وزارة التربية والتعليم

12

أمن وحماية المعلومات

كتاب الطالب

الصف الثاني عشر

نحو ثقافة إلكترونية آمنة

هيئة تنظيم الإتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

aeCERT Computer Emergency Response Team

تمهيد

الإنترنت .. عالم واسع .. شبكة عملاقة .. تلف الكرة الارضية شمالا وجنوبا ، شرقا وغربا.. دخول شبكة الإنترنت أشبه بالجولة في مملكة معظم الموجودين فيها سواحٌ ومسافرون من جميع بقاع العالم، والكل يتجول ويتنقل بحرية تامة دون هويات أو تأشيراتٍ للزيارة، حيث لا حدود ولا مراكز جمركية ولا فواصل طبيعية ، والتنقل والتجول فيها ممتعٌ جدا وشيقٌ وهو لا يعدو أكثر من نبضات الكترونية تربط أطراف ومعالم هذه المملكة العامرة..ودخول الشبكة (المملكة) يمثل مغامرة مثيرة للوهلة الأولى، ورغبة شديدة في التعرف على كل شيء والإطلاع عليه ..

هذا الإتساع المترامي لشبكة الإنترنت، صاحبه بروز ظواهر سلبية بين مرتادي الشبكة، وظهور جوانب تستلزم منا أخذ الحيطة والحذر من بعض التهديدات والمخاطر، ولذلك لحماية أنفسنا من التأثيرات المجهولة عبر هذا العالم الإلكتروني الهائل.

قد تكون البداية مجهولة ومشوشة .. ولكن سرعان ما تبدو جميع الأمور طبيعية ومنتظمة، حين إتباع الإرشادات والتعليمات التي ستأخذك لبر الأمان.

هذا المنهج يمثل أحد المصادر الهامة للتوعية بأمن وحماية المعلومات، وهو مادة مساندة للتعريف بكيفية الحد من المخاطر والإستفادة من فرص الإنترنت. كما يهدف إلى تعزيز قدرات وتغيير سلوك الطلاب في التعامل مع الإنترنت. يسعى هذا المنهج في نهاية المطاف الى نشر ثقافة إلكترونية آمنة عبر المؤسسات التربوية والتعليمية بالدولة.

والله ولي التوفيق ،

المقدمة

يحتوي هذا الكتاب على معلومات وتمارين سوف تغطي عددا من الموضوعات التقنية المتعلقة بأمن وحماية المعلومات. سوف نتطرق من خلال التمارين والانشطة إلى موضوعات سياسات أمن المعلومات، وكيف يمكن إختيار البرامج الآمنة، وما هي الاجراءات الواجب إتخاذها في حال وجود مشكلة في أمن المعلومات. كما سنتطرق الى كيفية التخلص من المعلومات وأجهزة الحاسوب بصورة آمنة في حال عدم الحاجة اليها والرغبة في التخلص منها. وستكون الانشطة والتمارين مصممة لكي تبحث في موضوع معين، ثم طرح الأفكار والنقاط في غرفة الصف (مختبر الحاسوب) من أجل إثراء النقاش وتبادل الآراء.

المخرجات

لعل من أهم محتويات هذا الكتاب ما سنقوم به من خلال شرح ما يلي:

- وصف العلاقة بين ثقافة أمن المعلومات ، والسلوكيات الآمنة في أمن المعلومات.
- تعريف سياسات أمن المعلومات.
- مناقشة أهمية الأمن المعلوماتي لمواقع العمل.
- تعلم أهمية إختيار البرامج الآمنة بعناية.
- شرح كيفية التعامل المناسب مع المشاكل الأمن المعلوماتي.
- تعلم كيفية التخلص الأمن من أجهزة الحاسب الألي والمعلومات التي لا حاجة لنا بها ،.

جدول المحتويات

الثقافة الأمنية	الدرس الاول

تعريفات

المعلومات الشخصية Personal Information – أي معلومة يمكن إستخدامها لتحديد هوية شخص ما، وهي معلومات بالامكان إستخدامها لتمييز أو تعقب شخص ما، مثل: الأسم، الرقم الشخصي، الصفات البدنية ، السجلات العضوية ، والمعلومات الطبية ، وتاريخ ومكان الميلاد وعنوان السكن عنوان البريد الإلكتروني ،رقم الهاتف ، ..... .

المعلومات الخاصة Private Information– أي معلومة تخص شخص معين وليس لديه رغبه في مشاركتها مع آخرين. وقد تشمل هذه المعلومات : الأسرار الخاصة ، الملكية الفكرية، أو أي معلومات لا يفترض أن تكون متاحة للآخرين.

الأجهزة المحمولة Mobile Devices – أي جهاز يمكن حمله وعمله أثناء التنقل به بحرية تامة ، ويستخدم في الاتصال ويرتبط بشبكة الإنترنت.

البرامج الخبيثة Malicious Software – (MALWARE)هي برامج يتم تصميمها بغرض التشويش أو تخريب أجهزة الحاسب الآلي. وهناك أنواع كثيرة للبرامج الخبيثة، كالفيروسات ، والديدان ، وبرامج التجسس، وأحصنة طروادة ، وغيرها.

المهندس الاجتماعي Social Engineer– هو الشخص الذي يستغل عفوية وعدم انتباه الناس للقيام بجمع المعلومات الخاصةبهم ، وسرقة الهويات والمعلومات الشخصية، بقصد الحصول على مكاسب بطرق الدهاء والمكر.

بطاقة الدخول Key Card– هي بطاقة تستخدم للسماح بدخول مكان ما ، وهي مزودة بترددات لاسلكية تتصل بقارىء خاص مثبت على قفل الباب ، مرتبطٌ بنظام آلي يتعرف على صاحب البطاقة ، ويصرح له بالدخول في مواقع معينة وأوقات محددة.

التغييرات في ثقافتنا الأمنية

مع مطلع تسعينيات القرن الماضي حينما بدأ الأفراد بمحاولة إستخدام بعض التقنيات وأجهزة الحاسب الآلي ، كانت تواجههم صعوبات عدة ، فكان عليهم تعلم :

- تشغيل جهاز الحاسب الآلي بطريقة سليمة.
- الكتابة بإستخدام لوحة المفاتيح ، وإستخدام الفأرة.
- إستخدام البرامج والانظمة لإنجاز غرض معين.
- ما يقومون به في حال تعطل أحد أجزاء هذه الاجهزة .

كل هذا أصبح من الماضي ، فأنت ووالديك ، أصبحتم مستخدمين متمكنين لأجهزة الحاسب الآلي منذ دخولك المدرسة ، أو لربما منذ فترة أطول. اليوم ترى الصغار يستخدمون التقنيات الحديثة بكل سهولة ويتعلمون في وقت قياسي قصير التعامل مع أجهزة الحاسب الآلي وأجهزة الهواتف الذكية ، والألواح المزودة بشاشة اللمس ، حتى قبل أن يتعلموا أبجديات القراءة !

وبدا هذا التغيير واضحا في حياة الافراد ، وذلك لدخول هذه الاجهزة وتقنيات الاتصال بشبكة الإنترنت في الحياة اليومية ، وأصبحت جزءاً من ثقافة الجميع . فكانت شبكة الإنترنت في التسعينيات من التقنيات الحديثة، والآن وبعد مضي عشرون عاما ، أصبح الإنترنت واقعاً نعيشه من حولنا .

وللأسف لم تحظ هذه التقنيات الجديدة وأجهزة الحاسب الآلي والهواتف الذكية بأي تثقيف ووعي كاف في الجانب الأمني وخاصة حين الإتصال بشبكة الإنترنت. فلدينا عادات وسلوكيات نمارسها في حياتنا اليومية تجعلنا في أوضاع آمنة وسليمة. فنقوم بقفل باب المنزل حين نخرج للتنزه، وكذلك نهتم بقفل باب السيارة حين نتركها في موقف السيارات. ونهتم بتزويد المنزل بأجهزة المراقبة والانذار للمحافظة على أمننا وسلامتنا. وبالمثل يجب أن نقوم بالاهتمام بسلامتنا المعلوماتية والمحافظة على أمن أجهزة الحاسب الآلي

لدينا وما تحتويه من معلومات .

