بسم الله الرحمن الرحيم

محمد بن عبدالله العريفي **422001576**

أهمية التوعية بأمن المعلومات

مـقدمـة:

يمكن تعريف التوعية بأمن المعلومات بأنها تـفهُم الناس لدورهم في ضمان امن المعلومات وتقنيتها وقـدرتهم علـى اتخـاذ قرارات صائبة بهذا الخصوص. ولا يقتصر ذلك على مجرد معرفة الأخطار ومخاطر كشف المعلومات، بل القدرة على اتخاذ القرارات الصحيحة وكيفية ومدى حماية المعلومات وتقنية المعلومات. إن اتخاذ القرارات الصائبة كما سيتضح لنا يجمع ما بين التدريب والتفكير الصائب والقدرة على التعامل. وهذا التعريف لأمن المعلومات يركز على أهمية اتخـاذ القـرار باعتبـار أن مستخدمي أجهزة الكمبيوتر يتخذون القرارات الخاصة بأمن المعلومات بشكل روتيني وغالباً ما يتم ذلـك بـدون العلـم بهـذه القرارات . وحيث انه يمكن الآن إطلاق صفة (مطلعين) على العديد من مستخدمي أجهـزة الكمبيـوتر ، فـإن المعلومـات أصبحت متوفرة في كل مكان بحيث يمكن الإطلاع عليها وتعديلها ونقلها أو إتلافها. وغالباً ما تكـون المعلومـات الحساسـة محفوظة بين أيدينا ومكتوبة على ورق ومحفوظة أيضاً في وسائل يمكن إزالتها مثل أقراص السي دي روم. كما يتم حفظها في مكتب الشركة أو المكاتب داخل المنازل. وفي كل مرة نتعامل مع المعلومات سواء بشكل طبيعي أو الكترونـي ، فإننـا نقـوم باتخاذ القرارات حول كيفية حمايتها .

ومع توفر المعلومات في كل مكان وكثرة تعاملنا معها ، فمن غير المستغرب أن تتسـبب الأخطـاء البسـيطة وعـدم اتخـاذ الاحتياطات المطلوبة في العديد من الحوادث التي تؤثر في أمن المعلومات . وفيما يلي الأخطاء الشائعة بين الناس في مجـال امن المعلومات وهي اكبر الأخطاء التي ترتكب في هذا المجال والتي نشرتها مجلة **كمبيوتر ورلد** بتاريخ 9 يوليه 2001 :

- كتابة كلمة المرور على ورق كتابة الملاحظات.
- الإهمال من خلال ترك أجهزة الكمبيوتر دون الانتباه لها(بدون حماية).
- فتح مرفقات البريد الالكتروني الواردة بشكل غير متوقع.
- اختيار الأرقام السرية التي يسهل اكتشافها.
- ترك أجهزة الكمبيوتر المحمولة دون حماية(حماية جسية).

وهذه الأخطاء هي نتيجة للقرارات غير الصائبة التي يتم اتخاذها. ومما يؤسف له أن هذه القرارات أصبحت شائعة ومن غيـر المستغرب أن تجد مؤسسات تواجه مشاكل من قراصنة ولصوص الكمبيوتر. إن الفيروسات التي تسمى **تروجان هورسيز** مثل **لوف بوج** هي نتيجة مباشرة لقيام مستخدمي الكمبيوتر بفتح الملفات المرفقات المرسلة لهم والتي يفترض فيهم الاشتباه بها قبـل فتحها. كما تتم سرقة أجهزة الكمبيوتر المحمولة بشكل متكرر بسبب إهمال أصحاب هذه الأجهزة بتركها في المكاتب وغـرف الفنادق والأماكن الأخرى.

تعمل هذه الدراسة على تحليل بعض الأسباب التي أدت إلى انتشار الأخطاء في مجال أمن المعلومات. وتسـاعد العديـد مـن العوامل على هذه الأخطاء، إلا أن سبب هذه الأخطاء هو بالدرجة الأولى انعدام الوعي والمعرفة.

