option consommateurs

Prévenir le vol d'identité

1. Qu'est-ce que le vol d'identité ?

Il y a vol ou usurpation d'identité lorsqu'un individu utilise vos renseignements personnels à votre insu afin d'en tirer frauduleusement un bénéfice, financier ou autre.

Quels renseignements ? Voici quelques exemples :

- nom, adresse, numéro de téléphone
- date de naissance
- nom de fille de la mère
- numéros de cartes d'identité importantes :
- assurance sociale (NAS)
- permis de conduire
- assurance maladie
- numéro de carte de crédit et date d'expiration
- numéro de compte bancaire, de carte de débit et numéro d'identification personnel (NIP).

Comment est-ce possible ?

Vous pouvez vous faire voler votre identité à la suite du :

- vol (ou perte) d'un sac à main ou d'un porte-monnaie
- vol de courrier (ou d'un changement d'adresse frauduleux)
- vol de documents mis à la poubelle ou au recyclage
- vol d'un ordinateur
- vol de maison ou de voiture.

Cependant, les fraudeurs n'ont pas besoin d'avoir vos renseignements personnels en main pour usurper votre identité. Bien d'autres moyens existent pour subtiliser vos renseignements là où ils se trouvent.

Ils utilisent :

- Le clonage de cartes de débit ou de crédit. Il s'agit de copier à votre insu les informations contenues sur vos cartes pour retirer ensuite des fonds.
- Le vol ou piratage d'une base de données appartenant à une organisation publique ou privée, où sont notés par exemple votre NAS, votre adresse, votre date de naissance, même vos coordonnées bancaires.
- Le piratage de votre ordinateur personnel ou professionnel.
- Les renseignements personnels volés ou révélés par des personnes provenant de votre entourage, ou encore par des employés corrompus au sein d'une organisation publique ou privée.
- Le télémarketing frauduleux. Par exemple, on fait croire au consommateur qu'il a gagné un prix, mais il doit acquitter des taxes ou divers frais fictifs pour le recevoir. Cette pratique est illégale et peut se faire par la poste, le téléphone ou le courrier électronique.
- L'hameçonnage. Vous recevez un courriel de votre banque ou d'une autre entreprise vous affirmant, par exemple, qu'elle a mis à niveau ses mesures de sécurité pour vous protéger contre le vol d'identité. En fait, des fraudeurs se faisant passer pour des employés d'une entreprise légitime vous invitent à cliquer sur un lien vous amenant sur un site fictif afin d'actualiser vos renseignements personnels. Ils utilisent ensuite ces renseignements pour commettre une fraude.

2. Les lois qui nous protègent

Au Québec, plusieurs lois assurent la protection de la vie privée, et plus particulièrement la protection de vos renseignements personnels. Ainsi, les numéros qui servent à vous identifier sont confidentiels et ne devraient être divulgués que dans certaines circonstances particulières.

Par exemple :

- En vertu de la *Loi sur l'impôt du revenu*, seules les personnes (employeurs, ministères, organismes gouvernementaux et institutions financières) ayant besoin du numéro d'assurance sociale à des fins fiscales peuvent l'exiger. Une exception : on doit également le fournir à Hydro-Québec.
- En vertu du *Code de la sécurité routière*, seuls les employés de la Société de l'assurance automobile du Québec (SAAQ) et les policiers (dans ce dernier cas, seulement lorsque la sécurité routière est en jeu) peuvent exiger le numéro de permis de conduire.
- En vertu de la *Loi sur l'assurance maladie*, seuls les professionnels de la santé peuvent exiger le numéro de carte d'assurance maladie, et seulement en vue de prodiguer des soins.

Les autres entreprises peuvent toujours demander ces numéros, mais elles n'ont pas le droit de les exiger. Dans un club vidéo, par exemple, vous pourriez montrer votre permis de conduire ou votre carte d'assurance maladie pour qu'on vous identifie avec la photo, sans toutefois permettre qu'on note le numéro.

Si vous consentez malgré tout à divulguer vos renseignements personnels à une entreprise, sachez que les entreprises privées sont soumises à la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP).

