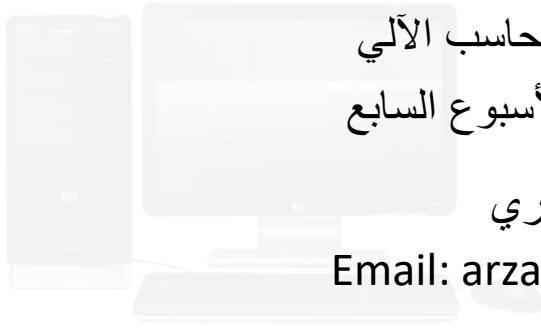




الكلية الجامعية بالقطيفة
قسم التربية وعلم النفس

مجالات تقنية المعلومات – أمن الحاسب - الفيروسات



حاسب آلي / مهارات الحاسب الآلي
المحاضرة الرابعة – الأسبوع السابع

د. أحمد البشير

Email: arzahrani@uqu.edu.sa

الفصل الأول: المفاهيم الأساسية لتقنية المعلومات

مفهوم تقنية المعلومات
ومجالات استخدامها في الحياة اليومية

توظيف الحاسب في قطاعات المجتمع (مجالات الاستخدام)

- الحاسب والتعليم.
- الحاسب والإدارة (نظم المعلومات الإدارية).
- الحاسب والمصارف.
- الحاسب في المجال الطبي (التدريب- التشخيص- الإدارة).
- الحاسب والصيدليات (الخاصة -الحكومية).
- الحاسب والقطاع الصناعي.
- الحاسب والأمن الداخلي(المرور-السجل المدني- الجوازات).

الفصل الأول: المفاهيم الأساسية لتقنية المعلومات

حماية تقنية المعلومات

حماية تقنية المعلومات

• **أمن المعلومات:** من زاوية تقنية هو عبارة عن الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، وهو العلم الذي يدرس كيفية توفير تدابير حماية سرية وسلامة المعلومات وكيفية مكافحة الاعتداء عليها.

• **الشروط الواجب توفرها في أي نظام معلومات:**

- السرية أو الموثوقية Confidentiality
- التكاملية وسلامة المحتوى Integrity
- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation

كيفية توفير الحماية لنظام المعلومات

- وضع كلمة سر او الرمز أو الرقم الشخصي
- برامج مكافحة الفيروسات
- مراعاة الإجراءات الأمنية لحماية الدخول إلى الشبكة
- حماية مواقع التجارة الإلكترونية
- اعتماد بصمة الأصبع او العين أو الصوت
- تحديد نطاق الاستخدام Authorization
- إجراء النسخ الاحتياطي Backup

المخاطر التي تواجه أي نظام معلومات

1. العبث والغش بالبيانات
2. خداع بروتوكول الانترنت: القرصنة والفيروسات
3. التقاط كلمات السر
4. استقبال الرسائل الالكترونية غير معروفة المصدر
5. تحميل البرامج المجانية من مواقع غير متخصصه

الخصوصية وحماية البيانات Privacy

- **الخصوصية:** حق الفرد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنه إلى الآخرين أو القدرة بالتحكم على دورة المعلومات التي تتعلق بهم.
- **المجالات التي تشملها خصوصية المعلومات:**
 1. أي معلومات عن الأفراد في أنظمة الدولة
 2. أجهزة الحاسب الشخصي المكتبي والمحمول
 3. أجهزة الجوال
 4. المؤسسات والشركات المكتبية

الخصوصية وحماية البيانات Privacy

أهم طرق حماية البيانات وخصوصيتها:

1. التأكد على حق الوصول (توزيع كلمات المرور)
2. استخدام كلمات الوصول ومعرفات المستخدم
3. استخدام التشفير
4. لا تترك الجهاز مفتوح
5. لا تترك أجهزتك الشخصية

حقوق الملكية للمصنفات الرقمية Copyright

- **المصنفات الرقمية:** هي عبارته عن البرمجيات وقواعد البيانات والدوائر المتكامله، ومع ظهور الانترنت أصبحت أيضاً تشمل: أسماء النطاقات والبريد
- **من هو مالك حق المصنفات ؟**
- **أخلاقيات التعامل مع المصنفات الرقمية:**
 1. الإشارة إلى مصدر البحث وصاحبه كمرجع
 2. استخدام النسخ الأصلية للبرامج وتجنب نسخها
 3. عدم استخدام أسماء مشابهة لأسماء النطاقات
 4. عدم العبث بالبريد الخاص بشخص كتوزيعه

حقوق النسخ © Copyright

* حقوق النسخ الخاصة بالبرامج Software Copyright:

إن حقوق النسخ المتعلقة بأغلب البرامج التي تشتريها تكون محفوظة ولا يجب عليك نسخها. وإذا قمت بذلك، فأنت تخرق القانون وإذا تم ضبطك، ستتم إدانتك. فالكثير من الناس يشترون نسخة من لعبة معينة ويقومون بنسخها لأصدقائهم وعائلاتهم؛ وهذا أيضاً تصرف غير قانوني. وفي أغلب الحالات، تكون أيضاً إغارة الأقراص المرنة أو المدمجة الخاصة بالبرامج التي اشتريتها للأشخاص الآخرين خرقاً للقانون.

