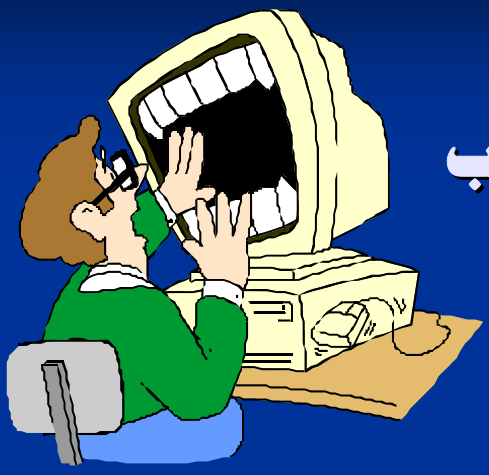


فيروسات الحاسب

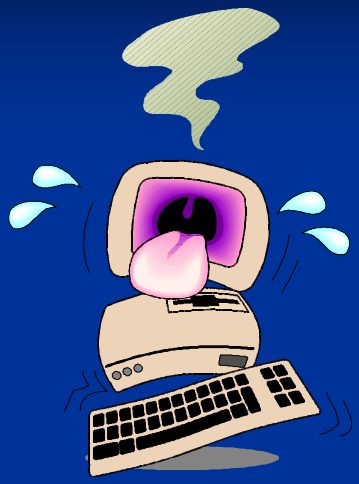
أ.د/ احمد وحيد مصطفى

فيروسات الحاسبات Computer Viruses

- ما هى فيروسات الحاسبات؟
  - فيروسات الحاسب برامج صغيرة الحجم ، بسيطة التكوين -فى الغالب- تحتاج إلى برامج أخرى وسيطة كعائل لها كما هو حال الفيروسات الحقيقية .
  - تعمل الفيروسات على الانتقال من مصدر مصاب وإلحاق نفسها بمواضع فى الحاسب .
  - عند التعامل مع الملف المصاب تنشط الفيروسات وتبدأ بنسخ نفسها عدد من المرات وتبحث عن مناطق جديدة لإصابتها بالعدوى أو تبدأ فورا تنفيذ مهامها التخريبية.
  - للفيروسات القدرة على تمييز البرامج أو الملفات المصابة وعدم إصابتها مرة أخرى.
  - بعض الفيروسات الحديثة ذات تأثير ضار ليس فحسب على البرامج والملفات وانما امتد تأثيرها لينال من اجهزة الحاسب ومعداته نفسها.

فيروسات الحاسبات Computer Viruses

- ما هى فيروسات الحاسبات؟



فيروسات الحاسبات Computer Viruses

- ما هى فيروسات الحاسبات؟
  - فيروسات الحاسب برامج صغيرة الحجم ، بسيطة التكوين -فى الغالب- تحتاج إلى برامج أخرى وسيطة كعائل لها كما هو حال الفيروسات الحقيقية .
  - تعمل الفيروسات على الانتقال من مصدر مصاب و إلحاق نفسها بمواضع فى الحاسب .
  - عند التعامل مع الملف المصاب تنشط الفيروسات وتبدأ بنسخ نفسها عدد من المرات وتبحث عن مناطق جديدة لإصابتها بالعدوى أو تبدأ فورا تنفيذ مهامها التخريبية.
  - للفيروسات القدرة على تمييز البرامج أو الملفات المصابة وعدم إصابتها مرة أخرى.
  - بعض الفيروسات الحديثة ذات تأثير ضار ليس فحسب على البرامج والملفات وانما امتد تأثيرها لينال من اجهزة الحاسب ومعداته نفسها.

