



محتويات الوحدة

رقم الصفحة	المحتوى
243	المقدمة
243	تمهيد
244	أهداف الوحدة
245	1. أنواع جرائم نظم المعلومات

246	2. تاريخ وأمثلة لجرائم الحاسوب ودوائر الاتصالات.
248	3. حماية البيانات من الفيروسات
262	4. الهاكرز والكرakers
276	الخلاصة
278	لمحة مسبقة عن الوحدة الدراسية التالية
279	إجابات التدريبات
279	مسرد المصطلحات
282	المراجع

المقدمة

تمهيد

عزيزي الدارس،

نرحب بك إلى الوحدة السابعة من مقرر " أخلاقيات المهنة " ، والتي تحمل العنوان " جرائم الحاسوب ". تشتمل الوحدة على أربعة أقسام: القسم الأول يتناول أنواع جرائم نظم المعلومات والتي تقسم إلى جرائم عامة، وجرائم مادية، وجرائم اقتصادية، وجرائم ضد الأفراد القسم الثاني يقدم تاريخاً وأمثلة لجرائم الحاسوب ودوائر الاتصالات . أما القسم الثالث فيتناول حماية البيانات من الفيروسات. وهو يبحث في المحاور الأساسية لحماية البيانات الذي يتركز على أربعة محاور مهمة ، تناولت الوحدة منها حماية البيانات من الأضرار التي تسببها الفيروسات التي تصيب أجهزة الحاسب الآلي ، وكذلك الناتجة عن عبث المخربين الذين يخترقون شبكات الحاسب ، وذلك من خلال التعرف على الفيروسات

والهاكرز وطرق الإصابة بهما والوقاية منهما. القسم الرابع يتناول الهاكرز والكراكرز ، حيث يتناول القسم فيروسات الحاسب ، تعريف الفيروس خصائص الفيروسات ، ويعرف أشباه الفيروسات، والأضرار التي تنتج عن الفيروسات ، وأعراض الفيروسات ، ومراحل عمل الفيروسات ، كما يقدم القسم أهم طرق وأسباب انتشار الإصابة بالفيروسات ، القسم يتناول كذلك الوقاية من الفيروسات والعلاج من الفيروسات . القسم الرابع من الوحدة يتناول الهاكرز والكراكرز (Hackers and Crackers) ، يبحث القسم كذلك في الاختراق ، وأيضاً ملفات التجسس .

أهداف الوحدة



عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- تصنف** جرائم نظم المعلومات.
- تقدم** أمثلة لبعض جرائم الحاسب.
- تنمي** قدراتك ومهاراتك العملية على طرق ووسائل حماية البيانات والحاسبات.
- تصف** فيروسات الحاسب وخصائصها.
- تقارن** بين الأنواع المختلفة للفيروسات.
- تشرح** مراحل عمل الفيروسات.
- تطبق** إجراءات الحماية من الفيروسات.
- تعالج** جهازك من الإصابة بالفيروسات.
- تقيّم** خطر الفيروسات على أمن المعلومات بمعرفة الأضرار التي تنتج عنها.
- تصف** الهاكرز. **تفرق** بين الهاكرز والكراكرز.
- تعرف** الاختراق. **تعدد** طرق الاختراق. **تعدد** أشكال الاختراق. **تتلافى** ثغرات الاختراق. **تبين** أسباب الاختراق. **تقيّم** خطورة الاختراق. **تصف** ملفات التجسس. **توضح** خطورة ملفات التجسس. **تعدد** طرق الإصابة بملفات التجسس. **تعدد** مقومات الاختراق. **تنفذ** إجراءات حماية جهازك من الإصابة بملفات التجسس باتباع طرق الوقاية منها.
- تمنع** دخول الهاكرز إلى جهازك.

1. أنواع جرائم نظم المعلومات

عزيزي الدارس، قسم حسن طاهر داود في كتابه المعنون بـ "جرائم نظم المعلومات" جرائم نظم المعلومات إلى جرائم عامة، وجرائم مادية، وجرائم اقتصادية، وجرائم ضد الأفراد والتي لخصها في الجدول التالي:

جرائم عامه	جرائم مادية	جرائم اقتصادية	جرائم ضد الأفراد
أخطاء الأداء المتعمدة إغفال الواجب التجاهل التهور والطيش التقصير والإهمال التأمر التواطؤ	السرقه التدمير والإتلاف تمزيق المستندات التعدي على الممتلكات السطو الليلي التهريب انتحال الشخصية قرصنة البرامج	النصب والاحتيال الاختلاس التلاعب الرشوة الابتزاز التهديد انتهاك الأسرار الاقتصادية	القذف والتشهير تسهيل الدعارة انتهاك الخصوصية الإهانة التحرش الجنسي الخطف

القتل الانتحار	التزييف والتزوير	التجسس العسكري التجسس الصناعي التجسس الاقتصادي	
-------------------	---------------------	---	--

تصنيف جرائم نظم المعلومات كما أوردها داود في كتابه "جرائم نظم المعلومات"

2. تاريخ وأمثلة لجرائم الحاسوب ودوائر الاتصالات.

في هذا الجزء سنسرد أهم جرائم الحاسوب التي ذاع صيتها في الفترة الأخيرة وتواريخ حدوثها:

التاريخ	الجريمة
سبتمبر 1970م	تمكن جون دراير والملقب بكابتن كرانس من عمل مكالمات تليفونية غير مدفوعة الأجر عن طريق استخدام بنس صفارته بدلا من العملة التي تستخدم لتليفونات شركة AT&T
أغسطس 1974م	تمكن شخص أسطوري والملقب بـ كيفن ميتنيك ولأول مرة من السطو على شبكات البنوك وتدمير بياناتها وتغيير بيانات أعدائه كما تمكن من السطو على شبكة المعلومات الخاصة بالقوات الأمريكية في كلورادو.
يوليو 1981م	تمكن شاب يدعى إين مرفي عمرة 23 عاما من السطو على شبكة البيت الأبيض وشبكة وزارة الدفاع

الأمريكية "البنتاجون".	
تمكن أحد المقتحمين من شل أداء شبكة IBM الدولية عن طريق إرسال رسالة تهنئة بالكريسماس ملايين المرات.	ديسمبر 1987م
خسر البنك المتحد السويسري ما يزيد عن 32 مليون جنيه إسترليني نتيجة فعل أحد المخترقين والذي قام بنشر الفيروسات في قواعد بياناته.	يوليو 1988م
تمكن صبي عمرة 15 عاما من اختراق حاسبات وزارة الدفاع الأمريكية.	أكتوبر 1989م
قدمت هونج كونج وثيقة خاصة بإصدار أول تشريعات خاصة بعقوبات الاختراق.	نوفمبر 1990م
قبض الإسرائيليون على شاب عمره 18 عاما لاختراقه شبكة البنك الرئيسي وتغييره لأرقام الحسابات.	أغسطس 1991م
تمكن أحد الأشخاص والذي يدعى كيفن بولسن من التنصت والاطلاع على الأوامر العسكرية الخاصة بالمناورات التي تؤديها القوات الجوية الأمريكية.	ديسمبر 1992م
قام نادي للكمبيوتر ألماني ببث فيلم تليفزيوني يشرح كيف يمكن السطو على أرصدة البنوك من خلال برنامج موجود على الويب.	فبراير 1997م
زاد من نشاط نشر الفيروسات المدمرة والديدان التي تشل أداء المكونات الحاسوبية من خلال شبكة الإنترنت.	مايو 1998م

أسئلة تقويم ذاتي



- 1/ قسمت الوحدة "جرائم نظم المعلومات" إلى جرائم عامة، وجرائم مادية، وجرائم اقتصادية، وجرائم ضد الأفراد . أعط مثلاً أو أكثر لكل واحد من هذه الأقسام .
- 2/ اذكر أمثلة لأهم جرائم الحاسوب والتي ذاع صيتها دولياً.

3. حماية

الفيروسات

Data Protection From Viruses 1.3 المحاور الأساسية لحماية البيانات

بصفة عامة ، تشمل حماية البيانات جميع الإجراءات الضرورية لحماية أجهزة وشبكات الحاسبات وما يتصل بها من طرفيات ووسائط تخزين ، وذلك لحماية البيانات المخزنة في تلك الأجهزة ووسائط التخزين المختلفة المتصلة بها ، ولذلك يطلق مصطلح حماية البيانات في بعض الأحوال للتعبير عن حماية الحاسبات.

وحماية البيانات - بصفة عامة - لجميع المستخدمين يتركز على أربعة محاور مهمة وهي :

- حماية جهاز الحاسب وملحقاته من التأثيرات الكهربائية غير المرغوب فيها : مثل تلك الناتجة عن: انخفاض أو ارتفاع الجهد الكهربائي ، وانقطاع التيار المفاجئ.
- حماية جهاز الحاسب الآلي من حدوث خلل بسبب ظروف بيئة التشغيل المحيطة بالجهاز : مثل تلك الناتجة عن : الموجات عالية التردد ، والكهرباء الساكنة ، والغبار والجسيمات الدقيقة ، والحرارة أو البرودة العالية.
- حماية البيانات عن طريق القيام بعملية التخزين الاحتياطي كل فترة زمنية وبصفة دورية.

