المحاضرة الثالثة

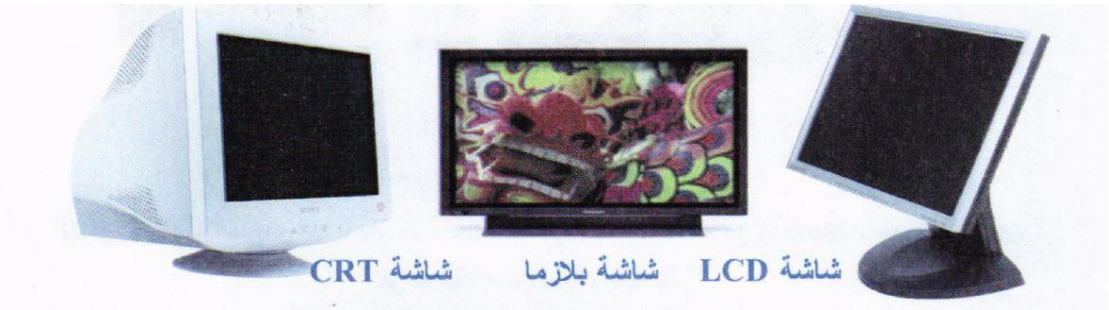
فيروس الحاسوب

اجهزة الاخراج (Output Devices)

هي الاجهزة التي تعمل على اظهار المعلومات الناتجة من الحاسوب بصورة يمكن فهمها من قبل المستخدم, وتوجد اشكال عديدة من اجهزة الاخراج وحسب نوع المعلومات (نص, صورة, صوت, الخ) ومن اهمها:

١- وحدة العرض البصري (الشاشة Monitor):

وهي شاشة مشابهة لشاشة التلفزيون ولكنها تعرض صور اكثر وضوحا. وتسمى جهاز الاخراج الاساسية Standard Output Device وتستخدم لاخراج البيانات بصورة مرئية, وكمثال عليها شاشة انبوب الشعة الكاثودية CTR (Cathode Ray Tube) وشاشة الكريستال LCD (Liquid Crystal Display) وشاشة البلازما (Plasma) وتمتاز بوزن وحجم اقل وكلفة اكثر من الاولى. وان زيادة عدد النقاط في الشاشة يؤدي الى دقة الصور التي تتمكن الشاشة من عرضها.



