٦٣
الدرس الرابع - قيود الأنظمة الخبيرة - ٦٥

الوحدة السادسة (الأمن السيبراني) - الذكاء الاصطناعي والأمن السيبراني - ٦٩

الدرس الأول - الأمان في استخدام الشبكات اللاسلكية (Wi-Fi) - ٧٠
الدرس الثاني - استخدام التعلم الآلي للكشف عن التهديدات - ٧٢
الدرس الثالث - كيف تستفيد الشركات من الذكاء الاصطناعي في الأمان؟ - ٧٤

SAJA
سجى المتخصصة
SAJA SPECIALIZED

١

الوحدة الأولى (أساسيات الحاسوب)

الفيروسات وأمن البيانات

السلام عليكم يا أبطال!

اليوم سنبدأ رحلة مثيرة إلى عالم الفيروسات وأمن البيانات. هل تعلمون أن هناك نوعين من الفيروسات؟ الأول هو الفيروسات التي تصيب الكائنات الحية، مثل البشر والحيوانات، والثاني هو الفيروسات الرقمية التي تهاجم أجهزة الحاسوب والهواتف. في هذه الوحدة؛ سنكتشف كيف تعمل الفيروسات الرقمية، وكيف يمكن أن تسرق معلوماتنا أو تدمر ملفاتنا.

لكن لا تقلقوا! ستكون لدينا أدوات وطرق لحماية أنفسنا من هذه الفيروسات.

هل أنتم مستعدون لمغامرتنا في عالم الفيروسات وأمن البيانات؟ **دعونا نبدأ**





أهداف التَعلُّـم

- تعرُّف ماهية فيروسات الحاسوب؛ بدايتها، وأسباب تصميمها.
- تحديد خصائص الفيروسات مثل الانتشار والتخفي.
- التمييز بين أنواع الفيروسات مثل المدمرة والمتنقلة.
- تعرُّف كيفية عمل الفيروسات وطرق انتشارها.
- التعرف على التدابير الوقائية مثل برامج مكافحة الفيروسات.
- التعرف على أنواع برامج مكافحة الفيروسات المتاحة.
- استخدام برامج مكافحة الفيروسات لإزالة الفيروسات من الجهاز.

في نهاية الوحدة ستتمكن من:



مقدمة عن الفيروسات الإلكترونية



السلام عليكم يا أبطال!

هل تساءلتم يومًا ماذا تعني الفيروسات الإلكترونية؟ إنها ليست مثل الفيروسات التي تصيبنا، بل هي برامج صغيرة يمكن أن تتسلل إلى أجهزة الحاسوب والهواتف الذكية. دعونا نستكشف سوياً هذا العالم المثير!



١- ما هي الفيروسات الإلكترونية؟ (Viruses) :

هي برامج خبيثة تُصمم لتعطيل أو تدمير أجهزة الكمبيوتر والبيانات أو حتى سرقة المعلومات.

تصوّر أن لديك مجموعة من الكتب مرتبة بشكل جميل على رف. يقوم الفيروس مثل "سارق سري" بإعادة ترتيب الكتب بعشوائية وإخفاء بعضها، مما يجعل من الصعب عليك العثور على أي شيء.

٢- بداية ظهور فيروسات الحاسوب:



ظهرت فيروسات الحاسوب لأول مرة في أوائل الثمانينيات من القرن العشرين.

- يُعد "فيروس إيلك كلونر" (**Elk Cloner**) الذي تم تطويره عام **١٩٨٢** أحد أوائل الفيروسات المعروفة، وقد كان يستهدف أجهزة (**Apple II**) وينتقل عبر الأقراص المرنة.
- في عام **١٩٨٦**، ظهر فيروس "براين" (**Brain**)، الذي يعدُّ أول فيروس حقيقي للحواسيب الشخصية، حيث طُوِّر في الأصل لحماية حقوق البرمجيات، لكنه انتشر لاحقًا بشكل غير متوقع، مما أثار الانتباه لمخاطر البرمجيات الضارة.

