وزارة التربية والتعليم

9

أمن وحماية المعلومات

كتاب الطالب

الصف التاسع

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 العديد من المعلومات والتدريبات التي تشمل موضوعات عن البريد المزعج والتصيد وكيفية إنشاء حسابات المستخدمين وبرامج مكافحة الفيروسات والتطبيقات المزيفة والطرق المناسبة للتخلص من الملفات التي بها معلومات خاصة و حساسة. وستناقش الدروس كذلك الأخطار المصاحبة لهذه الموضوعات وكيفية حماية نفسك و بياناتك من هذه الأخطار. حينما تتعلم كيفية حماية نفسك ستتمكن من استخدام جهاز الحاسب الآلي والإنترنت بشكل آمن.

المخرجات

بنهاية العام سيكون الطالب قادراً على :

- طرق التعرف على البريد المزعج وكيفية منعه.
- التعرف على التصيد وطرق تجنبه.
- مناقشة أهمية التحكم في صلاحيات الآخرين للوصول الى المعلومات الهامة.
- التمييز بين برامج مكافحة الفيروسات الحقيقية والمزيفة.
- التعرف على الطرق السليمة للتخلص من المواد أو الأجهزة التي تحتوي على بيانات شخصية أو معلومات خاصة.

المحتوى

الدرس الاول	إيقاف البريد المزعج ومحاربة التصيد

تعريفات

البريد المزعج Spam– هي رسائل تصل إلى صندوق بريدك الإلكتروني بدون إذنك وعادة ما يتم ارسالها لعدد كبير من الناس.

مصفي البريد المزعج Spam Filter – هو برنامج يفحص رسائل البريد الإلكتروني ليميز بين الرسائل المرغوب بها والغير مرغوب بها.

عنوان IP IP Address – هو المُعرِف أو العنوان الرقمي الذي يوضح موقع معين على أي شبكة أو على الإنترنت. ويستخدم الIP من قبل أجهزة الحاسب الآلي لتتمكن من التواصل مع بعضها من خلال شبكة الإنترنت.

اسم النطاق Domain Name – مجموعة من الحروف والأرقام وهو الاسم المصاحب لأجهزة الحاسب الآلي على شبكة الإنترنت IP Addresses وتستعمل لتسهيل التعرف على أجهزة الحواسيب الأخرى للتواصل معها.

التصيد Phishing – استخدام البريد الإلكتروني أو أي وسيلة تواصل، لإقناع الآخرين بالإفصاح عن البيانات الشخصية أو المعلومات الخاصة.

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

المهندس الإجتماعي Social Engineer – هو الشخص الذي يقوم بتجميع المعلومات وسرقة ملفات الآخرين أو التمكن من اختراق الحسابات السرية بعد استغلال أصحابها.

المعلومات الشخصية Personal Information – هي أي معلومات يمكن استخدامها للتعرف على هوية أي شخص مثل الاسم أو رقم الهوية الشخصية أو الصفات الجسدية أو العنوان أو تاريخ ومحل الميلاد.

المعلومات الخاصة Private Information– هي أي معلومات لا يرغب صاحبها في الإفصاح عنها لأحد وتتضمن الأسرار والعلاقات الشخصية والأحوال المادية وما إلى ذلك.

تعريف البريد المزعج

هي رسائل تصل إلى بريدك الإلكتروني بدون إذنك ، وتسمى أيضاً "البريد غير المرغوب به". وعادة ما يحتوي على إعلانات لشراء منتجات أو لزيارة مواقع إلكترونية بذاتها.

عادة من يقوم بإرسال البريد المزعج لأعداد كبيرة من الناس لأنه يجد أن ذلك غير مكلف وإجراءاته بسيطة. إن ارسال النشرات الإعلانية عبر البريد العادي أو الإعلان في الصحف يكلف الكثير من المال ولكن ارسال الملايين من الرسائل عبر البريد الإلكتروني لا يكاد يكلف شيئاً، وكل ما يتطلبه الأمر هو أن يقوم المستخدمون بفتح الرسائل ومطالعة العروض الترويجية ثم شراء ما يعجبهم، وبذلك يكسب المرسل الكثير من المال.

مشكلة البريد المزعج أنه منتشر بكثرة. وبناءاً على نتائج البحث الذي قامت به شركة كاسبرسكي Kaspersky لبرامج تأمين أجهزة الحاسبات الآلية، أن 70% من رسائل البريد الإلكتروني المرسلة عبر شبكة الإنترنت هي من نوع البريد المزعج.

وقد تبدو رسائل البريد المزعج غير مؤذية ولكنها قد تملىء بريدك الإلكتروني فيتعذر عليك إيجاد الرسائل المهمة من أصدقائك أو أفراد عائلتك. وقد يتسبب في إبطاء سرعة جهازك بسبب كثرة الرسائل التي يتعين على جهازك فتحها وحفظها. في حين أن بعض الرسائل، ماهي الا مجرد إزعاج ، ولكن البعض منها قد يسبب لك المشاكل. فقد تحتوي على برامج أو روابط لمواقع خبيثة وقد يكون بعضها محاولات للهندسة الإجتماعية لاستخلاص بيانات أو معلومات خاصة بك.

وعلى الرغم من أهمية تدقيق المستخدمين لتمييز البريد المزعج وحسن التصرف تجاهه، فإنه وبمساعدة مصفي البريد المزعج Spam Filter لن تصل معظم هذه الرسائل المزعجة للمستخدمين.

يقوم مرشح البريد المزعج بتفقد الرسائل في بريدك الإلكتروني ومحاولة التمييز بين البريد المزعج والبريد غير المزعج. تعمل بعض مصفيات البريد المزعج على مزود البريد الإلكتروني الذي يقوم بتخزين الرسائل الإلكترونية قبل قراءتها، وبعضها تعمل على جهاز الحاسب الآلي وعندما تقوم بتحميل أو قراءة رسائلك الإلكترونية فإنه يقوم بفحصها. وهناك تقنيات مختلفة لتصفية البريد المزعج، ولكل تقنية طريقتها و مميزاتها .

القوائم السوداء والقوائم البيضاء

القوائم السوداء هي قوائم معدة سلفاً تحتوى على عشرات الآلاف من العناوين لمنع المواقع أو العناوين الإلكترونية من الوصول للبريد الإلكتروني إذا صُنفت على أنها بريد مزعج. وتضم القوائم السوداء العديد من قوائم عناوين البريد الإلكتروني والتعريفات الرقمية وأسماء النطاقات المعروفة بأنها ترسل البريد المزعج. يمكن إنشاء قائمة وإضافة العناوين من قبل المستخدمين الذين يتتبعون العناوين التي ترسل لهم البريد المزعج، وتسمى **قائمة المنع** وتستخدم هذه القائمة من قبل مصفي البريد المزعج لمنع العناوين الموجودة بها من وصول رسائلها المزعجة الى جهاز المستخدم.