□ **حماية بيانات شبكة الحاسب من الإضرار بها :** مثل تلك الناتجة من عبث المخربين (Hackers and Crackers) ، وكذلك الأضرار الناتجة من الفيروسات والتي تصيب أجهزة الحاسبات وبالتالي الإضرار بالبيانات المخزنة بها. وسوف نتناول **عزيري الدارس** في هذه الوحدة حماية البيانات من الأضرار التي تسببها الفيروسات التي تصيب أجهزة الحاسب الآلي ، وكذلك الناتجة عن عبث المخربين الذين يخترقون شبكات الحاسب ، وذلك من خلال التعرف على الفيروسات والهاكرز وطرق الإصابة بهما والوقاية منهما.

2.3 فيروسات الحاسب (Computer Viruses)

في ظل تنامي استخدام الإنترنت وانتشارها كأداة لنقل البيانات بين جهات عديدة وتزايد تطبيقاتها في جميع مجالات الحياة ، فقد أصبح من السهل إصابة العديد من الأجهزة والشبكات بالفيروسات التي تقوم بإفساد البرامج وتخريب البيانات ، وقد يصل ضررها إلى إتلاف بعض أجزاء الحاسب الآلي المادية مثل وحدة النظام الرئيس للإدخال والإخراج (Basic Input Output System (BIOS)).(Unit

1.2.3 تعريف الفيروس

الفيروس هو: برنامج كمبيوتر يتكون من عدة برامج فرعية مكتوب بإحدى لغات البرمجة مثل أي برنامج تطبيقي آخر موجود على الحاسب الآلي ، ليس هناك اختلاف إلا في الغرض الذي صمم من أجله ، وهو - في معظم الأحيان - إصابة الحاسب الآلي وإتلاف برامجه وبياناته. وحتى يحقق برنامج الفيروس أهدافه التدميرية فإنه يتم إعداده بحيث يكون له إمكانية أن يربط نفسه بالبرامج الأخرى بدون زيادة حجمها ، وكذلك إمكانية نسخ نفسه بصورة تكرارية ، أي له القدرة على التكاثر والتوالد الذاتي ، مما يمكنه من الانتشار بين برامج وتطبيقات الحاسب الآلي المختلفة وأيضا في مواقع مختلفة من الذاكرة.

يمكن للفيروس أن يكون في شكل ملف مستقل بذاته ومخزن داخل أحد وحدات الحاسب، أو أن يكون ملتصقا بأحد الملفات كأن يلتصق بأحد ملفات الجداول الإلكترونية أو أحد ملفات الرسائل

المكتوبة ببرنامج معالجة الكلمات. عندما نقوم بالتعامل مع الملف الذي التصق به الفيروس فإن هذا الملف يجب أن ينتقل إلى الذاكرة الإلكترونية للحاسب لكي يتمكن الحاسب من التعامل معه، وفي هذه الحالة يضع الفيروس نسخة منه في الذاكرة الإلكترونية لكي يصيب أي ملف أو برنامج آخر ينتقل إلى الذاكرة الإلكترونية لكي يقوم الحاسب بتشغيله.

ولكن لماذا سميت الفيروسات بهذا الاسم ؟ : لأنها

تتصرف بطريقة تكاد تتماثل تماما مع أسلوب غزو الفيروس البيولوجي للخلايا الحية في جسم الإنسان، فهي تعيش داخل البرمجيات والتي تُعد المادة الحية التي يتكاثر فيها ومن خلالها الفيروسات.

ويمكن تلخيص وجه الشبه بين الفيروس البيولوجي (العضوي) وفيروس الحاسب في النقاط التالية :

- يقوم الفيروس العضوي بتغيير الخصائص العضوية لخلايا الجسم وإحداث آثار ضارة لمن تصيبه ، ويقوم فيروس الحاسب بتغيير وظائف البرامج الأخرى وكذلك إحداث أضرار بها.
- يتكاثر الفيروس العضوي بسرعة ويتسبب في إنشاء فيروسات جديدة ، ويقوم فيروس الحاسب بإعادة إنشاء نفسه بسرعة (Reproduce itself) فيظهر وكأنه يتكاثر ذاتيًا.
- الجسم الذي ينقل إليه الفيروس الطبيعي العدوى قد يظل مدة طويلة دون ظهور أعراض المرض عليه ، وكذلك البرامج المصابة بفيروس الحاسب قد تبقى مدة طويلة دون ظهور أعراض تخريرية عليها.
- في بعض الحالات يقوم الفيروس العضوي وفيروس الحاسب بتغيير شكلهما حتى يصعب اكتشافهما والتغلب عليهما.

أسئلة تقويم ذاتي

؟

- 1/ يطلق مصطلح حماية البيانات في بعض الأحوال للتعبير عن حماية الحاسبات ، وضح / ذلك.
- 2/ ما المحاور الأساسية التي تركز عليها عملية حماية البيانات؟.
- 3/ عرّف فيروس الحاسب، ثم وضح لماذا سميت فيروسات الحاسب بهذا الاسم.
- 4/ لخص أوجه التشابه بين فيروس الحاسب والفيروس البيولوجي.

2.2.3 خصائص الفيروسات

تتميز فيروسات الحاسب بالعديد من الخصائص أهمها ما يلي :

☑ القدرة على الاختفاء :

هناك عدة طرق يستخدمها الفيروس لإخفاء نفسه منها الآتي :

- 0 ارتباط الفيروس بالبرامج الشائعة التي عند تشغيلها يتوالد الفيروس ويقوم بتدمير البيانات.
- 0 يستطيع أن يدخل كملف مخفي ضمن الملفات بحيث لا يمكن استعراضه عند استعراض أسماء الملفات على القرص.
- 0 تستقر بعض الفيروسات في أماكن في الذاكرة يصعب على المستخدم ملاحظتها.
- 0 بعض الفيروسات تظل ساكنة فترة طويلة، والملفات المصابة بها تظل تعمل بكفاءتها فترة من الزمن.

☑ التكاثر :

لها القدرة على أن تتكاثر بمعنى أن يقوم الفيروس بعمل نسخة أخرى منه سواء أكان ذلك في الذاكرة أو داخل كل ملف يصيبه ، مما يتولد عنه فيروسات كثيرة.

☑ التنقل :

يستطيع الفيروس أن ينتقل داخل الذاكرة من مكان لآخر بحيث يصعب الاستدلال على مكان وجوده، وذلك يزيد من صعوبة إزالة الفيروس.

☑ البصمة :

لكل فيروس بصمة (عبارة معينة) يضعها داخل البرنامج المصاب بالفيروس يمكن التعرف عليه من خلالها.

☑ التدمير :

لكل فيروس ما يسمى بالمفجر الذي يقوم بتدمير البيانات بمجرد تشغيله، وهو إما يكون مرتبطاً بتاريخ معين مثل فيروس "مايكل أنجلو"، أو زمن معين يقرأه من الحاسب الآلي، أو عند ضغط مفتاح معين على لوحة المفاتيح أو تنفيذ أمر معين... إلخ.

3.2.3 أشباه الفيروسات

وهي أنواع من البرامج التدميرية ينطبق عليها تعريف الفيروس جزئياً

، أي يتوافر فيها بعض من خصائص الفيروسات سابقة الذكر وليس كلها ، حيث تشترك هذه الأنواع مع الفيروسات في أنها تعمل بدون علم المستخدم بصورة خفية ، وتقوم بأعمال ضمن الكمبيوتر مصممة عمداً لتنفيذها. ومن هذه الأنواع : الديدان (Worms) ، وأحصنة طروادة (Trojan horses).

والدودة (Worm) هي : برنامج يعيد إنتاج نفسه ، لكنها لا تلوث برامج أخرى ، وتنسخ نفسها من وإلى الأقراص المرنة ، أو عبر الشبكات ، ويعتمد بعضها على الشبكة في إنجاز عملها. تستخدم إحدى أنواع الديدان ، وهي الدودة المضيئة (Host Worm) ، الشبكة لنسخ نفسها إلى أجهزة الكمبيوتر المتصلة بالشبكة ، بينما توزع الدودة الشبكية (Network Worm) أجزائها على عدة كمبيوترات ، وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء. ويمكن أن تظهر الديدان على كمبيوترات منفصلة ، فتتسخ نفسها إلى أماكن متعددة على القرص الصلب. والفرق بين الفيروسات و الديدان هو أن الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم باستهلاك موارد الجهاز واستخدام الذاكرة بشكل يؤدي إلى بطء ملحوظ بشدة في أداء الجهاز.

