6

الفصل السادس

البرمجيات الخبيثة (Malware)

البرمجيات الخبيثة (Malware)

- **البرمجيات الخبيثة (Malware):**
- هي اختصار لكلمتين هما (Malicious Software) ويُطلِق عليها البعضُ أحياناً اسمَ (Malcode) أو الشيفرة الخبيثة.

- وهي عبارة عن كود برمجي يعمل على إيذاء نظام الحاسب أو الشبكة الحاسوبية بالسيطرة عليه والسرقة والتحكم به أو تعطيله بشكل جزئي أو كلي.

- وتتراوح أذى البرمجيات الخبيثة من إزعاج بسيط كالدعابات والنوافذ الإعلانية إلى أذى كبير مثل تدمير البيانات والمعلومات وتعطيل بعض المكونات المادية.

تصنيف البرمجيات الخبيثة (Malware Type)

1. حصان طروادة– التروجان (Trojan Horse):
2. الديدان البرمجية (Worms):
3. برامج التجسس (Spyware):
4. الإعلانات المتسللة (Adware):
5. القنابل المنطقية (Logic Bombs):
6. القنابل الموقوتة (Time Bombs):
7. برمجيات الأبواب الخلفية (Backdoor Malware):
8. مسجل لوحة المفاتيح - الكى لوجر(Keylogger):
9. الفيروسات :(Viruses)

1- حصان طروادة - التروجان (Trojan)

- سمي بهذا الاسم نسبة للأسطورة الإغريقية الواردة في ملحمة (الاوديسا) لهوميروس , حيث ارسل الجيش الإغريقي حصانا خشبيا ضخما, كهدية لسكان طروادة .
- التروجان عبارة عن برنامج يغري المستخدم بأهميته فعندما تقوم بتحميله يتسلل إلى حاسبك و يقوم بفتح باب خلفي بمجرد تشغيله,
- التروجان لا يتكاثر مثل الدودة ولا يلحق نفسه ببرنامج مثل الفيروس ولا ينتشر أيضا سواء عن تدخل بشري أو لا.

2- الدودة (Worm)

- الدودة تصيب الكمبيوترات الموصلة بالشبكة بشكل أوتوماتيكي و من غير تدخل الإنسان
- غالباً تنتشر الديدان عن طريق الإيميل، وعندما يشغّل المرسل إليه الملف المرفق، تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.
- الديدان لا تقوم بحذف بيانات بل **تقوم بتهليك موارد الجهاز المخدم للشبكة** واشغال الذاكرة بشكل فظيع مما يؤدي إلى شلل المخدم والمواقع الإلكترونية المرتبطة معها.

3- برامج التجسس (Spyware)

- تقوم بجمع معلومات شخصية عن المستخدم من **كلمات السر ورقم البطاقة الائتمانية** وعن المواقع التي يزورها وتقوم بإرسالها بدون علمه إلى جهة معينة, لهدف التسويق أو التجسس .
- انتشارها: تنتشر عن طريق البرامج المجانية, كبرامج التسلية أو عن طريق تحميلها من الانترنت عبر بعض المواقع التي تطالب المستخدم بتنصيب برامج معينه كشرط لدخول الموقع.

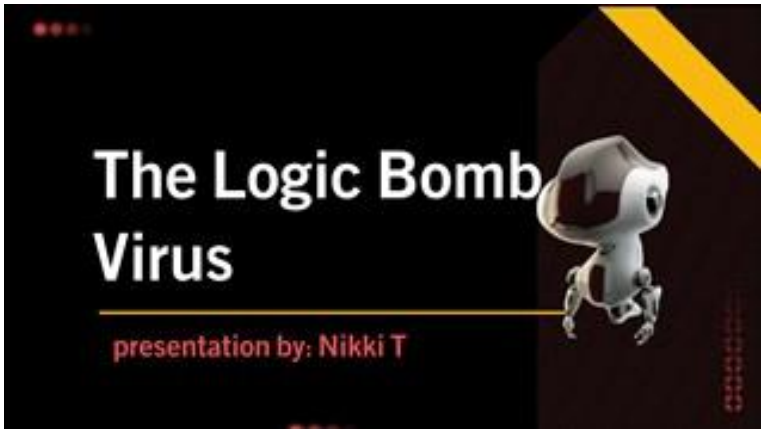
4- برامج الإعلانات المتسللة (Adware)

