

La sécurité de votre NIP et de vos mots de passe est la clé pour protéger votre argent.

Pour signaler la perte ou le vol de votre carte, une activité frauduleuse ou des problèmes de sécurité Internet, composez immédiatement un des numéros suivants :

Service en français : 1-800-575-2424  
Région de Toronto : 416-701-7222

Service in English: 1-800-4-SCOTIA  
(1-800-472-6842)

In the Toronto Area: 416-701-7200

Par télémétreur/ATS : 1-800-645-0288

Pour protéger votre argent...  
Protégez votre NIP

Paiement direct • GAB • Internet •  
Téléphone • Sans fil



Vous êtes plus riche que vous le croyez.<sup>MC</sup>

<sup>MD</sup> Marque déposée de La Banque de Nouvelle-Écosse.  
<sup>MC</sup> Marque de commerce de La Banque de Nouvelle-Écosse.  
† Interac Inc. propriétaire de la marque. La Banque de Nouvelle-Écosse usager autorisé.  
\* VISA Int./Usager lic. La Banque de Nouvelle-Écosse.

9221034 (01/09)



Votre numéro d'identification personnel (NIP) et vos mots de passe sont des codes secrets qui vous permettent – à vous et à vous seul – d'accéder à vos comptes à partir de guichets automatiques bancaires (GAB), de terminaux de paiement direct, des Services financiers Scotia en direct<sup>MD</sup> et des services bancaires par téléphone TéléScotia<sup>MD</sup>.

La sécurité de votre NIP, de votre code d'accès TéléScotia et de votre mot de passe Scotia en direct est la clé pour protéger votre argent. Même si la Banque Scotia prend de solides mesures pour assurer la sécurité de vos opérations financières et la confidentialité de vos renseignements personnels, c'est à vous qu'est dévolu le rôle principal. Le choix d'un NIP sécuritaire pour votre Carte Scotia<sup>MC</sup> aussi bien que pour votre carte VISA\* et le maintien du secret de ces renseignements contribuent à protéger votre argent.

### Comment protéger votre NIP et vos mots de passe :

- Choisissez un code unique de quatre caractères (chiffres, lettres ou mélange des deux) dont vous pourrez vous souvenir. NE CHOISISSEZ PAS votre date de naissance, votre numéro de téléphone, le code de votre plaque d'immatriculation ou toute autre combinaison facile à deviner.
- Mémorisez votre NIP et vos mots de passe. NE LES INSCRIVEZ nulle part et NE LES RÉVÉLEZ à personne.
- N'oubliez pas de masquer le clavier lorsque vous tapez votre NIP à un guichet automatique bancaire ou lorsque vous effectuez un achat par paiement direct Interac<sup>®</sup> ou en utilisant votre carte VISA.
- Contactez-nous immédiatement si vous avez des raisons de penser que la sécurité de votre carte et/ou de votre NIP a été compromise.



### Conseils pour prévenir la fraude

- Vérifiez vos relevés mensuels et avisez-nous immédiatement si vous constatez des activités inhabituelles (par exemple, des achats que vous n'avez pas faits ou des frais manquants).
- Ayez toujours l'œil sur votre carte pendant une opération et ne la prêtez JAMAIS à qui que ce soit.
- Signalez immédiatement la perte ou le vol d'une carte.
- Ne prêtez votre carte à personne, ni même à quelqu'un de très proche de vous.

Vous pouvez obtenir une nouvelle Carte Scotia ou une Carte Scotia de remplacement et changer de NIP pour votre Carte Scotia ou votre carte VISA dans toutes les succursales Scotia du Canada. Il est possible de modifier le NIP d'une Carte Scotia ou d'une carte VISA à un guichet Scotia. Pour de plus amples renseignements, reportez-vous à votre Contrat Carte Scotia (exemplaires disponibles dans toutes les succursales Scotia).

### Comment vous protéger lorsque vous faites des opérations bancaires en ligne :

- N'envoyez jamais de renseignements confidentiels (numéro de compte, numéro de Carte Scotia, mot de passe, etc.) par courriel. La Banque Scotia n'envoie jamais de courriel à ses clients leur demandant de lui communiquer des renseignements personnels ou confidentiels.
- Évitez d'utiliser un logiciel qui enregistre les mots de passe.
- Utilisez un navigateur recommandé à chiffrement de 128 bits.
- Installez un logiciel anti-virus efficace et un logiciel coupe-feu et mettez-les à jour régulièrement.
- Ne téléchargez aucun logiciel et n'acceptez aucun fichier ou pièce jointe lorsque vous accédez à un site Web, un groupe de discussion ou un groupe de nouvelles à moins d'être absolument certain de son authenticité.
- Désactivez la fonction de partage de fichiers sur votre ordinateur.

### Conseils de sécurité concernant l'utilisation de Scotia en direct

- Protégez votre mot de passe Scotia en direct et votre mot de passe Vérifié par Visa. Mémorisez-les et ne les révélez à personne.
- Tapez toujours l'adresse du site Web ou utilisez un signet pour accéder à Scotia en direct ([www.scotiaendirect.banquescotia.com](http://www.scotiaendirect.banquescotia.com)). Cette adresse sera toujours présente dans la première partie de la ligne d'adresse de toute page Web de Scotia en direct.
- Ne laissez jamais votre ordinateur sans surveillance durant une session Scotia en direct.
- Fermez toujours votre session Scotia en direct en utilisant le lien en haut à droite de l'écran.
- Videz le cache de votre navigateur après chaque session Scotia en direct. (Les instructions sont indiquées à l'écran de sortie de Scotia en direct.)

### Garantie de sécurité en ligne

À la Banque Scotia, nous nous engageons à assurer la sécurité de vos renseignements financiers et à vous permettre d'accéder à vos comptes en toute sécurité. Notre Garantie de sécurité en ligne vous donne l'assurance que nous vous rembourserons intégralement advenant l'éventualité peu probable d'une perte financière directement liée à une opération non autorisée dans vos comptes, par le biais des Services financiers Scotia en direct, à condition que vous ayez préalablement assumé votre responsabilité en matière de sécurité en ligne.

Pour de plus amples détails à ce sujet, veuillez consulter notre site à l'adresse [www.banquescotia.com/garantie](http://www.banquescotia.com/garantie)

