وزارة التربية والتعليم

7

أمن وحماية المعلومات

كتاب الطالب

الصف السابع

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 المعلومات والتدريبات التي ستمكنك من تعلم الطرق المختلفة للأمن والحماية عند إستخدام الحاسب الآلي والهاتف النقال والإنترنت. ستناقش الدروس كيفية حماية خصوصيتك والتسوق على الإنترنت بأمان. وكذلك التعرف على التصيد عبر رسائل البريد الإلكتروني وحماية أنفسنا عند استخدام الحاسب الآلي والهاتف النقال وأي أجهزة أخرى. سيزودك كل درس ببعض النصائح عن كيفية إستخدام مختلف أنواع التقنيات لتستمتع بها بشكل آمن.

المخرجات	

من خلال دروس هذا الكتاب سيتمكن الطالب من :

- التعرف على الطرق المختلفة لجمع بياناتك الشخصية ومعلوماتك الخاصة.
- تعلُم كيفية حماية بياناتك الشخصية ومعلوماتك الخاصة وكيف تستخدمها الشركات والمواقع الإلكترونية.
- معرفة مخاطر التسوق على الإنترنت.
- استعراض طرق الحماية والتسوق بأمان عبر المتاجر الالكترونية على الإنترنت.
- معرفة كيف يستخدم المهندسون الإجتماعيون البريد الإلكتروني لإقناعك بتزويدهم ببياناتك الشخصية ومعلوماتك الخاصة.
- تعلُم طرق تمييز ومقاومة التصيد وأي أشكال أخرى للهندسة الإجتماعية.
- عرض فوائد ومخاطر الحاسب الآلي النقال والهواتف الذكية والأجهزة الأخرى.
- تعلُم طرق حماية الهاتف النقال والهاتف الذكي والحاسب الآلي النقال.

جدول المحتويات	

الدرس الأول	الحفاظ على خصوصيتك

تعريفات

الخصوصية Privacy – إبقاء معلومات معينة سراً وعدم مشاركتها أو إخبارها للأخرين والحفاظ على سرية معلوماتك الشخصية.

المعلومات الشخصية Personal Information – معلومات يمكن استخدامها للتعرف على هوية الشخص مثل الإسم أو رقم الهوية الشخصية أو الصفات الجسدية أو بيانات العنوان أو تاريخ ومحل الميلاد.

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

البريد المزعج Spam email– رسائل ترد إلى بريدك الإلكتروني بدون إذنك أو بدون أن تطلب أن تُرسل إليك، وعادة ما يتم ارسالها لعدد كبير من الناس.

كوكيز "ملفات تعريف الإرتباط" Cookies – معلومات صغيرة تخزن على جهازك يرسلها الموقع الذي تقوم بزيارته لمتصفح الإنترنت الخاص بك والتي قد تحتوي على معلومات تخصك و تكشف هويتك.

سياسة الخصوصية Privacy Policy– مجموعة من القواعد والشروط التي توضح كيفية قيام الشركات والمواقع الإلكترونية بجمع واستخدام ومشاركة المعلومات التي تخص العملاء وزائري المواقع الإلكترونية.

المعلومات الشخصية

[insert image here]

(صورة لجواز سفر)

المعلومات الشخصية هي أي معلومات يمكن استخدامها للتعرف على هوية أي شخص باستخدام رقم الهوية الشخصية أو رخصة القيادة أو العنوان أو رقم الهاتف. قد تحمل بطاقة الإئتمان المصرفية اسم والدك وهذه وسيلة أخرى لمعرفة هويته ومعرفة رقم حسابه المصرفي.

انظر إلى جواز سفرك ، ستجد أنه يحمل صورتك الشخصية ورقم الجواز وتاريخ ومحل ميلادك. وهناك معلومات أخرى يتميز بها كل فرد منا للتعرف عليه.

من حين لآخر قد يُطلب منا التصريح ببعض المعلومات الخاصة بنا، على سبيل المثال عند استخراج بطاقة شخصية أو جواز سفر. إذن يجب عليك توفير معلومات مثل الاسم وتاريخ الميلاد والعنوان وغيرها من المعلومات التي تثبت هويتك وكيفية التعرف عليك. وإذا قمت بالتسجيل في مدرسة جديدة، فإن إدارة المدرسة ستطلب منك تزويدها بعنوانك ورقم هاتف ولي أمرك وربما رقم هاتف المنزل أيضاً. وينطبق هذا على المستوصف الطبي الذي تتردد عليه، فالطبيب بحاجة أن يتعرف على بعض المعلومات الخاصة عن حالتك الصحية وتاريخ الميلاد وفصيلة الدم وكذلك عنوان منزلك، وغيرها من المعلومات الشخصية التي يستعان بها للتعرف على هويتك الشخصية.

إذا أعطيت تلك المعلومات للأشخاص الخطأ، فيمكن لأي منهم إنتحال شخصيتك. يمكنهم تأجير أفلام الفيديو أو الإشتراك بإسمك في مواقع مشبوهة على الإنترنت أو شراء أشياء بإستخدام بطاقة والدك المصرفية أو قد يقوموا بشراء بعض السلع وإرسال الفواتير الخاصة لمنزلك بسبب استخدامهم معلوماتك الشخصية.

فهل فكرت جيداً قبل إعطاء مثل هذه المعلومات لأي شخص ؟

هل تسائلت لماذا قد يطلب أحدهم مثل تلك المعلومات؟

الخصوصية على الإنترنت Internet Privacy

عند استخدامك لشبكة الإنترنت تقوم بعض المواقع الإلكترونية بجمع المعلومات الخاصة بك. فمثلاً قد يطلب منك الموقع أن تقوم بتسجيل الدخول للتأكد من هويتك. ومن الممكن أن يطلب منك الموقع إدخال عنوان البريد الإلكتروني لإرسال معلومات وإشعارات notifications حول نشاط الموقع، أو حتى طلب إدخال عنوان المنزل وأرقام الاتصال، ربما لإرسال هدية أو بعض المراسلات. وقد يقوم الموقع بطلب الإجابة عن بعض الأسئلة الخاصة مثل تاريخ الميلاد أو النوع (ذكر – أنثى) والأشياء التي تفضلها أو تعجبك.

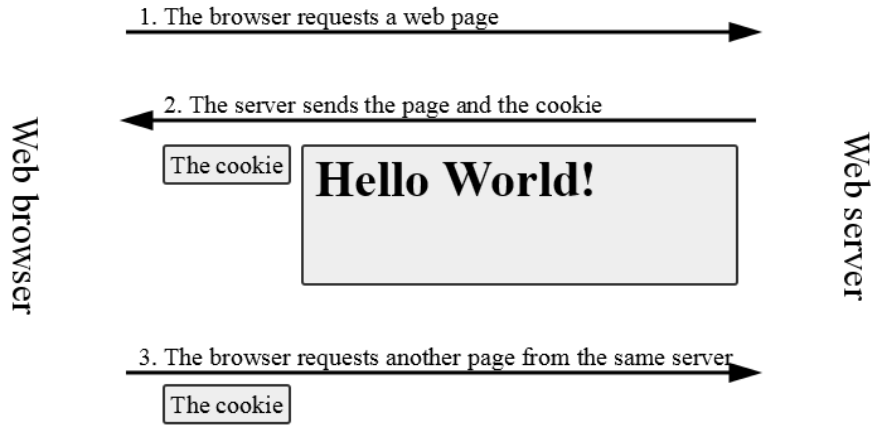
هذه جميعاً تعد معلومات شخصية وخاصة. وفيما يلي بعض الأمثلة عن المعلومات التي قد تطلبها المواقع وسبب جمعها والمخاطر الناجمة عن ذلك.

المعلومات	سبب طلبها	المخاطر
اسم المستخدم وكلمة المرور	تحتفظ بخصوصية حسابك الإلكتروني ومعرفة ما تفعله على الموقع وما تقوم به في زيارتك	من الأمان استخدام اسم مستخدم وكلمة مرور مختلفة لكل موقع. عند تسجيل الدخول. يقوم الموقع بتعقب ومعرفة نشاطاتك عليه وتوقيت تسجيل الدخول، ثم يستخدم تلك المعلومات لإرسال العروض الخاصة وما يتناسب مع ما تقوم بالبحث عنه.
عنوان البريد الإلكتروني	إرسال إشعارات notifications بكل ما هو جديد، إلى جانب إرسال الإعلانات ومعلومات عن المنتجات الجديدة.	يقوم الموقع باستخدام بريدك الإلكتروني لإرسال رسائل بشأن منتجات جديدة وخدمات وأخبار وعروض خاصة ومعلومات أخرى. وقد يتم تبادل بريدك الإلكتروني مع شركات أخرى لإرسال رسائل بشأن منتجاتها، ويترتب على ذلك وصول العديد من رسائل البريد الإلكتروني

		التي لا تحتاجها إلى جانب رسائل البريد المزعج.
عنوان المنزل	إرسال الهدايا والمراسلات والعروض الخاصة وشحن ما قمت بشرائه من أي موقع للتسوق أو محل تجاري.	يمكن أن يستخدم في إرسال رسائل البريد المزعج أو إعطاء عنوان منزلك لشركات أخرى التي قد ترسل لك أيضاً مراسلات وإعلانات مزعجة.
الأشياء المفضلة	تظهر لك المعلومات التي قد تجذب إنتباهك.	استخدام تلك المعلومات لإرسال العروض الجديدة والإعلانات التي تتماشى مع ما تقوم بالبحث عنه على الموقع.