٣- ما الأسباب التي تدفع بعض الناس لكتابة البرامج الفيروسية:

تتنوع الأسباب التي تدفع بعض الأشخاص لكتابة البرامج الفيروسية، ومنها:

التجريب والاستكشاف

قد ينشئ بعض المبرمجين فيروسات بدافع الفضول أو لاختبار حدود البرمجة وإثبات مهاراتهم التقنية.

الربح المالي

يستخدم البعض الفيروسات لسرقة المعلومات الشخصية، مثل بيانات البطاقات الائتمانية أو الحسابات المصرفية، أو ابتزاز المستخدمين من خلال برامج الفدية.

التخريب والانتقام

يلجأ بعض الأفراد أو المجموعات إلى البرمجيات الفيروسية كوسيلة للتخريب، الانتقام، أو توجيه ضربات ضد منافسين أو أعداء.

الشهرة وإثبات الذات

يبحث بعض الأشخاص عن الشهرة في مجتمع القرصنة، حيث يعتبرون كتابة فيروس ناجح دليلًا على مهاراتهم.

التجسس والاختراق

تستخدم الفيروسات أحيانًا من قبل حكومات أو جهات معينة للتجسس على أفراد أو دول أخرى، والوصول إلى معلومات سرية.

SAJA SPECIALIZED

٤- خصائص فيروسات الحاسب Characteristics of Computer Viruses:

هناك عدة خصائص تتميز بها فيروسات الحاسب، يمكن حصرها فيما يلي:

القدرة على النسخ الذاتي

تستطيع الفيروسات تكرار نفسها والانتقال من ملف إلى آخر أو من جهاز لآخر.
مثال: فيروس "Melissa" عام ١٩٩٩، الذي انتشر عبر رسائل البريد الإلكتروني بتكرار نفسه في المستندات المرفقة.

القدرة على التخفي

تستخدم بعض الفيروسات تقنيات للتخفي، مثل دمج نفسها في برامج موثوقة أو تغيير أكوادها باستمرار لتجنب اكتشافها.
مثال: فيروس "Polymorphic Virus"، الذي يُعدّل شفرته كلما أصاب جهازًا جديدًا، مما يجعله صعب الكشف.

التنفيذ المشروط

غالبًا ما تنتظر الفيروسات حتى تتحقق شروط معينة لتعمل، مثل فتح ملف محدد أو تاريخ معين.
مثال: فيروس "Michelangelo" الذي كان ينشط فقط في يوم ميلاد الفنان مايكل أنجلو (٦ مارس)، ويقوم بتدمير البيانات على الأقراص الصلبة.

التنوع والتكيف

تتنوع الفيروسات من حيث الأساليب والأهداف، ويطور المبرمجون أنواعًا جديدة تتكيف مع وسائل الحماية.
مثال: "Ransomware" أو برامج الفدية، التي تقوم بتشفير ملفات المستخدمين وتطلب فدية مالية لفك التشفير، مثل فيروس "WannaCry" الشهير.

هذه الخصائص المذهلة للفيروسات تجعل منها تهديدًا مستمرًا يتطلب تحديثات للحماية.

٥- أعراض إصابة الحاسب بالفيروسات

تشمل أعراض إصابة الحاسب بالفيروسات ما يلي:

- **بطء الأداء:** يصبح الجهاز بطيئًا بشكل غير معتاد، حتى عند تنفيذ مهام بسيطة.
- **الانهيار المتكرر:** يتعرض النظام للتجمد أو إعادة التشغيل بشكل مفاجئ.
- **رسائل خطأ غير مألوفة:** تظهر رسائل خطأ غير مبررة أو نوافذ منبثقة غريبة.
- **اختفاء أو تلف الملفات:** تُحذف بعض الملفات أو تتعرض للتلف دون تدخل من المستخدم.
- **تشغيل برامج غير مرغوبة:** قد تُفتح تطبيقات أو برامج تلقائيًا دون إذن.
- **استهلاك عالي للبيانات:** يزداد استخدام الإنترنت بشكل غير عادي دون تفسير.
- **إعلانات منبثقة مزعجة:** تظهر إعلانات مزعجة بكثرة، حتى عند عدم تصفح الإنترنت.





