مدخل إلى تقنية المعلومات
LEC #10

أستاذة المادة: ع.عذاري الراجحي
البريد الإلكتروني: athari.alrajhi@gmail.com

الحماية من المخاطر/ الهجوم

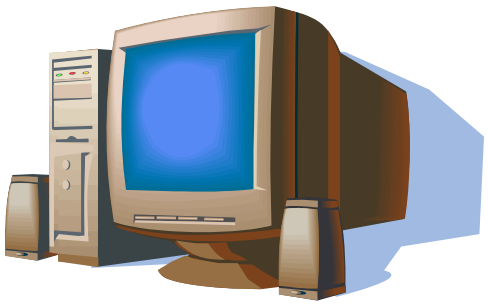
الفيروسات(Viruses)

فيروس الحاسوب: عبارة عن برنامج يدخل للحاسب ليدمر أو يشوه البيانات والبرامج المخزنة داخل الحاسوب.

- **ينتقل فيروس الحاسب إلى حواسيب أخرى عن طريق:**

١. شبكات الحاسوب Computer Network

٢. استخدام الأقراص النقالة الملوثة.



ما هي أنواع الفيروسات الحاسوبية؟

اسم الفيروس	طبيعة عمله
١- الفيروسات الدودية Worms	تتسبب بتوقيف النظام عن العمل من خلال إعادة نسخ نفسه ويحتل هذا النوع من الفيروسات الذاكرة الرئيسية وينتشر بسرعة فائقة جدا في الشبكات.
٢- فيروس القنبلة الموقوتة Time Bombs	عبارة عن برنامج يقوم بتفجير نفسه في وقت محدد أو بعد تنفيذ عدة مرات ويستخدم من قبل شركات الحاسوب التي تعطي نسخا مجانية على أمل شراء النسخة الأصلية لاحقا وإذا لم يقم المستخدم بشراء النسخة الأصلية سيقوم البرنامج بتفجير نفسه.

اسم الفيروس	طبيعة عمله
٣- فيروسات قطاع الإقلاع(الاستنهاض) Boot Sector Viruses	قطاع الإقلاع هو مكان وجود الملفات لتحميل نظام التشغيل عند بدء تشغيل الحاسب.ويحتل هذا الفيروس الأماكن التي يقرأها الحاسب وينفذ التعليمات المخزنة ضمنها على القرص الصلب ضمن جهازك وعند الإقلاع يصيب الفيروس منطقة الإقلاع الخاصة بنظام دوس (record DOS boot) مما يمنع من تشغيل الحاسب كليا.
٤- فيروس ملوثات الملفات File Viruses	تربط نفسها بالملفات التنفيذية التي تنتهي بالامتدادات com , exe وعندما يعمل أحد البرامج الملوثة فإن هذا الفيروس ينتظر في الذاكرة إلى أن يشغل المستخدم برنامجا آخر فيسرع إلى تلويثه وهكذا ويعيد هذا النوع من الفيروس نسخ نفسه.

اسم الفيروس	طبيعة عمله
٥- فيروسات الماكرو Macro Viruses	الماكرو هو عملية تنفذ مجموعة من الأوامر ضمن برنامج ،وقد أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج MS-Word.وعند فتح مستند،ينشط الفيروس ويؤدي مهمته التخريبية بإجرائه تغييرات على كل المستندات الأخرى المنشأة ضمن ذلك البرنامج وقد بُرمج هذا الفيروس لينسخ نفسه إلى ملفات المستندات الأخرى،مما يؤدي إلى ازدياد انتشاره مع استمرار استخدام البرنامج.
٦- فيروس حصان طروادة Trojan Horse	عبارة عن برنامج يدخل الحاسب بشكل شرعي وهذا النوع لاينسخ نفسه ولكن عند تثبيته يقوم بعمل معين كأن يقوم بسرقة ملفات أو أرقام سرية من جهازك.وكثير من حصون طروادة تنتقل عبر البريد الالكتروني E-mail ضمن أي ملف أو صورة ولا يعلم المستخدم عن وجودها غالباً.

كيف يصيب الفيروس نظام الحاسوب؟

- الفيروسات تختبئ على القرص وعندما تصل لهذا القرص بوضعه في جهازك أو الاتصال بالشبكة يظهر الفيروس وينسخ نفسه على جهازك ويبدأ بالتخريب .

