توعية أمن المعلومات

ثقافة استخدام الإنترنت

بنك قناة السويس
SUEZ CANAL BANK

19093
www.scbank.com.eg

عملاؤنا الأفاضل،

يعتقد البعض أن حرية الإنترنت من الأمور المُسّلم بها لدرجة أنّ البعض قد ينسى أنّ هذه الحرية نفسها قد تتسبب في خسارة خصوصيته أو ربما أسوء من ذلك، ومع ارتباط الإنترنت الوثيق بالحياة اليومية أصبح من الضروري زيادة الوعي بطرق حماية نفسك ومعلوماتك أثناء استخداماتك وتصفحك الإنترنت أو ما يطلق عليه الشبكة العنكبوتية العالمية.

وإليكم بعض الاستفسارات المتداولة والردود عليها: -

هل هناك من يتتبع خطواتي على الأنترنت عن كثب؟

نعم الاحتمال قائم ولابد لكل شخص أن يعلم أن السلطات الأمنية في البلدان مالكة خوادم الانترنت العملاقة والتي تتيح لنا استخدامه تُدون جميع النشاطات على الشبكة العنكبوتية وبكل السبل الممكنة على قواعد بيانات عملاقة وتستخدم برامج متخصصة لتحليل تلك البيانات وتحولها الى صورة معلومات–وهو الهدف الأساسي لتحمل تكلفة تلك الخوادم وإدارتها، كما يمكنهم رصد بيانات أجهزة كمبيوتر شخصية معينة، والحصول على بيانات من شركات الاتصالات بطريقة غير مباشرة.

هل تنتهك خصوصيتك أثناء تصفح الإنترنت؟

ليس كافيًا أبدًا الوثوق بالمواقع الإلكترونية والمتصفحات ومزودي الإنترنت للقيام بذلك من أجلك، في الحقيقة يجب عليك التوقف عن الوثوق بهم لأنّ إعدادات الخصوصية الافتراضية على هذه الخدمات تفتقر إلى الأمان المطلوب فكل متصفح إنترنت يُرسل ملفات تعريف الارتباط أو ما يسمى أيضا الكوكيز (Cookies) إلى الكمبيوتر وهذه الكوكيز تُعطي معلومات حول الصفحات التي تم زيارتها ، والعديد من المواقع التي نزورها تترك هذه الكوكيز في أجهزة الكمبيوتر وعند زيارتنا لهذه الصفحة مرة أخرى يتعرف الموقع علينا وعلى الأوقات التي زرنا فيها هذا الموقع ومن الممكن الأماكن التي استخدمنا الكمبيوتر منها وتظهر إعلانات لشركات عن الصفحات التي قمت بزيارتها أو معلومات عن منتج معين كنت بصدد البحث عنه في الإنترنت، وبتقييم هذه المعلومات يُظهر برنامج التصفح الإعلانات التي ربما تكون تتناسب مع متطلباتي، مع العلم بأن الكوكيز يمكن إزالتها متى نريد.

(وسيتم إلقاء الضوء على جوانب الحماية التي يُمكن اتباعها مع الكوكيز في نشرة توعية أمن معلومات قادمة بإذن الله).

هل هناك جهة أخرى تتطلع على الصفحات التي أزورها في الإنترنت؟

لجمع مزيد من المعلومات عن سلوك المتصفحين تستخدم العديد من المواقع برنامج "Google Analytics" هذا البرنامج ينقل كل البيانات التي حصل عليها إلى شركة جوجل أيضا، وبالتالي فإن شركة جوجل تحصل على العديد من المعلومات من مصادر مختلفة ويُمكنها أن تُكون لكل مستخدم ملفا خاصا به.

ماذا يحدث إذا استخدمتُ الشبكة المحلية اللاسلكية (الواي فاي) في مقهى أو مطار للدخول إلى الإنترنت؟

تعد الشبكة المحلية اللاسلكية (الواي فاي) منفذ غير آمن للإنترنت لأنه بإمكان صاحب المقهى أو أي شخص متطفل أو مقدم هذه الخدمة بكل سهوله أن يتعرف عن كل الصفحات التي زارها زبائنه.

هل ينطبق هذا كذلك على شبكات التواصل الاجتماعي؟

المعلومات التي تجمعها شبكات التواصل الاجتماعي عني لا تعد ولا تحصى، وحساب المستخدم في شبكات التواصل الاجتماعي يظل مفتوحا طيلة الوقت رغم أنه يتصفح مواقع أخرى، وإذا ضغط مستخدم الفيس بوك مثلا على زر "أعجبني Like" فإن كل المعلومات المتواجدة في الكوكيز (ملفات تعريف الارتباط) تنتقل مباشرة إلى الفيس بوك، وبهذه الطريقة يحصل الفيس بوك هو الآخر على معلومات عن الصفحات التي أزورها على شبكة الإنترنت.

