العنوان:	أمن معلومات المنشأة
المصدر:	الأمن والحياة
الناشر:	جامعة نايف العربية للعلوم الأمنية
المؤلف الرئيسي:	عمار، زكريا أحمد
المجلد/العدد:	مج 24, ع 273
محكمة:	لا
التاريخ الميلادي:	2005
الشهر:	صفر / إبريل
الصفحات:	72 - 77
رقم MD:	332507
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الفيروسات المدمرة، أمن المنشآت، الحاسبات الإلكترونية، أمن المعلومات، الخطأ الأمني، التوصيات الأمنية، الحماية الأمنية، الإجراءات الأمنية ، وسائط التخزين الإلكتروني، البريد الإلكتروني، مخاطر السطو التكنولوجي، إرشادات التأمين، الإنترنت
رابط:	http://search.mandumah.com/Record/332507

أمن معلومات المنشأة

اثنتا عشرة توصية ضرورية لموظفي المنشأة التي تستخدم الحاسبات الآلية

م. زكريا أحمد عمار*

لم يَعُد الحاسب الآلي حكراً على العلماء والمهندسين، ولا على الأغنياء القادرين، وإنما أضحى شائع الاستعمال لدى الكبير والصغير، بل غدا أداة للتسلية والترفيه، وظهر كحاجة ملحة لا يستقيم العمل الناجح دونه، وإن الذي عاصر الآلة الكاتبة، يُدرك أن الحاسب الآلي قد غير أسلوب حياة الناس، ناهيك عن أسلوب عمل المؤسسات والشركات، والوزارات والجيوش...، لقد حسّن هذا الاختراع العجيب جميع الأعمال، وسهّل القيام بالإجراءات للجميع، كل حسب مجال عمله، الطالب والأستاذ، الجندي والقائد، التاجر والمستهلك،... مما أوقعه موقع السحر في كل الأعمال، وفي المجالات كافة، لكن الضريبة المدفوعة كبيرة، فقد غدت المكتبة الضخمة قرصاً صغيراً، وكأن الفيل قد دخل في ثقب الإبرة، كومةٌ من البيانات في قرص صغير، لكن هذا القرص للأسف زورق عائم في بحر من الشبكات، حيث يمكن للآخرين الغوص، ثم الوصول إليه وثقبه، بتعديل محتوياته أو بتخريبها، بل إنّ مجرّد الاطلاع عليها يعد كارثة في بعض الحالات، وفي السطور التالية قواعد مهمة لمستخدمي الحاسب الآلي جميعاً، في المؤسسات الحكومية والخاصة، في القطاعات المدنية والعسكرية، في الإدارات القانونية والشُّرطية، بل إنها قواعد يمكن أن يستفيد منها المستخدم المنزلي أيضاً، وسأستبدل كلمة مؤسسة أو شركة بغض النظر عن نشاطها، بكلمة منشأة.

غلطة الشاطر بعشرة:

في الأمس القريب كان الموظف يحفظ ملفاته في خزانة، وفي نهاية الدوام يقفل خزانته بالمفتاح ثم يغادر منشأته، وفي اليوم التالي، يفتح الخزانة بمفتاحه، ثم يستأنف عمله مُوْقِناً أنّ ما من أحد قد عبث بملفاته دون علمه، وإن نسي قفل خزانته، فباب الغرفة مقفل، وإن تُرك باب الغرفة مفتوحاً، فإن باب المنشأة سيكون مقفلاً، وحتى إن تُرك هذا الأخير مفتوحاً، فإن دخول المنشأة يتطلب المشي والظهور خلال وقت محدود، كل ذلك يجعل اختراق الملفات الورقية صعباً أي أن غلطة الموظف الذي لا يستخدم الحاسب الآلي ستكون ذات آثار محدودة.

أما اليوم فالموظف يعمل على حاسب آلي، والملفات موجودة في قرص، ويعدّ القرص مورداً من موارد شبكة الحاسب الآلي، ويمكن الدخول إلى هذا القرص عبر الشبكة أوعبر الإنترنت من أي مكان على وجه الأرض بسهولة ويسر إن لم تتخذ الإجراءات اللازمة.

باختصار - بحالة الشبكات- تعد البيانات كأنها في زورق عائم، فإن نسي الموظف واحداً من الإجراءات الأمنية، فإن ملفاته ستكون مكشوفة، وبالتالي عرضة للتعديل أو التدمير أو على الأقل للكشف وقد يكون مجرد الكشف عن المعلومة خطأً قاتلاً.فقد تؤدي رؤيةُ موظفٍ (مجرد الرؤية) لجدول رواتب زملائه، إلى التذمر والمطالبة بزيادة الراتب والتعويضات أسوة بزملائه وقد يفقد وظيفته أو على الأقل يسبب المشاكل لزملائه.وقد يؤدي تسرب معلومة عن عرض أسعار للدخول في منافسة لخسارة الفوز بتلك المنافسة.وقد يؤدي كشف كلمة السر لحاسب مركزي لجيش ما إلى الهزيمة في المعركة.وقد يؤدي اختراق حسابات بنك ما، إلى سحب العملاء لأرصدتهم ومن ثم خسائر كبيرة للبنك. أي أن غلطة الموظف الذي يستخدم

الحاسب في عمله أخطر بكثير من غلطة زميله الذي يستخدم الأوراق والطريقة اليدوية.