ملفات تعريف الإرتباط Cookies

هناك أمر آخر يقوم به الموقع لجمع المعلومات الشخصية. حيث تقوم بعض المواقع الالكترونية عند الوصول اليها عن طريق برنامج المتصفح، بوضع ملفات صغيرة على حاسبك الآلي تسمى **ملفات تعريف الإرتباط Cookies**. وتستخدم المواقع هذه الملفات للتعرف على نشاطات زيارتك لها وإذا ما قمت بزيارة مسبقة لها ومتى كان ذلك. ملفات تعريف الإرتباط قد تحتوي على ما يكشف هويتك الشخصية والمفضلات لديك والمعلومات التي دائماً ما تقوم بقراءتها أو البحث عنها على تلك المواقع.



وتعد ملفات تعريف الإرتباط مهمة في أحيان كثيرة. فعند زيارتك لموقع ما، يحتاج هذا الموقع للتعرف عليك لتفادي إنتحال آخرين لهويتك الشخصية. لذا تقوم ملفات تعريف الإرتباط بمساعدة الموقع على سهولة التعرف عليك، إلى جانب إحتفاظ الموقع بما قمت بضبطه من تفضيلات معينة عليه.

وقد تكون ملفات تعريف الإرتباط ضارة في أحيان أخرى. لكونها تستخدم لتعقب وجمع معلومات نشاطك الالكتروني على الإنترنت، ومعرفة المواقع المختلفة التي تقوم بزيارتها. بعض ملفات تعريف الإرتباط لا تكون آمنة إذ يمكن لأي مواقع أخرى قراءتها، وقد يؤدي ذلك أن تقارن بعض الانظمة معلومات ومحتوى ملفات ارتباط لمواقع أخرى، ويمكن أن يُساء استخدام هذه المعلومات التي تجمعها، لذا يجب أن تعرف كيف تحمي نفسك.

كيف أحمي نفسي؟

إذا كنت معتاد على زيارة موقع معين فعليك أن تتحقق من سياسة الخصوصية التابعة لهذا الموقع. **سياسة الخصوصية** عبارة عن قواعد وشروط توضح لك كيف يقوم الموقع بجمع المعلومات وكيف يتم استخدامها. اقرأ سياسة الخصوصية للتعرف على كيفية إستخدام الموقع لمعلوماتك الخاصة التي يتم جمعها. هناك بعض المواقع التي ليس لديها سياسة للخصوصية وهناك غيرها من الشركات التي لا تتبع سياسة الخصوصية التي تضعها على موقعها الخاص، لذا يجب الحذر وحماية نفسك.

تجنب رسائل البريد المزعج. وهذا يتحقق عندما تحرص على عدم إعطاء عنوان بريدك الإلكتروني لكل من يطلبه. لذلك عندما يطلب موقع ما عنوان بريدك الإلكتروني، إسأل نفسك أولاً لماذا يحتاجون إليه؟ هل لإرسال الإشعارات والمعلومات التي تحتاجها، مثل معلومات عن منتجات قمت بشرائها أو عن رحلة تنوي القيام بها؟ فإذا لم تجد سببا قويا فلا تكتب بريدك الإلكتروني. ولكن إذا كان من الضروري إدخال عنوان بريدك الإلكتروني، فإبحث عن خيار الموافقة، التي يذكر الآتي "دائماً إطلعني على آخر الأخبار والمعلومات والعروض الخاصة" ثم أزل الإختيار الموجود بجانبها. بعض المواقع تحتوي على خانة "لا ترسل رسائل بريد إلكتروني"، يمكنك إختيارها إن وُجدت.

إذا قمت بالإشتراك في أحد المواقع عن طريق تسجيل بياناتك، إطّلع على إعدادات الخصوصية الموجودة على الموقع التي يمكنك التحكم فيها. العديد من مواقع التواصل الإجتماعي لديها إعدادات الخصوصية التي تمكنك من التحكم فيمن يستطيع الإطلاع على صفحتك أومعلوماتك الخاصة ومن يستطيع التواصل معك. استشر ولي أمرك بخصوص نوع المعلومات التي يمكنك نشرها على شبكة التواصل الإجتماعي مع التأكد أن أصدقائك فقط هم من يمكنهم رؤية تلك المعلومات.

لا تنشر عنوان منزلك أو رقم هاتف المنزل أو رقم هاتفك النقال على شبكة التواصل الإجتماعي لتحمي نفسك وتتجنب المخاطر، لأن هذه الشبكات عامة ويمكن لأي أحد رؤية ما بها ومن ثَمّ استخدام هذه المعلومات من قبل الغرباء لمضايقتك أو إنتحال شخصيتك.

يمكنك حماية نفسك بالقيام بما يلي:

- انتبه الى ما تقوم بها أثناء مشاركتك في مواقع الإنترنت، وتأكد من ما تنشره من معلومات خاصة بك.
- لا تنشر أي معلومات إذا لم يكن هناك ضرورة لذلك.

	**سياسات الخصوصية Privacy Policy**

إختر أي موقع من المواقع الإلكترونية على شبكة الإنترنت. قد يكون موقعاً تقوم دائماً بزيارته أو أي موقع آخر تفضله.

ابحث عن سياسة الخصوصية على هذا الموقع، ثم أجب عن الأسئلة التالية:

1. اذكر خمسة أمثلة بخصوص المعلومات التي يقوم الموقع بجمعها من المستخدمين. اكتب أسباب جمع تلك المعلومات إذا كانت مذكورة على الموقع، وإن لم يكن، فأكتب بإسلوبك الأسباب التي تعتقد قيام الموقع بجمع تلك المعلومات من أجلها.

2. في رأيك، لماذا يقلق الناس من جمع الموقع لتلك المعلومات؟

التسوق عبر شبكة الإنترنت	الدرس الثاني

تعريفات

بروتوكول طبقة المقابس الآمنة "Secure Sockets Layer" (SSL) - وسيلة تتيح لبرامج الحاسب الآلي إرسال معلومات بإستخدام التشفير.

بروتوكول نقل النص "Hyper-Text Transport Protocol" HTTP – الوسيلة التي يستخدمها متصفح الإنترنت للإتصال بمزود شبكة الإنترنت وإسترجاع المعلومات التي يتداولها مزود الشبكة.

بروتوكول النقل الآمن للنص "Hyper-Text Transport Protocol Secure" HTTPS – هو إصدار من بروتوكول نقل النص HTTP الذي يستخدم بروتوكول طبقة المقابس الآمنة SSL.

التشفير Encryption – وسيلة للتغيير في المعلومات من أجل إخفائها أو التمويه. وفك التشفير **Decryption** هو عكس عملية التشفير.

التسوق بحذر على شبكة الإنترنت

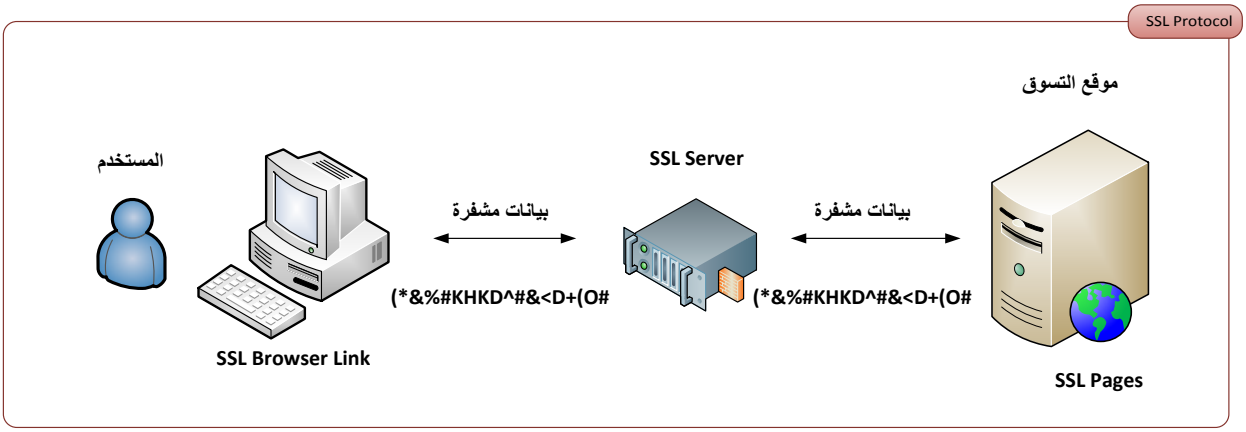
في تسعينيات القرن الماضي عندما أصبحت شبكة الإنترنت من أشهر الوسائل المستخدمة لتواصل الناس حول العالم، رأى البعض فرصة استخدامها لأغراض الشراء والتسوق.

ولكن كان يشغلهم تساؤل مهم ...