- هي برامج صغيرة الحجم ترتبط ببرامج مجانية حيث تقوم بتنصيب نفسها مع هذه البرامج أويتم تحميلها من بعض المواقع التي تقدم خدمات مجانية ومهمتها الأساسية إظهار الدعايات بشكل مستمر لمنتجات مختلفة.
- ياهو ماسنجر يحتوي على ادوير، ويقوم بتعقبك ليعرف اهتماماتك والصفحات التي تزورها لكي يعرض لك اعلانات تتناسب مع اهتماماتك، الادوير بشكل عام غير ضار.

5- القنابل المنطقية (Logic Bombs)

القنابل المنطقية (Logic Bombs):

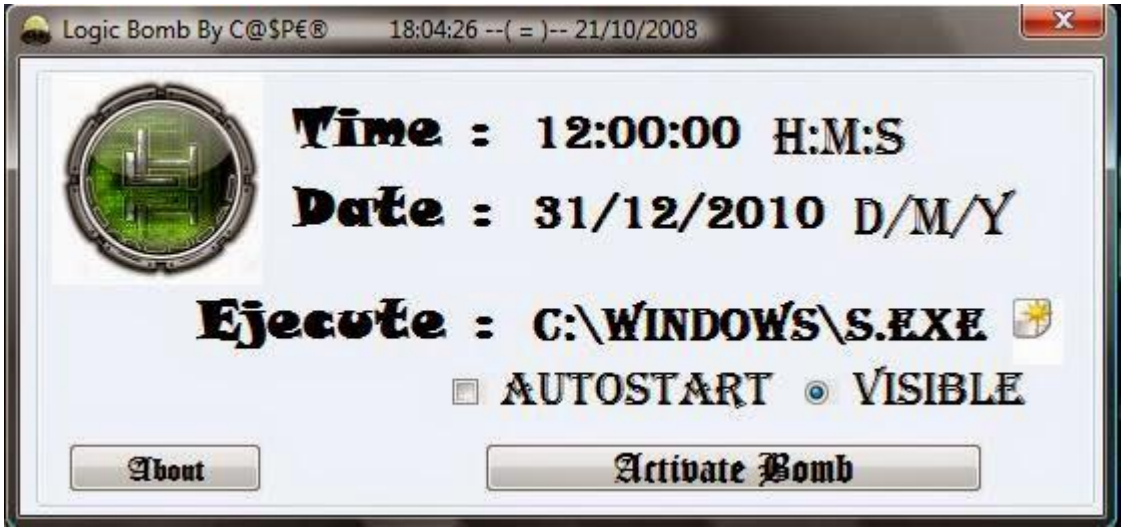
- هي أحد أنواع البرامج الخبيثة صمم ليعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين, فقد يتنفذ مثلا إذا تم رفع اسم المخرب (واضع القنبلة) من كشوف الراتب, وتؤدي القنبلة في هذه الحالة الى تخريب بعض النظم او الى مسح بعض البيانات أو تعطيل النظام عن العمل.



6- القنابل الموقوتة (Time Bombs)

القنابل الموقوتة (Time Bombs):

- القنبلة الموقوته هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين كأن تحدث مثلا عندما يوافق اليوم الثالث عشر من الشهر يوم الجمعة.