خطأ أمني

إن إهمال الموظف لإجراءات أمن المعلومات ما هو إلا عبَثٌ خطِر، وقد يصل إلى حد وصفه، بأنه أخطر من العبث بالسلاح المعبأ بالرصاص، كل خلل في سلسة الإجراءات الأمنية يعد ثغرة في منطقة الدفاع الأمني للمنشأة، كأنه ثقب في الزورق العائم. من هنا تأتي أهمية العناية بتعليمات الأمن الخاصة باستخدام الحاسب الآلي، وخاصة من قبل موظفي المنشآت حرصاً على سلامة منشآتهم قبل سلامتهم. من هنا تبرز الحاجة إلى خطة أمنية ترتكز على ثلاث دعائم أساسية هي: السرية والتكامل وقابلية التطبيق. ومما لا شك فيه أن إعداد الخطة الأمنية ليس موضوع هذه الدراسة، وعادة تقوم أقسام تقنية المعلومات بإعداد تلك الخطة، وتوزيع مهام تنفيذها على الموظفين، ولتأمين نجاح الخطة لا بد لكل موظف أن يتحمل المسؤولية، ويتّبع التوصيات المكلف بها، وقد اخترت اثنتي عشرة توصية، تعد مهمة لكل موظف حتى لو كان الموظف غير متخصص بعلوم الحاسب الآلي.

التوصية الأولى: تحمَّلْ بحسّ المسؤولية والوعي.

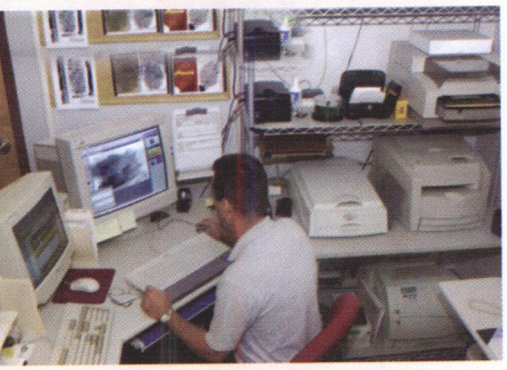
في منشآت اليوم، وفي الغرفة الواحدة قد تجد أكثر من موظف أو موظفة ولكل منهم حاسبه الآلي، يلِجُ عن طريقه بعض موارد الشبكة حسب واجباته الوظيفية، ونظراً لممارسة مهام العمل اليومي وتبادل الأحاديث واحتساء الشاي أو القهوة في نفس المكان، في وقت ليس بالقصير يومياً، فإنه مع مرور الأيام، تنشأ علاقات فيها من المودة والألفة ما يجعل الواحد منهم يأمن لزميله، فيعطيه مفاتيح مكتبه، وقد يصل به الأمر إلى أن يعطي زملاءه كلمة السر، التي يدخل بها موارد الشبكة الخاصة بعمله، لسبب ما، كخروجه قبل انتهاء الدوام مثلاً. إن مجرد إعلام الآخرين بكلمة السر، أمر خاطئ ولا يمتّ إلى روح المسؤولية بأية صلة، وليس فيه من الوعي وزن حبة من خردل. إن إعلام الآخرين حتى لوكانوا زملاء المكتب، بل حتى لو كانوا إخوة أو محبين، هو مخالفة يعاقب القانون على نتائجها، فإذا أعطى زميلٌ زميلَهُ كلمة سر حسابه، ودخل الأخير بها موارد الشبكة، ونتج عن هذا الدخول مخالفة ما، فإن المعطي مسئول قانوناً، وهوشريك في المخالفة سواء كان يقصد الخطأ أو لا يقصده.

وعلى كل موظف يستخدم الحاسب الآلي في إنجاز مهامه، أن يعد تنفيذ الإجراءات الأمنية المتعلقة بالحاسب الآلي جزءاً مهماً من عمله، وأنّ التقيد التام بتنفيذها أمر مهم جداً ولا بد للأخ الموظف أن يتذكر القواعد التالية:

- الحرص على حاسبه الآلي، فهو مسؤول عن كل حدث يتم من خلال ذلك الحاسب.
- أن يعرف كل ما يخصه من إجراءات أمنية، فإن لم يكن يعرفها فعليه المبادرة لتعلمها وتنفيذها بحذافيرها.
- أن يأخذ الإجراءات الأمنية على محمل الجدّ فأي إخلال بتنفيذها يؤدي إلى تعريضه للمساءلة القانونية.

التوصية الثانية: اختر كلمات السر بحكمة وعقلانية.

في المنشآت التي تعتمد على شبكة معلومات، يُفتح حساب لكل موظف يستخدم موارد الشبكة، ولهذا الحساب اسم وكلمة سر، وقد يُدعى اسم الحساب باسم المستخدم، وكلمة السر بكلمة المرور، وبناء على مهام الموظف واختصاصه يُعطى لهذا الحساب صلاحيات، تخوِّل الموظف بالدخول إلى موارد معينة في شبكة المعلومات، وعلى هذا فإن كلمة السر مهمة جداً فبمجرد معرفتها يمكن لمن عرفها أن يدخل الموارد غيرالمرخص له بدخولها ويحذف أو يعدل أو يطلع على مايريد، وهو مخالفة كبيرة. ولذلك يجب على الموظف اختيار كلمة السر الخاصة بحسابه بشكل يمكّنُه من تذكرها بسهولة من جهة، وبشكل يجعل تخمينها صعباً على الآخرين، من جهة أخرى. أخطئ ما قامت به تلك الموظفة التي عادت بعد ثلاثة أشهر، من إجازة الأمومة، وقد رُزقت بمولودة سمتها (لوريا)، شغَلت أم لوريا حاسبها الآلي، ثم دخلت الشبكة فظهرت لها الرسالة المعهودة في مثل هذه الأحوال » لقد انتهت صلاحية كلمة مرور حسابك يجب تغيير كلمة المرور» وما كان منها إلا أن اختارت الكلمة (lorya) ككلمة سر فرحاً بابنتها «لوريا»، إنه خطأ كبير، فما أسهل تخمين هذه الكلمة من قبل الأشخاص الذين يعرفونها. وعلى الموظف (أو الأخت الموظفة) أن تختار كلمة السر الخاصة بحسابه، بحيث تحوي حروفاً كبيرة وحروفاً صغيرة، وبحيث تحوي أرقاماً ورموزاً، وبحيث لا تكون موجودة بالقواميس، فوجودها بقاموس لغوي أو علمي، يجعلها عرضة لبرامج القراصنة والمخترقين، ولا بأس بأن تكون طويلة ما أمكن. أعطي مثالاً كلمة السر Year#10Ok وتُقرأ سراً عند إدخالها كالتالي year number ten ok وهي تحقق جميع تلك المواصفات.