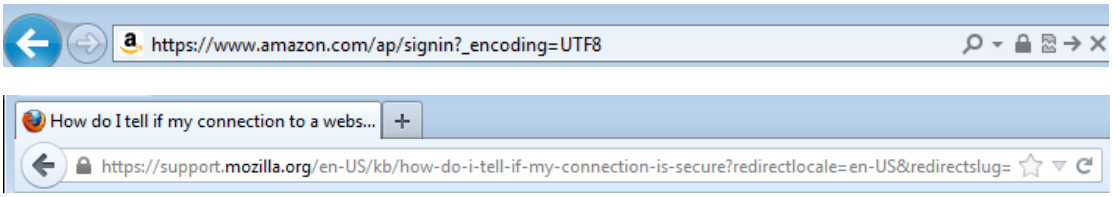
كيف يمكن للناس دفع مقابل ما يقومون بشراؤه عبر الإنترنت والتأكد أن الأموال يتم تداولها بأمان؟! عندما نذهب للمحلات التجارية للتسوق، يمكننا رؤية الشخص الذي يستلم منا النقود وأين يضعها نظير أي بضاعة ننوي شرائها. وإذا استخدمنا البطاقات الإئتمانية للشراء يكون ذلك أمامنا فنتأكد أنه لن يتم نقل أي بيانات موجودة على البطاقة. ولكن كيف يحدث ذلك على شبكة الإنترنت؟

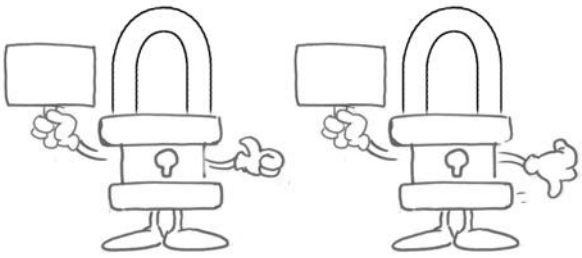
في الفترات الأولى لظهور شبكة الإنترنت، لم يكن هناك أي وسائل آمنة لإستخدام الموال لسداد قيمة السلعة لشخص ما عبر الإنترنت. وبالطبع لا يمكنك إرسال النقود الورقية أو المعدنية عبر الإنترنت، لذا استوجب استخدام البطاقات الإئتمانية المصرفية. ولكن كيف يتأكد أي متسوق أنه لن يتم سرقة بيانات بطاقته إذا قام بإدخالها في الموقع لشراء أي سلعة أو بضاعة؟

ولحل هذه المشكلة، قامت شركة نتسكيب Netscape بإبتكار ما يسمى ببروتوكول طبقة المقابس الآمنة SSL الذي يستخدم للتعرف على الموقع والتأكد أن معلومات بطاقة الإئتمان المدخلة محمية من أي محاولات لسرقتها. فعندما تبدأ بالتسوق على الإنترنت يقوم المتصفح بالتواصل مع موقع المتجر الالكتروني باستخدام بروتوكول طبقة المقابس الآمنة SSL، فهو يستخدم التشفير لإحداث تغييرات في المعلومات حتى لا يستطيع أحد قراءتها، والموقع وحده فقط القادر على فك شفرة المعلومات وقراءتها بصورة صحيحة.

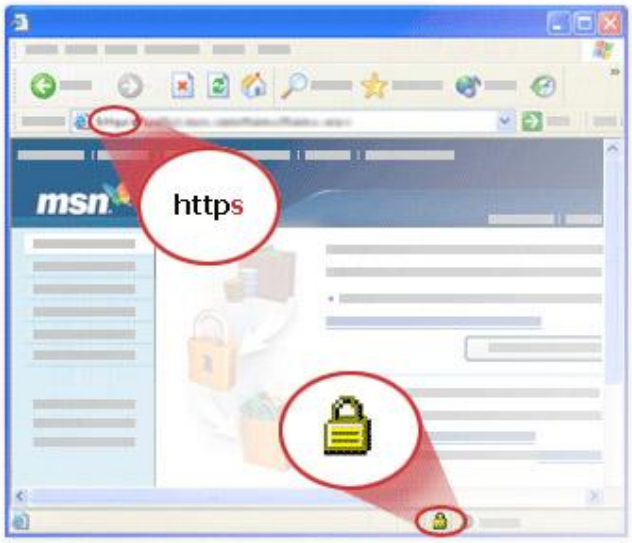


تأكد أثناء التسوق على أي موقع أنه يستخدم بروتوكول طبقة المقابس الآمنة SSL. وهنا يمكننا التعرف عليه إذا نظرنا إلى صورتي متصفح الإنترنت التاليتين. سنلاحظ أيضاً أن اسم الموقع يبدأ بـhttps . الـs هنا تعني أن المتصفح والموقع يستخدمان SSL ليضمنا خصوصية الإتصال بينهما. ومعظم المواقع العادية تستخدم http الغير مشفر.





هناك العديد من برامج التصفح لمواقع الإنترنت التي لها وسائلها الخاصة لإخبارك إذا ما كان الموقع الذي تقوم بزيارته آمناً أو غير ذلك. وتختلف تلك الوسائل بإختلاف أنواع برامج التصفح وإختلاف إصداراتها. فمنها ما يُظهر لك رمز القفل بألوان مختلفة. فالأخضر والأزرق عادة يدلان إلى أن الموقع آمن والأحمر يدل أنه غير آمن. راجع قائمة المساعدة Help لبرنامج التصفح الذي تستخدمه للتأكد من تلك المعلومة.



يواجه المتسوقون عبر شبكة الإنترنت مشكلة أخرى وهي كيفية التأكد من حصولهم على ما قاموا بالفعل بشراءه من مواقع التسوق. عندما تتسوق في المحلات التجارية يمكنك أن تشاهد وتختار بنفسك ما ترغب في إقتناءه، فتتحقق من مقاسات الملابس أو خلوها من أي تلف وبعد سداد ثمنها، تتأكد أن البائع قد أعطاك ما قمت باختياره وشراءه. وإذا رغبت لأي سبب إستبدال أو استرداد ثمن ما إشتريته، يمكنك ذلك بالرجوع مرة أخرى للمحل التجاري.

أما في التسوق عبر الإنترنت، فإنك لا تلتقي بالبائع ولا ترى إلا صور السلع ووصفها فقط، إذ لا يمكنك التأكد من مقاسات الملابس أو الأحذية المناسبة لك. ولذلك حرصت الشركات العريقة على الإنترنت أنه لكسب ثقة الناس تحتاج لرعاية زبائنها جيداً. والآن الكثير من الشركات التي تقوم بأعمالها التجارية عبر الإنترنت يكسبون ثقة العملاء أكثر فأكثر.

ليس من الصعب أبداً إيجاد مواقع وشركات التسوق على الإنترنت، ولكن يجب أن تكون حذراً لتحمي نفسك من أي مخاطر. قم بإجراء بحث عن آراء وتعليقات الزوار والعملاء بخصوص الموقع الذي تنوي التسوق فيه من حيث مستوى الخدمات، مثل خدمات ما بعد البيع وهل تسلّموا بالفعل ما قاموا بشراءه. ومن المفيد جدا تفقُد آراء عملاء تلك المواقع ، وقراءة كيف كانت تجربتهم مع موقع التسوق، فهذا يجعلك تتخذ القرار الصحيح للتسوق الآمن وأنت مطمئن.

التوعية بالتسوق عبر الإنترنت

حين تنوي الذهاب للتسوق في أحد المراكز التجارية، تقوم بتحديد المحلات التي تريد زيارتها وما الذي تريد شراؤه والتأكد من أنك تحمل نقوداً أو بطاقات إئتمانية لإقتناء ما تريد.

أما في حال التسوق عبر الإنترنت، فيتطلب ذلك الإنتباه لبعض الأمور.

- تفقد آراء وتعليقات الزوار والمشترين الآخرين في الموقع الذي تريد التسوق منه وتأكد أن العملاء قد تمتعوا بتجربة شراء ممتازة على هذا الموقع.
- تأكد من طرق التواصل مع الموقع وسياسة الإستبدال والإسترجاع.
- تأكد أن برنامج مكافحة البرامج الخبيثة الموجود على حاسبك الآلي يعمل ومعد على آخر تحديث ليساعد على حمايتك من البرامج الخبيثة وبرامج التجسس التي قد تحاول سرقة معلومات بطاقتك الإئتمانية التي تقوم بإدخالها عبر موقع التسوق.
- لا تتسوق عبر شبكات الإنترنت اللاسلكية الموجودة في الأماكن العامة. بعض الأشخاص يمكنهم إنشاء شبكات عامة لاسلكية مزيفة و يسرقون من خلالها المعلومات التي يدخلها المستخدمين.
- تأكد دائماً من وجود وصلة HTTPS بين برنامج المتصفح وموقع التسوق، لكي تطمئن أن الموقع آمن قبل إدخال أي معلومات خاصة مثل رقم البطاقة البنكية.
- بعد إتمام عملية الشراء، تأكد أن القيمة المطلوبة من موقع التسوق هي نفس القيمة المسحوبة من بطاقتك البنكية. راجع كشف حساب بطاقتك للتأكد من صحة جميع الرسوم المستحقة.
- إذا وجدت أي عمليات شرائية أخرى لم تقم بها، أبلغ ولي أمرك فوراً وقم بالإتصال بالبنك للإبلاغ عن هذا الخطأ.

التسوق عبر الإنترنت

فكر في أحد أقربائك الكبار ممن ليس لهم دراية بإستخدام الإنترنت. ستقوم بدعوتهم للتسوق معك عبر الإنترنت.

1. كيف ستشرح له عملية التسوق عبر الإنترنت؟

2. هل سيشعر بالراحة أثناء التسوق على الإنترنت؟ ولماذا؟

3. إذا قال لك "كيف أقوم بشراء أشياء لا استطيع رؤيتها على الطبيعة؟". ماذا سيكون ردك؟

4. ما النقاط التي يمكنك ذكرها لأي شخص ليشعر بالإطمئنان بشأن التسوق عبر الإنترنت؟

الدرس الثالث	التصيد

تعريفات

المهندس الإجتماعي Social Engineer– شخص يقوم بجمع المعلومات وسرقة معلومات الآخرين أو التمكن من إختراق أنظمة الحسابات الآلية بعد التأثير واستغلال أصحابها.

التصيد Phishing – إستخدام أساليب الهندسة الإجتماعية عبر تقنيات الإنترنت، من أجل خداع الآخرين وإقناعهم بالإفصاح عن البيانات الشخصية أو المعلومات الخاصة.

ما هو التصيد؟

رسائل التصيد هي رسائل البريد الإلكتروني التي تحاول إقناعك بفعل أشياء عادة لا تقوم بها.

التصيد هو نوع من الهندسة الإجتماعية، والهندسة الإجتماعية هي نوع خاص من التهديدات لأن المهندس الإجتماعي لا يحاول إختراق نظام الحاسب الآلي أو البرامج الموجودة عليه ولكن يحاول إستدراج الأفراد للقيام بما لا يفترض القيام به.