أما **القوائم البيضاء** فهي عكس القوائم السوداء، و تضم عناوين البريد الإلكتروني للمصادر الموثوق بها. وتضم كذلك العناوين والتعريفات الرقمية وأسماء النطاقات الآمنة. ومن خلال هذه القوائم سيسمح المرشح الإلكتروني للعناوين الموجودة بها فقط من وصول رسائلها الى جهاز المستخدم.

ويتطلب التعامل بهذه التقنية لمرشح البريد المزعج، التحديث المستمر للقوائم البيضاء والسوداء. وإذا لم يتم تحديث القائمة أو تم تمييز أحد العناوين أو التعريفات الرقمية أو أسماء النطاقات على أنه بريد مزعج بشكل خاطئ، فقد يتم منع بريد آمن من الوصول. وهناك تحدي آخر وهو أن الأشخاص الذين يقومون بإرسال البريد المزعج يغيرون الأنظمة باستمرار ويجعلون البرامج الخبيثة تسيطر على أنظمة أخرى لا توجد على القوائم السوداء للاستمرار بارسال البريد المزعج دون توقف. وتعتبر هذه الطريقة الرئيسية لهجمات البرامج الخبيثة للإستيلاء على عناوين غير معروفة لإرسال البريد المزعج منها.

منع المحتوى

هذه وسيلة حديثة ومشهورة لمنع رسائل البريد المزعج من الوصول الى بريدنا، وذلك عن طريق التعرف على محتواها. سيتحقق مرشح البريد المزعج من محتوى الرسالة عن طريق البحث عن كلمات معينة توضح إذا ما كان يندرج تحت البريد المزعج. وهناك قوائم تتضمن الكلمات التي دائماً ما تستخدم في البريد المزعج ورسائل التصيد.

دائماً ما يحاول الأشخاص الذين يرسلون البريد المزعج التحايل على المرشحات بإستبدال الحروف بأرقام أو كتابة الكلمات المشهورة بصورة مختلفة بحيث يمكن للمستخدم التعرف عليها في حين يعجز عن ذلك مرشح البريد الإلكتروني.

كما أن المشكلة الأساسية في هذا النوع من المنع هو إحتمالية استخدام بعض الكلمات الموجودة في قوائم المنع في محتوى رسائل سليمة. فقد يحتاج الطبيب لذكر اسم دواء في رسالته الإلكترونية، وهذا الاسم يكون موجوداً في قائمة المنع. أو تُستخدم كلمات دارجة في رسائل الأعمال هي أصلاً تستخدم في رسائل الإحتيال والنصب. وهناك أيضاً إحتمالية إستخدام كلمة نصفها في قوائم المنع والنصف الآخر في الرسائل السليمة، فيتسبب ذلك في تصنيف الرسالة من البريد المزعج.

المصفي المتعلم

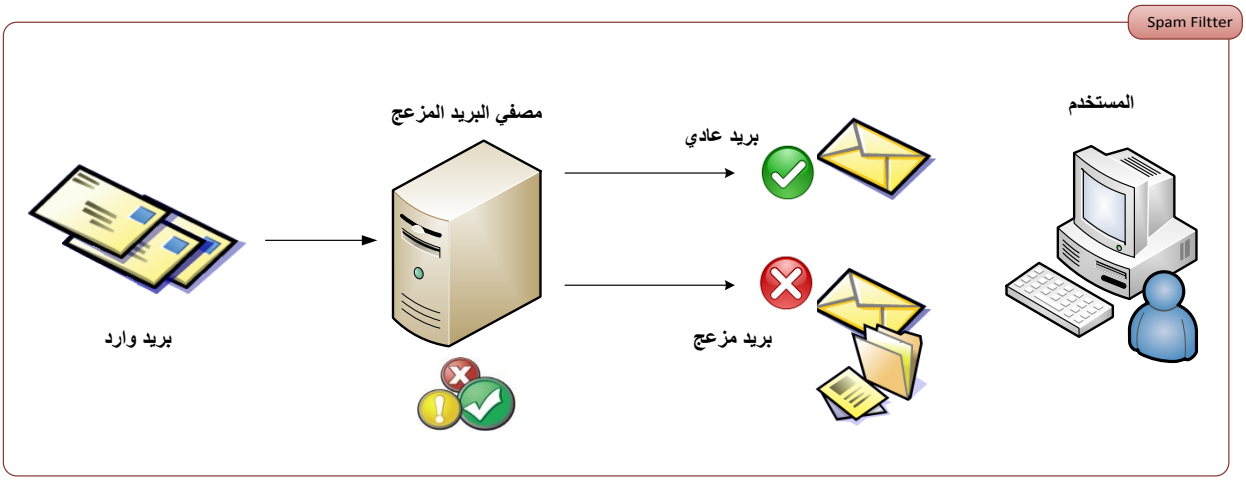
تعتبر هذه التقنية من أكثر الوسائل تعقيداً لترشيح المحتويات والبريد الإلكتروني، فهي تحتاج للتدريب و(التعلم)، لذلك تحتاج لجمع المعلومات عن محتويات البريد المزعج والسليم.

يتم تطبيق معادلة رياضية لتحديد سلامة أي كلمة ترد في رسائل البريد الإلكتروني. وكلما زاد حجم المعلومات الواردة لمرشح البريد الإلكتروني، كلما كانت النتائج أفضل. فعلى سبيل المثال، إذا استخدمت كلمة "نقداً" في 10 آلاف بريد إلكتروني في مؤسسة مالية أثناء فترة تدريب النظام، فإن المرشح يجب أن يعلم عدد المرات المسموح بها لاستخدام هذه الكلمة قبل اعتبارها ضمن قوائم المنع. فإذا كانت الإجابة 80% فلا يمكن إعتبارها من الكلمات الممنوعة لأنه من الواضح أنها تستخدم باستمرار في الرسائل الإلكترونية الخاصة بالمؤسسة. وقد تستخدم هذه العملية فيما يخص الأدوية أو الوصفات الطبية التي يستخدم فيها كلمات قد تبدو غير لائقة كما ترد في المراجع الطبية.