فيروسات الحاسبات Computer Viruses

للكائنات المتطفلة صفتين رئيسيتين :

- **تحتاج فيروسات الكومبيوتر دائماً إلى ملف عائل تعيش متستّرةً فيه:**
  تتستر الفيروسات دائما 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 بمجرّدتشغيل البرنامج المصاب. و هي تنسخ نفسها للأقراص الأخرى، فإذا كان الكومبيوتر مصاباً ووضعت فيه قرصاً مرناً، يتم نسخ الفيروس اوتوماتيكيا للقرص المرن. و نظراً لهذه الخاصية في الفيروسات، تجد أن القرص المصاب يعطيك علامة أنه ممتلئ تماماً برغم أنك لم تقم بتخزين غير ملفات ذات حجم صغير.

فيروسات الحاسبات Computer Viruses

الفرق بين الدودة و التروجان و الفيروس؟

- الدودة worm : تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل اوتوماتيكي و من غير تدخل الانسان و هذا الامر يجعلها تنتشر بشكل اوسع و اسرع عن الفيروسات . الفرق بينهم هو ان الديدان لا تقوم بحذف او تغيير الملفات بل تقوم بتهليك موارد الجهاز و استخدام الذاكرة بشكل فظيع مما يؤدي الى بطء ملحوظ جدا للجهاز ، و من المهم تحديث نسخ النظام المستخدم في الجهاز كي يتم تجنب الديدان.
  تنتشر غالبا عن طريق الإيميل. حيث يرفق بالرسالة ملفاً يحتوي على دودة، و عندما يشغّل المرسل إليه الملف المرفق، تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.

فيروسات الحاسبات Computer Viruses

الفرق بين الدودة و التروجان و الفيروس؟

- **التروجان Trogan : وهو برنامج يغري المستخدم بأهميته او بشكله او باسمه ان كان جذابا ، و في الواقع هو برنامج يقوم بفتح باب خلفي ان صح التعبير بمجرد تشغيله ، و من خلال هذا الباب الخلفي يقوم المخترق باختراق الجهاز و بامكانه التحكم بالجهاز بشكل كبير حتى في بعض الاحيان يستطيع القيام بأمور ، صاحب الجهاز نفسه لا يستطيع القيام بها ، و هذا لا يرجع لملف التروجان ، لكن ملف التروجان هو الذي فتح للمخترق الباب ان صح التعبير بتشغيله اياه.**

فيروسات الحاسبات Computer Viruses

الفرق بين الدودة و التروجان و الفيروس؟

- **الفيروس Virus : هو برنامج صمم لينشر نفسه بين الملفات و يندمج او يلتصق بالبرامج. عند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب او المرن ، لذا الفيروس يحتاج الى تدخل من جانب المستخدم كي ينتشر ، بطبيعة الحال التدخل عبارة عن تشغيله بعد ان تم جلبه من الايميل او تنزيله من الانترنت او من خلال تبادل الاقراص المرنة.**

أنواع الفيروسات

- هناك الآف من الفيروسات المنتشرة عبر الانترنت ، لكن اغلبها يقع تحت النقاط الستة التالية :

فيروسات بدء التشغيل او Boot Sector Virus

هذا النوع من الفيروسات يصيب قطاع الاقلاع في الجهاز ، و هو المكان المخصص الذي يتجه اليه الكمبيوتر في بداية تشغيل الجهاز. و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول الى النظام ويمنعه من اقلاع الجهاز.

فيروس الملفات او File Virus

يصيب البرامج عادة ، و ينتشر بين الملفات الاخرى و البرامج الاخرى عند تشغيله.

أنواع الفيروسات

- **فيروس الماكرو او Macro Virus**

هذه الفيروسات تصيب برامج الميكروسوفت اوفيس مثل الوورد و الاكسل، و تعتبر ذات انتشار واسع جدا تقدر ب ٧٥٪ من عدد الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصا الوورد ، قد تجد بعض التصرفات الغير منطقية في بعض الاحيان مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد ، و ايضا تجد بعض الكلمات قد تغير مكانها و اضيفت كلمات جديدة لا علاقة لها بالموضوع . هي اساسا ليست ضارة، لكنها مزعجة نوعا ما و قد تكون مدمرة احيانا!