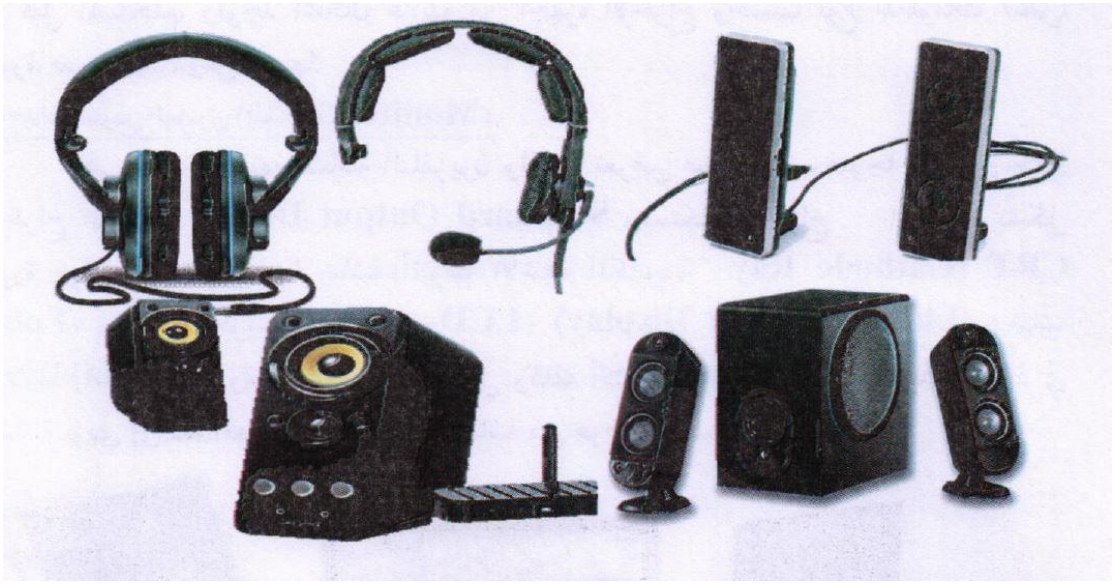
شكل ١: نماذج من شاشات العرض

٢- السماعات Speakers

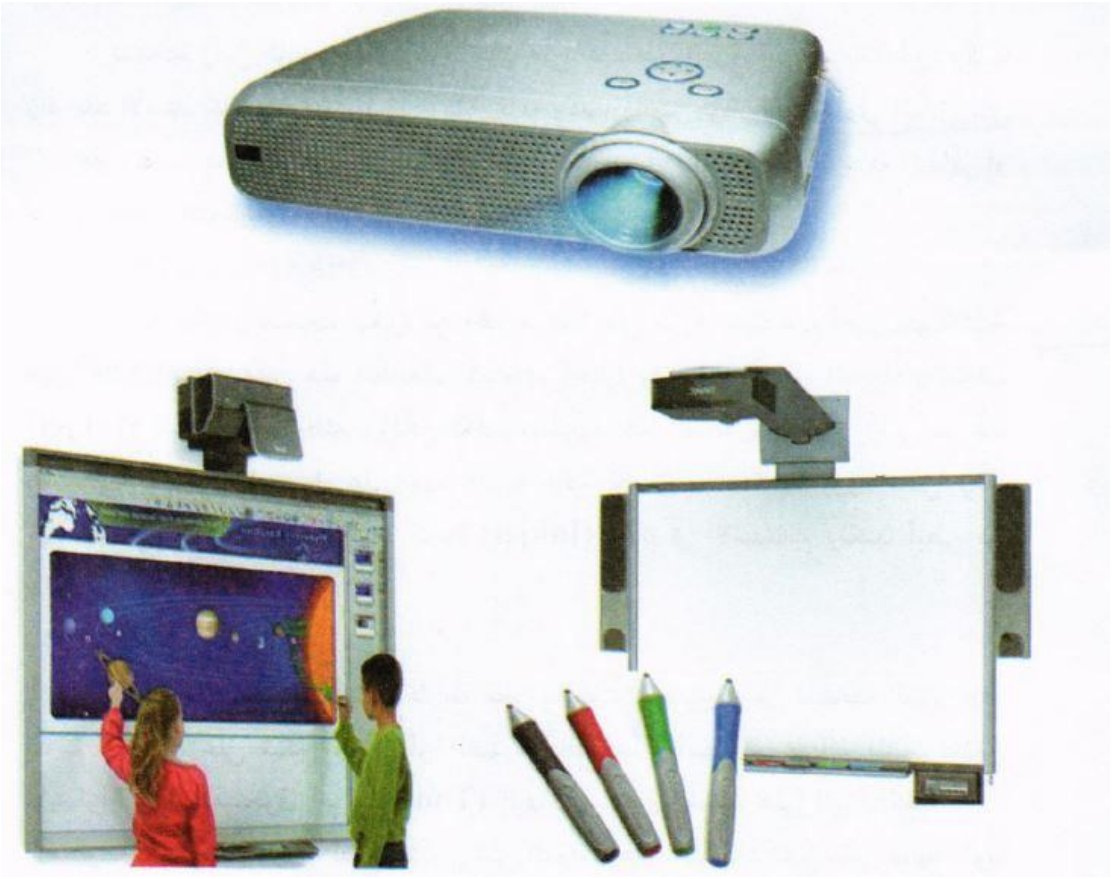
السماعات هي جزء اساسي في الحواسيب الحديثة المستخدمة في المنزل. اما في التعليم فسماعات الراس تناسب حجرات الدراسة حتى لا تحدث ضوضاء. عن طريقها يتم اخراج البيانات من الحاسوب على هيئة مسموعة, وتحتوي بعض السماعات على مضخم صوت يقوم بتكبير الاشارة الصوتية القادمة من الحاسوب ويزيد من وضوح الصوت. وهناك السماعات المنضدية التي تربط مع الحاسوب المكتبي وتضع على المنضدة. وتكون ضمنا في الحواسيب المحمولة, وسماعات الراس (Headphones).