مكافحة البريد المزعج

من السهل حماية أنفسنا من البريد المزعج ومن أبسط طرق الحماية هي عدم إعطاء عنوان البريد الإلكتروني الخاص بك لأناس لا تعرفهم. فبعض المواقع الإلكترونية تطلب إدخال البريد الإلكتروني للتمكن من قراءة موضوع أو مشاهدة فيديو أو تنزيل ملف ما، فيتم استخدامه لإرسال رسائل البريد المزعج إليك، أو إعطائه لأشخاص آخرين يقومون بارسال البريد المزعج. وعليك توخي الحذر من كتابة بريدك الإلكتروني على مثل هذه المواقع. وبهذه الطريقة يمكنك تفادي وصول تلك الرسائل لبريدك الإلكتروني، فإن استمرت فقم بحذفها بطريقة يدوية.

هناك الكثير من أنظمة البريد الإلكتروني تحتوي على مصفي البريد المزعج بصورة تلقائية وتحتوي معظم برامج الحماية على أدوات تعمل على تصفية بريدك الألكتروني من البريد المزعج وترسلها لمجلد خاص بالبريد المزعج. ويمكن لهذه الأدوات مساعدتك على تقليل نسبة البريد المزعج ولكن قد تصنف بعض الرسائل التي تحتاجها ضمن البريد المزعج. لذلك يُنصح بمراجعة الرسائل المصنفة كبريد مزعج للتأكد من خلوها من الرسائل التي تحاجها.



Activity	**التعامل مع البريد المزعج**

مسألة البريد المزعج تعتبر من الأمور التي تشغل بال الكثير من الناس والشركات. خلال هذا النشاط سيقوم مدرسك بمناقشة عامة في الفصل بخصوص البريد المزعج. محاور النقاش ستكون الاسئلة التالية :

1. هل تسلمت أي رسائل بريد مزعج من قبل؟
2. ما موضوع أو ما العرض الذي قدمته لك مثل هذه الرسائل؟
3. ما الأسباب التي قد تدفع أي شخص لإرسال بريد مزعج؟
4. هل يحتوي جهازك على مصفي للبريد المزعج؟ هل تستخدمه ؟ اذكر الأسباب في إجابتك ؟
5. اذكر المشاكل التي قد يسببها مصفي البريد المزعج؟

مكافحة التصيد الالكتروني

التصيد الالكتروني

رسائل التصيد هي نوع من رسائل البريد الإلكتروني التي تحاول إقناعك بفعل شئ ما عادة لا تقوم به. فقد تغريك بتقديم مبلغاً كبيراً من المال أو حصولك على أحد برامج الحاسب الآلي بسعر زهيد، أو قد تزعم الرسالة أنه تم تجميد حساب التواصل الإجتماعي الخاص بك ويتحتم عليك الرد على الرسالة ذاكراً اسم المستخدم وكلمة المرور الخاص بحسابك. وقد يحتوي البريد الإلكتروني على رابط لموقع إلكتروني يطلب منك إدخال نفس البيانات السابقة، فمشكلة التصيد أنه دائماً ما تظهر رسائلها أنها مرسلة من جهة أو موقع رسمي ويطلب منك زيارة الموقع من خلال الضغط على الرابط المرفق بالرسالة وإدخال بياناتك الشخصية واسم المستخدم وكلمة المرور الخاصة بك.

وفي حقيقة الأمر فإن البريد الإلكتروني والموقع زائفين وقد صممما خصيصاً لتصيد الناس واستدراجهم لإدخال بياناتهم الخاصة مثل الاسم والعنوان ورقم الهاتف وكلمات المرور وأرقام الحسابات البنكية، ومن ثم يتم استخدام تلك المعلومات لسرقة حساب البريد الالكتروني أو حساب التواصل الإجتماعي أو سرقة الأموال من الحساب البنكي.

الشخص الذي يقوم بإرسال رسائل التصيد يفعل تماماً مثلما يفعل مرسل رسائل البريد المزعج. فكلاهما يرسل تلك الرسائل لأكبر عدد من الناس. وتسمى هذه العملية بالتصيد لأنها تماماً مثل الإصطياد في البحر، فالبحر ملئ بالعديد من الأسماك، ولكن لن تنجح عملية الصيد إلا إذا علقت بالسنارة إحدى تلك الأسماك.

يحتاج المتصيد ولو لشخص واحد فقط ليصدق رسالته ويقوم بارسال بياناته الخاصة، لذلك يرسل المتصيد أكبر عدد ممكن من رسائل البريد الإلكتروني.

يسهل عليك حماية نفسك من رسائل التصيد بالبريد الإلكتروني، ويتطلب ذلك تعلم كيفية التعرف على مثل تلك الرسائل والتفكير جيداً قبل الرد على أي بريد إلكتروني غريب مهما بدا مغريا وجاذبا.

التعرف على رسائل التصيد الإلكترونية وكيفية تجنبها

أول طريقة للحماية من رسائل التصيد الإلكترونية هي التعرف عليها. فاعلم أن هذه الرسائل هي محاولة للحصول على معلوماتك الخاصة مثل عنوانك وبيانات شخصية أخرى، أو معلومات عن حسابك البنكي أو كلمات المرور. لتنجح هذه المحاولات، لن تطلب رسائل التصيد أي من هذه البيانات أو المعلومات الشخصية بشكل مباشر، ولكن ستطلب منك هذه المعلومات، عن طريق الضغط على رابط لموقع معين ، تقوم بزيارته ربما لتحديث بياناتك أو إعادة تنشيط حسابك الخاص بشبكة التواصل الإجتماعي. ومن يستخدم هذه الطرق هو المهندس الإجتماعي الذي يعرف كيف يقنعك بأن رسائله شرعية فينجح في إستخراج بياناتك الشخصية ومعلوماتك الخاصة.

احذر العروض التي تبدو سخية أكثر من اللازم. قد تصلك رسالة بريد إلكتروني تزعم أنها من مؤسسة أو محامي أحد الأثرياء أو من شركة كبرى تمنحك مبلغ من المال كجائزة (اليانصيب). ولكي تصلك الجائزة أو الأموال عليك تزويدهم ببياناتك الشخصية. وفي بعض الحالات يطلب منك إرسال مبلغ صغير من المال لتستلم جائزتك أو إعطاء بيانات حسابك البنكي لتحويل المال إليه، ثم يتم سرقة أموالك ولا تردك أي رسائل منهم بعد ذلك.

لا تتسرع أو ترتبك. بعض رسائل التصيد ستجعلك تشعر بأهمية التصرف الفوري تجاهها. فقد تذكر تلك الرسائل أنه تم تجميد أو إغلاق حسابك البنكي أو حسابك على شبكة التواصل الإجتماعي ولا يمكن إعادة فتحه إلا بعد تأكيد بعض البيانات. يعلم المهندس الإجتماعي جيداً أنك ستقلق بشأن الوضع الملح أكثر من قلقك على خطورة كشف معلوماتك الخاصة، فهو يحرص على إثارة قلقك الذي في الغالب ينتج عنه قرارات خاطئة.

