Prévention des fraudes financières et protection des renseignements personnels

Conseils de RBC

Contenu

Nous disposons aujourd'hui d'un choix de produits, de technologies et de services incomparables, et nous n'avons jamais bénéficié d'autant de façons de gérer vos affaires. Ces choix nous obligent cependant à mieux protéger nos renseignements personnels, commerciaux et financiers contre la fraude. Nous pouvons vous y aider.

Pour vous protéger contre la fraude financière

À RBC®, nous croyons que nous devons travailler avec nos clients pour bien nous et vous protéger contre la fraude financière. Nous mettons en place des mesures de sécurité rigoureuses pour que vous puissiez effectuer vos opérations bancaires et faire des affaires avec RBC de façon sécuritaire.

Vous trouverez dans la présente brochure de nombreux conseils utiles au quotidien, notamment des pratiques informatiques sans risque que vous pouvez adopter pour prévenir le vol et l'emploi abusif de vos renseignements personnels et financiers.

Protection de votre identité

Souvenez-vous de tenir confidentiels votre numéro d'assurance sociale (NAS), votre numéro d'identification personnel (NIP), vos mots de passe, vos questions et réponses de vérification ainsi que vos codes d'accès secrets.

Votre numéro d'assurance sociale (NAS)

Émise par le gouvernement fédéral, votre carte d'assurance sociale représente une pièce d'identité dont vous devez toujours préserver la confidentialité. Votre numéro d'assurance sociale sert à recueillir des renseignements de nature fiscale et est nécessaire à l'administration des impôts sur le revenu des particuliers. Selon la loi, vous devez fournir votre NAS uniquement aux personnes ou aux institutions suivantes :

- votre employeur ;
- le gouvernement fédéral ;

› des institutions financières ou d'autres organisations qui paient des intérêts sur votre(vos) compte(s) et qui doivent établir des documents d'ordre fiscal en votre nom (p. ex., une banque, une société de fiducie, une société de crédit ou un courtier en placements).

RBC est tenue par la loi de vous demander votre NAS à des fins de déclaration de revenus, par exemple, à l'ouverture d'un compte enregistré ou pour déclarer le revenu acquis sur un certificat de placement garanti, un compte de placement ou des produits d'assurance tels que l'assurance vie universelle. Si vous faites une demande de produit de crédit, RBC vous demande votre NAS, mais vous n'êtes pas tenu de le fournir à cette fin. Nous vous demandons l'autorisation d'utiliser votre NAS durant le traitement de votre demande pour nous assurer d'obtenir de l'agence d'évaluation de crédit vos renseignements financiers et non ceux de quelqu'un d'autre portant un nom similaire.

Ne fournissez jamais votre NAS en réponse à une demande non sollicitée par courriel, par téléphone ou dans une fenêtre contextuelle sur un site Web. RBC ne vous demandera jamais votre NAS à des fins de vérification dans un courriel, dans une fenêtre contextuelle ou au téléphone.

Numéros d'identification personnels (NIP) et mots de passe

Les NIP et les mots de passe sont votre signature électronique pour vous identifier comme étant l'utilisateur autorisé de vos comptes RBC (carte-client, carte de crédit, Banque en direct, Services bancaires par téléphone, etc.). Utilisés avec la carte ou le numéro de compte correspondant, les NIP et les mots de passe vous donnent accès à vos fonds et aux renseignements sur votre compte, nuit et jour, pratiquement où que vous soyez dans le monde. Vous devez protéger vos NIP et vos mots de passe en tout temps ; ne les révélez jamais à qui que ce soit.

Comment choisir votre NIP

Choisissez un NIP comportant des chiffres et des lettres dont vous pouvez vous souvenir aisément, mais évitez les nombres ou les mots faciles à deviner.

Voici quelques exemples de nombres ou de mots que vous devez éviter :

- votre date de naissance ;
- votre numéro de téléphone ;
- votre adresse ;
- votre NAS.

Lorsque vous partez à l'étranger, n'oubliez pas que dans de nombreux pays, seuls les NIP à quatre chiffres sont acceptés.

Comment protéger votre NIP

La protection de votre NIP est l'un des moyens les plus efficaces de vous protéger contre les fraudes.

Voici quelques conseils pour vous aider à choisir votre NIP et à le protéger :

- Changez votre NIP de temps à autre.
- Évitez les numéros qui sont faciles à deviner ou liés à des renseignements personnels comme votre date de naissance, votre NAS, votre adresse ou votre numéro de téléphone.
- Ne notez pas votre NIP par écrit et ne le consignez pas de manière électronique.
- Ne révélez votre NIP à personne, y compris les institutions financières, les organismes d'application de la loi, vos amis et les membres de votre famille. Si quelqu'un (un membre de votre famille, un ami, un associé, un soignant, etc.) doit effectuer des opérations bancaires pour vous, parlez-en d'abord à votre représentant des services bancaires pour connaître les moyens de le faire sans divulguer votre NIP.
- Lorsque vous effectuez une opération, ne perdez jamais votre carte de vue et cachez toujours le clavier lorsque vous tapez votre NIP.
- Si vous croyez que votre NIP a été compromis, modifiez-le immédiatement à votre succursale RBC Banque Royale® la plus près.

Protection de vos comptes

Certaines de nos opérations bancaires exigent encore le traitement de documents papier tels que chèques et bordereaux de dépôt, qui sont souvent encodés au moyen de votre numéro de compte. Voici quelques suggestions pour préserver la confidentialité de vos comptes et éviter les accès non autorisés :

- Rédigez vos chèques avec un stylo à l'encre indélébile (qui ne peut pas s'effacer) en inscrivant les détails à partir de la marge de gauche et en ne laissant aucun espace blanc.
- Si vous commettez une erreur en rédigeant un chèque, un bordereau de dépôt ou de retrait, détruisez-le en le déchirant ou en le déchiquetant.
- Dans la mesure du possible, évitez de faire des chèques payables « comptant » ou « au porteur » et ne laissez jamais en blanc l'espace réservé au bénéficiaire.
- Si un chèque est endossé (signé au verso par le bénéficiaire), il pourrait être encaissé par quiconque l'a en sa possession. N'endossez vos chèques que lorsque vous êtes prêt à les encaisser ou à les déposer.
- Soyez au courant de la date de réception de vos relevés ; si la date de réception habituelle d'un relevé est passée, communiquez avec l'émetteur. Les relevés électroniques, sans papier, pourraient s'avérer une meilleure option.
- Rangez les chèques en blanc, les chèques annulés et les relevés dans un endroit sûr. Détruisez les chèques annulés et les relevés de façon sûre dès que vous n'en avez plus besoin.
- Vérifiez rapidement et régulièrement vos relevés, vos copies d'images de chèques, vos chèques annulés (pour les entreprises clientes) et vos livrets bancaires, et signalez sur-le-champ toute anomalie, y compris les opérations manquantes. Vous pouvez également vous inscrire à Banque en direct afin de pouvoir surveiller ou rapprocher régulièrement vos comptes. Si vous remarquez une anomalie, signalez-la sans tarder.