هناك هيئات كثيرة - مثل FAST (Federation Against Software Theft) - تختص بمحاربة النسخ غير القانوني للبرامج. أما إذا طلب منك مديرك بالعمل نسخ أحد البرامج، فيجب أن تتأكد من أن لديك ترخيصاً يسمح لك بنسخ هذا البرنامج، لأن في الكثير من الدول، ستعرض أنت للمسائلة القانونية ودفع التعويض المناسب!

حقوق النسخ © Copyright

* عواقب نقل الملفات عبر الشبكة:

البرامج التي تجدها على الإنترنت: توفر بعض المواقع على الإنترنت والتي تديرها شركات مشبوهة نسخاً مجانية من بعض البرامج المعروفة. فلذلك، إذا قمت بتنزيل أي برنامج من الإنترنت، تأكد من أنه قانوني.

* رخص المستخدم:

ما هي التراخيص الخاصة بالمواقع؟ لا تقوم الكثير من الشركات بشراء نسخ من البرامج التي تحتاج إليها لجميع العاملين بها، عوضاً عن ذلك، تشتري هذه الشركات ترخيص للموقع بحيث تستطيع بموجبه عمل عدد معين من النسخ للعاملين فيها أو استخدام النظام من خلال الشبكة.

حقوق النسخ © Copyright

الملكية ضمن الحدود التي ينص عليها القانون

- برامج مجانية لا تحتاج أي ترخيص قبل الاستخدام مثل البرامج التي تحمل من الإنترنت Freeware.
- برامج تجريبية (Shareware) غالباً ما تكون محدودة الإمكانيات أو المدة .
- برامج غير مصرح بها إلا عن طريق شراء النسخة الأصلية: تحتاج ترخيص قبل استخدامها أو نسخها (EULA: End User License Agreements) وهي تحتاج إلى عقد بين الناشر والمستخدم, ومفتاح المنتج (Product Key) .

©تستخدم للدلالة على ان حقوق ملكية المصنف محفوظة

النسخ الاحتياطي Backup

لماذا يجب تخزين النسخ الاحتياطية من البيانات بعيداً عن الحاسوب؟

إن أهم شيء تقوم بتخزينه على الحاسوب هي المعلومات. فعادةً ما تمثل محتويات القرص الصلب خلاصة سنوات من العمل. فإذا توقف القرص الصلب عن العمل، من الممكن أن تفقد كل هذا المجهود. ولذلك، من الواجب عليك إنشاء نسخ احتياطية من المعلومات المخزنة على الحاسوب.

النسخ الاحتياطي Backup

الهدف من النسخ الاحتياطي لملفات الكمبيوتر إلى أجهزة التخزين المتحركة :

لا معنى لعمل نسخ احتياطي من البيانات والإبقاء عليها بالقرب من الحاسوب. فإذا قام أحد الأشخاص بسرقة الحاسوب الذي تعمل عليه، فمن المتوقع أن يستولي أيضاً على النسخ الاحتياطي التي قمت بها وإذا حدث حريق، ستفقد أيضاً هذه النسخ إذا كنت تحفظها في مكان بالقرب من الحاسوب.

ولذلك، يجب عليك تخزين النسخ الاحتياطي في مكان آمن بعيد عن الحاسوب. على الأقل، يجب أن تفكر في وضعها في خزانة مضادة للحريق، لحمايتها من خطر الحريق.

أنواع النسخ الاحتياطي

النسخ الاحتياطي الكامل في مقابل النسخ الاحتياطي التزايدى:

إن النسخ الاحتياطي الكامل يعني أنك تقوم بنسخ كل البيانات الموجودة على الحاسوب الخاص بك احتياطياً ولكن من الممكن أن تأخذ هذه العملية وقتاً طويلاً إذا احتوى الحاسوب الذي تعمل عليه على كم كبير من البيانات.

أما النسخ الاحتياطي التزايدى، فيعني أنك تقوم مرة أسبوعياً بنسخ كل بياناتك احتياطياً، وتقوم أيضاً في نهاية كل يوم بنسخ الملفات حديثة الإنشاء أو التعديل احتياطياً، وذلك لتوفير الوقت وحماية البيانات. وإذا استخدمت برنامج نسخ احتياطي مناسب، ستكون هذه العملية تلقائية وسيكون عليك فقط الاختيار بين النسخ الاحتياطي الكامل والتزايدى.