لا تجعل فضولك يسيطر عليك. بعض رسائل التصيد قد تثير فضولك بعرضها لسماع أحدث الأغنيات أو مشاهدة صور مثيرة أو رابط لمشاهدة فيديو مضحك أو عروض لبرامج غالية الثمن للحاسب الآلي ولكن بأسعار مخفضة، أو قد تحتوي تلك الرسائل على مرفقات لملفات تبدو مغرية ولكنها في حقيقة الأمر تحمل برامج خبيثة يتم تثبيتها على جهازك أو هاتفك النقال بمجرد تحميلك لها.

احذر من محاولات المجهولين لجذب ثقتك أو تعاطفك. قد تصلك بعض رسائل التصيد التي تحتوي على معلومات تخصك والتي تعتقد أن القليل ممن تعرفهم فقط لديهم فكرة عنها. وقد تروي الرسالة قصة تثير

تعاطفك أو شفقتك على صاحبها وهذا شعور طبيعي تجاه قصص المآسي مثل هذه. ولكن يجب عليك مقاومة إرسال بياناتك الشخصية التي قد يطلبها مضمون الرسالة ربما لمساعدة صاحب القصة بشكل أو بآخر.

لا ترسل أو تشارك بياناتك الشخصية عبر البريد الإلكتروني أو المراسلة الفورية. إذا وصلتك رسالة من مجهول يطلب منك بياناتك الشخصية، قم بحذفها فوراً. فإنه لا يحق لأي شخص لا تعرفه أن يطلع على أي معلومات تخصك مثل رقم هاتفك أو عنوانك أو أي معلومات تخص أفراد أسرتك ووالديك.

تجاهل أي روابط لمواقع إلكترونية أو مرفقات في أي بريد إلكتروني مرسل من مجهول. احذر المرفقات وروابط المواقع المرسلة لك من بعض الشركات أو المواقع الإلكترونية، فأنت لاتدري من قام بإرسالها، و أعلم أن المواقع والشركات الرسمية والبنوك لا يطلبون منك الإفصاح عن اسم المستخدم وكلمة المرور الخاصين بك أو الضغط على أية روابط غير موثوقة. فإذا وصلتك رسائل من هذا النوع، قم بالإتصال بالشركة أو البنك هاتفياً وإستفسر عن الموضوع أو تأكد من وجود الموضوع على موقعهم الرسمي الذي تعرفه. فإن كان هناك أي معوقات فحتماً سوف يقومون بإخبارك ومساعدتك على حلها.

قم بتفعيل مصفي البريد المزعج على في برنامج بريدك الألكتروني . سيساعدك مصفي البريد المزعج على منع معظم رسائل التصيد الإلكترونية من الوصول إليك. ورغم تشابه تلك الرسائل كثيراً، إلا أن مصفي البريد المزعج سيساعدك على التعرف عليها ومن ثم التخلص منها.

واجب منزلي

تفادي التصيد

قم بالبحث عن رسالة الكترونية وصلت لبريدك الالكتروني أو إبحث على الإنترنت عن قصة حقيقية للتصيد الألكتروني، ثم قم بالإجابة على الأسئلة التالية بناءاً على القصة التي قمت بإختيارها.

1. ما المصدر الذي ادعت رسالة التصيد أنها مرسلة منه (شركة – شخص – مكان)؟
2. في إعتقادك، ما الغرض من وراء رسالة التصيد هذه؟
3. ما الأسلوب الذي اتبعه مرسل الرسالة لإقناع المستلم بفعل ما يرغبه المرسل؟
4. بماذا تنصح مستلم الرسالة ؟ ما الذي يجب فعله؟

الحسابات الإلكترونية والصلاحيات	الدرس الثاني

تعريفات

حساب المستخدم (اسم المستخدم – هوية المستخدم) User Accounts– هو اسم يستخدمه أي شخص للتعريف بهويته لتسجيل الدخول لجهاز الحاسب الآلي أو للموقع الإلكتروني.

كشف الهوية Identification- إدعاء هوية المستخدم صاحب حساب معين على الأنظمة الإلكترونية.

إثبات الهوية Authentication – إثبات صحة الهوية .

السماح Authorization – منح الإذن والسماح لمستخدم معين للدخول بناءً على هويته.

صلاحية الدخول Permission/Access Rights – حقوق وصلاحيات وامتيازات تمنح لإنجاز مهام محددة. ومن أمثلة تلك الصلاحيات طريقة السماح للوصول إلى المعلومات للقيام بعمل ما.

كشف وإثبات الهوية لحسابات المستخدمين

الهوية شئ في غاية الأهمية لإثبات من تكون. وهوية إستخدام حاسبك الآلي لها أهميتها أيضاً، فهي الطريقة التي يتعرف بها الحاسب الآلي على هويتك وما المسموح لك بفعله. ويتم التعرف على هويتنا في الحاسب الآلي باستخدام اسم المستخدم أو هوية المستخدم. لذلك نقوم بإدخال اسم المستخدم لتعريف هويتنا للحاسب وتسمى هذه العملية "كشف الهوية". ثم يطلب الحاسب الآلي إثبات تلك الهوية فنقوم بإدخال كلمة المرور وتسمى هذه العملية "إثبات الهوية".

تنفذ هذه الخطوات أيضاً عند استخدام بطاقة الإئتمان البنكية. فعند استخدام البطاقة، نقوم بكشف الهوية ثم ندخل الرمز السري لإثبات الهوية والسماح باستخدام البطاقة. تتكرر نفس الخطوات عند استخدام حسابات البريد الإلكتروني والمراسلة الفورية وإستخدام شبكة التواصل الإجتماعي.

الإستخدام اليومي للترخيص

نستخدم الترخيص في حياتنا اليومية لحماية أنفسنا وبيوتنا وممتلكاتنا وذوينا. وسنتعلم فيما يلي أهمية الترخيص في استخدام الحاسب الآلي.