Adoptée en 1994, la LPRPSP encadre les activités des entreprises privées qui recueillent, détiennent, utilisent ou communiquent des renseignements personnels. Elle établit des principes qui visent à protéger vos renseignements personnels dès leur cueillette et jusqu'à leur destruction. Ces principes aident à prévenir l'usurpation d'identité dans la mesure où ils sont respectés par les entreprises privées.

Voici les huit principes qu'une entreprise doit suivre pour protéger vos renseignements personnels collectés :

1. Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées.
2. Toute personne doit être informée et consentir à toute collecte, utilisation ou communication des renseignements personnels qui la concernent.
3. Une entreprise ne doit recueillir que les renseignements nécessaires aux fins déterminées.
4. Les renseignements personnels recueillis ne doivent être utilisés qu'aux fins prédéterminées auxquelles la personne concernée a consenti.
5. On ne doit pas conserver les renseignements personnels plus longtemps que nécessaire pour la réalisation des finalités déterminées.
6. Les renseignements personnels doivent être aussi exacts et à jour que le requièrent les fins pour lesquelles ils sont recueillis.
7. Les renseignements personnels doivent être protégés au moyen de mesures de sécurité appropriées.
8. La personne doit avoir accès aux renseignements personnels qui la concernent et pouvoir y faire apporter les corrections appropriées.

« Pas de numéro ? Pas de service ! »

Une entreprise ne peut, sauf exception, vous obliger à divulguer un renseignement personnel. Si on refuse de vous offrir un service parce que vous avez refusé de transmettre un numéro de permis de conduire, de carte d'assurance maladie ou autre, n'hésitez pas à porter plainte. Voici, selon le cas, où vous pouvez déposer votre plainte.

Lorsqu'une entreprise publique ou privée, qui refuse de vous offrir un service, exerce ses activités dans un domaine de compétence fédérale (par exemple une banque ou une entreprise de télécommunications), vous devez vous adresser au Commissaire à la vie privée du Canada. Information : 1 800 282-1376, www.privcom.gc.ca.

Si l'entreprise qui refuse de vous offrir un service exerce ses activités dans un domaine de compétence provinciale (par exemple, un club vidéo ou un bureau professionnel), vous devez vous adresser à la Commission d'accès à l'information. Information : 1 888 528-7741, www.cai.gouv.qc.ca.

En refusant de divulguer vos numéros personnels et en portant plainte au besoin, vous contribuerez à renverser la tendance qui consiste à stocker le plus de renseignements possible. Une tendance dangereuse puisque plus un fraudeur en sait long sur vous, plus il lui sera facile d'usurper votre identité.

3. Les attitudes qui nous protègent

Prenez de bonnes habitudes pour éviter des problèmes

Soyez prudent lorsque vous divulguez des renseignements personnels.

Surtout, ne donnez vos numéros d'identification – assurance sociale, assurance maladie, permis de conduire – que lorsque vous êtes tenu de le faire par la loi. Dans ce cas, informez-vous de ce qui motive une telle demande, des personnes qui auront accès à vos renseignements et de la façon dont ils seront utilisés et protégés.

Faites le tri dans votre portefeuille

N'apportez avec vous que les cartes d'identité dont vous avez vraiment besoin.

En cas de perte ou de vol de votre portefeuille, communiquez immédiatement avec les sociétés émettrices de cartes de crédit et les institutions financières. Signalez également la perte ou le vol de documents délivrés par le gouvernement ou les établissements publics, comme un permis de conduire, une carte d'assurance maladie, une carte d'hôpital.

Soyez vigilant à propos de vos cartes bancaires

Ne perdez jamais de vue votre carte de crédit ou de débit lorsque vous l'utilisez pour faire un achat.

Choisissez un code d'accès (NIP) qui ne peut pas être découvert facilement. N'utilisez pas une combinaison qui comprend votre nom, votre numéro de téléphone, votre date de naissance, votre adresse, votre numéro d'assurance sociale ou la date de naissance d'un enfant dont vous auriez la carte dans votre portefeuille.

