مصرف الراجحي
Al Rajhi Bank

نظرة عامة على الأمان عبر الإنترنت

تركيزنا على السلامة

إن مصرف الراجحي ملتزم بالتأكد من أن معلوماتك على الإنترنت دائما آمنة ومحمية. مع وجود بنية تحتية أمنية متطورة على مستوى مصرف الراجحي، وبالإضافة إلى الأمان المضمن في المتصفح الخاص بك، فنحن واثقون من أن معلوماتك على الإنترنت خاصة وآمنة من أعين المتطفلين.

مسؤوليتك

على الرغم من قيام مصرف الراجحي بكل ما في وسعه لحماية سرية المعلومات الخاصة بك على الانترنت، فإنه لا يمكننا أن نتولى ذلك بمفردنا. كما هو الحال في العالم الحقيقي، حيث يمكنك اتخاذ خطوات لحماية المعلومات المالية الخاصة بك، سوف تحتاج إلى تولي مسألة سلامتك على الانترنت. فيما يلي بعض الخطوات الرئيسية لحماية نفسك أثناء استخدام خدمات مصرف الراجحي عبر الإنترنت:

5 خطوات الأمان عبر الإنترنت

1. لا تقم أبداً بكشف هوية المعرف وكلمة السر الخاصة بخدماتك في مصرف الراجحي عبر الإنترنت لأي شخص! لقد تم تصميم كلمة المرور ومعرف الهوية لحماية خصوصية المعلومات المصرفية الخاصة بك، ولكنهما لا يمكن أن يعملا إلا إذا حافظت على السرية. تتم مراقبة محاولات لكسر كلمات المرور هذه بواسطة برامج خاصة، والتي سوف تسمح فقط ببضع محاولات قبل أن تحتاج كلمة المرور إلى إعادة تعيين. إذا كنت تعتقد أن كلمة المرور الخاصة بك على الانترنت أو معرف تم اختراقها، قم بتغييرها على الفور!

2. لا تترك جهاز الكمبيوتر الخاص بك أثناء قيامك باستخدام أي من الخدمات عبر الإنترنت المقدمة من قبل مصرف الراجحي

3. عند الانتهاء من استخدام خدمات الراجحي عبر الإنترنت، تأكد من تسجيل الخروج من الصفحات الآمنة الخاصة بها. والا سيؤدي هذا إلى تسجيل الخروج تلقائيا من الجلسة

4. إذا كان هناك أشخاص آخرون يستطيعون الوصول إلى جهاز الكمبيوتر الخاص بك، قم بمسح ذاكرة التخزين المؤقت للمتصفح الخاص بك لإزالة نسخ من صفحات الويب التي قد تكون مخزنة مؤقتا على النظام الخاص بك، المتصفحات لديها القدرة على ذاكرة التخزين المؤقت المعلومات، وذلك لتذكر صفحة أو صورة من موقع على شبكة الانترنت. وهذا يجعل تصفح الإنترنت أسرع، فعند العودة إلى صفحة ويب قد تمت زيارتها سابقا، يمكن للمتصفح تقديم الصفحة مخزنة دون الحاجة إلى طلب الصفحة من الخادم مرة أخرى. راجع ملف التعليمات في المتصفح للحصول على إرشادات حول محو ذاكرة التخزين المؤقت

5. إذا أرسلت مصرف الراجحي رسالة بريد إلكتروني فتذكر عدم تضمين معلومات خاصة بك أو بحساباتك. فإنه يمكن للبعض أن يقرأ البريد الإلكتروني المرسل عبر الإنترنت

نصائح لإنشاء كلمة مرور آمنة:

1. استخدام الأحرف الكبيرة والصغيرة معاً

2. استخدام الحروف الهجائية والأرقام معاً (على سبيل المثال omega3ruh1)

3. إنشاء اختصار فريد من نوعه

4. تضمين بدائل لفظية، مثل "Luv2Laf" ل "Love2Laugh"