لتتمكن من دخول منزلك، عليك استخدام المفتاح الخاص به. حيازتك للمفتاح يعطيك الحق في دخول المنزل. فعندما أعطاك ولي أمرك المفتاح، فقد أجازا لك الدخول للمنزل وقت ما تشاء، إلى جانب أنه قد يعطي والديك المفتاح لآخرين مثل أحد أقربائك، وهذا أيضاً يجيز له الدخول في أي وقت. يمكنك أيضاً السماح لأصدقائك بدخول منزلك ولكن بدون إعطائهم المفاتيح، فعليهم طرق الباب لتسمح لهم بالدخول وفي أوقات محددة فقط وليس لهم الحق بالدخول الى الأماكن الخاصة بالمنزل. وإذا أردت استقبال شخصاً لا تعرفه جيداً، فيلزم لك أولاً الإستئذان من ولي أمرك لذلك، ولا يسمح له بالتجول في المنزل حيثما يشاء والقيام بالزيارة مثلما يفعل أصدقائك.

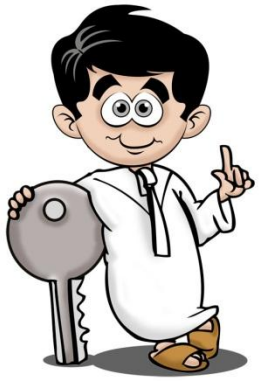
كل شخص في المثال السابق كان مسموحاً له، القيام بمهام معينة وكل شخص له امتيازات و صلاحيات مختلفة عن الآخر.

إسلوب الترخيص والسماح على الحاسب الآلي

الحاسب الآلي يعمل بنفس الفكرة، فإسم المستخدم وكلمة المرور يشكلان المفتاح لدخول المنزل. عندما تقوم بتسجيل الدخول لحاسبك الآلي فإنك تدخل اسم المستخدم الخاص بك (كشف الهوية) وكلمة المرور (إثبات الهوية)، فيسمح لك الحاسب الآلي بالقيام بأعمال محددة (مرخصة) ويسمح لك بفعل أي شئ بناءاً على المهام المسموح لحسابك على الحاسب الآلي القيام بها.

سيتم الكشف على حسابك ومقارنة الصلاحية والترخيص، ما إذا كان مسموحاً لك تحميل برامج جديدة أو الإطلاع على الملفات والمعلومات أو التغيير في إعدادات الحاسب الآلي أو نوعية البرامج المستخدمة.

ماذا لو أراد شخص آخر استخدام حاسبك الآلي؟ ماذا لو أراد أصدقائك زيارتك للعب معك على إحدى ألعاب الحاسب الآلي؟ هل ستسمح لهم باستخدام حساب المستخدم الخاص بك على جهازك الآلي؟ فكر جيداً – لأنك لو سمحت لهم بذلك، فيعني ذلك أنهم سيتمكنون من تفقد ملفاتك والمعلومات الخاصة أو ربما استخدام بريدك الإلكتروني أو حذف ملفاتك أو رؤية صورك الموجودة على الحاسب الآلي.



وعليه، فإنه من الأفضل أن تنشئ حسابا آخرا ليستخدمه أي شخص آخر، وذلك باستخدام حساب المستخدم الخاص بك، حيث يمكنك تحديد نوع الأشياء التي يمكن القيام بها على هذا الحساب، إلى جانب منع الإطلاع على ملفاتك الخاصة.

تحتوي أجهزة الحاسب الآلي على حسابات مستخدمين مختلفة. وبعض هذه الحسابات لها صلاحيات تختلف عن الأخرى، فمعظم أجهزة الحاسب الآلي يوجد عليها ما يسمى بحساب المدير والذي يستطيع القيام بأي شئ مثل تحميل وتثبيت البرامج والإطلاع على أي ملفات أو القيام بحذفها وتغيير إعدادات الجهاز. وهناك بعض أجهزة الحاسب الآلي حيث يكون حساب المدير محمي، ولكن بالإمكان إعطاء صلاحيات حساب المدير لحساب آخر.

مثال آخر للصلاحيات التي يمكن منحها على مواقع التواصل الإجتماعي مثل السماح لأشخاص محددين الإطلاع على بياناتك الخاصة والسماح لآخرين لرؤية صورك، وغيرهم بتفقد صفحتك. ولكن ينبغي أن تكون حذرا لما تقوم بنشره على مواقع التواصل الإجتماعية لأنك قد تعتقد أن كل ما تنشره لا يراه الآخرون.

حماية حساب المستخدم الخاص بك

كما رأينا في المثال، أن السماح لآخرين باستخدام حسابك قد يشكل تهديداً لك مثل حساب المدير على حاسبك الآلي.

يمكنك القيام ببعض الأشياء البسيطة التي تضمن حمايتك:

لا تعطي كلمة المرور الخاصة بك لأي شخص، فهذا يعطي الفرصة لأي شخص أن ينتحل شخصيتك واستخدام الصلاحيات المتاحة على حاسبك الشخصي بشكل خاطئ. الحاسب الآلي لا يفرق بينك وبين غيرك في الاستخدام طالما هذا المستخدم لديه بيانات المرور.

كن حذراً عند إعطاء صلاحيات الإستخدام للآخرين. إذا قمت بإنشاء حساب آخر على حاسبك الآلي ووفرت لذلك الحساب الصلاحيات لفعل أي شئ على الجهاز، وقتها سيتمكن من يستخدمه من الإطلاع على ملفاتك أو إحداث أي تغيرات لا تعجبك أو قد لا يكون حريصاً أثناء استخدام جهازك مثلما تفعل أنت.

	**حساب المدير**

قام أحد أصدقائك بزيارتك في المنزل للعمل معاً على مشروع مدرسي على الحاسب الآلي الخاص بك. ماذا ستفعل؟ هل ستسمح له باستخدام حساب المستخدم الخاص بك؟ وضح إجابتك ؟

قم بالبحث على الإنترنت عن كتب توضيحية تخص نظام التشغيل المستخدم على حاسبك الآلي. اقرأ ما يتعلق بحساب المدير واذكر ما الذي قد يفعله أي شخص يقوم باستخدام هذا الحساب على جهازك.

كيف سيؤثر ذلك عليك؟

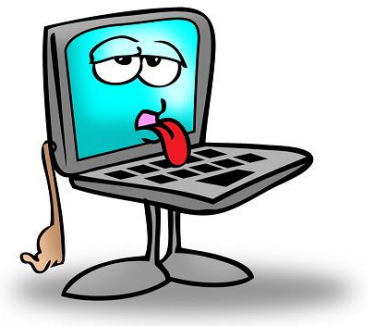
الدرس الثالث	برامج مكافحة الفيروسات الوهمية

تعريفات

النوافذ المنبثقة Pop-up window - هي نافذة من نوافذ متصفح الإنترنت التي تظهر بشكل مفاجئ وهذا يحدث عند زيارة موقع معين فيطلب من المتصفح أن يفتح نافذة جديدة.