Cachez toujours votre NIP avec votre main lorsque vous le saisissez sur le clavier. Même s'il n'y a personne autour de vous, des caméras vous surveillent.

Ne divulguez pas les numéros de vos cartes de crédit par téléphone, à moins que vous ayez fait vous-même l'appel ou que vous sachiez à qui vous avez affaire.

N'utilisez pas un téléphone cellulaire ou un téléphone sans fil pour effectuer des opérations bancaires.

Prenez en note le numéro et la date d'expiration de vos cartes de crédit et gardez ces renseignements en lieu sûr, afin de pouvoir aviser rapidement les sociétés émettrices d'une perte ou d'un vol.

Coupez toute carte de débit ou de crédit périmée ou inutilisée.

Ne laissez pas traîner vos documents

Vérifiez vos comptes et votre courrier. Ayez une boîte aux lettres verrouillée et, lorsque vous êtes en voyage, demandez à un voisin de ramasser rapidement votre courrier ou à Postes Canada de le retenir.

Déchiquetez ou brûlez les documents sur lesquels figurent des renseignements personnels ou financiers, comme les relevés, les factures, les reçus ou les offres de carte de crédit.

Ne laissez pas traîner de documents contenant des renseignements personnels dans la voiture, au travail, ni même à la maison. Rangez-les plutôt à l'abri des regards indiscrets.

Protégez votre ordinateur

Protégez les informations dans votre ordinateur (voir détails ci-dessous). Soyez très prudent lorsque vous donnez des informations personnelles sur Internet. (voir page 12).

Ne laissez jamais votre ordinateur portable dans la voiture ou dans un autre endroit où il pourrait être volé facilement.

Assurez-vous de supprimer vos renseignements personnels avant de vous débarrasser de votre ordinateur ou de le vendre. Utilisez un logiciel de nettoyage ou reformatez le disque dur, car celui-ci peut contenir des renseignements même après que vous avez supprimé les fichiers dans les dossiers.

Vérifiez votre dossier de crédit

Consultez chaque année votre dossier de crédit afin de vous assurer que les informations qui y sont consignées sont exactes et qu'il ne contient aucune dette que n'avez pas contractée.
(Equifax : 514 493-2314, www.equifax.ca
TransUnion : 514 335-0374, www.transunion.ca.)

4. Les pièges dans Internet

Chaque consommateur doit adopter certains comportements sécuritaires dans Internet afin de réduire au minimum les risques d'être victime de vol d'identité.

Code de conduite à suivre :

1. Limitez l'accès à votre ordinateur, protégez votre réseau si vous avez un routeur sans fil wi-fi (voir page page 11).
2. Créez des mots de passe difficiles à deviner. Les mots de passe devraient contenir au moins huit signes (lettres et chiffres). N'utilisez pas les fonctions d'accès automatique qui mémorisent votre mot de passe et votre code d'utilisateur.
3. Maintenez à jour vos logiciels, surtout vos logiciels de sécurité.
4. Soyez prudent lorsque vous donnez des renseignements personnels sur Internet (voir page 12).
5. Faites une copie de vos fichiers importants et rangez-la en lieu sûr.
6. Prenez garde avant d'ouvrir un fichier joint ou d'activer un hyperlien. Si vous ne connaissez pas l'adresse courriel de l'expéditeur, méfiez-vous!
7. Ne donnez pas suite à un courriel vous invitant à communiquer des renseignements à votre banque ou à votre caisse. Les entreprises dignes de confiance ne procèdent jamais de la sorte. Si vous avez le moindre doute, communiquez avec votre institution financière en composant un numéro de téléphone de l'annuaire, et surtout pas celui qui est indiqué dans le courriel.
8. Avant de faire des transactions et achats en ligne, assurez-vous que l'adresse du site est bien sécurisée. L'adresse URL doit commencer par https//. Le « s » après http vous signifie qu'il s'agit d'un site sécurisé, de même que le petit cadenas fermé ou une clé au bas à droite de la page web. Si le site les accepte, c'est que vous êtes sur un site frauduleux.