- Utilisez fréquemment l'option de consultation des chèques en ligne afin de vérifier les chèques tirés de votre compte ou qui y sont déposés. Si vous remarquez une anomalie, signalez-la sans tarder.
- Soyez vigilant lorsque vous acceptez des effets négociables, par exemple des chèques personnels d'inconnus. Les fraudeurs mettent beaucoup de soin à s'assurer que leurs chèques contrefaits sont de grande qualité et comportent toutes les caractéristiques des chèques authentiques. Examinez attentivement les effets pour vérifier qu'ils ne comportent aucun défaut ou erreur évident et que la police est uniforme ; avisez immédiatement RBC si vous ne connaissez pas l'émetteur du chèque ou si vous soupçonnez qu'un chèque est faux.
- L'utilisation du dépôt direct et du débit électronique réduit les formalités administratives ainsi que la quantité de papier liée aux opérations.

Sécurité et protection des cartes

Les cartes-clients et les cartes de crédit RBC sont un moyen pratique d'effectuer vos opérations quotidiennes. Acceptées à de nombreux endroits, elles vous permettent de retirer de l'argent, d'effectuer des paiements et de procéder à des opérations financières dans des guichets automatiques et dans des magasins à l'échelle mondiale.

La protection et l'utilisation prudente de vos cartes contribuent grandement à prévenir les fraudes. Voici quelques conseils à suivre :

- Signez votre nouvelle carte dès que vous la recevez et, s'il y a lieu, activez-la immédiatement à la réception.
- Communiquez avec la société émettrice pour annuler toute carte dont vous ne voulez pas. La simple destruction d'une carte ne suffit pas à fermer le compte. Détruisez toutes les cartes annulées, échues ou émises antérieurement.
- Évitez de laisser votre carte sans surveillance dans un lieu public. Ne perdez pas votre carte de vue pendant que vous l'utilisez. Après une opération, assurez-vous qu'on vous redonne votre carte et vérifiez que votre nom y figure. Détruisez les reçus et les relevés dont vous n'avez plus besoin.

- N'oubliez pas que des vendeurs peuvent glisser votre carte dans l'appareil de lecture pour vous. Ne la perdez jamais de vue pour vous assurer qu'elle n'est pas glissée dans un autre appareil sous le comptoir. Autant que possible, glissez vous-même votre carte dans l'appareil de lecture. Pour les opérations effectuées au moyen d'une carte à puce avec NIP, assurez-vous de toujours insérer et retirer la carte vous-même.
- Vérifiez le reçu de vente et le montant de l'achat avant de valider l'opération au moyen de votre signature ou de votre NIP.
- Ne prêtez jamais vos cartes, ni ne révélez vos NIP ou mots de passe à qui que ce soit, même vos amis ou les membres de votre famille.
- Évitez d'utiliser vos cartes ou d'approcher d'un guichet si vous ne vous sentez pas à l'aise ou si des gens sont trop près de vous.
- Si des personnes sont trop près de vous, demandez-leur de s'éloigner pendant que vous composez votre NIP.
- Lorsque vous retirez votre argent, vérifiez-le discrètement et rangez-le aussitôt dans votre portefeuille.
- Vérifiez régulièrement toutes les opérations effectuées dans votre compte qui figurent sur vos relevés papier et sur vos relevés de Banque en direct. Signalez sans tarder toute anomalie, y compris les opérations manquantes.
- Évitez de donner votre numéro de carte de crédit au téléphone, sauf si vous êtes l'auteur de l'appel. Si vous n'êtes pas l'auteur de l'appel, vérifiez de manière indépendante le numéro de téléphone et l'identité de l'appelant, car le numéro indiqué sur votre afficheur pourrait ne pas être le numéro d'où provient réellement l'appel.
- Faites une photocopie des pièces d'identité que vous portez sur vous, et notamment de votre carte-client et de votre carte de crédit, de façon à tenir une liste des numéros en cas de perte. Conservez les photocopies des documents originaux dans un endroit distinct et sûr (p. ex., un coffre).

› Consignez les numéros de soutien clientèle afin de pouvoir annuler vos cartes ou signaler immédiatement les problèmes au besoin.

Perte ou vol de cartes

Si vous savez ou soupçonnez que votre Carte-client RBC Banque Royale ou votre carte de crédit RBC a été perdue ou volée, signalez-le immédiatement en composant le 1 800 769-2511 ou en communiquant avec une succursale.

Nous travaillons sans relâche pour vous protéger contre la fraude. Si nous remarquons que des opérations qui ne correspondent pas à vos activités bancaires normales ont été effectuées avec votre carte, il se peut que nous communiquions avec vous pour nous assurer que vous avez bien effectué ces opérations et que votre carte n'a pas été perdue, volée ou utilisée sans votre consentement. Le cas échéant, nous communiquerons avec vous par l'intermédiaire d'un agent ou d'un appel automatique.

Nous ne vous demanderons jamais de fournir de renseignements confidentiels comme votre NIP, votre mot de passe, votre valeur de vérification de la carte 2 (numéro figurant au verso de votre carte) ou votre NAS. Si vous recevez un appel semblable et si vous avez des doutes sur l'identité de la personne qui vous appelle, raccrochez et composez le numéro 1 800 769-2511. Ne composez pas un numéro que l'on vous a donné au téléphone ou par courriel avant d'avoir personnellement vérifié le numéro.

Quelles sont mes responsabilités ?

Vos responsabilités en tant que titulaire de cartes figurent dans les conventions régissant l'utilisation de vos cartes. Prenez le temps de les lire attentivement. L'utilisation de vos carte confirme que vous avez lu et compris l'entente et que vous en acceptez les modalités.

Nous avons également une Garantie de sécurité RBC Banque en direct. Pour en savoir plus, rendez-vous au rbcbanqueroyale.com/endirect/rbcbanqueendirect et consultez notre Guide de la sécurité et de la confidentialité au rbcroyalbank.com/online/guidetosecurity.

Opérations par voie électronique

Internet permet d'effectuer des opérations par voie électronique, en tout temps. Cette commodité s'accompagne du besoin de s'assurer que les opérations financières confidentielles s'effectuent en toute sécurité. RBC fait appel à la technologie la plus à jour pour protéger vos données confidentielles. Nous utilisons des procédures internes pour protéger les paramètres des comptes et les mots de passe des clients. De plus, nous surveillons constamment nos sites Web Banque en direct et Placements en direct ainsi que nos mesures de sécurité pour que leur efficacité soit toujours optimale.

Un grand nombre de clients décident de gérer leurs finances par voie électronique ou par téléphone et utilisent les services bancaires avec codes d'accès et mots de passe. En prenant des précautions lorsque vous effectuez des opérations, vous pouvez vous protéger contre l'utilisation non autorisée de vos données personnelles.

Si vous êtes en ligne ou au téléphone, assurez-vous que l'écran ou le clavier de votre ordinateur ou l'afficheur de votre téléphone est à l'abri de tout regard indiscret lorsque vous entrez votre numéro de compte, votre mot de passe, vos réponses aux questions de vérification ou vos codes d'accès sécuritaire.

Afin de sécuriser davantage vos opérations de virement de fonds par courriel Interac†, choisissez une question à laquelle le destinataire peut répondre, mais qui n'est pas facile à deviner. Veillez à ce que la réponse ne se trouve pas dans la question.

Voici quelques étapes supplémentaires que vous pouvez suivre pour protéger vos opérations en ligne :

Évitez d'utiliser des ordinateurs publics

Pour effectuer des opérations financières ou d'autres opérations qui nécessitent l'introduction de renseignements personnels, évitez de vous servir d'ordinateurs publics (dans les bibliothèques ou les cafés Internet, par exemple) et tout autre ordinateur que votre propre ordinateur personnel ou

d'entreprise. Vous ne connaissez pas les pratiques de sécurité de ces ordinateurs, et vous ne pouvez pas vous assurer que des logiciels malveillants n'enregistreront pas vos renseignements personnels tels que vos mots de passe.