البرامج الخبيثة Malicious Software (also called Malware)– هي برامج مصممة لتخريب جهاز الحاسب الآلي. وهناك أنواع كثيرة من البرامج الخبيثة مثل الفيروسات والديدان وبرامج التجسس وحصان طروادة والبوتنت وغيرها.

المواقع الخبيثة



تعد البرامج الخبيثة شيئا مقلقا بالنسبة لجميع مستخدمي أجهزة الحاسب الآلي، فهي قد تسبب بطء لأداء الجهاز وسرقة الملفات والمعلومات الخاصة أو تخريبه بالكامل. وهناك بعض البرامج الخبيثة التي يتم التحكم بها لتستخدم في مهاجمة أجهزة أخرى.

هذه بعض المشاكل المقلقة التي تسببها البرامج الخبيثة، ولهذا يقوم الكثير منا بتحميل وتثبيت برامج مكافحة الفيروسات والبرامج الخبيثة لمنع تلك البرامج من تخريب حاسباتنا الآلية.

برامج مكافحة الفيروسات الوهمية

لاحظ المهندسون الإجتماعيون القلق الذي يصيب المستخدمين إذا أحسوا بإصابة أجهزتهم بالبرامج الخبيثة والذي قد ينتج عنه قرارات متسرعة وغير صائبة. على سبيل المثال قد يظهر فجأة أحد النوافذ المنبثقة التي تذكر أن جهازك مصاب بأحد البرامج الخبيثة، وتطلب منك أن تتبع بعض التعليمات الموجودة بها، الأمر الذي قد يدفعك لإتباع تلك المعلومات دون تفكير في العواقب التي قد تحدث.

المهندسون الإجتماعيون على دراية تامة بتلك التصرفات، الأمر الذي يجعلهم ينشؤن النوافذ المنبثقة والمواقع التي تبدو رسمية ولكنها تحتوي على البرامج الخبيثة. فعندما تقوم بزيارة لمثل هذه المواقع، يقوم البرنامج الخبيث الموجود على الموقع بفتح نافذة منبثقة من متصفح الإنترنت لديك. وتظهر الصفحة المنبثقة محذرة أنه يوجد إحدى البرامج الخبيثة على جهازك وأنه يجب عليك اتباع بعض التعليمات لتحميل برنامج يقوم بالتخلص من تلك البرامج الخبيثة.

وفي حقيقة الأمر أن البرنامج الذي طلبت منك النافذة المنبثقة تحميله، هو في الأصل من البرامج الخبيثة، فيصاب جهازك في الحال عند تثبيته.

انظر كيف خدعك المهندس الإجتماعي وجعلك تقلق بأن جهازك مصاب بالبرامج الخبيثة، وأشغلك كي لا تفكر بأن البرنامج الذي قمت بتحميله هو نفسه من البرامج الخبيثة.

ولذلك ، فعلينا أن نفكر جديا في كيفية حماية أنفسنا من تلك الهجمات؟

منع النوافذ المنبثقة

تحتوي معظم متصفحات الإنترنت على إعدادات معينة ، يمكنك عن طريقها منع ظهور النوافذ المنبثقة أثناء تصفحك لمواقع الإنترنت. هذا الضبط يجنبك ظهور النوافذ المنبثقة ورسائل برامج مكافحة الفيروسات المزيفة ويحميك أيضاً من أشياء أخري.

تجاهل أي نوافذ منبثقة ما لم تكن من برنامج مكافحة الفيروسات المركب على حاسبك الآلي

استخدم فقط برامج مكافحة الفيروسات الموثوق بها فهي تحمي حاسبك الآلي من أي ضرر.

العديد من شركات برامج مكافحة الفيروسات توفر أدوات مجانية على شبكة الإنترنت قد تساعدك على التخلص من أي فيروسات على جهازك خصوصاً إذا لم يوجد عليه برنامج لمكافحة الفيروسات. يمكن لهذه الأدوات عمل فحص شامل للحاسب الآلي والتخلص من أي فيروسات، إن وجدت. يمكنها أيضاً المساعدة في التعرف على البرامج الخبيثة والبوتنت وغيرها ومن ثم التخلص منها.

هناك العديد من البرامج و الأدوات التي تفحص الحاسب الآلي بحثاً عن أي فيروسات أو برامج خبيثة. تقدم بعض المواقع مساعدة فنية للتعرف على نقاط الضعف والقوة في مثل هذه البرامج. كما أنه من الصعب تحديد برنامج بعينه وإعتباره الأفضل لمكافحة الفيروسات. ولكن من اللازم إختيار برنامج معروف لمكافحة الفيروسات. يمكنك التوجه لإحدى المحال المعروفة التي تبيع أجهزة الحاسب الآلي وبرامجه وقم بشراء أحد برامج مكافحة الفيروسات المعروفة. يمكنك أيضاً زيارة أحد مواقع الإنترنت الخاصة بأي من الشركات المعروفة بإنتاجها لبرامج مكافحة الفيروسات وقم بشراء البرنامج من الموقع مباشرة.

واجب منزلي

التعرف على برامج مكافحة الفيروسات الوهمية

تعرف على نوع برنامج مكافحة الفيروسات الموجود على حاسبك الآلي، وابحث عن الدليل الخاص به على موقع الشركة المنتجة له على شبكة الإنترنت. يمكنك الإستعانة ببرنامج آخر لمكافحة الفيروسات إذا لم تتمكن من الحصول على الدليل الخاص به.

1. بم سينصحك برنامج مكافحة الفيروسات إذا أصيب حاسبك الآلي بفيروس؟

2. ماذا ستفعل إذا اكتشفت أن جهازك به أحد البرامج الخبيثة؟

3. اذكر ثلاثة أسماء لبرامج مكافحة الفيروسات موثوقة ومعروفة.

4. لماذا تثقك بتلك البرامج؟ وضح اجابتك.

الدرس الرابع	كيفية التخلص من البيانات

تعريفات

البيانات الشخصية Personal Information – هي أي معلومات يمكن استخدامها للتعرف على هوية أي شخص مثل الاسم أو رقم الهوية الشخصية أو الصفات الجسدية أو العنوان أو تاريخ ومحل الميلاد.

سرقة الهوية Identity Theft – استخدام بيانات شخص ما لأغراض غير شرعية كالسرقة 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 من وثائق وملفات ووسائط وأشياء أخرى قد تحتوي على معلومات خاصة أو شخصية.