أما حصان طروادة (Trojan horses) فهو : برنامج مكر مدمر يختبئ ضمن برامج يبدو مظهرها بريئاً (خدمة أو تطبيق) بحيث يغري المستخدم بأهميته أو بشكله أو باسمه ، وعندما يشغل المستخدم واحداً من هذه البرامج ، ينشط الجزء الماكر ويقوم بعمل معين مصمم له. وفي الغالب يقوم بعمل بوابة خلفية (Backdoor) تمكن المخترقين من الدخول على الجهاز المصاب والعبث به. وتختلف أحصنة طرواده عن الفيروسات العادية في أنها لا تعيد إنتاج نفسها.

4.2.3 الأضرار التي تنتج عن الفيروسات

- عزيزي الدارس ،** يوجد العديد من الأضرار التي تنتج عن إصابة جهاز الحاسب بالفيروسات من أهمها ما يلي :
- فقدان بعض ملفات التطبيقات الهامة التي تؤدي إلى توقف عمل التطبيق.
 - إمتلاء الذاكرة نتيجة نسخ الفيروس لنفسه مما يبطئ عمل الذاكرة أو يعطى رسائل مؤداها أن الذاكرة ممتلئة ولا يمكن العمل عليها إلا بغلق بعض التطبيقات.
 - فقد جدول توزيع الملفات (FAT) مما يؤدي إلى فقدان الملفات وعدم الاستدلال عليها.

- فقد قطاع الإقلاع (Boot Sector) وبالتالي يفقد القرص القدرة على تحميل نظام التشغيل.
- تلف بعض الأقراص المصابة بالفيروس نظرا لعدم القدرة على إزالة الفيروس منها.
- ظهور رسائل فجائية تغير من تركيب بعض البرامج وخاصة مع لغات البرمجة مما يجعل البرنامج غير قابل للتنفيذ.
- توقف الجهاز فجأة عن العمل مما يؤدي إلى فقدان البيانات الجارية العمل عليها.
- تغيير مواضع حروف لوحة المفاتيح مما يؤدي إلى تعطيل العمل وإهدار الوقت.
- يؤدي إلى فقدان نظام كامل أحيانا وخاصة مع الشبكات مما يؤدي إلى إعادة إعداد نظام الشبكات من جديد.
- يعطل تنفيذ بعض التطبيقات والبرامج.

5.2.3 أعراض الفيروسات

عزيزي الدارس، في حالة إصابة جهاز الحاسب بالفيروسات تظهر عليه بعض الأعراض التي توحى بذلك ، ومن أهم هذه الأعراض ما يلي :

- عدم تحميل نظام التشغيل ، أو عدم القدرة على التعامل معه بشكل ملائم.
- توقف النظام عن العمل أثناء التشغيل بدون سبب واضح.
- زيادة أو نقصان حجم ملف بدرجة ملحوظة.
- **تغيير عدة الملفات.**
- عدم ظهور أسماء الملفات أثناء استعراض محتويات القرص.
- عرض رسالة خطأ فجائية وغير متوقعة ، مثل : "لا توجد ذاكرة كافية لتشغيل البرامج" ، وذلك بالرغم من أن الذاكرة المتاحة كافية.
- ظهور ملفات جديدة لها أسماء وامتدادات غريبة وبدون حجم.
- ظهور حروف غريبة عند الضغط على لوحة المفاتيح.
- تغيير مظهر العلامات الدالة على الملفات.
- التعامل مع الأقراص أكثر من المعتاد.
- بطء تشغيل النظام بصورة ملحوظة.
- عدم قدرة بعض التطبيقات على التشغيل.
- نقص شديد في سعة الذاكرة.
- عند استخدام برنامج "Disk Scan" تظهر رسالة تفيد "لا يوجد تطابق بين المساحة الخالية الموجودة على القرص الصلب ، والتي تم تخزينها في ملفات (FAT) ، والمساحة الحقيقية الخالية على

لتكاثر الفيروس وهي مرحلة الانتشار (Propagation Phase).
▪ **المرحلة الثالثة :** مرحلة التنفيذ : بعد أن تنتهي مرحلة الانتشار تبدأ مرحلة قدح الزناد (Triggering Phase) لبدء عمل الفيروس ، ويمكنك اعتبارها مرحلة شرطية يتوقف تنفيذها على تحقيق شرط خاص (يحدده مصمم برنامج الفيروس) كتاريخ معين أو حدوث عدد محدد من مرات تكاثر الفيروس أو أي شرط آخر يضعه المبرمج وعند تحقق هذا الشرط ينفذ الفيروس مهامه التخريبية.

7.2.3 طرق وأسباب انتشار الإصابة بالفيروسات

يوجد العديد من طرق وأسباب انتشار الإصابة بالفيروسات ، من أهمها ما يلي :

- **مشاركة الملفات عن طريق شبكات الحاسب الآلي**
حيث إنه في حالة ما أصيب خادم ملفات (File Server) بفيروس فإن ذلك يؤدي إلى إصابة باقي الأجهزة الطرفية بنفس الفيروس كما أن إصابة أحد الأجهزة الطرفية يمكن أن تؤدي إلى انتقال العدوى إلى الجهاز الخادم ومن ثم إلى باقي أجهزة الشبكة وحيث إن الشركات التي تستخدم شبكات الحاسب الآلي هي أكثر الأمكنة عرضة للإصابة فإنه يجب على المشرف على الشبكة القيام بفحص دوري لكافة الأجهزة للتأكد من خلوها من الفيروسات
- **نسخ البرامج من النشرات الإلكترونية**
النشرات الإلكترونية : مجموعة ملفات تتضمن قواعد بيانات وبرامج عامة يتم تحديثها بانتظام ، توضع في متناول كثير من المستخدمين الذين يتقاسمون عملاً مشتركاً.
- **تثبيت برنامج جديد في الحاسب الآلي**
لا يوجد ضمان أكيد بخلو كافة البرامج الجديدة من عدوى فيروس الحاسب الآلي حتى ولو كانت هذه البرامج أصلية ومغلقة ومختومة حيث هناك احتمالات قليلة للتلاعب بفعل فاعل في النسخة الرئيسية.
- **من خلال نقل الأجهزة نفسها**
تحدث هذه الحالة عند طلب جهاز من المورد أو نقل جهاز من إدارة إلى إدارة أخرى قد ينتقل الفيروس مع الجهاز إلى موقعه الجديد وعند استخدامه في الموقع الجديد ينشط الفيروس ويحدث الإصابة في جميع أجهزة الحاسب الآلي التي يكون على اتصال بها.

▪ استخدام اسطوانة مصابة بالفيروس

بعض الفيروسات تدمج أو تلتصق نفسها بالبرامج الموجودة في الاسطوانة وعندما نقوم بتشغيل الجهاز أو نقل ملف من اسطوانة إلى اسطوانة أخرى تنتقل الفيروسات ويبدأ التكاثر والانتشار.

▪ من خلال مرفقات البريد الإلكتروني

تُعد الرسائل الإلكترونية أكبر مصدر للفيروسات وذلك لسهولة إضافتها كملفات ملحقة وسرعة انتشارها على الشبكة في زمن قصير جدا. وقراءة نص البريد الإلكتروني في حد ذاته غير ضار أبداً ، ولكن إذا كانت الرسالة الإلكترونية يصاحبها مرفقات (Attachments) فإن عليك أن تكون حذرا وعدم القيام بفتح ما هو مرفق مع أي رسالة بدون أن تقوم بفحصها (Scanning) أولا. ويجب عليك عدم ضبط قارئ البريد الإلكتروني كي يبدأ برنامج مايكروسوفت وورد تلقائيا عندما يصله مستند نص مرفق.

▪ التداول السيئ للبرامج

ويعنى نسخ البرمجيات من أقراص ليست أصلية مما يعطى الفرصة لإصابة هذه البرمجيات بالفيروسات.

8.2.3 الوقاية من الفيروسات

الوقاية من الفيروسات تعني حماية النظام من دخول أي فيروس ، ولكن ليس هناك حماية 100% من الفيروسات ، إلا إذا عزلت جهازك من شبكة الإنترنت ، ومنعت تحميل أي برنامج في جهازك ، ولكن هذه الفكرة ليست منطقية على الإطلاق إذ إن جهاز الحاسب الآلي والشبكة (محلية أو إنترنت) أمران متلازمان لا يمكن فصلهما ، فلا فائدة من الحاسب الآلي إذا لم يكن هناك شبكة تربطه بغيره من الحاسبات الآلية تتبادل فيها المعلومات وتتحقق فيها فوائد كثيرة ، ولا فائدة أيضا من الشبكة إذا لم يكن هناك حاسبات آلية متصلة بها.

ويمكن تلخيص الإجراءات الوقائية التي يجب مراعاتها للوقاية من الفيروسات ، والتي يعفي تطبيقها الكثير من العواقب الوخيمة التي قد تترتب على الإصابة بالفيروسات فيما يلي :

- استخدام البرامج الأصلية وعدم استخدام النسخ.
- تجهيز عدة نسخ احتياطية من البرمجيات الأصلية (نسخ غير ملوثة بالفيروس)، وحفظها بحيث يمكن استرجاعها عند الحاجة.

- الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج المعدلة إلى البيئة الإنتاجية، وبخاصة تلك البرامج المجلوبة من مصادر أخرى أو من الإنترنت.
- عدم تحميل أي برنامج مجلوب من الخارج، فهذا هو أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة. وخصوصاً البرامج المجانية التي تنتقل من يد إلى يد أو التي يتم توزيعها بواسطة مجلات الكمبيوتر المتخصصة ، أو تلك الموجودة ضمن مواقع غير موثوق بها على الإنترنت ، يجب دائماً الحذر في التعامل معها، حتى تلك البرامج التي تأتي من مصادر لا يرقى إليها الشك فيجب فحصها جيداً.
- يجب فحص البرمجيات أو اختبارها قبل استخدامها، ويجب أن يتم ذلك على جهاز مستقل غير مرتبط بالشبكة. وذلك من خلال استخدام أحد البرامج التي تكشف عن الفيروسات ، وأيضاً عن طريق البحث عن أي سلوك غير مفهوم في البرنامج مثل أعراض الفيروسات التي تم ذكرها أعلاه. ولو أن خلو البرنامج من مثل هذا السلوك غير المفهوم لا يعني بالضرورة نظافة البرنامج فالفيروسات تظل كامنة ولا تكشف عن سلوكها إلا في اللحظة المناسبة.

- حماية الأقراص عن طريق فتحة الحماية للأقراص المرنة.
- اختبار الملفات من وقت لآخر لملاحظة حجمها وامتداداتها.
- مراجعة الملفات الخفية فإذا وجدت أسماء ملفات جديدة يكون هناك احتمال الإصابة بفيروسات.
- مراقبة الملفات التنفيذية وملفات التهيئة من حين لآخر.
- إجراء عملية مسح شامل للجهاز بصفة دورية مرة في الأسبوع مثلاً ، للتأكد من عدم وجود فيروسات على الجهاز، وتنظيفها إن وجدت. ويجب إعطاء اهتمام خاص لنظافة ملفات النسخ الاحتياطي (مثل : الملفات المضغوطة وملفات الأرشفة ، وخلافه)، وذلك لأن الفيروسات يمكن أن تنتشر في مثل هذه الأنواع من الملفات وتظل كامنة فيها لفترة طويلة جداً، ثم تنشط هذه الفيروسات بمجرد استخدام هذه الملفات (النسخ الاحتياطية) وتبدأ عملها التدميري من جديد.
- الكشف الدوري على الأقراص المرنة والممغنطة ، أو أي وحدات تخزين متنقلة عند أخذها من آخرين ، وذلك باستخدام أي برنامج مضاد للفيروس.

- استخدام الأقراص الضوئية وهي للكتابة فقط.
- عدم فتح أي ملفات ملحقة (Attachment Files) مع البريد الإلكتروني حتى لو كانت من أشخاص معروفين بالنسبة لنا ، إلا إذا كنا نعلم محتوى الملف الملحق مسبقاً ، وخصوصاً التي لها الامتداد .exe & vbs
- عدم الدخول على مواقع غير معروفة ، أو تقديم مواد منافية للأخلاق.
- تجنب التصفح بشكل عشوائي أو الاستجابة العشوائية للإعلانات المقدمة وخصوصاً التكنولوجية منها.
- تحميل برنامج داخل جهاز الحاسب للتحقق من وجود فيروسات وحمايته منها، ويفضل أن يكون هذا البرنامج دائم الوجود في الذاكرة ويتم تحميلها مع بداية تشغيل الجهاز. وهذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة لها ، ولكنها تقف عاجزة أمام الفيروسات الأحدث وغير المدرجة ضمن قائمة الفيروسات التي يمكنها التعرف عليها لأن بصمة الفيروس الحديث تكون غير معروفة لهذه البرامج ، ومن هنا كان لزاماً على المستخدم تحديث ملف تحديثات الفيروسات (Virus Definition File) الخاصة بهذه البرامج، أو استخدام إصدارات أحدث من هذه البرامج.

أسئلة تقويم ذاتي



- 1/ تمثل مرحلة الدخول ، ومرحلة بداية الانتشار، ومرحلة التنفيذ : المراحل الأساسية لعمل الفيروسات ، وضح ذلك ، مع شرح كل مرحلة.
- 2/ ما أهم طرق وأسباب انتشار الإصابة بالفيروسات؟.
- 3/ لخص أهم الإجراءات التي يجب مراعاتها للوقاية من الفيروسات.

9.2.3 مبادئ مكافحة الفيروسات

قبل البدء عزيزي الدارس في عملية العلاج (التخلص) من الفيروسات نقترح دائماً عمل نسخ احتياطي للمعلومات الهامة الموجودة على جهازك إن لم يكن لديك نسخ احتياطية حديثة. وذلك لأن الكثير من برامج الحماية قد لا تستطيع التخلص من الفيروسات ما لم يتم حذف الملفات المصابة منها ، وربما تحتاج إلى تهيئة القرص الصلب (نادراً) ، ومن الأفضل الحصول على ملفاتك وحتى وإن كانت مصابة بفيروسات بدلا من ضياعها لعلك تستطيع الاستفادة

منها أو تنظيفها فيما بعد باستخدام برامج أخرى لمعالجة فيروسات مع أخذ الاحتياطات اللازمة لذلك .

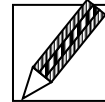
وعادة ما يتم التخلص (العلاج) من الفيروسات عن طريق برامج صممت خصيصاً لهذا الغرض تسمى برامج الحماية من الفيروسات (Antivirus Programs) - أو (Virus Protection Software) وجميعها تخدم نفس الغرض ، ألا وهو فحص الجهاز لمعرفة ما إذا كان قد أصيب بأحد الفيروسات المعروفة لتلك البرامج من خلال قاعدة بيانات تحتويها لكل الفيروسات المعروفة حتى تاريخه . كما تقوم تلك البرامج بفحص كل ملف قادم إلى جهازك ، وتقوم بتحذيرك في حالة وصول أي ملف مصاب بأي نوع من الفيروسات المعروفة.

ملحوظة

الشيء المهم والمتعلق بتلك البرامج للحماية من الفيروسات هو أن بعض تلك البرامج تكون فعالة في حالة واحدة فقط ألا وهي متى ما كانت قادرة على اكتشاف الفيروسات قبل وصولها إلى ذاكرة الجهاز. ولذلك على كل مستخدم للكمبيوتر أن يعد قرصاً خارجياً يحتوي على ملفات النظام (Bootable Disk) لبدء تشغيل الجهاز منها في حالة الاضطرار إلى ذلك ، بالإضافة إلى أي برنامج مضاد للفيروسات. وهذا القرص لا بد وأن يكون محمية من الكتابة عليه.

تدريب (1)

اذكر بعضاً من أشهر برامج الحماية من الفيروسات (Antivirus Programs) .



نشاط

التعرف على أهم الفيروسات المنتشرة في وقت تدريس هذا التدريب وخصائصها وكيفية المعالجة منها ، وكذلك إجراء تدريب عملي على كيفية تحميل برنامج Norton Antivirus ، أو برنامج McAfee Virus Scan داخل جهاز الحاسب، وكذلك التدريب على كيفية استخدامه في الكشف عن الفيروسات في حالة إصابة القرص الصلب بالجهاز أو القرص المرن بالفيروسات.



4. الهاكرز والكرakers (Hackers and Crackers)

عزيزي الدارس، الهاكرز : أول ما أطلقت هذه الصفة كانت تشير إلى المبرمجين المهرة في تقنيات الحاسب الآلي وبرمجته وشبكاته والقادرين على التعامل معها بخبرة ودراية ؛ بحيث يقدمون حلولاً لمشاكل صعبة بدافع الإصلاح وضمن قوانين معمول بها. وبالرغم من أنه في المجتمع الحاسوبي (المتخصصين في الحاسب الآلي وتقنياته) مازال هذا الوصف قائماً وله مدلولات إيجابية ولا يجب خلطه خطأً مع الفئة الأخرى من المبرمجين اللذين يمتلكون مهارات الهاكرز نفسها (يطلق عليهم المخربون أو الكراكرز (Crackers)) ولكنهم يوظفونها في القيام بأعمال غير شرعية مثل السطو على البرامج وفك شيفرتها ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب ، إلا أنه في المجتمعات الأخرى غير المتخصصة (مثل مجتمع مستخدمي الإنترنت) أطلق على الكراكرز لقب هاكرز لأنه اسم مترادف مع كلمة هاكرز مما أثر سلباً على المعنى الإيجابي للهاكرز ، وبالتالي أصبحت كلمة "هاكرز" كلمة شائعة الاستخدام في الإنترنت ومقترنة دائماً بأفعال تخريبية والدخول غير المشروع على أجهزة وشبكات الحاسب الآلي بغرض التجسس أو السرقة أو التخريب...وخلافه. وانطلاقاً من هذه النقطة سوف نستخدم كلمة "هاكرز" بمعناها الشائع في الإنترنت.