- **أسوأ مافي الفيروسات:**
  قدرتها على الانتشار من حاسوب لآخر بواسطة أقراص التخزين.

- الانترنت يتيح لك الاتصال بحواسيب العالم كله فلا تدري هل الحاسب الذي تتصل معه نظيف أم مصاب؟ .. لذلك عليك أن:

١. تفعّل دائما برامج فحص الفيروسات والتخلص منها ولا تدخل على الانترنت إلا وهذا البرنامج فعّال لديك.
٢. يجب الاحتفاظ بآخر نسخة من هذه البرامج.

حماية الحاسوب من الفيروسات

عوارض إصابة الحاسوب بالفيروس:

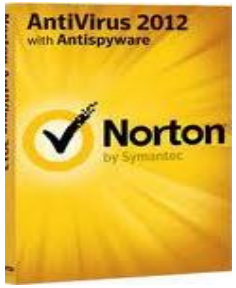
١. بطء تشغيله.
٢. اختفاء الملفات.
٣. إظهار رسالة تبليغ عن ملفات معطوبة.
٤. تعذر الوصول إلى بعض أجزاء الذاكرة.
٥. عدم قدرة البرامج على العمل لعدم وجود مساحة كافية لها في الذاكرة.

حماية الحاسوب من الفيروسات

- لحماية الجهاز من الفيروسات نستخدم برامج مضادة للفيروسات تنتجها شركات خاصة مثل (Norton, PC-Cillin, McAfee)

عمل البرامج المضادة للفيروسات:

١. اكتشاف الفيروسات حين دخولها للحاسب وإخبار المستخدم بوجودها.
٢. تنظيف الأجهزة والبرامج من الفيروسات.



- تسكن هذه البرامج في الذاكرة وتكون نشطة دائما لاكتشاف أي فيروس قادم.
- ينصح المستخدمون باستخدام برنامج مضاد يكون قادر على تنظيف أقراص معينة وتخليص النظام من التلوث وتسمى عملية التنظيف بـ تطهير Disinfecting وكذلك يجب الاحتفاظ بالنسخ المحدثة من هذه البرامج.

حماية الحاسوب من الفيروسات

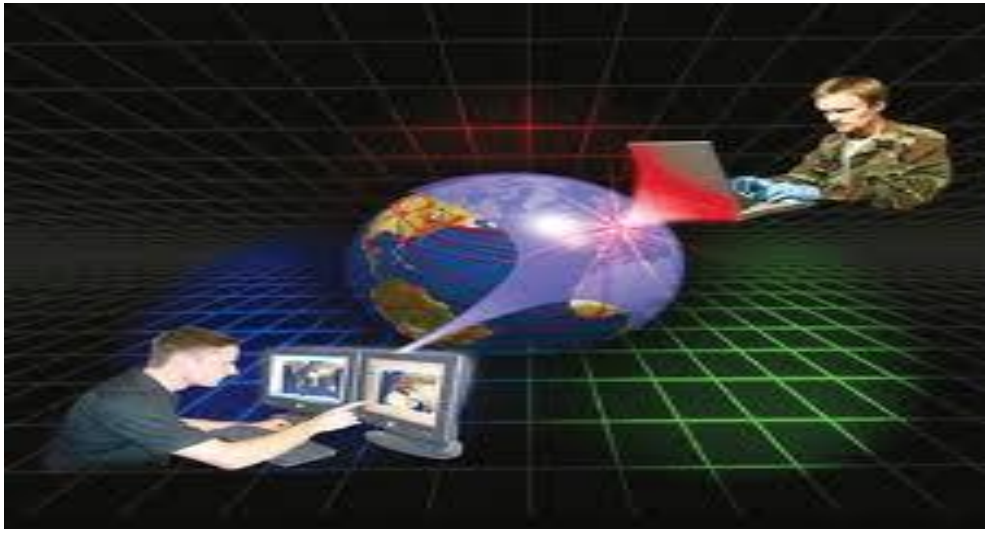
إذا لم تكن النسخة الحديثة من مضادات الفيروسات موجودة لديك قم بما يلى:

١. فحص كل الأقراص للتأكد من خلوها من الفيروسات قبل الاستخدام.
٢. استخدام البرمجيات المسجلة فقط، ولا تقم بإعارة الأقراص الخاصة بالبرمجيات فهذا يعتبر خرقا لقانون حقوق الملكية كما أنها وسيلة سريعة لانتقال الفيروسات.
٣. قم بفحص الملفات التي تقوم بتحميلها من الانترنت.
٤. لا تفتح الملفات المرفقة بالبريد الالكتروني إلا إذا كانت الرسالة من مصدر موثوق.
٥. اجعل الأقراص المرنة في حالة القراءة فقط مما يجعل من الممكن الاطلاع على محتوياتها دون المساس بها، وهناك جزء خاص بتأمين القرص يمكن فتحه أو إغلاقه.
٦. قم بعمل النسخ الاحتياطية بانتظام لتتجنب الضرر الواقع في حال دخول الفيروس.

طرق الوصول غير القانونية(Illegal Access)

الوصول الغير مخول للمعلومات فى أنظمة الحواسيب يتضمن :

- نسخ وتعديل وقفل البيانات في حاسب واحد أو في نظام كامل أو في شبكة من الحواسيب.
- ذلك لان لكل شخص حقا خاصا في بياناته لا يجوز التعدي عليها.



طرق الوصول غير القانونية(Illegal Access)

أشكال الوصول غير المخول:

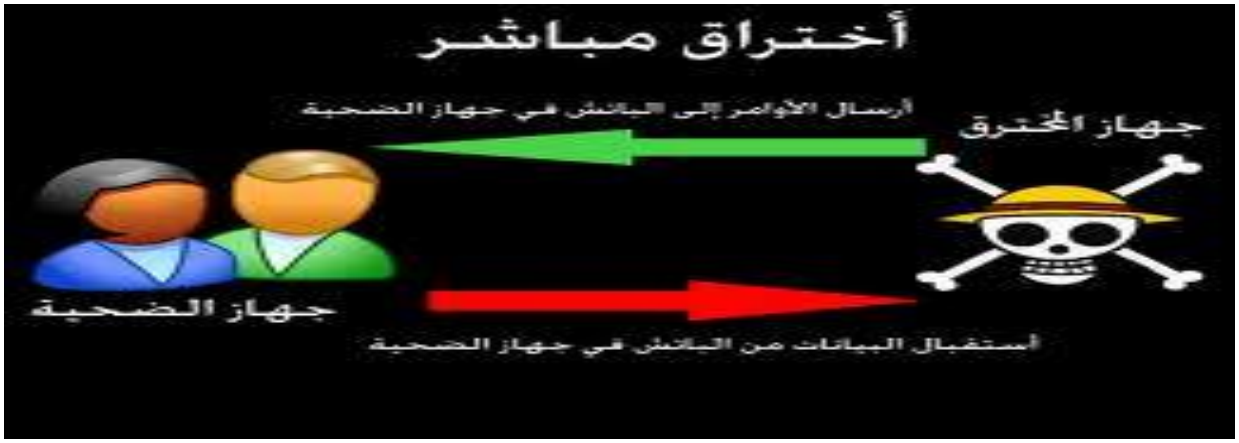
١. إلغاء مواقع الويب أو تخريبها أو التعديل عليها.
٢. ضغط غير مبرر على الشبكة.
٣. تغيير الخادم إلى خادم آخر.
٤. هجوم فيروسي على الشبكة.
٥. استقبال رسائل غريبة على البريد الالكتروني.
٦. البريد الالكتروني مشاهد من قبل أشخاص غير مخولين.
٧. معلومات النظام تصل لأشخاص غير مخولين.
٨. التعديل على قواعد البيانات والوثائق أو تدميرها.

الاختراق (Hacking)

المخترق Hacker:

هو الشخص الذي يمتلك الإمكانات الفنية والمواهب الفائقة في تكنولوجيا المعلومات والذي يخترق أنظمة الحواسيب **بغرض**:

- الاطلاع على بيانات لا يحق له الاطلاع عليها.
- التلصص على خصوصيات الأفراد.
- تخريب حواسيب الغير.
- سرقة الأموال بنقلها الكترونيا من حساب الأشخاص إلى حسابه.