التخلص من المعلومات

لماذا التخلص الآمن؟

قبل إلقاء أي وثائق بسلة المهملات، هل تطالعها أولاً؟ ما نوع المعلومات الموجودة بها؟ هل تحتوي على بيانات خاصة أو شخصية؟ هل تفقدتها قبل الإستغناء عنها؟

عندما نستغنى عن وثائق أو أوراق فإننا نلقي بها في سلة المهملات. بعضها يمكن التخلص منه بهذه الطريقة وغيرها تحتاج لعناية أكثر أثناء التخلص منها. فإذا كانت تحتوي تلك الوثائق أو الملفات على بيانات أو معلومات خاصة فيجب التخلص منها بشكل آمن. إذا قررت التخلص من أي ملفات أو وثائق ورقية، فالأفضل التحقق إن كانت تحتوي على أي من التالي:

- اسمك بالكامل
- تاريخ ميلادك
- أسماء والديك أو تواريخ ميلادهم
- رقم بطاقتك الشخصية أو رقم بطاقة شخص آخر
- تفاصيل أو بيانات عن حالتك الصحية أو أي علاج طبي تتلاقاه
- معلومات عن وثائق ممتلكاتك
- كشف لحسابك البنكي أو بطاقات الإئتمان الخاصة بك
- معلومات عن رقم السيارة وتاريخ تسجيلها وشركة التأمين المسجلة معها.
- فاتورة هاتفك أو فاتورة استهلاك الكهرباء والماء.
- أوغيرها من المعلومات الخاصة .

هذه المعلومات قد يستغلها شخص ما لإنتحال شخصيتك أواستخراج بطاقات إئتمان على سبيل المثال، وهذا يسمى "سرقة الهوية" والذي قد يسبب مشاكل كثيرة لصاحب الهوية المسروقة.

ذكر مكتب مفوضي المعلومات في بريطانيا بعد التحقيق الذي تم في ديسمبر 2010، أن 11% من الأقراص الصلبة وذاكرات الفلاش والهواتف النقالة التي تم الإستغناء عنها كانت تحتوي على معلومات تصلح للقراءة.

"كان يحتوي اثنين من الأقراص الصلبة على كم هائل من المعلومات الشخصية التي كانت تخص أصحابها، وكانت تتضمن صور ضوئية لتقارير حسابات بنكية وجوازات سفر وشهادات ميلاد وإدانات لمخالفات قيادة وتقارير طبية وتقارير ضريبية وصور عائلية"

وقال المتحدث باسم مكتب مفوضي المعلومات "تضمن القرصين معلومات أكثر من كافية لأن يقوم طرف ثالث بإنتحال صفة أصحاب المعلومات"

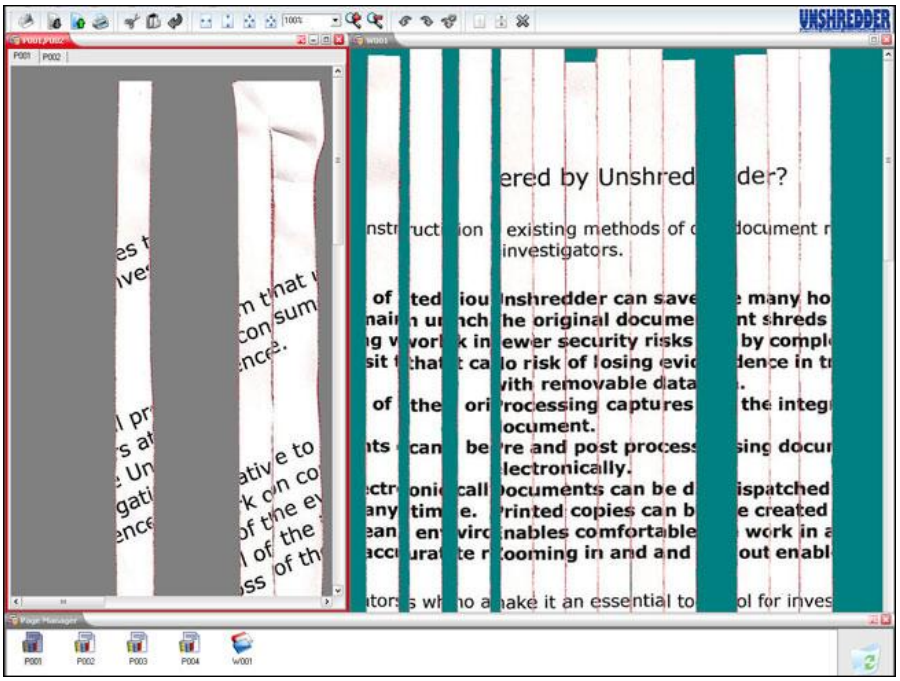
التخلص السليم من المعلومات

التخلص السليم من الأشياء 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 يقوم غيرك بالبحث 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.

1. الوثائق الورقية

أسهل طريقة للتخلص الصحيح من الوثائق الورقية هي التقطيع. احرص على استخدام ماكينة تقطيع الورق التي تقطعه لقطع صغيرة جدا بحجم 5 ملم، لأنه لو تم تقطيعه كشرائط طويلة فإنه من السهل تجميعها مرة أخرى كما هو مبين في الصورة التالية...



2. الحاسب الآلي

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

محو القرص

إذا أردت الإستغناء عن الحاسب الآلي الخاص بك بأي شكل، من الأفضل محو القرص الصلب. هناك العديد من البرامج المجانية التي تقوم بمحو 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.

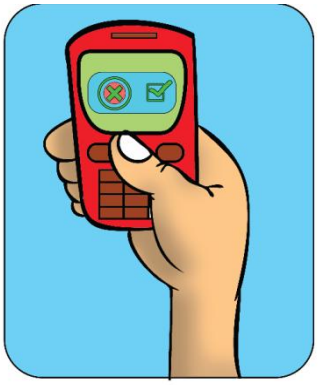
التحطيم

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 مهندس خبير. 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.

3. الهواتف الجوالة



الهواتف الجوالة هي عبارة عن أجهزة حاسب آلي صغيرة ، تحتوي على المعلومات التي قمت بتخزينها. 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 بتقطيع الهاتف!

ما لا تحتاجه... لا تحتفظ به...

إن أبسط طريقة للتأكد من التخلص السليم من أي معلومات هو التخلص منها 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 والتخلص منها. لا تبقي أي معلومات لم تعد تحتاجها حتى لا يتم سرقتها من قبل لصوص المعلومات في وقت ما.

واجب منزلي **التخلص من المعلومات بالمنزل**	

كما ناقشنا من قبل، فإنه من الضروري التخلص السليم من أي شئ عليه معلومات خاصة أو شخصية. تفقد الأشياء الموجودة بمنزلك وغرفتك التي قد تحتوي على معلومات شخصية أو خاصة ثم أجب عن الأسئلة التالية.