وتنجح محاولات التصيد عند إقناعك بمساعدة شخص ما، ومقابل ذلك تحصل على جائزة أو مكافأة أو إيهامك أن الرسالة مرسلة من صديق. والشخص الذي يرسل رسائل التصيد غرضه إقناعك أن تشاركه في بيانات أو معلومات شخصية.

تطلب رسائل التصيد بأساليب مختلفة، معلومات خاصة مثل الإسم أو رقم الهاتف أو العنوان أو كلمة المرور أو أرقام بطاقتك البنكية. يستخدم المتصيد هذه المعلومات للتحكم بحسابك على شبكة التواصل الإجتماعي أو سرقة أموال من حسابك البنكي. كما ستحاول دائماً رسائل التصيد خداعك للقيام بأشياء يفترض أنك لا تقوم بها والتي ستزوِد المهندس الإجتماعي بالمعلومات التي يسعى ورائها.

قد تخبرك رسائل التصيد عن فوزك بمبلغ كبير من المال أو إبلاغك بمساعدة صاحب الرسالة نظير حصولك على مبلغ كبير من المال. وبالفعل يُستدرج بعض الناس لمثل هذه الخدع وتأخذهم الحماسة لظنهم أنهم سيحصلون على مبالغ كبيرة، وبالتالي يرسلون معلوماتهم الخاصة للمهندس الإجتماعي فيرد بطلب بياناتهم البنكية لإرسال المال. وعندما يحصل المهندس الإجتماعي على المعلومات البنكية، يستخدمها لسرقة المال من الحساب وليس لإرسال المال كما إدعى من قبل.

وبالأسفل مثال حقيقي للتصيد عن طريق رسائل البريد الإلكتروني.

Mr. John Winter, Foundations Officer
The James Clerk Maxwell Foundation
23, Mangotsfield,Edinburgh, BS16 9JE, SCOTLAND

Dear Sir,

NOTIFICATION FOR CASH AID.

This is to notify you that you have been chosen By the Board of Trustees of the above International charity organization based in the U. K as a one of the final recipients of a Cash Grant/Donation for Business, Economic, social and Research developments in your community.

The James Clerk Maxwell Foundation as established 1977 by the Multi-Million Maxwell family was conceived with the objective of Human Growth, Educational and Community development. In line with the 28 years anniversary program this year the James Clerk Maxwell foundation in conjunction with the British Council is giving out One Hundred Million United States Dollars as specific Donations/Grants to 150 lucky international recipients worldwide in different categories for Business development and Social uplift of their various communities. These funds are freely given to you to use for your business and educational development and your community development at large.

Based on the random selection exercise of millions of Super market cash invoices worldwide you were selected among the lucky recipients to receive the award sum of US$850,000.00(eight hundred and fifty thousand United states Dollars) as charity donations/aid from the Maxwell Foundation in accordance with the enabling act of Parliament.(note that your email was selected from a Shop's cash invoice around your area in which you might have purchased something from).

You are required to Contact immediately the Executive Secretary below for qualification documentation and processing of your claims. And you are to contact back this email when you have collected your US $850,000.00.

Please quote your Qualification numbers (N-222-6747, E-900-56) in all discussions.

Please note that this donations/Grants are administered by a British Bank and therefore subject to British Laws. On behalf of the Board kindly accept our warmest congratulations

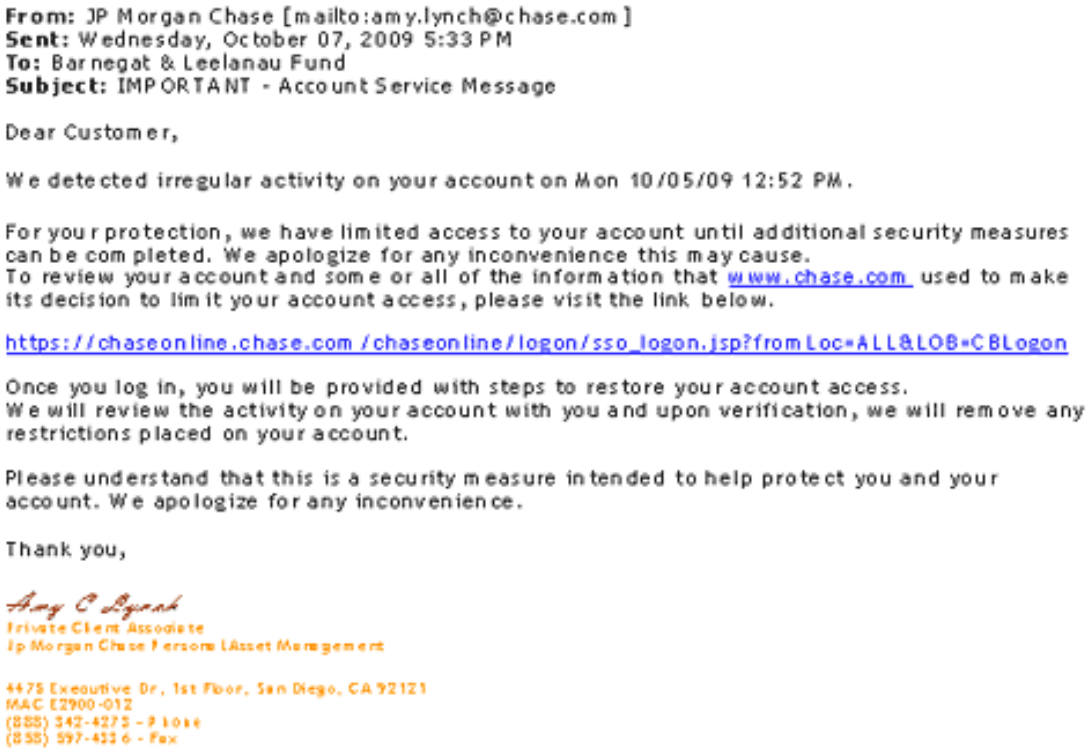
Yours faithfully,

Mr. John Winter (Foundation officer)

وقد تخبرك رسالة التصيد أنه تم تجميد حسابك على أحد المواقع ويجب عليك الرد على تلك الرسالة لإعادة تنشيطه مرة أخرى. قد تحتوي رسالة التصيد على رابط لموقع آخر حيث يطلب إدخال بيانات حسابك الالكتروني مثل اسم المستخدم وكلمة المرور. سيبدو ذلك الموقع رسمياً أو حقيقياً إذ ربما تجد عليه شعاره المميز مما يجعلك تظن أنه حقيقياً بالفعل. بعض الناس يشعرون بالقلق على حساباتهم الالكترونية فيقوموا بالضغط على الرابط الموجود بالرسالة فيفتح الموقع المزيف ويطلب إدخال اسم المستخدم وكلمة المرور أو معلومات الحساب البنكي. ولكن إذا نظرنا جيداً لمحتوى رسالة التصيد ستجد أن الرابط المرفق بالرسالة لا يبدو مألوفاً مثل روابط المواقع الحقيقية.

{picture of an official website's link and another fake one to recognize the difference}

وبالأسفل مثال آخر للتصيد بهذا النوع من رسائل البريد الإلكتروني.



From: JP Morgan Chase [mailto:amy.lynch@chase.com]
Sent: Wednesday, October 07, 2009 5:33 PM
To: Barnegat & Leelanau Fund
Subject: IMPORTANT - Account Service Message

Dear Customer,

We detected irregular activity on your account on Mon 10/05/09 12:52 PM.

For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause.
To review your account and some or all of the information that www.chase.com used to make its decision to limit your account access, please visit the link below.

https://chaseonline.chase.com/chaseonline/logon/sso_logon.jsp?fromLoc=ALL&LOB=CBLogon

Once you log in, you will be provided with steps to restore your account access.
We will review the activity on your account with you and upon verification, we will remove any restrictions placed on your account.

Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Thank you,

Amy C Lynch
Private Client Associate
Jp Morgan Chase Persons |Asset Management

4475 Executive Dr, 1st Floor, San Diego, CA 92121
MAC E2900-012
(888) 342-4273 - Phone
(888) 597-4336 - Fax

عند النظر للوهلة الأولى لرابط الموقع سيبدو عادياً ولكن عندما تضع مؤشر الفأرة عليه سيظهر رابط لموقع آخر. وستجد أن رسالة البريد الإلكتروني يظهر بها اسم الموقع ولكن ليس صحيحاً بالكامل. كما ستلاحظ عدد من الكلمات المحورة في محتوى الرسالة. هذا الموقع المزيف أنشأه مهندس إجتماعي وقد يحتوي على برامج خبيثة. وقد يطلب إدخال اسم المستخدم وكلمة المرور ورقم البطاقة البنكية والرمز السري PIN بقصد التأكيد أو تفعيل الحساب. يجمع المهندس الإجتماعي هذه المعلومات ليقوم بتزوير بطاقات أخرى ليستخدمها في سحب الأموال من حسابك المصرفي.

قد يرسل أحد المهندسين الإجتماعيين رسالة إلكترونية يذكر فيها وصول طرد خاص بك لدى مكتب البريد ويرفق بالرسالة ملف يدّعي أن به معلومات عن إستلام الطرد، ولكن في حقيقة الأمر هذه رسالة تصيد والملف المرفق هو أحد البرامج الخبيثة. وبمجرد تحميلك للملف المرفق سيقوم البرنامج الخبيث بتثبيت نفسه على حاسبك الآلي ثم يقوم بتجميع أي معلومات يجدها على الجهاز وقد يرسلها عبر الإنترنت لجهاز المتصيد. انظر كيف نجح المهندس الإجتماعي في إقناعك بتحميل البرنامج الخبيث على حاسبك الآلي! والآن وبعد أن حصل على المعلومات الخاصة بك، سيستخدمها لعمليات تصيد أخرى والإحتيال أو للتحكم في الحاسب الآلي الخاص بك لمهاجمة أجهزة أخرى.