Quand vous utilisez des ordinateurs en réseau, nous vous recommandons de ne pas accéder à Banque en direct de RBC Banque Royale ni à RBC Placements en Direct[MC] dans un lieu très fréquenté comme une bibliothèque ou un café Internet. Si vous devez le faire, n'oubliez pas de fermer votre session et de fermer correctement le navigateur une fois que vous avez terminé vos opérations. Vous empêchez ainsi les utilisateurs non autorisés d'avoir accès à l'information vous concernant en cliquant sur le bouton « Précédent ».

Comme mesure de précaution supplémentaire, nous vous suggérons de vous inscrire au service de protection de l'ouverture de session, une caractéristique de sécurité de RBC Banque en direct qui offre une meilleure protection contre les abus potentiels de votre compte en ligne. Vous choisissez trois questions auxquelles vous êtes le seul à connaître les réponses. Puis, lorsque vous tentez d'ouvrir une session à partir d'un autre ordinateur que ceux que vous utilisez habituellement, vous devez répondre à l'une de vos questions de sécurité. Un utilisateur non autorisé ne connaîtra pas les réponses à ces questions, et l'accès lui sera donc refusé. Pour en savoir plus, visitez notre site Web au rbcbanqueroyale.com/endirect/guidedesecrite.

De plus, souvenez-vous de vérifier si vous êtes sur des sites Web privés. Dans votre navigateur, recherchez la présence de l'icône représentant un cadenas fermé ou une clé non brisée ainsi que d'une adresse de site Web débutant par « https » plutôt que par « http », ce qui représente les sites Web publics.

Maintenez le logiciel de protection de votre ordinateur à jour

Les virus et les autres programmes malveillants qui se transmettent par Internet constituent en tout temps une menace pour les systèmes informatiques. Adoptez des logiciels de protection, y compris un pare-feu personnel, un logiciel antivirus, un logiciel antipourriel et un antilogiciel-espion, nécessaires à la protection de votre ordinateur et de vos renseignements. Utilisez les processus autorisés de mise à jour des logiciels pour votre navigateur Web, votre système d'exploitation et tous les logiciels requis pour vos activités en ligne (par exemple, vos modules externes de navigation tels que des visualisateurs PDF), et vérifiez régulièrement les sites pertinents afin d'obtenir les rustines et les mises à jour les plus récentes. Pour connaître les outils importants à installer et savoir comment tester votre ordinateur afin de vous assurer que ces outils fonctionnent correctement, rendez-vous au www.rbc.com/rensperssecurite.

Choisissez des mots de passe, des questions et des confirmations de sécurité efficaces

Cela peut sembler une évidence, mais le choix d'un mot de passe unique, à la fois difficile à deviner pour les autres et facile à mémoriser pour vous, est un élément fondamental de la sécurité informatique. Il est également important de changer ce mot de passe fréquemment. Évitez d'utiliser la fonction « mémoriser le mot de passe » sur les sites Web, puisque cela enregistre votre mot de passe sur le disque dur de l'ordinateur.

Voici quelques conseils pour choisir un bon mot de passe :

- Utilisez une combinaison de lettres capitales et minuscules.
- Intégrez des chiffres et des caractères spéciaux à votre mot de passe.
- Assurez-vous que votre mot de passe comporte au moins huit caractères.

S'inspirer d'une phrase ou de paroles de chansons peut se révéler un bon moyen de créer facilement un mot de passe complexe.

Services bancaires par téléphone protégés

Notre technologie de service bancaire par téléphone vous permet d'effectuer vos opérations bancaires par téléphone au moyen d'un téléphone à clavier. Les clients qui utilisent un téléphone à clavier n'ont qu'à appuyer sur la touche appropriée pour entrer l'information numérique. Avant de pouvoir effectuer des opérations bancaires par téléphone, vous devez entrer votre numéro de carte-client et votre mot de passe ou code d'accès.

Conseils de sécurité

- Si vous vous trouvez dans un endroit où quelqu'un risque de vous voir taper votre mot de passe, cachez le clavier du téléphone au moyen de votre main ou d'un objet.
- Évitez les situations où quelqu'un peut vous entendre lorsque vous donnez des renseignements sur votre identité.
- Lorsque vous utilisez un téléphone pour effectuer des opérations bancaires, sachez que le bouton de recomposition de certains téléphones affiche la dernière suite de touches composée, ce qui pourrait comprendre les numéros entrés au cours de votre session de service téléphonique bancaire. Si cette éventualité vous inquiète, vous n'avez qu'à composer une série de touches au hasard une fois que vous avez terminé votre appel bancaire, de sorte que ce nouveau numéro s'affiche lorsque la prochaine personne appuiera sur le bouton de recomposition.

Investir avec prudence

Voici quelques suggestions pour vous aider à vous protéger le mieux possible contre les activités frauduleuses lorsque vous effectuez des opérations de placement :

- N'achetez qu'auprès d'institutions en qui vous avez confiance.
- Évitez les placements que vous ne comprenez pas ou avec lesquels vous n'êtes pas à l'aise.

- Ne prenez jamais de décision de placement si on exerce des pressions sur vous.
- Méfiez-vous des promesses d'enrichissement rapide et des bons tuyaux : en fin de compte, vos pertes pourraient être bien supérieures à vos gains. Méfiez-vous particulièrement des pourriels vous pressant d'acheter de nouvelles actions.
- Bien que beaucoup d'opérations soient effectuées par téléphone ou en ligne, vous devez être vigilant quand vous traitez avec des sociétés de placement qui n'ont pas pignon sur rue. Étudiez soigneusement le placement si on vous demande d'envoyer de l'argent à une boîte postale et vérifiez personnellement la légitimité de l'entreprise.
- Ne fournissez jamais vos renseignements confidentiels ou financiers en réponse à des courriels ou des appels téléphoniques non sollicités.

Protection de vos objets précieux

Il est essentiel pour chacun de protéger ses biens personnels contre la fraude et le vol. Il existe de nombreux services à cet effet. En voici quelques exemples :

Coffres

La meilleure façon de mettre à l'abri vos documents et petits objets de valeur comme des certificats d'actions, des obligations, des certificats de placement, des pièces de monnaie de collection, des documents importants et autres objets précieux, c'est encore un coffre. Il est conseillé également d'y conserver des photographies ou des vidéos des bijoux et des autres objets précieux aux fins des assurances.

Remboursement des titres

Soyez vigilant lorsque vous encaissez ou vous vous faites rembourser des titres immatriculés à votre nom. En effet, une fois que vous les avez signés, ils sont complètement négociables et peuvent être encaissés par quiconque les a en sa possession. Ne les signez qu'à la banque ou dans le bureau de votre courtier.

Usurpation d'identité

L'usurpation d'identité se produit lorsqu'une personne accède aux renseignements personnels d'une autre (p. ex., nom, date de naissance, NAS) et les utilise pour effectuer des activités financières au nom de cette dernière. L'usurpateur d'identité peut alors accéder aux comptes bancaires, ouvrir de nouveaux comptes de carte de crédit ou porter des achats aux comptes de carte de crédit existants, émettre des chèques, ouvrir des comptes bancaires ou obtenir de faux emprunts ou de fausses hypothèques. Votre identité peut être usurpée au moyen de votre NAS, du nom de jeune fille de votre mère, de votre date de naissance ou de vos numéros de comptes bancaires.