تعد هذه الأعراض مؤشرًا على وجود فيروسات، ويُنصح باستخدام برامج مكافحة الفيروسات للتأكد ومعالجة الجهاز.

أنواع الفيروسات الإلكترونية



مرحباً أصدقائي!
هل تساءلتم يومًا ماذا تعني الفيروسات الإلكترونية؟ إنها ليست مثل الفيروسات التي تصيبنا، بل هي برامج صغيرة يمكن أن تتسلل إلى أجهزة الحاسوب والهواتف الذكية. دعونا نستكشف سوياً هذا العالم المثير!

١- أنواع الفيروسات الإلكترونية:

تتنوع فيروسات الحاسوب إلى عدة أنواع، تشمل:

الفيروسات المتنقلة / الديدان (Worms)



تنتشر عبر الشبكات دون تفاعل المستخدم. مثال "Code Red" الذي انتشر في عام ٢٠٠١.

فيروسات الملفات (File Infectors)



تصيب الملفات التنفيذية وتنتشر عند فتحها. مثال "Cascade"

الفيروسات متعددة الأشكال (Polymorphic Viruses)



تتغير شيفرتها باستمرار، مما يصعب الكشف عنها. مثال "Storm Worm".

فيروسات قطاع الإقلاع (Boot Sector Viruses)



تصيب قطاع الإقلاع وتبدأ عند تشغيل الجهاز. مثال "Michelangelo".

فيروسات الماكرو (Macro Viruses)



تصيب مستندات التطبيقات مثل Word وExcel. مثال "Melissa"

فيروسات حصان طروادة (Trojan Horses)



تبدو كبرامج عادية لكنها تحتوي على أكواد ضارة. مثال "Zeus Trojan"

فيروسات الفدية (Ransomware)



تشفر البيانات وتطلب فدية لفك التشفير. مثال "WannaCry".

الفيروسات المتخفية (Stealth Viruses)



تتلاعب هذه الفيروسات بالنظام لتخفي آثارها وتتجنب اكتشافها. مثال: فيروس "Frodo"

الفيروسات المتعددة الأجزاء (Multipartite Viruses)



تصيب أجزاء مختلفة من النظام. وتكون أكثر صعوبة في الإزالة لأنها تنتشر في أماكن متعددة.مثال "Tequila".



كل نوع من هذه الفيروسات يختلف في طريقة عمله وأهدافه، مما يجعل من الضروري استخدام حلول حماية شاملة لمنع أضرارها.

٢- كيفية عمل الفيروسات وكيف تدخل الجهاز:

تعمل الفيروسات على استخدام تقنيات متنوعة للاختراق والتأثير على الأجهزة كما يلي:

أ) أساليب دخول الفيروسات إلى الجهاز

١- من خلال البريد الإلكتروني (Email Attacks):
تعد الرسائل الإلكترونية واحدة من أكثر طرق انتشار الفيروسات شيوعًا. يُرسل الفيروس عادة كمرفق أو رابط ضار في البريد الإلكتروني. عند فتح المرفق أو النقر على الرابط، يتم تحميل الفيروس وتشغيله على الجهاز.
مثال: فيروس "ILOVEYOU" (٢٠٠٠)، الذي انتشر عبر البريد الإلكتروني وأصاب ملايين الأجهزة حول العالم، من خلال مرفقات تبدو كرسائل حب.

٢. من خلال تنزيلات الإنترنت (Downloads):
قد يُرفق الفيروس ببرامج أو ملفات تبدو مشروعة يتم تحميلها من الإنترنت. عند تنزيل البرنامج أو الملف وتشغيله، يتم تفعيل الفيروس.
مثال: الفيروسات التي تنتشر عبر تحميل برامج أو ألعاب من مواقع غير موثوقة، مثل "Freeware" أو "Pirated Software".