لماذا سُمي بالتصيد؟

وُجِد أن طريقة استخدام المهندس الإجتماعي للبريد الإلكتروني تماماً مثل استخدام أي شخص لسنارة صيد السمك. فالمهندس الإجتماعي يقوم بإلقاء "الطُعْم" وهو الإشارة بجائزة مالية أو وجود حالة طارئة تحتاج للمساعدة الفورية، ليرى إن كان سيقوم أي شخص بأخذ الطُعم ومن ثم اصطياده بحيل المهندس الإجتماعي.

يقوم المهندس الإجتماعي بإرسال أكبر عدد من الرسائل وهو يعلم أنه فقط يحتاج لشخص واحد ليرد على الرسالة بمعلوماته الشخصية ليستولي على أمواله في النهاية.

أنواع التصيد

هناك أنواع مختلفة لأساليب التصيد، نذكر منها :

التصيد الموجّه Spear Phishing – إرسال رسالة تصيد لشخص أو شركة معينة، ويكون هدف المهندس الإجتماعي هو الحصول على معلومات تخص هذا الشخص أو هذه الشركة. سيحرص المهندس الإجتماعي أن تبدو رسالة البريد الإلكتروني مرسلة من شخص ذو ثقة، مثل موظف آخر أو صديق أو المدير التنفيذي الخاص بالشركة.

التصيد عن طريق رسائل الهواتف النقالة Smishing – إرسال رسائل إلي الهواتف النقالة بهدف التصيد. يقوم المهندس الإجتماعي بإنتحال صفة شخصية ذات أهمية أو ذات ثقة لإقناع مستقبل الرسالة بالرد عليه بمعلومات شخصية أو خاصة.

التصيد عن طريق المكالمات الهاتفية الآلية Vishing – يقوم المهندس الإجتماعي مسبقاً بتسجيل الرسائل الصوتية من أجل المكالمات الهاتفية الآلية، حيث يطلب من متلقي المكالمة إدخال رقم البطاقة الإئتمانية أو غيرها من التفاصيل شفهياً أو عن طريق لوحة مفاتيح الهاتف. ويقوم المهندس الإجتماعي بتسجيل رسالة صوتية تذكر أن هناك مشكلة تقنية أدت إلى فقد أحد العمليات الشرائية ببطاقة الإئتمان ويجب إدخال رقم البطاقة مرة أخرى. يقوم الشخص الذي يتلقى الرسالة بإدخال المعلومات وتقوم أحد الأجهزة بتسجيله على الفور أثناء إجراء المكالمة.

لماذا يقع الناس في التصيد؟

المهندسون الإجتماعيون يعرفون جيداً كيف يتم إستقطاب الناس وإقناعهم بتنفيذ ما يريدون.

كلنا نحب مساعدة الآخرين

إذا صادفت شخصاً يحتاج للمساعدة، فستقوم بمساعدته على الفور. قد يكون هذا الشخص تلميذ جديد بمدرستك ويريدك أن تساعده على الوصول لمكان فصله. فماذا لو طلب منك شخص ما بعض المال لشراء الطعام لأنه يشعر بالجوع؟ أو أن تعيره بطاقتك البنكية ليتمكن من شراء ملابس جديدة بدلاً من ملابسه القديمة؟! فليس من السهل معرفة إذا ما كان هذا الشخص بالفعل يحتاج ما يطلبه منك أو أنه يكذب عليك. ولكن طبيعة البشر إفتراض حسن النوايا في الآخرين، ومن هذا المنطلق يرسل المهندس الإجتماعي رسائل بريد إلكتروني تحتوي على قصص مؤثرة تجعلك تشعر بضرورة القيام بالمساعدة.

تجذبنا الهدايا والعروض الخاصة

الكثير من الناس تغريهم الهدايا أو أي فرص للحصول على المال، لذلك تعرض رسائل التصيد مبالغ كبيرة من المال، الأمر الذي يجعلنا لا ننتبه جيداً ومن ثم نتخذ قرارات غير مدروسة.

في تجربة تم تكرارها عدة مرات، قام فريق من بعض الأشخاص بعمل مسح ودراسة ميدانية عن مدى قوة كلمات المرور للمستخدمين. فطلبوا من الجمهور إعطاء كلمات المرور الخاصة بهم مقابل لوح من الشيكولاته. وبالفعل قام العديد من الجمهور بإعطاء كلمات المرور الخاصة بهم مقابل لوح الشيكولاته.

لا نفكر جيداً مع وجود أمر عاجل أو طارىء

إن المهندسين الإجتماعيين يعلمون جيداً أننا عادة لا نتخذ القرار الصائب وقت الطوارئ. ويمكننا فقط التركيز على القيام بعدد محدد من الأمور في وقت واحد. وغالباً يكون تركيزنا منصب على ما نعتقده أمرا ملحا. فإذا تلقيت بريد إلكتروني يذكر أنه قد تم غلق حسابك الالكتروني أو مهاجمته، سينتابك القلق بالتأكيد. والأسئلة التي ستدور برأسك هي "ما الذي حدث لحسابي؟ أتمنى ألا يكون الأمر مرتبط بسرقة معلوماتي أو حسابي البنكي المرتبط بهذا الحساب الالكتروني ؟". أضف إلى ذلك وصول ذلك البريد الإلكتروني وقت إنشغالك بشئ مهم أو شعورك بالتعب، فسيؤدي ذلك بالتأكيد في وقوعك ضحية لحيَل المهندس الإجتماعي.

من السهل حماية أنفسنا من الوقوع فريسة التصيد، فقط عليك التفكير جيداً قبل الرد على أي من رسائل البريد الإلكتروني.

تعرف على رسائل التصيد الالكتروني وتجنبها

هذه بعض الإرشادات و النصائح لتساعدك على تجنب وحماية نفسك من التصيد الالكتروني.

لا ترد على أي رسائل بريد إلكتروني تطلب بيانات شخصية أو معلومات خاصة

إذا وصلك بريد إلكتروني غريب يطلب منك إرسال أي معلومات شخصية أو خاصة، قم بحذفه فوراً. لا يحق لأي شخص غريب أن يطلب منك أي معلومات تخصك أو تخص ولي أمرك. لا ترد على تلك الرسائل واحذفها على الفور.

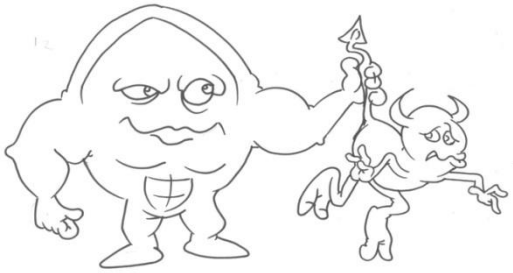
معظم المواقع الإلكترونية الرسمية والبنوك لا يطلبون منك الضغط على أية روابط داخل رسائل البريد الإلكتروني التي يرسلونها ولا يطلبون إرسال اسم المستخدم الخاص بك أو كلمة المرور.

لا تضغط أي روابط لمواقع إلكترونية مرفقة برسائل البريد الإلكتروني المرسلة من الغرباء

إذا وصلتك أية رسائل تبلغك أنه قد تم غلق حسابك الخاص ويجب الضغط على الرابط المرفق بالرسالة لإدخال اسم المستخدم وكلمة المرور لإصلاح الأمر وإعادة فتح الحساب، فلا تضغط على الرابط أبداً. ولكن عليك زيارة الموقع الأصلي للمصرف أو الشركة وإذا كان هناك أي مشكلة، تأكد أن الموقع سيقوم بإبلاغك فوراً.

لا تفتح أي ملفات مرفقة برسائل البريد الإلكتروني المرسلة من الغرباء

إذا وصلتك أي رسالة بها ملفات مرفقة ومرسلة من شخص غريب أو شركة لم تسمع عنها أو لم تتعامل معها من قبل، لا تفتح تلك المرفقات، لأنها ببساطة قد تحتوي على برامج خبيثة قد تقوم بتثبيت نفسها على جهاز الحاسب الآلي الخاص بك. احمي نفسك ولا تفتح تلك المرفقات.



حدث برنامج مكافحة الفيروسات دائما على آخر تحديث

لنفترض أنك وعن طريق الخطأ، ضغطت على رابطا كان موجودا في أحد الرسائل أو فتحت أحد الملفات المرفقة. يمكن

لبرنامج مكافحة الفيروسات أن يساعدك في حماية جهازك. يستطيع البرنامج كشف البرامج الخبيثة إذا حافظت على تحديثه أولا بأول، حتى لا يصاب حاسبك الآلي بتلك البرامج الضارة.