أهمية الوعي بأمن المعلومات :

تقضي الكثير من المؤسسات وقتاً كبيراً وتنفق المال في التركيز على الجوانب الفنية المتعلقة بأمن المعلومات في حين تعطي الجوانب البشرية الجزء اليسير من الوقت وغالباً ما يؤدي عدم التوازن هذا إلى نتائج عكسية في حماية التقنيات ومن ثم الاعتماد على التكنولوجيا في مجال الأمن بحيث تتعرض تلك المؤسسات للمخاطر من الجانب البشري .

واليوم انتشر الخطر المدمر للهجمات الفنية والهندسة الاجتماعية. وتعتمد معظم فيروسات البريد الالكتروني مثل **تورجان هورسرز** على سذاجة المستقبل لها وهي تهدف إلى تعريض أجهزة الكمبيوتر للخطر وبالتالي تعمل على الاستفادة من أنظمة البريد الالكتروني وشبكة الانترنت للوصول إلى هذه الأنظمة. إننا لا ندعو إلى تجاهل الجوانب الفنية لأمن المعلومات، ذلك أن الإخفاق في الالتفات إلى الجوانب التكنولوجية ينتج عنه العديد من المخاطر التي يتم استغلالها بسهولة من قبل الفيروسات والهجمات التي تعيق إيصال الخدمات واستغلال المشاكل في برامج الكمبيوتر . لكن التحكم البشري يُعتبر في نفس الوقت حيوياً لأمن النظام وأن الإخفاق في الاهتمام في الجانب البشري من شأنه تعريض النظام إلى العديد من المخاطر وكشف المعلومات مثل :

الهندسة الاجتماعية : يستغل المهاجم حسن النية من قبل المستخدم أو جهله في الحصول على المعلومات أو الوصول إليها . إن توعية المستخدمين حول مخاطر الأشخاص الآخرين الذين يستغلون حسن النية تؤدي إلى استعداد لؤلئك المستخدمين للتنبه من خطر تلك الهجمات.

إساءة استخدام الأنظمة والشبكات : يستخدم العاملون في أجهزة الكمبيوتر الموارد الرئيسية في الكمبيوتر مثل الاتصال بالانترنت أو المساحة المخصصة للتخزين لإغراض محظورة مثل(المشاركة في ملفات ام بي 3 أو الألعاب) بالإضافة إلى الاستفادة من موارد مكلفة، وهذا التصرف يعرض الأنظمة لإخطار أمن المعلومات أو مخالفة القوانين. إن الاستخدام السليم للأنظمة في المؤسسات يساعد على التقليل من استهلاك الموارد وكشف المعلومات الناتجة عن سوء الاستخدام.

سهولة التعرف على كلمة المرور : غالباً ما يختار مستخدمو أجهزة الكمبيوتر كلمات مرور يسهل التعرف عليها أو الوصول إليها. وأن توعية لؤلئك العاملين بكيفية اختيار كلمة المرور التي لا يمكن كشفها وأهمية ذلك يساعد على الحيلولة دون اختيار كلمات المرور التي يسهل التعرف عليها وكشفها.

الإطلاع التلقائي على الأجهزة : غالباً ما يترك مستخدمو أجهزة الكمبيوتر المحمول أجهزتهم دون حماية أو يضعون هذه الأجهزة أو أجهزة السيرفر في أماكن غير آمنة. إن وضع معايير للحماية يشجع مستخدمي الكمبيوتر على الاهتمام بهذا النوع من المخاطر.

