فيروسات الكمبيوتر
أولاً :ما هي الفيروسات :

هي برنامج أو جزء في الشفرة التي تدخل إلى الحاسب الألي لهدف التخريب وتتميز بقدرتها على نسخ نفسها إلى نسخ كثيرة وقدرتها على الانتقال من مكان إلى مكان ومن حاسب إلى حاسب والاختفاء وتغطية محتوياتها .
ثانياً : مما يتكون الفيروس؟
1) برنامج فرعي ليصيب البرامج التنفيذية ..
2) برنامج فرعي لبدء عمل الفيروس ..
3) برنامج فرعي لبدء التخريب ..
ثالثاً: أنواعها :
1) يبدأ عمل الفيروس التخريبي إذا تحقق شرط معين كتاريخ - أو فتح برنامج أو انتقال من نظام إلى نظام.
2) يبدأ عمل الفيروس التخريبي بمجر التشغيل الحاسب وتعمل على نسخ نفسها لإعادة تشغيلها.
3) يبدأ عمل الفيروس التخريبي بمجرد الانتقال ولمرة واحدة .
رابعاً: مكان الإصابة بالفيروسات :
1) فيروسات قطاع التشغيل (Boot Sector Virus)وهو الذي ينشط في منطقة نظام التشغيل وهو من اخطر أنواع الفيروسات حيث انه يمنعك من تشغيل الجهاز
2) فيروسات الماكرو (Macro Virus)وهي من أكثر الفيروسات انتشارا حيث أنها تضرب برامج الأوفيس و كما أنها تكتب بالورد او 3) فيروسات الملفات (File Virus)وهي تنتشر في الملفات وعند فتح أي ملف يزيد انتشارها ..4) الفيروسات المخفية (Steath Virus)وهي التي تحاول آن تختبئ من البرامج المضادة للفيروسات و لكن سهل الإمساك بها
5) الفيروسات المتحولة (Polymorphic virus)وهي الأصعب على برامج المقاومة حيث انه صعب الإمساك بها وتتغير من جهاز إلي آخر في أوامرها ..ولكن مكتوبة بمستوى غير تقني فيسهل إزالتها.
6) فيروسات متعددة الملفات (Multipartite Virus)
تصيب ملفات قطاع التشغيل و سريعة الانتشار ..7) فيروسات الدودة (Worm)
وهو عبارة عن برنامج ينسخ نفسه على الاجهزه و يأتي من خلال الشبكة و ينسخ نفسه بالجهاز عدة مرات حتى يبطئ الجهاز وهو مصمم لإبطاء الشبكات لا الأجهزة و بعض الناس تقول انه هذا النوع لا يعتبر فيروس حيث انه مصمم للإبطاء لا لأزاله الملفات و تخريبها ..
الباتشات (Trojans)
وهو أيضا عبارة عن برنامج صغير قد يكون مدمج مع ملف آخر للتخفي عندما ينزله شخص و يفتحه يصيب ال Registry و يفتح عندك منافذ مما يجعل جهازك قابل للاختراق بسهوله و هو يعتبر من أذكى البرامج فمثلا عند عمل سكان هناك بعض التورجن يفك نفسه على هيئة ملفات غير محدده فيمر عليها السكان دون التعرف علية و من ثم يجمع نفسه مره ثانيه.
خامساً : خطوات عمل الفيروس :
تختلف طريقة العدوى من فايروس لأخر و من نوع لأخر و هذا شرح مختصر لكيفية عمل الفيروسات : -
1) تحدث العدوى لبرنامج تنفيذي و لن تشعر باي تغيير فيه .
2) عندما يبدأ البرنامج المصاب بالعمل يبدأ نشاط الفيروس كما يلي : -أ- ينفذ البرنامج الفعلي الخاص بالبحث , فيبحث الفيروس عن البرامج ذات الامتداد .exe او .com أو أن واجد أي منها يحضر جزء صغير من بداية البرنامج إلى الذاكرة و من ثم يبحث عن علامته فان وجدها ترج البرنامج و بحث عن غيره و إذا لم يجدها يضعها في أول البرنامج .ب- بعد ذلك تكون حدثت العدوى فتحدث عملة التخريب التي تسبب الأخطاء عند عمل البرنامج المصاب .
3) بعد ذلك يعود التحكم للبرنامج مره أخرى (بعد ان كان الفيروس يتحكم فيه) ليبدو انه يعمل بصورة طبيعية .
4) بعد ذلك تكون عملية العدوى انتهت يتم التخلص من الفيروس الموجود في الملف التنفيذي الأول حيث أن الفيروس قد انتشر في البرامج الأخرى .
سادساً: ما هو تأثير الفيروس :
1) تباطؤ أداء الكمبيوتر ، أو حدوث أخطاء غير معتادة عند تنفيذ البرنامج .
2) زيادة حجم الملفات ، أو زيادة زمن تحميلها إلى الذاكرة .
3) سماع نغمات موسيقية غير مألوفة .
4) ظهور رسائل أو تأثيرات غريبة على الشاشة .