٣. عبر وسائل التخزين الخارجية (External Devices):
قد تنتقل الفيروسات من جهاز إلى آخر عبر أجهزة التخزين الخارجية مثل الأقراص الصلبة، USBs، أو بطاقات الذاكرة. عند توصيل هذه الأجهزة بجهاز آخر، قد تُنقل الفيروسات بدون علم المستخدم.
مثال: فيروس "Stuxnet" الذي استخدم أجهزة USB لانتقاله بين الأنظمة، وكان يستهدف بشكل خاص الأنظمة الصناعية.

٤. من خلال الثغرات الأمنية في النظام (Exploiting Vulnerabilities):
تستغل بعض الفيروسات الثغرات الأمنية في أنظمة التشغيل أو البرمجيات لتسلل إلى الجهاز. قد لا يكون للمستخدم علم بها، مما يجعل من الصعب اكتشاف الفيروس قبل أن يتسبب في أضرار.
مثال: فيروس "Conficker" الذي استغل ثغرة في نظام Windows ليصيب ملايين الأجهزة حول العالم.

ب) كيف يعمل الفيروس بعد دخوله الجهاز؟

١- التكرار والانتشار (Replication and Spread):
بمجرد أن يدخل الفيروس إلى جهاز، يبدأ في التكرار والانتشار إلى ملفات أو برامج أخرى على نفس الجهاز أو إلى أجهزة أخرى عبر الشبكة أو وسائل التخزين.
مثال: الفيروسات من نوع "Worms" مثل "Code Red"، التي تنتقل من جهاز إلى آخر عبر الإنترنت أو الشبكة، دون تدخل المستخدم

٢- إتلاف البيانات أو البرامج (Data or Program Corruption):
بعد الانتشار، قد يبدأ الفيروس في تلف أو حذف البيانات أو إتلاف الملفات. في بعض الحالات، يمكن أن يجعل الجهاز غير قابل للاستخدام.
مثال: فيروس "CIH" الذي دمر البيانات على الأقراص الصلبة وأدى إلى تلف النظام

٣- تعطيل وظائف النظام (System Disruption):
قد يتسبب الفيروس في إبطاء أداء النظام، تعطيل بعض الوظائف، أو حتى منع تشغيل النظام بشكل كامل.
مثال: فيروس "Melissa"، الذي كان يرسل نسخًا من نفسه عبر البريد الإلكتروني، مما أدى إلى إبطاء النظام وتعطيله

٤- السيطرة على الجهاز أو سرقة المعلومات (Remote Control and Data Theft):
بعض الفيروسات، مثل "Trojan Horses"، تقوم بتثبيت برامج خبيثة تسمح للمهاجمين بالتحكم في الجهاز عن بُعد أو سرقة البيانات الحساسة.
مثال: فيروس "Zeus Trojan"، الذي كان يستخدم لسرقة معلومات الحسابات المصرفية عبر تسجيل ضربات لوحة المفاتيح

٥- تشفير البيانات (Data Encryption):
فيروسات الفدية (Ransomware) تقوم بتشفير ملفات المستخدم، وتطلب فدية مقابل فك التشفير. تؤدي هذه الفيروسات إلى فقدان الوصول إلى البيانات حتى دفع المبلغ المطلوب.
مثال: فيروس "WannaCry"، الذي قام بتشفير الملفات على أجهزة الحاسوب المُصابة وطلب فدية لفك التشفير

SAJA SPECIALIZED
سجى المتخصصة

الحماية من الفيروسات

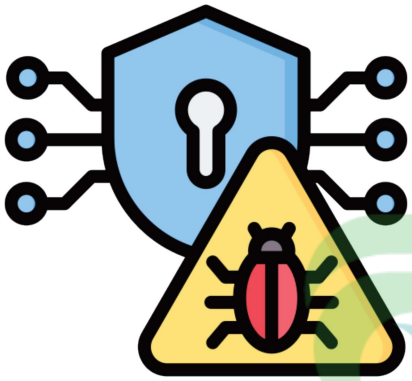


مرحباً أصدقائي!
في هذا الدرس، سنتعلم معًا كيف نحمي أنفسنا وأجهزتنا من هذه الفيروسات بطريقة بسيطة وفعالة.

