الموضوع السادس

أمن المعلومات

مقدمة في أمن المعلومات

أمن المعلومات

هو عملية الحفاظ على المعلومات بشكل آمن، وحمايتها من الوصول الغير المصرح به. وذلك لكي تبقى محمية و آمنة.

Definition

- **تعريف الأمن SECURITY :**
- هي الحالة أو المرحلة التي تصبح فيها آمناً و خالٍ من الأخطار
- SECURITY IS "Quality or State of being Secure", "to be free from Danger."

INFORMATION SECURITY

- **أمن المعلومات :**

هو حماية المعلومات و الأنظمة و المعدات الفيزيائية HARDWARE التي تعالج و تخزن و تنقل المعلومات .

مكونات أنظمة المعلومات
Components of Information Systems

- البرامج SOFTWARE.
- الأجزاء المادية HARDWARE.
- البيانات DATA .
- المستخدمين PEOPLE .
- الإجراءات و اللوائح PROCEDURES .

SOFTWARE

البرامج

- تتكون البرامج من التطبيقات Applications المختلفة و نظم التشغيل Operating Systems و أدوات الأوامر Command Utilities .

HARDWARE الأجزاء المادية

- هي المكونات التي تحتوي و تشغل البرامج المختلفة و يتم تخزين البيانات و نقلها خلال تلك الوسائط . ونجد أن قوانين الحماية المادية لهذه المكونات تتعامل معها كجزء من الأصول التي يجب حمايتها من الإتلاف أو السرقة .

DATA البيانات

- البيانات المخزنة و التي تتم معالجتها و التي تنقل خلال نظام الكمبيوتر يجب حمايتها والتي تمثل الهدف الأساسي لمعظم الهجمات على المعلومات .

PEOPLE المستخدمين

- إن المستخدم كجزء أساسي لا يتجزأ من بيئة أنظمة المعلومات يجب أن يكون مشتركاً في تطبيق قواعد الحماية للنظام ، ويجب تعليمهم و تدريبهم التدريب اللازم للحرص على الأمور الأمنية في نظام المعلومات و إلا فإن إهمال ذلك الجانب من الحماية قد يؤدي إلى بعض المخاطر و الهجمات على المعلومات.

PROCEDURES الإجراءات و اللوائح

- هي القواعد و الخطوات المكتوبة لإنجاز مهمة معينة ، فإذا تم اكتشاف تلك الخطوات من قبل أشخاص غير مصرح لهم بمعرفتها فعندها ينتج الخطر في سلامة و وحدة المعلومات .

أهمية أمن المعلومات

- إن المخاطر التي تتعرض لها المعلومات ناتجة من عدد كبير من الأحداث التي يمكن أن ينتج عنها تخريب أو تدمير أو سرقة أو تعديل غير مشروع لجهة ما غير مخول لها بالتصرف في تلك المعلومات بصورة متعمدة أو غير متعمدة . و يدخل في نفس الإطار سوء الإستخدام من قبل المستخدم لتلك المعلومات سواء أكان بشراً أو أداة من الأدوات .
- من هنا ظهرت الحاجة لإيجاد نظام أمني يقوم بتوفير البيئة المناسبة للتعامل مع المعلومات .

مقدمة في أمن المعلومات

كلمة المرور Password

هي مجموعة من الرموز التي تسمح للدخول إلى الحاسوب، أو الموارد على شبكة الاتصال أو المعلومات.

فوائد كلمة المرور:

- تسمح للمستخدمين المصرح لهم فقط لدخول النظام
- إدارة و تحديد هوية الأشخاص بفاعلية و التدقيق في عملية الوصول.
- حفظ و حماية المعلومات
- حماية المعلومات الشخصية الخاصة بك.