5) زيادة في زمن قراءة القرص إذا كأن محمياً وكذلك ظهور رسالة FATALI/O ERROR
6) تغيير في تاريخ تسجيل الملفات كما في فيروس Vienna الذي يكتب 62 مكان الثواني .
7) حدوث خلل في أداء لوحة المفاتيح كأن تظهر رموز مختلفة عن المفاتيح التي تم ضغطها كما في فيروس Haloechon أو حدوث قفل للوحة المفاتيح كما في فيروس Edv.
نقص في مساحة الذاكرة المتوفرة كما في فيروس Ripper الذي يحتل 2 كيلو بايت من أعلى الذاكرة الرئيسة . ويمكن كشف ذلك بواسطة الأمر MEM أو CHKDSK .
9) ظهور رسالة ذاكرة غير كافية لتحميل برنامج كأن يعمل سابقاً بشكل عادي .
10) ظهور مساحات صغيرة على القرص كمناطق سيئة لا تصلح للتخزين كما في فيروس Italan وفيروس Ping Pong اللذين يشكلان قطاعات غير صالحة للتخزين مساحاتها كيلوبايت واحد .
11) تعطيل النظام بتخريب قطاع الإقلاع BOOT SECTOR
12) إتلاف ملفات البيانات مثل ملفات وورد واكسل …… وغيرها .
سابعاً : ما هي مراحل العدوى ؟
1) مرحلة الكمون : حيث يختبأ الفيروس في الجهاز لفترة ..
2) مرحلة الانتشار : و يبدأ الفيروس في نسخ نفسه والانتشار في البرامج وأصبتها ووضع علامته فيها ..3) مرحلة جذب الذناد: و هي مرحلة الانفجار في تاريخ معين او يوم .. مثل فيروس تشرنوبيل ..4) مرحلة الأضرار : و يتم فيها تخريب الجهاز ..ثامناً: كيف تنتقل أو تصيب الأجهزة :1) تشغيل الجهاز بواسطة اسطوانة مرنه مصابه.
2) تنفيذ برنامج في اسطوانة مصابه .
3) نسخ برنامج من اسطوانة مصابة بالفيروس إلى الجهاز .
4) تحميل الملفات أو البرامج من الشبكات أو الإنترنت
5) تبادل البريد الإلكتروني المحتوي على الفيروسات (attachments). .
6) فلاشات الميمورى والميمورى كاردس.

تاسعاً : الإجراءات الواجبة عند اكتشاف الإصابة بالفيروسات :
1) تصرف بهدوء وبدون استعجال لئلا تزيد الأمر سوءاً ولا تبدأ بحذف الملفات المصابة أو تهيئة الأقراص .
2) لا تباشر القيام بأي عمل قبل أعداد وتدقيق خطة العمل التي تبين ما ستقوم به بشكل منظم .
3) أعد إقلاع جهازك من قرص نظام مأمون ومحمي وشغل أحد البرامج المضادة للفيروسات التي تعمل من نظام دوس ومن قرص لين ولا تشغل أي برنامج من قرصك الصلب .
4) أفحص جميع الأقراص اللينة الموجودة لديك مهما كأن عددها لعزل الأقراص المصابة من السليمة .عاشراً: الوقاية من الإصابة بالفيروسات :
1) فحص جميع الأقراص الغريبة أو التي استخدمت في أجهزة أخرى قبل استعمالها .
2) تهيئة جميع الأقراص اللينة المراد استخدامها على جهازك .3) عدم تنفيذ أي برنامج مأخوذ من الشبكات العامة مثل إنترنت قبل فحصه .
4) عدم إقلاع الكمبيوتر من أي قرص لين قبل التأكد من خلوه من الفيروسات .5) عدم ترك الأقراص اللينة في السواقة عند ما يكون الجهاز متوقفا عن العمل .
6) التأكد من خلو سواقة الأقراص اللينة قبل إعادة إقلاع الجهاز .
7) عدم تشغيل برامج الألعاب على الجهاز ذاته الذي يتضمن البيانات والبرامج الهامة .
حماية الأقراص اللينة ضد الكتابة لمنع الفيروسات من الانتقال إليها .
9) استخدام برامج أصلية أو مرخصة .
10) استخدام كلمة سر لمنع الآخرين من العبث بالكمبيوتر في غيابك .
11) الاحتفاظ بنسخ احتياطية متعددة من جميع ملفاتك قبل تجريب البرامج الجديدة .
12) تجهيز الكمبيوتر ببرنامج مضاد للفيروسات واستخدامه بشكل دوري .
13) تحديث البرامج المضادة للفيروسات بشكل دائم لضمان كشف الفيروسات الجديدة .
14) الاحتفاظ بنسخة DOS نظيفة من الفيروسات ومحمية ضد الكتابة لاستخدامها عند الإصابة.
15) الانتباه للأقراص اللينة الواردة من المعاهد والكليات ( الأماكن التقليدية للفيروسات ) .
15) إغلاق الجهاز نهائياً وإعادة تشغيله عند ظهور عبارة non bootable diskette .‏