



كلية: الآداب

القسم او الفرع: قسم اللغة الإنجليزية

المرحلة: الأولى

أستاذ المادة: أحمد وليد خليل الناصر

اسم المادة باللغة العربية: الحاسبات

اسم المادة باللغة الإنكليزية: **Computers**

اسم المحاضرة الثامنة باللغة العربية: فايروسات الحاسوب

اسم المحاضرة الثامنة باللغة الإنكليزية: **Computer Viruses**

محتوى المحاضرة الثامنة

- فايروسات الحاسوب (المكونات / الأنواع / طرق الوقاية)

- برامج مكافحة الفايروسات

- المخاطر الأمنية في الوقت الحالي

فايروس الحاسوب (Computer Virus)

الفايروس هو عبارة عن برنامج صغير قابل للتنفيذ مكتوب بلغة برمجة معينة له القدرة على نسخ شفرته داخل البرامج، ومهمته إحاق الضرر بالحواسيب من خلال تغيير خصائص الملفات التي يصيبها لتقوم بمهام إزالة أو تعديل أو تخريب البرامج الموجودة في الحاسوب.

مكونات برنامج الفايروس: يتكون الفايروس من ثلاثة أجزاء رئيسية يمكن توضيحها كما في أدناه:

- ١- آلية العدوى (**Infection mechanism**): التي تعثر على الملفات الجديدة وتصيبها،
- ٢- المشغل أو الزناد (**The trigger**): الذي يحدد وقت تفعيل الحمولة،
- ٣- الحمولة (**The payload**): وهي الشفرة الخبيثة المراد تنفيذها، ويُطلق عليها أيضاً مصطلح ناقل العدوى (**Infection vector**)، وهذه هي الطريقة التي ينتشر بها الفايروس.

طرق العدوى: تتم إصابة الحاسوب بالفايروسات بطرق عديدة يمكن تلخيصها بما يلي:

- تناقل واستخدام الأقراص والفلأش ميموري المصابة بالفايروسات
- البريد الإلكتروني والملفات المصابة المرفقة مع الرسائل البريدية
- تحميل البرامج غير المرخصة من شبكة الانترنت
- تصفح مواقع مشبوهة ملغومة بالفايروسات.

أعراض الإصابة بالفايروسات

١. فشل في تحميل نظام التشغيل
٢. بطء في تشغيل وأداء النظام
٣. ظهور نقص مفاجئ في سعة الذاكرة
٤. توقف بعض البرامج عن العمل بدون سبب
٥. ظهور ملفات بامتدادات عشوائية وغريبة
٦. توقف النظام فجأة عن العمل بدون رسالة خطأ.

أنواع الفيروسات

يمكن تقسيم الفيروسات الى أنواع عديدة يمكن اختصارها بالأنواع الرئيسية التالية:

١. فيروسات تصيب الملفات: وتنتشر هذه الفيروسات عن طريق نسخ الملفات والبرامج المصابة أو إرفاقها مع رسائل البريد الإلكتروني.
٢. فيروسات تصيب قطاع التحميل في القرص الصلب (Boot sector)
٣. فيروسات تسمى بالبرامج الخبيثة: وهي مصممة لإلحاق الضرر بالمستخدم ومن أمثلتها:
 - الديدان (Worms): وهي مصممة للانتشار بين شبكات الحاسوب وتعمل على إبطاء عمل الشبكات.
 - أحصنه طروادة (Trojan horse): وهي برامج خبيثة تختفي داخل برامج أخرى مهمة وغرضها جمع المعلومات وإرسالها والسماح للهackerز بتصفح الجهاز والتحكم بملفات الضحية.
 - برامج التجسس (Spyware): وهو أي برنامج يثبت نفسه على جهاز الكمبيوتر الخاص بك ويبدأ في مراقبة سلوكك عبر الإنترنت سرًا دون علمك أو إذتك.
٤. فيروس متعدد الأجزاء: وهو نوع من الفيروسات شديد العدوى ويمكن أن ينتشر بسهولة على نظام الكمبيوتر الخاص بك. يمكن أن يصيب أجزاء متعددة من النظام بما في ذلك الذاكرة والملفات وقطاع التمهيد مما يجعل من الصعب احتوائه.
٥. فيروس متعدد الأشكال: هذا الفيروس لديه القدرة على التهرب من برامج مكافحة الفيروسات لأنه يمكنه تغيير الرموز في كل مرة يتم فيها تنفيذ ملف مصاب.