٣- عارض الفيديو Video Projector واللوحة الذكية (Smart Board)

يستخدم عارض الفيديو (او عارض البيانات) لاخراج المعلومات من نصوص وصور وافلام على شاشة خارجية اكبر. كما تستعمل اللوحة او السبورة الذكية مباشرة لاظهار المعلومات مع امكانية الكتابة عليها.



شكل ٢ : انواع من السماعات: سماعات منضدية, سماعات راس مع لاقط صوت, سماعات تتكون من ثلاثة اجزاء, سماعات لاسلكي



شكل٣: عارض الفيديو و اللوحة الذكية التي تعمل باستخدام الاقلام او باللمس

٤- الطابعات Printers:

تستخدم لاخراج المعلومات على الورق باشكال مختلفة تسمى بالنسخة الورقية Hard Copy وتوجد انواع عديدة منها, تختلف حسب سرعتها وباسلوب الطباعة وبنوع الورق المستخدم. ومن تلك الطابعات.

أ- طابعات محفورة (Daisy Wheel)

الحروف محفورة على جزء معدني او بلاستيك مع شريط كربون. يمكن طباعة الحروف على الورق بالضرب على شريط الحبر والكربون, وبذلك يمكن عمل نسخ كربون. وهي طابعات بطيئة وصوتها مزعج تستخدم مثل الالات الكاتبة الكهربائية.

ب- طابعات نقطية (Dot Matrix)

تستخدم راس طابع باسنان لانتاج نقاط على الصفحة بالطرق على شريط الحبر. وكلما زاد عدد الاسنان زاد عدد طرق منطقة محددة وكلما زادت جودة الطباعة, وفي المقابل تقل السرعة. وتصدر هذه الطابعات نوعا من الازعاج. وتستخدم هذه الطابعات في طباعة التذاكر او كوبون المحلات التجارية.

جـ: طابعات ضخ الحبر (Inkjet)