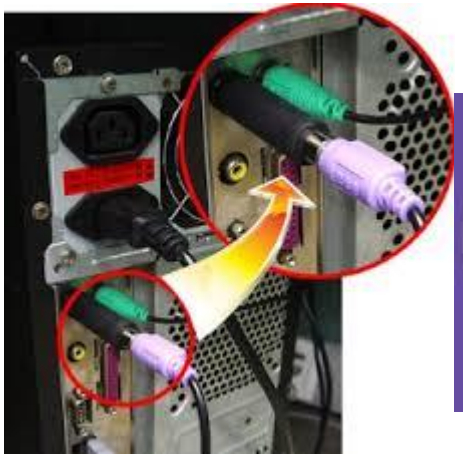
7- برمجيات الأبواب الخلفية (Backdoor Malware)

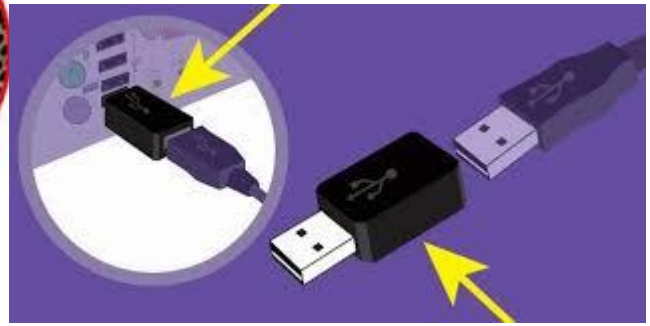
- هي عبارة عن وسيلةٍ غير موثوقة من أجل الوصول إلى النظام من خلال تجاوز آليات المصادقة العادية.
- تم وضعُ بعضٍ هذه الأبواب من قِبل المصمّمين الأصليين للبرامج، وتمَّ وضعُ البعض الآخر من خلال فايروس معين أو دودة .
- عادةً ما يستخدمُ المهاجمون هذه الأبواب للوصول السهل إلى النظام والتحكم به عن بعد .

8- مسجل لوحة المفاتيح - الكى لوجر (Keylogger)

مسجل لوحة المفاتيح - الكى لوجر(Keylogger):

- هو احد برامج التجسس يقوم المستخدم بتحميله من احد المواقع غير الموثوقة أو يكون ضمن البرامج المجانية بدون علم المستخدم ، ويقوم برنامج التجسس بنقل كل ما يكتب بلوحة المفاتيح إلى مرسل البرنامج أو مبرمجه، مثل كلمات السر أو أرقام بطاقات الائتمان أو أسماء المواقع التي يزورها المستخدم.





9- فيروسات الحاسب (Viruses)

- فيروسات الكومبيوتر هي برامج تتم كتابتها بطريقة معينة بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه.
- وضرر الفيروس يتراوح بين إظهار رسائل ترحيب طريفة أو حذف محتويات الذاكرة الدائمة ROM وحذف محتويات القرص الصلب.

Image courtesy of: Tech Tips.com

سُمّيت بالفيروسات، لأنها تشبه الفيروسات بصفتين رئيسيتين

- **تحتاج فيروسات الكومبيوتر دائماً إلى ملف عائل تعيش متستّرةً فيه:**

فالفيروسات، دائماً تتستر خلف ملف آخر، و لكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أولاً .

- **تستطيع فيروسات الكومبيوتر أن تنسخ نفسها:**

تتم كتابة هذه البرامج المؤذية بحيث تقوم بنسخ نفسها فوراً بمجرّد تشغيل البرنامج المصاب. و هي تنسخ نفسها للأقراص الأخرى، فإذا كان الكومبيوتر مصاباً ووضعت فيه قرصاً مرناً، يتم نسخ الفيروس أوتوماتيكياً للقرص المرن.