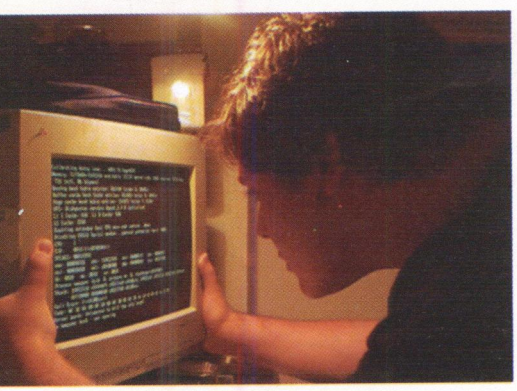


ويمكن تلخيص صفات كلمة السرّ الفعّالة التي يوصى باختيارها بما يلي:

١ - سهلة التذكر حتى لا يضطر لكتابتها وبالتالي فضحها.
٢ - تتضمن حروفاً وأرقاماً.
٣ - تحوي حروفاً كبيرة وأخرى صغيرة.
٤ - تتضمن رموزاً مثل: × ، # ، $ ...
٥ - أن يكون طولها فوق ثماني خانات، و تمثل الخانة الواحدة حرفاً أو رقماً أو رمزاً.
٦ - صعبة التخمين من قبل الآخرين.
٧ - عدم وجودها في أي قاموس لغوي أو علمي.

التوصية الثالثة: احفظ كلمات السر في مكان آمن.

تعدّ أوراق الملاحظات الصفراء، وما شابهها، من أخطر التهديدات لأمن معلومات المنشأة، حيث إن كثيراً من الموظفين يكتبون عليها كلمات السر، ثم يلصقونها في مكان واضح جلي على شاشة الحاسب الآلي، أو على حامل الورق، بل إنّ بعضهم يكتب في هذه القصاصة الخطرة اسم حسابه وكلمة السر معاً، ثم يلصقها في مكان ما في مكتبه.



إن عرْضَ كلمة السر بشكل يتيح للآخرين رؤيتها، أخطر بكثير من تسليم شخص مفاتيحَ سيارته لشخصٍ آخر، فتسليم مفتاح السيارة قد يؤدي إلى حادث مروري مثلاً، وتكون النتيجة أضراراً مادية أو جسدية، وأياً كانت هذه الأضرار فإنها ستُعرض على مالك السيارة، وبالتالي ستُعرف المخالفة والأضرار، بينما عرضُ كلمة السر يجعل من السهولة بمكان الدخول إلى موارد الشبكة والعبث بمحتوياتها، ومن ثم استخدام هذه المعلومات القيمة بطريقة تنتج عنها أضرار تتراوح من خسارة المنافسة، أو هدر لمشروع، إلى تفويت فرصة القبض على عصابة، ومن ضرر لمنشأة واحدة إلى ضرر بمنطقة بأكملها.

كما أن الواجب الوظيفي يحتّم على الموظف، عدم إعطاء كلمة السر الخاصة بحسابه لأي شخص آخر مهما كان العذر أو السبب، حتى لو طلب الزميل ذلك فيجب أن يواجه بالرفض التام. ولتجنب عرض كلمة السر، يُفضَّلُ حفظها ذهنياً، لذا يجب اختيارها بدقة، ويجب تجنب كتابتها في أي مكان تصل اليه عيون الآخرين، فإن كان لا بدّ من كتابتها، فيجب وضعها في خزانة مزودة بقفل، ولا بدّ من تذكير الموظف بالآتي:

- ألا يكتب كلمة السر أبداً وإن اضطر لذلك فلا يضعها بمكان مكشوف.
- كلمة السر هي مفتاح معطى له فقط (للموظف)، وليس لأحد غيره فليتأكد من جعل هذه الكلمة شخصية تماماً.
- ألا يشارك أحداً في كلمة السر.
- اختيار كلمة السر، بحيث يسهل عليه حفظها، ويصعب على الآخرين تخمينها.

التوصية الرابعة: الحذر من البرامج الضارة كالفيروسات ومثيلاتها.

برز في السنوات الأخيرة مصطلح malware ويعني البرامج الضارة، وتضم الفيروسات والديدان وأحصنة طروادة. ويعد الفيروس من أسوأ البرامج الضارة، والذي يمكن أن يسبب الضرر والتدمير لكثير من ملفات الحاسب المصاب، مستخدماً طرقاً ماكرة وأساليب خادعة، حيث ان من يقوم بتصميم برنامج الفيروس مبرمج ماكر، بحيث يقوم الفيروس بنسخ نفسه مئات المرات، وبحيث يبدأ عمله عند بدء حدَث معين. وأما الدودة فتمتاز إضافة لنسخ نفسها بسرعة إصابتها لشبكات الحاسب الآلي المحلية، والواسعة عبر شبكة الإنترنت، والبريد الإلكتروني. وأما حصان طروادة فهو برنامج صغير يتم زرعه بطريقة ماكرة في الحاسب المستهدف، ليقوم بجمع المعلومات المطلوبة مثل كلمات السر لكل من: نظام التشغيل، حساب دخول الشبكة، البطاقات الائتمانية وأرقام البطاقات البنكية.... وغيرها.

كيف تصل الفيروسات وأقرانها إلى حاسباتنا الآلية؟

تدخل معظم البرامج الضارة الحاسبات الآلية من خلال إحدى الطرق التالية:

- مرفقات رسائل البريد الإلكتروني attachments.
- تنزيل البرامج من شبكة الإنترنت downloading
- التطبيقات المعتمِدة على المشاركة بالملفات file-sharing.
- الأقراص القابلة للإزالة: القرص المرن،القرص الضوئي، قرص الذاكرة (flash disk).