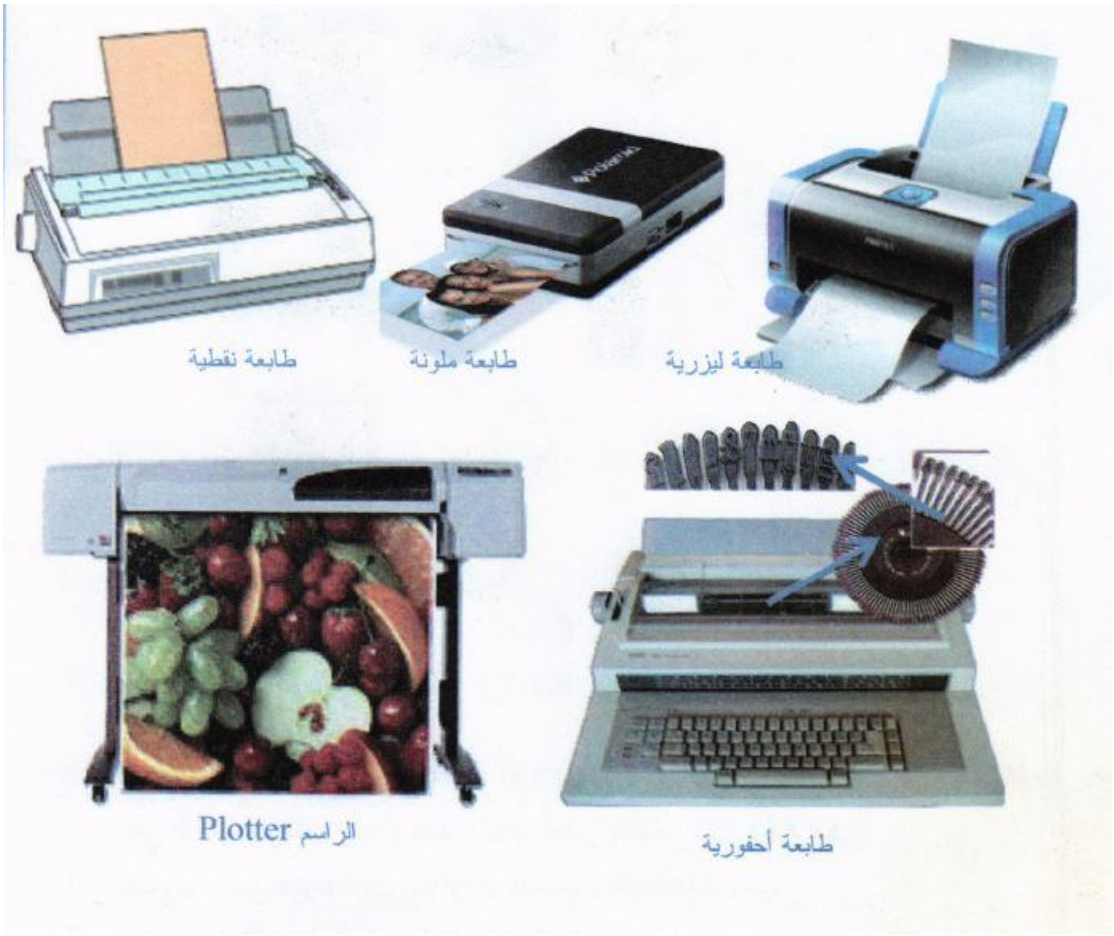
تعمل باطلاق ضخات صغيرة من الحبر مباشرة على الورق وتستخدم احبار ملونة تنتج صور عالية الجودة. بعض هذه الطابعات تستخدم احبار سوداء للنصوص العادية. وطابعات (Inkjet) ليست مرتفعة الثمن ولكن تكلفة تشغيلها عالية, اذ يجب تغيير الحبر بعد عدة مئات من النسخ, وللحصول على جودة طباعة عالية فانه يجب استخدام ورق خاص وهذا يضاعف من تكاليف تشغيلها. تعد طابعة (Inkjet) هادئة في الاستخدام ولكنها ابطئ من طابعات الليزر.

د- طابعات الليزر (Laser)

تعمل تلك الطابعات بنفس طريقة عمل ماكينات التصوير, وهي تستخدم الليزر لرفع شحنة كهربائية على شكل النص او الصورة لتطبع على اسطوانة. المنطقة المشحونة من الاسطوانة تجذب مسحوق اسود (Toner) اليها والمسحوق يضغط على الورق كلما دارت الاسطوانة. ثم تسخن الورقة لطبع الشكل على الورقة. وهذه الطابعات تنتج صور عالية الجودة تستخدم اللون الابيض والاسود تكون تكلفة طابعة الليزر بالالوان ضعف او ثلاث اضعاف طابعة الابيض والاسود. يرتفع سعر طابعات الليزر عن الطابعات الاخرى ولكنها اسرع وذات فائدة في الاعمال التي تحتاج الى طباعة كميات كبيرة. وهي لا تحدث ضوضاء اثناء الطباعة, ويمكن طباعة ٥٠٠٠ صفحة قبل الحاجة الى تغيير اسطوانة الطباعة او اعادة مليء الحبر الاسود المستخدم.