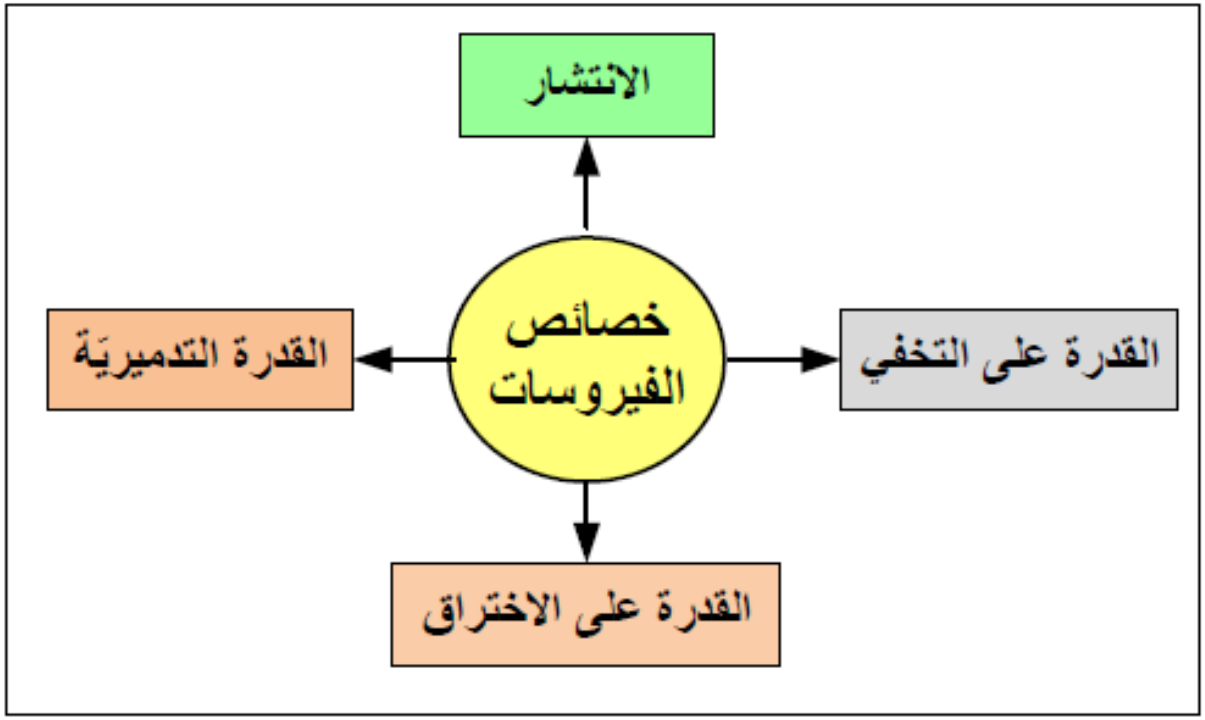
الفرق بين الدودة و التروجان و الفيروس

دائما يخلط البعض في المصطلحات فيسمي التروجان والدودة فيروساً. وهذا غير صحيح فالكلمات تروجان وفيروس ودودة هي مصطلحات تطلق على أنواع مختلفة من البرمجيات المؤذية للحاسب .

	الدودة	التروجان	الفيروس
الانتشار	تنتشر بشبكات الحاسب بشكل ذاتي دون تدخل بشري	لا يتكاثر ولا ينتشر لا بشكل ذاتي ولا بتدخل بشري	تنتشر بتدخل بشري او عن طريق المستخدم
طريقة انتقاله	بواسطة الإيميل وشبكات الحاسب	يتم تحميله من مواقع انترنيت	يلتصق بملف تنفيذي وينتشر
الأضرار	تقوم بتهليك موارد الجهاز أو المخدم و استخدام الذاكرة بشكل فظيع مما يؤدي إلى بطء ملحوظ جدا للجهاز.	يقوم بفتح باب خلفي ليمكن المخترق باختراق الجهاز. يحذف بعض الإيقونات على سطح المكتب. مسح بعض ملفات النظام. تغير الصفحة الرئيسية للإنترنت إكسبلورر.	مسح البيانات– إغلاق الحاسب– تغير خصائص الملفات– تخريب نظام التشغيل

خصائص فيروسات الحاسوب

تتميّـــــز فيروســـــات الحاســـــوب بعـــــدد مـــــن الخصـــــائص



مكوّنات برنامج الفيروس

يتكوّن برنامج الفيروس عامّةً من أربعة أجزاء رئيسيّة هي:

1. **آليّة التناسخ :** وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.
2. **آليّة التخفّي :** وهو الجزء الذي يخفي الفيروس عن الاكتشاف.
3. **آليّة التنشيط:** وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يتمّ تشغيله، كاستخدام توقيت الساعة في الحاسوب
4. **آليّة التنفيذ** :وهو الجزء الذي ينفذ الفيروس عندما يتمّ تنشيطه.

