

فكرة عامة عن أمن الاتصال بالشبكة

أمن المعلومات هو مركز اهتمامنا

إن مصرف الراجحي ملتزم بالتأكد من أمن وسلامة معلوماتك التي تنتقل عبر الاتصال المباشر. on-line ومع وجود بنية مصرف الراجحي الأمنية التحتية التي تتمتع بأحدث ما توصلت إليه التقنية بالإضافة إلى الخاصية الأمنية المدمجة في المتصفح الخاص بك فإننا على ثقة من أن معلوماتك التي تتم عبر الاتصال المباشر ستحتفظ بسريتها وخصوصيتها من الأعين المتطفلة.

مسئوليتك أنت

بينما يبذل مصرف الراجحي كل ما في وسعه للحفاظ على سرية معلوماتك التي تتم عبر الاتصال المباشر إلا أن مصرف الراجحي لا يمكن أن يقوم بهذه المهمة بمفرده. فكما هو الحال تماماً في العالم الحقيقي حيث تتخذ أنت خطوات لحماية معلوماتك المالية فإنك ستحتاج إلى جعل سلامة اتصالاتك المباشرة من صميم خصوصياتك وفيما يلي بعض الخطوات الأساسية لحماية نفسك أثناء استخدامك لخدمات الاتصال المباشر مع مصرف الراجحي عبر الإنترنت .

الخطوات الخمس لأمن الاتصال المباشر

- 1- لا تكشف أبداً كلمة المرور أو الهوية الخاصة بخدمات الاتصال المباشر مع مصرف الراجحي إلى أي شخص إن كلمة المرور والهوية الخاصة بك قد وضعت للحفاظ على سرية معلوماتك المصرفية ولكنهما لا يكونان ذا جدوى إلا إذا حافظت على سريتهما. هناك برنامج خاص يراقب محاولات إختراق كلمات المرور هذه وهو لا يسمح إلا بالقليل جداً من المحاولات قبل أن تحتاج كلمة المرور إلى إعادة تفعيل. وإذا اعتقدت أن كلمة المرور الخاصة باتصالك المباشر قد تعرضت للخطر فما عليك إلا تغييرها فوراً.
- 2- لا تتباعد عن حاسبك الآلي الشخصي عندما تكون في حالة استخدام لأي من خدمات الاتصال المباشر التي يقدمها مصرف الراجحي.
- 3- عندما تنتهي من استخدام خدمات مصرف الراجحي الخاصة بالاتصال المباشر تأكد من إنهاء عملية اتصالك بالخدمات المباشرة وذلك بعمل خروج.
- 4- إذا كان لدى أناس آخرون إمكانية دخول على حاسبك الآلي قم بإفراغ ذاكرة متصفحك لإزالة نسخ من صفحات الشبكة التي قد يكون تم تخزينها بصفة مؤقتة في جهازك فالمتصفحات لديها المقدرة على تخزين المعلومات أي تتذكر صفحة أو صورة من شبكة وهذا يجعل تصفح الإنترنت أسرع لأنك عندما ترجع إلى صفحة في الشبكة قد زرتها من قبل فإنك لا تحتاج إلى طلب الصفحة من الخادم مرة أخرى . ارجع إلى ملف المساعدة الخاص بالمتصفح للحصول على تعليمات عن إفراغ الذاكرة.
- 5- إذا أرسلت رسالة بريد إلكتروني إلى مصرف الراجحي تذكر عدم تضمينها معلومات سرية أو شخصية. فمن المحتمل أن يتمكن الآخرون من قراءة البريد الإلكتروني الذي يرسل بواسطة الإنترنت .

إرشادات لإنشاء كلمة مرور آمنة

-استخدم علامات الترقيم و / أو إعداد

-استخدم مزيج من الأحرف الكبيرة والأحرف الصغيرة.

-استخدم بدائل تبدو مماثلة مثل الرقم صفر بالانجليزي (0) بديلاً للحرف (O) أو (\$) بدلاً عن الحرف.(s)

-انشئ لفظة من أوائل الكلمات لجملة معينة

-استخدم بدائل صوتية مثل " Luv2laf " بديلاً عن " love to laugh "

أخطاء يجب تفاديها

- لا تستخدم كلمة مرور واردة كمثال لاختيار كلمة مرور جيدة.
- لا تستخدم كلمة مرور تحتوي على معلومات شخصية (الاسم ، تاريخ الميلاد ، الخ)
- لا تستخدم كلمات يمكن الحصول عليها من القاموس.
- لا تستخدم أنماط لوحة مفاتيح (asdf) أو أرقام متسلسلة (1 2 3 4)
- لا تجعل كلمة مرور كلها أعداد ، أو كلها أحرف كبيرة أو كلها أحرف صغيرة.
- لا تستخدم أحرف متكررة .(aa 11)

إرشادات للحفاظ على أمن كلمة المرور

- لا تخبر أي شخص بكلمة مرورك.
- لا تكتب كلمة مرورك مطلقاً.
- لا ترسل كلمة مرورك بالبريد الإلكتروني مطلقاً.
- قم بتجربة كلمة مرورك الحالية دورياً و غيرها بكلمة جديدة بانتظام .