1.4 الاختراق

يُعرف الاختراق - بصفة عامة - بأنه اقتحام مكان معين عن طريق الوصول عن بُعد (Remote Access) بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بهذا المكان بغرض القيام بأعمال غير مشروعة ، وبصفة خاصة ، الدخول على جهاز أو شبكة حاسب بطريقة غير شرعية من قبل جهاز آخر بغرض القيام بأعمال غير مشروعة.

□ طرق الاختراق

بطبيعة الحال تتوقف طرق الاختراق على قدرات المخترق ، ومن أهم

- هذه الطرق ما يلي :
- اختراق المزودات أو الأجهزة الرئيسة للشركات والمؤسسات أو الجهات الحكومية، وذلك باختراق الجدران النارية التي عادة توضع لحمايتها. وغالبا ما يتم عن طريق انتحال شخصية للدخول إلى النظام من خلال محاكاة عناوين بروتوكول الإنترنت (IP Addresses) التي يثق بها النظام المراد اختراقه.
 - اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات، وهي طريقة للأسف شائعة لعدم دراية أصحاب الأجهزة الشخصية بمبادئ حماية أجهزتهم من جانب ولسهولة تعلم برامج الاختراقات وتعددتها من جانب آخر. ومن أهم آثار هذا الاختراق اقتناص كلمات السر التي يستخدمها الشخص للحصول على خدمات مختلفة كالدخول إلى الإنترنت حيث يلاحظ الضحية أن ساعاته تنتهي دون أن يستخدمها وكذلك انتحال شخصية في مندييات الحوار.
 - التعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة. وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية. ومن آثار هذا الاختراق السطو بقصد الكسب المادي كتحويل حسابات البنوك أو الحصول على خدمات مادية أو أي معلومات ذات مكاسب مادية كأرقام بطاقات الائتمان والأرقام السرية الخاصة ببطاقات الـ ATM. وفي هذا السياق نحذر من إعطاء أرقام بطاقات الائتمان لمواقع التجارة الإلكترونية عبر الإنترنت بدون التأكد بالتزام تلك المواقع بمبدأ الأمان.

□ أشكال الاختراق

- تتعدد أشكال الاختراق بتعدد الجهات التي تقوم به والتقنيات المستخدمة في ذلك ، ومن أهم أشكال الاختراق التي يتعرض لها مستخدم الانترنت ما يلي:
- اختراق نظامي من السلطات بشكل معلن أو غير معلن ، وجميع الدول تقريبا فيها اختراق من هذا النوع بما فيها الدول الغربية والعربية وأمريكا.
 - اختراق من قبل الهاكرز من خلال ثغرة في منافذ اتصال المستخدم. وفي هذا الخصوص يجب على المستخدم معرفة ثغرات الاختراق والعمل على تلافيها ، وكذلك مبادئ حماية جهازه من

الهاكرز وتطبيقها بقدر ما يستطيع مع الأخذ بالاحتياطات اللازمة
الواجب إتباعها للوقاية من عمليات الاختراق من قبل الهاكرز.
• اختراق عن طريق ملفات (فيروسات) التجسس ، وهو أكثر
خطورة من السابق حيث يتمكن الهاكرز من تثبيت ملف تجسس في
جهاز المستخدم للقيام بإرسال معلومات حسب الطريقة التي يرمج
بها. وفي هذا السياق يجب على المستخدم معرفة كيف يصاب جهازه
بملفات التجسس ، وكيفية البحث عنها وإزالتها ، وكذلك الاحتياطات
الواجب إتباعها للوقاية من ملفات التجسس.

❑ ثغرات الاختراق

- يوجد العديد من الثغرات التي يمكن من خلالها اختراق أنظمة
الحاسبات منها :
- اختراق النظام عن طريق الحصول على صلاحيات المسؤول عنه أو
ما يعرف بمصطلح (Administrator Control) في نظام الويندوز
والذي يتميز بقدرته على القيام بأي عمل في النظام.
 - اختراق النظام من قبل موظف ذي صلاحيات كثيرة والقيام بالعديد
من العمليات الخطيرة على النظام من داخل النظام نفسه بغرض
الانتقام من شركته لأي سبب من الأسباب ، وتشير الإحصائيات إلى
أن هذه النوعية من الاختراقات تشكل النسبة الكبيرة من الاختراقات
التي تتم في العالم.
 - اختراق النظام عن طريق تثبيت برمجيات في لب نظام التشغيل
نفسه بغرض السيطرة على أوامر النظام ، والدخول إلى البيانات
بغرض تدمير النظام.
 - اختراق النظام عن طريق الثغرات الأمنية فيه.
 - اختراق النظام عن طريق سرقة كلمات السر الخاص بالنظام .
 - اختراق النظام عن طريق الفيروسات و ملفات التجسس حصان
طروادة (Trojan)، وهي برامج تزرع خلصة ومصممة خصيصا
للتسبب في التدمير ، أو لفتح ثغرات أمنية لتنفيذ هجمات من خلالها
في أوقات لاحقة، وهو الأسلوب الذي يطلق عليه "الأبواب الخلفية" (Backdoors).

❑ أسباب الاختراق

- بعض الهاكرز يمارسون عمليات الاختراق كهواية وفرصة لإظهار
الإمكانات وتحدي الذات ، والبعض الآخر يمارس هذا العمل بدافع
تحقيق عدة أهداف غير مشروعة أو تدميرية تختلف من هاكرز لآخر ،
نذكر منها ما يلي :
- الحصول على المال من خلال سرقة المعلومات البنكية مثل أرقام

- الحسابات أو البطاقات الائتمانية.
- الحصول على معلومات أو صور شخصية بدافع الابتزاز لأغراض مالية.
- الحصول على الرموز السرية للبريد الإلكتروني ليتسنى له التجسس على الرسائل الخاصة أو سرقة اسم البريد الإلكتروني بأكمله.
- الحصول على الرمز السري لأحد المواقع بهدف تدميره أو التغيير في محتوياته.
- الانتقام من أحد الأشخاص من خلال تدمير جهازه الشخصي أو من أحد الجهات من خلال تدمير شبكتها الخاصة أو موقعها على الإنترنت.
- اقتناص كلمات السر التي يستخدمها الضحية للحصول على خدمات مختلفة كالدخول إلى الإنترنت حيث يلاحظ الضحية أن ساعاته تنتهي دون أن يستخدمها، وكذلك انتحال شخصيته في منتديات الحوار.

أسئلة تقويم ذاتي



- 1/ من هم الهاكرز ومن هم الكراكرز وما الفرق بينهم؟
- 2/ انتشرت في الآونة الأخيرة ظاهرة الاختراق ما أهم طرقه؟
- 3/ ما أهم أشكال الاختراق التي يتعرض لها مستخدم الإنترنت؟
- 4/ اشرح هذه العبارة : " هناك العديد من الثغرات الأمنية التي يمكن من خلالها اختراق الأنظمة مهما تعددت وسائل حماية الحاسبات".
- 5/ ما أهم الدوافع وأسباب الاختراق؟

ملف 2.4

عزيزي ال

أيضاً حصان طروادة "Trojan" أو الحزم "Patch" ما هي إلا نوع من أنواع أشباه الفيروسات يتم دسها وتشغيلها داخل جهاز الحاسب الخاص بالضحية بدون علمه للقيام بأغراض التجسس على جميع أعماله التي يقوم بها على حاسبه الشخصي وتسجيلها. وبواسطة هذه

الملفات يستطيع الهاكرز الدخول إلى جهاز الضحية من خلال المنافذ الخاصة بها والتي تقوم بفتحها ، وذلك عن طريق أحد برامج التجسس (في هذه الحالة يطلق عليه عميل "Client" التي ترتبط مع ملف التجسس (الذي يعمل في هذه الحالة كخادم "Server") والذي يستطيع الهاكرز أن يضع له "اسم مستخدم" و "كلمة مرور" تخوله أن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى جهاز الضحية ، وكذلك يستطيع أن يجعل جهاز الضحية مفتوحاً فيستطيع أي هكرز أن يدخل إلى هذا الجهاز.

1.2.4 طرق الإصابة بملفات

التجسس

عزيزي الدارس ، من أهم الطرق التي يمكن من خلالها أن يصاب جهازك بملفات التجسس ما يلي :

① الطريقة الأولى : عبر جلسات المحادثة أو الحوار : أن يصلك ملف التجسس من شخص خلال استخدامك برامج المحادثة أو الحوار عبر الإنترنت بأن يرسل أحد الهاكرز لك صورة أو ملفاً يحتوي على الحزم (Patch) أو حصان طروادة (Trojan) بدون علمك.

② الطريقة الثانية : عبر البريد الإلكتروني : أن يصلك ملف التجسس من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ما هو الشخص المرسل، فتقوم بتنزيل الملف المرفق مع الرسالة ومن ثم فتحه وأنت لا تعلم بذلك.