Pour vous protéger, vous devez connaître quelques-unes des méthodes qui peuvent être employées pour usurper votre identité. Il s'agit notamment du vol de portefeuilles qui contiennent des renseignements personnels et des cartes de crédit, du vol de relevés d'institutions financières dans les boîtes aux lettres et du détournement du courrier par l'envoi d'une demande de changement d'adresse, de la fouille de poubelles ou de l'accès aux dossiers professionnels. L'information transmise par voie électronique non sécurisée peut également être interceptée. Si vous ne recevez pas vos relevés en format papier ou électronique, communiquez immédiatement avec votre banque.

Recommandations pour combattre l'usurpation d'identité

- Déchirez ou détruisez entièrement les demandes de carte de crédit préapprouvées, les relevés bancaires, les reçus de carte de crédit, les factures et l'information connexe, les cartes expirées et toute autre carte de crédit que vous n'utilisez plus.
- N'ayez sur vous que les cartes de crédit dont vous avez besoin.
- Signez toutes vos cartes de crédit dès que vous les recevez.
- Évitez de transporter votre carte d'assurance sociale sur vous.

- Ne fournissez aucun renseignement personnel, notamment des numéros de carte de crédit ou de carte-client, des NIP, des mots de passe, votre NAS ou votre date de naissance en réponse à une demande non sollicitée (y compris les demandes par courriel, sur un site Web ou par téléphone), sauf si vous êtes l'auteur de l'appel ou que vous pouvez vérifier que l'appel provient d'une personne autorisée.
- Ne prêtez pas vos cartes à qui que ce soit.
- Signalez immédiatement la perte ou le vol de cartes.
- Retirez rapidement le courrier de votre boîte aux lettres et ne laissez pas traîner de correspondance à la maison ou au bureau.
- Ne répondez pas aux offres par courriel ou par téléphone déguisées en promotion ou en sondage promettant des prix instantanés. Ces offres visent en fait à obtenir des renseignements personnels comme votre numéro de carte de crédit.
- Demandez une copie de votre dossier de crédit tous les ans auprès d'Equifax (1 800 465-7166 ou 514 493-2314 ou www.equifax.ca) ou de TransUnion (1 877 525-3823 ou www.transunion.ca/sites/ca/home_fr.page).

Liste de vérification à la suite d'une usurpation d'identité

Si vous avez été victime d'une usurpation d'identité, des mesures rapides peuvent en limiter les répercussions. Voici une liste de vérification à suivre si vous êtes victime d'une usurpation d'identité :

- Si vous découvrez des opérations non autorisées ou manquantes dans l'un de vos comptes, communiquez immédiatement avec votre succursale ou composez notre numéro accessible en tout temps, le 1 800 769-2511, ou encore le 1 800 769-2555 pour les services en ligne.
- Communiquez avec vos créanciers : sociétés de carte de crédit, sociétés de prêt hypothécaire et autres sociétés de financement avec qui vous faites affaire.
- Signalez la fraude aux autorités policières locales.

- Communiquez avec les agences de notation. Dans le cas d'une usurpation d'identité personnelle, vous devez communiquer avec les deux principales agences de notation, soit TransUnion et Equifax. Examinez votre rapport de solvabilité actuel pour déterminer si des changements non autorisés se sont produits.
- Si vous ne recevez pas votre courrier, communiquez avec Postes Canada en vous rendant au www.postescanada.ca ou en composant le 1 800 267-1177.
- Signalez l'incident à PhoneBusters, le centre d'appels antifraude du Canada. PhoneBusters recueille des renseignements sur l'usurpation d'identité et offre des conseils et du soutien aux victimes : www.phonebusters.com ou 1 888 495-8501.

Vous trouverez d'autres détails dans la section « Coordonnées » du présent document.

Manœuvres frauduleuses les plus courantes

Voici quelques manœuvres frauduleuses couramment utilisées pour obtenir l'accès aux données personnelles et financières, ainsi que nos suggestions de mesures de précaution à prendre. Vous pouvez vous protéger en demeurant informé.

Écrémage

L'écrémage consiste à obtenir des renseignements à partir de la bande magnétique d'une carte de débit ou de crédit. Bien que la carte à puce avec NIP permette de réduire le nombre de cas d'écrémage sur cartes de débit ou de crédit, il est encore possible d'écrémer la bande magnétique des cartes. La plupart du temps, les données sont enregistrées au moyen d'un lecteur de cartes lorsque la carte y est insérée. Le NIP est souvent obtenu séparément, en général par quelqu'un qui surveille le client, au moyen d'une caméra cachée ou par un dispositif perfectionné branché à l'appareil. Une fois que les données de la bande magnétique et le NIP ont été obtenus, une carte falsifiée est fabriquée puis utilisée.

Pour vous protéger contre l'écrémage, masquez toujours le clavier quand vous entrez votre NIP à un guichet automatique ou à un terminal de point de vente. N'utilisez pas un guichet automatique qui semble avoir été altéré. Vérifiez régulièrement le solde de votre compte et gardez une trace de vos débits, et signalez immédiatement toute activité frauduleuse ou disparition de fonds à votre succursale ou en appelant au 1 800 769-2511.

Fausses œuvres de bienfaisance

Si on vous demande de contribuer à une œuvre de bienfaisance, ne donnez pas votre numéro de carte de crédit au téléphone et n'acceptez pas que quelqu'un vienne chercher un chèque chez vous. Demandez à la personne qui appelle de vous envoyer une formule de don ou de vous donner son numéro de téléphone afin que vous puissiez la rappeler. Ne rappelez pas avant d'avoir vérifié personnellement que le numéro de téléphone est celui d'une organisation régulière.

Substitution de carte et piquage de NIP

Cette manœuvre frauduleuse peut survenir dans un guichet automatique. Méfiez-vous si une personne vous dit que vous avez laissé tomber quelque chose ou si elle offre de vous aider à entrer votre NIP. Pendant que vous vous penchez pour récupérer l'objet en question, le malfaiteur peut échanger votre carte contre une autre carte. Puis, un complice se tenant tout près tente de noter votre NIP pendant que vous l'entrez, ce qui permet aux deux malfaiteurs de mettre la main sur votre carte et votre NIP. Ne laissez jamais quiconque vous aider à entrer votre NIP ou voir les numéros que vous entrez. Avant de remettre votre carte dans votre portefeuille, vérifiez que le nom inscrit dessus est bien le vôtre. Dans le cas contraire, signalez l'incident en appelant sans tarder au 1 800 769-2511 (numéro accessible en tout temps) et faites annuler votre carte. N'utilisez pas un guichet automatique ni un terminal de point de vente qui semble avoir été altéré.

Télémarketing frauduleux

Certaines entreprises de télémarketing peuvent communiquer avec vous sous prétexte que vous avez gagné un prix et vous demandent ensuite votre numéro de carte de crédit ou vous informent que vous devez acheter un article promotionnel pour avoir droit au prix en question. Si vous avez des soupçons, communiquez avec PhoneBusters au 1 888 495-8501.