أمن المتصفح الخاص بك

تستخدم خدمات مصرف الراجحي الخاصة بالاتصال المباشر تشفير

قوي 128 bit SSL-أثناء اتصالاتك المباشر وذلك للحفاظ على سرية معلوماتك. التشفير في الأساس عبارة عن طريقة مطورة لتفكيك و خلط معلوماتك التي ترسلها عن طريق الاتصال المباشر قبل مغادرتها لجهاز الكمبيوتر الخاص بك بحيث أنه إذا تم اعتراضها تكون غير مقروءة تماماً. ونحن نطلب بأن يدعم متصفح الشبكة الخاص بك التشفير 128 بت لأنه أقوى من التشفير 40 بت ثلاثمائة مرة تقريباً. وفي حين نجد أن التشفير 40 بت قد يكون لا بأس به للتعاملات ذات المستوى المنخفض من المخاطر لكن يتفوق جميع مختصي الأمن على أنها غير كافية لحماية التعاملات المالية.

عندما تطلب معلومات بواسطة خدمة الاتصال المباشر للراجحي على الانترنت فإن طلبك يتم تشفيره أثناء انتقاله بعد ذلك نقوم بفك شفرة طلبك وإعادة الرد إليك مرة أخرى مشفراً بطريقة آمنة. وعندما تستقبله فإن متصفحك يقوم بفك شفرة المعلومات وعرضها.

يمكنك أن تتعرف على أن معلوماتك المنقولة مشفرة في متصفحات مايكروسوفت بظهور صورة لقفل مغلق في أسفل الزاوية اليسرى(أو اليمنى) من الشاشة يظهر أثناء الاتصال.

نوصي بشدة بأن تستخدم أحدث نموذج من متصفحك المفضل. إن النموذج الأحدث من متصفحك المفضل متاح عادة من شبكة الشركة الصانعة للمتصفح نفسه.

إن النماذج الأحدث من المتصفحات هي أكثر أماناً من النماذج الأقدم وهي مهمة بصفة خاصة عند القيام بتعاملاتك المصرفية عبر الإنترنت.

إن معظم أجهزة الحاسب الشخصية المبنية على ويندوز مزودة مسبقاً بمستكشف Explorer مايكروسوفت للإنترنت لذلك فهو المتصفح الأكثر شيوعاً من حيث الاستخدام . ولهذا السبب فإن مستكشف الإنترنت هو المتصفح الأكثر عرضة للهجوم من قبل الفيروسات وبرامج التجسس.

إذا استخدمت متصفح إنترنت من المهم بصفة خاصة أن تشغل برنامج مكافحة الفيروسات وبرامج التجسس بصورة منتظمة وتحديثه بانتظام. واحرص أيضاً على تحميل جميع التحديثات المتاحة من مايكروسوفت .

سرقة الهوية

إن سرقة الهوية والاحتيال على الهوية هي عبارات تستخدم للإشارة إلى كافة أنواع الجرائم التي يحصل فيها شخص ما على معلومات شخصية خاصة بشخص آخر بطريقة ما تشتمل على احتيال أو خداع لكسب اقتصادي في الأساس.

إن سرقة الهوية والاحتيال على الهوية هي عبارات تستخدم للإشارة إلى كافة أنواع الجرائم التي يحصل فيها شخص ما على معلومات شخصية خاصة بشخص آخر بطريقة ما تشتمل على احتيال أو خداع لكسب اقتصادي في الأساس.

يستخدم المحتالون المعلومات المقدمة بواسطة صفحات التحقق الاحتمالي هذه لاستخدام بطاقات الائتمان لعمليات شراء غير مصرح بها أو لا فراغ حسابات أو لبيع معلومات إلى عصابات سرقة الهوية.

هناك طرق وأساليب عديدة يمكن أن تحدث بها سرقة الهوية ولكن موضح أدناه الطريقتين الأكثر شيوعاً

Phising وهو عندما يرسل محتال رسائل (إلى عناوين بريد إلكتروني حصل عليها بصورة غير قانونية) متظاهراً بأنها من شركة أخرى (مثلاً البنك). والغرض من عناوين البريد الإلكتروني هذه هي انتزاع معلوماتك الشخصية التي يمكن أن يستخدمها المحتال بعد ذلك لارتكاب عملية احتيال باسمك. تذكر أن مصرف الراجحي لن يسأل أبداً عن اسم المستخدم أو كلمة المرور بواسطة البريد الإلكتروني.

Spoofing وهي عندما ما ينشئ محتال موقعاً على الشبكة يبدو مثل موقع حقيقي- كموقع مصرف الراجحي ولديه أيضاً عنوان موقع (URL) مماثل. بعد ذلك يرتكب عملية احتيال على الخط on-line وذلك بحث الناس على التعامل في هذا الموقع المزور (مثلاً إيداع مبلغ ، شراء سلع). تذكر إن عنوان موقع مصرف الراجحي هو <http://www.alrajhibank.com.jo> ولا تستطيع شركة أخرى استخراج نسخة من هذا العنوان .