③ الطريقة الثالثة : من خلال إنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع المخلة بالآداب، أو المواقع التي تساعد على تعليم التجسس.

④ الطريقة الرابعة : من خلال زيارة المواقع المشبوهة : الدخول إلى مواقع مشبوهة مثل المواقع المخلة بالآداب أو المواقع المشبوهة ، حيث إنه بمجرد دخولك إلى هذه المواقع فإنه يتم تنزيل ملفات التجسس في جهازك بطريقة لا تدري عنها شيئاً.

⑤ الطريقة الخامسة : استخدام أقراص تخزين خارجية مصابة : بأن تقوم بتحميل أو تشغيل ملفات أو برامج من قرص مرن أو مدمج مصاب بملف تجسس.

□ طرق الوقاية من الإصابة بملفات التجسس

- من أهم طرق الوقاية من إصابة جهازك بملفات التجسس ما يلي :
- عدم فتح أي رسالة لا تعرف صاحبها أو مصدرها.
- عدم استقبال أي ملف أو برنامج من أشخاص لا تعرفهم معرفه جيده أثناء استخدام برامج المحادثة أو الحوار.
- عدم القيام مطلقاً بتنزيل أي ملفات أو برامج من مواقع غير معروفة أو غير موثوق بها.
- عدم القيام مطلقاً بزيارة المواقع المخلة بالآداب أو المواقع المشبوهة الأخرى.
- تثبيت برنامج لكشف ملفات التجسس والفيروسات (مثل : Norton و Cleaner) لفحص أي ملف أو برنامج تستقبله أثناء جلسات المحادثة أو الحوار أو قمت بتنزيله من موقع قبل فتحه أو استخدامه.
- عدم استخدام أقراص تخزين خارجية قبل فحصها من قبل برامج كشف ملفات التجسس والتأكد من عدم تلوثها بها.

□ مقومات الاختراق من خلال ملفات التجسس

- من أهم المقومات التي تساعد الهاكرز على عملية الاختراق من خلال ملفات التجسس ما يلي :
- **وجود ملف تجسس :** يستطيع الهاكرز اختراق جهازك والعبث به في حالة وجود ملف تجسس (يطلق عليها أيضاً حصان طروادة "Trojan"، أو الحزم "Patch" والذي يُعد بمثابة بوابة الدخول لجهازك عن طريق أحد برامج الاختراق التي ترتبط مع ملف التجسس الموجود على جهازك ، كما تم توضيحه سابقاً).
- **الاتصال بالإنترنت :** لا يستطيع الهاكرز أن يدخل إلى جهازك إلا إذا كنت متصلاً بالإنترنت ، أما إذا كان جهازك غير متصل بشبكة الإنترنت أو أي شبكة أخرى فمن المستحيل أن يدخل أحد إلى جهازك سواك. ولذلك إذا أحسست بوجود هكر في جهازك فسارع إلى قطع الاتصال بسرعة حتى تمنع الهاكرز من مواصلة التلصص والعبث في جهازك.
- **برنامج اختراق :** حتى يتمكن الهاكرز العادي من اختراق جهازك لابد أن يتوافر معه برنامج يساعده على الاختراق ، بحيث يكون مرتبطاً مع ملف التجسس الموجود على جهازك. ومن أشهر برامج الاختراق التي يستخدمها الهاكرز ما يلي :

Back Oriface , Net Bus 2000 , Sub Seven , Heack'a
.Tack'a

□ في العموم تُعد كلمة السر من أهم المداخل الخطيرة للاختراق ،
لذا يجب مراعاة بعض القواعد المهمة عند اختيار
كلمات السر للمستخدمين منها على سبيل المثال

؛

- لا يجب أن تكون كلمات السر أقل من ثمانية أحرف.
- لا تكون من الأسماء المشهورة.
- لا تكون من الكلمات الموجودة في القواميس.
- لا تكون هي اسم المستخدم أو بيانات خاصة به.
- لا تكون كلها أرقاماً أو حروفاً.
- لا تدوم فترة طويلة.

أسئلة تقويم ذاتي

؟

- 1/ ما طبيعة ملفات التجسس؟ وما أهم الطرق التي يمكن من خلالها إصابة الأجهزة بها؟
- 2/ عدد في نقاط أهم طرق الوقاية لمنع إصابة جهازك بملفات التجسس.
- 3/ ملف التجسس في حد ذاته لا يقوم بأي عمل تخريبي ولا يسبب أي أضرار للجهاز ، ولكنه يُعد أداة للتصنت ، اشرح هذه العبارة.
- 4/ وضح أهم المقومات التي تساعد الهاكرز على عملية الاختراق من خلال ملفات التجسس .
- 5/ هناك قواعد مهمة عند اختيار كلمات السر للمستخدمين اذكر بعضاً منها.

□ ومن أهم الأخطاء التي تؤدي إلى سهولة اختراق الشبكة ما يلي :

- وضع كلمات مرور سهلة عند الدخول إلى الإنترنت.
- عدم تحديث الأنظمة عند العثور على فجوات أمنية.
- استخدام بروتوكولات غير مشفرة لإدارة الشبكة مثل Telnet .
- إرسال الكلمات السرية عبر الهاتف .
- تعيين أشخاص غير مدربين للعمل في أمن الأنظمة.
- عدم استيعاب مفهوم الأمن بالشكل العملي.
- الاعتماد على الجدران النارية وترك المتابعة الشخصية.
- فتح الملحقات التي تأتي مع البريد الإلكتروني و لو من مصدر مجهول.
- عدم استخدام الرقع الأمنية وخصوصاً رقع المتصفحات.
- تركيب برامج من مصادر غير معروفة.
- ربط الأنظمة قبل تركيب برامج الحماية ، ويُعد استخدام برمجيات الحماية مع الشبكات أمراً ضرورياً للحد من المخاطر التي قد تواجه الشبكة ، وخصوصاً عند اتصال الشبكة مع الإنترنت بصورة دائمة .

□ وتنقسم برامج حماية الشبكات إلى ثلاثة أنواع :

① **برامج جدار ناري بين الشبكة و العالم الخارجي (Firewall) :** و برامج الجدران النارية يفضل أن تكون على أجهزة مستقلة وتعمل كنقطة دخول وحيدة إلى الشبكة. وتكون هذه البرامج على قدر كبير من الذكاء الذي يمكن أن يستغل لتدريبها على قبول الطلبات الصديقة ورفض الطلبات المتلصصة ، ويمكن كذلك أن تمنع أجهزة معينة من الدخول ، ويمكن أن تصرح لعدد محدود من المستخدمين أو الأقسام للاتصال بالعالم الخارجي ، وكذلك يمكن أن تمنع عدداً من التطبيقات و الخدمات من التعامل مع الشبكة مثل خدمة تصفح الإنترنت. وهناك عدد من الشبكات تكون بها الجدران النارية غير عملية، وذلك عندما تكون الشبكة مخصصة لتقديم الخدمات لمستخدمين يتصلون من أماكن غير معروفة، مثل الجامعات التي من المفترض أنها تقدم خدمات لأشخاص مجهولين.

② **برامج فحص حالة المنافذ و الثغرات في مكونات الشبكة ((Security Scanners :** وهي عبارة عن برامج تفحص الشبكة من الداخل للبحث عن الثغرات التي يمكن أن تتعرض منها للهجوم من قبل متلصصين.

③ **برامج حماية من الفيروسات (Virus Protection) :** وهي برامج تقوم بالكشف عن الفيروسات وإزالتها من قرص التخزين الثابت في جهاز الحاسب ، كما أنها تُعد خط دفاع أول لمنع الفيروسات من الدخول لجهاز الحاسب.

بصفة عامة ، تواجه أجهزة وشبكات الحاسبات مخاطر أمنية يمكن تصنيفها إلى ثلاثة أصناف: مخاطر طبيعية ، ومخاطر داخلية ، ومخاطر خارجية. فالمخاطر الطبيعية تشمل الكوارث الطبيعية كالحرائق والزلازل ، أما المخاطر الداخلية فتتمثل في عمليات التخريب التي تصدر من أشخاص يعملون داخل المؤسسة نفسها التي تملك أجهزة الحاسبات والشبكات ، وأما المخاطر الخارجية فتصدر من أشخاص من خارج المؤسسة بدخلوهم على الشبكة بطريقة غير مشروعة ، وهم ما ينطبق عليهم وصف المخربين (Crackers) ، أو من خلال تصدير فيروس مدمر للشبكة يقوم بتدمير بياناتها.

