سياسة السرية والأمان للمصرفية عبر الإنترنت

بالنسبة لمباشر الأفراد

مقدمــة:

يقر مصرف الراجحي بحقوقك المتعلقة بسرية أي معلومات شخصية تقدمها لمصرف الراجحي خلال أدائك لمعاملات مصرفية عبر الإنترنت. إن مصرف الراجحي ملتزم بتوفير مستوى عالي من الأمن والسرية لأي معلومات تتعلق بخدماته المصرفية التي يقدمها للأفراد عبر الإنترنت. ويضمن المصرف معالجة أي عملية تتم عبر مصرفية تتم عبر الإنترنت وأي معلومات شخصية أو مالية يتم تبادلها بمثل هذه الوسائل بطريقة مأمونة ومشفرة تلتزم بالمعايير الأمنية الخاصة بالصناعة.

تبادل وحفظ معلومات العميل

التسجيل

يتطلب منك مصرف الراجحي التسجيل في الخدمة وتحديد اسم المستخدم وكلمة المرور المفضلة لك وذلك لحماية معلوماتك الشخصية والمالية. وتقتضي عملية التسجيل توثيق ذي عاملين بالحصول على رقم بطاقة الصراف الآلي، رقم إثبات الشخصية ورقم الحساب. وبنفس القدر تحتاج للدخول إلى المصرفية عبر الإنترنت إلى تحديد اسم المستخدم وكلمة المرور. وأي معلومات يتحصل عليها المصرف لن تستخدم إلا لأغراض تزويد العميل بخدمات مصرفية.

نقل المعلومات

يحتفظ مصرف الراجحي بسرية وسلامة معلومات العميل التي يحتفظ بها ويتم تبادل المعلومات بطريقة مأمونة. ولا يتم تبادل معلومات العميل الشخصية والمالية مع أي طرف ثالث إلا عندما تكون هذه المعلومات مطلوبة للوفاء بتعليمات صادرة منك شخصياً. ولا يتم الإفصاح عن هذه المعلومات إلا إذا اقتضى أو سمح النظام أو الجهات الحكومية أو النظامية بذلك بسبب التحقيق أو المراجعة للاشتباه في حدوث عملية احتيال. أو عندما تطلب أو تسمح أنت شخصياً بالإفصاح عن هذه المعلومات كتابياً.

دخول موظفي المصرف إلى المعلومات:

لا يتم دخول موظفي المصرف إلى معلوماتك الشخصية والمالية إلا في نطاق محدود جداً ولا يتاح لهؤلاء الموظفين ذلك إلا لتقديم خدمة تطلبها أنت.

ويستمر المصرف في القيام بمراجعة وتطوير وحماية جميع مواردنا بأفضل الضوابط الرقابية والأمنية المتاحة والمعروفة لدى الصناعة المصرفية. ولن يطلب منك أبداً أي موظف يعمل لدى البنك رمز المستخدم لمصرفية الإنترنت ورقم بطاقة الصراف الآلي ورقم اثبات الشخصية الخاص بك كما يجب عليك عدم تقديمها إلى أي أحد في أي سياق أو لأي سبب. إن مصرف الراجحي لن يطلب منك أبداً الإفصاح عن كلمة المرور أو رقم إثبات الشخصية الخاص بك لأي موظف أو أي فرد يعمل لدى المصرف.

الأمن:

يسعى مصرف الراجحي إلى الاحتفاظ بأفضل المعايير الأمنية لمنع أي دخول غير مصرح به إلى معلوماتك السرية. وتتضمن الإجراءات الأمنية المستخدمة أنظمة كشف/منع التطفل وأنظمة كشف الفيروسات وتشفير البيانات والإجراءات الواقية (fire walls).

يتخذ مصرف الراجحي كافة الخطوات اللازمة لحماية المعلومات الشخصية للعميل بما في ذلك الحسابات والعمليات وأسماء المستخدمين وكلمات المرور أثناء تبادل المعلومات بينك وبين المصرف.

اسم المستخدم وكلمة المرور:

يشكل اسم المستخدم وكلمات المرور أداة حماية من الوصول إلى مصرفية الانترنت الخاصة بك. وكلمة المرور يجب أن تستخدمها وحدك عندما تريد الدخول على حساباتك وعندما تطلب تنفيذ عمليات لصالحك يجب عليك حماية اسم المستخدم وكلمة المرور والتأكد من سلامة بطاقة الصراف الآلي ورقم إثبات الشخصية وفي حالة تعرض رقم بطاقة الصراف الآلي خاصتك ورقم الهوية الشخصي وإسم المستخدم وكلمة المرور الخاصة بالمباشر للأفراد لمخاطر عليك اتخاذ الإجراءات اللازمة لتغييرها أو إشعار المصرف فوراً لحماية نفسك من أي خسارة مالية. ويمكنك الاتصال بمصرف الراجحي على مركز الهاتف المصرفي أو بالقيام بزيارة أقرب فرع.