مصرف الراجحي
Al Rajhi Bank

أشياء يجب تجنبها:

1. لا تستخدم كلمة مرور مستخدمة كمثال لكيفية اختيار كلمة مرور جيدة
2. لا تستخدم كلمة مرور تحتوي على معلومات شخصية كـ (الاسم وتاريخ الميلاد وما إلى ذلك)
3. لا تستخدم الكلمات أو المختصرات التي يمكن العثور عليها في القاموس
4. لا تستخدم أنماط لوحة المفاتيح (asdf) أو أرقام متتابعة (1234)
5. لا تجعل كلمة المرور الخاصة بك كلها أرقام أو أحرف كبيرة أو أحرف الصغيرة
6. لا تستخدم الأحرف المتكررة (aa11)

نصائح للحفاظ على كلمة المرور آمنة:

1. لا تخبر كلمة المرور الخاصة بك لأي شخص (بما فيهم المقربين، الأصدقاء، البيبغاوات، الخ)
2. عدم كتابة كلمة المرور الخاصة بك في أي ركن أو ورقة
3. لا ترسل كلمة المرور الخاصة بك عن طريق البريد الإلكتروني
4. اختبار كلمة المرور الحالية وتغييرها إلى أخرى جديدة بشكل دوري

أمن المتصفح الخاص بك:

جميع خدمات الراجحي المصرفية عبر الإنترنت تستخدم تقنية 128 بت وتقنية SSL القوية للتشفير خلال جلسات العمل الخاصة بك على الانترنت لحماية بياناتك الخاصة. التشفير أساسا هو وسيلة متطورة لتخليط المعلومات الخاصة بك على الانترنت قبل أن يتم ارسالها من جهاز الكمبيوتر الخاص بك، بحيث تكون غير قابلة للقراءة إذا تم اعتراضها تماما. نحن نوصي أن يدعم متصفح الويب الخاص بك تقنية تشفير 128 بت لأنها تعتبر أقوى بما يقرب بـ 300 مرة من تقنية التشفير 40 بت. في حين أن تقنية تشفير 40 بت قد تكون مناسبة للمعاملات منخفضة المخاطر، على الرغم من أن جميع المتخصصين في مجال الأمن يتفقون على أنها ليست كافية لحماية المعاملات المالية. عند طلب المعلومات عبر مصرف الراجحي عبر الإنترنت، فإنه يتم تشفير طلبك أثناء ارساله. ثم فك شيفرة طلبك للحصول على المعلومات وإرسالها مرة أخرى مشفرة لك بأمان. وعند استلامه، يقوم المتصفح الخاص بك بفك تشفير المعلومات وعرضها. يمكنك تحديد أن المعلومات الخاصة بك على الانترنت يتم تشفيرها في متصفح نيتسكيب إذا كان رمز المفتاح الصغير أو القفل في الزاوية اليسرى السفلى من الشاشة غير منقطع. وسيظهر لمستخدمي متصفحات مايكروسوفت علامة قفل أثناء جلسة مشفرة.

• نوصي بشدة باستخدام أحدث إصدار من المتصفح المفضل لديك. تتوفر أحدث نسخة من المتصفح المفضل لديك عادة كتنزيل مجاني من موقع الويب للشركة المصممة للمتصفح.

• أحدث الإصدارات من المتصفحات هي أكثر أمنا من الإصدارات القديمة، وهو أمر مهم بشكل خاص عند القيام بالعمليات المصرفية عبر الإنترنت. تعمل معظم أجهزة الكمبيوتر المستندة إلى ويندوز على تضمين متصفح ميكروسوفت إنترنيت إكسبلورر، وبالتالي فإنه تعتبر المتصفح الأكثر استخداما. ولهذا، تعتبر متصفح إنترنيت إكسبلورر هو المتصفح الأكثر عرضة للهجوم من الفيروسات وأدوات التجسس.