حماية الكمبيوتر من التطفل

كلمات المرور:

حماية الحاسوب من خلال كلمة المرور Password: يمكنك إعداد (وضع) كلمة مرور يتم استخدامها عند بدء تشغيل الحاسوب. ولهذا النوع من كلمات المرور ميزة وهي أن الحاسوب لن يتم تشغيله إلا إذا تم إدخال كلمة المرور الصحيحة. وهذا يعني أنه لا يمكن لأي شخص غيرك العبث بالحاسوب الخاص بك وإدخال فيروس للإضرار به.

يجب اختيار كلمة السر بحيث تكون دمج للأرقام و الحروف مع بعض و أن تكون غير متوقعة أو غير متصلة بمعلومات المستخدم حتى لا يمكن التنبؤ بها.

حماية الكمبيوتر من التطفل

- إذا كان للحاسوب الذي تعمل عليه كلمة مرور تمنع المستخدمين الآخرين من الوصول إليه، يجب ألا تخبر أي شخص بهذه الكلمة.
- وألا تكتب كلمة المرور على بطاقة وتلصقها بالقرب من الشاشة واحذر من أن تخفي كل كلمات المرور التابعة لك أسفل المكتب الذي تعمل عليه (فهذا هو أول مكان يبحث فيه أغلب الأشخاص الذين يحاولون اقتحام الحاسوب الخاص بك).
- ويجب عليك ألا تنسى كلمات المرور الخاصة بك؛ ففي حالات كثيرة، لا يمكن استعادة البيانات إذا فقدت كلمة المرور.

ماذا يحدث لبياناتك و ملفاتك إذا كان هناك انقطاع في التيار الكهربائي؟

أهمية إيقاف تشغيل الحاسوب بشكل صحيح

- إذا كنت تعمل على حاسوب يعتمد على نظام ويندوز، فمن المهم أن تتذكر أنك قد تفقد البيانات إذا قمت بإغلاق الحاسوب بشكل غير صحيح أو إغلاقه فجأة بسبب انقطاع التيار الكهربائي. ولكي تتجنب هذا، يجب أن تقوم بحفظ عملك بشكل منتظم. وتشتمل الكثير من البرامج على إمكانية حفظ عملك تلقائياً، على سبيل المثال: كل عشر دقائق (أو أية فترة زمنية تحددها).
- تقوم بعض نظم التشغيل - مثل الإصدارات التالية لويندوز 95 و NT - بصورة تلقائية بتحديد ما إذا كان قد تم إيقاف تشغيل الحاسوب بشكل صحيح أم لا في آخر مرة تم فيها استخدامه. وعند اكتشاف هذا، يتم تشغيل برنامج تصحيحي (Recovery) خاص لإصلاح أي ضرر حدث بسبب انقطاع التيار الكهربائي.

حماية و تأمين الحاسب الشخصي

1. احتفظ بنسخة احتياطية من البرامج و البيانات مأخوذة على فترات متقاربة.
2. احتفظ بهذه النسخ في مكان آمن بعيداً عن الحاسب الشخصي.
3. احتفظ بسرية كلمة المرور و قم بتغييرها من وقت لآخر.
4. لا تترك البيانات معروضة على الشاشة و تغادر المكان.
5. أغلق الجهاز قبل أن تترك مكانك أمامه.
6. احتفظ لديك بالرقم المتسلسل للجهاز و للقرص الصلب.
7. لا تقم بتحميل أي بيانات شخصية دون التنسيق مع مسؤول أمن المعلومات.
8. ضع شريط الحماية أو أغلق فتحة التأمين للأقراص المرنة بعد الانتهاء من استخدامها لمنع الكتابة عليها بشكل غير مقصود.

الفصل الأول: المفاهيم الأساسية لتقنية المعلومات

الفيروسات

الفيروسات

تعريف الفيروس:

عبارة عن برنامج تم تصميمه بهدف إلحاق الضرر بنظام الحاسب له القدرة على ربط نفسه بالبرامج الأخرى و تكرار نفسه.

بعض أعمال الفيروسات

1. حذف جميع مستندات الملف الملتصق فيه الفيروس أو تخريبه أو التعديل عليه
2. تخريب أجهزة الحاسب الخاصة بالمستخدم
3. الحصول على ملفات وبيانات مهمة من جهاز مستخدم ما

الفيروسات

مكونات الفيروس

التناسخ Replication: وهو أحد أجزاء برنامج الفيروس الذي يمنحه خاصية التناسخ والانتشار بشكل تلقائي.