الفيروسات وتوجان هورسز : هذه الأشكال من الفيروسات ربما تكون اخطر ما يهدد أمن المعلومات وغالبا ما تعتمد هذه الأخطار على مستخدمي الكمبيوتر من خلال إرسال الملفات بحيث يترك لؤلئك المستخدمون أجهزة الكمبيوتر دون حماية أو تشغيل تلك الأجهزة ببرامج منتهية الصلاحية للحماية من الفيروسات . إن توعية مستخدمي الكمبيوتر بوجوب الاشتباه بالملفات التي تصل فجأة بصورة غير متوقعة يساعد على حماية الأجهزة من تلك الفيروسات والأخطار. إن وضع معايير لنظام الكمبيوتر يقلل من انتشار عيوب البرامج القابلة للاستغلال وكذلك البرامج المنتهية الصلاحية لحماية الكمبيوتر من الفيروسات.

التكنولوجيا الجاهزة : غالباً ما يجهل مستخدمو الكمبيوتر الإخطار ومخاطر كشف المعلومات في أنظمة الكمبيوتر والتي تكون بحوزتهم. إن التوعية ووضع الأسس الاسترشادية الفنية يساعد مدراء النظام وغيرهم على توفير الحماية الكافية لأمن المعلومات.

التحديات التي تواجه أمن المعلومات

تسهم العديد من العوامل في صعوبة إيجاد الوعي في مجال أمن المعلومات . وهذه العوامل إما أن تؤثر على السلوكيات تجاه امن المعلومات أو تعيق القدرة على اتخاذ القرارات الصائبة لحماية المعلومات. وفيما يلي العديد من العوامل الرئيسية والتي ينبغي دراستها من قبل كل من يسعى إلى زيادة الوعي الخاص بأمن المعلومات :

مشغوليات رجال الأعمال :

إن رجال الأعمال لا يتوفر لديهم الوقت لأجل التدريب على أمن المعلومات فهم لا يلتفتون إلى هذا الموضوع كما أنهم لا يجدون الوقت للإطلاع على الإجراءات الخاصة بذلك أو التواصل معها.

عدم فهم الناس لأجهزة الكمبيوتر :

ينظر معظم الناس إلى أجهزة الكمبيوتر على أنها مجرد صناديق سوداء تعمل على تنفيذ ما نحتاج إليه. لكننا لا نفهم كيفية تعامل هذه الأجهزة مع بعضها البعض أو كيفية قيامها بتخزين المعلومات والتعامل معها . ويتراوح الفهم من مستوى لآخر بشكل كبير لكن المستوى العام يعتبر متدنياً. ولذلك من الصعب بالنسبة لمستخدمي الكمبيوتر تفهم المخاطر و الأخطار التي تتعرض إليها أجهزة الكمبيوتر والمعلومات الموجودة بها.

عدم تفهم الناس للمخاطر :

تعتبر المخاطر حسية وليست تقيميه. كما لا يفهم الناس بصورة كافية طبيعة المخاطر على أمن المعلومات والأخطار والقيمة الفعلية للمعلومات وغالباً ما يُساء تقديرها. إن القرارات الخاصة بأمن المعلومات والمستفيد من وعي أمن المعلومات تتطلب دراسة هذه المخاطر بسبب العلاقة المتبادلة بشكل عام بين الأمن والتكلفة والأداء والخطر والجوانب الأخرى.

رجال الأعمال يتحملون الأخطار أو يسعون إلى التعرف عليها

تسود لدى رجال الأعمال مقولة لا تعلم بدون مجازفة وهم غالباً ما يسعون للتعرف على المخاطر وبالتالي فهم يتفادون النظر في الاحتمال السلبي للخطر على أمن المعلومات . وحيث أن الأمن يكلف الوقت والمال، فان مدير الأعمال يتجاهل الأمن في سبيل تنفيذ نظام أو تقديم خدمة بشكل أسرع واقل تكلفة. وحتى عندما يتم إبلاغ هؤلاء المدراء بالمخاطر على امن المعلومات ، فهم يختارون المقامرة بأصول الشركات . إن العديد من هذه العوامل هي متأصلة ولا يمكن السيطرة عليها . وبالرغم من المصاعب المتزايدة التي يواجهها هؤلاء المدراء في تحقيق الوعي بأمن المعلومات ، فهم لا يعتبرون ذلك بمثابة المستحيل.