أنواع الفيروسات

1- فيروسات قطاع الاقلاع (Boot Sector Viruses):

وهي الفيروسات التي تتوضع في ملفات الإقلاع، و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول إلى النظام ويمنعه من إقلاع الجهاز.

2- فيروسات البرامج:

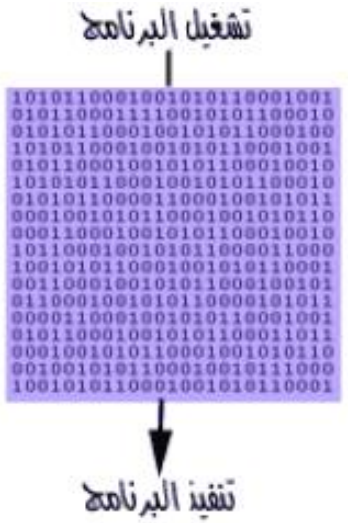
تلصق هذه الفيروسات نفسها بملفات البرامج التنفيذية من نوع .bat أو .exe أو .sys وغيرها وتكون العدوى بهذا النوع فعالة وسريعة .

3- الفيروسات الماكروية:

هذه الفيروسات تصيب برامج الوورد و الاكسل, يقوم هذا النوع من الفيروسات بتغيير بعض المستندات مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد , أو إضافة كلمات جديدة لا علاقة لها بالموضوع . هي اساساً ليست ضارة, لكنها مزعجة.

طريقة عمل الفيروس والتصاقه بالبرنامج

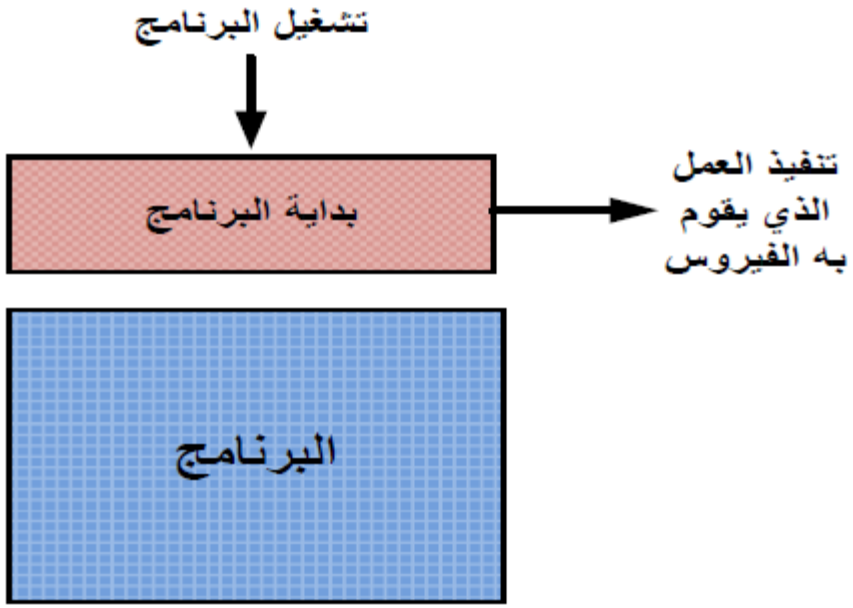
- في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. لننظر للصورة التالية التي توضّح شكل البرنامج غير المصاب بفيروس :