إن من أفضل الطرق لتجنب دخول البرامج الضارة للحاسب الشخصي، وشبكة معلومات المنشأة، هو الانتباه والحذر الشديدين قبل فتح رسائل البريد الإلكتروني، والمقصود من ذلك: عدم فتح أي رسالة مجهولة المصدر، وعدم فتح أي ملف مرفق غير متوقع، وخاصة إذا كان مرسلاً من أناس غير معروفين. وأفضل نصيحة في هذه الأحوال عدم فتح تلك الرسائل وعدم تنزيل الملفات المرفقة بل حذفها فوراً.

بعض أعراض الإصابة بالبرامج الضارة:

- إقلاع بطيء غير معهود.
- تشغيل بعض الملفات بشكل غير مرئي (back ground).
- التوقف أو الجمود المفاجئ بدون سبب معروف.
- إعادة التشغيل بدون سبب معروف.

وعدم وجود الأعراض السابقة أو أي واحد منها لا يعني عدم وجود تلوث بالبرامج الضارة. وعند الشعور بوجود برنامج ضار في الحاسب الآلي فيجب عدم محاولة فحصه من قبل المستخدم بل عليه الاتصال فوراً بقسم الدعم الفني المخصص لهذه الأغراض في المنشأة.

مضاد الفيروسات هو خط الدفاع الأول.

إن من أهم خطوط الدفاع ضد البرامج الضارة، هي تركيب مضاد للفيروسات، ولا شك أن القسم المختص بتقنية المعلومات، قد قام بتركيبه في جميع حاسبات المنشأة، وإذا لوحظ عدم وجود برنامج مضاد للفيروسات فلا بأس من إعلام قسم الدعم الفني بذلك وترك الباقي لهم.ومن خطوط الدفاع ضد البرامج الضارة أيضاً تجنب تركيب برامج غير ضرورية، و تجنب تركيب أي برنامج دون موافقة الجهة المتخصصة. وينبغي للموظف تذكر النقاط التالية التي تساعد في الوقاية من الإصابة بالبرامج الضارة:

- من واجباته أخذ الحيطة من إصابة حاسبه بالفيروسات أو تعريضه للتهديدات.
- يجب التأكد من تحميل مضاد الفيروسات في حاسبه، والتأكد من فحص ملفات المرفقة بالبريد الإلكتروني قبل تنزيلها.
- الحذر من فتح أي رسالة عبر البريد الإلكتروني لا يُعرف مصدرها.
- الانتباه إلى أن السبب الأول للانتشار السريع للتلوث بالبرامج الضارة، هو عدم تطبيق إجراءات الحماية من قبل الموظفين.

التوصية الخامسة: استخدم مصادر المنشأة لأداء مهام عملك فقط.

لم يكن بالإمكان سابقاً استخدام الحاسب الآلي، إلا لتشغيل برامج العمل، بهدف إنجاز مهام خاصة بالمنشأة. أما في أيامنا هذه،

فيمكن للحاسب الآلي تشغيل كثير من البرامج غير المتعلقة بالعمل الواجب إنجازه للمنشأة، فيمكن للموظف تشغيل الألعاب البرمجية، أو ممارسة الدردشة عبر الإنترنت، أو فتح البريد الإلكتروني الشخصي، ويَنصَح خبراء أمن المعلومات بعدم تشغيل أي برنامج غير مخصص لمهام العمل داخل المنشأة وخاصة في بيئة الشبكات، ويعد هؤلاء الخبراء أن تشغيل البرامج غير المطلوبة للعمل، تصرفٌ ممنوع.

أسباب منع استخدام الحاسب الآلي في المنشآت للأغراض الشخصية:

- استهلاك جزء مهم من موارد شبكة الحاسب الآلي، من المفترض استخدامه لأغراض عمل المنشأة.
- التعارض مع قيم العمل، والواجب الوظيفي، وتأخير الوصول للهدف الإنتاجي المطلوب (Target).
- عدم التلاؤم مع بيئة العمل الوظيفي.

وقبل التطرق لاستخدام الحاسب الآلي من قبل الموظف لأغراض شخصية، لا بأس من إلقاء نظرة على استخدام عيِّنة من الأصول الخاصة بالمنشأة للتمييز بين المقبول وغير المقبول:

الهاتف الثابت: لا شك أن استخدام الهاتف الثابت مسموح، كأن يتصل الموظف بمنزله للاطمئنان على ابنه المريض، فهذا أمر مقبول، وليس عليه غبار، أما إذا كان ابنه، الشاب اليافع، يستمتع برحلة ترفيهية خارج الوطن، في دولة بعيدة، وهو في غاية السعادة، ولا يعاني من أية مشكلة، فإن اتصال الوالد بابنه، من داخل المنشأة، للدردشة ومشاركته المتعة، أمر غير مقبول.

البريد الإلكتروني: يعدّ البريد الإلكتروني، وسطاً لتبادل المعلومات، كالهاتف الثابت تماماً، فإرسال الموظف (من داخل المنشأة) رسالة إلكترونية لتهنئة صديق بنجاحه في السنة الدراسية، أمر مقبول، أما إرساله رسالة لصديق بدون مناسبة، وملء هذه الرسالة بالكلام المحشو حشواً وتزيينها بالصور بدون أي مبرر، في الوقت الذي تتكدس فيه مهام العمل، فهذا لاشك أنه غير مقبول. ولكن ثمة ما يمكن أن نطلق عليه «ممنوع» كاستخدام الحاسب الآلي للعب واللهو ضمن الدوام الرسمي أولكتابة عروض أسعار خاصة بمنشأة ثانية، أو استخدام البريد الإلكتروني الخاص بالعمل لأغراض منشأة أخرى أو العمل لصالح الغير.