تقنيات الخدع الاجتماعية: –

الخدع الاجتماعية ببساطة هي فن الوصول الى معلومات حساسة عن أنظمة الكومبيوتر او البيانات الشخصية وكلمة السر من مستخدمي النظام ويتم ذلك عادة بإقناع المستخدمين بأن المتحدث هو شخص مسموح له بالحصول على هذه البيانات مثال ذلك يقوم هذا الشخص بالاتصال التليفوني ومحاولة تعريف نفسه وإقناعك بأنه ممثل للبنك ويناقش معك بعض التفاصيل الخاصة والمعلومات السرية لحساباتك البنكية، أو قد تكون في صورة رسالة بريد الكتروني من مصدر مجهول ولزيادة اتقان الاحتيال يقوم الهاكر المحتال بمحاولة كسب ثقة المستخدم ودفعه لتحميل الملف الماكر المدرج برسالته بعدة طرق منها على سبيل المثال ارسال ملف مرفق في صورة جدول (Excel) تحت عنوان (كيفية احتساب زكاة المال (، او طلب تحديث لبرامج مثل اكروبات ريدر (Adobe Reader) ، ,,,,, الخ

بمجرد تحميل المستخدم لتلك الملفات على الجهاز يتم تشغيل برنامج خفي على جهاز الحاسب الخاص بك يشفر كافة الملفات الموجودة عليه، وتصبح غير مقروءة، ويقوم ايضا بتغيير اسم كل ملف لعدم الاستدلال عليه، ثم يرسل رسالة للمستخدم لابتزازه ماليا ويطلب دفع مبلغ مالي في حساب يحدده لاسترجاع ملفات المستخدم بصورة مقروءة.

كلمة السر ؟

تعد كلمة السر مفتاح المعلومات الخاصة بحسابك على الانترنت. تجنب استخدام نفس كلمة السر للعدد من الأنظمة المختلفة وتتمثل أهمية ذلك في أنه إذا فعلت ذلك فإنك بذلك قد توسع منطقة الخطر وتسهل عملية الاختراق والانتهاك من القراصنة وتعرض أموالك للخطر، فقد يكتشف شخص ما كلمة السر الخاصة بك لهذا السبب، ولذا ننصحك بشدة بجعل كلمة سر مختلفة لكل نظام، مع استخدام كلمة سر قوية (لا يقل طولها عن ثمانية حروف وأرقام، حرف او أكثر منهم على الوضع الحروف الكبيرة Caps Lock Button، واستخدم أحد الرموز الخاصة بلوحة المفاتيح مثل $ أو # أو % مثلا)

وعليك أيضا أن تأخذ الأمور التالية بعين الاعتبار عند اختيار كلمة سر قوية:

- أن تكون مختلفة – تجنب استخدام نفس كلمة السر في أي خدمات أخرى.
- ألا تكون شخصية – لا تلجأ إلى استخدام كلمة سر يمكن تخمينها بسهولة؛ كأن تكون أسماء لأطفالك أو زوجتك او الحيوانات أو تواريخ الميلاد أو أرقام الهاتف.
- لا تقم بكتابتها مطلقا – ننصحك بشدة ألا تكتب كلمة السر أو تقوم بتسجيلها مطلقا، وإذا لم تكن أمامك طريقة أخرى سوى كتابتها فحاول أن تضمن كتابتها أو تسجيلها بطريقة تجعلها غير مفهومة لأي شخص آخر.

الإنترنت الآمن

يرجى العلم بأن موظفي بنك قناة السويس لا يقومون بالاتصال بكم لمعرفة التفاصيل السرية الشخصية مثل: رقم التعريف الشخصي، رقم التعريف الهاتفي، كلمة المرور السري، أو الثلاث أرقام الموجودة على ظهر بطاقة الائتمان وفي حالة تلقيكم أي مكالمات هاتفية تطلب منكم معلومات شخصية، نرجو منكم عدم الإدلاء بأية معلومات والاتصال فوراً بمركز خدمة العملاء على الفور على رقم ١٩٠٩٣ +٢٠٢.