شبكة الإنترنت مكنتنا من الاطلاع على الافكار الجديدة والتواصل مع الافراد بصورة سريعة. في بعض الجوانب ، هناك معلومات مثيرة لإهتمامنا، وتجعل الافراد يتشاركون في تبادل بعض المعلومات مع من يشاركهم نفس الاهتمام. ولكن للأسف ليس كل من يتواجد على الإنترنت لهم إهتمامات إيجابية مشتركة، فهناك من له مأرب اخرى كالإضرار بالاخرين، والإحتيال ، والسرقة، وخداع الناس. ولذلك يجب أن نولي موضوع حماية المعلومات الخاصة بنا مزيدا من الاهتمام والعناية، تماما مثلما نحافظ على أمن وسلامة منزلنا وسيارتنا والممتلكات الآخرى.

تهذيب العادات

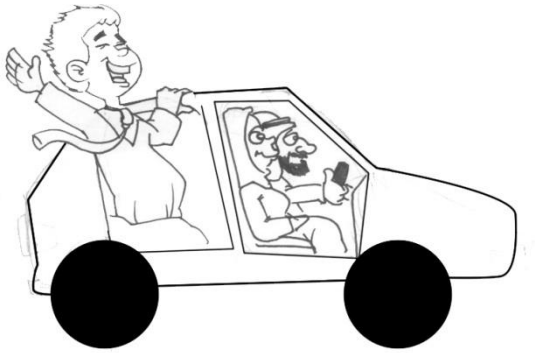
أفضل الوسائل والطرق لحماية أنفسنا من الايذاء والضرر هو إتباع سلوك أمني فاعل. والسلوكيات الآمنة هي تلك التي تتشكل بقناعة منا بأننا نقوم بالتصرف السليم، ونمارس هذه التصرفات بصورة متكررة ومتواصلة.

خلال تعاملنا مع أجهزة الحاسب الآلي والإنترنت، يجب علينا أن نتبع سلوكا أمنيا سليما وبصورة مستمرة . حين نؤمن بأهمية أمن وحماية معلوماتنا وأجهزتنا والإنترنت ، فإنه يستلزم أن نمارس العادات الآمنة للوقاية من مخاطر قد تعترض طريقنا ونحن نستخدم جهازنا الشخصي أو خلال تجوالنا بشبكة الإنترنت أو خلال تعاملنا مع البريد الإلكتروني، أو اي تقنية قد تبرز في المستقبل.

هذه العادات الآمنة ستؤثر حتما في الاخرين من حولك، وسيتعلمون منك افضل الممارسات والسلوكيات الحسنة ، وسيدركون أنها الوسيلة الصحيحة لإستخدم الحاسب الآلي أو أثناء التعامل مع الإنترنت. وبالطبع ستمرر وتنتقل هذه العادات الى أصدقاءهم والمحيطين بهم وهكذا ..

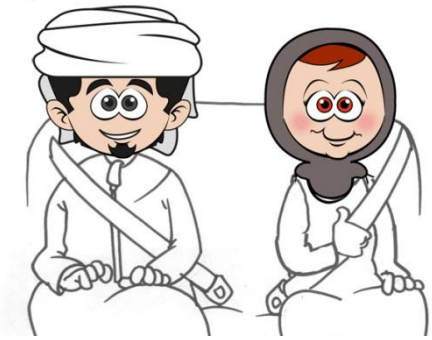
تبدأ ثقافة أمن وحماية المعلومات بإدراك أهمية إتباع سلوك أمني واعٍ ، ثم الإيمان بتغيير بعض العادات الخاطئة ، ثم ممارسة العادات السليمة وتطبيقها بصورة مستمرة ومتواصلة خلال استخدام الحاسب الآلي ، وأثناء إبحارنا في شبكة الإنترنت.

الأمن غير المزعج



في بعض الأحيان لا يجب أن تكون المسألة الامنية مزعجة، والا تمنعنا من أداء ما نود أن نقوم به بإستخدامنا للتقنيات المختلفة. بل على العكس، يجب أن نشعر بالارتياح حين نمارس العادات الآمنة ونستمتع بما نقوم به في شبكة الإنترنت وقنوات الاتصال الإلكترونية.

وخير مثال على الأمن غير المزعج ، هو أقفال الباب الخاص بك . فإن كنت ترغب بدخول السيارة بسرعة وبسهولة، فيتحتم عدم وجود أبواب للسيارة ، ولكن في هذه الحالة لن تكون السيارة آمنة للإستخدام. ولذلك نرى الأبواب موجودة في السيارة التي نركبها. قد يستغرق فتح الابواب وركوب السيارة وقتا أطول ولكن في النهاية هذه الابواب هي التي تحمينا وتجعلنا في أمان وقت السياقة في الطرق والشوارع السريعة. كما أن وجود أقفال للابواب يجعلنا مطمئنين من عدم سرقتها ، حين نقف بالسيارة في المواقف العامة.



وأمن أجهزتنا الشخصية والإنترنت هو تماما كما في المثال السابق. فنواجه في بعض الاحيان بعض الصعوبات ومزيدا من الوقت في بداية استخدامنا لجهازنا الشخصي أو دخولنا المواقع والخدمات الإلكترونية في شبكة الإنترنت ، الا انها ضرورية من أجل توفير سلامة وأمن أفضل لهذه الاجهزة، بالضبط مثل أقفال أبواب السيارة. وعندما تستخدم جهازك بدون ان يكون لديك برنامج لمكافحة الفيروسات، فإنه من المحتمل إصابة جهازك بفيروس خلال الاتصال بشبكة الإنترنت، وإن كان دخولك ووصولك للشبكة بسرعة وسهولة ، الا انه يفتقد الأمان. وكذا الحال حينما لا تقوم بتحديث نظام التشغيل لديك بصورة دورية ومستمرة فإنه على الأرجح أن تكون هناك ثغرات وفجوات أمنية خطرة تهدد أمن جهازك حين تكون متصلا بشبكة الإنترنت.

هذه المهام السهلة يمكن ببساطة أن تصبح عادات حميدة تواظب عليها لتحمي أجهزتك ومعلوماتك الخاصة وقت إتصالك بشبكة الإنترنت، ولن تكون هناك عقبات أمنية في طريقك في المستقبل.

عادات حميدة

العادات الأمنية الحميدة مهمة ويجب أن تعتاد على ممارستها بصورة مستمرة. فيجب عليك النظر في أفضل الطرق لحماية جهازك ومعلوماتك . وحين تتعرف على أنواع التهديدات الأمنية لجهازك ، فإنك حتما ستتوصل الى بعض الحلول الجيدة لتضمن حماية وأمان معلوماتك الخاصة.

عليك أن تحدد بصورة واضحة الأجهزة والحاسبات الالية والمعلومات الهامة المخزنة عليها والتي تريد المحافظة عليها بأمان.

ثم عليك أن تعرف التهديدات والمخاطر التي تواجه هذه الاجهزة والمعلومات التي تريد تأمينها. فهناك التهديد المادي ، مثل الاضرار الناتجة عن السرقة أو ارتفاع درجة الحرارة ، أو تسرب المياه، وأي نوع من الحوادث العارضة التي من الممكن أن تحدث إذا لم نحافظ على أجهزتنا المحمولة أو الشخصية. وهناك تهديد من الأشخاص المتطفلين من الخارج ، والذين يستخدمون الهندسة الاجتماعية لخداع الناس بحيل مختلفة بقصد الوصول للمعلومات الخاصة أو الاطلاع على الحسابات البنكية.

وهناك تهديدات البرامج الخبيثة المرسلة عن طريق البريد الإلكتروني ، والتي تحوى ملفات التجسس والفيروسات، ووصلات المواقع المشبوهة. ومن التهديدات كذلك ، محاولة الأشخاص المتطفلين الذين يسعون للوصول والدخول لحسابك الشخصي في خدمات البريد الإلكتروني، ومواقع التواصل الاجتماعي ، وغيرها ممن يحاول سرقة كلمة المرور الخاصة بك للدخول لتلك الانظمة وإنتحال شخصيتك والإطلاع على ما يمكن الوصول اليه من معلوماتك الخاصة. وهناك الاشخاص الذين ينقبون في سلال المهملات من أجل تعقب بعض المعلومات الموجودة على الأوراق والتقارير القديمة. مما قد يسهل عليهم الدخول لجهازك الشخصي والوصول لمعلوماتك الخاصة.

وعند السفر، فإن التهديدات تتضاعف وبطرق مختلفة، والتزامك بعادات أمنية سليمة تقيك وتحميك من أنواع أخرى من التهديدات الخطرة في أمن المعلومات.