الفيروس المتعدد الاجزاء او Multipartite Virus

و هو الذي يقوم باصابة الملفات مع قطاع الاقلاع في نفس الوقت و يكون مدمرا في كثير من الاحيان اذا لم تتم الوقاية منه.

أنواع الفيروسات

- **الفيروس المتطور او Polymorphic Virus**
  هي فيروسات متطورة نوعا ما حيث انها تغير الشفرة كلما انتقلت من جهاز الى آخر. نظريا ، يصعب على مضادات الفيروسات التخلص منها لكن عمليا و مع تطور المضادات فالخطر اصبح غير مخيف.
- **الفيروس المختفي او Stealth Virus**
  تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم و ليس مصابا بفيروس. مع تطور مضادات الفيروسات اصبح من السهل كشف هذا النوع.

فيروسات الحاسبات Computer Viruses

- الظواهر التى تدل على وجود فيروسات بالحاسب
  - إختفاء بعض البيانات، أو الملفات الهامة من وسائط التخزين.
  - توقف بعض البرامج عن العمل أو عملها ببطء غير معهود .
  - ظهور اشكال ورسوم وصور غير معهودة على الشاشة.
  - توقف الحاسب أو بعض أجزاءه عن العمل تماما بدون سبب واضح.
  - تعامل البرامج مع مشغلات الأقراص اكثر من المعتاد .
  - تحميل البرامج وبدأ تشغيلها اكثر بطئا عما سبق .
  - ظهور الرسائل التى لايوجد ما يبررها مثل Not Enough Memory
  - نقص مساحة القرص الصلب وازدياد حجم الملفات البرامجية والوثائقية فجاة

فيروسات الحاسبات Computer Viruses

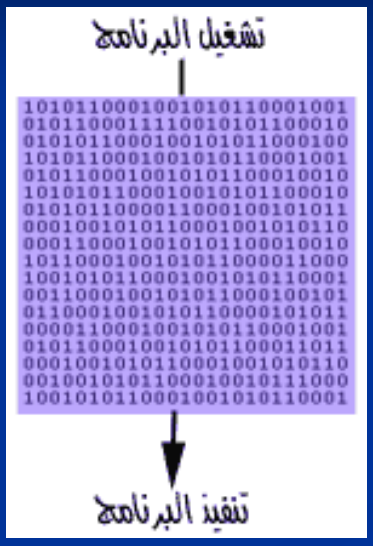
- أين يتواجد الفيروس داخل الحاسب:
  - ملفات البرامج الموجودة فى الاقراص الليّنة او القرص الصلب .
  - مناطق وقطاعات التحميل Boot Sector فى القرص الصلب أو منطقة فهرسة الملفات FAT،
  - التسجيل المباشر فى مناطق البيانات فى القرص الصلب إما كملفات مختفية Hidden أو فى شكل بيانات مسجلة على قطاعات الاسطوانة بشكل مباشر
  - الذاكرة وتسمى هذه فيروسات مقيمة فى الذاكرة Memory resident Viruses

فيروسات الحاسبات Computer Viruses

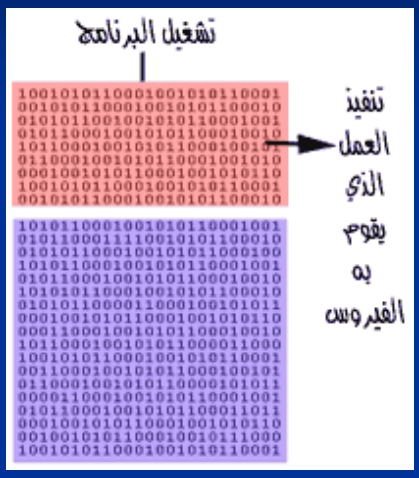
- البرامج الفرعية التى تشكل المكونات الرئيسية للفيروس:
  - برنامج فرعى يسعى للبحث عن الملف أو البرنامج المطلوب اصابته والتأكد من خلوه من نسخة من الفيروس ثم اصابته عندئذ بالعدوى.
  - برنامج فرعى يبحث عن توافر شروط معينة فى الملفات او بيانات الحاسب وعند توفرها فإنه يعمل على تشغيل الجزء الثالث
  - برنامج فرعى يقوم بالمهام التخريبية المطلوبة من الفيروس كما يقوم أيضا بوضع بصمته على البرامج المصابة لكى يسهل على الفيروس التعرف عليها فيما بعد لعدم اصابتها مرة اخرى.