أوضاع الحماية:

عندما تدخل على موقع البنك يشار إلى أنه في وضع استخدام آمن، وتستطيع أن تعرف ذلك إذا كان عنوان الوصلة تبدأ بـ //https أو كان رمز القفل يظهر بجانب عنوان الوصلة بلون أخضر كما بالشكل التالي:

التشفير

تستخدم تكنولوجيا تشفير (SSL) عند الدخول على المعلومات البنكية لتشفير المعلومات الشخصية وجعلها آمنة قبل مغادرة الجهاز لتضمن ألا يقرأها أي شخص آخر ووفق إعدادات المتصفح سوف تظهر لك صفحة منبثقة لإخبارك بأنك قد دخلت على صفحة تتمتع بالحماية، وتقوم عملية التشفير بتحويل بياناتك الخاصة على شكل شفرات قبل إرسالها على الانترنت وبذلك لا يتاح لمستخدمي الانترنت غير المسموح لهم بقراءة هذه البيانات، وفي بنك قناة السويس نستخدم طبقات التشفير الآمنة والتي تعد مقبولة طبقا لمعايير التشفير.

وقت الاستراحة في وضع الحماية

في حالة إذا نسيت إغلاق الصفحة والخروج من الموقع بعد دخولك على معلوماتك البنكية أو في حالة ما إذا أصبح الكمبيوتر غير نشط لفترة من الوقت أثناء وضع الحماية، فإن نظامنا سوف يقوم تلقائيا بإغلاق الصفحة والخروج منها لكن نوصيك بإغلاق الصفحة فور انتهائك من تصفحها.

التكنولوجي

إننا نستخدم العديد من طبقات الحماية وبالطبع لا يمكن الإفصاح عنها كاملة ولكن الوسائل التالية تستخدم بشكل مثالي:

- يتم تحديث كافة البرامج المضادة للفيروسات بشكل منتظم
- نستخدم حواجز متعددة لمنع الدخول بغير إذن
- لدينا مراكز معلوماتية أمنة
- يتم تحديث كافة أنظمة التشغيل بشكل منتظم مع أحدث ملفات الحماية

خصوصية بيانات الهوية

نستخدم كلمات السر وبيانات الدخول، وكذلك يمكن أن نستخدم أجهزة تأكيد الهوية المساعدة Token –أجهزة رموز الأمان لكلمات السر التي تستخدم لمرة واحدة –لنكون متأكدين من أننا نتعامل معك، ويكون الدخول على حسابك الخاص ممكنا فقط في حالة تأكيد هويتك واستخدامك الاسم وكلمة السر الصحيحين الخاصين بك لدي البنك، ولهذا السبب فإنه من الأهمية بمكان عدم إفشاء كلمة السر الخاصة بك لأي شخص وتأمين الأجهزة المساعدة التي بحوزتك والتي تستخدم في تأكيد الهوية سواء التليفون المحمول او أجهزة رموز الأمان Token.

الإغلاق التلقائي

بعد عدد من المحاولات غير الصحيحة للدخول، فإنك لن تصبح قادرا على الدخول لحسابك، وحتى تستطيع إعادة تنشيط حسابك مرة أخرى عليك الاتصال برقم المساعدة في البنك.

"الحماية على الانترنت واجبات ومسئوليات شخصية"

وإضافة لهذه الإجراءات من الحماية فإنك أيضا تلعب دورا هاما في حماية معلوماتك الشخصية فهناك الكثير الذي يمكنك فعله لحماية نفسك أثناء اتصالك على الانترنت.

ولكي تبدأ عليك بإتباع القواعد الهامة التي ذكرناها آنفا والقواعد التالية:

من فضلك ضع في اعتبارك هذه التفاصيل الهامة التالية

- حافظ على سرية بياناتك الشخصية
- حافظ على سرية كلمة السر الخاصة بك
- حافظ على حماية الحاسب الشخصي وتليفونك المحمول
- حافظ على أجهزة تأكيد الهوية حوزتك
- حافظ على وضع الحماية عند الدخول على حسابك على الانترنت
- حافظ على سرية بريدك الالكتروني
- حافظ على سرية معلوماتك – حتى في حالة عدم اتصالك بالأنترنت
- عدم الانجراف وراء فتح الروابط المجهولة المصدر والغير موثوقة لتجنب وقوعك ضحية لهجمات E–Phishing من خلال حقن جهازك بأكواد برمجية خبيثة.
- تحميل وتنصيب أنظمة مكافحة الفايروسات والملفات الضارة على أجهزة الهاتف الذكي الخاص بك وخصوصاً عند استخدامك للشبكات اللاسلكي.
- إغلاق خاصية الواي فاى والبلوتوث بأجهزتك الخاصة أثناء تواجدك في الأماكن العامة.