نشاط



التعرف على إحدى برمجيات مكافحة التجسس وليكن برنامج "Zone Alarm pro" والذي يُعد من أحدث وأقوى برامج مكافحة الاختراق التي تعمل على مبدأ الجدران النارية (Firewall) في الوقت الحالي ، حيث إنه يتحكم ألياً ويمنع أي محاولة للاختراق ويقوم بإظهار شاشة تحوي رقم الـ IP ورقم المنفذ لكل محاولة اختراق ، ويعطي المستخدم حرية الاختيار في منعه أو السماح له أو تجاهله. ويتميز هذا البرنامج بالعديد من المميزات من الأفضل التعرف عليها من خلال البرنامج نفسه والذي يمكن الحصول عليه من موقع الشركة المنتجة www.zonealarm.com . كما ينصح العديد من الخبراء والكتاب باستخدام هذا البرنامج كبرنامج حماية من الاختراق.

أسئلة تقويم ذاتي

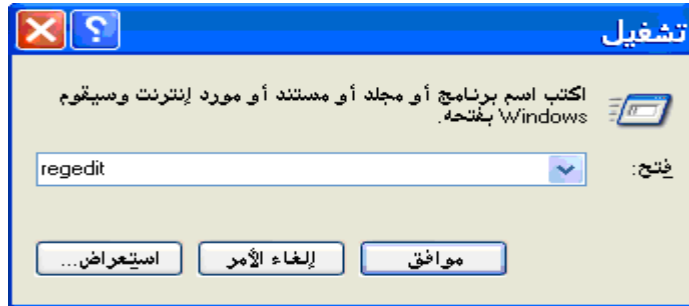


- 1/ ما أهم الأخطاء التي تؤدي إلى سهولة اختراق شبكات الحاسب الآلي ؟
- 2/ ما هي أهم أنواع برمجيات حماية الشبكات؟ مع تحديد الفرق بينهم.
- 3/ بصفة عامة ، تواجه أجهزة وشبكات الحاسب الآلي مخاطر أمنية يمكن تصنيفها إلى ثلاثة أنواع : مخاطر طبيعية ، ومخاطر داخلية ، ومخاطر خارجية ، اشرح هذه العبارة مستعيناً بأمثلة.

١١ التعرف على الطرق اليدوية التي يمكن للمستخدم العادي القيام بها للبحث عن ملفات التجسس وإزالتها

● طريقة البحث داخل محرر النظام (Registry Editor) :

للبحث داخل ملفات التسجيل اتبع الخطوات التالية : اضغط على زر
"ابدأ" (Start) ، ثم اختر الأمر "تشغيل" (Run) ، ثم اكتب الأمر "
regedit" كما هو موضح بالشكل التالي ، ومن ثم انقر على الزر
"موافق".



ثم بعد النقر على زر "موافق" سوف تظهر لك شاشة "محرر
النظام" (Registry Editor) ، افتح المجلدات التالية (بالنقر عليها)
بالترتيب :

HKEY_LOCAL_MACHINE

Software

Microsoft

Windows

Current Version

Run (and Run Service , and Run Once , ...etc.)

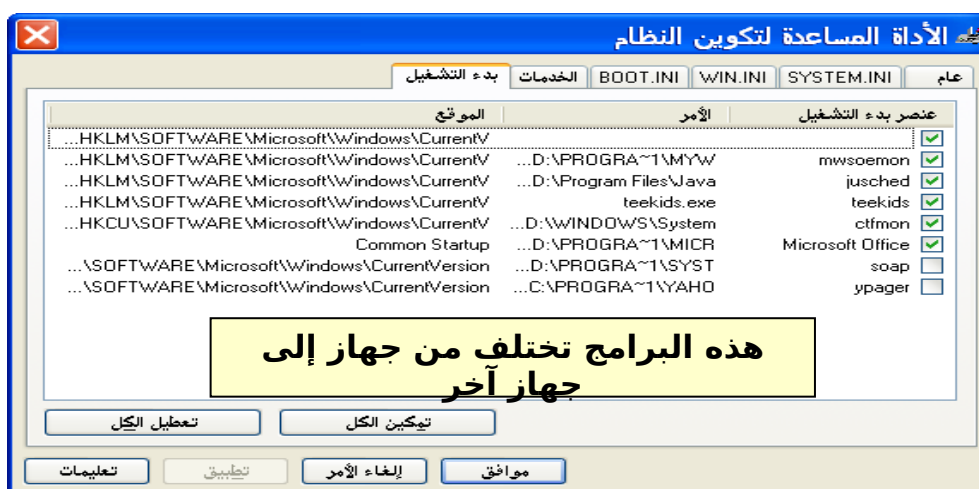
بعد فتح المجلد "Run" سوف تظهر لك شاشة "محرر النظام" كما
هي موضحة بالشكل التالي ، الجزء الأيسر منها (في حالة وجود
قائمة "ابدأ" على يمين الشاشة ، أي النسخة العربية من ويندوز إكس
بي) ، منقسم إلى ثلاث قوائم : "الاسم" (Name) ، و "النوع" (Type) ، و "البيانات" (Data) ، حيث يوجد في قائمة "الاسم" أسماء
الملفات التي تعمل مع بدء تشغيل نظام التشغيل ويندوز ويقابلها
في قائمة "البيانات" عنوان (مسار) الملف.



ابحث عن ملفات التجسس (الخادم) مثل Server.exe , Patch.exe , umg32.exe , Explo32.exe , .exe , وخلافه من الملفات المعروفة بالتجسس) في قائمة "البيانات". وفي حالة العثور على ملف تجسس قم بإزالته بالضغط عليه بالزر الأيمن

ملحوظة
في حالة وجود ملف في قائمة "الاسم" لا يقابله عنوان في قائمة "البيانات" أو ظهر أمامه سهم صغير >--- , فهو ملف تجسس إذ ليس له عنوان معين بالويندوز. وكذلك الأمر في حالة وجود برامج ذات امتداد ".exe" تحت قائمة "الاسم" فإن ذلك يعني أن جهازك مصاب بملف تجسس. على الفور قم بحذف هذه الملفات. ولكن كن حذراً من أن تقوم بحذف ملف من ملفات النظام الضرورية لتشغيل النظام بصورة

واختر الأمر "delete" وبعد ذلك
● طريقة البحث داخل قائمة بدء التشغيل (Start Up) : للبحث داخل قائمة بدء التشغيل اتبع الخطوات التالية : اضغط على



زر "ابدأ" (Start)، ثم اختر الأمر "تشغيل" (Run)، ثم اكتب الأمر "msconfig" في المكان المخصص لتشغيل البرامج ، ومن ثم انقر على الزر "موافق" ، سوف تظهر لك نافذة "الأداة المساعدة لتكوين النظام" (System Configuration Utility) ، ومن ثم اختر تبويب "بدء التشغيل" (Startup) لعرض البرامج التي تعمل مع بداية تشغيل الجهاز كالموضحة بالشكل التالي.

بعد ذلك افحص برامج قائمة "بدء التشغيل" وتأكد من عدم وجود أي برنامج غريب أو غير معروف لك . وفي حالة وجود أي ملف من ملفات التجسس قم بإلغاء الإشارة الموجودة في المربع المقابل له ، فتكون بذلك قد أوقفت نشاط هذا البرنامج أو أي برنامج آخر غير مرغوب في وجوده. فمثلاً يوجد بالشكل السابق الملف "teekids" خاص بالفيروس "w32.Blaster.c.worm" ، لذا يجب إلغاء الإشارة الموجودة بالمربع المقابل له ، ومن ثم العمل على إزالته من جميع المواقع الموجودة بها داخل الجهاز وخصوصاً ملف التسجيل إما يدوياً بالبحث عنه في ملف التسجيل وإزالة القيم الخاصة به ، أو يفضل استخدام برنامج مكافحة الفيروسات الخاص به لإزالته.

الخلاصة

❏ **عزيزي الدارس،** قسمت الوحدة جرائم نظم المعلومات إلى جرائم عامة، وجرائم مادية، وجرائم اقتصادية، وجرائم ضد الأفراد .
 ❏ حماية البيانات - بصفة عامة - لجميع المستخدمين يتركز على أربعة محاور مهمة وهي :
 - حماية جهاز الحاسب وملحقاته من التأثيرات الكهربائية غير المرغوب فيها .
 - حماية جهاز الحاسب الآلي من حدوث خلل بسبب ظروف بيئة التشغيل المحيطة بالجهاز .
 - حماية البيانات عن طريق القيام بعملية التخزين الاحتياطي كل فترة زمنية وبصفة دورية.
 - حماية بيانات شبكة الحاسب من الإضرار بها .
 ❏ عرّفت الوحدة الفيروس بأنه برنامج كمبيوتر يتكون من عدة برامج فرعية مكتوب بإحدى لغات البرمجة مثل أي برنامج تطبيقي آخر موجود على الحاسب الآلي ، ليس هناك اختلاف إلا في الغرض الذي صمم من أجله ، وهو - في معظم الأحيان - إصابة الحاسب الآلي وإتلاف برامجه وبياناته.
 ❏ بينت الوحدة أهم خصائص الفيروسات وهي : القدرة على الاختفاء، التكاثر، التنقل، البصمة، التدمير .
 ❏ تناولت الوحدة أشباه الفيروسات وذكرت أنها أنواع من البرامج التدميرية ينطبق عليها تعريف الفيروس جزئياً ، أي يتوافر فيها بعض من خصائص الفيروسات سابقة الذكر وليس كلها، حيث تشترك هذه الأنواع مع الفيروسات في أنها تعمل بدون علم المستخدم بصورة خفية ، وتقوم بأعمال ضمن الكمبيوتر مصممة عمداً لتنفيذها.
 ❏ تناولت الوحدة أهم طرق وأسباب انتشار الإصابة بالفيروسات ، وهي :
 مشاركة الملفات عن طريق شبكات الحاسب الآلي، نسخ البرامج من النشرات الإلكترونية - تثبيت برنامج جديد في الحاسب الآلي - من خلال نقل الأجهزة نفسها استخدام اسطوانة مصابة بالفيروس من خلال مرفقات البريد الإلكتروني والتداول السيئ للبرامج .
 ❏ بينت الوحدة أن كلمة "هاكرز" كلمة شائعة الاستخدام في الإنترنت ومقترنة دائماً بأفعال تخريبية والدخول غير المشروع على أجهزة وشبكات الحاسب الآلي بغرض التجسس أو السرقة أو التخريب...وخلافه.
 ❏ يُعرف الاختراق - بصفة عامة - بأنه اقتحام مكان معين عن طريق الوصول عن بُعد (Remote Access) بطريقة غير مشروعة عن

