الفيروسات:

- فيروس الكمبيوتر هو برنامج صغير يتم إدخاله على الحاسب الآلي من غير علم المستخدم بغرض تدمير بعض أو جميع البرامج والأجهزة المكونة للحاسب الآلي.

ظهور الفيروسات:

لقد بدأت الفيروسات بالإنتشار في منتصف الثمانينات من القرن الماضي و منذ ذلك الوقت تطورت وظهرت أنواع أكثر شراسة و سرعة خاصة مع نهاية عقد التسعينات و لقد وصل العدد المعروف من الفيروسات الشهيرة و النسخ المعدلة منها المئات الالوف من الفيروسات و هي في ازدياد كل يوم وهنالك الاف من الفيروسات الجديدة الفتاكة و المتواجدة داخل المختبرات و مراكز الأبحاث في دول عديدة وهي مخزنة كأسلحة الكترونية ضد الأعداء في حالة الحرب لتخريب أجهزة الكمبيوتر التابعة للعدو .

كيفية عمل الفيروسات:

يقوم من أنشأ الفيروس ببرمجة الفيروس و توجيه الأوامر له حيث يقوم بتحديد الزمان و متى و كيف يبدأ الفيروس بالنشاط وعادة ما تعطى فرصة كافية من الوقت للفيروس حتى يضمن حرية الإنتشار دون أن يلفت الإنتباه ليتمكن من إصابة أكبر عدد ممكن من المستخدمين ، و تختلف الفيروسات من حيث بدأ النشاط فهنالك من يبدأ بتاريخ أو وقت محدد و هنالك من يبدأ بالعمل بعد تنفيذ أمر معين في البرنامج المصاب و هناك من الفيروسات من يبدأ بالنشاط بعد التكاثر و الوصول الى رقم معين من النسخ.

و بعد أن ينشط الفيروس يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من انشاء ذلك الفيروس فهنالك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك انواع اخرى تقوم بحذف أو تعديل بعض الملفات وهناك من يقوم بتكرار ونسخ نفسه حتى يشل جهازك تماما و هناك انواع اشد فتكا فتقوم بمسح كل المعلومات من القرص الصلب .

من أنواع الفيروسات:

1-حصان طراودة (Trojan Horse):

هو جزء صغير من الكود يضاف الى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملا تخريبيا للنظام , وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة له ليؤدي دوره التخريبي .

2-الديدان (Worms)

الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه, وتتميز الدودة بقدرتها على إعادة توليد نفسها , بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث , وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد .

تقسيم الفيروسات:

1- فيروسات تعمل عند بدء التشغيل : Boot Sector Virus

يحتاج الكمبيوتر عند تشغيله إلى تعليمات خاصة داخلية لمعرفة مكونات الجهاز ، وهي توجد عادة في ملفات تدعى ملفات النظام (System Files) ، التي تحتوي على البرامج الخاصة ببدء التشغيل.

ويقوم هذا النوع من الفيروسات بالتسلل إلى القطاع الخاص ببرنامج الإقلاع على القرص (Boot Sector) ، وإتلاف محتوياته والعبث بها، ما يؤدي إلى تعطل عملية الإقلاع.

2- فيروس الملفات : File Infector Virus

يهاجم هذا النوع نظام التشغيل، وأي برامج أخرى موجودة على الكمبيوتر، كالتطبيقات المكتبية والألعاب وغيرها، ويعمل على العبث بمحتويات الملفات التي تنتهي بامتداد bin, com sys, exe, وتدميرها.

3- فيروسات الماكرو : Macro Viruses

تصيب هذه الفيروسات برامج التطبيقات المكتبية مثل مايكروسوفت وورد أو أكسل.
وهي من أكثر أنواع الفيروسات انتشاراً واستخداماً في عمليات التسلل إلى كمبيوترك عبر التطبيقات.

4- الفيروسات المتعددة الملفات :

تنسخ هذه الفيروسات نفسها في صيغة أولية ثم تتحول إلى صيغ أخرى لتصيب ملفات أخرى.

5- الفيروسات الخفية (الأشباح) :

وهذه فيروسات مخادعة.. إذ أنها تختبئ في الذاكرة ثم تتصدى لطلب تشخيص وفحص قطاع التشغيل، ثم ترسل تقرير مزيف إلى السجل بأن القطاع غير مصاب.

6- الفيروسات متعددة القدرة التحوليّة :

وهذه الفيروسات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الإنتقال من ملف إلى آخر، لكي يصعب اكتشافها.

من خصائص الفيروسات :

1- الإنتشار :

يتميز الفيروس أيضاً بقدرة هائلة على الإنتشار .. وقد سبق وأن قدمت العوامل التي تساعده في ذلك ..

2- القدرة على التخفي :

للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الإرتباط ببرامج أخرى كما تم أيضاً تزويد الفيروسات بخاصية التوميه والتشبّه حيث أن الفيروس يرتبط ببرنامج يقوم بأعمال لطيفة أو له قدرة عرض أشياء مثيرة، وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه.

3- القدرة التدميرية :

تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين (كفيروس تشرنوبل).

طرق الوقاية من الفيروسات:

1- تجهيز عدة نسخ من البرمجيات وحفظها بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرنامج عند الحاجة .

2- الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج المعدلة إلى البيئة الإنتاجية , وبخاصة تلك البرامج المجلوبة من خارج المؤسسة .

3-يجب توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية, فهذا هو أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة .

4-عند فحص البرمجيات أو اختبارها قبل السماح بنشرها في المؤسسة للاستخدام العام , يجب ان يتم ذلك على جهاز مستقل غير مرتبط بالشبكة.

5- تركيب برنامج للتحقق من وجود فيروسات ويفضل ان يكون هذا البرنامج دائم الوجود في الذاكرة , وهذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة لها, ولذلك فهي تكون عديمة الفائدة في مواجهة الفيروسات الجديدة, وبعض هذه البرامج يقوم بمقارنة محتويات بعض مناطق القرص (الصلب او المرن) أو بعض مناطق الذاكرة بمحتوياتها المتوقعة والمفترض أن توجد بها والإبلاغ عن أي تغيير فيها مما قد ينبئ عن وجود فيروس .

6-ويجب عدم إجازة البرامج للاستخدام العام في المؤسسة إلا بعد اجتيازها بنجاح هذه الاختبارات.

برامج الحماية من الفيروسات

توجد العديد من برامج الحماية من الفيروسات لكن أفضلها وأشهرها على الإطلاق هما هذان البرنامجان :

- برنامج النورتون أنتي فايرس Norton Antivirus

- برنامج مكافي Mcafee

وهذان البرنامجان هما الأفضل والأقوى في دنيا مكافحة الفيروسات وخصوصاً مع التحديث الدائم لهما ولتعريفات الفيروسات من خلال الإنترنت لأن التحديث الدائم للبرنامج يتيح له الفرصة في التعرف على الفيروسات الجديدة ومن ثم منعها من إحداث أي ضرر بالجهاز ..
وكنصيحة شخصية أنصح الأصدقاء الأعزاء باستخدام برنامج .