مقدمة في أمن المعلومات

نصائح لإنشاء كلمات المرور

كلمة المرور مسؤولية مالكها، لذا يجب عليه أن يتبع النقاط التالية عند إنشاء كلمة مرور:

١. يجب أن يكون تخمينها صعب
٢. يجب ألا يكون طولها اقل من (٨) أحرف
٣. يجب أن تتسم بميزة التعقيد، و التي ينبغي أن تحتوي على خليط من الأرقام و الأحرف و الرموز الخاصة مثل (*/-@+$)
٤. يجب أن لا تحتوي على اسم المستخدم
    ١. يجب أن لا تحتوي كلمة المرور على معلومات شخصية مثل رقم الهاتف، أو اسم أحد الأقارب، أو تاريخ الميلاد

مقدمة في أمن المعلومات

نصائح للاستخدام كلمات المرور

١. لا تفصح عن كلمات المرور لأي شخص
٢. لا تستخدم نفس كلمة المرور للعمل في مواقع متعددة مثل البريد الإلكتروني أو الحاسب المصرفي
٣. لا تكتب أو تحفظ كلمة المرور على ورقة أو في رسالة بريد الالكتروني
٤. لا تستخدم خاصية تذكر كلمة المرور المتوفرة في بعض أنظمة التشغيل
٥. قم بتغير كلمة المرور بشكل دوري

The Malicious Software البرامج الخبيثة

هي أحد تهديدات الحاسوب في هذا العصر. ونقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض. و الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.و يمكن يتصنيف أنواع البرمجيات الخبيثة على النحو التالي:

١. الفيروسات (Viruses)
٢. الديدان (Worms)
٣. برامج التجسس (Spywares)
٤. الخداع (Hoax)
٥. عمليات الاحتيال واصطياد الضحايا The Phishing Scam
٦. أحصنة طروادة Trojan Horses

الفيروسات Viruses

- فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف برامج معينة ، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة ، كما تقوم بالتلاعب بمعلومات الكمبيوتر المخزنة
- ينتقل الفيروس إلى جهازك عندما تقوم بنقل ملف ملوث بالفيروس إلى جهازك أو عند زيارة احد المواقع المشبوهة او اثناء تبادل السي ديات أو الفلاشات مع الأصدقاء و ينشط الفيروس عند محاولة فتحه ويمكن ان يصلك ايضا عن طريق البريد الألكتروني على هيئة مرفقات

الديدان Worms

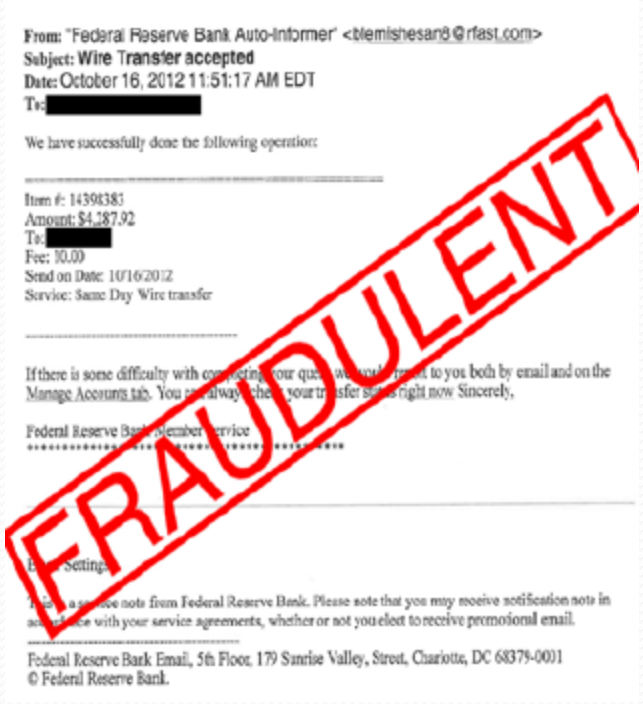
- ديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها
- يمكن أن تسبب الضرر بشكل واسع.
- على عكس الفيروسات، التي تتطلب نشر ملفات المضيف المصابة.

الديدان تعتبر برنامج مستقل ولا يحتاج إلى برنامج مضيف أو مساعدة أشخاص للنشر.