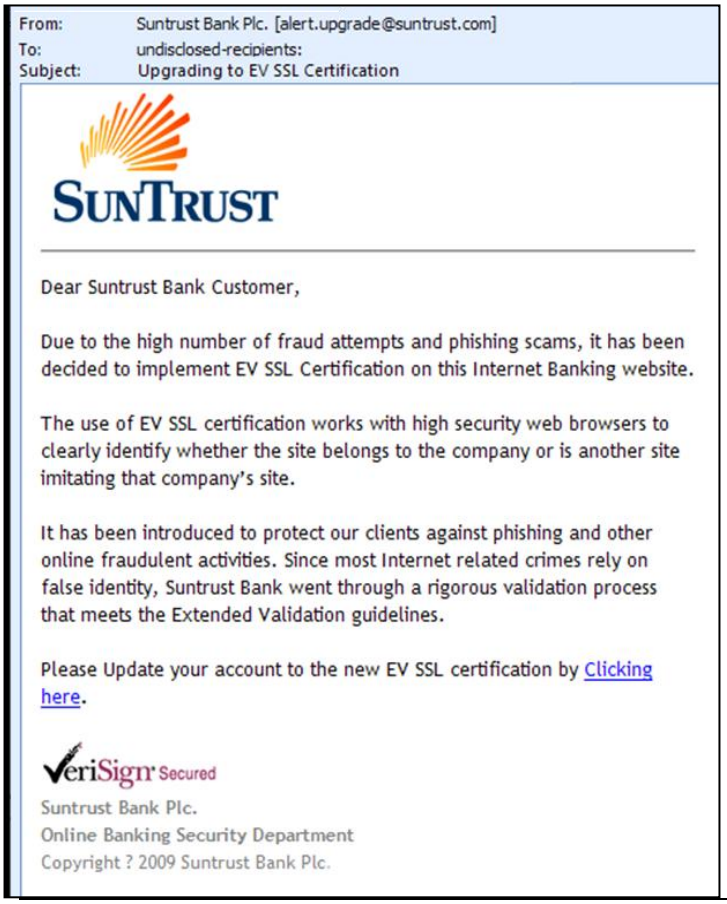
ولكن في حال إصابة جهازك، فأبلغ ولي أمرك على الفور ليطلبا المساعدة من متخصص للتخلص من البرامج الخبيثة.

لا تكسر القواعد !

لقد تعلمت من خلال هذا الدرس القاعدة المهمة وهي (عدم مشاركة المعلومات الشخصية أو الخاصة مع الآخرين أو إرسالها لأحد). وعندما تتذكر هذه القاعدة قبل أن تفتح أي مرفق أو رابط مشبوه في رسالة بريد إلكتروني وصلتك أو أي موقع يطلب منك هذا النوع من المعلومات، حينها تكون قد حصنت نفسك من مخاطر التصيد الالكتروني. أما اذا شككت بمحتوى أي رسالة غريبة، فاستشر ولي أمرك بشأنها قبل القيام بأي تصرف.

التصيد الالكتروني

تمعن جيدا في رسالة البريد الإلكتروني التالية وهي مثال للتصيد الالكتروني.


From: Suntrust Bank Plc. [alert.upgrade@suntrust.com]
To: undisclosed-recipients:
Subject: Upgrading to EV SSL Certification

SUNTRUST

Dear Suntrust Bank Customer,

Due to the high number of fraud attempts and phishing scams, it has been decided to implement EV SSL Certification on this Internet Banking website.

The use of EV SSL certification works with high security web browsers to clearly identify whether the site belongs to the company or is another site imitating that company's site.

It has been introduced to protect our clients against phishing and other online fraudulent activities. Since most Internet related crimes rely on false identity, Suntrust Bank went through a rigorous validation process that meets the Extended Validation guidelines.

Please Update your account to the new EV SSL certification by Clicking here.

VeriSign Secured
Suntrust Bank Plc.
Online Banking Security Department
Copyright ? 2009 Suntrust Bank Plc.

ثم أجب عن الاسئلة التالية:

1. من الذي يدعي إرسال هذا البريد الإلكتروني؟
2. ماذا تطلب هذه الرسالة من مستلمها؟
3. هل بالإمكان أن تعرف إن كان الرابط في نهاية الرسالة صحيحاً أم لا؟
4. إذا قام مستلم الرسالة بالرد عليها، ماذا يمكن أن يحدث؟
5. كيف يمكن لمستلم تلك الرسالة حماية نفسه؟
6. ما هي الأساليب التي يمكن أن يستخدمها المهندس الإجتماعي لإغراء أي شخص بالإفصاح عن كلمة المرور الخاصة به؟

الدرس الرابع	أمن الأجهزة النقالة

تعريفات

الحاسب الآلي المحمول Mobile Computers– المقصود به أي نوع من أنواع الحاسب الآلي الذي يمكن حمله معك بسهولة إلى أي مكان.

أمن الحاسب الآلي النقال

كانت أجهزة الحاسب الآلي في السابق كبيرة الحجم وثقيلة الوزن، الأمر الذي جعل نقلها مسألة صعبة ومرهقة، إلى جانب أن محتوياتها كانت قابلة للكسر أو التلف.

[insert image here]

{صورة حاسب آلي من الأجيال القديمة}

ثم ظهر أول حاسب آلي نقال، ولكنه كان ثقيل الوزن أيضا. أوزبورن1 هو أول جهاز حاسب آلي نقال يُطرح للبيع في الأسواق في عام 1981، وكان يزن تقريباً 11 كجم – أي أثقل 11 مرة من الحواسيب النقالة التي نستخدمها اليوم. و كان من الممكن حمله للبيت للعمل عليه ولكن لم يكن بالإمكان حمله أثناء التجول في أي مكان أو العمل عليه أثناء رحلة سفر. ولم يكن يتصل بالإنترنت لأنها لم تكن قد أنشئت بعد، ولم تكن سعة التخزين الموجودة به بالحجم الكافي لتخزين العديد من المعلومات مثلما هو الحال في أيامنا هذه.

عندما تطورت تقنيات تصنيع الحديثة، تم تركيب أجزاء أصغر للحاسب الآلي، وأصبح حجم الحاسب أصغر وأسهل في حمله أثناء التجول في أي مكان. الآن يمكنك أن تجد الحواسيب بمختلف الأشكال والأحجام والألوان. وأينما وجدت وسيلة للإتصال بالإنترنت، يمكنك الجلوس والعمل على حاسوبك النقال والتواصل مع من تحب، فلا عجب أن العديد من الناس الآن ينجزون بعض أعمالهم أثناء التنقل أوالسفر.

يمكن للمستخدمين العمل على الملفات وفتح البريد الإلكتروني في أي مكان لأن أجهزة الحاسب الآلي الجديدة الآن أصغر وأكثر قوة. ويمكنهم نقل ملفاتهم لأي مكان يريدون، ويمكنهم قراءة رسائل البريد الإلكتروني وتخزين الملفات على الهواتف الذكية. لذلك يمكنك العمل وقراءة الملفات ومشاهدة أفلام الفيديو وأنت مسافر. وجود أجهزة خفيفة وصغيرة الحجم يجعل حياتنا أسهل كثيراً حيث يمكن إستخدامها في الكثير من الأماكن.

الأجهزة النقالة

فكر في كيفية إستخدام أجهزتك النقالة، وذلك يتضمن الحاسوب النقال والهاتف النقال.

1. ما هي نوع المعلومات التي تتوقع أن تجدها على الهاتف الذكي الشخصي؟

2. ما نوع المعلومات التي تخزنها عادة على هاتفك الذكي؟

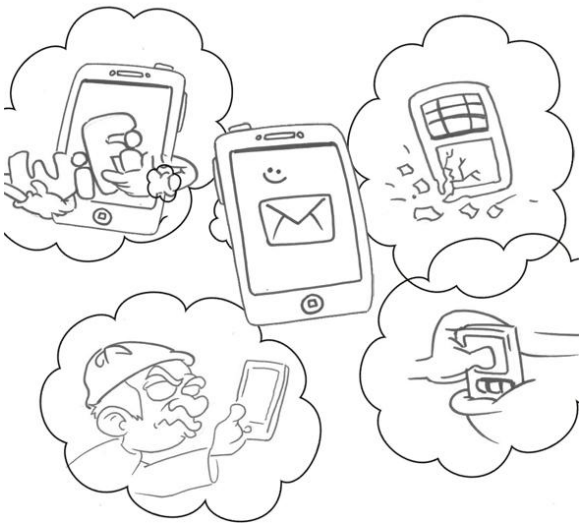
3. ما نوع المشاكل التي قد تواجهها إذا فقدت هاتفك الذكي؟

4. إذا فقدت هاتفك النقال، فكم ستأخذ من الوقت لتتمكن من إسترجاع قائمة الإتصال الخاصة بك؟

مخاطر إستخدام الأجهزة النقالة

إن إمكانية حمل هاتف يحمل كل أسماء وأرقام من تعرفهم وصور وأناشيد وكتب وأفلام فيديو ووثائق إلى جانب الإتصال بالإنترنت لشئ رائع. ولكن قبل عشر سنوات لم يكن الكثير من الناس يعتقدون أنه سيكون ممكناً فعل ذلك. والمدهش أن تلك الأجهزة تتطور أكثر بمرور الوقت فتصبح أسرع وأصغر وأسهل في الإستخدام. الأمر الذي يجعل معظمنا يعمل على تلك الأجهزة ليس فقط بعيداً عن الأجهزة المكتبية ولكن بعيداً عن أي مكتب ومكان عمل. بالتأكيد رأيت العديد من الأشخاص الذين يقومون باستخدام أجهزتهم النقالة في الأماكن العامة ولكن هذا الأمر يعنى تعرُض المعلومات الموجودة على تلك الأجهزة للمخاطر و للضياع أو التلف.

ما الذي يمكن أن يحدث لهاتفك الذكي أو حاسبك النقال؟



- من الممكن أن يضيع الجهاز وبالتالي ضياع المعلومات الموجودة عليه.
- من الممكن أن يسقط منك الجهاز أو يتلف بشكل كامل.
- من الممكن إلتقاط المعلومات عن طريق الشبكات اللاسلكية العامة.
- من الممكن أن يراقبك أحد من الناس وأنت لا تدري ليرى ما تقوم به على الجهاز.

لنلقي الآن بنظرة على النقاط السابقة، وكيف يمكن أن تؤثر علينا.