9. Effectuez vos achats en ligne auprès d'entreprises renommées. Avant d'utiliser un service dont vous n'avez jamais entendu parler, faites certaines vérifications. Consultez le site web de l'entreprise, appelez son service à la clientèle et lisez les modalités de contrat et l'énoncé de confidentialité. Si vous n'êtes pas rassuré, n'utilisez pas ce service.
10. Conservez une preuve de vos transactions, par exemple en notant les numéros de confirmation, et vérifiez vos relevés.
11. N'utilisez pas la connexion sans fil pour donner des renseignements personnels. Débranchez ou désactivez votre équipement sans fil lorsque vous ne vous en servez pas.
12. Si vous êtes dans l'obligation d'utiliser un ordinateur public pour effectuer des opérations bancaires, videz la mémoire cache de votre navigateur, supprimez l'historique et fermez le navigateur.

Comment sécuriser son réseau wi-fi ?

Toute l'information que vous donnez ou que vous recevez par le routeur sans fil (wi-fi) est transmise sous forme de signal radio et peut donc être interceptée par n'importe qui. D'où la nécessité de sécuriser votre réseau. À cette fin, lisez bien les instructions qui accompagnent votre routeur. La première étape est de changer le mot de passe par défaut de l'appareil. Ainsi, personne d'autre que vous ne pourra accéder au routeur. Bien sûr, il faudra noter ce mot de passe pour ne pas l'oublier. Deuxième étape, il est bon de configurer une clé d'accès au routeur (voir votre guide d'utilisation). On vous demandera cette clé vous pour vous connecter au réseau sans fil. Donc, même si quelqu'un détecte votre réseau, il ne lui sera pas possible de se brancher sans la clé. Cette clé peut être une suite de lettres et de chiffres. Veillez à ce qu'elle ne soit pas trop facile à imaginer. Beaucoup de routeurs offrent également d'autres niveaux de sécurité, notamment le cryptage des données. Explorez votre guide d'utilisation, cela peut être très intéressant !

5. Les dangers sur les réseaux sociaux (Facebook, Myspace, Classmate, Réseau Contact, etc.)

Via les réseaux sociaux, un fraudeur pourrait :

- se faire passer pour quelqu'un d'autre afin de gagner votre confiance, puis vous harceler ou nuire à votre réputation
- épier vos échanges pour obtenir des renseignements personnels et usurper votre identité
- transmettre à votre ordinateur des virus ou des logiciels espions en vous envoyant un courriel.

Comment vous protéger ?

N'affichez aucun renseignement personnel dans votre profil. La GRC recommande, dans la mesure du possible, de ne pas entrer votre nom au complet, votre date de naissance, votre adresse résidentielle, votre numéro de téléphone, votre NAS et tout renseignement qui pourrait présenter de l'intérêt pour un prédateur financier. Peut-être pourriez-vous plutôt utiliser un pseudonyme.

