# Sécurité en ligne de Portefeuille futé BMO

## Comment nous vous protégeons

### Garantie de sécurité en ligne

Nous offrons une garantie de remboursement complet en cas de transaction non autorisée dans votre compte Portefeuille futé BMO entraînant une perte directe.*

Pour avoir droit au remboursement prévu par la présente garantie, vous devez prendre les mesures suivantes :

- fermer la session et le navigateur Internet à la fin de chaque session;
- préserver la confidentialité de votre mot de passe;
- vérifier les opérations de votre compte en ligne et vos relevés; et
- nous appeler dans les cinq jours si :
  - vous croyez que votre mot de passe ou numéro de compte Portefeuille futé BMO a été obtenu par quelqu'un d'autre sans votre autorisation;
  - des opérations suspectes que vous n'avez pas autorisées ont eu lieu dans votre compte; ou
  - vous croyez que votre système informatique a été fragilisé par un virus ou un logiciel espion.

### Protection de vos renseignements

Nous ne communiquerons jamais avec vous pour vous demander votre code d'utilisateur, votre mot de passe, votre numéro d'assurance sociale ou d'autres renseignements personnels.

- Si vous doutez qu'un appel provienne d'un représentant de Portefeuille futé BMO, appelez-nous au 1-844-895-3721.
- Protégez-vous des problèmes de sécurité sur Internet en faisant preuve de prudence lorsque vous donnez vos renseignements personnels sur des sites Web.

### Paramètres du délai d'inactivité

Le délai d'inactivité avant l'expiration de votre session est une mesure de sécurité visant à prévenir tout accès non autorisé à votre compte lorsque vous ne vous servez pas de votre ordinateur ou de votre appareil mobile. Si votre compte reste inactif pendant une certaine période, le système fermera automatiquement votre session.

### Vérifications périodiques de la sécurité

Pour vous aider à protéger vos renseignements, BMO Nesbitt Burns évalue régulièrement la sécurité de ses systèmes informatiques pour s'assurer qu'ils n'ont pas été compromis. À BMO Nesbitt Burns, la sécurité de l'information est capitale et nos employés connaissent bien leurs responsabilités lorsqu'il est question d'assurer la sécurité et la confidentialité des renseignements. Que vous choisissiez de faire affaire avec nous en ligne ou par téléphone, nous suivons des pratiques rigoureuses en matière de sécurité et utilisons des technologies de pointe pour protéger vos renseignements et vos transactions contre un accès non autorisé, la divulgation, l'altération et une mauvaise utilisation.

Même si nous faisons de notre mieux pour garantir la confidentialité et la sécurité de vos renseignements, vous pouvez également prendre des mesures pour rehausser votre niveau de sécurité lorsque vous utilisez Internet et Portefeuille futé BMO.

## Ce que vous pouvez faire pour vous protéger

### Gestion du mot de passe

- de modifier votre mot de passe périodiquement;
- de choisir des mots de passe qui ne sont pas trop simples;
- d'utiliser un mot de passe différent de celui de vos autres comptes en ligne (courriels, médias sociaux, etc.);
- de veiller à ce que personne ne puisse voir ce que vous faites lorsque vous entrez vos numéros de compte et les mots de passe connexes; et
- de ne jamais divulguer votre nom d'utilisateur et les renseignements sur votre compte à quiconque.

### Vérification en deux étapes

Le processus de vérification en deux étapes est une fonctionnalité de sécurité qui aide à protéger votre compte en vous demandant de confirmer votre identité à l'aide d'un code de vérification que nous envoyons à votre téléphone. Des taux normaux peuvent s'appliquer de la part de votre fournisseur de service de télécommunication ou de transmission de données pour les messages de la vérification en deux étapes que vous recevez ou envoyez. Pour des raisons de sécurité, nous pouvons temporairement bloquer l'accès à votre compte ou à votre code de l'utilisateur jusqu'à ce que nous puissions confirmer votre identité.

### Protégez vos ordinateurs et vos appareils mobiles

En plus d'utiliser un pare-feu et un programme antivirus, protégez la confidentialité de votre ordinateur en effectuant les mises à jour de sécurité, en vidant la mémoire cache de votre navigateur et en protégeant votre appareil à l'aide d'un mot de passe. N'oubliez pas qu'il arrive souvent que les antivirus ne détectent pas les logiciels espions dans un appareil. Vous pourriez avoir besoin d'un programme spécial pour supprimer les logiciels espions.

### Mémoire cache

Pour protéger vos renseignements personnels, nous vous recommandons vivement de vider la mémoire cache de votre navigateur ou de fermer ce dernier (ce qui remet à zéro la mémoire cache du navigateur) après chaque session.

La mémoire cache est conçue pour améliorer le rendement de votre système et réduire l'engorgement des réseaux. Lorsque vous affichez une page Web, celle-ci est emmagasinée à la fois dans la mémoire cache de votre navigateur et celle du disque de votre appareil.

### Naviguez de façon sécuritaire

Prenez des mesures pour vous protéger contre l'hameçonnage, un type de fraude en ligne qui vous demande de fournir des renseignements personnels. Pensez-y à deux fois avant de cliquer sur des liens fournis dans des courriels qui vous demandent d'accéder à votre compte. Un site Web peut également être suspect si l'adresse du site est mal orthographiée ou légèrement modifiée. Vérifiez l'adresse URL à partir de votre navigateur pour vous assurer que le site Web est authentique.

