

Conseils pour protéger vos données personnelles et financières

Nous sommes tous inquiets face à nos données personnelles et financières. Bien que RBC ait adopté des mesures de protection rigoureuses en ce qui concerne la sécurité et la technologie, vous pouvez vous aussi contribuer à la protection de vos données personnelles. En suivant les étapes simples ci-dessous, vous réduisez le risque de vol ou de mauvaise utilisation de vos données personnelles et financières.

Dix conseils pour préserver votre sécurité informatique

1. Protégez vos renseignements personnels.

Soyez à l'affût des escrocs sur le Web qui essaient de vous soutirer des renseignements personnels ou financiers. Ne répondez pas aux courriels ou messages vocaux non sollicités vous demandant des renseignements confidentiels.

2. Protégez votre ordinateur. Il est très important de consulter les sites Web des fournisseurs de votre système d'exploitation et de votre navigateur pour y trouver les correctifs et mises à jour qui vous protégeront contre les vulnérabilités de vos logiciels.

3. Protégez vos NIP et vos mots de passe.

Ne divulguez jamais vos mots de passe. Choisissez des mots de passe difficiles à deviner et comportant de préférence des lettres et des chiffres. Changez fréquemment vos mots de passe.

4. Utilisez un logiciel antivirus. Les logiciels antivirus peuvent vous protéger des virus potentiellement dangereux qui peuvent entrer à votre insu dans votre ordinateur. Vous devez toujours utiliser un logiciel antivirus à jour capable de vérifier si les fichiers et les messages électroniques ne contiennent pas de virus.

5. Utilisez un pare-feu personnel. Les pare-feux créent une barrière entre votre ordinateur et Internet. Ils peuvent déjouer les attaques malicieuses et empêcher certains types de données d'entrer dans votre ordinateur.

6. Utilisez un anti-logiciel espion. Un anti-logiciel espion protégera votre ordinateur contre les intrus qui tentent d'installer des programmes dans votre ordinateur à votre insu. Il contribuera également à la protection de votre logiciel

contre les publicités intempestives et la diminution de la performance.

7. Utilisez un logiciel anti-pourriel. Les pourriels sont des sources croissantes de virus informatiques. Utilisez un logiciel anti-pourriel avec votre logiciel antivirus. Si vous recevez des pourriels, suivez cette règle d'or : pas d'essai, pas d'achat, pas de réponse. Supprimez-les tout simplement.

8. Utilisez un chiffrement poussé. Plus le chiffrement qu'utilise votre navigateur est complexe, plus un utilisateur non autorisé aura du mal à intercepter vos activités en ligne.

9. Déconnectez-vous d'Internet quand vous ne l'utilisez pas. En vous déconnectant d'Internet quand vous ne l'utilisez pas, vous réduisez le risque que quelqu'un accède à votre ordinateur.

10. 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 visualiser l'information.

Pour en savoir plus, visitez le site www.rbc.com/securite.

Dix conseils pour protéger vos actifs

1. Protégez vos renseignements personnels.

Les usurpateurs d'identité fouillent dans les poubelles ou 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. Sachez quels sont vos cycles de facturation. Si vos factures n'arrivent pas à temps, faites un suivi immédiat pour vous assurer qu'elles n'ont pas été réacheminées de façon frauduleuse.

4. Protégez votre courrier. 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.

5. Protégez votre NIP. Ne communiquez à personne votre NIP, pas même aux membres de votre famille et à vos amis. Lorsque vous effectuez une opération à un guichet automatique ou à un point de vente de détail, ne perdez pas de vue votre carte-client et dissimulez le clavier lorsque vous composez votre NIP.

6. 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.

7. Opérations anormales. N'effectuez jamais d'opération financière au nom de personnes inconnues.

8. Passez vos opérations en revue. Vérifiez régulièrement vos relevés de comptes bancaires et de cartes de crédit pour vous assurer que toutes les opérations sont autorisées et pour signaler toute opération manquante. Vérifiez votre rapport de solvabilité une fois par an.

9. Limitez votre exposition à la fraude. N'ayez dans votre portefeuille que les cartes de crédit dont vous avez besoin. Laissez votre certificat de naissance et votre carte d'assurance sociale à la maison, dans un endroit 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.

Pour obtenir de plus amples renseignements sur les fraudes visant les consommateurs, ainsi que sur la politique de protection des renseignements personnels ou les produits et services de RBC, composez le 1 800 769-2511 ou consultez le site www.rbc.com.