Offre « trop belle pour être vraie »

On peut communiquer avec vous par téléphone, par la poste, par courriel ou par télécopieur pour vous annoncer que vous avez gagné une participation dans une entreprise comportant des sommes importantes, ou que vous en avez hérité. Si vous vendez des biens personnels (p. ex., votre voiture ou tout autre bien), un fraudeur peut se faire passer pour un acheteur intéressé, faire un chèque pour un montant nettement supérieur au prix que vous demandez, puis vous rappeler pour vous demander de lui remettre le paiement en trop. Dans bien des cas, le chèque en question est volé, contrefait ou altéré et n'est retourné à RBC que bien plus tard. Tant que vous n'avez pas retourné le prétendu « paiement en trop », la victime ne s'aperçoit pas que le chèque pose un problème. N'envoyez aucun remboursement par chèque ou télévirement.

Si vous effectuez un télévirement, assurez-vous de connaître le destinataire des fonds. Si quelqu'un vous demande de faire un dépôt ou d'ouvrir un compte à son nom, vérifiez l'identité de cette personne et la validité des motifs de sa demande, même si vous entretenez un lien affectif avec elle. Soyez extrêmement vigilant lorsqu'on vous fait ce type de demande. Vous pourriez devenir le complice involontaire d'une opération de blanchiment d'argent (manipulation de fonds volés ou obtenus de façon illicite).

Fraudes d'emploi

Internet offre tant de ressources en matière d'emploi que les occasions d'affaires, de travail à la maison et de réorientation de carrière n'ont jamais été si nombreuses. Malheureusement, toutes ces offres d'emploi ne sont pas légitimes.

Méfiez-vous des offres d'emploi où l'on vous demande d'accepter des fonds et de les virer d'un compte bancaire à un autre. Souvent, le compte destinataire se trouve dans un autre pays, et on vous demande de détenir un compte dans une banque particulière au Canada. On peut vous conseiller de conserver une petite part des fonds à virer, en guise de rétribution.

Ces fraudes prennent différentes formes et peuvent être très convaincantes. Les fraudeurs peuvent demander les coordonnées du compte bancaire du candidat afin d'établir un calendrier de paiement par dépôt direct ou virer les fonds eux-mêmes à l'insu du candidat. Les fraudeurs peuvent utiliser le nom d'une entreprise et ses logos pour ajouter de la crédibilité à leur annonce ou à leur courriel. Ils peuvent également consulter les curriculum vitæ affichés en ligne et communiquer directement avec les candidats. Soyez conscient que si les fonds que vous virez sont le produit d'un vol ou d'un blanchiment, vous pourriez être le complice d'un crime en vertu de la loi.

Fraudes sur commission

Des fraudeurs peuvent utiliser le nom d'une institution financière réputée et copier sa marque et son logo pour faire la promotion de soi-disant prêts et hypothèques préapprouvés ou de taux d'intérêt inhabituellement élevés pour des produits de placement. Ils misent sur la réputation de l'institution financière et demandent à la victime un paiement immédiat pour qu'elle puisse profiter du crédit approuvé ou du produit de placement à rendement élevé.

Hameçonnage et hameçonnage vocal : fraude par courriel ou par téléphone

L'hameçonnage consiste à envoyer un courriel pour inciter le destinataire à divulguer ses renseignements personnels ou financiers. Le courriel peut parfois prévenir le destinataire d'un faux problème lié à son compte auquel il doit prêter attention sur-le-

champ. Le courriel contient un lien vers un site Web frauduleux, qui est une copie du site Web réel d'une institution financière. Le destinataire est ensuite appelé à entrer des renseignements personnels confidentiels dans le faux site Web, tels que son numéro de compte et son mot de passe, qui sont recueillis par le fraudeur. Parmi les autres types de courriels à des fins d'hameçonnage, on retrouve les annonces d'un soi-disant concours gagné par le destinataire ou d'un héritage qu'il vient de recevoir. L'objectif est de vous amener à entrer vos renseignements personnels, qui sont ensuite volés par le fraudeur afin de commettre des fraudes financières. L'hameçonnage vocal est une variante du même principe. Il existe deux approches d'hameçonnage vocal :

- Le fraudeur envoie un courriel pour avertir le destinataire à propos d'un soi-disant problème lié à son compte. Mais au lieu de fournir un lien vers un faux site Web, le courriel indique un faux numéro de téléphone pour le soutien clientèle. Lorsque le client compose ce numéro, un message automatique lui demande d'ouvrir une session en entrant son numéro de compte et son mot de passe à l'aide du clavier téléphonique. Le fraudeur obtient alors ces renseignements.
- Le fraudeur appelle directement un client ou lui laisse un message pour l'informer que son compte est peut-être à risque et qu'il doit immédiatement communiquer avec le service à la clientèle. Le fraudeur demande ensuite au client d'appeler immédiatement le soutien clientèle. Cependant, un faux numéro de téléphone est donné au client. Lorsque le client compose ce numéro, un message automatique lui demande d'ouvrir une session en entrant son numéro de compte et son mot de passe à l'aide du clavier téléphonique. Le fraudeur obtient alors ces renseignements. Le fraudeur peut aussi vous demander des renseignements confidentiels comme votre NIP, votre numéro de carte de crédit, votre code CVV2 (le numéro au verso de votre carte de crédit), votre date de naissance. Ne divulguez pas de renseignements confidentiels avant d'avoir vérifié la légitimité de la demande en composant un numéro de téléphone publié.

Ne donnez pas de renseignements personnels (en particulier votre numéro de compte, votre numéro de carte, votre NIP, votre mot de passe et vos questions et réponses de vérification) à des personnes que vous ne connaissez pas et qui communiquent avec vous en prétendant représenter votre institution financière. Afin de vous assurer que l'appel provient vraiment d'une institution financière réputée, vérifiez personnellement le numéro de téléphone avant de répondre à toute question, puis rappelez à ce numéro, même si les questions semblent légitimes.

Combines à la Ponzi

Les combines à la Ponzi attirent les investisseurs en leur offrant des rendements garantis et exceptionnellement élevés, au moyen d'instruments de placement à court terme et souvent très complexes. Les instruments de placement sous-jacents n'existent cependant pas. Les revenus de placement sont versés aux premiers investisseurs à partir de fonds provenant d'autres investisseurs, plutôt que de revenus réellement réalisés. La perpétuation de la combine demande un flux continu de fonds de nouveaux investisseurs.

Conseils pour éviter de tomber dans une combine à la Ponzi :

- Méfiez-vous des promesses de placements garantis dont les rendements sont supérieurs à la moyenne.
- Assurez-vous de recevoir des renseignements détaillés par écrit qui vous permettent de bien comprendre et évaluer les détails du placement sous-jacent.
- Informez-vous sur la personne qui vous propose le placement ; effectuez une vérification de ses antécédents et vérifiez si elle est autorisée à vendre des valeurs mobilières. Si cette personne vous dit qu'elle est exempte d'un agrément, vérifiez auprès de l'organisme de réglementation local.
- Si vous avez déjà investi et qu'on fait pression sur vous pour que vous réinvestissiez vos revenus de placement ou s'il y a arrêt de services par le promoteur, communiquez avec l'organisme de réglementation local.

Avant d'investir, prenez toujours le temps de bien vous renseigner sur le programme et le promoteur.