هـ - الراسم (Plotter)

هي نوع خاص من الطابعات تستخدم عادة في برامج (CAD) وخرائط البرامج ويستخدم سنون مباشرة على الورق وباستخدامهم يمكن رسم لوحات فنية معقدة وباكثر من لون. ويشبه شكلها الى حد كبير الطابعة. ويستخدم لاخراج النتائج على شكل رسوم (مثل الخرائط والاعلانات) وبدقة عالية. وتستخدم في طباعة اللافتات القماشية والبلاستيكية والزجاجية الخاصة بالاعلانات.



شكل٤: انواع من الطابعات

فيروس الحاسوب

فيروس الحاسوب هو برنامج خارجي صنع عمدا بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

يتصف فيروس الحاسوب بأنه :

١ برنامج قادر على التناسخ Replication والانتشار .

٢ الفيروس يربط نفسه ببرنامج أخر مسمى الحاضن host.

٣ لا ممكن أن تنشأ الفيروسات من ذاتها .

٤ ممكن أن تنتقل من حاسوب مصاب لاخر سليم .

يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي

- آلية التناسخ The Replication Mechanism

وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه .

- آلية التخفي The Protection Mechanism

وهو الجزء الذي يخفي الفيروس عن الاكتشاف .

- آلية التنشيط The trigger Mechanism

وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس (Michelangelo) الذي ينشط في السادس من آذار من كل عام .

- آلية التنفيذ The Payload Mechanism

وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه .

للوقاية من الفيروس

١ - استخدام برامج للكشف عن الفيروسات في الجهاز .

٢ - احتفظ بنسخ احتياطيه من البرامج والملفات الموجودة على الجهاز .

٣ - إجرا الفحص على البرامج المحملة (المنزلة) أو المنقولة من شبكة الإنترنت قبل تشغيلها .

٤ - استخدام برمجيات الجدار الناري .

٥ - استخدام نظام التشغيل جنو/لينكس فهو يعتبر اكثر أمانا و فيه فيروسات قليلة عكس نظام التشغيل وندوز .

٦ - لا تشغل أي برنامج أو ملف لا تعرف ما هو بالضبط

اللغات التي يكتب بها الفيروس

من أهم اللغات التي يكتب بها كود الفيروس هي لغة التجميع اسمبلي لسهولة الوصول لعتاد الحاسوب وهنالك أيضا اللغات الراقية مثل لغة سي ولغة سي ++ وفيجوال سي وفيجوال بيسك .

طرق انتقال الفيروسات (العدوى)

ممكن أن نميز فئتين من فيروسات الحاسوب تبعا لالية العدوى وانتشار الفيروس :

١- فيروس العدوى المباشر Direct Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع, فان ذلك الفيروس يبحث بنشاط عن ملف أو اكثر لينقل العدوى إليه, وعندما يصاب أحد الملفات بالعدوى فانه يقوم بتحميله إلى الذاكرة وتشغيله, وهذا النوع قليل الانتشار.

٢- فيروس العدوى غير المباشر Indirect Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع, فان 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 التغذية الكهربائية عن الحاسوب أو إعادة تشغيله .

أسباب التسمية

سمي الفيروس (Virus) بهذا الاسم لأنها تشبه تلك الكائنات المتطفلة في صنفتين رئيسيتين:

اولا : فالفيروسات دائما تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أيضا

ثانيا : تتواجد الفيروسات في مكان أساسي في الحاسوب كالذاكره رام وتصيب اي ملف يشتغل في أثناء وجودها بالذاكره مما يزيد عدد الملفات المصابه كلما طال وقت اكتشاف الفايروس. تستخدم عادة لغة التجميع (الاسمبلي) لكتابة كود تنفيذ الفيروس.

أنواع الملفات التي يمكن ان يصيبها الفيروس

بشكل عام الفيروس تصيب الملفات التنفيذية أو الملفات المشفرة غير النصية مثل التالية :

١- الملفات ذاتية التنفيذ مثل ملفات ذات امتداد (.COM, EXE) ضمن أنظمة

التشغيل دوس وميكروسوفت و وندوز , أو (ELF) في أنظمة لينكس .