١- طرق الحماية من الفيروسات:

هناك عدة طرق لحماية أجهزة الحاسوب من خطر الفيروسات من أهمها:

أ- استخدام برامج مكافحة الفيروسات:



برامج مكافحة الفيروسات هي برامج تساعد على اكتشاف وإزالة الفيروسات والبرامج الضارة التي قد تضر أجهزتنا.

- أهمية برامج مكافحة الفيروسات:

- حماية الجهاز: تمنع الفيروسات من الدخول إلى الحاسوب وتخريب الملفات.
- الأمان الشخصي: تحمي معلوماتك السرية مثل الصور، الملفات، وكلمات المرور.
- الأداء الجيد: تساعد برامج مكافحة الفيروسات في الحفاظ على سرعة الجهاز وعدم بطئه بسبب البرامج الضارة.

- أنواع برامج مكافحة الفيروسات:

توجد العديد من أنواع برامج مكافحة الفيروسات، وكل نوع منها يقدم ميزات مختلفة لحماية أجهزة الحاسوب والبيانات. الجدول التالي يعرض بعض الأنواع الرئيسة:

نوع برنامج مكافحة الفيروسات	التعريف	المزايا	الأمثلة
برامج مكافحة الفيروسات المجانية	برامج مجانية تقدم حماية أساسية من الفيروسات	حماية أساسية، مناسبة للاستخدام الشخصي	Avast Free، AVG Free
برامج مكافحة الفيروسات المدفوعة	برامج مدفوعة تمنح حماية شاملة مقابل اشتراك	حماية متقدمة، مراقبة المواقع والبريد الإلكتروني	Norton، McAfee
برامج مدمجة مع نظام التشغيل	تأتي مدمجة مع نظام التشغيل، تعمل تلقائيًا	مجانية، سهلة الاستخدام، تحديثات تلقائية	Windows Defender
برامج مكافحة الفيروسات السحابية	تعتمد على الإنترنت لإجراء فحص سريع وتحديث السحابة	خفيفة، سريعة التحديث	Panda Cloud Antivirus
برامج للأجهزة المحمولة	حماية الهواتف والأجهزة اللوحية	حماية التطبيقات والملفات الموجودة على الهاتف	Avast Mobile Security
برامج مخصصة للشركات	مخصصة لحماية أجهزة وخوادم الشركات	حماية شاملة، إدارة مركزية للفيروسات	Symantec Endpoint، Trend Micro

- احرص على تحميل وتثبيت برنامج مكافحة الفيروسات من مصدر موثوق.
- إذا أردنا تثبيت برنامج مثل "Avast" أو "Norton"، ندخل إلى موقع البرنامج الرسمي، ونضغط على زر التنزيل، ثم نتبع التعليمات التي تظهر لى الشاشة ثبيته.
- إذا كنت تستخدم جهاز حاسوب يعمل بنظام Windows، فقد يكون Windows Defender مفعّلًا بالفعل ويعمل لى حمايتك دون الحاجة إلى تثبيت أية برامج إضافية.

ب- تحديث البرامج والنظام بانتظام



تعمل التحديثات على إصلاح الثغرات التي قد يستغلها الفيروس للتسلل إلى الجهاز.

إذا كان لديك نظام Windows، فتأكد من تفعيل التحديثات التلقائية. نفس الشيء لأجهزة الهواتف، حيث تضمن التحديثات الدورية أمان الجهاز.

ج- تجنب فتح الروابط أو المرفقات غير المعروفة



الفيروسات قد تكون مخبأة في مرفقات الرسائل أو الروابط غير الموثوقة. لذلك يجب الحذر عند فتح الروابط أو الملفات من أشخاص مجهولين.

إذا وصلك بريد إلكتروني من شخص لا تعرفه بعنوان "احصل على جائزة مجانية" مثلاً، تجنب فتحه لأن الرابط قد يحتوي على فيروس.