كيفية الوقاية من الفيروسات

- عمل نسخ احتياطية من الملفات المهمة بصورة دورية
- عدم فتح الملفات المرفقة بالبريد الإلكتروني من جهة مشبوهة أو غير معروفة
- استخدام برامج مكافحة الفيروسات لفحص الأقراص وبصورة مستمرة
- عدم نسخ أي ملفات من مصادر مجهولة ومواقع الإنترنت غير المعروفة
- عمل نقطة استعادة للنظام (Restore point)
- فحص الأقراص القابلة للإزالة مثل الأقراص والفلاش ميموري قبل استخدامها
- عدم زيارة وتصفح المواقع الغير آمنة وعدم النقر على الروابط المشبوهة في شبكة الإنترنت.

برامج مكافحة الفيروسات

وهي نوع من البرامج المستخدمة لمنع الفيروسات من اختراق جهاز الكمبيوتر ومسحها ضوئياً واكتشافها وحذفها. بمجرد التثبيت، تعمل معظم برامج مكافحة الفيروسات تلقائياً في الخلفية لتوفير حماية في الوقت الفعلي ضد هجمات الفيروسات. وهناك العديد من البرامج المستخدمة في الكشف عن الفيروسات والقضاء عليها والتي تعمل مع مختلف أنظمة التشغيل، ومن أمثلة هذه البرامج:

Bitdefender Anti-virus -	McAfee -
Avast Anti-virus -	Norton Anti-virus -
Eset nod32 Anti-virus -	Kaspersky Anti-virus -
F-Secure Anti-virus -	G Data Anti-virus -

المخاطر الأمنية الأكثر انتشاراً في الوقت الحالي:

1- الفيروسات Viruses: وهي برامج مصممة للانتقال الى اجهزة الحاسوب بطرق عدة وبدون إذن المستخدم وتؤدي الى تخريب او تعطيل عمل الحاسوب او اتلاف الملفات والبيانات.

2- ملفات التجسس Spywares: وهي برامج مصممة لجمع المعلومات الشخصية عن سلوك المستخدم مثل المواقع الالكترونية التي يزورها المستخدم بصورة متكررة وسجل بياناته وكلمات المرور للحسابات الالكترونية و كذلك تستطيع الحصول على امور مهمة تخص المستخدم مثل رقم بطاقة الائتمان دون علمه.

3- ملفات دعائية Adware: وهي برامج مصممة للدعاية والاعلان وتغيير الاعدادات العامة في اجهزة الحاسوب مثل تغيير الصفحة الرئيسية للمتصفح و اظهار بعض النوافذ الدعائية الغير مرغوبة اثناء الاتصال بالإنترنت وتصفح المواقع الالكترونية.

4- قلة الخبرة في التعامل مع بعض البرامج: مع ازدياد استخدام الانترنت من عامة الناس غير المتخصصين واستخدامهم وتعاملهم مع برمجيات متطورة لخاصة بخدمة تطبيقات الانترنت وبشكل مستمر وبدون خبره كافية لكيفية التعامل مع تلك البرمجيات قد يفتح ذلك ثغرة في جهاز الحاسوب تمكن الاخرين من اختراق الجهاز.

5- اخطاء عامة: مثل سوء اختيار كلمة السر او كتابتها على ورقة مما يمكن الاخرين من قراءتها او ترك الحاسوب مفتوحاً مما يسمح للآخرين (خاصة غير المخولين او الغرباء) بالدخول لملفات الحاسوب وسرقتها أو تخريبها او تغيير بعض الاعدادات.