فيروسات الحاسبات Computer Viruses

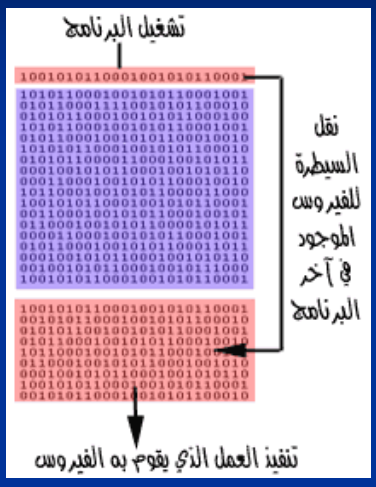
- مصادر العدوى بفيروس الحاسبات
  - الاقراص المرنة وأحيانا الاقراص الصلبة المضافة الىالحاسب حديثا والمصابة بالفيروس.
  - الاقراص المضغوطة cd غير الاصلية الملوثة.
  - الجهاز الرئيسى أو الخادم Server المصاب فى شبكات الحاسب المحلية أو الاتصال بأحد الاجهزة الاخرى على الشبكة.
  - شبكات الحاسب الدولية مثل الانترنيت ورسائل البريد الإلكترونى



- يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهايةٍ الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. الصورة التالية التي توضّح شكل البرنامج غير المصاب بفيروس
- عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.



- إذا تمت اصابة البرنامج بفيروس. يقوم الفيروس بلصق نفسه في البرنامج دون أن يغير في محتويات الملف شيئا. و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه



- وقد، يختبئ هذا الفيروس في نهاية الملف المصاب، و يضع في مقدّمة البرنامج مؤشّرا بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج.
- في الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج، و قد لا يعود أيضا.

فيروسات الحاسبات Computer Viruses

- اتقاء الإصابة بفيروسات الحاسب؟
  - توخى الحذر الشديد عند استخدام قرص غريب استُعمل من قبل على جهاز آخر أو ادخال أقراص فى جهاز قبل تامينه ضد الكتابة .
  - الحصول على وسيلة فعالة للتخلص من الفيروس اذا ما اصاب ملفاته والموقاية منه لمنعه من الوصول الى هذه الملفات .
  - الحصول على برامج للتعرف على الفيروس ومنع دخوله للحاسب واستخدامها دوريا.
  - تحديث برنامج مقاومة الفيروسات بشكل دائم، عن طريق متابعة الإصدارات الجديدة من برامج مهاجمة الفيروسات.
  -

فيروسات الحاسبات Computer Viruses

- اتقاء الإصابة بفيروسات الحاسب؟
  - توخى الحذر الشديد عند استخدام قرص غريب استُعمل من قبل على جهاز آخر أو ادخال أقراص فى جهاز قبل تامينه ضد الكتابة .
  - الحصول على وسيلة فعالة للتخلص من الفيروس اذا ما اصاب ملفاته والموقاية منه لمنعه من الوصول الى هذه الملفات .
  - الحصول على برامج للتعرف على الفيروس ومنع دخوله للحاسب واستخدامها دوريا.

  - تحديث برامج مقاومة الفيروسات بشكل دائم، و متابعة الإصدارات الجديدة من برامج مهاجمة الفيروسات.
  - لا تقم بفتح المرفقات في أي إيميل لا تعرف مرسله. و لا تقبل ملف من شخص لا تعرفه أبداً.
  - لا تقم بفتح المرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـ exe أو bat أو أي امتداد لا تعرفه.
  - إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية، فقد يكون صديقك نفسه ضحية.
  - احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من قرص مرن أو سي دي، قبل أن تشغّلها.