د- تحميل البرامج من مواقع موثوقة فقط



تحميل التطبيقات من مواقع رسمية مثل متاجر التطبيقات أو المواقع الموثوقة يقلل من خطر تنزيل برامج ضارة.

إذا أردت تحميل لعبة، تأكد من أن المصدر هو متجر "Google Play" أو "App Store"، حيث يتم فحص التطبيقات من الفيروسات قبل نشرها.

ه- استخدام كلمات مرور قوية وعدم مشاركتها



كلمات المرور القوية التي تحتوي على أحرف كبيرة وصغيرة، وأرقام ورموز، تحمي الحسابات من الاختراقات.

إذا كان لديك حساب على الإنترنت، احرص على أن تكون كلمة المرور قوية مثل "StroNG!٢٠٢٤" وليس كلمة بسيطة مثل "١٢٣٤٥٦".

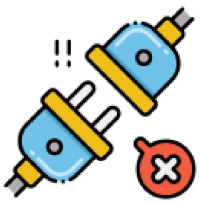
و- إجراء نسخ احتياطية للملفات المهمة



النسخ الاحتياطي يحمي ملفاتك المهمة من الضياع إذا أصيب جهازك بفيروس.

يمكن تخزين الملفات على خدمات السحابة مثل Google Drive أو على جهاز تخزين خارجي.

ز- فصل الإنترنت عند عدم الحاجة



قطع الاتصال بالإنترنت عند عدم الحاجة يقلل من احتمالية تعرض الجهاز للهجمات الإلكترونية.

إذا كنت لا تستخدم ا نترنت لفترة، يمكنك قطع الاتصال لتقليل المخاطر.

SAJA SPECIALIZED
سجى المتخصصة

٢- كيفية إزالة الفيروسات إذا أصاب الجهاز:

إذا أصيب جهاز الحاسوب بفيروس، فلإزالته علينا اتباع الخطوات التالية:

أ- التحقق من وجود الفيروسات



أول خطوة هي التأكد من أن جهازنا مصاب بفيروس.

بعض العلامات قد تكون مؤشرات على وجوده مثل أن يكون الجهاز بطيئًا أو تظهر عليه رسائل غريبة، أو أن الجهاز وقف عن العمل فجأة أو إذا ظهرت نوافذ غير معروفة.

ب- فصل الجهاز عن الإنترنت



عند اكتشاف الفيروس، يجب فصل الجهاز عن الإنترنت فوراً لمنع الفيروس من الانتشار أو سرقة البيانات.

إذا كان جهازك موصولًا بشبكة Wi-Fi، يمكنك إيقاف الاتصال من الإعدادات أو من زر Wi-Fi على الحاسوب.

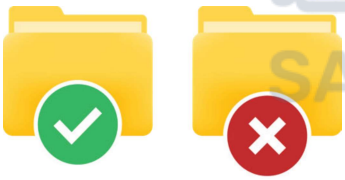
ج- تشغيل برنامج مكافحة الفيروسات



الآن، نقوم بفتح برنامج مكافحة الفيروسات المثبت على جهازنا ونبدأ عملية الفحص الكامل. الآن، نقوم بفتح برنامج مكافحة الفيروسات المثبت على جهازنا ونبدأ عملية الفحص الكامل.

يمكنك فتح برنامج Windows Defender أو Avast، ثم الضغط على "الفحص الكامل" ليقوم البرنامج بالبحث عن الفيروسات.

د- حذف الملفات المصابة أو عزلها



بعد انتهاء الفحص، سيعطينا برنامج مكافحة الفيروسات خيار حذف الملفات المصابة أو عزلها (وضعها في منطقة آمنة بعيدًا عن الملفات الأخرى).

هـ- تحديث برنامج مكافحة الفيروسات



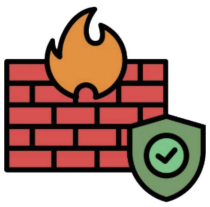
بعد إزالة الفيروسات، نحدث برنامج مكافحة الفيروسات ليكون مستعدًا لمكافحة الفيروسات الجديدة، يمكنك الذهاب إلى إعدادات البرنامج، والضغط على "التحديث"، لتثبيت التحديثات التي تجعل البرنامج أقوى.