وهكذا يجب الانتباه إلى:

- الحاسب الآلي وأجهزة الاتصال هي أصول وفّرتها المنشأة لخدمة أغراض العمل فقط.
- وجوب احترام الموظفين لتعليمات نظام العمل في المنشأة.
- يجب استخدام أصول المنشأة بحرص.
- استخدام أصول المنشأة ومنها موارد الشبكة لأغراض شخصية، قد يعرض المخالفين لفقدان الوظيفة.
- يُقال لمن يستخدم أصول منشأته لأغراضه الشخصية: إذا استعرت سيارة صديقك فلا تشارك بها في سباق السيارات.

التوصية السادسة: احرص على تأمين البيانات عند الإرسال أو الاستقبال.

يجب عدم إرسال أي معلومة مهما كانت بسيطة وحتى لو كانت غير مهمة، إلا بعد التحقق من حاجة تلك الجهة للمعلومة، وبناء على موافقة الرؤساء بإرسال تلك المعلومة، ويمكن أن تكون المعلومة عرض أسعار، أو منافسة، وقد تكون بيانات لإحداثيات قمر اصطناعي، أو هدف عسكري. إضافة إلى أن المعلومة بالأصل، يُفترض أنها غير متاحة للجميع بل حسب الاختصاصات، فمعلومات شؤون الموظفين تُتاح لموظفي شؤون الموظفين فقط، ومعلومات المالية تتاح لموظفي المالية، وهكذا.. فإن كل موظف يحتاج إلى صلاحيات للدخول إلى الموارد المتاحة له. ولكن في بعض الشبكات يُعطى للموظف صلاحيات على موارد تزيد بمقدار ١٠ إلى ٢٠ مرة عن حاجته الفعلية، وفي هذا ضياع لوقت الموظف وإضعاف لأدائه حيث إنه يضطر للمرور على عدة نوافذ قبل النوافذ التي تخص عمله، بالإضافة إلى اطلاعه على معلومات لا تخص واجباته الوظيفية. ويجب أخذ التأثيرات المرافقة لإرسال المعلومة إلى جهة ما، داخل المنشأة أو خارج المنشأة بمحمل الجِدّ، ولذلك ينبغي إجراء كل ما يلزم للتأكد من وصول المعلومة إلى من هم بحاجة إليها، دون زيادة أو نقصان، ودون تسريب.

عند إرسال معلومة لا بدّ من الانتباه إلى:

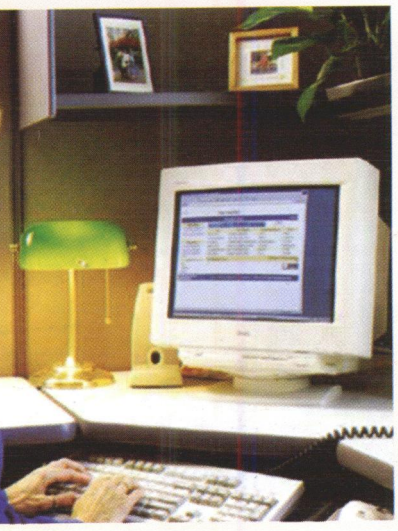
- أن تحسين الإنتاجية بإرسال الرسائل سريعاً، قد يكون في نفس الوقت إضعافٌ لأمن المنشأة، فاحرص ألا تضحي بأي إجراء أمني لصالح سرعة الإرسال.
- ينبغي استخدام زر الإرسال (FORWARD)بحذر.
- ينبغي التأكد من صحة المادة المرسلة ومن مدى الثقة بالجهة المرسل إليها.

التوصية السابعة:احترس من أخطار التعامل مع البريد الإلكتروني واتق الخدع المرافقة له.

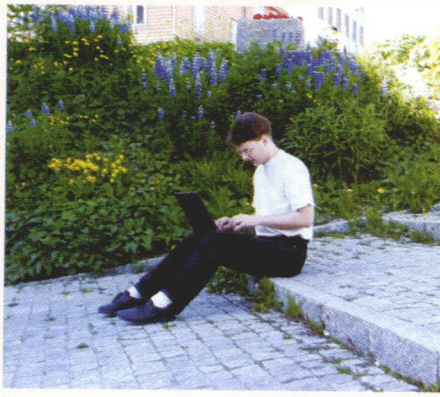
يعد البريد الإكتروني من أهم مصادر البرامج الخطرة، ففي حين أن معظم الرسائل البريدية مفيدة، وليس فيها خطر إلا أن رسالةً واحدة خطرة، قد تهدد أمن شبكة المنشأة كاملة، وخصوصاً أن الرسائل في أيامنا هذه أصبحت تحتوي على صور وروابط ومرفقات بعد أن كانت سابقاً مجرد نص لا أكثر، ويمكن أن يعلق بالصور والمرفقات برامج ضارة، وكذلك يمكن أن تُصمّم الروابط بشكل خادع وماكر، ولذلك يجب معرفة طريقة التعامل مع البريد الإلكتروني.

والنقاط التالية تساعد على معرفة طريقة التعامل مع البريد الإلكتروني:

- يجب تجنب فتح الملفات التي تنتهي بالامتداد .exe فهي الأكثر عرضة لحمل البرامج الضارة.
- يجب عدم فتح أي مرفق لرسالة إلا بعد التأكد من مصدرها، حتى لو دعا الأمر إلى استخدام الهاتف والاتصال بالمرسِل، وإلا فحذفُ الرسالة أفضل.
- تحديث نظام التشغيل وبرامج التطبيقات أولاً بأول.
- التأكد من صحة اسم وهوية المرسِل، إجراء لا بد منه.