الدخول إلى المعلومات:

إن الدخول إلى المصرفية عير الانترنت تتيح لك كامل الوصول إلى كافة حساباتك الجارية والبطاقات الائتمانية التحذيرات عبر الجوال ومختلف المعلومات الشخصية والمالية الهامة.

كيفية تحديد طريقة دخول مأمونة:

عند استخدام المصرفية عبر الانترنت سوف ترى علامة قفل تظهر في المتصفح الخاص بك ويظهر في بداية عمود العناوين (URL) يعني أنك قد توصلت بموقع مأمون. وفي حالة عدم رؤية العلامات المذكورة أعلاه التي تظهر في متصفحك عليك عدم تقديم

أي معلومات شخصية أو مالية لذلك الموقع ورفع المسألة إلى المصرف لمزيد من المساعدة.

تفويض صلاحية استخدام المباشر للأفراد:

إن مصرف الراجحي مخول بالعمل بموجب أي تعليمات يتلقاها باستخدام اسم المستخدم وكلمة المرور الخاصة بك وذلك بالنسبة للعمليات أو الاستفسارات. ففي حالة تتشارك رمز المستخدم وكلمة المرور ورقم بطاقة الصراف الآلي ورقم الإثبات الشخصي الخاص بك مع شخص آخر فإنك تكون بذلك قد فوضت ذلك الشخص باستخدام خدماتنا المصرفية عبر الانترنت. وفي هذه الحالة سوف تتحمل المسئولية التامة عن جميع العمليات التي تتم باستخدام اسم المستخدم وكلمة المرور الخاصة بك حتى لو لم تكن تقصد أو لم تفوض ذلك الشخص المعين بالاستخدام.

سلامة العمليات:

تقتضي بعض العمليات في المصرفية عبر الانترنت استخدام كلمة مرور لمرة واحدة وهو إجراء أمني إضافي يتم تنفيذه لحماية العمليات العالية المخاطر. ويتطلب منك هذا الإجراء الأمني تقديم رقم جوالك في أي مكينة صراف آلي خاص بمصرف الراجحي حيث يقوم المصرف بإرسال كلمة مرور عملياتيه إلى جوالك عبر رسالة قصيرة. وعليك تقديم رقم جوالك بحذر وعناية وعدم إدخال رقم جوال أي شخص آخر أو رقم جوال ليس في حوزتك أو لا يبقي في حوزتك.

الجلسات (فترات العمل على الحاسب) غير النشطة:

إن مصرفيتنا عبر الانترنت سوف تقوم بإنهاء تعاملك مع الحاسوب تلقائياً إذا لم تقم بإجراء عملية عند دخولك على الخدمة. وهذا الإجراء للحد من دخول شخص آخر على حسابك إذا ابتعدت عن الجهاز. ومع ذلك فإن الراجحي يوصي بشدة بأن تستخدم وظيفة إنهاء التعامل مع الموقع بمجرد أن تنتهي من جلستك المصرفية عبر الانترنت وقفل المتصفح من أجل أقصى درجة من الأمن والسلامة.

التحوطات وإجراءات الحماية:

حماية المعلومات الشخصية:

لا تشارك أي شخص في رقم بطاقة الصراف الآلي ورقم الإثبات الشخصي PIN الخاصة بك أو تسجيله في أي ورقة أو حاسب شخصي أو رقم هاتف أو أي وسيلة تخزين أخرى يمكن أن تضيع أو تتعرض للمخاطر. وتوصي بأن تحفظ رقم هويتك الشخصي للصراف الآلي في ذاكرتك ولا تكتبه أبداً في أي مكان خاصة على ظهر بطاقة الصراف الآلي أو في محفظتك.

إجراءات حماية كلمة المرور:

لا تشارك أي شخص في اسم مستخدم المصرفية عبر الانترنت وكلمة المرور الخاصة بك ولا تخزنه أو تسجله أبداً في ورقة أو حاسب آلي. وينصح مصرف الراجحي جميع العملاء يحفظ أسماء المستخدمين وكلمات المرور في ذاكرتهم وتغييرها دورياً.

عمليات تحديث نظام التشغيل والمتصفح والبرمجيات:

حافظ على مجاراة أنظمة إصلاح البرمجيات (التي تعرف أيضاً بوسائل تصحيح الذاكرة أو التحديثات الأمنية). إن استخدام المتصفح الحالي سوف يزيد من النواحي الأمنية إلى أقصى حد. كما ينصحك مصرف الراجحي باستخدام برمجيات مرخصة وتحديثها دورياً حسب الحاجة وعند الحاجة.

الوقاية من الفيروسات:

تأكد من أن جهاز الحاسب التابع لك لديه برنامج حماية من الفيروسات حديث لكشف الفيروسات والقضاء عليها. كما عليك أن تدرس ترشيح البريد الالكتروني SPAM. ولا يعتبر المصرف مسئولاً عن أي فيروسات أو رموز أخرى ضارة قد تواجهها أثناء استخدامك للإنترنت إن مصرف الراجحي يستحثك على إجراء مسح روتيني لجهاز الحاسب والبريد الإلكتروني والتخزين باستخدام منتجات حماية من الفيروسات موصى بها ومعترف بها من قبل الجهة الصانعة.