برامج التجسس Spywares

- هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس، المستخدم يجهل هذا الغزو.
- يمكن لبرامج التجسس جمع ونقل المعلومات الشخصية.
- المعلنين وغيرهم يرغبون في معرفة ماهي المواقع الإلكترونية التي يقوم المستخدمون بزيارتها وما هي عادات وأساليب تصفح الإنترنت لديهم.
- في بعض الأحيان تقوم برامج التجسس بإعادة توجيه مدخلات المتصفح لتوجه المستخدم إلى موقع آخر غير المقصود.
- بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية

Hoax الخدعة



- هو إنذار كاذب عن فيروس في الحاسوب. وعادة التحذير يصل عن طريق مذكرة البريد الإلكتروني أو يتم توزيعها من خلال مذكرة في الشبكة الداخلية للشركة
- فيروسات الخدعة، عادة ما تكون غير ضارة ولكنها تكون مزعجة باعتبارها خداع وتضيع للوقت وذلك من خلال إعادة توجيه الرسالة. و هناك عدد من الخداع من خلال تحذير المستخدمين أن ملفات النظام المهمة توجد بها فيروسات وبالتالي تقوم بتشجيع المستخدم عل حذف الملف، مما يسبب إت اف النظام.

The Phishing Scam رسائل الاصطياد الخادعة

- التصيد هو محاولة الحصول على معلومات مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان من قبل محتالين متنكرين بوصفهم أنهم يعملون في منظمات جديرة بالثقة.
- البريد الإلكتروني غالبا ما يستخدم أساليب التخويف في محاولة الإغراء الضحية إلى زيارة مواقع ويب مخادعة. يشعر فيها الضحية بانها مواقع عامة مثل التجارة الإلكترونية أو الخدمات المصرفية

The Trojan Horses أحصنة طروادة

- وهو من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة. تقوم بخداع المستخدمين من أجل تحميلها وتطبيقها على أنظمتهم.
- فيتم بذلك تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار

أضرار الإصابة بالفيروسات و البرامج الخبيثة

١. تعطيل الحاسوب
٢. ظهور شاشة الموت الزرقاء
٣. سرقة النقود إلكترونيا
٤. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات
٥. تسرق البيانات
٦. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات
٧. تبطئ الحاسب
٨. تبطئ الاتصال بالانترنت

أعراض الإصابة بالفيروسات و البرامج الخبيثة

- تباطؤ أداء الحاسوب.
- زيادة حجم الملفات، أو زيادة زمن تحميلها للذاكرة .
- ظهور رسائل تخريبية على الشاشة، أو الرسوم أو صدور بعض الأصوات الموسيقية.
- حدوث خلل في لوحة المفاتيح كأن تظهر على الشاشة أحرف ورموز غير التي تم ضغطها أو حدوث قفل للوحة المفاتيح .
- ظهور رسالة ذاكرة غير كافية لتحميل برنامج كان يعمل سابقاً بشكل عادي.
- سعة الأقراص أقل من سعتها الحقيقية.

الفيروسات

- **بعض طرق الحماية:**
  - برامج مكافحة الفيروسات مثل:

(**Macafee , Kaspersky, Norton, Avira, AVG, NOD٣٢**)

  - توفير نسخ احتياطية (backup) .
  - جدار الحماية.
  - كلمة المرور(Password).

نصائح عند فتح ملحقات البريد الإلكتروني

- لا تفتح أية ملفات ملحقة ببريد إلكتروني من مصدر غير موثوق.
- لا تفتح أية ملفات ملحقة ببريد إلكتروني ما لم تعرف محتواها.
- لا تفتح أية ملفات ملحقة ببريد إلكتروني إذا كان حقل الموضوع مشكوكاً فيها وغير متوقع.
- احذف سلسلة رسائل البريد الغير هامة وتجنب الرد عليها.
- لا تقم بتحميل أية ملفات من الغرباء.
- توخي الحذر عند تحميل الملفات من الانترنت، تحقق من شرعية المصدر وحسن سمعته.

الهدف من إعداد البرامج الخبيثة

- تختلف دوافع إعداد الفيروسات فمنها الدوافع الحسنة ومنها الدوافع المادية ومنها الدوافع الانتقامية ، فبعض الناس يقوم بإعداد الفيروسات للتسلية أو ولإظهار القدرة على البرمجة ولكن هناك من يعدها لهدف مادي وذلك لضمان تردد المستخدم لمحلات الكمبيوتر للصيانة او التخلص من هذا الفيروس او السطو على حسابات البنوك او المعومات العامة للشركات والمؤسسات الكبرى ، ومهما كان هدف اعداد الفيروس لابد من الوقاية منه لأنه يسبب الكثير من المشاكل والخسائر لمستخدمي الكمبيوتر .