أما بالنسبة لخدع البريد الإلكتروني، فعادة ما تأتي رسائل خادعة، تُظهِر الخير وتخفي الشر،فقد تصل رسالة تحذر من وجود فيروس خطير في حين أن الحقيقة عكس ذلك، أو تأتي رسالة تحذرك من ظاهرة ما، وتطلب إعادة إرسالها للآخرين، والخطر الأساسي لخدع البريد الإلكتروني هو إقناع المستخدم بتوجيه الرسالة إلى كل العناوين الموجودة في قائمة العناوين—every one— وفي ذلك سرعة انتشار رهيبة حول العالم. ومن الخدع المستخدمة بمكر شديد،



وضع الرابط في صورة وبلون أزرق وتحته خط، وعند نقر الصورة يتم فتح موقع آخر أو تنزيل ملف تجسسي، أو تشغيل حدث ضار، ثم تكون النتائج قاسية. ولا بد من فهم وإدراك خطورة مرفقات البريد الإلكتروني، وألا يفتح أي رسالة إلا بعد التأكد من هوية المرسل، وألا يحول أي رسالة تحوي معلومات تحذّر من برنامج ضار كالفيروس أو الدودة. كما عليه أن يتعلم طرق التعامل مع خدع البريد الإلكتروني.

التوصية الثامنة:استعرض الإنترنت بعقلانية وحكمة، واحذر أخطار الإنترنت.

كما تم ذكره في فقرة سابقة فإن حاسبات اليوم قابلة لتشغيل برامج شخصية، وقد يحلو لبعض الموظفين خلال دوامهم ، ممارسة استعراض الإنترنت للأغراض الشخصية، وخصوصاً في أوقات الاستراحة، معتبرين ذلك حقاً لهم، ويجب عليهم التحلي بالحكمة والعقلانية، وخصوصاً عند الاتصال بالمنشآت الأخرى وتبادل المعلومات معها، أو عند الدخول في غرف الحوار، والاسترسال في الحديث ونسيان الموظف لنفسه، بأنه في منشأة وعليه احترام أعرافها. ومن الأعراف السائدة في معظم المنشآت منع التعامل مع المواقع التي تتصف بما يلي:

- المواقع الجنسية الصريحة.
- ألعاب القمار وما شابهها.
- المشاركة في أعمال لا أخلاقية كالتمييز العنصري أو الدعوة إلى الفساد كالمخدرات.
- جميع الأعمال التي تؤدي إلى سوء الخُلُق والعنف والضرر بالأملاك العامة.

وعلى الرغم من أن كثيراً من المنشآت تحجب المواقع التي تحوي هذه الأنشطة، إلا أنها لا تستطيع منعها كلياً، نظراً للحاجة لفريق متخصص ومتفرغ للمهام الأمنية، وهذا الفريق غير متوفر في معظم المنشآت، وخصوصاً في البلدان التي أدخلت تقنية الإنترنت إليها حديثاً.

التوصية التاسعة: تأمين الحاسب المحمول بشكل سليم وخصوصاً خارج المنشأة.

من المعلوم إن الحاسب المحمول، حسب ما يوحي اسمه، أنه قابل للحمل وبالتالي قابل للنقل، ويخطئ من يعتقد بعدم ضرورة تأمين الحاسب المحمول بكلمة سر، وحيث أن الحاسب المحمول مزود بقرص صلب يمكنه تخزين كمية كبيرة من البيانات التي غالباً ما تكون ذات صفة شخصية وهذه البيانات مهمة للمخترقين، وقد يشكل الحصول عليها ثروة، تستخدم ضد مستخدم الحاسب المحمول أو ضد منشأته.

وفي ظل هذا التطور المنطلق كالسهم الثاقب، فإن جميع الحاسبات المحمولة الحديثة مزودة بميزة الاتصال اللاسلكي، وهذا وحده كاف لنسخ جميع البيانات في القرص الصلب، أو مسحها بالكامل، وبزمن لا يسمح بارتداد الطرف.ويزداد خطر اختراق الحاسب المحمول في حالة استخدامه في الأماكن العامة، لأن إعداد الشبكة اللاسلكية غالباً ما تكون قياسية وتتعرف بشكل افتراضي في أنظمة التشغيل الحديثة.و ينبغي لمستخدمي الحاسب المحمول، التأكد من تأمين حاسباتهم، لأن محتوياتها تخص المنشأة، ويتم تأمين الحاسب بإجراءات متعددة أهمها إلغاء المشاركة بالملفات، وتشفير البيانات المهمة، وتزويد مستخدمي الحاسب بكلمات سر فعّالة. ويمكن إيجاز قواعد إجراءات تأمين الحاسب المحمول والاتصال البعيد:

- يجب تجنُّب الأخطار الأمنية الناتجة عن العمل من خارج حدود المنشأة حيث إن هذه الأخطار لا تعد ولا تحصى.
- يجب تشفير البيانات والمعلومات المهمة.
- يجب عدم إهمال أو نسيان إجراءات الأمن الفيزيائية، وخصوصاً خارج المنشأة، حيث يصبح الحاسب المحمول هدفاً واضحاً للمهاجمين يشبه نقطة في ساحة واسعة.
- إن استخدام الحاسب المحمول، في قارعة الطريق يجعله هدفاً واضحاً للمهاجمين، حتى لو لم يرتدِ مستخدمه قميصاً رسمت على ظهره حلقات التصويب ذات المركز الواحد.
- يجب استخدام الأجهزة الرقمية القابلة للحمل بحرص مع تطبيق قواعد السلامة.
- يجب تشغيل جدار الحماية للحاسب المحمول.
- يُمنع استخدام المودم للاتصال بالإنترنت بحالة عضوية الحاسب المحمول في شبكة محلية، لتجنب أخطار البرامج الضارة وأخطار المهاجمين.
- أن يتذكر كل من يستخدم الحاسب المحمول المقولة: الحرص أفضل من الاعتذار.