ما هو الشيء الذي يجب أن تبحث عنه

الموضوعات الخادعة :

تبدو هذه الخطوط كأنها هي ترجع حقيقة إلى الشركة التي من المفترض أنها هي المرسل للبريد الإلكتروني.

عنوان المرسل المزور :

من طرق الخداع السهلة بحيث تجعل البريد الإلكتروني يبدو كأنه قادم من الشركة المزعومة.

محتويات شبه حقيقية :

إنهم ينسخون صور وهينة ونص المواقع الحقيقية لخداع الزائر وربما يكون لديهم روابط صحيحة بنظام سرية الشركة وصفحات أخرى على الموقع الشرعي لخلق نوع من الثقة.

روابط العناوين الخادعة : (hyperlink)

يمكن أن تعرض رسائل البريد الإلكتروني عنوان موقع حقيقي ولكن عندما تنقر عليه فإن الرابط سينقلك إلى موقع مختلف احذر من العنوان الطويلة فعندما تنقر عليها ستنتقل إلى الموقع الذي بعد الرمز. @

مثال:

<http://www.genuine-site.com-name@fraud-site.com>

إذا نقرت على هذه التوصيلة الفائقة سوف تنقلك إلى الموقع

<http://fraud-site.com> الذي بعد الرمز . @

إرشادات لحمايتك

لا تقدم أية معلومات سرية مثلاً رقم الحساب ، رقم التمييز الشخصي Pin ، كلمة المرور أو رقم تحقق عشوائي في أي مكان آخر غير صفحة انترنت مصرف الراجحي الرسمية لتسجيل التعاملات المصرفية.

قم بتفعيل وظيفة الأخطار الإشعار لمستخدمي الانترنت للتعاملات المصرفية وأحصل على الإشعارات من خلال نظام الرسائل القصيرة عندما يكون هناك نشاط في خدمة الانترنت المصرفية في أي وقت نهاراً أو ليلاً.

لا تنقر على الروابط في رسائل البريد الإلكتروني إذ قد يكون الرابط يحتوي على عنوان مختلف عن تلك الموضحة في البريد الإلكتروني إذ يمكن اخفاء العنوان داخل الرابط في البريد الإلكتروني بسهولة.

استخدم برنامج الفلترة لتقليص عدد رسائل البريد الإلكتروني الاحتمالية والضارة التي قد تتعرض لها.

استخدم برنامج مكافحة الفيروسات

استخدم جدار ناري Firewall شخصي

حافظ على تحديث البرنامج (الأنظمة التشغيلية ومتصفحات الشبكة)

أبحث دائماً عن وقفل padlock على مواقع الشبكة التي تتطلب معلومات شخصية. وعلى الرغم من أن ذلك لا يضمن أن يكون الموقع الذي أنت بصدد دخوله موقع حقيقي أو لا يضمن أنه آمن إلا أن غياب هذه الأشياء يشير إلى أن موقع الشبكة غير آمن بالتأكيد.

استخدم برنامج مكافحة التجسس.

تقف نفسك بمتابعة احدث الطرق لمكافحة الاحتيال على الانترنت.

راجع وراقب التقارير الخاصة بانتهاكك .

مزايا مصرف الراجحي الأمنية الأخرى

إننا بمصرف الراجحي نتابع بصورة وثيقة في كل مرة نتصل بنا للتأكد من أن المعلومات التي ترسل جينة وذهاباً مرسله إلى حاسبك الشخصي فقط. ولدينا جدار ناري Firewall وهو عبارة عن جهاز على مستوى عالي من التطور وبرنامج يقوم بالإطلاع على الرسائل الواردة والصادرة من مصرف الراجحي بحيث لا يستطيع العبور إلى نظام المصرف إلا المستخدمين المعتمدين وأي رسائل لا تنطبق عليها المتطلبات الأمنية الشديدة الصرامة يتم رفضها وبالتالي يتم إنهاء الاتصال المباشر وهذا النوع من التقية مصمم بحيث لا يستطيع قرصان الشفرة الأكثر تطوراً تدمير موقعنا أو الوصول إلى معلومات حسابك الخاص. ولمساعدتك على التأكد من أنك موصل حقاً بمصرف الراجحي أثناء جلسات اتصالاتك المباشر فإننا نستخدم نظام رقمي للتحقق من الهوية ونحن حاصلين على شهادة خادم رقمي من فيريساين - Verisign جهة الشهادات الرئيسية بالنسبة للانترنت . ويستخدم متصفحك نظام التحقق هذا في كل مرة تدخل فيها ليتيح لك التحقق أنك متصل بمصرف الراجحي. وكما قد يتبادر إلى ذهنك فلدينا عدد من الإجراءات الأمنية الأخرى لا تستطيع الحديث عنها ولكنها مصممة بحيث تكون خدماتنا في الانترنت آمنة وسرية .