مصرف الراجحي
Al Rajhi Bank

إذا كنت تستخدم متصفح إنترنيت إكسبلورر فمن المهم بشكل خاص تشغيل برنامج تفحص الفيروسات وبرامج التجسس بانتظام والحفاظ على تحديثه مع أحدث التصحيحات الأمنية من ميكروسوفت.

سرقة هوية المعرف:

تحديد السرقة وتزوير الهوية هي مصطلحات مستخدمة للإشارة إلى جميع أنواع الجرائم التي يحصل فيها شخص ما بصورة غير مشروعة على بيانات شخصية لشخص آخر ويستخدمها بطريقة تنطوي على احتيال أو خداع، وذلك عادة لتحقيق مكاسب اقتصادية. يستخدم المحققون المعلومات المقدمة عبر صفحات التحقق الاحتيالية هذه لاستخدام بطاقات الائتمان للمشتريات بشكل غير مصرح به أو مسح الحسابات المصرفية أو بيع المعلومات إلى مجموعات سرقة المعرفات الشخصية. وهناك العديد من الطرق والسلوكيات التي تعمل على سرقة المعرفات الشخصية، ويعتبر هناك نوعان من الأكثر شيوعا ووهي المبينة أدناه:

طريقة الاحتيال Fishing: عندما يقوم المحتال بإرسال الرسائل (إلى عناوين البريد الإلكتروني التي تم الحصول عليها بشكل غير قانوني)، ويقوم بالتظاهر بأنه من شركة أخرى (على سبيل المثال المصرف). والغرض من هذه الرسائل الإلكترونية هو استخراج المعلومات الشخصية الخاصة بك، والتي يمكن بعد ذلك استخدامها من قبل المحتال للقيام بالاحتيال باستخدام اسمك. تذكر: لن يطلب مصرف الراجحي أبدا اسم المستخدم أو كلمة المرور الخاصة بك عبر البريد الإلكتروني.

طريقة الانتحال Spoofing: هو عندما يقوم المنتحل بإنشاء موقع ويب مشابه لموقع ويب حقيقي، مثل موقع مصرف الراجحي، ويملك أيضا عنوان موقع ويب مماثل (رابط انترنت شبيه). ثم يقوم بالاحتيال عبر الإنترنت عن طريق حث الأشخاص على التعامل في هذا الموقع المزيف (مثل إيداع الأموال، وشراء السلع). تذكر: عنوان مصرف الراجحي على شبكة الإنترنت: http://www.almubasher.com.sa ولا يمكن لأي شركة أخرى تكراره.

ما يمكن ملاحظته والبحث عنه:

سطور لعناوين مخادعة: وتبدو كما لو أنها متعلقة حقا بالشركة التي يفترض أن ترسل لها رسائل البريد الإلكتروني.

عنوان المرسل المزور: عنوان البريد رغم كونه مزور يظهر كما لو أنه قادم بالفعل من الشركة التي يدعيها.
محتوى مشابه للأصل: مبني على نسخ الصور وأنماط النص من المواقع الحقيقية من أجل خداع القارئ. بتكرار علامات التوثيق وربما يحتوي على روابط حقيقية تتبع لسياسة خصوصية الشركة والصفحات الأخرى على موقع الويب الشرعي لخلق وهم المصداقية.