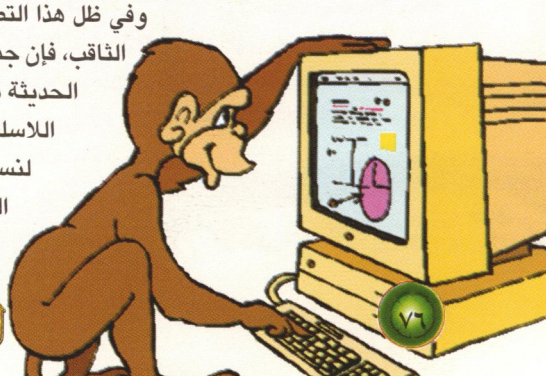
التوصية العاشرة: لا تهمل النسخ الاحتياطي، ولا تنسَ تأمين البيانات حتى بحالة إتلاف وسائط التخزين.

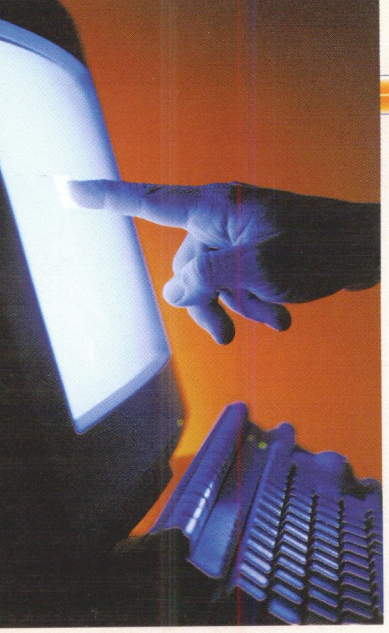
يمكن إدراك أهمية النسخ الاحتياطي بعد الإجابة على السؤال التالي: متى سيفشل القرص الصلب؟ جاءت صيغة السؤال بشكل يوحي بأن تعطل القرص الصلب قادم لا محالة وهذا شيء لا يتعارض مع سنة الكون فكل شيء سيتوقف عن العمل، حتى القرص الصلب نظراً لكونه جهازاً إلكترونياً شديد التعقيد، وفي حالة تعطله سيكون من الصعب استخراج البيانات المخزنة فيه، بالطرق العادية، ولذلك يجدر التنويه بأهمية تخزين بيانات النسخ الاحتياطي على مادة مرنة (أشرطة)، وتشفير البيانات، و إعداد النُّسخ الاحتياطية بحيث يتم طلب كلمة سر عند استرجاع البيانات.وعند تطبيق إجراءات النسخ الاحتياطي لا بد من حفظ وسائط النسخ بأمان.ولا بد من إجراء النسخ الاحتياطي دورياً، ويختار مسئول النسخ الاحتياطي زمن الدور، ويستحسن إعداد برنامج النسخ الاحتياطي ليعمل آلياً بشكل دوري.

وبالنسبة للتخلص من وسائط التخزين الرقمية المنتهية الصلاحية،فينبغي إتلاف وسائط التخزين باستخدام وسائل وبرامج متخصصة لإتلاف البيانات داخل وسيط التخزين قبل رميه بحاوية النفايات. وينضم تحت مظلة وسائط التخزين الرقمية كل من: الأقراص القابلة للضغط (zip drive)، الأقراص الضوئية (CDs) ، والأشرطة المغناطيسية (tape drive)، والأقراص الصلبة (hard disk drive) .

الإجراءات الممكن اتخاذها للتخلص الآمن من وسائط التخزين؟

إذا مارغبت المنشأة بإتلاف وسائط التخزين المنتهية الصلاحية التي تقع تحت سيطرتها، وجب عليها استخدام إحدى الطرق التالية:





- تعريض الوسط الذي يعتمد مبدأ المغنطة على حقل مغناطيسي، تدعى هذه العملية (degauss) ولها أدواتها ولا تصلح للأقراص الضوئية.
- الكتابة العشوائية على وسط التخزين، وتدعى هذه العملية (zeroization) وذلك باستخدام برامج خاصة، تجعل وسط التخزين غير قابل للكتابة أو القراءة.
- تدمير وسائط التخزين المراد إتلافها بتعديل خصائصها الفيزيائية كحرقها في فرن أو تفتيتها بالطحن، ولا يكفي طرق الواحد منها بمطرقة عدة مرات، وتعد طريقة الحرق أوالطحن الأكثر استخداماً نظراً لاقتصاديتها.

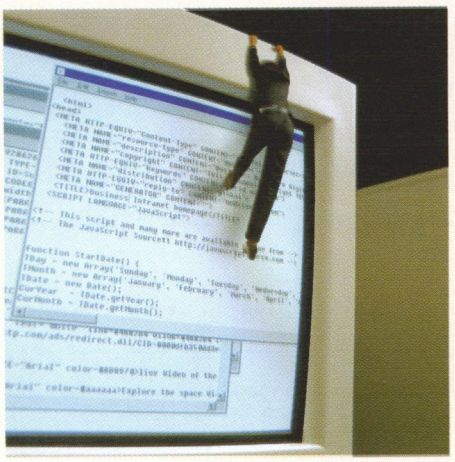
التوصية الحادية عشرة: إدارة المعلومات الحساسة بحكمة.

تعدّ قواعد البيانات، معلومات حساسة، ولذلك تصنّف إلى أربعة مستويات: سرية، موثوقة، داخلية، وعامة. ويقوم المتخصصون بتقنية المعلومات بتوزيع الصلاحيات على الموظفين كل بما يتناسب مع واجبه الوظيفي، والمهم بالنسبة للموظف أن يدرك مفهوم تصنيف المعلومات في مستويات، ليقوم بواجبه المتمثل بعدم السماح لأحد بالقيام بعمله الذي ينتمي إلى صنف معين بمستوى معين.وعندما يصل الموظف إلى هذا الإدراك سيقوم تلقائياً باتباع إجراءات أمن المعلومات دون حساسية أو تذمر.