و- إعادة تشغيل الجهاز



بعد تنظيف الجهاز، يُفضل إعادة تشغيله للتأكد من أن كل شيء يعمل بشكل طبيعي،

ز- تثبيت جدار ناري (Firewall)



جدار الحماية (Firewall) هو برنامج يمنع البرامج الضارة من الدخول إلى جهازك ويعزز حماية جهازك من الفيروسات.

يمكنك تشغيل جدار الحماية من إعدادات الجهاز أو من برنامج مكافحة الفيروسات الذي قد يحتوي على جدار ناري مدمج.

سجى المتخصصة
SAJA SPECIALIZED

تدريب

١- اختر الإجابة الصحيحة لكل من العبارات التالية:

١ ما هو الهدف الأساسي من تصميم بعض الأشخاص للفيروسات؟

أ حسين أداء الحاسوب ب للتجسس أو سرقة ا علومات ج لحماية البيانات

٢ ما هو أول فيروس حاسوب معروف تم تصميمه ليصيب أجهزة الحاسوب الشخصية؟

أ فيروس "ستورم" (Storm) ب فيروس "ميليسا" (Melissa) ج فيروس "براين" (Brain)

٣ أي من الخصائص التالية تميز فيروسات الحاسوب؟

أ القدرة لى التناسخ ب حماية النظام من البرامج الضارة ج تحسين سرعة النظام

٤ ما هو العرض الأكثر ش وعًا لإصابة الحاسوب بفيروس؟

أ زيادة في سرعة النظام ب ظهور نوافذ منبثقة غير مرغوب فيها ج تحديث لقائي للبرامج

٥ ما نوع الفيروسات الذي يعمل على تغيير التعليمات البرمجية الخاصة به لتجنب اكتشافه؟

أ الفيروسات متعددة الأشكال ب الفيروسات المتسللة ج فيروسات الديدان

٦ كيف يمكن لفيروس الحاسوب الدخول إلى جهازك؟

أ من خلال توصيل شاحن الهاتف ب عبر شبكة ا نترنت أو البريد ا لكتروني ج من خلال تحديثات النظام الآمنة

٧ أي من الخيارات التالية يعدُّ أفضل طريقة لحماية الحاسوب من الفيروسات؟

أ تنزيل الملفات من مصادر غير موثوقة ب تشغيل برامج مكافحة الفيروسات وتحديثها نتظام ج إيقاف تشغيل جدار الحماية

٨ ما هو النوع الأساسي من برامج مكافحة الفيروسات الذي يمنح حماية مجانية لكن محدودة؟

أ برامج المكافحة السحابية ب برامج مكافحة الفيروسات المدفوعة ج برامج المكافحة المجانية

٩ ما هو أول إجراء يجب اتخاذه عند اكتشاف فيروس على الجهاز؟

أ فصل الجهاز عن ا نترنت ب حذف الملفات المهمة يدويًا ج إعادة تشغيل الجهاز

١٠ أي من الخطوات التالية تأتي بعد فحص الجهاز ببرنامج مكافحة الفيروسات؟

أ حذف الملفات المصابة أو عزلها ب إيقاف برنامج مكافحة الفيروسات ج تشغيل جدار الحماية

١١ ما الذي يفعله الفيروس عندما يصيب ملفًا؟

أ يحميه من أي ديلات ب يحذف كل ا ملفات لقائيًا ج يعطله أو يغير محتواه

١٢ متى بدأت فيروسات الحاسوب في الظهور لأول مرة؟

أ في السبعينيات ب في الثمانينيات ج في التسعينيات

سجلي المتخصصة SAJA SPECIALIZED



٢- صل كل عملية مع وظيفتها المناسبة:

أ) تناسخ الفيروس	١) يتنكر كبرنامج مفيد لإيقاع المستخدم في فخ إصابة الجهاز.
ب) التجسس	٢) تكاثره بسرعة واصابته ملفات متعددة.
ج) فيروس حصان طروادة	٣) أول فيروس معترف به في عام ١٩٨٢.
د) فيروس "ألتير" (Altair)	٤) مراقبة بيانات المستخدمين والحصول على معلومات.

