إجراءات الأمان العامة لأجهزة الحاسوب

تهدف هذه النشرة إلى تحديد مجموعة من النصائح الهامة والضرورية لضمان أفضل درجة أمان على أجهزة الحاسوب المكتبية والمحمولة:

1- إقفال جهاز الحاسوب عند عدم استخدامه (Lockdown)

والتي بدورها تعتبر من أسهل الطرق وأسلمها للحفاظ على جلسة العمل على الحاسوب بدون تدخل خارجي ولمنع اي مستخدم آخر من الولوج للحاسوب والعبث بمحتوياته، وللقيام بذلك يمكن الضغط على [L + ⊞].

2- استخدام كلمات مرور قوية

من الضروري استخدام كلمات مرور صعبة التخمين، فلا تكون سهلة كالاسم أو رقم الهوية أو الهاتف، كما يجب ألا تتم مشاركة الغير بكلمة المرور مهما كانت الأسباب الداعية لذلك.

3- الحرص أثناء استخدام البريد الالكتروني

لا تقم مطلقاً بفتح المرفقات في البريد الالكتروني بدون التأكد أولاً من خلوها من الفيروسات أو أي نوع آخر من البرامج الخبيثة، كما لا تقم بفتح الروابط الالكترونية في رسائل البريد إلا بعد التأكد من موثوقية مصدر هذه الرسالة ويستحسن القيام بنسخ الرابط ومن ثم فتحه يدوياً من المتصفح وليس النقر عليه مباشرةً، وللمزيد يمكن مراجعة النشرة (1) الخاصة بموضوع الاحتيال الالكتروني.

4- الحماية من الفيروسات

فرصة تعرض جهاز الحاسوب للفيروسات المختلفة تزيد عن فرصة اصابة البشر بالفيروسات، ولهذا فمن الضروري استخدام برامج الحماية من فيروسات الحاسوب والتأكد من فعاليتها وتحديثها باستمرار.

5- التعرف على برامج التجسس وتجنبها

يستخدم مصطلح برامج التجسس للدلالة على بعض البرامج التي تقوم بأنشطة رقابية على سلوك المستخدم في الانترنت، ويتم الاستفادة منها في نشر المواد الدعائية ذات العلاقة بسلوك المستخدم بالاضافة إلى جمع المعلومات الشخصية وقد تقوم بتغيير إعدادات الحاسوب ، وعادةً ما تقوم بذلك بدون إذن المستخدم.

6- تحديث البرامج وأنظمة التشغيل

من الضروري تحديث البرامج المختلفة وأنظمة التشغيل المستخدمة وتطبيق كافة التحديثات الأمنية والهامة التي يتم اصدارها من المنتج، لأن هذه التحديثات تعمل على حل مشاكل أمنية في برمجة هذه الأنظمة وهي تهدف بالدرجة الأولى إلى حماية المستخدم.

7- استخدام جدار حماية ناري (Firewall)

تُوفر برامج الجدر النارية حماية من المتطفلين الذين عادةً ما يقومون بتفحص الأجهزة والتدقيق في الثغرات الموجودة بهدف استغلالها، ويمكن لهؤلاء المتطفلون القيام بهذه الأعمال عبر الشبكة المحلية أو عبر الانترنت ولذلك فإن استخدام الجدار الناري يوفر حماية اضافية ضد محاولات التطفل الخارجي. مع ملاحظة أن جدار الحماية الناري لا يوفر

حماية ضد برامج التجسس التي يتم زرعها أثناء تصفح المواقع الملغومة بها لأن تصفح الانترنت في حد ذاته ليس ممنوعاً.

8- التخلص من المعدات القديمة بالشكل المناسب

عند الرغبة في التخلص من أي معدات الكترونية كأجهزة حاسوب تالفة أو الأقراص التخزينية (CD, Flash, Hard Desk)، ينبغي أولاً إزالة كافة الملفات الموجودة عليها إن أمكن أو الاستعاضة عن ذلك بالتدمير الفعلي لهذه المعدات بشكل يجعل استعادة الملفات أمراً غير قابل التحقيق.

9- مشاركة الملفات عبر برامج المشاركة المختلفة

تعتبر برامج المشاركة عبر الانترنت من اكثر المصادر انتشاراً للفيروسات والبرامج الخبيثة بأنواعها. كما أنها تمثل في أغلب الأحيان انتهاكاً لحقوق الملكية الفكرية لما تشمله من نشر ونسخ غير قانوني لمختلف الأعمال الأدبية والابداعية. وكثيراً ما يتم ضبط ومحاكمة البعض بتهم تتعلق بانتهاك حقوق الملكية باستخدام هذه البرامج.

10- تصفح الانترنت بحذر

الانترنت مصدر للمعرفة والعلوم والثقافة، ولكن لا يخفى كونه مصدراً للعديد من التهديدات على خصوصية المستخدم وأمانه، ولهذا فإن مزيداً من الحرص أثناء استخدام وتصفح الانترنت عادةً ما يكون أفضل وسائل الحماية على الاطلاق.

11- النسخ الاحتياطي للملفات الهامة

عند حدوث خلل في جهاز الحاسوب أو في نظام التشغيل فإن الحاسوب يحتاج إلى صيانة وهذه الصيانة قد تفقده كافة البيانات الموجودة عليه، ولهذا فمن الضروري اجراء نسخ احتياطي للملفات الهمة على أقراص خارجية كأقراص الـ DVD أو الـ Flash وإذا توفر قرص صلب خارجي ذو سعة كبيرة نسبياً فيمكن استخدامه كقرص احتياطي للملفات والبيانات الهامة.

دائرة أمن المعلومات