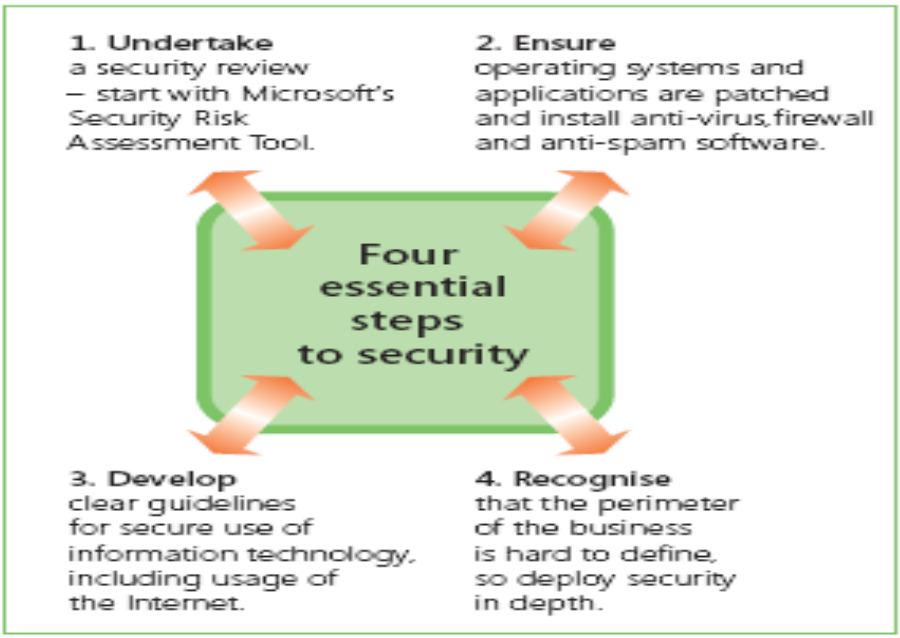
تتعاون شركة **ميكروسوفت** مع مؤسسة **ناشيونال سايبر سكيورتي اليانس** للمساعدة في زيادة امن شبكة الانترنت من خلال القيام بحملة توعية للمستهلكين والمؤسسات الصغيرة والأكاديميين والأسر في المنازل تستمر مدة شهر لتقديم المعلومات. وشركة **ناشيونال سايبر سكيورتي** هي مؤسسة غير ربحية يقوم برعايتها أكاديميون في مجال التعليم والحكومة الأمريكية

ومؤسسات متخصصة وشركات خاصة مثل **ميكروسوفت** . وتقدم هذه الشركة المعلومات والمصادر والوسائل التي تمكن الأفراد والمؤسسات الصغيرة من تحسين مستوى حماية أجهزة الكمبيوتر والمعلومات الشخصية لديهم من الأخطار المنتشرة في شبكة الانترنت.

لا شيء يمكن ان يضمن السلامة في عصر الانترنت، إلا انه يمكن عمل الكثير للتقليل إلى الحد الأدنى من التعرض للمخاطر . إننا نوفر العديد من المصادر للمساعدة على حماية المؤسسات وأجهزة الكمبيوتر والمعلومات الشخصية. كما أن المواقع في شبكة الانترنت تقدم الإرشادات للمساعدة في حماية الأطفال المستخدمين لشبكة الانترنت وبالتالي التصدي لعمليات النصب والاحتيال والتقليل من الرسائل الدعائية في البريد الالكتروني وبالتالي حفظ خصوصيات مستخدمي الكمبيوتر.