الاختراق (Hacking)

ولذلك كان لزاما على المنشاة التي ستحتفظ ببيانات الأشخاص والمؤسسات أن تحمي هذه البيانات من المخترقين بالطرق التالية:

١. أن تحدد هل سيتم الاحتفاظ بالبيانات لشخص واحد أو لعدة أشخاص أو لأغراض مشروعة.
٢. يجب عدم الإفراط في البيانات وان تكون متناسبة مع الغاية من وجودها.
٣. يجب أن لا يتم الاحتفاظ بالبيانات لمدة أكثر من اللازم.
٤. يجب أن تغلق البيانات أمام أي غرض ينافي الغرض من وجودها.
٥. يجب وضع قيود الأمان والسرية على البيانات من الوصول غير المخول أو التدمير.
٦. حقوق الشخص في الوصول إلي بياناته.

كاسر حماية كلمة المرور Password Cracker

كاسر حماية كلمة المرور:

هو محاولة استرجاع كلمة السر من البيانات المخزنة في النظام، و أحيانا عندما تريد الدخول للنظام أو المنتدى أو للبريد الالكتروني يطلب منك النظام إدخال كلمة السر، وقد تدخلها خطأ أو تكون قد نسيتها،عندها يعطيك النظام عدة فرص لتكتبها مرة أخرى فإذا فعلت تدخل للنظام وإلا تظهر رسالة اعتذار وتمنع من الدخول.
وهذه المحاولات الفاشلة تخزن في ملف يطلع عليه مدير النظام.

علم التشفير
Cryptography

علم التشفير Cryptography

علم التشفير: هو علم تخبئة المعلومات ويعتمد على عدة فروع من العلوم مثل الرياضيات وعلم الحاسب والسرية ونظرية المعلومات والهندسة.

استخداماته:

- في التطبيقات التي تحتاج للسرية مثل بطاقة الصراف الآلي وكلمات العبور والتجارة الالكترونية.
- وهو ضروري جدا في عمليات نقل المعلومات عبر الوسائط غير الموثوق بها والنقل عبر الانترنت.

التشفير وفك التشفير Encryption and Descryption

التشفير: هو تحويل البيانات إلى صيغة لا يمكن فهمها بسهولة من قبل الأشخاص غير المخولين وذلك عند إرسالها.

أما **فك التشفير:** فهو إعادة البيانات المشفرة إلى شكلها الأصلي ليتم فهمها وذلك عند وصولها للطرف المخول.