فقدان الجهاز

ماذا لو نسيت هاتفك الذكي عند أحد أصدقائك الذي يسكن خارج المدينة؟ هذا يعني أنك لن تستطيع استخدام الهاتف لبعض الوقت وقد يكون ذلك مزعجاً بالنسبة لك، لأنك لن تستطيع إجراء المكالمات الهاتفية أوإرسال وإستقبال الرسائل النصية. وعندها ستضطر لقراءة رسائل البريد الإلكترونى على حاسبك الآلي.

والآن تخيل أنك نسيت حاسبك النقال عند صديقك وبه معلومات أنت في حاجة لها بشأن مشروع مدرسي. أصبحت المشكلة الآن أكبر من مجرد "إزعاج" لأن هذا الأمر سيؤثر على قدرتك على إنهاء المشروع.

هناك العديد من رجال الأعمال الذين يستخدمون أجهزة مثل الهواتف الذكية والحواسيب النقالة والحواسيب اللوحية. إن ضياع الجهاز ولو ليوم أو يومين، يعني مشكلة كبيرة لهم. وإذا كان الجهاز يحتوي على المعلومات الخاصة بأعمالهم فبالتالي سيؤثر ذلك على إنجاز وإتمام تلك الأعمال في وقتها.

سرقة المعلومات

من مخاطر ضياع الهاتف الذكي أو الحاسب الآلي النقال أن يجده شخص آخر ومن ثم يحصل على المعلومات التي توجد عليه. قد تكون خزنت عليه بعض المعلومات الخاصة مثل كلمات المرور ورقم بطاقتك البنكية ومعلومات أخرى شخصية و هامة، وبهذا الشكل يحصل عليها حين يلتقط جهازك.

قد يتعمد شخص ما سرقة الحاسب الألي النقال أو الهاتف الذكي الخاص بشخص آخر يعمل في إحدى الشركات الكبرى بهدف معرفة المعلومات السرية عن تلك الشركة التي يعمل بها. ومن الممكن أن يتم سرقة الجهاز لأنه ذو قيمة إذ يمكن بيعه بمبلغ كبير من المال، أو الإستفادة من المعلومات الموجودة بداخله.

وما يجعل سرقة تلك الأجهزة شئ خطير هو عدم حمايتها جيداً بكلمة مرور أو إقفال الشاشة. فإذا وجده أحد من الناس سيتمكن بكل سهولة من الإطلاع على ما بداخل الجهاز من معلومات.

تلف الجهاز

إذا تلف الجهاز بالكامل بشكل لا يمكن استخدامه مرة أخرى، فهذا يعني فقد وضياع كل المعلومات والبيانات على هذا الجهاز. وكما ذكرنا من قبل أن فقد جهازك والمعلومات التي بداخله قد ينتج عنه العديد من المشاكل التي من المؤكد بعدم رغبتك في الوقوع فيها. إذن تلف هاتفك الذكي هذا يعني عدم القدرة على إنجاز أعمالك أو وصولك للمعلومات التي عليه أو فتح بريدك الإلكتروني. ولن تستطيع الإتصال بولي أمرك وستفقد أرقام كل من تعرفهم.

قد يتلف الجهاز بالكامل إذا تم سكب أي سائل عليه أو وقع على الارض. فإذا لم تحافظ على أجهزتك الإلكترونية قد تفقد كل ما يحتويه الجهاز من ملفات ومعلومات مخزنة أو تفقد الجهاز بالكامل بما فيه.

الإهمال

حين تستخدم جهازك في الأماكن العامة، فمن الممكن أن يرى أو يسمع أي شخص ما تقوم به وأنت لا تشعر. من الجائز أن يتحدث رجال الأعمال عن أسرار العمل أو ذكر أسماء الشركات والزبائن الذين يتعامل معهم. وقد يكون أحد المنافسين في نفس قطاع الاعمال يجلس بالجوار ويستمع لما يُقال، أو أن يكون شخص ما في القطار ويذكر كلمة المرور الخاصة به أثناء التحدث لأحد ممثلي البنك الذي يتعامل معه وهذا يعني الإفصاح عن معلومات قيمة لمن حوله من راكبي القطار.

وكذلك العمل على الحاسب الآلي النقال في الأماكن العامة أمر له خطورته. فإذا كنت تقوم بإدخال كلمة السر الخاصة ببريدك الإلكتروني أو حسابك البنكي، قد يكون هناك من يراقب شاشتك وأنت لا تدري. فكن حذراً عند التعامل مع المعلومات الشخصية أو الخاصة في الأماكن العامة.

شبكات الإنترنت اللاسلكية العامة Public Wi-Fi

هناك العديد من المقاهي والفنادق وغيرها من الأماكن العامة التي توفر خدمة الإنترنت اللاسلكي مجاناً. ولكن تداوُل المعلومات على تلك الشبكات يعرضها للكشف من قبل آخرين ممن يعملون على نفس الشبكة. يستخدم جهاز توزيع المعلومات اللاسلكي موجات الراديو التي تنتقل عبر الهواء. وهناك بعض البرامج المجانية التي يمكن استخدامها لكشف المعلومات المتنقلة عبر الشبكة اللاسلكية. فإذا كنت تزور بعض المواقع العادية أو تلعب ألعاب على الإنترنت، فليس هناك مشكلة. ولكن ماذا لو كنت تقوم ببعض العمليات المصرفية في حسابك البنكي على الموقع الرسمي للبنك، أو تقوم بإدخال كلمة المرور الخاصة ببريدك الإلكتروني؟ قد يكون هناك من يراقب موجات الشبكة اللاسلكية تلك، وبالتالي يمكنه الإطلاع على كل ما تقوم أنت به من عمليات الكترونية.

المقلق في استخدام الناس لشبكات الإنترنت اللاسلكية أنهم لا يعتبرونها مصدراً لأي تهديدات أمنية، في حين إذا تم تناقل معلومات شخصية أو خاصة على هذه الشبكات، فقد يشكل ذلك خطراً على صاحبها.

احمي نفسك عند استخدام الأجهزة النقالة

لقد ناقشنا فيما سبق أهم المخاطر المحيطة باستخدام الأجهزة النقالة، فلنستعرض معاً طرق الحماية أثناء استخدامها.

احرص أن يكون جهازك دائماً معك

لا تترك هاتفك الذكي أو حاسوبك النقال بأي مكان دون الإنتباه له بحيث يكون عرضة للسرقة أو أن تنساه في مكان ما. فمن الممكن نسيان أي شئ إن تركته دون انتباه في أي مكان ما ولم تضعه في جيبك أو حقيبتك. ودائماً تذكر أن ضياع الجهاز يعني ضياع ما عليه. بماذا ستشعر إذا فقدت كل ملفاتك الهامة على حاسوبك النقال أوصورك والأغاني المفضلة لديك الموجودة على هاتفك الذكي ؟

تشغيل خاصية إقفال الشاشة على الجهاز النقال

جميع الأجهزة النقالة بما فيها الهواتف الذكية والحاسبات الآلية النقالة تسمح بإقفال الشاشة أو حفظ الشاشة الذي يتطلب إدخال كلمة مرور لفتحها واستخدام الجهاز مرة أخرى. قم بتفعيل تلك الخاصية، وبهذه الطريقة لن يتمكن أحد من الحصول على المعلومات الموجودة على الجهاز في حالة ضياعه. واحرص أن تكون كلمة السر صعبة التخمين على الآخرين وسهلة التذكر بالنسبة لك. لا تستخدم كلمات مرور مثل 0000 أو 1234 أو password، فهذه جميعها أشهر كلمات المرور سيحاول من استولى على جهازك تجربتها أولاً.

عمل نسخة إحتياطية من المعلومات الموجودة على أجهزتك

يجب أن تقوم بعمل نسخة إحتياطية لجميع المعلومات والملفات الموجودة على أجهزتك مرة كل شهر على الأقل. بالنسبة لهاتفك الذكي، قد تحتاج لتوصيله بالحاسب الآلي ليقوم الحاسب بعمل النسخة الإحتياطية. وقد تحتاج لحاسب آلي أخر أو قرص صلب نقال لعمل نسخة إحتياطية لحاسبك النقال. وبهذه الطريقة إن تعرض أي من أجهزتك النقالة لأي ظرف طارىء أدى لفقد المعلومات المخزنة عليه، فلا تقلق لأنك قمت بعمل نسخ إحتياطة لها.

احرص على تحديث جهازك أولاً بأول

يجب تحديث برامج التشغيل والبرامج الموجودة على حاسوبك النقال أو هاتفك الذكي بإستمرار. قم بإجراء التحديثات مرة كل شهر على الأقل. قد تعتقد أن التحديثات تزود جهازك بالمميزات الجديدة ، ولكنها تقوم كذلك بمعالجة المشاكل وتسد الثغرات التي تحاول البرامج الخبيثة لإختراق جهازك.

وأهم أمر يجب أن تقوم به هو الحرص على تشغيل برنامج مكافحة الفيروسات وتحديثه بانتظام، ليتمكن من كشف الفيروسات أو البرامج الخبيثة قبل إختراقها أو مهاجمتها لجهازك.

كن حذراً بشأن الأماكن التي تستخدم فيها جهازك

يمكنك استخدام جهازك النقال في الأماكن العامة إذا لم تكن تعمل على المعلومات الشخصية أو الخاصة. يمكنك تفَقُّد المواقع الإلكترونية أو إرسال الرسائل النصية أو متابعة بريدك الإلكتروني. ولكن لا تقم بالعمل على حسابك البنكي الإلكتروني أو أي مواقع خاصة لاسيما حين تتصل بالإنترنت عن طريق شبكات الإنترنت العامة.

احرص ألّا يسمعك أحد عند التعامل مع المعلومات الخاصة والسرية، وألا يطلع الآخرين على شاشات أجهزتك أثناء تواجدك في الأماكن العامة.

