مدخل إلى تقنية المعلومات
LEC # 9

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

الأمن

الهوية/التوثيق Identity/Authentication:

- لابد من حماية البيانات من الفقدان غير المقصود أو المتعمد، وضمان سلامة وخصوصية البيانات ومنع الوصول الى البيانات المخزنة في الحاسب من قبل الاشخاص غير الشرعيين.

الهوية/التوثيق Identity/Authentication

طرق التحكم بعمليات الوصول Access Control:

- **تحديد هوية المستخدم Identification:**

ينشئ مسؤول الشبكة هوية للمستخدم User ID يمثل هوية المستخدم بالنسبة للنظام، لذا لن يتمكن المستخدم من الدخول الى النظام قبل ادخال اسم المستخدم، مثل هوية المستخدم المطبوعة على بطاقة الصراف الآلي.

- **اثبات هوية المستخدم (التوثيق) Authentication:**

دليل مادي أو معنوي يُستخدم لإثبات أن الشخص هو نفسه الشخص المسموح له بالدخول إلى النظام ، وهذا الدليل يمكن أن يكون بطاقة ذكية أو توقيعاً أو صوت المستخدم أو كلمة السر، فمثلا ادخال البطاقة في جهاز الصراف الالي لا يعني أنك صاحب البطاقة فقد تكون مسروقة،ولكن الذي يؤكد انك صاحب البطاقة هو ادخالك كلمة السر الصحيحة.

الهوية/التوثيق Identity/Authentication

تابع/طرق التحكم بعمليات الوصول Access Control:

- **تحديد صلاحيات المستخدم (التفويض) Authorization:**

الصلاحيات هي تحديد صلاحيات الوصول لمصادر النظام من قبل المسؤولين عنه .

✓ يتمتع المستخدمون بصلاحيات محددة للتعامل مع البيانات المخزنة ، فقد يتمتع البعض بصلاحية قراءة البيانات فقط ، بينما يمكن لمستخدم آخر القراءة والتعديل على هذه البيانات .

سياسات كلمة المرور Password Policies

كلمة المرور Password: عبارة عن تشكيلة من الأرقام والأحرف ، يختارها المستخدم ويحتفظ بها ولا يطلع أحداً عليها.

- **سياسات كلمة المرور Password policies:**

✓ يجب ألا تخبر أي شخص بهذه الكلمة.

✓ يجب اخفاؤها وأن لا تكون على مرأى من الناس.

✓ يجب تغييرها بشكل دوري.

✓ يجب عليك عدم نسيان كلمات المرور.

✓ يجب عدم استخدام الكلمات التي يسهل تخمينها.

- غالبا عند كتابة كلمة مرور تظهر كسلسلة من النجوم ********.

أمن البيانات Data Security

أمن البيانات : هو مصطلح عام يستعمل بقصد حماية البيانات من الفقدان المقصود أو غير المقصود.

- ضمان سلامة وخصوصية البيانات لا تُعنى فقط بتوفير الأمان للمعدات وإنما للبرمجيات والبيانات المخزنة في ذاكرة الحاسوب.

- **هناك بعض التدابير الوقائية لحماية البيانات بإستخدام:**

١. النسخ الاحتياطي Backups.
٢. جدران النار Firewalls.
٣. البطاقات الذكية Smart Cards.

النسخ الاحتياطي Backups

النسخ الاحتياطي: هي نسخ من البرمجيات والملفات والبيانات يتم الاحتفاظ بها للاستفادة منها في حالة خراب النسخ الأصلية بسبب وجود فشل أو عطل في جهاز الحاسوب أو أخطاء المستخدم أو الحوادث الطبيعية أو بسبب الإهمال.