الارتباطات التشعبية المقنعة: قد تعرض الرسائل عنوان موقع ويب حقيقي، ولكن عند النقر عليها، فإن الرابط يقودك إلى موقع ويب مختلف. قم بالبحث عن عنوان موقع ويب طويل حيث سيأخذك إلى الموقع بعد رمز "@" كما في المثال:

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

كونها بعد

site.com-http://fraud

وإذا ضغطت على الرابط، سيأخذك إلى محتوى الرمز @

نصائح لحمايتك

1. عدم كتابة بياناتك الشخصية على سبيل المثال رقم الحساب أو رقم التعريف الشخصي أو كلمة المرور أو رقم التحقق العشوائي في أي مكان آخر غير صفحة تسجيل الدخول إلى الخدمات المصرفية عبر الإنترنت التابعة لمصرف الراجحي

2. تفعيل الإشعار. وظيفة إعلام لمستخدمي الخدمات المصرفية عبر الإنترنت والحصول على إخطار من خلال الرسائل القصيرة عندما يكون هناك نشاط على الخدمة المصرفية عبر الإنترنت في أي وقت، ليلا أو نهارا

3. عدم النقر فوق الارتباطات التشعبية داخل رسائل البريد الإلكتروني حيث أن الارتباط التشعبي الذي تقوم بفتحه قد يكون مختلفا عن الارتباط الذي يظهر لك رسالة في البريد الإلكتروني. يمكن أن تكون الارتباطات التشعبية داخل البريد الإلكتروني مخفية بسهولة

4. استخدام برامج تصفية الرسائل التطفلية للحد من عدد رسائل البريد الإلكتروني الاحتيالية والخبيثة التي تتعرض لها

5. استخدام برامج مكافحة الفيروسات

6. استخدام برنامج جدار حماية شخصي

7. الحفاظ على تحديث البرامج (أنظمة التشغيل ومتصفحات الويب)

8. ابحث دائما عن الروابط الآمنة Https:// ورمز القفل على مواقع الويب التي تتطلب معلومات شخصية. على الرغم من أن هذا لا يضمن أن الموقع الذي تدخله هو موقع حقيقي أو أنه آمن، وعدم وجود هذه الأمور يشير إلى تأكيد أن الموقع ليس أمناً.

9. حافظ على جهاز الكمبيوتر الخاص بك نظيفاً وخالياً من برامج التجسس

10. تثقيف نفسك فيما يتعلق بالنشاط الاحتيالي على شبكة الإنترنت

11. قم بالتحقق من بيانات حسابك ومراقبتها بشكل دوري

ميزات أمنية أخرى لمصرف الراجحي:

نحن نتابع عن كثب في كل مرة تقوم فيها بالاتصال بمصرف الراجحي ومراقبة الجلسة للتأكد من أن المعلومات المرسلة ذهابا وإيابا يتم إرسالها فقط إلى جهاز الكمبيوتر الخاص بك. لدينا منظومة "جدار حماية" خاصة بنا تعتبر جزءاً متطوراً للغاية من ناحية البرامج والأجهزة بحيث لا يسمح إلا للمصرح لهم باستعراض الرسائل الصادرة والواردة من مصرف الراجحي، بحيث يمكن للمستخدمين المصرح لهم فقط الولوج إلى النظام المصرفي. فيما يتم رفض أية رسائل لا تتوافق مع المتطلبات الصارمة للغاية، ويتم إنهاء الجلسة عبر الإنترنت. تم تصميم هذا النوع من التكنولوجيا بحيث لا يمكن حتى لأكثر القراصنة احترافاً بأن تضر بالموقع الخاص بنا أو الوصول إلى معلومات الحسابات الخاصة. ولمساعدتك على التأكد من أنك مرتبط حقا بمصرف الراجحي خلال جلساتك، فإننا نقوم باستخدام تقنية التحقق من الهوية الرقمية ولدينا شهادة الخادم الرقمي من Verisign – والتي تعتبر من أوائل سلطات المصادقة على شبكة الإنترنت. متصفحك يستخدمها في كل مرة تقوم فيها بتسجيل الدخول لتتيح لك التحقق من أنك متصل بمصرف الراجحي. وكما عهدتمونا، فإن لدينا عدد من الإجراءات الأمنية الأخرى المعمول بها، والتي لا يمكننا الكشف عنها لأسباب أمنية. وهي مصممة بحيث تكون شراكتنا على الإنترنت آمنة ومحمية.