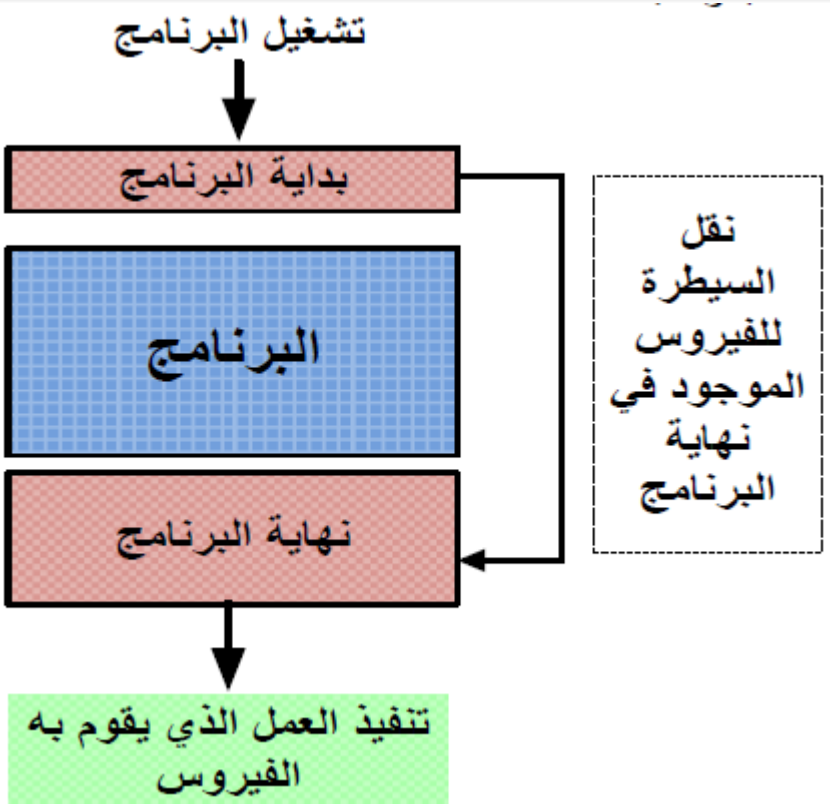
نلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.

1- التصاق الفيروس في بداية الملف

- في هذه الحالة يلصق الفيروس نفسه في البرنامج دون أن يغير في محتويات الملف شيئاً. و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه:



2- التصاق الفيروس في نهاية الملف



هنا يختبئ في نهاية البرنامج المصاب، و يضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج.

3- الكتابة فوق الملف (Overwrite into File)

- يقومُ هذا النوع من الفيروسات بمسح جزء معّين من الملف ويتوضّع مكانه داخل الملف، وهكذا سيتمّ تجنب زيادة الحجم الواضح للملف المُصاب الذي يكون عند استخدام الطريقتين السابقتين وبالتالي يَصعُب كشف هذا النوع من الفيروسات.

العلامات الشائعة لوجود فيروس في الحاسب

1. بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت
2. امتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه .
3. حذف ملفات ومجلدات أو تغير خصائصها.
4. ظهور مناطق على القرص كمناطق سيئة لا تصلح للتخزين .
5. حدوث خلل في أداء لوحة المفاتيح كأن تظهر رموز مختلفة عن المفاتيح التي تم ضغطها.

الأسباب التي تدفع بعض الناس لكتابة البرامج الفيروسية

1. من اجل حماية البرامج من النسخ مثل فيروسات (Pakistani, brain) اللذان كتبا من قبل اخوين من باكستان كحماية للملكية البرمجية للبرامج التي قاما بكتابتها.
2. البحث العلمي كما في فيروس (STONED)الذي كتبه طالب دراسات عليا في نيوزيلندا وسرق من قبل أخيه الذي اراد أن يداعب أصدقائه بنقل الفيروس إليهم.
3. الرغبة في التحدي وابراز المقدرة الفكرية من بعض الأشخاص الذين يسخرون ذكائهم وقدراتهم بشكل سيئ مثل فيروس V2P
4. التشجيع على شراء البرامج المضادة للفيروسات حيث تقوم بعض شركات البرمجة بنشر فيروسات جديدة ثم تعلن عن منتج جديد لكشفها.