التخفي Protection: يضيف هذا الجزء على برنامج الحاسوب خاصية السرية أي عدم القدرة على الكشف عن وجوده بسهولة.

التنشيط The Trigger: ويعطي هذا الجزء للفيروس خاصية القدرة على الانتشار قبل اكتشافه ويكون عادة ضمن توقيت معين كساعة معينة أو تاريخ معين، مثال على ذلك الفيروس الشهير الذي يمارس نشاطاته في السادس من شهر آذار من كل سنة وهو مايكل انجلو. Michelangelo.

التفيد The Payload: وهو المهمة المناطة بالفيروس لتنفيذها عند بدء نشاطه وانتشاره.

الفيروسات

طرق انتقال الفيروس

العدوى المباشرة Direct Infector: يغزو الفيروس ملفات الحاسوب وعندما يتم تشغيل أو استخدام أحد هذه الملفات فإن الفيروس يبدأ بنشاطه وانتشاره وينتقل بين الملفات الموجودة على جهاز الحاسوب، وفور انتقال العدوى لأي ملف فإنه يتم تحميله ونقله إلى الذاكرة تلقائياً ومن ثم تشغيله.

العدوى غير المباشرة Indirect Infector: يُنقل البرنامج المصاب بالفيروس إلى ذاكرة جهاز الحاسوب فور بدء تشغيل الملف المصاب وينفذ الحاسوب أوامر الملف الأصلي، وبعد ذلك تنتقل الإصابة بالفيروس لأي ملف يتم تحميله إلى الذاكرة، ويتوقف هذا النوع من الانتشار في حال فصل التيار الكهربائي عن جهاز الحاسوب أو إعادة التشغيل.

الفيروسات

بعض أنواع الفيروسات

- أحصنة طروادة: دخل هذا الفيروس برفقة أحد البرامج إلى جهاز الحاسوب بشكل سري، ويبدأ بعمله بعد أن يتم تنفيذ البرنامج الذي دخل برفقته ويمارس أعماله التخريبية
- ديدان الحاسوب: ينتقل هذا النوع بالاعتماد على الاتصال بالشبكة العنكبوتية العالمية ويكون عادة عبر البريد الإلكتروني.

الفيروسات

تأثير الفيروسات في الحاسب

- إبطاء عمل جهاز الحاسوب، وحدوث أخطاء مجهولة عند تشغيل البرامج وتنفيذ أوامرها.
- توسيع حجم الملفات وزيادتها، وكما يزيد من المدة التي يتم بها تحميل البرامج والملفات إلى ذاكرة جهاز الحاسوب.
- ملاحظة وجود تأثير غير مسبوق ورسائل على الشاشة.
- ظهور رسالة FATALI/o ERROR عند بدء قراءة الأقراص وزيادة المدة الزمنية في قراءتها في حال كانت محمية.
- ملاحظة المستخدم صدور نغمات موسيقية غير مألوفة له.

الفيروسات

تأثير الفيروسات في الحاسب

- إحداث تغييرات في تواريخ تسجيل الملفات.
- اختلال عمل لوحة المفاتيح.
- تراجع المساحة المتوفرة في ذاكرة الجهاز، نظراً لما يشغله الفيروس من مساحة كبيرة.
- إظهار رسائل تكشف عن عدم وجود ذاكرة كافية لتحميل البرامج والملفات.
- عدم صلاحية بعض المساحات للتخزين في القرص الصلب.
- إلحاق الضرر بالنظام من خلال تعطيل BOOT Sector.
- تعرض البيانات والملفات للإتلاف.

الفيروسات

الوقاية من فيروسات الحاسب

- عدم تحميل أي برامج دون إجراء فحص لها، وكذلك الأمر بالنسبة للملفات المحملة والمنقولة من الشبكة العنكبوتية فيتوجب الفحص قبل التشغيل.
- تحميل البرامج الخاصة للكشف عن وجود الفيروسات ومكافحتها في جهاز الحاسوب.
- الاحتفاظ بنسخ احتياطية (Backup) للملفات والبرامج.
- الاعتماد على برامج الجدار الناري التي تقف عائقاً في وجه الفيروسات.
- تنصيب أنظمة تشغيل أكثر أماناً كنظام التشغيل جنو/لينكس.
- عدم تشغيل ملفات وبرامج مجهولة المصدر.
- أخذ الحيطة والحذر من الرسائل التي تصل عبر البريد الإلكتروني والروابط المجهولة المصدر وفحصها قبل فتحها

الفيروسات

- بعض طرق الحماية وإزالة الفيروسات:
- برامج مكافحة الفيروسات مثل:
([McAfee](#) , [Antivirus](#) , [Adwar](#) , [spyware](#))
- برامج جدار الحماية مثل (Kaspersky Security).

نهاية المحاضرة