



حقوق الملكية للمصنفات الرقمية Copyright

■ **المصنفات الرقمية:** هي عبارته عن البرمجيات وقواعد البيانات والدوائر المتكامله، أما مع ظهور الانترنت اصبحت تشمل: أسماء النطاقات والبريد

■ **من هو مالك حق المصنفات ؟**

■ **أخلاقيات التعامل مع المصنفات الرقمية:**

1. الإشارة إلى مصدر البحث وصاحبه كمرجع
2. استخدام النسخ الصلية للبرامج وتجنب نسخها
3. عدم استخدام اسماء 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 إعارة 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 نسخًا 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، و عوضًا 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 الانترنت .Freeware
- برامج تجريبية (Shareware) غالبا 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 احتياطية من البيانات والإبقاء عليها بالقرب من الحاسوب. فإذا قام أحد الأشخاص بسرقة الحاسوب الذي تعمل عليه، فمن المتوقع أن يستولي أيضاً على النسخ الاحتياطية التي قمت بها وإذا حدث حريق، ستفقد أيضاً هذه النسخ إذا كنت تحفظها في مكان بالقرب من الحاسوب.

ولذلك، يجب عليك تخزين النسخ الاحتياطية 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 تلقائيًا، 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





تعريف الفيروس:

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

أسباب انتشار الفيروسات

أنواع الفيروسات :

- حصان طروادة
- القنابل المنطقية
- القنابل الموقوتة
- باب المصيدة
- الديدان

■ بعض طرق الحماية:

- برامج مكافحة الفيروسات مثل:
(McAfee , Antivirus, Adwar, spyware)
- توفير نسخ احتياطية (backup) .
- جدار الحماية.
- كلمة المرور (Password).
- توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية و الحذر من التعامل مع البرامج المجانية و خصوصا التي يتم توزيعها بواسطة محلات لكمبيوتر
- فحص البريد قبل فتحه.