استخدم الوسائل الآمنة للتواصل

لقد ناقشنا من قبل برتوكول HTTP عندما تحدثنا عن المواقع الإلكترونية. يمكن أيضاً استخدام البريد الإلكتروني عن طريق الوسائل الآمنة. هناك العديد من الهواتف بها إعدادات معينة للبريد الإلكتروني التي تستخدم SSL. إستخدم برتوكول SSL لبريدك الإلكتروني إذا أمكن، لأنها ستحفظ لك كلمة المرور وتحفظ لك سرية وخصوصية رسائل بريدك الإلكتروني.

كيف تُستخدم الأجهزة النقالة – 1
(مجموعة عمل)

قم بعمل دراسة مسحية على طلاب فصل آخر غير فصلك. صمم بنفسك الأستبيان الذي ستوزعه على الطلاب ، والذي يحوي الاسئلة التالية:

1. كم شخصاً في الفصل يمتلك هاتفاً ذكياً؟
2. ما هي الأماكن المفضلة للطلبة لإستخدام الهاتف الذكي؟
3. ما هي أهم الأماكن التي يحتاجون لإستخدام الهاتف الذكي بها؟
4. كم شخصاً يستخدم خاصية إقفال الشاشة وكلمة مرور لفتحها؟
5. كم شخصاً يمتلك حاسب آلي نقال؟
6. ما هي الأماكن المفضلة لإستخدام الحاسب الآلي النقال؟
7. ما هو أهم مكان يحتاجون لإستخدام الحاسب الآلي النقال به؟
8. كم شخصاً يستخدم كلمة مرور لفتح حاسبه النقال؟
9. كم شخصاً يستخدم حافظ للشاشة الذي يطفئ آليا بدون تدخلهم؟
10. كم شخصاً يستخدم كلمة مرور لحافظ الشاشة؟

اكتب تقريراً يوضح نتائج الدراسة المسحية، مع رسم بياني يوضح تلك النتائج.

كيف تُستخدم الأجهزة النقالة - 2

قم بدراسة مسحية عن أفراد عائلتك وأصدقائك من خارج المدرسة.

1. كم شخصاً في الفصل يمتلك هاتفاً ذكياً؟
2. ما هي الأماكن المفضلة لهم لإستخدام الهاتف الذكي؟
3. ما هي أهم الأماكن التي يحتاجون لإستخدام الهاتف الذكي بها؟
4. كم شخصاً يستخدم خاصية إقفال الشاشة وكلمة مرور لفتحها؟
5. كم شخصاً يمتلك حاسب آلي نقال؟
6. ما هي الأماكن المفضلة لإستخدام الحاسب الآلي النقال؟
7. ما هو أهم مكان يحتاجون لإستخدام الحاسب الآلي النقال به؟
8. كم شخصاً يستخدم كلمة مرور لفتح حاسبه النقال؟
9. كم شخصاً يستخدم حافظ للشاشة الذي يطفئ آليا بدون تدخلهم؟
10. كم شخصاً يستخدم كلمة مرور لحافظ الشاشة؟

اكتب تقريراً يوضح نتائج الدراسة المسحية، مع رسم بياني يوضح تلك النتائج.

نصائح سريعة

ابحث عن سياسة الخصوصية الموجودة على المواقع التي تقوم بزيارتها دائماً لتتعرف على نوع المعلومات التي يتم جمعها وكيفية استخدامها. وإذا لم تعجبك سياسة جمع المعلومات الخاصة بأي موقع، لا تزودهم بأي معلومات شخصية أو خاصة، مثل عنوان البريد الإلكتروني أو أرقام الهواتف والاتصال.

- لا تُدخل عنوان بريدك الإلكتروني بأي موقع إلّا في حالات الضرورة فقط.
- راجع آراء وتعليقات الزوار والمشترين السابقين للموقع قبل الشراء منه لتزداد معرفة ايجابيات وسلبيات هذه الموقع، وتأكد أنه له سمعة طيبة ويتعامل مع المشكلات بشكل مناسب.
- احرص على وجود وسائل للتواصل مع الموقع إذا صادفتك أي مشكلة.
- عند التسوق على الإنترنت، تأكد من وجود وصلة آمنة بين المتصفح والموقع ، وذلك بالتأكد من وجود بروتوكول https بجوار عنوان الموقع قبل إدخال بيانات البطاقة البنكية والشخصية. تحقق من أن الموقع قانوني باستخدام الطرق المتوفرة في المتصفح الخاص بك.
- راجع حسابك البنكي بإستمرار للتأكد من عدم وجود أي تعاملات مالية إضافية غير التي قمت بها.
- لا ترد على أي رسائل بريد إلكتروني تطلب منك معلوماتك الشخصية أو المعلومات الخاصة.
- لا تضغط على الروابط المرفقة برسائل البريد الإلكتروني.
- لا تفتح الملفات المرفقة برسائل البريد الإلكتروني المرسلة من الغرباء.
- احرص على تشغيل برنامج مكافحة الفيروسات وتحديثه أولاً بأول.
- لا تخالف القواعد – التي يطمع المهندس الإجتماعي منك القيام بها.
- استخدم كلمات مرور لتأمين كل أجهزتك الإلكترونية الثابتة والنقالة.
- انتبه لأجهزتك النقالة طوال الوقت ولا تتركها في أي مكان دون انتباه.
- قم بعمل نسخ إحتياطية لمحتويات جهازك بشكل دوري تحسباً لأي موقف قد تتعرض فيه محتويات الجهاز للضياع.
- قم بتحديث جهازك باستمرار لعلاج أي مشاكل لنظام التشغيل لتضييق الفرص على المخترقين والبرامج الخبيثة من إختراق جهازك.
- تجنب الحديث عن البيانات الشخصية والمعلومات الخاصة أثناء التواجد بالأماكن العامة.
- احرص ألّا يلاحظك أحد وأنت تستخدم جهازك النقال، وعندما تقوم بإدخال كلمات المرور أو أي بيانات شخصية أخرى.

إختبر معلوماتك	

1. ما أهمية مراجعة سياسة الخصوصية الموجودة على المواقع التي تعتاد زيارتها؟

2. لكل نوع من المعلومات التالية، اكتب بأسلوبك مخاطر تزويد المواقع بهذه المعلومات.

المعلومات	سبب طلبها	المخاطر
اسم المستخدم وكلمة المرور	تحتفظ بخصوصية حسابك الإلكتروني ومعرفة ما تفعله وما تقوم بزيارته	
عنوان البريد الإلكتروني	إرسال إشعارات بخصوص كل ما هو جديد، إلى جانب إرسال الإعلانات والمنتجات الجديدة.	
عنوان المنزل	إرسال الهدايا والمراسلات والعروض الخاصة وشحن ما قمت بشراءه من أي موقع أو محل تجاري.	
المفضلات	تظهر لك المعلومات التي قد تجذب إنتباهك.	

3. لماذا يجب عليك مراجعة آراء وتعليقات الزوار السابقين للموقع الذي تنوي التسوق منه قبل القيام بشراء أي شئ؟ اختر الإجابة الصحيحة فقط.
   أ. لتتعرف على أشهر المنتجات والمعروضات.
   ب. لتعرف إن كان الموقع جدير بالثقة ويوفر الدعم.
   ج. لتعرف إن كانوا يقدمون أرخص الأسعار.
   د. كل ما سبق ليس بصحيح.
4. ما هو HTTPS؟ اختر الإجابة الصحيحة فقط.
   أ. HTTPSpeed – طريقة أسرع لعرض المواقع.
   ب. خطأ إملائي في كتابة بروتوكول HTTP.
   ج. إصدار من بروتوكول HTTP الذي يستخدم SSL لإخفاء المعلومات المرسلة من وإلى أي موقع إلكتروني.
5. ما هو التصيد الالكتروني؟ اشرح بأسلوبك.

6. ما هي أشهر الطرق التي تُقنع الناس بالرد على رسائل التصيد؟ إختر جميع الإجابات الصحيحة.
   أ. إغرائهم بالهدايا والجوائز.
   ب. إغرائهم بمبالغ كبيرة من المال.
   ج. إبلاغهم بأمر طارئ.
   د. يُطلَب منهم المساعدة.
   ه. يرسل لهم معلومات شخصية عنهم.
7. كيف تحمي نفسك من التصيد؟ اختر جميع الإجابات الصحيحة.
   أ. الرد على الرسائل التي تطلب البيانات الشخصية.
   ب. عدم الضغط على الروابط المرفقة بالرسائل الإلكترونية من الغرباء.
   ج. عدم فتح الملفات المرفقة برسائل البريد الإلكتروني من الغرباء.
   د. قم بتشغيل برنامج مكافحة الفيروسات وتحديثه أول بأول.

8. ما هي مخاطر الحديث عن المعلومات الخاصة والشخصية بالأماكن العامة؟. اختر جميع الإجابات الصحيحة.
   أ. لا يوجد أي مخاطر.
   ب. لا تعرف من يستمع إليك.
   ج. قد يسمعك أحد ما بدون علمك ويقوم باستخدام المعلومات للدخول على حسابك البنكي أو بريدك الإلكتروني أو أي أشياء خاصة أخرى.

9. كيف تقوم بحماية جهازك النقال؟ اختر جميع الإجابات الصحيحة.
   أ. استخدم كلمة مرور لإقفال الجهاز.
   ب. تشغيل إقفال الشاشة وحافظ الشاشة لجميع الأجهزة والحاسب الآلي.
   ج. تأكد من حمل جهازك معك باستمرار.
   د. قم بعمل نسخة إحتياطية على حاسب آلي آخر.
   ه. قم بتحديث جهازك والبرامج المتواجدة عليه أولاً بأول.

10. اشرح بأسلوبك أهمية تشغيل حافظ الشاشة للهاتف والأجهزة النقالة، وجهاز الحاسب الآلي.