Protection de vos renseignements personnels

RBC PH&N Services-conseils en placements met en place des mesures de sécurité rigoureuses afin d'assurer une protection efficace de votre patrimoine et vos renseignements personnels. Découvrez davantage comment RBC vous protège, comment repérer les communications frauduleuses et protéger vos renseignements personnels.

Prévention des fraudes

Nous incorporons à nos activités quotidiennes la détection et la prévention de la fraude. RBC a une équipe d'experts en fraude qui travaille 24 heures sur 24, 7 jours sur 7 pour prévenir, détecter et étudier les cas de fraude. De plus, nous travaillons en étroite collaboration avec les associations sectorielles, le gouvernement et les services de police pour tenter d'éradiquer la fraude. Nous investissons dans les technologies nouvelles et émergentes de prévention de fraudes, et nous suivons des mesures de sécurité rigoureuses pour vous permettre de bénéficier de nos produits et services dans un cadre sécuritaire.

Notre politique de contrôle diligent pour la protection de votre compte

Il peut arriver, dans de rares cas, que des pirates détournent vos courriels ou encore que des fraudeurs envoient des courriels déguisés. Nous prenons très au sérieux notre responsabilité de protection de votre patrimoine et de vos renseignements personnels. En tout temps, lorsque nous recevons un courriel avec des instructions relatives à votre compte, nous effectuons toujours un suivi direct en communiquant avec vous au moyen du numéro de téléphone que nous avons en dossier pour confirmer les instructions, même si celles-ci semblent crédibles.

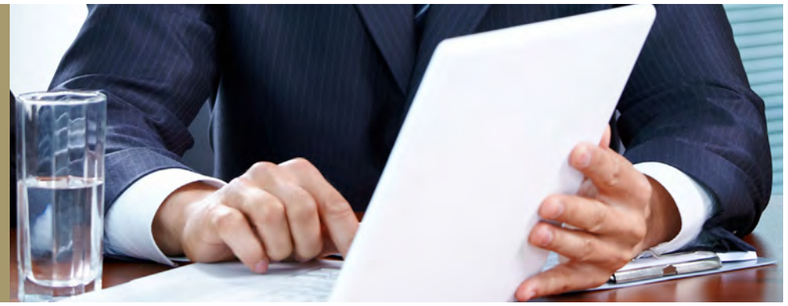
Afin d'assurer la confidentialité de vos renseignements personnels, tous les courriels que nous vous envoyons et qui contiennent des renseignements personnels sur vous et des données de votre compte sont chiffrés. Il pourrait ne pas être nécessaire d'envoyer de manière sécurisée les correspondances normales (par exemple, un message pour confirmer une rencontre), mais toute autre communication contenant un quelconque renseignement sur votre ou vos comptes ou encore vos placements vous sera transmise en mode chiffré.

Nous communiquons avec vous de façon proactive pour confirmer que certaines opérations passées à votre compte sont légitimes. Avant de fournir tout renseignement, demandez d'abord un numéro de téléphone aux fins de validation de l'appel et rappelez-nous à un numéro que vous avez préalablement vérifié.

Evitez les fraudes par courriel

L'« hameçonnage par courriel » est un type courant de fraude en ligne qui consiste à envoyer des courriels factices pour vous inciter à fournir vos renseignements personnels dans le but de commettre une fraude financière ou d'usurper votre identité.

Si vous croyez avoir communiqué les données de votre compte ou d'autres renseignements personnels en répondant à un courriel frauduleux, communiquez immédiatement avec votre conseiller.



RBC organise à l'occasion des campagnes de promotion par téléphone, par la poste et par courriel. Si vous avez des doutes sur l'origine des messages que nous vous envoyons, n'y répondez pas et communiquez avec votre conseiller.

RBC ne vous enverra jamais, sous aucune considération, des courriels non sollicités comportant un lien ou un numéro de téléphone, en vous demandant d'actualiser ou de vérifier les données de votre compte et d'autres renseignements personnels. Les courriels d'hameçonnage typique par courriel contiennent une raison fictive comme une atteinte à la sécurité ou un concours et éveiller un sentiment d'urgence pour vous inciter à répondre ou à cliquer sur un lien.

Ne mordez pas à l'hameçon – ne cliquez pas sur ces liens ni ne répondez au message. Les liens peuvent vous mener à des sites Web fictifs ou usurpateurs conçus pour enregistrer vos renseignements personnels.

Les sites Web ont souvent une apparence authentique et arborent même des bandeaux et des logos RBC pour duper le visiteur.

RBC ne vous enverra jamais de courriel non sollicité pour vous demander de fournir des renseignements confidentiels comme des mots de passe, un NIP, un numéro d'assurance sociale ou tout autre renseignement personnel. Si vous recevez un courriel dans lequel on vous demande de fournir de tels renseignements, n'y répondez pas. Informez-nous-en plutôt en faisant suivre le message à l'adresse phishing@rbc.com. Si vous croyez avoir communiqué les données de votre compte ou d'autres renseignements personnels en répondant à un courriel frauduleux, communiquez immédiatement avec votre conseiller au 1 800 769-2511.

Consultez régulièrement vos relevés pour vous assurer que toutes les opérations sont autorisées, et vérifiez annuellement votre rapport de solvabilité.