السياسات الأمنية

السياسة الأمنية هي نسخة مكتوبة من مجموعة من العادات السليمة ، والتي تأمل المؤسسة من موظفيها بالالتزام والتقيد بها. تماما كما تعرفت في الفقرة السابقة حول التهديدات والمخاطر التي تستند عليها لحماية أجهزتك ومعلوماتك الخاصة.

هذه السياسات تغطي مجموعة واسعة من القضايا والمواضيع التي تهم المؤسسة ، نذكر منها:

1. كيف تتم عملية توظيف الموظفين.
2. آلية العمل وتبادل المعلومات مع الأشخاص الغرباء والشركات الأخرى.
3. كيفية حماية أجهزة الحاسب الآلي من الاضرار الخارجية.
4. كيفية تشغيل أجهزة الحاسب الالي والشبكات بشكل آمن.
5. متطلبات برامج مكافحة الفيروسات والبرامج الخبيثة.
6. التهيئة الصحيحة والأمنة لكافة الأجهزة والشبكات بحيث تكون آمنة.
7. صلاحيات المستخدمين وكيفية دخولهم للأجهزة والشبكات.
8. آلية إختيار البرامج والأنظمة الجديدة وطرق تثبيتها.
9. كيفية التعامل مع الحوادث الناتجة عن إختراق أمني.
10. آلية التصرف في حالة وقوع كوارث مرتبطة بإنقطاع خدمات الكهرباء أو إنقطاع الشبكة.
11. الالتزام بالقوانين والأنظمة العامة عند إستخدام أجهزة الحاسب الآلي والإنترنت.

هذه القواعد تكتب وتنشر للموظفين كافة لتوجيههم بالطرق الصحيحة لكيفية التعامل والاستخدام الأمثل والآمن لموارد المؤسسة من أجهزة حاسب آلي والدخول لشبكة الإنترنت. هذه التعليمات مهمة للموظفين كافة، ويتحتم عليهم الالتزام والتقيد بها لما تظنه المؤسسة هاما للمحافظة عليه وحمايته، كالمعلومات الخاصة بأفكار المنتجات الجديدة، وإستراتيجية المؤسسة تجاه الشركات المنافسة، والمعلومات المالية، والمعلومات الشخصية للافراد العاملين في المؤسسة.

التقيد بهذه السياسات الامنية يساعد المؤسسة في حماية أعمالها ووضعها الاداري ، مما يضمن بقاء العاملين فيها في وظائفهم. وعدم إتباع هذه السياسات قد يؤدي الى الاضرار بالمؤسسة وإضطراب وضعها المالي والاداري مما قد يؤدي الى تسريح العاملين فيها وفقدهم لوظائفهم. وفي بعض الحالات يؤدي الى مخالفة القوانين العامة ، والمساءلة القانونية التي لا يرغب أحد بأن يكون في مثل هذا الموقف. فمثلما لا ترغب في تسريب معلوماتك الخاصة من أجهزتك الشخصية بواسطة صديق أو شخص قريب منك، فإن المؤسسات لا ترغب بسرقة معلوماتها أو تسريبها للآخرين.

الأمن المادي والتحكم بالدخول

جانب يغفل عنه الكثيرون في مجال أمن المعلومات، هو الأمن المادي. ويشمل الامن المادي نقاط عديدة ومختلفة.

التحكم بالدخول الى المبنى

الدخول الى منزك والذي تحتفظ فيه بأشياء ثمينة وخاصة ومن ضمنها أجهزتك الشخصية، يتم التحكم بالدخول اليه وحمايته عن طريق مفتاح المنزل. وغالبا ما يحتفظ أفراد الاسرة البالغين فقط، بنسخة من هذا المفتاح، ولا تصرح لأي أحد من الغرباء بالحصول على هذا المفتاح الخاص بمنزلك.

وتقوم المؤسسات بحماية مواردها الثمينة وأجهزتها ومعلوماتها عن طريق مفاتيح أو بطاقات دخول للمبنى. وتصرح فقط للعاملين فيها بالحصول على هذه المفاتيح الخاصة للدخول الى المبنى والوصول الى مكاتبهم ومناطق معينة في المؤسسة. وحينما يحاول شخص غريب بالدخول لمبنى المؤسسة ولا يملك مفتاحا أو بطاقة دخول ، فإنه يحاول إيجاد وسيلة أو حيلة للدخول.

وهناك العديد من الحيل والاساليب للدخول بدون تصريح، لعل أبسطها وأوسعها إنتشارا الدخول مباشرة وراء شخص مصرح له بالدخول، والتظاهر بالإنتماء للمؤسسة أو الادعاء بنسيان بطاقة الدخول أو عدم الارتباك والتظاهر بعدم المبالاة وكأنه أحد العاملين بالمؤسسة.

فمن المهم عدم السماح للأشخاص الآخرين بالدخول خلفك بدون تصريح أو مخولين بالوصول لمنطقة ما في المؤسسة. وإن كان المدخل محمي بمفتاح للدخول ، تأكد من غلقه بإحكام خلفك، ولا تدع الغرباء يدخلون بدون إذن أو أي تصريح واضح.

حماية الوصول الى الأجهزة

من الامور الهامة المرتبطة بالأمن المادي ، حماية الوصول الى الاجهزة. فإن تمكن شخصا ما من الوصول الفعلي الى جهاز حاسب آلي أو جهازاً محمولاً، فهناك أشياء كثيرة وعديدة يمكنه القيام بها، ولعلها تسهل عليه عملية الإختراق للأنظمة بدلاً من أن يقوم بها عن بعد عبر الإنترنت. فإن حصنت المؤسسة أجهزتها وأنظمة المعلومات الخاصة بها عبر الإنترنت، ووضعت الحلول التقنية المتقدمة، وأغفلت حماية الوصول لأجهزتها بصورة مادية، وتمكن المخترق من الوصول الفعلي للأجهزة، فإنها وضعت مواردها المادية كافة تحت سيطرة المخترق وبصورة سهلة جدا وساذجة. فمن السهولة بمكان سرقة الجهاز نفسه أو الاطلاع على ما يحويه من معلومات، أو محاولة تسجيل الدخول للنظام عن طريق الجهاز، أو تركيب برامج وأدوات تسهل عملية إختراق وإقتحام الانظمة بكل سهولة.

ولعل من أهم الطرق للتأكد من الحماية المادية لأجهزة الحاسب والاجهزة النقالة،الأنتباه للنقاط الآتية:

- في حالة عدم استخدام الحاسب الآلي والهاتف الخلوي، اتركهم في مكان آمن بمنزلك. يمكن الدخول المباشر لمنزلك عن طريق الباب الذي لا يمكن فتحه إلا باستخدام المفتاح. فإذا توصل أحد لمفتاح منزلك، بإمكانه الدخول وسرقة الحاسب الآلي الخاص بك. وبالتالي الإحتفاظ بأجهزتك في أماكن آمنة يجعل سرقتها أمر في غاية الصعوبة.
- لا تترك حاسبك الآلي أو هاتفك المحمول في الأماكن العامة بعيداً عن نظرك. فهذه أنسب فرصة للسرقة بالنسبة لأي لص، فالأمر يتطلب لحظات معدودة لتختفي أجهزتك من أمامك، ولكن للأسف قد تختفي معها أيضاً المعلومات المخزنة بداخلها.
- لا تترك الحاسب الآلي المحمول أو الهاتف النقال في سيارتك أثناء توقفها في مواقف السيارات. قد تتم سرقتهم أثناء غيابك. وهناك الكثير من حوادث سرقة الأجهزة الإلكترونية من داخل السيارات حول العالم.
- إذا كنت مسافراً، فلا تترك الحاسب الآلي المحمول أو الهاتف النقال في غرفتك بالفندق المقيم به، لإنك لا تدري من قد يدخل إلى غرفتك في غيابك ويسرق أجهزتك الإلكترونية. ضع أجهزتك في خزانة الغرفة أو احملها معك لتتجنب سرقتها.