فيروسات الحاسبات Computer Viruses

- انواع برامج مقاومة الفيروسات
  - برامج التعرف على الفيروسات وهذه تستخدم من قبل النظام او المستخدم لتفحص الجهاز والملفات واحدا واحدا للتعرف على تاثرها بأى تغيرات
  - برامج القضاء على الفيروسات وهذه تستخدم من قبل النظام او المستخدم للتخلص من اثار الفيروسات او من وجودها.
  - برامج مقيمة فى الذاكرة لتصيد الفيروسات بمجرد تحركها للعمل
  - برامج لتطعيم الحاسبات ضد الفيروسات وهذه تقوم على تمييز الفيروسات والتعرف عليها عند دخولها الحاسب

مواقع هامة

- مواقع توفّر معلومات عن الفيروسات:
- موقع يقدّم أحدث المعلومات عن الفيروسات مع ملفات التخلّص منها من مكافي
- Introduction to Viruses

  http://www.stiller.com/vintro.htm
- تعرّف على الفيروسات و ـرق الوقاية منها
- How Computer Viruses Work

  http://www.howstuffworks.com/virus.htm

مواقع هامة

- مواقع برامج الحماية من الفيروسات:
- s'McAfee Virus Information Library
- http://vil.mcafee.com/
- Symantec AntiVirus Research Center :SARC
- http://www.sarc.com/
- يقدم هذا الموقع إمكانية كشف الفيروسات مجاناً مباشرة عبر النت، و لكن لابد من معرفة أن هذه العملية تعني أنّك تعطي الموقع إمكانية حذف الملفات في جهازك، فإذا شئت فقم بها على مسؤوليتك الخاصة.
- http:\\www.antivirus.com

ملاحظات مهمّة:

- تتم اصابة جهازك أو قرصك بفيروس فقط حين تقوم بتشغيل برنامج مصاب.
- يمكن لأي قرص أن يصاب بفيروس الـ boot sector.
- مجرّد وجودك في الانترنت لا يعرّضك للاصابة بفيروس. و لكنك تصاب به فقط إذا قمت بتنزيل برنامجاً مصاباً من الانترنت و قمت بتشغيله.
- لابد أن تحرص على استخدام نسخاً قانونية و مسجّلة من البرامج.
- لابد أن تقوم بعمل باك أب لملفاتك المهمة بشكل دوري و ذلك لاسترجاعها في حالة فقدانها لأي سبب تقني أو تعرّضك لفيروس.
- لابد أن يكون في جهازك برنامجاً للحماية من الفيروسات، و تحديثه دوريا.
- افحص جميع البرامج التي تنوي تشغيلها، و كذلك الأقراص التي تشتريها قبل تشغّيلها

الهاكرز

- عالم الهاكرز عالم دائم التطور، فالهاكرز يخترعون برامج و طرق جديدة معقدة يستطيعون من خلالها اختراق الشبكات و الأجهزة مهما كانت محمية. تختلف برامج التجسس في المميزات و طرق الاستخدام، ولكن الطرق التقليدية التي يستعملها الهاكرز المبتدئين جميعها تعتمد على فكرة واحدة و هي ما يسمى (الملف اللاصق) (Patch file) و الذي يرسله المتجسس إلى جهاز الضحية عن طريق البريد الإلكتروني أو برامج المحادثة فيقوم الأخير بفتحه بحسن نية دون دراية منه أنه قام في نفس الوقت بفتح الباب على مصراعيه للمتجسس ليقوم بما يريد في جهازه، و في بعض الأحيان يستطيع المتجسس عمل ما لا يستطيع الضحية عمله في جهازه نفسه.

