مقياس : المعلوماتية
طلبة السنة الأولى جذع مشترك - السداسي الأول

المحاضرة الثانية: الأمن والحماية المعلوماتية

مقدّمة:

إنّ الأمن والحماية في ميدان المعلوماتية من القضايا المهمة في العصر الحديث، وتخص جانبين مهمين متصلين ببعضهما البعض وهما : حماية الجانب المادي (Hadware) وحماية الجانب البرمجي (Software)، وسنقوم بالتفصيل، بعرض وسائل وطرق الحماية الخاصة بكل جانب من هذين الجانبين.

I- الحماية المعلوماتية في الجانب المادي :

تعد صيانة المعدات المعلوماتية مهمة جدًا لأنها تتيح:

- تقليل مخاطر الخلل والأعطاب
- إطالة عمر التجهيزات
- تقليل تكاليف الإصلاح

تشمل المعدات المعلوماتية جميع المكونات التي تمكّن الجهاز من أداء وظيفته، بما في ذلك المعالجة عبر برمجيات، الحفظ والطباعة والتعديل وما إلى ذلك، وبالتالي، فالمعدات المعنية بالحماية يمكن أن تكون وحدة المعالجة المركزية، أو الطابعة ، أو كابلات الطاقة، واللوحة الأم ، والقرص الصلب، وما إلى ذلك.

الإجراءات المتخذة لحماية المعلومات المخزنة داخل حاسوبك:

1- استخدام الـ **UPS** (المُموّج Onduleur) لحماية الحاسوب من مخاطر الانقطاع المفاجئ للتيار الكهربائي، والعديد من الفوائد الأخرى التي يوفرها UPS في تأمين الحاسوب وحماية المعلومات، وتشمل:

- توفير الطاقة المستمرة: يعمل UPS على توفير تيار كهربائي مستمر للحاسوب حتى في حالة انقطاع التيار الكهربائي المفاجئ. يعمل UPS كجهاز احتياطي يقوم بتخزين الطاقة الكهربائية وتوفيرها في حالة الحاجة، مما يمنع انقطاع التيار الكهربائي المفاجئ ويحمي الحاسوب من فقدان البيانات أو التلف.

- حماية الحاسوب من التغيرات في التيار الكهربائي: يمكن لـ UPS أن يقدم حماية ضد التغيرات الكهربائية مثل التقلبات الكهربائية وترددات الجهد غير المستقرة.

يقوم UPS بتنقية وتنظيم التيار الكهربائي الوارد إلى الحاسوب، وبالتالي يحمي الأجهزة الإلكترونية الحساسة داخل الحاسوب من التلف.

- وقت للإغلاق الآمن: يوفر UPS وقتًا إضافيًا للمستخدم لإغلاق الحاسوب بشكل آمن في حالة انقطاع التيار الكهربائي. يتيح هذا الوقت للمستخدم حفظ البيانات وإغلاق البرامج بشكل صحيح قبل أن ينفد الطاقة المخزنة في UPS.

- حماية الحاسوب ضد ارتفاعات الجهد وانخفاضاته: تتسبب ارتفاعات الجهد وانخفاضاته المفاجئة في القدرة على تلف الأجهزة الإلكترونية. يمكن لـ UPS أن يحمي الحاسوب من هذه التغيرات الكهربائية الضارة ويساعد في تقليل خطر التلف.

2- إطفاء الحاسوب بشكل نظامي :

Start → shut down → shut down → OK

أو بالنسخة الفرنسية

Demarrer → Arrêter **→** Arrêter **→ OK**

أما بالنسخة العربية، في جهاز يشتغل بنظام **Windows XP** مثلا، يمكنك اتباع الخطوات التالية:

- انقر على زر "ابدأ" الموجود في الزاوية السفلية اليسرى من الشاشة.
- في قائمة "ابدأ"، انقر على خيار "إيقاف التشغيل".
- ستظهر لك نافذة حوارية تحتوي على خيارات إيقاف التشغيل المختلفة.
- حدد خيار "إيقاف التشغيل" لإيقاف تشغيل الكمبيوتر بشكل كامل.
- إذا كنت ترغب في إعادة تشغيل الحاسوب، يمكنك تحديد خيار "إعادة التشغيل" بدلاً من ذلك.

تأكد من حفظ جميع أعمالك الجارية قبل إيقاف تشغيل الحاسوب، حيث سيتم فقدان أي معلومات غير محفوظة.