الحماية من الظروف البيئية

الظروف الطبيعية مثل الحر الشديد أو البرد الشديد قد تتسبب في التلف الكامل للحاسبات الآلية أو الهواتف المحمولة. إذا تلف هاتفك المحمول، معنى ذلك أنك ستخسر كل المعلومات المخزنة عليه. ولذلك ينبغي عليك المحافظة على أجهزتك الإلكترونية من تلك الظروف، الأمر الذي يتطلب منك الإنتباه للنقاط الآتية:

- لا تترك الحاسب الآلي المحمول أو هاتفك النقال في سيارتك حيث الحر الشديد. فقد تتسبب شدة الحرارة في تلف بعض أجزاء الجهاز الحساسة، الأمر الذي قد يؤدي إلى تعطل الجهاز بالكامل وفقد المعلومات المخزنة بداخله.
- من الأفضل إبقاء أي سوائل، مثل الماء والعصير والشاي والقهوة وغيرها، بعيداً عن أجهزتك الإلكترونية. فهذه الأجهزة تعمل بالكهرباء، والسوائل قد تؤدي إلى تلف المكونات الإلكترونية بالجهاز وبالتالي تلف الجهاز نفسه.

العادات الأمنية السليمة

فكر بالعادات الأمنية السليمة التي يجب عليك اتباعها لتحمي المعلومات الشخصية والخاصة. ومن المؤكد أنك تحتفظ بمعلومات لها قيمة كبيرة عندك على هاتفك المحمول أو حاسبك الآلي. اتبع التعليمات التالية لتنشئ قائمتك الخاصة بالعادات السليمة التي يجب إتباعها.

1. اكتب قائمة بأجهزة الحاسب الآلي والهواتف الخلوية التي تستخدمها عائلتك، واذكر المعلومات الشخصية أو الخاصة التي قد تتواجد على كل منها. اذكر مدى استخدامك لتلك البيانات وأهميتها عندك.
2. رتب الأجهزة التي أدرجتها بقائمتك من حيث الأهمية.
3. اكتب في ورقة منفصلة الطرق التي من خلالها يمكنك حماية تلك الأجهزة. آخذاً بالإعتبار طرق الحماية من السرقات والتلف المباشر لها (الماء والجو أو السقوط)، أوالحماية من الهندسة الإجتماعية والبرامج الخبيثة ومحاولات الإختراق وإنتحال الشخصية. اضف إلى القائمة أي طرق أخرى للحماية من أي تهديدات.
4. اختر عشر طرق من طرق الحماية التي قمت بكتابتها واذكر كيفية اتخاذها كعادات. اشرح ما ستقوم به وأهمية تلك العادات وكيف ستدرب نفسك على ممارستها بشكل دائم.

الدرس الثاني	اختيار البرامج

تعريفات

البرمجيات **Software**– مجموعة من الاوامر (التعليمات) لتوجيه الحاسب الآلي للمهام المراد أداؤها. العديد من البرمجيات يكون لها واجهة مستخدم User Interface لتسهيل التعامل مع البرنامج. ومن أمثلة تلك البرامج: نظم التشغيل وبرامج معالجة النصوص وبرامج الجداول الحسابية.

انتقاء وشراء برامج الحاسب الآلي

هناك العديد من الأمور التي يجب وضعها بالإعتبار عند شراء وتحميل البرامج الإلكترونية على الحاسب الآلي.

البرامج الإلكترونية على حاسبك الآلي

اكتب قائمة بالبرامج المثبتة على حاسبك الآلي.

1. اكتب الغرض من كل برنامج (استخداماته). رتب البرامج من حيث أولوية الاستخدام. البرامج المهمة هي التي تستخدمها بشكل مستمر ولا يمكنك الإستغناء عنها في المنزل أو المدرسة.
2. اذكر كيفية حصولك على كل برنامج سواء قمت بشراءه من أحد محال الحاسب الآلي أو من أحد المواقع الإلكترونية أو قمت بتحميله مجاناً من شبكة الإنترنت.
3. أعد النظر في قائمتك لتعرف كيف اتخذت قرارك بتثبيت تلك البرامج على حاسبك الآلي.

اسم البرنامج	الغرض	الاولوية	المصدر

كيف تختار البرامج الإلكترونية؟

أول أمر لا بد لك أن تفكر فيه، هو "ما الذي تحتاجه؟"، فكل برنامج له غرض للاستخدام، وكي نقوم بقرار شراءه أو تحميله أو تثبيته على الحاسب الآلي، فإننا بالطبع لا بد أن نكون متأكدين أنه يؤدي الغرض والمهمة التي نحتاجها.

الأمر الثاني هو النظر في أي برنامج نختار مع توافر العديد من البرامج التي قد تؤدي نفس المهمة. أبسط مثال هي برامج تصفح الإنترنت، فهناك العديد منها مثل انترنت إكسبلورير وفايرفوكس وجوجل كروم وسفاري وغيرها من المتصفحات الأقل شهرة. هل تعرف كيف تختار البرنامج المناسب منها ؟

هذه بعض المميزات التي قد تضعها بالإعتبار عند اختيار متصفح الإنترنت:

- سرعة عرض صفحات الإنترنت.
- سهولة استخدام القوائم.
- التأمين ضد البرامج الخبيثة والمواقع المشبوهة.
- هل يعمل جيداً أم أحياناً ما يتعطل.
- كيف يدير الصفحات المفضلة.
- هل يسمح بفتح تبويبات مختلفة.

الأمر ذاته يحدث عندما تبحث الشركات الكبرى عن البرنامج المناسب للمساعدة على إنجاز الأعمال. المطلوب هو برامج للقيام بمهام الحسابات المالية، فيتم تحديد قائمة بالمميزات المطلوب توافرها في البرنامج مثل توافقه مع النظم الادارية في المؤسسة أو مدى سهولة استخدام البرنامج أو مدى قابليته للتعامل مع العملات المختلفة...إلخ. وهذا يسهل عملية تحديد واختيار البرنامج المناسب.

واحدة من أهم المميزات التي يركز عليها الجميع عند اختيار أي برنامج هي السعر. إذا كان مجاناً فسيكون هذا بالطبع مغرياً للحصول عليه بل وقد يدفعك هذا للتغاضي عن خلوه من بعض المميزات التي تحتاجها. وإذا كنت ستشتريه فمؤكد أنك تتطلع أن يحتوي على جميع المميزات التي تريدها.

هناك أمر آخر وهو الأهم عند اختيارك للبرنامج الذي تحتاج تحميله أو شرائه وهو مصدره، فهل مصدرالبرنامج موثوق به؟ إذا كانت الشركة المنتجة للبرنامج من الشركات المشهورة مثل مايكروسوفت أو آبل فهذي برامج ذات ثقه لدى المستخدم.

ولكن ماذا لو اصدرت هذه الشركات الكبيرة برامج بها مشاكل أو نقاط ضعف؟ برامج أدوبي، مثلا بها العديد من المشاكل التي يعملون على حلها سريعاً، على الرغم من وجود غيرها من الثغرات في برنامج أكروبات Acrobat وفلاش Flash. وكذلك برامج شركة آبل Apple قد تحوي بعض برامجها على مشاكل وثغرات مماثلة. وخلال السنوات السابقة، انتقد كثيرٌ من المستخدمين شركة مايكروسوفت لأحتواء برامجها وأحد اصداراتها من برامج نظم التشغيل – على مشاكل فنية ونقاط الضعف.

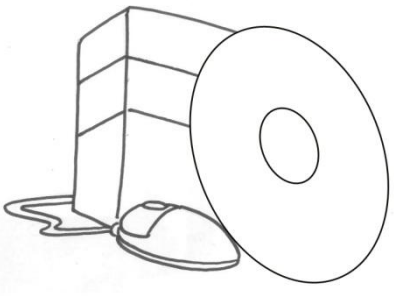
ويصبح التحري عن الثقة في البرامج أكثر وأكثر عندما تكون منتجة من قبل شركات غير معروفة. هذه الشركات تقدم العديد من الخدمات من خلال برامجها مثل التوقيت الدولي المختلف لدول العالم أوطرق جديدة لإرسال الملفات أو التراسل أو التواصل بالفيديو عبر الإنترنت.

كيف تتأكد أن هذه البرامج آمنة؟

يصعب ذلك الأمر في الكثير من الأحيان.