ست نصائح للبقاء أمناً على الانترنت :

1- **تقوية وتحديث دفاعات أجهزة الكمبيوتر :** من خلال استخدام جدار الحماية وتحديث برامج الحماية من الفيروسات وبرامج امن المعلومات وتحميل برامج حماية من الفيروسات واكتشاف وحذف ومنع كل ما من شأنه التجسس على الكمبيوتر.
2- **استخدام كلمات مرور يصعب اكتشافها أو الدخول منها** تتكون مما لا يقل عن ثمانية خانات وتشمل الأحرف والأرقام والرموز سهلة التذكر للمستخدم وصعبة الاكتشاف من قبل الآخرين.
3- **تروى أولاً ثم انقر بالفأرة بعد ذلك :** حتى لو عرفت المرسل تروى قبل فتح البريد الالكتروني أو المرفقات التي تصل مع رسائل البريد الالكتروني . لا تنقر على الروابط داخل البريد الالكتروني والرسائل الفورية والنوافذ التي تظهر على الشاشة.
4- **أحرص على حماية المعلومات الشخصية :** وعدم تقديم معلومات شخصية خاصة جداً في البريد الالكتروني والرسائل الفورية والنوافذ التي تظهر على الشاشة . ويجب التعامل مع رقمك الخاص بالتأمينات الاجتماعية بحذر وإعطاء عنوان بريدك الالكتروني إلى الأشخاص الذين تعرفهم فقط.
5- **تأكد من وجود الحماية لمعلوماتك الشخصية في مواقع الانترنت :** أقرأ التعليمات الخاصة بالمعلومات الشخصية. وقبل الإفصاح عن أي معلومات شخصية أو تنزيل البرامج ، تأكد من وجود حماية في الموقع للبيانات الحساسة. تأكد من وجود الأحرف **https** في عنوان الموقع ووجود رمز القفل () أو المفتاح في الزاوية اليمنى السفلى من الصفحة في الموقع . انقر نقرتين على رمز القفل أو المفتاح لتأكد من أن الاسم الصادر في شهادة أمن المعلومات مطابق للاسم الموجود في عنوان الموقع.
6- **أحرص على حماية الأطفال على الانترنت :** ينبغي الاهتمام بما يفعله الأطفال على الانترنت ومن يتحادثون معهم . امنع الأطفال من إعطاء أية معلومات شخصية بما في ذلك الصور بدون تصريح منك مع التنبيه على الأطفال بعدم الالتقاء شخصياً مع الأشخاص الذي يتم التعرف عليهم على الانترنت.