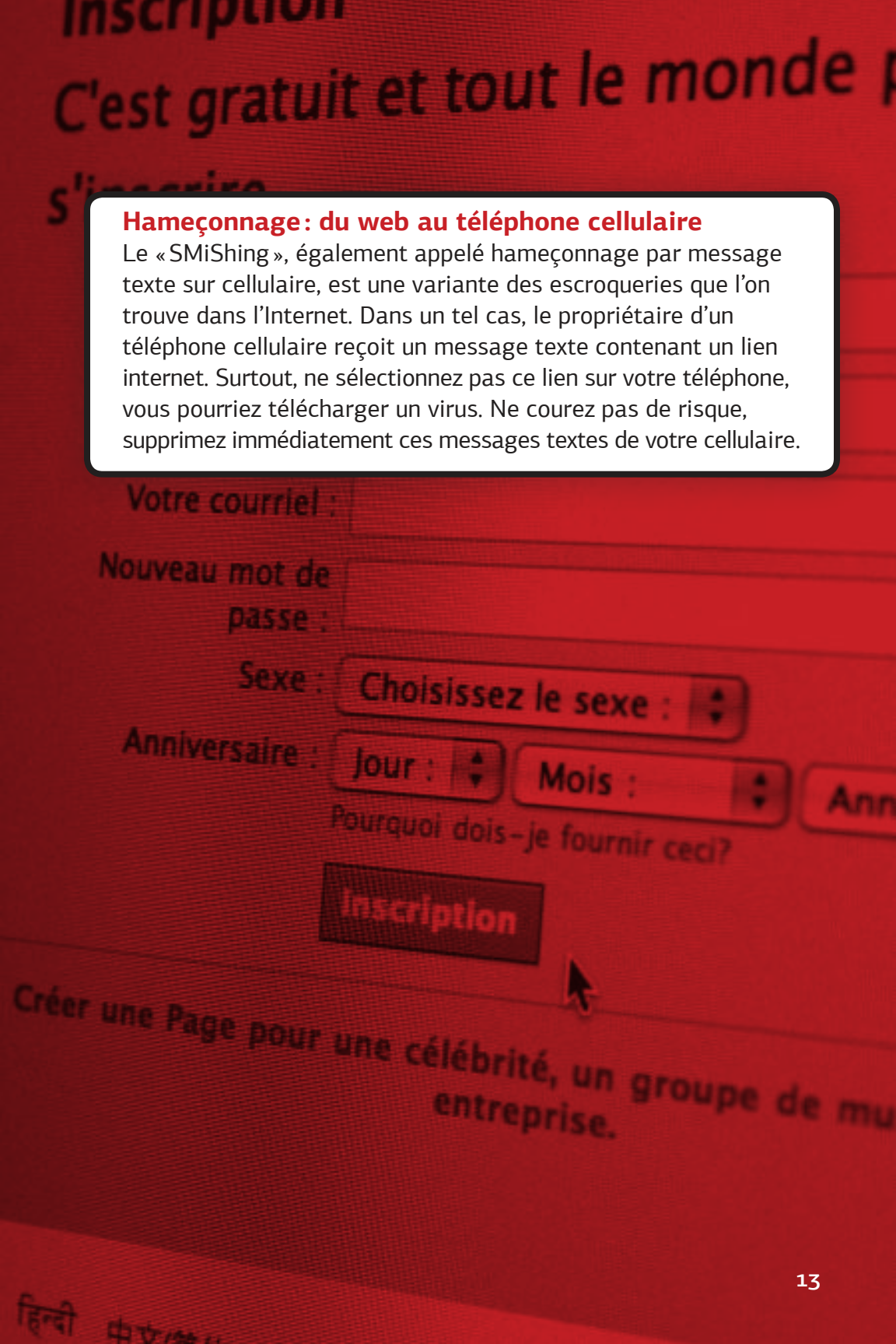
Ne donnez aucun renseignement personnel lors de vos conversations (messagerie instantanée ou groupes de discussion).

Protégez la confidentialité de vos parents et de vos amis en ne donnant aucun renseignement personnel à leur sujet.

Ne permettez pas à des étrangers d'accéder à votre profil.

Utilisez des logiciels antivirus et anti-espion.

Soyez prudent quand vous écrivez dans les blogues et les groupes de discussion, car il est très facile de perdre le contrôle de ce qui est publié sur le web.



Hameçonnage : du web au téléphone cellulaire

Le « SMiShing », également appelé hameçonnage par message texte sur cellulaire, est une variante des escroqueries que l'on trouve dans l'Internet. Dans un tel cas, le propriétaire d'un téléphone cellulaire reçoit un message texte contenant un lien internet. Surtout, ne sélectionnez pas ce lien sur votre téléphone, vous pourriez télécharger un virus. Ne courez pas de risque, supprimez immédiatement ces messages textes de votre cellulaire.

6. En cas de vol d'identité : agir vite et ne rien oublier !

Avec votre identité, un voleur peut ouvrir des comptes de banque, acheter un téléphone cellulaire, contracter une hypothèque sur votre propriété, même acheter une automobile ou des meubles.

Arrivent alors...