بعض برامج مكافحة الفيروسات تجري تقييم للبرامج ومدى الثقة بها. يمكنك أيضاً عمل بحث بشأن البرامج والشركات غير المعروفة، على شبكات التواصل الإجتماعي أو المواقع التي تقيّم أداء البرامج التي يستخدمها الأخرون. فكر بالمعايير الثلاثة التالية قبل تحميل أي برنامج تحتاج لإستخدامه:

- هل تعرف شركة البرمجة وتطوير الانظمة؟ وهل لها سمعة طيبة؟ الكثير من شركات البرامج مثل Google, Apple, Adobe, VMware, Microsoft لها تاريخ معروف ويمكنك الوثوق بها. قد لا تخلو جميع برامج هذه الشركات من المشاكل أو نقاط الضعف ولكن من المؤكد أنها تخلو من الفيروسات والبرامج الخبيثة.
- هل يتوفر تحميل البرنامج من موقع شركة البرامج أم يمكن شرائه من المحال المعروفة ببيع مستلزمات الحاسب الآلي أم تحميله من أحد الروابط العشوائية أو مواقع مشاركة الملفات؟ تحميل التطبيقات أو البرامج من الموقع الأصلي للشركة التي تصدره أكثر أماناً من تحميله من مواقع مجهولة. والأفضل تحميل أو شراء التطبيقات والبرامج من منافذ البيع المسموح لها من قبل الشركات المنتجة وليس من أي مواقع مجهولة أو روابط مرسلة لك من مجهولين لزعمها أنك ستحصل على البرنامج مجاناً أو بسعر مخفض. فإذا كنت تعلم أن البرنامج الذي تحتاجه يساوي قدر محدد من المال، فكيف يعرضه أحد للبيع مجاناً أو بسعر زهيد؟ كما أن استخدام مواقع مشاركة الملفات يعد أمراً فيه مجازفة إذ أنك لا تدري، ربما يكون قد وُضِع أحد البرامج الخبيثة بدلاً من البرنامج الذي تريد تحميله. فهناك العديد من البرامج الخبيثة التي تبدو تماماً مثل البرامج الآمنة حتى أنها قد تخدع برامج مكافحة الفيروسات والبرامج الخبيثة. لذلك، فمن الأفضل تحميل البرامج من موقع الشركة الأصلي.



- عدد الذين إستخدموا البرنامج ولم يواجهوا أي مشاكل. إذا كان عددهم لا يتجاوز مئات معدودة من الاشخاص، فمن الأفضل عدم تحميله لكي لا تجعل من نفسك فأر تجارب لما قد يحدث، إذ من الممكن أن يكون برنامج غير موثوق أو غير آمن. حاول معرفة آراء وتعليقات مستخدمي البرنامج، إذا ما كان يُظْهِر أي نوافذ منبثقة أو يتعطل أو هل ينجز البرنامج بما تدعيه الشركة المنتجة من مهام ووظائف ؟ فإذا كانت استطلاعات الرأي سلبية، فالأفضل عدم استخدام هذا النوع من البرامج.

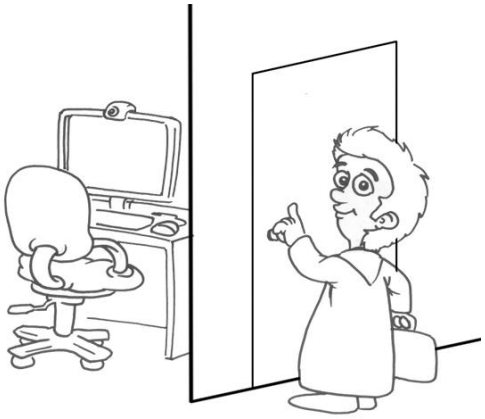
الدرس الثالث	إدارة الإختراق الأمني

تعريفات

حوادث الإختراق الأمني Security Incidents –محاولة لإنتهاك القوانين والسياسات الأمنية المتعلقة بالمعلومات و إستخدام اجهزة الحاسب الآلي.

الإختراق - Compromise: الدخول غير المسموح به - إختراق - لجهاز الحاسب الآلي أو للشبكة وقد يؤدي إلى الإطلاع على المعلومات الخاصة أو سرقتها أو استخدامها بشكل خاطئ.

حوادث إختراق الحماية



حوادث إختراق الحماية الأمنية تشمل العديد من الممارسات مثل:

- البرامج الخبيثة كالفيروسات والبوتنت.
- سرقة الهوية.
- الإحتيال.
- سرقة المعلومات الخاصة (أفكار وتصميمات لمنتج جديد).
- الدخول غير المسموح على الحاسب الآلي أو الحساب الإلكتروني لأحد المواقع.

نحاول دائماً تجنب حدوث مثل هذه الممارسات غير أنه لا ضمان من حدوثها، لأن أجهزة الحاسب الآلي المتصلة بالإنترنت معرضة لأي تهديدات. وقد تتعرض لإختراقات معقدة تعجز الخطوات التقليدية للحماية من صدها. كما أن المخترقين الماهرين دائماً ما يجدون طرقهم الخاصة لإختراق الحواسب الآلية حتى مع الحرص الشديد. وخطأ صغيرا غير مقصود، قد يعرض أجهزتنا للإختراق والتخريب.

كيف تتصرف في هذه المواقف؟

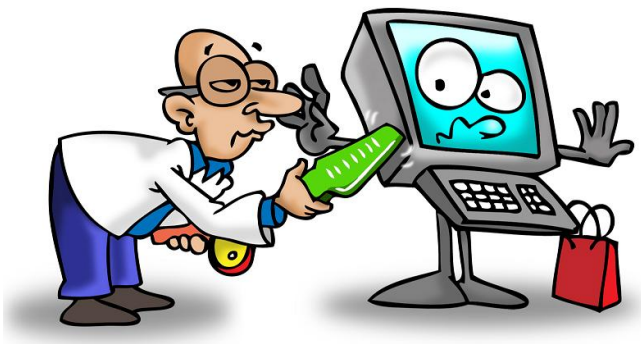
الأمر المهم هو اكتشاف متى تم التعرض للإختراق.

اكتشف حوادث الإختراق الأمني

أهم شئ يمكن فعله لحماية نفسك هو اكتشاف حوادث الإختراق سريعاً. واستناداً لعدة دراسات، فإن معظم حوادث الإختراق لا يتم إكتشافها إلا بعد شهور من حدوثها، حتى أن من يكتشفها عادة، لا يكون ضحية هذا الإختراق.

اتبع الإقتراحات الآتية لتساعدك على كشف حوادث الإختراق مبكراً...

1. قم بمراجعة حسابك البنكي بشكل مستمر لأنه من المهم اكتشاف عمليات الإحتيال مبكراً. ابحث عن عمليات شراء أو سحب لم تفعلها واحتفظ بتواريخ العمليات التي أجريتها على حسابك حتى يسهل عليك اكتشاف أي عمليات احتيال في حال تمت. فإذا حدث، عليك الإتصال فوراً بالمصرف لإتخاذ الإجراءات اللازمة.
2. راجع الفواتير وكشوف الحساب التي تصلك. اتصل فوراً بالشركة إذا وصلتك فواتير بما لم تشتر أو تستخدم. إذا تأكدت من أي محاولات إحتيال، عليك إبلاغ الجهات المعنية لإتخاذ الإجراءات اللازمة.
3. افحص حاسبك الآلي جيداً وتأكد من خلوه من أي ممارسات غير طبيعية. لن تكون هذه مهمة سهلة، حيث أن بعض الممارسات صعب كشفها. ولكن إليك بعض الدلالات التي قد تقودك أثناء البحث:
   أ. ينبهك برنامج مكافحة الفيروسات بإصابة حاسبك الآلي. انتبه لتلك الرسائل واتبع الإرشادات التي تظهر لك.
   ب. ظهور نوافذ منبثقة إعلانية أو تحذيرية من خلال متصفح الإنترنت الخاص بك والتي تستمر بإزعاجك طوال الوقت. هذه إشارة لإصابة متصفح الإنترنت بالبرامج الخبيثة.
   ج. قد يغلق الحاسب الآلي من تلقاء نفسه أو تعطُّل الجهاز بشكل مستمر. قد يتسبب في ذلك أحد البرامج الخبيثة التي تسبب تعطُّل الحاسب الآلي أو ربما تواجه مشكلة خطيرة بأحد البرامج التي تؤثر على أداء نظام التشغيل.
   د. قد تعمل التطبيقات والبرامج بشكل غير طبيعي. ولكن قد تظهر لك نوافذ لم ترها من قبل أو يتغير الشكل التقليدي لنوافذ ادخال بيانات حساب المستخدم أو قد يعمل الحاسب الآلي بشكل مختلف عن المعتاد.
   ه. قد يعمل حاسبك الآلي بسرعة أبطأ بكثير من المعتاد. فإذا تم إختراق جهازك، فغالباً ما يتحكم المخترق بالجهاز عن بعد للقيام بهجمات إختراق أخرى مما يقلل سرعة أداء الحاسب



الآلي.