ويجب الحذر من نقاط الضعف البشرية، فبعض المهاجمين يستخدمون الهندسة الاجتماعية. حيث يستخدمون مزايا الهندسة الاجتماعية للتعامل مع الطبيعة الشخصية للموظف، فقد يحصل على معلومة معينة عن طريق سؤال لا يتعلق بالمعلومة، ويكون السؤال ذا طبيعة شخصية بهيئة طلب المساعدة الإنسانية. وتكمن خطورة الهندسة الاجتماعية المستخدمة من قبل المهاجمين في إبطال فعالية المنتجات الأمنية لدى المنشأة المقصودة، ومن ثم تعريضها لأخطار الاختراق.ومن أهداف استخدام الهندسة الاجتماعية الحصولُ على المعلومات دون أسئلة مباشرة، لتمكنهم من الدخول لشبكة المعلومات، فقد يسألون عن معلومات صغيرة في أوقات مختلفة ثم يجمعون المعلومات الصغيرة ليحصلوا على معلومات متكاملة مفيدة لغاياتهم. وغالباً ما يستخدمون البريد الإلكتروني وغرف الحوار كمطيات للحصول على المعلومات المطلوبة، وهم بارعون في اكتشاف نقاط الضعف في أمن معلومات المنشأة، ومن ثم الدخول منها وتوجيه أسئلة جمع المعلومات. ولا بد من الانتباه إلى النقاط التالية لحماية بيانات المنشأة:

- يجب عدم إعطاء أية معلومة لأي منشأة غير معروفة حتى لو كانت تلك المعلومة تافهة. كما يجب عدم الكشف عن أية معلومة تخص المنشأة لأي فرد غير معروف، شفهياً أو هاتفياً أو بأي وسيلة أخرى.

ويجب التذكر بأن المنشأة تتكلف الكثير لشراء المعدات لتأمين شبكة المعلومات وأن الإجابة على سؤال بسيط من قبل موظف، قد يجعل كل تلك المعدات بلا فائدة.



التوصية الثانية عشرة:

اجعل مكتبك آمناً(نظيفاً) وتصرف بحكمة عندما تسير الأمور بغير ما يرام. حيث إن تنظيف طاولة المكتب من فوضى الأوراق والملفات -وليس من الغبار- لهو إجراء أمني مهم، وخصوصاً عندما يكون صاحب المكتب خارج مكتبه، فيفترض أن تكون الأوراق والملفات والأقراص داخل أدراج مقفلة. وبجانب تنظيف الطاولة وجعلها تبدو لامعة، يجب عدم نسيان السبورة في حالة وجودها، إذ يجب مسحها بعد الانتهاء من الحاجة إليها، ويمكن ضم إقفال شاشة الحاسب الآلي بكلمة سر إلى إجراءات التنظيف هذه. إن إجراءات النظافة هذه تمنع مَن لديهم صلاحية الدخول لغرف المكاتب من أخذ أية معلومة دون جهد يُذكر.

ولا بد بهذا الخصوص من تذكر النقاط التالية:

- يجب قفل أدراج المكتب عند مغادرة مكان العمل.
- يجب وضع الأقراص المرنة والأقراص الضوئية وما في حكمها في أدراج مزودة بأقفال.
- يجب التأكد من أن شاشة الحاسب بوضع مناسب يمنع رؤيتها بسهولة من قبل الآخرين.

أما عن حسن التصرف عند وقوع مشكلة فينبغي تذكر النقاط التالية:

- عند حدوث خلل أمني في شبكة المعلومات يجب عدم الانفعال بل من الأفضل الاتصال بخبير.
- عدم محاولة إصلاح الخلل من قبل الموظف نفسه، لأن الخبير لديه أدوات وقد قضى وقتاً طويلاً بالتدرب على استخدامها.
- ينبغي عدم مناقشة حوادث الخلل الأمنية مع الأصدقاء والمعارف، بل من خلال قسم تقنية المعلومات التابع للمنشأة فقط.

بعد استعراض التوصيات السابقة التي تحصّن خطوط الدفاع الأمنية لشبكة المعلومات، هل يكفي تطبيقها من بعض الموظفين فقط؟ بمعنى آخر إذا طبقها جزء، سقط عن الآخرين، طبعاً لا يكفي. لذلك ينبغي ملاحظة النقاط التالية:

- اتباع التوصيات المذكورة ووضع كل توصية في مكانها.
- على كل موظف أن يكون قدوة لمرؤوسيه في تنفيذ التوصيات الأمنية، ويتابعها باستمرار وليس بشكل متقطع.
- أن يضع كل موظف في اعتباره أن الخطة الأمنية خطة شاملة وله دور مهم فيها، وعند إخلال أي موظف بدوره، فإنه بذلك يفتح ثغرة في الخطة، تتناسب هذه الثغرة طرداً مع حجم الإخلال الحاصل.

وليتذكر كل موظف في أي منشأة تستخدم أنظمة الحاسب الآلي في أعمالها، بأنه مسؤول عن أمن معلومات منشأته، وأن أي تسريب لهذه المعلومات سيضر نفسه أولاً، ويضر منشأته ثانياً، بل يتعدى الأمر إلى أبعد من ذلك، فتسريب المعلومة في بعض الحالات قد يضر باقتصاد البلد أو بأمنه وقد يسبب أحياناً مئات الضحايا.ولا ينسى أن إجراءات السياسة الأمنية ما هي إلا سلسلة متلاصقة من الحلقات، يمثل واجب كل موظف حلقة منها، فإن أخل أحدهم بواجبه انقطعت السلسلة وعندها تقع المنشأة بخطر ما، يتناسب هذا الخطر مع الثغرة الحاصلة في أمن شبكة المعلومات.

* مركز المعلومات والحاسب الآلي - جامعة نايف العربية للعلوم الأمنية