أنواع النسخ الاحتياطي:

- **النسخ الاحتياطي الكامل:**

عمل نسخة احتياطية للمعلومات بشكل كامل(جميع محتويات القرص الصلب) وذلك لأهمية وقيمة البيانات ، تقوم الشركات الكبيرة باستخدام هذا النوع من النسخ الاحتياطي ، ولكن هذا النوع يستغرق وقت طويل خصوصا اذا كان الحاسوب يحتوي معلومات كثيرة.

النسخ الاحتياطي Backups

تابع/أنواع النسخ الاحتياطي:

- **النسخ الاحتياطي التراكمي :**

أن تقوم بعمل نسخة احتياطية كاملة مرة أسبوعياً، وتقوم في نهاية كل يوم بنسخ الملفات حديثة الإنشاء أو التعديل احتياطياً.

- **النسخ الاحتياطي الخارجي :**

حفظ النسخ الاحتياطية في مكان آمن بعيداً عن الأخطار والحريق والغبار وضوء الشمس والمجالات المغناطيسية ، فعلى سبيل المثال إذا حدث حريق ستفقد أيضاً هذه النُسخ اذا كنت تحفظها في مكان بالقرب من الحاسوب، لذلك ينصح بوضعها في خزانة مضادة للحريق .

حاجز الحماية (النار) Firewall

حاجز الحماية(الجدار الناري): نظام أمني لمنع المستخدمين الخارجيين غير المرخص لهم من الوصول إلى الشبكة ، فهو الذي يسمح ويمنع ويشفر ويفك الشيفرة لكل شئ يدخل إلى الشبكة.

- مثلا في شبكة الانترنت تقوم الجامعات بوضع **المفوض Proxy** لمنع موظفي الجامعة والطلاب من الدخول الى مواقع معينة.
- اذن كل ما يدخل الى الشبكة يمر على حاجز الحماية الذي يحلله ومن ثم يسمح له بالعبور أو لا يسمح.
- قد تكون الحواجز النارية عبارة عن:
  - ✓برمجيات فقط.
  - ✓برمجيات ومعدات.

البطاقات الذكية Smart Cards

البطاقة الذكية: هي بطاقة صغيرة بحجم المحفظة توضع بالجيب تحتوي دوائر إلكترونية تستطيع معالجة البيانات ، أي تستطيع استقبال البيانات بطريقة ما ومن ثم إعطاء نتائج.

- تعد البطاقات الذكية طريقة ذات فاعلية عالية في التعريف بهوية المستخدم.
- **هناك نوعان من البطاقات الذكية :**

١) بطاقة الذاكرة Memory Card : تحتوي على ذاكرة غير متطايرة لتخزين البيانات الشخصية مثلاً .

٢) بطاقة المعالج الميكروي MicroProcessor Card : تحتوي على ذاكرة ومعالج ميكروي بسيط لمعالجة البيانات .

قضايا سرقة البيانات Data Theft Issues

- تمثل السرقة Theft نوعاً من الجرائم الحاسوبية ، وعند سرقة الحاسوب المحمول تكون نية اللص على الغالب سرقة الحاسوب نفسه ولكنه قد يجد بعد ذلك أن البيانات المخزنة فيه أكثر قيمة وأهمية .

ولمنع سرقة البيانات اتخذ الخطوات التالية :

✓استخدم هوية المستخدم وكلمة المرور على أجهزة الحاسوب لمنع المستخدمين الآخرين من الوصول إليه.

✓تشفير البيانات بحيث تظهر بلا معنى وغير مفهومة.

قضايا سرقة البيانات Data Theft Issues

- ✓قفل الجهاز والمعدات باستخدام أسلاك أمنية، فهذه الطريقة تعمل على تعطيل السارق وإعاقته.
- ✓حفظ الجهاز في مكان مناسب وآمن.
- ✓تقوم بعض الشركات بمنع استخدام الأقراص والذاكرة المحمولة وذلك لسهولة نسخها وخروجها خارج الشركة ، مما قد يؤدي إلى إساءة استخدامها .
- ✓التقيد بالإجراءات المتبعة في التعامل مع البيانات .