و. قد تومض المؤشرات الضوئية للشبكة باستمرار، حتى في حالة عدم استخدامك للحاسب الآلي. فمعظم أجهزة الحاسب الآلي تقوم بمهام بسيطة أثناء تركك للجهاز بدون العمل عليه، وهذه الأعمال البسيطة قد لا تتطلب استخدام الشبكة أو الإنترنت. فإن كنت متصلا بالإنترنت عن طريقة شبكة لاسلكية، فقد لا تنتبه لوجود خرق لجهازك أو من يستخدم الشبكة التي تتصل بها، ولكن إذا اشتبهت أنه قد تم إختراق جهازك فعليك إذاً التحقق من ذلك.

ز. قد يكون المؤشر الضوئي الخاص بالقرص الصلب مضاءً حتى وإن كان الحاسب الآلي لايعمل. وهذا يدل أن حاسبك الآلي يؤدي أشياء أكثر من مجرد أداءه الأشياء البسيطة، حين لا تعمل عليه. إلا إذا كنت قد فعَّلت ضبط برنامج النسخ الإحتياطي، أو تفعيل المسح التلقائي لبرنامج مكافحة الفيروسات، والذي ينجزه الحاسب الآلي تلقائياً، فليس من المعتاد أن ترى نشاطاً زائداً للقرص الصلب.

ح. تصلك رسائل من حساب البريد الإلكتروني الخاص بك، أو قد يخبرك أحد أصدقائك أنه تلقى رسالة إلكترونية من بريدك الإلكتروني والتي تبدو مثل رسائل البريد المزعج. وهذا أيضاً يدل أن حساب بريدك الإلكتروني قد تعرض للإختراق.

التصرف الملائم

هناك ثلاث خطوات هامة للتصرف تجاه عمليات الإختراق:

1. **انتظر لحظة!** هناك بعض الأشخاص الذين يتصرفون بشكل مرتبك عند اكتشاف تعرضهم للإختراق، والبعض لا يفعلون شيئاً تجاه المشكلة، ظناً منهم أنها ستنتهي يوماً ما. ولكن من الأفضل أن نتحقق من أي أمر قد لا يبدو صحيحاً، مثل عملية سحب لم تقم بها من حسابك البنكي أو أن شيئاً غريباً قد حدث لجهاز الحاسب الآلي الخاص بك. لا تتسرع و تفترض دائماً أنها عملية إختراق، لأنه ببساطة من الممكن أن يكون تحديثاً جديداً أو مشكلة صغيرة في أحد البرامج. ولكن التحري مهم.

2. **قم بالإبلاغ!** قد تجد عمليات سحب مصرفية تمت على حسابك البنكي لم تجرها أنت، أو تشاهد برامج لم تقم بتحميلها أو تثبيتها على جهازك. اخبر ولي أمرك ليساعدك. ومن الأفضل الإستعانة بفني صيانة أجهزة الحاسب الآلي إذا وجدت فيروسات أو برامج خبيثة على جهازك، وإذا اكتشفت أي تلاعب بحسابك البنكي فأبلغ البنك فوراً.

3. **سجل الوقائع!** هذه خطوة غاية في الأهمية وعادة ما ننساها. سجل أي حادثة أو أمر مريب وكيف تعاملت معه، ليكون مرجع لك في المستقبل. سجل من استعنت بهم لحل مشكلتك.

إذا تأكدت من وجود برامج خبيثة أو حدوث ممارسات غريبة على حاسبك الآلي وتأكدت من وجود إختراق، قم بفصله عن شبكة الإنترنت أو أي شبكة متصل بها جهازك. فإذا كانت طريقة اتصالك بالشبكة باستخدام الأسلاك، إنزع الأسلاك وإن كان عن طريق اللاسلكي، افصل جهاز استقبال اللاسلكي من جهازك. سجّل الواقعة وتفاصيلها، مثل وقت اكتشافها وما الدلائل التي ساعدتك على اكتشاف اختراق الحاسب الآلي.

إن كان هذا الجهاز هو حاسبك الشخصي، يمكنك إجراء مسح شامل باستخدام برنامج مكافحة الفيروسات والبرامج الخبيثة. فإذا كان الحاسب خالياً من أي فيروسات أو برامج خبيثة فربما من الأفضل استشارة والديك. وهناك مؤسسات وطنية مثل aeCERT، حتما يمكنها مساعدتك.

كيفية إدارة الإختراق الأمني

اقرأ الوقائع الآتية، واذكر كيفية التصرف تجاه كل منها.

1. أثناء العمل على الحاسب الآلي تصلك رسالة متكررة تذكر وجود خطأ ما، مع ملاحظتك البطء الشديد لسرعة الجهاز في إنجاز المهام. ولإشتباهك بوجود فيروسات أو برامج خبيثة وقلة خبرتك في تلك الأمور تعتقد أنه من الأفضل الإستعانة بخبير. اشرح كيف ستتعامل مع الوضع وأهمية كل خطوة.
2. جاءتك رسالة بريد إلكتروني تذكر أن لديك مشكلة بحسابك الإلكتروني البنكي. الرسالة تبدو مرسلة من قبل البنك وتطلب منك الرسالة الضغط على رابط مرفق بالرسالة لتسجيل الدخول على حسابك للتعامل مع المشكلة.
   a. ماذا ستفعل؟
   b. ما هو هدف تلك الرسالة؟
   c. كيف تتأكد أن حسابك البنكي في أمان؟
3. إذا أصيب الحاسب الآلي الخاص بك بالبرامج الخبيثة، هل يعني ذلك أنك فعلت شيئاً خاطئاً؟
4. ما هي المؤسسة المسؤولة عن أمر الأمن المعلوماتي على شبكة الإنترنت في الإمارات العربية المتحدة؟
5. ما هي الخدمات التي تقدمها؟
6. ما هي المؤسسة التي يجب إبلاغها في الإمارات العربية المتحدة إذا كنت أحد ضحايا الجرائم الإلكترونية؟

الدرس الرابع	كيفية التخلص من البيانات

تعريفات

سرقة الهوية Identity Theft– استخدام بيانات شخص ما لأغراض غير شرعية كسرقة المال أو الحصول على خدمات بغير وجه حق.

الإحتيال Fraud or Scam – هو نوع من الخداع أو تزييف الحقائق لإقناع شخص ما بالتخلي عن شئ ذي قيمة.

التنقيب في المهملات Dumpster Diving – هي طريقة للبحث في الأشياء المهملة مثل الوثائق والملفات والوسائط أو أشياء أخرى قد تحتوي على معلومات خاصة أو شخصية.

أهمية التخلص الآمن من المعلومات

لدى كلٍ منا المعلومات الشخصية والخاصة التي يجب حمايتها. فكلمات المرور هي من المعلومات الخاصة التي لا ينبغي أن يعرفها أحد، لأنها تمكننا من الدخول إلى حساباتنا المختلفة مثل الحساب البنكي وشبكة التواصل الإجتماعي والبريد الإلكتروني . إذا أدخلت كلمة المرور الخاصة بك على ورقة ثم ألقيت بها في سلة المهملات لأنك لا تحتاجها مجدداً. هل هذا تصرف آمن؟

ماذا قد يفعل أي شخص حين يتفقد سلة المهملات؟

بمرور سنوات طويلة، تخصص بعض الناس في تفقد مهملات غيرهم في محاولة للعثور على معلومات قد تفيدهم. وفي الثمانينيات من القرن الماضي وجد بعض الأشخاص أوراق ومستندات لشركة اتصالات بها شفرات وكلمات مرور تخص نظم الاتصالات بالشركة وإستخدموا تلك المعلومات للحصول على مكالمات هاتفية مجانية. وبمرور الزمن كان هناك دائماً من يهتم بمهملات الشركات بحثاً عن بيانات مالية وكلمات مرور وخطط للأعمال وتصميمات سرية أخرى. إن قصاصة الورق تلك التي قمت بإلقائها في سلة المهملات، قد تكون إحدى المعلومات التي حصل عليها الذين يبحثون في المهملات. فهل كان هذا تصرفاً آمناً؟

أحياناً نحتفظ بالمعلومات الهامة في أماكن متفرقة، مثل القرص الصلب للحاسب الآلي. ماذا يحدث إذا تخلصت من جهازك أو قمت ببيعه؟ هل تخلصت من المعلومات الموجودة على القرص الصلب؟

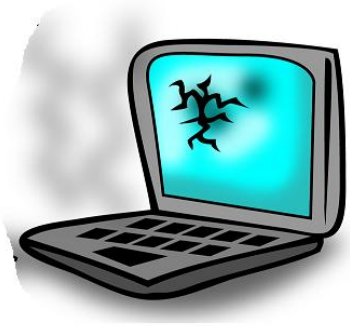
إستغنى جيش إحدى الدول الأجنبية عن بعض أجهزة الحاسب الآلي لديهم، ثم إشتراها أشخاص آخرون فوجدوا عليها كماً هائلاً من المعلومات السرية الخطيرة. تخيل نفس الموقف إذا إشترى أحدهم جهازك بعد أن تخلصت منه، ليجد عليه معلومات تخصك مثل بيانات حسابك البنكي وبيانات مالية ومعلومات وصور وملفات شخصية أخرى.