٣- ضَعْ علامة (✓) أمام العبارات الصحيحة، و علامة (✗) أمام العبارات الخطاء فيما يأتي :

١- الفيروسات تتسبب عادة في تباطؤ أداء الجهاز وتوقف بعض البرامج فجأة ( )
٢- فيروسات "الدودة" يمكنها الانتشار عبر الشبكات بدون الحاجة لوجود ملف مصاب ( )
٣- برنامج مكافحة الفيروسات لا يحتاج إلى تحديثات لأن الفيروسات لا تتطور. ( )
٤- من الأفضل فتح المرفقات المجهولة في رسائل البريد الإلكتروني لأنها لا تحتوي على أي فيروسات. ( )
٥- يمكن استخدام برامج مكافحة الفيروسات المجانية بشكل فعال مثل تلك المدفوعة. ( )
٦- يمكن للفيروسات أن تدخل جهاز الحاسوب عن طريق الوسائط القابلة للإزالة مثل الفلاش ميموري. ( )
٧- جدران الحماية (Firewall) تساهم في منع الفيروسات من دخول الجهاز عبر الإنترنت. ( )
٨- العدوى بفيروس الحاسوب لا يمكن أن تؤثر على الأداء العام للجهاز. ( )
٩- فيروسات "الجذر" (Rootkits) تساعد في إخفاء وجود الفيروس من برامج مكافحة الفيروسات. ( )
١٠- ظهرت فيروسات الحاسوب لأول مرة في بداية التسعينيات. ( )
١١- فيروس "براين" كان أول فيروس حقيقي يتم تصميمه لإصابة أجهزة الحاسوب الشخصية. ( )
١٢- تتواجد الفيروسات في الأجهزة المحمولة بنفس القدر الذي توجد فيه على أجهزة الحاسوب الشخصية. ( )

٤- ما هي طرق الحماية التي يمكن اتباعها لتجنب الإصابة بالفيروسات؟

.....

.....

.....

.....

.....

.....

SAJA SPECIALIZED

تدريب

٥- املأ الفراغات بالكلمات الصحيحة فيما يلي:

مواصلة "نورتون" فتح المرفقات مكافحة الفيروسات "مكافي" الفيروسات الدودية

١- البرامج التي تساعد في اكتشاف وإزالة الفيروسات من جهاز الحاسوب تسمى برامج .....

٢- من أشهر برامج مكافحة الفيروسات المتوافرة في السوق هي ..... و ..... .

٣- من الطرق التي قد يدخل من خلالها الفيروس إلى جهاز الحاسوب هي ..... .

٤- الفيروسات التي يمكن أن تسبب أضرارًا في النظام دون أن يتطلب تدخل المستخدم تسمى .....

.....

٥- من أكثر الطرق الفعالة في الوقاية من الفيروسات هي ..... تحديث نظام التشغيل والبرامج بشكل مستمر.

٦- قارن بين الفيروسات والديدان من خلال طريقة دخولها إلى الأجهزة

.....

.....

.....

.....

.....

SAJA
سجى المتخصصة
SAJA SPECIALIZED

٧- ما الإجراء الذي ينبغي عليك فعله في الحالات التالية:

الحالة (١): تلقيت رسالة بريد إلكتروني تحتوي على مرفق من شخص لا تعرفه، وتطلب منك فتح المرفق لعرض محتوى مثير.

- الإجراء: .....

.....

الحالة (٢): جهازك يعمل ببطء شديد بعد تثبيت برنامج جديد من الإنترنت.

- الإجراء: .....

.....

الحالة (٣): أثناء التصفح على الإنترنت، ظهرت لك صفحة تحذيرية تخبرك أن جهازك مصاب بفيروس ويجب عليك تحميل برنامج من تلك الصفحة لحل المشكلة.

- الإجراء: .....

.....