٢- سجلات الملفات والبيانات (VOLUME BOOT RECORD) في الأقراص المرنة والصلبة والسجل رقم (٠) في القرص الصلاب MASTER BOOT

٣- ملفات الأغراض العامة مثل ملفات الباتش والسكريبت في وندوز وملفات الشل في يونيكس .

٤- ملفات الاستخدام المكتبي في نظام تشغيل مايكروسوفت و وندوز التي تحتوي ماكرو مثل مايكروسوفت وورد ومايكروسوفت إكسل ومايكروسوفت أكسس .

٥- قواعد البيانات وملفات الاوتولوك لها دور كبير في الاصابة ونشر الاصابة لغيرها لما تحويه من عناوين البريد الالكتروني .

٦- الملفات من النوع (PDF) وبعض نصوص HTML احتمال احتوائها على كود خبيث .

٧- لملفات المضغوطة مثل ZIP و .RAR

٨- ملفات .MP3

طرق الانتقال

أهم طرق الانتقال الان هي الشبكة العنكبوتية الإنترنت تكون وسيلة سهلة لانتقال الفيروسات من جهاز لاخر ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات ياتي ثانيا وسائط التخزين مثل ذواكر الفلاش والأقراص الضوئية والمرنة سابقا وياتي أيضا ضمن رسائل البريد الإلكتروني وأيضا تنتقل الفيروسات إلى نظام عند استلامه ملفات اي كانت الملفات مخزنة على (اقراص مرنة أو اقراص مضغوطة أو اقراص ,zip)

أعراض الإصابة

١- تكرار رسائل الخطأ في أكثر من برنامج .

٢- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة .

٣- تكرار اختفاء بعض الملفات التنفيذمة .

٤- حدوث بطئ شديد في إقلاع (نظام التشغيل) أو تنفيذ بعض التطبيقات. رفض بعض التطبيقات للتنفيذ .

٥- فعند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في قرص صلب أو المرن, لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر, بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الايميل أوإنترنت أو تبادل الأقراص المرنة.

تعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجة هناك فيروسات تعمل على خلق رسائل مزعجة وأنواع تعمل على تشغيل برامج غير مطلوبة وأنواع تعمل على اشغال المعالج بحيث تبطئ سرعة الحاسوب أو سرقة بيانات من حاسوب المستخدم مثل ارقام حسابات وكلمات السر أو ارقام بطاقات الائتمان وبيانات مهمة أخرى وهذه أهم اهداف الفيروسات الحديثة وبرامج التجسس التي يتم تطويرها يوما بعد يوم.

أنواع الفيروسات من حيث الانتشار

من حيث النوع

أنواع الفيروسات ثلاثة :(الفيروس والدودة وحصان طروادة) ما الفرق بين الفيروس والدودة وحصان طروادة؟

الفيروس : ممكن القول بأنه برنامج تنفيذي (ذات نوع scr,.pif,.bat,.exe .com.) يعمل بشكل منفصل ويهدف إلى أحداث خلل في نظام الحاسوب وتتراوح خطورته حسب مهمته فمنه الخطير ومنه الخفيف وكلاهما خبيث. وينتقل بواسطة نسخ الملفات من جهاز به ملفات مصابة إلى جهاز اخر عن طريق الأقراص المدمجة سي دي وذواكر الفلاش .