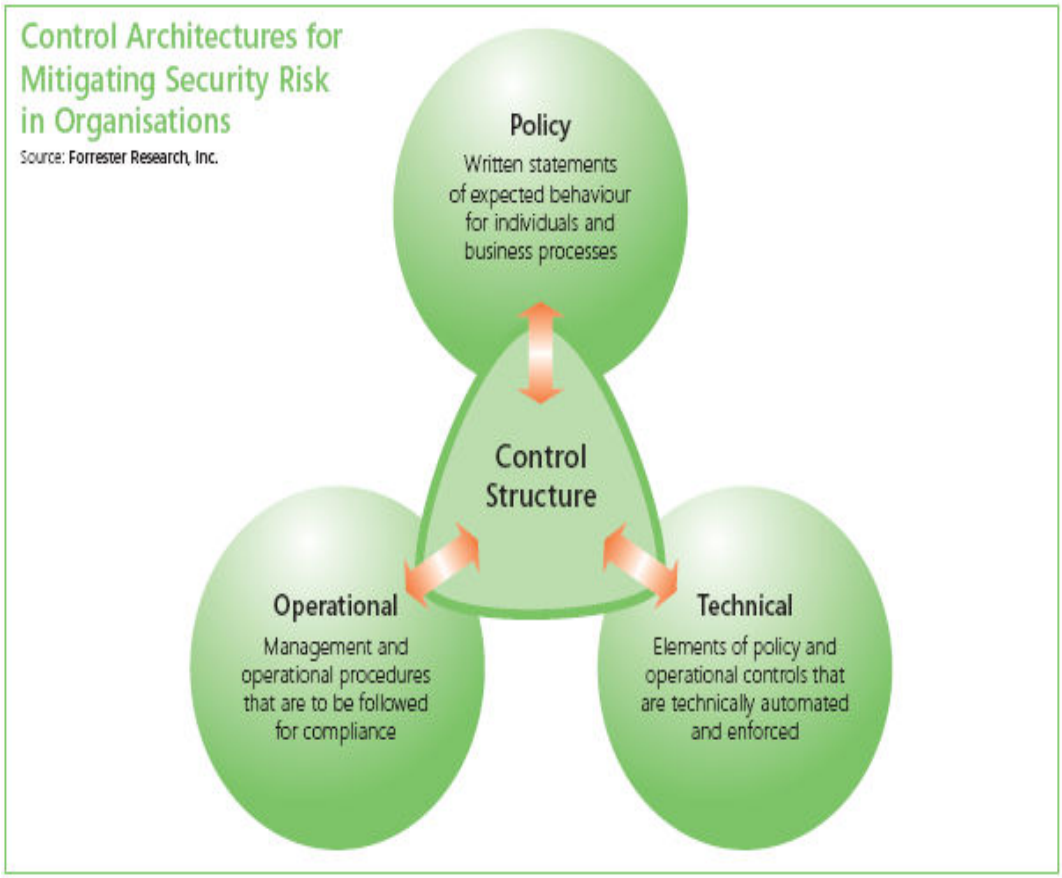
التعامل مع التوعية بأمن المعلومات في الوقت الحاضر

إن السياسات والنظم الخاصة بأمن المعلومات هي جوهر التوعية بأمن المعلومات . ذلك أن هذه السياسات التي تتعلق بأمن المعلومات تعتبر حيوية للوعي بسبب أنها تضفي الصفة الرسمية على أمن المعلومات في جميع أنحاء المؤسسة. وينبغي على تلك النظم تحديد الحد الأدنى من المتطلبات لأمن المعلومات وتبيان أن امن المعلومات هو من مسؤولية كل فرد. وينبغي أن تكون النظم الخاصة بأمن المعلومات صادرة من أعلى مصدر في المؤسسة وهو المدير العام بدلاً من المناصب الدنيا – مدير امن المعلومات. ذلك أن صدور هذه النظم من أعلى مصدر في المؤسسة من شأنه زيادة الوعي في المؤسسة ككل. كما ينبغي إيصال هذه النظم إلى الأقسام المعنية في المؤسسة. إن تحقيق الوعي الكامل في أمن المعلومات داخل المؤسسة يتجاوز مجرد النظم التي تعتبر الحد الأدنى للتوعية بأمن المعلومات. أما الإجراءات الأخرى فهي إجراءات الالتزام والتدريب والاختبار. وبناء عليه ، فيما يلي تحليل للمجموعات التالية من النظم الخاصة بالتوعية بأمن المعلومات في هذا القسم :

النظم الخاصة بسياسات أمن المعلومات : وهو محتوى النظم والمعايير والإرشادات الأخرى في أمن المعلومات وكذلك وسائل وضع هذه النظم وتسهيل استخدامها .

إجراءات الالتزام : وهي الأساليب الخاصة بضمان اطلاع مستخدمي الكمبيوتر على النظم وفهمها وكذلك استخدام الإجراءات الخاصة بالاستخدام.

السياسات الأخرى : وهي التدريب والتعليم والعمل على نشر المعلومات الخاصة بأمن المعلومات.