طرق الوقاية من الفيروسات

1. لابد من وجود برنامج حماية من الفيروسات في الحاسب وان يحدث بشكل دوري
2. لا تقم بفتح المرفقات في أي ايميل لا تعرف مرسله .
3. احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت.
4. لابد أن تحرص على استخدام نسخاً قانونية و مسجّلة من البرامج .
5. لابد أن تقوم بعمل باك أب للبيانات بشكل دوري و ذلك لاسترجاعها في حالة التعرض للفيروسات .

النسخ الإحتياطي للبيانات (Backup)

- عندما يحتوي الحاسوب على برامج كثيرة و كمية هائلة من البيانات المهمة خاصة مثل الشركات والبنوك والمؤسسات.
- وممكن أن تتعرض هذه البيانات للحذف أو الحريق أو التلف
- لذلك ينصح بإنشاء نسخة احتياطية من هذه البيانات في مكان بعيد نوعاً ما عن الحاسب

أنواع النسخ الإحتياطي

- **النسخ الإحتياطي الكامل: يعني عمل نسخة إحتياطية للبيانات بشكل كامل، الميزة في ذلك أن كل محتويات القرص الصلب سوف تنسخ لكن السيء أن هذه العملية تستغرق وقت طويل خاصة إذا كان الحاسوب يحتوي على معلومات كثيرة .**

- **النسخ الإحتياطي التراكمي: يعني عمل نسخة إحتياطية كاملة مرة كل أسبوع، لكن في كل ليلة لباقي الأسبوع يضاف فقط التغيرات و الإضافات إلا أخر نسخة، وهذه الطريقة توفر الوقت وتعمل تلقائياُ.**

نهاية الفصل السادس

شكراً لإصغائكم

أنواع الفيروسات

1- فيروسات قطاع الاقلاع (Boot Sector Viruses):

وهي الفيروسات التي تتوضع في ملفات الإقلاع، و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول إلى النظام ويمنعه من إقلاع الجهاز.

2- فيروسات البرامج:

تلصق هذه الفيروسات نفسها بملفات البرامج التنفيذية من نوع .bat أو .exe أو .sys وغيرها وتكون العدوى بهذا النوع فعالة وسريعة .

3- الفيروسات الماكروية:

هذه الفيروسات تصيب برامج الميكروسوفت اوفيس مثل الوورد و الاكسل, يقوم هذا النوع من الفيروسات بتغيير بعض المستندات مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد , أو إضافة كلمات جديدة لا علاقة لها بالموضوع . هي اساساً ليست ضارة, لكنها مزعجة نوعاً ما و قد تكون مدمرة احيانا!

طرق الوقاية من الفيروسات

1. لابد من وجود برنامج حماية من الفيروسات في الحاسب وان يحدث بشكل دوري
2. لا تقم بفتح المرفقات في أي ايميل لا تعرف مرسله .
3. إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية.
4. احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من سي دي. قبل أن تشغّلها.
5. لابد أن تحرص على استخدام نسخاً قانونية و مسجّلة من البرامج .
6. لابد أن تقوم بعمل باك أب للبيانات بشكل دوري و ذلك لاسترجاعها في حالة التعرض للفيروسات .

النسخ الإحتياطي للبيانات (Backup)

- عندما يحتوي الحاسوب على برامج كثيرة و كمية هائلة من البيانات المهمة خاصة مثل الشركات والبنوك والمؤسسات.
- وممكن أن تتعرض هذه البيانات للحذف أو الحريق أو التلف
- لذلك ينصح بإنشاء نسخة احتياطية من هذه البيانات في مكان بعيد نوعاً ما عن الحاسب

نهاية الفصل الرابع

شكراً لإصغائكم