الهاكرز

- يتم الاختراق عن طريق معرفة الثغرات الموجودة في ذلك النظام و غالبا ما تكون تلك الثغرات في المنافذ (Ports) الخاصة بالجهاز، و يمكن وصف هذه المنافذ بأنها بوابات للكمبيوتر على الإنترنت.
- يستخدم الهاكر برامج تعتمد على نظام (الزبون/الخادم) (client/server) حيث أنها تحتوي على ملفين أحدهما هو الخادم (server) الذي يرسل إلى جهاز الضحية الذي يقوم بفتحه و يصبح عرضة للاختراق حيث أنه تم فتح إحدى المنافذ بواسطة هذا الخادم.

الهاكرز

- هناك طرق عديدة و مختلفة تمكن المتطفلين من اختراق الأجهزة مباشرة دون الحاجة إلى إرسال ملفات
- ابتكرت أحد جمعيات الهاكرز في أمريكا طريقة للاختراق تتم عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر الإنترنت حيث يتم اعتراضها و التحكم في جهاز الضحية.
- يستخدم الهاكرز نظام التشغيل (Unix) لأنه نظام أقوى و أصعب من (Windows)، كما يستخدمون أجهزة خادمة تعمل على الإنترنت و تستخدم خطوط سريعة الاتصال بالشبكة عن طريق الحصول على حساب (Shell Account).

الهاكرز

- الهاكرز، هذه الكلمة تخيف الكثير من الناس خصوصا مرتادي شبكة الإنترنت الذين يحملون خصوصياتهم الموجودة في أجهزتهم و يبحرون في هذا البحر، و معظم الأحيان يرجعون و قد تلصص أحدهم على هذه الخصوصيات و ربما استخدمها في أمور غير شرعية. عالم الهاكرز عالم ضخم غامض، و بدايته كانت قبل الإنترنت بل و قبل الكمبيوتر نفسه، و لربما تسائل البعض، من هو الهاكر؟

الهاكرز

تعريف الهاكرز:

- الهاكرز، هذا اللفظ يطلق على المتحمسين في عالم الحاسب و لغات البرمجة وأنظمة التشغيل الجديدة، و يستخدم هذا اللفظ ليصف المبرمجين الذين يعملون دون تدريب مسبق.
- انتشر هذا المصطلح انتشارا رهيبا في الآونة الأخيرة و أصبح يشير بصفة أساسية إلى الأفراد الذين يلجئون بطريقة غير شرعية إلى اختراق أنظمة الحاسب بهدف سرقة أو تخريب أو إفساد البيانات الموجودة بها.
- في حالة قيام المخترق بتخريب أو حذف أي من البيانات الموجودة يسمى (كراكر)، لأن الهاكر يقوم عادة بسرقة ما خف من البرامج و الملفات ولا يقوم بتخريب أو تدمير أجهزة الغير.

الهاكرز

بدايتهم :

- تعود إلى عام ١٨٧٨م، في الولايات المتحدة الأمريكية، كان أغلب العاملين في شركات الهاتف المحلية من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة و التي حولت و غيرت مجرى التاريخ. فقد كانوا يستمعون إلى المكالمات الشخصية و يغيرون الخطوط الهاتفية بغرض التسلية و تعلم المزيد حتى قامت الشركات بتغيير الكوادر العاملة بها من الرجال إلى كوادر نسائية للانتهاء من هذه المشكلة.

الهاكرز

بدايتهم :

- مع ظهور الكمبيوتر في الستينات من هذا القرن، انكب المتحمسون على هذا الصندوق العجيب، و ظهر الهاكرز بشكل ملحوظ، فالهاكر في تلك الفترة هو المبرمج الذكي الذي يقوم بتصميم و تعديل أسرع و أقوى البرامج، و يعتبر كل من (دينيس ريتشي و كين تومسون) أشهر هاكرز على الإ طلاق في تلك الفترة لانهم صمموا نظام التشغيل (اليونكس) و الذي كان يعتبر الأسرع في عام ١٩٦٩م.