إذا حصل أي مجرم على بيانات حسابك البنكي أو كلمات المرور الخاصة بك أو أرقام بطاقة هويتك، أو أية ملفات أخرى، حتماً ستكون العواقب وخيمة. وينطبق الشئ ذاته على الشركة التي تعمل بها. فإذا فُقِدت أي معلومات مهمة تخص الشركة مثل خطط الأعمال ومعلومات مالية وما إلى ذلك، وحصلت عليها إحدى الشركات المنافسة، فقد يتسبب كل هذا في خسارة شركتك، مما قد يؤدي لفقد الكثير من موظفي الشركة لوظائفهم ويحتمل أن يكونوا مسئولين عن عائلاتهم. لذلك خسارة الشركات غالباً ما تدمر حياة من يعمل بها.

وحماية المعلومات بطريقة سليمة يتطلب حمايتها وقت انشائها واستخدامها والإنتهاء من العمل عليها. وتذكر أن تتخلص منها بشكل سليم حتى لا يتم سرقتها.

تحديد مكان المعلومات

قديماً، كانت أجهزة الحاسب الآلي تحتوي على وثائق وملفات قمنا بكتابتها أو قراءتها، بعضها بيانات حساسة وبعضها غير ذلك. ولكن حالياً تحتوي أجهزة الحاسب الآلي على صور خاصة وأفلام فيديو، وملفات شخصية وسجلات للمعاملات المالية وحساب الإدخار وغيرها من الملفات التي لا تحب أن يطلع عليها أحد.



تحديد المعلومات الحساسة هي واحدة من أهم الخطوات وهذا يتطلب معرفة المعلومات الحساسة أو الهامة. كلمات المرور وأرقام الحسابات البنكية والمعلومات المالية وعناوين المراسلات وأرقام بطاقة الهوية كلها معلومات حساسة، حتى الملفات التي تخص دراستك أو عملك هي أيضاً معلومات حساسة. ولكي تقيس مدى حساسية المعلومات التي تملكها، فكر إذا كنت لا تمانع نشر تلك المعلومات على إحدى شبكات التواصل. فإذا كنت تمانع، إذا هي معلومات خاصة وسرية وتندرج تحت مسمى المعلومات الحساسة.

فكر بجميع الأماكن التي تحتفظ فيها بأي معلومات! بالطبع على الحاسب الآلي ولكن ماذا بشأن الوثائق والمستندات الورقية مثل الفاكسات والمطبوعات والمراسلات؟

وماذا بشأن هاتفك الجوال؟ إذ يمكنك استخدامه لإلتقاط الصور الخاصة ، ولاستقبال رسائل البريد الإلكتروني وإجراء بعض العمليات البنكية، إلى جانب حفظ كلمات المرور الخاصة بك.

وماذا بشأن وحدات الذاكرة الفلاشية USB والأقراص المضغوطة CDs وأقراص الفيديو الرقمية DVDs والأقراص الصلبة والأقراص الصلبة المحمولة. هذه كلها وسائط مختلفة لتخزين المعلومات.

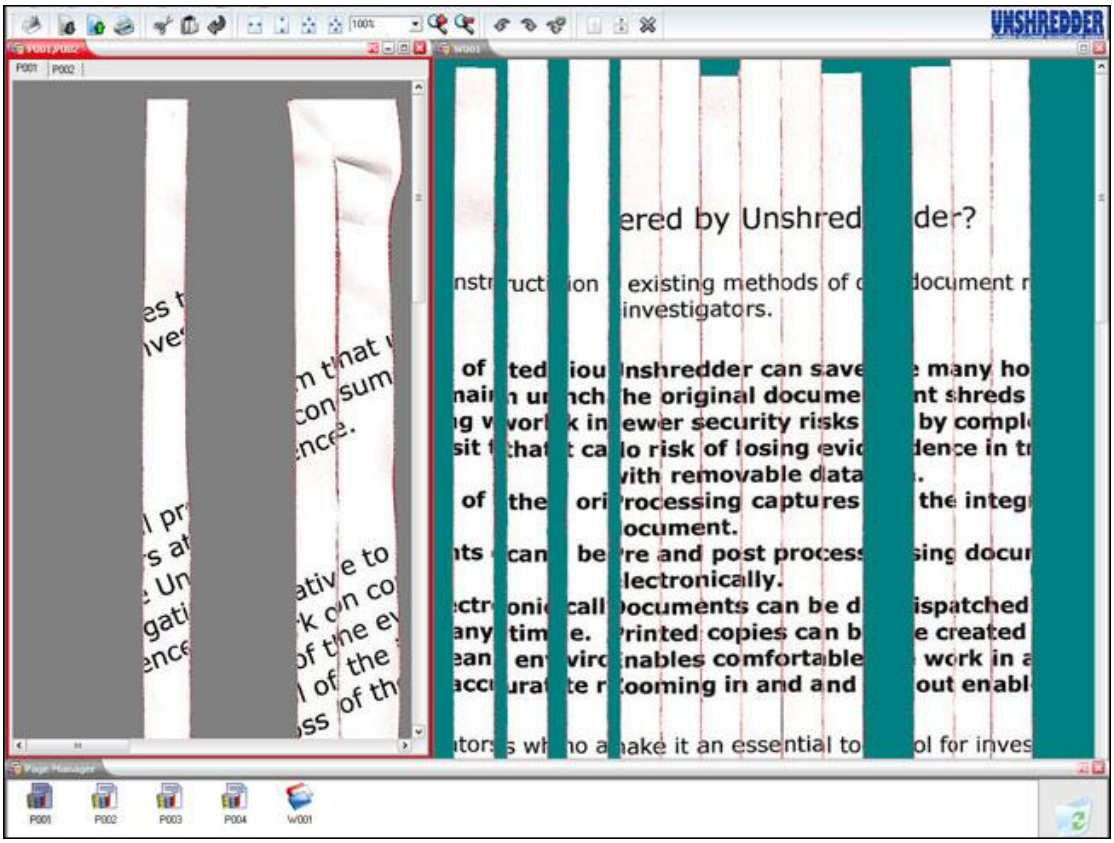
التخلص الآمن من المعلومات

التخلص السليم من الوسائط التي تحتوي على معلومات خاصة أو شخصية ليس بإلقائها في سلة المهملات فحسب، ولكن يجب التأكد أن تلك المعلومات لن يتم استرجاعها. إذا قمت بإلقاء كتب أو ملفات في سلة المهملات، قد يبحث غيرك في المهملات ويجدها وهذه العملية تسمى "التنقيب في المهملات". فمن يبحث عن أي معلومات لا يبالي بحجم المهملات التي يجب أن يبحث فيها عما يرغب.

تعلم كيفية التخلص من الأشياء التي تحتوي على المعلومات الخاصة أو الهامة لتمنع غيرك من العثور عليها وإستغلالها.

الوثائق الورقية

أسهل طريقة للتخلص الصحيح من الوثائق الورقية هي التقطيع. احرص على استخدام ماكينة تقطيع الورق التي تقطعه لقطع صغيرة جدا بعرض 5 ملم او أقل ، كما هو مبين في الصورة التالية...



ملفات الحاسب الآلي

أثناء استخدامنا للحاسب الآلي، فإننا نخزن عليه كما هائلا من المعلومات التي يكون أغلبها خاص أو شخصي والتي تكون مخزنة بشكل ملفات على القرص الصلب في الجهاز. وهناك العديد من الطرق للتخلص من تلك المعلومات بشكل يجعلها غير قابل للاسترداد.