توصيات لزيادة التوعية بأمن المعلومات :

يمكن للمؤسسات أن تقوم بإجراء حاسم في مستويات التوعية بـأمن المعلومـات مـن خـلال وضـع الـنظم الخاصـة بالتوعية،ومعظم هذه الإجراءات ذات تكلفة قليلة نسبياً. وفيما يلي التوصيات والنصائح التـي ينبغـي إعطائهـا الأولويـة القصوى لزيادة التوعية بأمن المعلومات :

- **التعامل مع التوعية بأمن المعلومات على أساس خطوة تسويقية :** من خلال تحليل المجموعات التي تستخدم الـنظم والمعايير والأسس الاسترشادية الأخرى. إن تسويق الأمن ليس مجرد القيام بحملة دعائية بل أيضاً تفهـم احتياجـات العملاء الداخليين وتسهيل الحصول على أمن المعلومات وتفهمها واستخدامها.
- **ضمان موافقة المدير العام في المؤسسة أو من في حكمه على هذه النظم :** من اجل صدور هذه الـنظم مـن قمـة المؤسسة وليس من قاعدتها. وليس المقصود في المصادقة التوقيع بل الالتزام بنظم امن المعلومات ووضعها موضـع التنفيذ.
- **أن تشمل النظم الشاملة لأمن المعلومات العناصر الاعتيادية المتعارف عليها :** أي تصنيف الخطة الخاصـة بـأمن المعلومات من حيث معايير الأمن وتحديد الاستخدام المقبول والأسس الاسترشـادية المحـددة لضـمان التكنولوجيـا الرئيسية بين الآخرين . مع السهولة في استخدام نظم الأمن والمعايير والإجراءات والأسس الاسترشـادية الأخـرى. ونشر هذه النظم الكترونياً وطباعة كتيبات موجزة تغطي الجوانب الهامة في نظم الأمن واستخدام هذه النشرات لتنبيه مستخدمي الكمبيوتر بالرجوع إلى النسخ الأصلية الالكترونية منها.
- **إيجاد الوسائل المتطورة لتسهيل استخدام هذه النظم والمعايير والإجراءات والأسس الاسترشادية.** إن أكثر الوسـائل انتشاراً تشمل مرافق البحث أو الفهارس الشاملة أو المطبوعات (المخصصة على سبيل المثـال لمـدراء النظـام)

والإشعارات التلقائية بالتغيرات على تلك النظم . وإن أمكن استخدام أدوات من شأنها التأثير الفاعل على مختلف الأقسام المعنية في المؤسسة.

- **وضع نظام كامل ينسجم مع النظم :** يشمل المتطلبات من جميع مستخدمي الكمبيوتر للإطلاع على نظم أمن المعلومات والمعايير والإجراءات والأسس الاسترشادية الخاصة بذلك وكذلك الحاجة إلى إعادة الاطلاع عليها على الأقل سنوياً. ووضع تعليمات بالالتزام بهذه النظم وتخزينها الكترونياً حتى يتم استخدامها بسهولة. والتعرف على مستخدمي الكمبيوتر الذين لم يطلعوا على أو لم يطلعوا مرة أخرى على هذه النظم والمتابعة معهم لضمان التزامهم بذلك.
- **التعاون مع الموارد البشرية لضمان نشر وإيصال أمن المعلومات :** من خلال التدريب وإصدار كتيبات النظم والمراجعة الدورية للأداء . وكذلك ضمان معرفة مستخدمي الكمبيوتر التامة عند نقلهم إلى عمل جديد . إن عمليات التكامل مع الموارد البشرية مهمة بصفة خاصة للعاملين في المجال الفني مثل المدراء والمهندسين المعماريين والمقاولين.

المراجع المستخدمة في هذا التقرير :

1- Information Security Awareness, by Timothy P. Layton Sr
2- Information Security Awareness Basics, by Fred Cohen
3- Building an Information Security Awareness Program, by Mark B. Desman
www.microsoft.com/uk/business/security; www.microsoft.com4-
www.itsafe.gov.uk 5-
, yale university, security education *www.yale.edu/securityawareness6-*
www.pentasafe.com 7-

جدول بمحتويات التقرير :