1. اذكر ثلاثة أشياء في منزلك تحتوي على معلومات شخصية أو خاصة.
2. اذكر مثالين على أشياء في منزلك تحتوي على معلومات شخصية أو خاصة ولم تعد تحتاج للإحتفاظ بهما.
3. اذكر كيفية التخلص السليم من الخمس أشياء التي قمت بذكرها سابقاً.

قم بعمل بحث على الإنترنت عن الإرشادات الخاصة بالتخلص الآمن لأي شئ قد يحتوي على معلومات.

1. ما هي الإرشادات التي وجدتها؟ اذكر عناوينها واسم كاتبها ؟.
2. هل تحتوي أمثلة سهلة لشرح كيفية التخلص الآمن من الوسائط المختلفة التي تحوي على معلومات؟
3. اذكر مثالاً لفت انتباهك عن كيفية التخلص من وسائط الحفظ.

نصائح سريعة

- فعِّل مصفي البريد المزعج ليساعدك على خفض عدد رسائل البريد المزعج التي تصلك.
- لا تنشر بريدك الإلكتروني على مواقع التواصل الإجتماعي أو تقوم بإدخاله على أي من المواقع التي تطلب ذلك.
- احذر من رسائل التصيد المغرية أو التي تثير قلقك أو فضولك
- لا ترسل معلومات شخصية على البريد الإلكتروني أو المراسلة الفورية
- لا تفتح المرفقات أو روابط المواقع في البريد الإلكتروني المرسلة من مجهولين
- لا تعط كلمة المرور الخاصة بك لأي شخص
- فعِّل مانع النوافذ المنبثقة في متصفح الإنترنت
- تجاهل أي نوافذ منبثقة ما لم تكن من برنامج مكافحة الفيروسات الموجود على جهازك
- تعلم كيفية التخلص السليم من الأشياء التي تحتوي على المعلومات الشخصية والخاصة
- تخلص من المعلومات الشخصية والخاصة التي لم تعد تحتاجها بشكل سليم حتى لا يجدها غيرك ويستخدمها بشكل خاطئ

إختبر معلوماتك	

1. ما هو البريد المزعج؟ اكتب بأسلوبك.

2. هناك أنواع مختلفة من مرشحات البريد الإلكتروني. صل نوع مصفي البريد الإلكتروني من جهة اليمين بتعريفه من جهة اليسار.

أ	القوائم البيضاء		يستخدم قائمة بعناوين البريد الإلكتروني سيئة المصدر
ب	القائمة السوداء		يجمع المعلومات عن محتويات رسائل البريد الإلكتروني المقبولة والغير مقبولة
ج	منع المحتوى		يستخدم قائمة بعناوين البريد الإلكتروني حسنة المصدر
د	المصفي المتعلم		يستخدم قائمة بالكلمات والمصطلحات التي توضح إذا ما كان من البريد المزعج ويجب منعه

3. كيف يمكنك حماية نفسك من البريد المزعج؟ اختر جميع الإجابات الصحيحة.
   أ. إعطاء عنوان بريد الإلكتروني لكل من يطلبه
   ب. حذف رسائل البريد الإلكتروني المرسلة من مجهولين
   ج. شغل مصفي البريد المزعج على بريدك الإلكتروني
   د. اقفل مصفي البريد المزعج على بريدك الإلكتروني

4. ما هو التصيد الالكتروني؟ وضح بأسلوبك.

5. كيف يمكنك حماية نفسك من التصيد؟ اختر جميع الإجابات الصحيحة.
   أ. حذف رسائل البريد الإلكتروني المرسلة من مجهولين
   ب. الرد على رسائل البريد الإلكتروني التي تطلب معلومات خاصة
   ج. عدم فتح الروابط في أي بريد إلكتروني مرسل من مجهول
   د. فكر جيداً بشأن البريد الإلكتروني قبل القيام بأي تصرف
6. ما هي بعض الطرق السائدة التي تقنع المستخدمين بالرد على رسائل التصيد؟ اختر جميع الإجابات الصحيحة.
   أ. تقديم الهدايا و العروض المغرية
   ب. تقديم مبالغ كبيرة من المال
   ج. عرض الأمر على أنه عاجل وضروري
   د. طلب المساعدة
   ه. إعطاء معلومات خاصة عن المستخدم
7. كيف يمكنك حماية نفسك من التصيد؟ اختر جميع الإجابات الصحيحة.
   أ. الرد على رسائل البريد الإلكتروني التي تطلب معلومات خاصة
   ب. عدم فتح الروابط في أي بريد إلكتروني مرسل من مجهول
   ج. عدم فتح أي مرفقات مرسلة لك من مجهول
   د. تشغيل برنامج مكافحة الفيروسات وتحديثه
8. اكتب ثلاثة أمثلة مختلفة لحسابات المستخدم.
   أ.
   ب.
   ج.

9. من الأفضل أن تسمح لأشخاص محددين باستخدام حاسبك الآلي. يمكن لجهازك أن يساعدك من خلال ثلاثة أشياء للتحكم في تحديد من يستخدم حاسبك الآلي وماذا يمكنهم أن يفعلوا. ستجد تعريفات لثلاثة أشياء، وعليك كتابة المصطلح المناسب أمام كل تعريف.
   أ. _____ إدخال اسم المستخدم لتعرف الحاسب الآلي أنك تملك حساب عليه.
   ب. _____ إدخال كلمة المرور لتأكيد أنك الشخص الذي يملك الحساب على الحاسب الآلي.
   ج. _____ يعطيك الحاسب الآلي صلاحيات بالقيام بأشياء معينة عليه.
10. كيف يمكنك التعرف على برنامج مكافحة الفيروسات الوهمي؟ اختر جميع الإجابات الصحيحة.
   أ. تظهر نافذة منبثقة لا تنتمي لبرنامج مكافحة الفيروسات الموجود على حاسبك الآلي
   ب. تصلك رسالة من شركة برمجيات لم تسمع عنها من قبل.
   ج. تصلك رسالة بها مشكلة تبدو ضرورية
   د. تجبرك الرسالة على تحميل برنامج مكافحة الفيروسات التي تعرضه عليك

11. ما هي المعلومات الشخصية؟ وضح بأسلوبك.

_____

_____

_____

12. الأشياء التالية قد تحتوي على معلومات شخصية أو خاصة. وضح كيفية التخلص منها بشكل سليم .
   أ. الأوراق
   ب. حاسب آلي يحتوي على قرص صلب
   ج. هاتف محمول