حذف محتويات القرص

إذا أردت الإستغناء عن الحاسب الآلي الخاص بك بأي شكل، من الأفضل حذف محتويات القرص الصلب. هناك العديد من البرامج المجانية التي تقوم بحذف محتويات القرص الصلب عن طريق كتابة مجموعة من الآحاد والأصفار (0 و 1) على القرص الصلب بنمط معين. ولا تستعجل الأمر، فعادة ما تأخذ هذه العملية بعض الوقت.

التحطيم

هناك بعض الشركات التي تمتلك ماكينات مخصصة لكسر أو ثني الأقراص الصلبة بحيث تجعلها غير صالحة للعمل مرة أخرى. يمكنك الإستعانة بتلك الشركات للتخلص من قرصك الصلب حيث لن يتمكن أحد من استرجاع المعلومات الموجودة عليه إلا إذا كان مهندساً خبيراً. ولكن لعامة الناس أو اللصوص فسيكون ذلك في غاية الصعوبة.

التقطيع

يمكن تقطيع القرص الصلب لقطع صغيرة. وهناك بعض الشركات التي بها الماكينات المخصصة لذلك الغرض. هذه الطريقة فعالة جداً لأنه يستحيل استرجاع أي بيانات من القرص بعد تقطيعه. ويمكن استخدام تلك الطريقة للتخلص من أي أجهزة أخرى.

الهواتف الجوالة

الهواتف الجوالة هي عبارة عن أجهزة حاسب آلي صغيرة ، تحتوي على المعلومات التي خزنتها. ماذا لو فكرت في بيع هاتفك أو التخلص منه؟ كثير من الهواتف الجوالة بها خيار يسمى "محو الهاتف" الذي يمحو جميع البيانات من الهاتف. ولكن هذا إجراء بسيط للمستخدمين العاديين ولكن هناك بعض الهواتف التي تحتفظ

بأجزاء بسيطة من المعلومات التي يمكن استرجاعها. ولكن إذا أردت التأكد من عدم استرجاع تلك البيانات نهائياً، فعليك بتدمير الهاتف!

ما لا تحتاجه... لا تحتفظ به...

إن أبسط طريقة للتأكد من التخلص السليم من أي معلومات هو بمجرد عدم إحتياجها مرة أخرى. فعلى سبيل المثال، إذا قمت بطباعة أي أوراق بها معلومات عن الحساب البنكي أو لديك بطاقة إئتمان قديمة ولم تعد تحتاجها فقم بتقطيعها. لا تبقي أي معلومات لم تعد تحتاجها حتى لا يتم سرقتها من قبل لصوص الهويات في وقت ما.

التخلص من المعلومات بالمنزل	

قم بعمل بحث على الإنترنت عن الإرشادات الخاصة بالتخلص الآمن لأي وسيط أو مادة قد يحتوي على معلومات.

1. ما هي الإرشادات التي وجدتها؟ إذكر عنوان الموقع واسم كاتبها.
2. هل تحتوي أمثلة سهلة لشرح كيفية التخلص الآمن من الوسائط المختلفة التي تحمل عليها معلومات؟
3. اذكر مثالاً لفت انتباهك عن كيفية التخلص من وسائط الحفظ؟
4. لو أنك كتبت معلومة ذات حساسية على قطعة ورقة، مثل بيانات عن حسابك البنكي. ماذا ستفعل للتخلص من هذه الورقة؟
5. اختر واحدة من تلك المعايير واكتب بجانب كل نوع من وسائل الحفظ كيفية التخلص الآمن منها. على سبيل المثال، إذا قررت التخلص من الحاسب الآلي الخاص بك بسبب تعطله أو نيتك في شراء جهاز جديد. كيف ستتخلص منه؟

نصائح سريعة

- اجعل حماية المعلومات عادتك اليومية.
- اتبع قوانين الحماية والأمان، فهي لحمايتك وحماية من حولك.
- حافظ على المفاتيح الخاصة بمنزلك وسيارتك ولا تتركها لأي شخص ليس أهلاً للثقة.
- احفظ حاسبك الآلي وهاتفك المحمول في مكان آمن ولا تتركهم بدون انتباه أو في السيارة.
- ابق حاسبك الآلي بعيداً عن الحر أو البرد الشديد وبعيداً عن أي سوائل.
- فكر جيداً قبل تحميل وتثبيت أي برنامج على الحاسب الآلي الخاص بك. لابد أن يكون من مصدر معروف وموثوق به.
- إنتبه لأي دلالات قد تشير لوجود أي نشاطات غير عادية أو محاولات إحتيال. تفقد بصورة دورية كشوف الحساب البنكي وسجلات برنامج مكافحة الفيروسات وأي ممارسات غريبة على الحاسب الآلي.
- تصرف بشكل ملائم عند حدوث أي إختراق أمني ولا تتصرف بشكل مبالغ فيه.
- تخلص من وسائل حفظ المعلومات الخاصة والشخصية بعد الإنتهاء من استخدامها.
- تعرف على كيفية التخلص الآمن من وسائل حفظ المعلومات.

إختبر معلوماتك	

1. أي من التالي يعتبر من العادات الحسنة عند استخدام أجهزة الحاسب الآلي أو الهواتف المحمولة أو الإنترنت؟ ضع إشارة (✓) أمام العبارة التي تعبر عن العادة الحسنة .
   أ. ( ) تعرف على الأشياء التي يجب حمايتها.
   ب. ( ) احمِ جميع أجهزتك من الضرر.
   ج. ( ) تعرف على الهندسة الإجتماعية وحاول تجنبها.
   د. ( ) شارك كلمة المرور مع الآخرين.
   ه. ( ) تخلص من المستندات القديمة والحاسب الآلي وأي أجهزة بشكل ملائم.
2. ما هو المصطلح المقصود به – القوانين التي تسنها الشركة والتي يجب على موظفيها اتباعها؟
3. أي من الطرق الآتية: يعد مهماً لحماية أجهزة الحاسب الآلي والهواتف المحمولة؟ ضع إشارة (✓) أمام العبارة التي تعبر عن الطريقة المهمة
   أ. ( ) لا تترك الحاسب الآلي المحمول أو الهاتف المحمول بدون انتباه خاصة في الأماكن العامة.
   ب. ( ) ابقِ حاسبك الآلي وهاتفك المحمول في مكان آمن في حالة عدم استخدامهما.
   ج. ( ) لا تترك أجهزة الحاسب الآلي والهواتف المحمولة في أماكن شديدة الحرارة.
   د. ( ) نظف الحاسب الآلي بالماء والصابون ليبقى نظيفاً.
   ه. ( ) لا تعطي فرصة لأحد أن يتبعك عند القيام بفتح أي أبواب مغلقة.
4. ما الأشياء المفيدة التي يجب وضعها بالإعتبار أثناء شراء أو تحميل أي برنامج إلكتروني؟ اختر جميع الإجابات الصحيحة.
   أ. ( )تحميل أو شراء البرامج من شركات ذات سمعة طيبة.
   ب. ( )يمكنك شراء أو تحميل البرنامج من الموقع الخاص بالشركة أو أحد المحال المسموح لها ببيع تلك البرامج.
   ج. ( )إستخدم الكثير هذا البرنامج ويوصون به.
   د. ( )وجدته على أحد مواقع مشاركة الملفات.
   ه. ( )نسخة مجانية لبرنامج غالي الثمن.

5. ما هي الاحراءات التي يمكن فعلها لمساعدتك على الكشف المبكر لحوادث الإختراق الأمني؟ اختر جميع الإجابات الصحيحة.
   أ. ( )راجع حسابك البنكي بشكل مستمر لكشف أي عمليات مصرفية لم تقم بها.
   ب. ( )راقب باستمرار وجود أي أنشطة غير عادية على الحاسب الآلي.
   ج. ( )انتبه لتحذيرات برنامج مكافحة الفيروسات.
   د. ( )الحاسب الآلي يغلق من تلقاء نفسه بإستمرار.
6. اذكر الخطوات الثلاث التي يجب اتباعها عند اكتشافك أي نشاطات مثيرة للشك على الحاسب الآلي.
   أ.
   ب.
   ج.
7. وضح بإسلوبك أهمية التخلص من أي وسيط يحتوي على معلومات شخصية أو خاصة.
8. ما المقصود بالتنقيب في المهملات dumpster diving؟
9. قد تحتوي الوسائط التالية على معلومات شخصية أو خاصة. وضح كيفية التخلص السليم لكل منها.
   أ. الأوراق
   ب. حاسب آلي يحتوي على قرص صلب
   ج. هاتف محمول