بعض التهديدات
وما علينا أن نفعله ..

المواقع المزيفة:

هناك مواقع تبدو كالأصلية تم تصميمها على أيدي المزورين لتشبه كثيرا المواقع المحترمة الأخرى مثل موقعنا مثلا وهي تجذب عددا من الأشخاص لتلك المواقع من خلال تصيد البريد الالكتروني ودائما ما يطلبون معلومات شخصية سرية.

ماذا نفعل؟

- تأكد من أنك متصل بالموقع الرسمي لبنك قناة السويس وهذا الموقع هو www.scbank.com.eg وذلك قبل قيامك بإدخال أية معلومات شخصية
- لا تقم بالدخول على حسابك البنكي مباشرة بواسطة وصلات تأتيك عبر البريد الالكتروني
- قم بكتابة اسم الموقع www.scbank.com.eg في عنوان المتصفح أو قم بالدخول من خلال علامة مكتبية.
- حاول فحص رمز الإغلاق (الحماية/ شكل القفل) وأنه باللون الأخضر بالشاشة
- تأكد من أن وضع حماية المتصفح موجود من بنك قناة السويس وذلك بتأكيد المعلومات مثل الإصدار والتاريخ على شهادة السرية والحماية
- عليك بتغيير كلمة السر التي تستخدمها للدخول إلى حسابك البنكي بشكل منتظم
- يجب التأكد دائمًا من الاسم الدقيق للتطبيقات الإلكترونية الخاصة ببنك قناة السويس والذي سيكون فريدًا وغير متكرر–مثل تطبيق خدمة المحفظة الإلكترونية "SCB E–Wallet" وذلك أثناء تحميل تلك التطبيقات من متاجر التطبيقات عبر الانترنت.

التصّيد:

ويحدث هذا عندما يرسل المحتالون رسائل ماكرة بشكل عشوائي، وتظهر هذه الرسائل على أنها مرسلة من مصدر له شرعية مثل بنك قناة السويس وقد يطلب منك أن تؤكد بعض المعلومات الهامة جدا مثل رقم حسابك وكلمة السر الخاصة بك ورقم الكود.

ماذا نفعل؟

- لا تفعل شيئا إلا بعد تأكدك بشكل تام من الصفة الشرعية لهذا المرسل وشرعية الطلب الذي يطلبه
- كن على يقين بأن بنك قناة السويس لن يطلب من العملاء مطلقا إعطاء أية بيانات سرية هامة عن حسابهم البنكي من خلال رسائل بريدية
- لا تعطي أية ردود لمثل هذه الرسائل التي تطلب منك مثل هذه المعلومات ولا تقم بالضغط على أية وصلات داخل أي من هذه الرسائل
- عليك بتحديث البرامج المضادة للفيروسات وتغيير كلمة السر الخاصة بدخولك على حسابك البنكي وتغييرها بشكل منتظم لحماية بياناتك الشخصية والحفاظ عليها

برامج ماكرة لتهديد الحاسبات:

الفيروسات الحاسوبية: هي عبارة عن برامج حاسوبية والتي ترتبط مع برامج حاسوبية اخرى أو ملفات بيانات من اجل تنفيذها بطريقة خاطئة.
البرامج الدودية: هي برامج حاسوبية مستقلة تقوم بنسخ نفسها من كمبيوتر الى اخر عبر الشبكة.
برنامج حصان طروادة: هو برنامج في ظاهرة يبدو انه سينفذ شيء معين ولكن عند البدء يقوم بعمل اخر مضر بنظم المعلومات.
برامج التجسس: هي برامج حاسوبية تُحمَل بشكل سري على جهازك عبر الشبكة وتقوم بتسجيل كل ضغطة بلوحة المفاتيح التي استخدمت من اجل معرفة الكلمات السرية والارقام المتسلسلة.

ماذا نفعل؟

- قم بإنزال برامج مضادة للفيروسات، وبرامج الجدار الناري وأحزمة الأمان
- قم دائما بتشغيل برنامج مضاد للفيروسات قبل تحميل أية برامج أخرى أو فتح أية رسائل إلكترونية
- لا تفتح أي رابط او تحمل أي مرفق غير موثوق المصدر.
- قم بتحديث البرامج المضادة للفيروسات وغير كلمة السر الخاصة بحسابك البنكي بانتظام وذلك بهدف حماية بياناتك الشخصية.

توعية أمن المعلومات

ثقافة استخدام الإنترنت

بنك قناة السويس
SUEZ CANAL BANK

19093
www.scbank.com.eg