الهاكرز

- و مع ظهور الإنترنت و انتشاره دولياً، أنتجت شركة IBM عام ١٩٨١م جهاز أسمته (الكمبيوتر الشخصي) الذي يتميز بصغر حجمه و وزنه الخفيف بالمقارنة مع الكمبيوترات القديمة الضخمة، و أيضا سهولة استخدامه و نقله إلى أي مكان و في أي وقت، و استطاعته الاتصال بالإنترنت في أي وقت. عندها، بدأ الهاكرز عملهم الحقيقي بتعلم كيفية عمل هذه الأجهزة و كيفية برمجة أنظمة التشغيل فيها و كيفية تخريبها، ففي تلك الفترة ظهرت مجموعةٍ منهم قامت بتخريب بعض أجهزة المؤسسات التجارية الموجودة في تلك الفترة. يوما بعد يوم ظهرت جماعات كبيرة منافسة ، تقوم بتخريب أجهزة الشركات و المؤسسات حتى بدأت هذه المجموعات الحرب فيما بينها في التسعينات من هذا القرن و انتهت بإلقاء القبض عليهم.

الهاكرز

- و من عمليات الإختراق الملفتة للأنظار، قيام مجموعة من الهاكرز مؤخرا بالهجوم على موقع هيئة الكهرباء والمياه في دبي و مكتبة الشارقة العامة و ذلك بنشر كلمات غريبة في الصفحة الرئيسة للموقعين !
كما قامت مجموعة أخرى من البرازيل باختراق ١٧ موقعاً من الولايات المتحدة الأمريكية إلى بيرو، و من أهمهم موقع (ناسا) تاركة رسالة تقول " لا نرى فارقا كبيرا بين نظامكم الأمني و نظام حكومة البرازيل... هل فهمتم؟"

الهاكرز

- أشهر الهاكرز:
- كيفن ميتنك، الشخص الذي دوّخ المخابرات الأمريكية المركزية و الفيدرالية FBI كثيرا.
قام بسرقات كبيرة من خلال الإنترنت لم يستطيعوا معرفة الهاكر في أغلبها. و في إحدى اختراقاته، اخترق شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company و سرق بعض البرامج فتم القبض عليه و سجنه لمدة عام.
خرج ميتنك من السجن أكثر ذكاء، فقد كان دائم التغيير في شخصيته كثير المراوغة في الشبكة وكان من الصعب ملاحقته، و من أشهر جرائمه سرقة الأرقام الخاصة بـ٢٠٠٠٠ بطاقة ائتمان و التي كانت آخر جريمة له. و يعتبر ميتنك أول هاكر تقوم الFBI بنشر منشورات عنه تطالب من لديه أية معلومات عنه بإعلامها، حتى تم القبض عليه عام ١٩٩٥ و حكم عليه بالسجن لمدة عام لكنه لم يخرج إلا أواخر عام ١٩٩٩ و بشرط عدم اقترابه من أي جهاز كمبيوتر لمسافة ١٠٠ متر على الأقل!

الهاكرز

- أشهر الهاكرز:
- كيفن ميتنك، الشخص الذي دوّخ المخابرات الأمريكية المركزية و الفيدرالية FBI كثيرا.
قام بسرقات كبيرة من خلال الإنترنت لم يستطيعوا معرفة الهاكر في أغلبها. و في إحدى اختراقاته، اخترق شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company و سرق بعض البرامج فتم القبض عليه و سجنه لمدة عام.
خرج ميتنك من السجن أكثر ذكاء، فقد كان دائم التغيير في شخصيته كثير المراوغة في الشبكة و كان من الصعب ملاحقته، و من أشهر جرائمه سرقة الأرقام الخاصة ب٢٠٠٠٠ بطاقة ائتمان و التي كانت آخر جريمة له. و يعتبر ميتنك أول هاكر تقوم الFBI بنشر منشورات عنه تطالب من لديه أية معلومات عته بإعلامها، حتى تم القبض عليه عام ١٩٩٥ و حكم عليه بالسجن لمدة عام لكنه لم يخرج إلا أواخر عام ١٩٩٩ و بشرط عدم اقترابه من أي جهاز كمبيوتر لمسافة ١٠٠ متر على الأقل!