- Des achats inexpliqués sur vos relevés mensuels.
- Des factures pour des comptes inconnus.
- Des appels d'agences de recouvrement réclamant une dette inconnue.
- Des dettes mystérieuses dans votre dossier de crédit.
- Etc.

Ce qu'il faut faire

En cas de vol ou de perte de vos cartes, agissez vite ! Annulez rapidement vos cartes de crédit et de débit auprès des institutions qui les ont émises.

Contactez rapidement les agences de crédit Equifax et TransUnion. Afin de faire inscrire à votre dossier un avis de fraude. (Equifax: 514 493-2314, www.equifax.ca. TransUnion: 514 335-0374, www.transunion.ca.)

Si vous avez l'impression que quelqu'un détourne votre courrier, communiquez avec la Société canadienne des postes.

Appelez la police ou présentez-vous au poste de police de votre quartier (ou ville) afin de faire un rapport.

Demandez le numéro du rapport qui a été fait et conservez-le précieusement. Il se peut qu'un fraudeur ne se serve que des années plus tard d'informations amassées à propos d'un consommateur.

Signalez la fraude à PhoneBusters. (voir l'encadré de la page suivante).

Signalez la fraude !

Que vous soyez victime d'un vol d'identité ou que vous ayez repéré quelque chose d'anormal (un appel téléphonique ou un message électronique douteux), n'hésitez pas à contacter le centre d'appel anti-fraude du Canada, PhoneBusters. Créé en janvier 1993, PhoneBusters est dirigé par la Police provinciale de l'Ontario, la Gendarmerie royale du Canada et le Bureau de la concurrence du Canada. C'est l'organisme national chargé de recueillir les plaintes en matière de télémarketing, de lettres et de courriers électroniques frauduleux, ainsi qu'en matière de vol d'identité. PhoneBusters reçoit ainsi plus 145 000 appels par an et pas moins de 40 000 courriels par mois de personnes leur signalant une pratique frauduleuse. Les données recueillies sont ensuite utilisées dans l'évaluation des répercussions de la fraude sur le public et aident à prévenir d'autres crimes. Experts en vol d'identité, les agents d'appel de PhoneBusters répondront à vos questions. Vous pouvez les joindre au 1 888 495-8501. Site web : www.phonebusters.com.

Sources d'information

- Les agences de crédit Equifax et TransUnion
- Phonebusters
- Commissaire à la protection de la vie privée du Canada
- Commission d'accès à l'information
- Communication Québec
- Sécurité publique du Québec
- Mon identite.isiq.ca

Ouvrage produit par Option consommateurs
Coordination : Claire Harvey, rédactrice en chef du Service d'agence de presse
Rédaction et recherche : Séverine Galus, journaliste, Service d'agence de presse
Design : Renzo design
La commissaire à la vie privée du Canada a apporté son aide financière à cette initiative

option consommateurs

Un argument de poids

À propos d'Option consommateurs

Créée en 1983, Option consommateurs est une association sans but lucratif vouée à la défense et à la promotion des droits des consommateurs. Pour ce faire, elle s'intéresse de près aux questions reliées notamment aux pratiques commerciales, aux services financiers, à la protection de la vie privée, à l'énergie et à l'agroalimentaire. Elle ne craint pas non plus de s'engager dans des recours collectifs lorsqu'elle le juge utile.

2120, rue Sherbrooke Est
bureau 604
Montréal (Québec) H2K 1C3

Téléphone : 514 598.7288
Télécopieur : 514 598.8511
info@**option-consommateurs.org**

✂ ----------

❍ Oui, je désire devenir membre d'Option consommateurs

Adhésion + cotisation(s)
(2 $ de part sociale obligatoire)

❍ 1 an : 22 $
❍ 2 ans : 42 $

Don de charité _____ $
(un reçu d'impôt sera émis pour tout don supérieur à 10 $)

Je joins un chèque de _____ $

Je souhaite payer par ❍ Visa ❍ Mastercard date d'expiration ___ / ___

_____
Nom du détenteur

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Numéro

Nom _____

Adresse _____

Ville _____ Province _____

Code postal _____

Courriel _____