Exploitation financière

L'exploitation financière est l'usage illégal ou abusif des actifs, des biens ou des renseignements personnels d'une personne, parfois par un parent ou par une personne en position de confiance. Les victimes d'exploitation financière sont souvent des personnes âgées ou invalides. La personne qui exerce cette activité peut faire appel à la ruse ou à la menace pour convaincre la victime de lui remettre de l'argent, des biens ou des renseignements personnels. Si vous soupçonnez avoir été victime d'exploitation financière, communiquez immédiatement avec votre succursale pour obtenir de l'aide.

Protection des renseignements personnels

Notre engagement envers la protection des renseignements personnels

La protection de vos renseignements personnels et commerciaux constitue la pierre angulaire de notre entreprise et demeurera toujours l'une de nos priorités.

Les sociétés membres de RBC suivent des politiques et des pratiques de protection des renseignements personnels et de sécurité très rigoureuses, qui sont conformes aux lois et qui confirment notre engagement à faire preuve d'intégrité dans toutes nos actions. Nos principes de protection des renseignements personnels décrivent dans quelles conditions les renseignements sur les clients sont recueillis, utilisés et partagés, et précisent nos pratiques en matière de sécurité et vos choix à cet égard.

À RBC, nous nous sommes engagés à respecter ou à dépasser les normes de protection des renseignements personnels établies par les autorités fédérales et provinciales et par les organismes sectoriels.

Nos principes et notre politique en matière de protection des renseignements personnels

Notre politique de protection des renseignements personnels comprend nos principes de protection des renseignements personnels, qui s'appliquent à toutes les affaires que nous faisons avec vous. Les principes, tels que décrits dans la présente brochure, s'appliquent à toutes les sociétés de RBC au Canada.

Les principes sur la protection des renseignements personnels ci-dessous tiennent compte de notre engagement à préserver la confidentialité et à protéger vos renseignements personnels, financiers, en matière de santé et commerciaux.

Quels sont les renseignements recueillis ?

La plupart des renseignements recueillis proviennent directement de vous ou des références que vous nous avez fournies au moment de présenter une demande de produits ou services, de remplir un sondage ou de vous inscrire aux offres spéciales. Nous vous demandons de nous fournir uniquement les renseignements qui nous permettent de traiter votre demande, de vous offrir de meilleurs produits ou services ou de vous offrir des produits ou services susceptibles de vous intéresser.

Notre utilisation de vos renseignements

Nous utilisons uniquement vos renseignements personnels et financiers aux fins précisées dans la ou les conventions que nous avons établies avec vous. De plus, nous ne divulguerons pas vos renseignements personnels et financiers aux personnes non autorisées à les obtenir. De plus, nous ne conservons vos renseignements que pour la durée nécessaire à l'atteinte de l'objectif initial de leur obtention.

Autres utilisations de vos renseignements personnels

Dans certaines circonstances, nous pouvons partager vos renseignements personnels avec des sociétés membres de RBC ou des tiers, afin

de nous permettre de vous aider à atteindre vos objectifs financiers. Toutefois, si vous choisissez de ne pas partager vos renseignements, nous respecterons votre choix et en aviserons les autres sociétés de RBC et les tiers. Si vous ne voulez pas recevoir de documentation promotionnelle de notre part ou que vous ne voulez pas que nous partagions vos renseignements personnels avec les autres sociétés de RBC, faites-le-nous savoir en vous rendant tout simplement à l'adresse suivante : rbc.com/rensperssecurite/ca/your-consent-and-your-choices.

Protection de vos renseignements

La protection de vos renseignements personnels et financiers contre la fraude est l'une de nos priorités.

En plus des pratiques de protection des renseignements personnels rigoureuses que nous adoptons, nous utilisons une vaste gamme de technologies et de mécanismes de sécurité pour veiller à la sécurité, la confidentialité et l'intégrité de vos renseignements et opérations. Nous mettons continuellement à jour nos normes de sécurité pour que les renseignements que nous détenons sur vous soient à l'abri de toute intrusion et protégés contre toute transmission, modification ou utilisation non autorisée.

Garder vos renseignements à jour

Nous ne négligeons aucun effort pour nous assurer que les renseignements que nous détenons à votre sujet sont exacts et complets. Nous vous incitons à nous aider à conserver vos renseignements à jour en communiquant avec nous, en tout temps, pour nous donner des renseignements à jour.

Votre accès à vos renseignements personnels

Vous pouvez consulter en tout temps les renseignements que nous détenons sur vous, en vérifier l'exactitude et les faire corriger au besoin. Pour accéder à ces renseignements ou pour poser des questions au sujet de nos politiques de protection des renseignements personnels et savoir de quelle façon elles vous touchent, veuillez communiquer avec nous.

Renseignements provenant de sources externes

En plus des renseignements recueillis auprès de vous et de vos références, nous pouvons également recueillir des données financières et autres renseignements des agences d'évaluation de crédit et d'autres institutions financières. Ces renseignements sont limités à ce dont nous avons besoin pour vous offrir le meilleur service possible.

Renseignements personnels

Voici une liste des renseignements dont nous nous servons pour répondre à la plupart des demandes d'ordre financier :

- votre nom et autres coordonnées (pour les entreprises clientes, cela comprend les propriétaires, les responsables et les directeurs) ;
- votre numéro d'assurance sociale (à l'ouverture du compte) ;
- date de naissance ;
- numéros de comptes RBC ;
- historique des paiements et solvabilité.

Si vous détenez un produit qui génère un revenu, il se peut que nous utilisions votre numéro d'assurance sociale à des fins fiscales et que nous le transmettions aux organismes gouvernementaux appropriés. Nous pouvons aussi l'utiliser pour vous identifier auprès des agences de notation.

Nous pouvons recueillir des renseignements concernant votre santé auprès de vous ou de tiers, au besoin et dans la mesure autorisée par la loi, pour les produits et les services d'assurance. Les renseignements confidentiels sur votre état de santé ne seront en aucun cas partagés ou utilisés à des fins autres que celles prévues initialement.

Vous êtes toujours libre de nous fournir les renseignements demandés ou de ne pas le faire. Toutefois, si vous faites appel à nos services pour un produit d'assurance ou tout service

financier connexe et que vous refusez de nous communiquer certains renseignements, il peut être difficile, voire impossible pour nous de vous fournir les produits ou services que vous avez demandés. Il peut être d'autant plus difficile de vous conseiller ou de vous suggérer d'autres possibilités.

Nous avons besoin de renseignements pour communiquer avec vous, protéger vos intérêts et vous procurer les services que vous désirez utiliser. Vos renseignements nous servent aussi à vous tenir au courant des opérations touchant votre compte, à vérifier votre identité, à vous envoyer des avis importants et à nous efforcer de répondre à vos besoins et à vos demandes. Avec votre consentement, nous les utiliserons peut-être également pour vous envoyer des renseignements sur des produits et services qui pourraient vous intéresser offerts par d'autres sociétés membres de RBC ou par nos tiers fournisseurs.

Autres renseignements

Notre objectif est d'améliorer constamment les services que nous vous offrons. Ainsi, nous recueillons régulièrement de l'information au moyen de sondages, d'archives publiques et de sites Internet pour nous aider à comprendre les intérêts de nos clients et à gérer nos risques.