طريق ثغرات في نظام الحماية الخاص بهذا المكان بغرض القيام بأعمال غير مشروعة ، وبصفة خاصة ، الدخول على جهاز أو شبكة حاسب بطريقة غير شرعية من قبل جهاز آخر بغرض القيام بأعمال غير مشروعة.

الخصت الوحدة أهم مقومات الاختراق من خلال: ملفات التجسس، وجود ملف تجسس، - الاتصال بالإنترنت، برنامج اختراق. وبينت الوحدة أن كلمة السر تُعد من أهم المداخل الخطيرة للاختراق، وبينت أنه يجب مراعاة بعض القواعد المهمة عند اختيار كلمات السر للمستخدمين وذكرت منها على سبيل المثال : لا يجب أن تكون كلمات السر أقل من ثمانية أحرف، لا تكون من الأسماء المشهورة - لا تكون من الكلمات الموجودة في القواميس، لا تكون هي اسم المستخدم أو بيانات خاصة به، لا تكون كلها أرقام أو حروف، ولا تدوم فترة طويلة.

- بينت الوحدة أن برامج حماية الشبكات تنقسم إلى ثلاثة أنواع هي:
 - برامج جدار ناري بين الشبكة و العالم الخارجي (Firewall) .
 - برامج فحص حالة المنافذ و الثغرات في مكونات الشبكة ((Security Scanners .
 - برامج حماية من الفيروسات (Virus Protection) .

لمحة مسبقة عن الوحدة التالية

الوحدة التالية تأتي بعنوان " بعض القضايا الاقتصادية في الحوسبة "، وهي تتناول الاحتكار والصور المتعددة له ، كما تناقش مفهوم الاحتكار في النظرية الاقتصادية والفكر الإسلامي ، وتتناول الوحدة الاحتكار ومزاياه للشركات و الضرر الذي يسببه الاحتكار للمستهلك ، تقدم الوحدة كذلك العديد من التفاصيل المتعلقة بأحوال العمالة في حقول العمل عامة وفي حقول الحاسب الآلي خاصة في كل من الهند والصين ، وتتناول الوحدة كذلك التسعير والعوامل التي تؤثر على السعر المقترح للمنتج: أهم طرق التسعير استراتيجيات التسعير، والتسعير وحيثياته في المنظور الإسلامي .

إجابات التدريبات

تدريب (1)

يُعد برنامج Norton Antivirus وبرنامج McAfee VirusScan من أشهر برامج الحماية من الفيروسات .

مسرد المصطلحات

❖ الفيروس Virus

هو برنامج كمبيوتر يتكون من عدة برامج فرعية مكتوب بإحدى لغات البرمجة مثل أي برنامج تطبيقي آخر موجود على الحاسب الآلي ، ليس هناك اختلاف إلا في الغرض الذي صمم من أجله وهو - في معظم الأحيان - إصابة الحاسب الآلي وإتلاف برامجه وبياناته.

❖ الدودة (Worm)

هي برنامج يعيد إنتاج نفسه ، لكنها لا تلوث برامج أخرى ، وتنسخ نفسها من وإلى الأقراص المرنة ، أو عبر الشبكات ، ويعتمد بعضها على الشبكة في إنجاز عملها.

❖ حصان طروادة (Trojan horses)

هو برنامج مكر مدمر يختبئ ضمن برامج يبدو مظهرها بريئاً (خدمة أو تطبيق) بحيث يغري المستخدم بأهميته أو بشكله أو باسمه ، وعندما يشغل المستخدم واحداً من هذه البرامج ، ينشط الجزء الماكر ويقوم بعمل معين مصمم له. وفي الغالب يقوم بعمل بوابة

خلفية (Backdoor) تُمكن المخترقين من الدخول على الجهاز المصاب والعبث به.

❖ النشرات الإلكترونية

مجموعة ملفات تتضمن قواعد بيانات وبرامج عامة يتم تحديثها بانتظام ، توضع في متناول كثير من المستخدمين الذين يتقاسمون عملاً مشتركاً.

❖ الهاكرز Hackers

أول ما أطلقت هذه الصفة كانت تشير إلى المبرمجين المهرة في تقنيات الحاسب الآلي وبرمجته وشبكاته والقادرين على التعامل معها بخبرة ودراية ؛ بحيث يقدمون حلولاً لمشاكل صعبة بدافع الإصلاح وضمن قوانين معمول بها. وبالرغم من أنه في المجتمع الحاسوبي (المتخصصين في الحاسب الآلي وتقنياته) مازال هذا الوصف قائماً وله مدلولات إيجابية ولا يجب خلطه خطأً مع الفئة الأخرى من المبرمجين اللذين يمتلكون مهارات الهاكرز نفسها (يطلق عليهم المخربون أو الكراكرز "Crackers")

❖ المخربون أو الكراكرز Crackers

اسم يشير للفئة الأخرى من المبرمجين اللذين يمتلكون مهارات الهاكرز نفسها ولكنهم يوظفونها في القيام بأعمال غير شرعية مثل السطو على البرامج وفك شفرتها ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب ، إلا أنه في المجتمعات الأخرى غير المتخصصة (مثل مجتمع مستخدمي الإنترنت) أطلق على الكراكرز لقب هاکرز لأنه اسم مرادف مع كلمة هاکرز مما أثر سلباً على المعنى الإيجابي للهاكرز ، وبالتالي أصبحت كلمة "هاكرز" كلمة شائعة الاستخدام في الإنترنت ومقترنة دائماً بأفعال تخريبية والدخول غير المشروع على أجهزة وشبكات الحاسب الآلي بغرض التجسس أو السرقة أو التخريب... وخلافه.

❖ الاختراق

يُعرف الاختراق - بصفة عامة - بأنه اقتحام مكان معين عن طريق الوصول عن بُعد (Remote Access) بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بهذا المكان بغرض القيام بأعمال غير مشروعة ، وبصفة خاصة ، الدخول على جهاز أو شبكة حاسب بطريقة غير شرعية من قبل جهاز آخر بغرض القيام بأعمال غير مشروعة .

❖ ملفات التجسس

يمكن القول بأن ملفات التجسس (يطلق عليها أيضاً التروجان Trojan) أو الباتش (Patch)) وما هي إلا نوع من أنواع أشباه الفيروسات يتم دسها وتشغيلها داخل جهاز الحاسب الخاص بالضحية بدون علمه للقيام بأغراض التجسس على جميع أعماله التي يقوم بها على حاسبه الشخصي وتسجيلها.

❖ برامج فحص حالة المنافذ و الثغرات في مكونات

الشبكة ((Security Scanners

وهي عبارة عن البرامج التي تفحص الشبكة من الداخل للبحث عن الثغرات التي يمكن أن تتعرض منها للهجوم من قبل متلصصين.

❖ برامج حماية من الفيروسات (Virus Protection)

وهي برامج تقوم بالكشف عن الفيروسات وإزالتها من قرص التخزين الثابت في جهاز الحاسب ، كما أنها تُعد خط دفاع أول لمنع الفيروسات من الدخول لجهاز الحاسب.

المراجع

أولاً:- مراجع باللغة العربية:

حسن طاهر داود، "جرائم نظم المعلومات"، أكاديمية نايف

العربية للعلوم الأمنية، الرياض 1420-2000م.

**السيد محمود الربيعي، وآخرون، "أساسيات الحاسب الآلي
وتطبيقاته في التعليم"، مكتبة الرشد، الرياض 2006م.**

ثانياً:- مراجع باللغة الإنجليزية:

**Infotech, English for Computer Users, Student Book, (3
.Second Edition, Santiago Remacha Esteras, 1999**