Faites preuve de vigilance lorsque vous êtes en ligne, particulièrement quand vous utilisez une connexion internet gratuite ou non sécurisée dans des lieux publics, et quand vous accédez à des sites d'information sensible, comme banque en direct.

Dix conseils pour protéger vos actifs

En plus des mesures de contrôle que nous utilisons, la connaissance est souvent la meilleure défense contre la fraude. Ces dix étapes sont une façon simple et efficace de réduire le risque de vol ou de mauvaise utilisation de vos données personnelles et financières.

1. Assurez la protection de vos renseignements personnels

Un usurpateur d'identité peut recourir à tous les moyens pour obtenir vos renseignements personnels (fouiller même dans vos ordures et votre bac de recyclage). Assurez-vous de déchiqueter vos reçus, vos copies de demande de crédit, vos formulaires d'assurance, les offres de crédit reçues par la poste, etc. Prenez l'habitude de retirer le contenu de votre boîte à lettres après chaque livraison. Assurez-vous que le courrier est réacheminé si vous déménagez ou changez d'adresse postale. Ne donnez aucun renseignement personnel par téléphone, par courriel ou par internet, sauf si vous êtes à l'origine de la communication et connaissez la personne avec qui vous traitez.

2. Souvenez-vous des cycles de facturation des relevés

Si vos factures ou vos relevés ne vous parviennent pas à temps, faites immédiatement un suivi pour vous assurer qu'ils n'ont pas été réacheminés frauduleusement. Consultez régulièrement vos relevés pour vous assurer que toutes les opérations sont autorisées, et vérifiez annuellement votre rapport de solvabilité.

3. Protégez votre NIP

Ne divulguez à personne votre NIP, incluant les employés de RBC, les membres de votre famille ou vos amis. Lorsque vous effectuez une opération dans un guichet automatique ou dans un magasin (point de vente), ne perdez jamais de vue votre carte-client et masquez le clavier pendant que vous entrez votre NIP.

4. Limitez vos risques

Revoyez vos limites de retrait quotidiennes sur votre carte de débit. Si vous n'avez pas besoin d'une limite élevée, faites-la diminuer. Vous réduirez ainsi le risque de fraude en diminuant le montant pouvant être retiré. N'ayez dans votre portefeuille que les pièces d'identité et les cartes de crédit dont vous avez besoin ; laissez le reste (en particulier votre acte de naissance, votre carte de nas et votre passeport) à la maison en lieu sûr.

En plus des mesures de contrôle que nous utilisons, la connaissance est souvent la meilleure défense contre la fraude.

Ne divulguez jamais vos mots de passe, et choisissez-en toujours des difficiles à deviner (les mots de passe à toute épreuve sont constitués d'une combinaison de lettres, de numéros et de caractères, et sont souvent modifiés).

5. Protégez vos renseignements personnels en ligne

Faites preuve de vigilance lorsque vous êtes en ligne, particulièrement quand vous utilisez une connexion internet gratuite ou non sécurisée dans des lieux publics, et quand vous accédez à des sites d'information sensible, comme banque en direct. Assurez-vous de sécuriser votre connexion sans fil par un mot de passe.

6. Choisissez un mot de passe futé

Ne divulguez jamais vos mots de passe, et choisissez-en toujours des difficiles à deviner (les mots de passe à toute épreuve sont constitués d'une combinaison de lettres, de numéros et de caractères, et sont souvent modifiés). Ne recyclez pas les mots de passe et n'utilisez pas les mêmes mots de passe pour les services bancaires en ligne que pour les autres services comme les sites des réseaux sociaux.

7. Vérifiez avant de cliquer

Vérifiez toujours un message avant de prendre des mesures, comme cliquer sur un lien ou lancer une opération. Ne cliquez jamais sur les liens et n'ouvrez pas les fichiers inclus dans des courriels envoyés par des personnes que vous ne connaissez pas, ni dont vous n'attendez pas de message (cela pourrait exposer votre ordinateur à des enregistreurs de mots de passe ou à des logiciels espions).

8. Chiffrez vos données pour une sécurité renforcée

Utilisez toujours une technique de chiffrement quand vous envoyez par courriel des renseignements confidentiels, et n'enregistrez jamais des données sensibles sur vous-même ou d'autres personnes dans vos dossiers de courriel. Même des courriels chiffrés peuvent être piratés.

9. Utilisez une suite de solutions logicielles de sécurité

Installez une suite complète de logiciels de sécurité bien connus sur vos appareils (ordinateur/tablette/téléphone) et maintenez ces logiciels à jour. Méfiez-vous des fenêtres contextuelles qui indiquent que votre ordinateur est contaminé par un virus et vous incitent à acheter ou à télécharger un logiciel pour régler le problème.

10. Fermez toujours votre session

Assurez-vous de toujours bien fermer la session et de quitter votre navigateur pour éviter que d'autres personnes puissent accéder plus tard à vos renseignements.

Pour obtenir plus de renseignements sur la protection de vos renseignements personnels, visitez le site http://www.rbc.com/rensperssecurite/ca/index.html, ou communiquez avec nous dès aujourd'hui.

SYPI-FR (03/14)