RBC utilise des outils de collecte de données en ligne afin d'améliorer la fonctionnalité, d'accroître la sécurité et d'évaluer l'efficacité de nos sites Web et de nos campagnes de marketing, ainsi que d'offrir à nos visiteurs une expérience en ligne personnalisée. Toutefois, au cours de vos visites aux sites Web de RBC, nous ne recueillons aucun renseignement permettant de vous identifier, sauf ceux que vous nous donnez volontairement. Vous pouvez naviguer librement à travers nos sites Web sans vous identifier ni nous donner aucun renseignement personnel.

Partage de vos renseignements

Nous ne transmettrons vos renseignements que dans les conditions suivantes :

En obtenant votre autorisation

Les organismes de crédit et d'autres institutions financières nous demandent régulièrement des renseignements de crédit sur nos clients. Pour pouvoir leur fournir les renseignements demandés, nous obtenons votre consentement par l'intermédiaire des conventions avec le client que vous signez lorsque vous faites l'acquisition de produits ou services précis de RBC. Ces conventions énoncent les conditions et les dispositions pour l'utilisation des renseignements.

Lorsque la loi l'exige ou nous y autorise

Nous sommes légalement tenus de communiquer les renseignements liés aux exigences officielles en matière de déclarations fiscales. Dans certains cas, tels que des poursuites judiciaires ou en réponse à une ordonnance d'un tribunal, nous pouvons aussi être tenus de communiquer certains renseignements aux autorités.

Nous prenons de strictes précautions pour nous assurer que les autorités présentant la demande ont des motifs légitimes de le faire. La loi nous autorise à communiquer des renseignements personnels lorsque nous refusons un chèque pour provision insuffisante, lorsque nous prenons des mesures juridiques à l'endroit d'un compte en souffrance, en cas d'urgence médicale ou si un client est soupçonné d'activités illégales.

À des sociétés membres de RBC

Pour vous permettre de bénéficier de la gamme complète de nos produits et services, et dans la mesure autorisée par la loi, nous pouvons communiquer des renseignements vous concernant à d'autres sociétés de RBC. Nous ne le faisons que dans les cas où les services envisagés sont offerts par une autre société de RBC, et seulement avec votre consentement.

À des employés de RBC

L'accès à vos renseignements personnels est réservé aux employés autorisés qui ont une raison légitime d'y accéder. Par exemple, si vous nous appelez, si vous vous présentez en succursale ou si vous communiquez avec nous par courriel, les préposés autorisés pourront accéder à votre dossier pour vérifier que vous êtes bien le titulaire du compte et pour vous aider à réaliser l'opération demandée.

Il est strictement interdit à tout employé de RBC de consulter ou de communiquer à des tiers des renseignements sur un client sans y avoir été autorisé. Nous exigeons que tous les employés respectent en toute circonstance le caractère confidentiel des renseignements touchant les clients, et toute infraction à cet égard entraînera des mesures disciplinaires appropriées qui peuvent aller jusqu'au renvoi.

À des fournisseurs de services externes

Il se peut que nous confiions à des tiers la prestation de services spécialisés tels que l'impression de chèques, la conduite de recherches, la création d'activités de marketing ou le traitement de données. Ces fournisseurs peuvent au besoin être chargés de traiter et de manipuler certains renseignements que vous nous fournissez. Toutefois, ils reçoivent uniquement les données nécessaires pour s'acquitter de leurs tâches. De plus, ils doivent se conformer à nos politiques et pratiques de protection des renseignements personnels et de sécurité.

Dans l'éventualité où un fournisseur de services serait situé à l'étranger, il est lié par les lois en vigueur dans le pays dans lequel il se trouve et il peut divulguer les renseignements personnels qu'il détient conformément aux lois en vigueur dans ce pays.

Questions, préoccupations et plaintes

Pour toute question concernant les politiques de protection des renseignements personnels mentionnées dans la présente brochure ou si vous désirez nous communiquer des commentaires touchant les pratiques des sociétés membres de RBC, de ses employés ou de ses fournisseurs de services à propos de la protection des renseignements personnels, du respect de leur caractère confidentiel ou du traitement de l'information, passez à votre succursale ou appelez-nous au 1 800 769-2511.

Si vous n'êtes pas entièrement satisfait de notre réponse, reportez-vous au document intitulé « Comment adresser une plainte », qui vous indiquera d'autres recours. Vous pouvez vous en procurer un exemplaire à une succursale ou à un bureau de RBC Banque Royale, par téléphone au 1 800 769-2511 ou par courriel à l'adresse clientcarecentre@rbc.com. Les utilisateurs d'ATS/téléimprimeurs doivent appeler au 1 800 661-1275.

Coordonnées

Signalement de courriels frauduleux

Sachez que les sociétés membres de RBC ne demandent jamais de renseignements confidentiels par courriel ordinaire. Si vous recevez un courriel par lequel on vous demande de fournir des renseignements confidentiels comme votre numéro de compte, votre NIP ou votre mot de passe, n'y répondez pas et veuillez nous en aviser par courriel à l'adresse information.security@rbc.com.

Pour nous aider dans nos recherches, veuillez fournir une description détaillée de l'incident et joindre à votre message tous les courriels que vous avez reçus et qui vous semblent suspects. Évitez de modifier ou de retaper une partie du message original ; cela pourrait nuire à nos recherches. Une fois que vous nous avez transmis les courriels suspects, veuillez les supprimer de votre boîte de réception. Pour de plus amples renseignements, rendez-vous au www.rbc.com/securite/bulletinPhishingf.html.

Numéros de téléphone de RBC pour les opérations bancaires, cartes de crédit et autres renseignements sur les comptes

Opérations bancaires :

- Au Canada et aux États-Unis continentaux
  1 800 769-2511
- Partout dans le monde (appels à frais virés acceptés)
  1 506 864-2275
- ATS/téléimprimeurs seulement
  1 800 661-1275

Cartes de crédit :

- Au Canada et aux États-Unis continentaux
  Service clientèle 1 800 769-2512
  Cartes perdues ou volées 1 800 361-0152
- Partout dans le monde (appels à frais virés acceptés)
  Généralités – 1 416 974-7780
  Cartes perdues ou volées – 1 514 392-9167
- ATS/téléimprimeurs seulement
  1 800 769-2518

Si vous soupçonnez que quelqu'un accède à vos comptes de RBC sans votre autorisation ou que vous avez été victime d'une fraude portant sur vos comptes, composez le 1 800 769-2511, notre numéro accessible en tout temps.

Sites Web de RBC connexes

- Protection des renseignements personnels et Sécurité
  rbc.com/rensperssecurite
- Banque en direct de RBC Banque Royale
  rbcbanqueroyale.com/endirect/guidedesecrite
- Site Web « Porter plainte »
  rbc.com/servicealaclientele

Programmes d'aide aux victimes de fraude

- PhoneBusters
  1 888 495-8501
  1 888 654-9426 (télécopieur)
  info@PhoneBusters.com

PhoneBusters entre l'information sur les fraudes dont sont victimes les consommateurs dans une base de données sécurisée qu'elle partage avec les organismes d'application de la loi à l'échelle municipale, provinciale et fédérale. La base de données est configurée et approuvée par la Police provinciale de l'Ontario et la GRC.

- Bureau de la concurrence d'Industrie Canada
  1 800 348-5358
  compbureau@ic.gc.ca

Cet organisme gouvernemental fait enquête sur les activités frauduleuses, par exemple dans le domaine du télémarketing.