3- الالتزام بالتعليمات والإرشادات التالية:

- تأكد من تأمين شروط الحماية المناسبة للحاسوب من حيث الطاقة الكهربائية

- لا تقوم بإشراك أي محرك أخر على نفس مأخذ الكهرباء الذي يتغذى منه الحاسوب
- إبعاد الحاسوب عن مصادر الضجيج
- أن لا تتجاوز درجة الحرارة الأعظمية أن 80 درجة مئوية
- أن لا تنخفض درجة الحرارة الأصغرية عن 40 درجة مئوية
- إبعاد أي مصدر من مصادر الاهتزاز على نفس الطاولة

4- إستعمال الأغطية المناسبة عندما لا تكون الأجهزة قيد التشغيل، وهذه الأغطية دورها حماية وحدات جهاز الحاسوب من الغبار والسوائل. وفيما يلي بعض الأسباب التي تجعل استخدام الأغطية مهمًا:

- حماية من الغبار: الغبار يمكن أن يتجمع داخل الأجهزة ويتراكم على المكونات الداخلية مثل المراوح والمشتتات الحرارية والمنافذ. تراكم الغبار قد يؤدي إلى ارتفاع درجة حرارة الجهاز وتقليل كفاءة التبريد، مما يزيد من خطر حدوث أعطال وتلف في الأجهزة. باستخدام الأغطية المناسبة، يمكن تقليل دخول الغبار إلى الجهاز والحفاظ على نظافته.

- حماية من السوائل: قد يحدث تسرب السوائل إلى الأجهزة سواء عن طريق السقوط المفاجئ للمشروبات أو التسرب من الأجزاء المجاورة للحاسوب. تسرب السوائل يمكن أن يتسبب في تلف الدوائر الإلكترونية وقصر الدوائر وتعطل الأجهزة. باستخدام الأغطية المناسبة، يمكن تقليل احتمال تسرب السوائل إلى الأجهزة وحمايتها من التلف.

- حماية من الخدوش والتلف الجسدي: الأغطية توفر طبقة إضافية من الحماية للأجهزة من الخدوش والتلف الجسدي. قد يحدث تلف الأجهزة نتيجة للصدمات أو الخدوش التي يمكن أن تحدث في حالة عدم وجود غطاء واقٍ. باستخدام الأغطية المناسبة، يمكن تقليل خطر التلف الجسدي للأجهزة والحفاظ على مظهرها الخارجي.

يجب اختيار الأغطية المصممة خصيصًا للأجهزة وتناسب حجمها وتهوية الهواء المناسبة. وقبل وضع الأغطية على الأجهزة، يجب التأكد من إيقاف تشغيلها وفصلها عن مصدر الطاقة لتجنب أي مشاكل أثناء التركيب.

II- الحماية المعلوماتية في الجانب البرمجي (برمجيات وبيانات) :

أما الحماية في الجانبة البرمجي، بمعنى حماية التطبيقات والبيانات، فهناك العديد من وسائل ومن أهمها:

1) استخدام نظام (**Backups**) أي التخزين المستمر (أو النسخ الاحتياطي) و المنظم للمعلومات المخزنة داخل الحاسوب على أقراص التخزين، أو استخدام تقنيات متطورة للنسخ الاحتياطي مثل التقنية السحابية (Cloud Technology)أو تقنية الدرايف (Drive).

2) تحديث البرمجيات: يجب تحديث البرمجيات الخاصة بك بانتظام، بما في ذلك نظام التشغيل والتطبيقات والأدوات الأخرى. التحديثات الأمنية تسد ثغرات الأمان المعروفة وتقدم تصحيحات للثغرات الأمنية التي يمكن استغلالها من قبل المهاجمين.

3) استخدام برامج مكافحة الفيروسات (**Antivirus**) والبرمجيات الخبيثة: يجب تثبيت برامج مكافحة الفيروسات والبرمجيات الخبيثة الموثوقة وتحديثها بانتظام. هذه البرامج تكشف وتحجب وتزيل البرامج الضارة والفيروسات المحتملة. إن الفيروس المعلوماتي (**Virus**) هو برنامج صغير يخفي نفسه داخل القرص الصلب وله وقت محدد للعمل وعندما يحين وقته يبدأ بالتخريب في البيانات والبرامج، لكل فيروس برنامج مضاد خاص به. إن فيروسات والقرصنة المعلوماتية هم أعداء برامج الحاسوب، يمكن أن يكون لها عواقب وخيمة على الأعمال المخزنة في الحاسوب إذا لم يتم تثبيت برامج مكافحة فيروسات أو جدران حماية قوية بما فيه الكفاية.

4) تنفيذ الحماية من الاختراق: يمكن استخدام الجدران النارية (Firewalls) للحماية من الوصول غير المصرح به إلى النظام الخاص بك. تقوم الجدران النارية بمراقبة حركة البيانات إلى ومن الشبكة، وتمنع الوصول غير المصرح به والهجمات الاعتراضية.

5) التحقق من الهوية وإدارة الوصول: يمكن استخدام أنظمة التحقق من الهوية وإدارة الوصول للتحكم في الوصول إلى البرامج والبيانات (باستخدام كلمات السر مثلا **Password**) حيث يتم تعيين أذونات محددة للمستخدمين بناءً على الدور والمسؤولية، وتسجيل ورصد الأنشط لتحديد أي نشاط غير مشروع أو غير مصرح به.

6) التشفير والتوقيع الرقمي: يمكن استخدام التشفير لحماية البيانات الحساسة والمعلومات الشخصية من الوصول غير المصرح به. يتم توقيع البيانات الرقمية للتحقق من هوية المرسل وضمان سلامة البيانات أثناء النقل.