الدودة (ديدان الحواسيب) : فيروس ينتشر فقط عبر الشبكات والإنترنت ويعمل على الانتشار على الشبكات عن طريق دفتر عناوين البريد الإلكتروني مثلا فعند اصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص

وهكذا... مما مؤدي إلى انتشاره بسرعه عبر الشبكه وقد اختلف الخبراء فمنهم اعتبره فايروس ومنهم من اعتبره برنامج خبيث وذلك كون الدوده لاتنفذ اي عمل مؤذي انما تنتشر فقط مما يؤدي إلى اشغال موارد الشبكه بشكل كبير ومع التطور الحاصل في ميدان الحوسبه أصبح بامكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدوده بحيث تؤدي عمل معين بعد انتشارها (مثلا بعد الانتشار إلى عدد ٥٠٠٠٠ جهاز يتم تخريب الأنظمة في هذه الأجهزة) أو اي شي اخر (مثلا في يوم معين أو ساعة أو تاريخ...الخ)

وأصبحت الديدان من أشهر الفيروسات على الشبكه العالميه واشهر عملياتها التخريبيه واخطرها تلك التي يكون هدفها حجب الخدمه تسمى (هجمات حجب الخدمه) حيث تنتشر الدوده على عدد كبير من الأجهزة ثم توجه طلبات وهميه لجهاز خادم معين) يكون المبرمج قد حدد الخادم المستهلك من خلال برمجته للدوده) فيغرق الخادم بكثرة الطلبات الوهميه ولا يستطيع معالجتها جميعا مما يسبب توقفه عن العمل وهذه الديدان استهدفت مواقع لكثير من الشركات العالميه اشهرها مايكروسوفت وغيرها الكثير.

حصان طروادة :Trojan Horseسمي هذا الفيروس بحصان طروادة لانه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طرواده والتغلب على جيشها وهكذا تكون الية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج دون أن يعلم المستخدم. فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما حيث تم توزيع قرص مجاني على المشافي به برنامج حول مرض التهاب الكبد الفيروسي (أسبابه طرق - انتشاره طرق العلاج .. الخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسيب الحاضنه للفايروس وظهرت رساله مفادها ان الحاسب مصاب بالمرض (المقصود هنا انه تم تشفير ملفات الحاسب وايقافها عن العمل بطريقه نظاميه) ارسل مبلغ كذا إلى الحساب كذا ليتم إرسال رقم فك الشيفره مما اجبر المختصين بالرضوخ للطلب كونهم لم يستطيعو فك التشفير.

من حيث السرعة

توجد عدة تقسيمات للفيروسات، فمثلا من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فهناك فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعا ، وفيروسات الماكرو macroالتي تختص باصابة الوثائق والبيانات الناتجة عن حزمة مامكروسوفت أوفيس، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة طبعا لايوجد فايروسات خارقه بحيث انها تدمر الأجهزة كما نسمع أحيانا (احترق المعالج بسب الفايروس, تعطلت وحدة التغذيه بسب الفايروس أو تلفت الشاشة بسبب الفايروس ،... الخ) ولكن ممكن للفايروس ان يؤذي الذاكره روم في الحاسب كما في فايروس تشرنوبل أو ان يمحي معلومات ال (MBR (Main Boot Sectorعلى القرص الصلب فتعود الأقراص الصلبه كما اتت من المصنع وفي الحالتين السابقتين لا يتم اقلاع الجهاز مما يوحي للبعض ان الفايروس (حرق) الحاسب طبعا هذه الفيروسات تعتبر خطيره جدا لانها تتسبب في اتلاف البيانات المخزنه والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤدي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبل مما مؤدي إلى توقف الخدمات المقدمه، وهنال أيضا الفيروسات المدمرة للبرامج وتاثيرها محدود طالما ان البيانات لم تتاثر حيث يمكن تخزين البيانات واعادة تهياة الحاسب واعادة البرامج المتضرره من اقراصها الاصليه، والفيروسات عديمة الضرر وهي التي لاتقوم باي عمل مؤذي وانما تم برمجتها لاثبات الذات والقدره على البرمجه من بعض المراهقين فمنها ما يرسم كرة أو اي شكل على الشاشه طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الاحرف (كتغيير حرف بحرف اينما وجد) أو تغيير مؤشر الماوس.. الخ .