- Equifax
  1 800 465-7166 ou 514 493-2314
  www.equifax.com
- TransUnion Canada
  1 877 525-3823
  www.transunion.ca/sites/ca/home_fr.page

Equifax et TransUnion Canada sont les deux agences d'évaluation de crédit qui détiennent tous vos antécédents de solvabilité dans leurs dossiers.

Autres sites Web d'intérêt

Visitez les sites Web suivants pour obtenir plus d'information sur la fraude et sur les moyens de vous protéger :

- Interac
  www.interac.ca/fr
- Association des banquiers canadiens
  www.cba.ca/index.php
- Industrie Canada
  www.strategis.ic.gc.ca
- Bureau de la consommation du Canada
  www.ic.gc.ca/eic/site/oca-bc.nsf/fra/accueil
- Agence de la consommation en matière financière du Canada – Avis au consommateur
  www.fcac-acfc.gc.ca/fra/consommateurs/avis/default.asp
- Commissariat à la protection de la vie privée du Canada
  www.priv.gc.ca/index_f.cfm
- Visa Canada
  http://www.visa.ca
- MasterCard Canada
  www.mastercard.com/ca/gateway/fr/index.html

Annexe

Dix conseils pour protéger vos actifs

1. **Assurez-vous que vos renseignements personnels sont en sécurité.** Les usurpateurs d'identité fouillent dans les ordures et les bacs de recyclage. Vous devez donc déchiqueter vos reçus, vos copies de demande de crédit, vos formulaires d'assurance, les offres de crédit reçues par la poste, etc.
2. **Assurez-vous que vos renseignements personnels restent confidentiels.** 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.
3. **Souvenez-vous des cycles de facturation et de 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. Demandez des relevés électroniques.
4. **Protégez votre courrier.** Prenez votre courrier chaque jour. Faites-le suivre ou faites-le réacheminer si vous déménagez ; changez votre adresse postale si vous vous absentez.
5. **Protégez votre NIP et vos mots de passe.** Ne divulguez à personne votre NIP et vos mots de passe, y compris aux employés de RBC, aux membres de votre famille ou à vos amis. Lorsque vous effectuez une opération, ne perdez jamais de vue votre carte et cachez le clavier numérique lorsque vous entrez votre NIP.
6. **Limitez vos risques.** Signez toutes vos cartes de crédit dès que vous les recevez. Signalez immédiatement toute perte ou tout vol de carte.
7. **Opérations anormales.** Méfiez-vous des offres qui semblent trop belles pour être vraies ou des demandes inattendues et inespérées de type : « Vous avez hérité d'un gros montant d'argent. Pour le réclamer, envoyez-nous d'abord un

dépôt. » Vous ne devriez jamais consentir à exécuter des opérations financières pour le compte d'inconnus.

8. **Passez vos opérations en revue.** Vérifiez régulièrement vos relevés pour vous assurer que toutes les opérations sont autorisées et pour signaler toute opération manquante ou frauduleuse. Vérifiez votre rapport de solvabilité tous les ans.
9. **Limitez votre exposition à la fraude.** N'ayez dans votre portefeuille que les cartes de crédit que vous utilisez. Ne transportez pas votre extrait d'acte de naissance ni votre carte d'assurance sociale lorsque vous n'en avez pas besoin ; conservez-les plutôt en lieu sûr.
10. **Communiquez avec les autorités.** Si vous pensez être victime d'une fraude ou d'un vol, communiquez sur-le-champ avec les autorités.

Dix conseils pour des pratiques informatiques sécuritaires et la protection des renseignements personnels en ligne

1. **Protégez vos renseignements personnels.** Soyez à l'affût des escrocs qui essaient de vous soutirer des renseignements personnels ou financiers. Ne répondez pas aux courriels ou aux appels téléphoniques non sollicités de personnes qui vous demandent de donner des renseignements personnels.
2. **Choisissez des mots de passe efficaces.** Le choix d'un mot de passe unique, à la fois difficile à deviner pour les autres et facile à mémoriser pour vous, est essentiel à la sécurité informatique. Utilisez plusieurs mots de passe, modifiez-les fréquemment et composez-les au moyen d'une combinaison de lettres et de chiffres.
3. **Vérifiez toujours un message avant de prendre des mesures.** Évitez de cliquer sur un lien, de composer un numéro de téléphone, de procéder à un télévirement ou de prendre toute mesure demandée dans un message

avant d'avoir confirmé l'authenticité de ce message. Pour la vérification, servez-vous de renseignements provenant d'une autre source que le message lui-même.

4. **Limitez l'accès en ligne à vos renseignements personnels.** Soyez vigilant à propos de la diffusion de vos renseignements personnels en ligne, dans les sites de réseautage, lors de séances de clavardage et dans les courriels non chiffrés car les fraudeurs peuvent tenter d'accéder à vos renseignements pour les utiliser à leurs fins.
5. **Faites preuve de vigilance lorsque vous êtes en ligne.** N'oubliez pas que de nouvelles fraudes par courriel et de nouveaux sites Web malveillants surgissent lors d'événements publicisés ou de l'apparition de nouvelles manchettes. Supprimez les courriels suspects et soyez prudent lorsque vous accédez à de nouveaux sites.
6. **Méfiez-vous des fenêtres contextuelles.** Méfiez-vous des fenêtres contextuelles, particulièrement de celles qui demandent des renseignements financiers ou d'identification.
7. **Installez une suite complète de logiciels de sécurité sur votre ordinateur.** La suite doit comprendre un coupe-feu personnel, un antivirus, un outil pour lutter contre les pourriels et un anti-logiciel espion ; tous ces produits sont nécessaires à la protection en ligne de votre ordinateur et de vos renseignements. Méfiez-vous des fenêtres contextuelles vous indiquant que votre ordinateur est contaminé et vous demandant d'acheter ou de télécharger un logiciel servant à résoudre le problème.
8. **Protégez votre ordinateur.** Utilisez les processus autorisés de mise à jour des logiciels pour votre navigateur Web, votre système d'exploitation et tous les logiciels requis pour vos activités en ligne (par exemple, vos modules externes de navigation tels que des visualisateurs PDF), et vérifiez régulièrement les sites pertinents afin d'obtenir les rustines et les mises à jour les plus récentes.

9. **N'oubliez pas de fermer votre session.** Assurez-vous de toujours bien fermer la session et de quitter votre navigateur. Vous éviterez ainsi que d'autres personnes puissent consulter vos renseignements.
10. **Si cela semble trop beau pour être vrai, c'est probablement une arnaque !** Méfiez-vous des courriels et des sites Web qui promettent des affaires en or et des occasions à ne pas manquer. Vous pourriez fournir vos renseignements financiers à des fraudeurs ou télécharger un logiciel malveillant en cliquant sur un lien attirant.

Pour en savoir plus, rendez-vous sur le site rbc.com/rensperssecurite/ca/index.

Pour obtenir des renseignements supplémentaires concernant nos produits et services, consultez un représentant du service clientèle ou :

› allez dans une succursale près de chez-vous pour rencontrer un conseiller ;

› composez le 1-800 ROYAL® 1-1 (1 800 769-2511) ;

› allez à rbc.com/francais/canada.html.

Composez le 1 800 661-1275 (ATS/téléimprimeurs seulement). Cette publication est également disponible dans des formats convenant aux personnes ayant une perte de vision.

This document is also available in English.
Ce document est aussi offert en anglais.

RBC®

57469 (04/2010)