حماية البرمجية المضادة للتجسس:

استخدم البرنامج الحالي الخاص بحماية البرمجيات المضادة للتجسس لكشف وإبعاد برمجية التجسس من جهاز الحاسب الخاص بك.

إجراء الوقاية (الجدار الواقي):

استخدم إجراءات واقية لمنع المستخدمين الغير مرخص لهم من إمكانية الوصول إلى جهاز الحاسب أو الشبكة التابعة لك.

المراقبة بعناية:

ينصح مصرف الراجحي جميع العملاء بالتأكد من حالة دخولهم السابق التي تظهر على الصفحة الترحيبية. ويتيح لك ذلك تحديد ما إذا كانت هناك محاولة للدخول إلى حسابك من قبل محتال.

مزيد من الحرص والعناية:

يوصي مصرف الراجحي بعدم استخدام مرافق انترنت في أماكن عامة لأن فرصة تعرض معلوماتك الحساسة للمخاطر تكون هنا أكبر. ولكن إذا فعلت ذلك يقترح مصرف

الراجحي أنه متى ما دخلت على المصرفية عبر الإنترنت من حاسب آلي عام أو حاسب آلي مشترك مثل تلك الموجودة في مقاهي الإنترنت والمكتبات والمطارات والفنادق...إلخ فعليك التقيد بالتدابير الاحتياطية التالية:

1. تأكد من عدم وقوف شخص خلفك ينظر من وراء ظهرك عند دخولك إلى الموقع.
2. أخرج من الموقع بمجرد الانتهاء من جلسة المصرفية عبر الإنترنت.
3. أقفل المتصفح بالنقر على الأيقونة "X" التي توجد عادة في الزاوية العليا اليمنى للشاشة.
4. عندما تأتي للعمل على الحاسب مرة أخرى تأكد من أن آخر وقت عمل لك على الحاسب متوافق مع آخر جلسة عمل مصرفية لك على الانترنت.
5. قم بتغيير كلمة المرور أو رمز الدخول بأسرع ما يمكن عندما تبدأ العمل في المرة التالية على حاسب موثوق ومأمون.
6. لا تقم مطلقاً بتنزيل أو حفظ كشوف حساباتك أو معلومات ذات صلة من أو في حاسب عام.

رسائل البريد الإلكتروني الخادعة ومواقع الاحتيال:

من المعروف أن المحتالين يقومون بإنشاء نسخ من المواقع المصرفية بهدف اصطياد بيانات العميل الشخصية الخاصة ببدء التعامل مع المصرفية عبر الانترنت. ثم يقومون بعد ذلك بإرسال رسالة بريد الكتروني توجه المرسل إليه بزيارة الموقع وبدء التواصل مع الحاسب للتأكد من صحة بياناته. ولسوء الحظ عندما يقوم الناس بإدخال بياناتهم في هذه المواقع تتسجل البيانات ويستخدمها المحتالون لتحويل مبالغ من وسائل المصرفية الحقيقية عبر الإنترنت.

وتبدو هذه المواقع ورسائل البريد الإلكتروني حقيقية في الغالب لذلك يكون من الصعب التمييز بين البريد الإلكتروني الزائف من الحقيقي. وفيما يلي بعض الأشياء التي يجب وضعها في الاعتبار:

1. قد تبدأ رسائل البريد الإلكتروني هذه بعبارة "عزيزي عميل مصرف الراجحي". إننا نعلم من أنت لذلك سوف نخاطبك دائماً بصفة شخصية في حين أن المحتالين من الأرجح أن لا يعرفوا أسمك. وننصح الأعضاء بعدم النقر على أي رابط أو فتح مرفقات أو إدخال أي معلومات شخصية.
2. إن هذه الرسالة ليس لها أي علاقة بمصرف الراجحي بأي حال من الأحوال. فمصرف الراجحي لديه سياسة تتمثل في عدم طلب أي معلومات أمنية عن طريق البريد

الإلكتروني أو الطلب من الأعضاء متابعة روابط الإنترنت. ومصرف الراجحي لن يرسل بيانات من مصرفية الإنترنت الخاصة بك.

3. يجب على العملاء الدخول فقط إلى موقع مصرف الراجحي الخاص بالمصرفية عبر الإنترنت وذلك بطباعة عنوان الموقع www.alrajhibank.com.sa في عمود العنوان على المتصفح الخاص بهم وبعد ذلك الإشارة إلى المصرفية عبر الإنترنت الخاصة بالمباشر للأفراد. ويمكن للعملاء الدخول إلى المباشر للأفراد مباشرة بتحديد روابط العنوان التالي في المتصفح https://www.almubasher.com.sa .

نأمل إغفال أي رسالة بريد إلكتروني تنصحك بالدخول على موقعنا وتقديم أي من بياناتك الشخصية. وبدلاً من ذلك أرفع رسالة البريد الإلكتروني إلى مصرف الراجحي بالاتصال برقم الهاتف المصرفي ثم أحذفها فوراً.