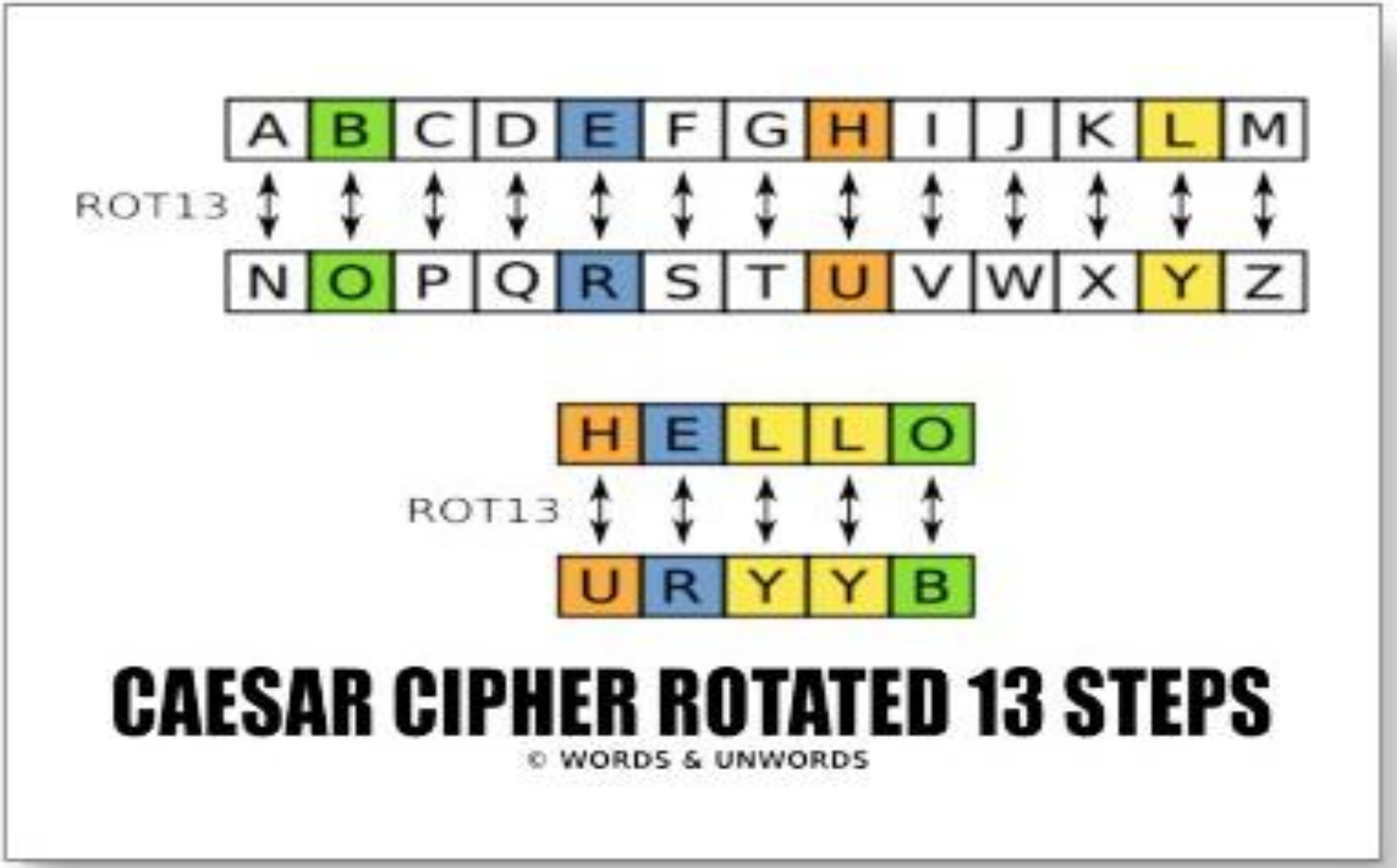
ما الفرق بين الشخص المخول والشخص الغيرمخول؟

الشخص المخول	الشخص الغير مخول
يتمكن من فك التشفير لأنه يمتلك مفتاح الخوارزمية التي على أساسها تم تشفير البيانات.	لا يتمكن من فك التشفير فهو لا يمتلك هذه الخوارزمية فلن يستطيع فهم شي من البيانات التي حصل عليها.

التشفير وفك التشفير Encryption and Descryption

عملية فك التشفير:

- ضرورية جدا في الشبكات اللاسلكية لأنها أكثر عرضة للاختراق.
- فعالة جدا في نقل العمليات والحركات الحساسة مثل الدفع ببطاقة الائتمان عن طريق الشبكة أو المراسلات السرية التي تتم بين أعضاء الشركة عبر الشبكة.
- كلما كانت خوارزمية التشفير أصعب كلما كانت أقوى وكلما كانت التكلفة اكبر.


A B C D E F G H I J K L M
ROT13
N O P Q R S T U V W X Y Z
H E L L O
ROT13
U R Y Y B
CAESAR CIPHER ROTATED 13 STEPS
© WORDS & UNWORDS

التوقيع الرقمي Digital Signature

- احد الطرق المستخدمة في التوثيق لتوثيق المستندات الكترونيا حيث تعتمد على توقيع الموقع على مفتاح التشفير/فك التشفير وعلى الوثيقة الموقع عليها.
- تعتمد صناعة التوقيع الالكتروني على علم التشفير ذلك أن التوقيع نفسه يخزن بالنظام على شكل مجموعة من البتات تعتمد على خوارزمية رياضية وعلى مفتاح لفك هذه المعادلة الرياضية.
- التواقيع الالكترونية طويلة وصناعتها والتأكد منها ليس بالأمر السهل وتكمن أهميتها في أن الطرف المستقبل يتأكد من أن الرسالة أو الوثيقة جاءته من الطرف المرسل وبالتالي يكشف أي محاولة للعبث بالمعلومات.