### Vérifiez la sécurité du site

Les organisations légitimes qui vous permettent d'effectuer des transactions en ligne prennent habituellement des mesures pour vous protéger. Vérifiez le certificat de sécurité de chaque site pour vous assurer qu'il est valable. Vous pouvez confirmer ce renseignement en double-cliquant sur l'icône de cadenas fermé. En vous renseignant sur les façons d'assurer votre sécurité en ligne, vous faites plus que protéger la confidentialité de vos données : vous obtenez également les connaissances dont vous avez besoin pour profiter des avantages offerts par les placements en ligne. Si vous nous informez qu'une transaction non autorisée a eu lieu, nous travaillerons en étroite collaboration avec vous pour effectuer une enquête approfondie dans les plus brefs délais. Nous aurons besoin de votre aide pour prendre toutes les mesures nécessaires pour vous protéger contre des pertes supplémentaires. Nous devrons notamment obtenir votre permission pour faire appel à un tiers, qui procédera à l'enquête et vérifiera les virus qui se trouvent sur votre ordinateur.

## Comment utiliser les témoins et le suivi de l'information?

Les témoins sont une technologie couramment utilisée et de nombreux navigateurs les acceptent automatiquement. Ils sont conçus pour donner au propriétaire d'un site Web des renseignements sur la façon dont son site est utilisé, comme les pages, les liens, les boutons, ainsi que les endroits que l'utilisateur utilise.

Portefeuille futé BMO utilise des témoins à divers endroits. Nous utilisons parfois des pixels invisibles (ou GIFS invisibles) et des témoins dans des courriels de promotion et des publicités en ligne. Ces outils nous permettent d'évaluer l'efficacité de nos campagnes publicitaires. Nous faisons également des analyses pour améliorer continuellement notre site.

Vous pouvez configurer votre navigateur pour qu'il vous avise lorsqu'un témoin est établi, de façon à ce que vous puissiez décider si vous voulez ou non l'accepter. Pour savoir comment établir vos préférences au sujet des témoins ou supprimer ceux-ci, consultez l'aide en ligne de votre navigateur.

## Comment éviter l'hameçonnage?

### Comment vous protéger contre l'hameçonnage?

Vous ne devez jamais envoyer de numéro de compte ou de renseignement personnel par courrier électronique non sécurisé, car ce mode de communication n'est pas sûr.

Aucune entreprise digne de confiance ne vous demandera de fournir des renseignements personnels par courrier électronique; elle ne vous fera pas non plus parvenir de courriel non sollicité vous indiquant d'ouvrir une pièce jointe.

### Qu'est-ce que l'hameçonnage par courriel?

L'hameçonnage est un moyen utilisé pour tenter d'obtenir vos renseignements confidentiels par des courriels semblant provenir d'une source digne de confiance.

### Un courriel d'hameçonnage peut :

- être conçu pour ressembler à une communication provenant d'une entreprise digne de confiance;
- être rédigé en mauvais français ou de façon incompréhensible;
- être envoyé de façon non sollicitée et contenir des pièces jointes;
- provenir d'une adresse Web contenant le symbole @ ou une

série de chiffres (p. ex., 123.456.1.2.) qui vous oriente vers un site qui n'est pas lié à bmo.com;

- comporter dans le champ réponse une adresse sans aucun lien avec celle du champ de l'expéditeur.

### Comment fonctionne la fraude par hameçonnage?

1. Vous recevez un courriel non sollicité contenant l'une des lignes d'objet qui suivent :

- Vos renseignements personnels doivent être mis à jour
- Vous avez gagné à un concours!
- MESURE À PRENDRE : Votre carte ou votre compte a été suspendu
- Bonne nouvelle : Votre demande de tel produit a été approuvée. Votre compte a été fermé.

2. On vous invite ensuite à ouvrir une pièce jointe ou à envoyer une réponse à une adresse de courriel.

3. Si vous suivez ces instructions, vous vous retrouvez sur un site malveillant où l'on vous demande des renseignements confidentiels (numéros de carte bancaire, codes d'utilisateur, numéros de compte, NIP, numéros de carte de crédit, NAS, mots de passe).

Visualisez notre présentation « Ne mordez pas à l'hameçon » pour vous protéger contre ce genre de fraude.

http://www.bmo.com/media/dont-take-the-bait/fr/index.htm

## Navigateurs pris en charge

Pour vous aider à protéger vos renseignements personnels et financiers, le site de Portefeuille futé BMO est compatible avec les navigateurs suivants :

### Windows

- Internet Explorer 11.0+
- Firefox 41+
- Chrome 46+

### Mac OS X

- Safari 8+

### iOS

- Safari 8+

## Lecteurs d'écran pris en charge

Portefeuille futé BMO prend en charge les lecteurs d'écran suivants :

### Ordinateur de bureau

- NVDA
- JAWS

### Appareils mobiles

- Voiceover pour iOS

## Ce que nous faisons

Voici certaines des mesures de sécurité mises en place pour vous protéger lorsque vous utilisez Portefeuille futé BMO :

- une technologie de chiffrement fort qui fait en sorte de protéger les données qui circulent entre votre appareil et notre serveur Web; votre navigateur doit donc permettre ce niveau de chiffrement sécurisé (en jargon technique, le chiffrement à 128 bits);
- des certificats numériques que délivrent des entreprises tierces de confiance pour confirmer que notre site Web est sécurisé et authentique;
- la fermeture de session automatique après une période d'inactivité;
- des pare-feu qui protègent vos renseignements dans Portefeuille futé BMO;
- .• La vérification en deux étapes pour vérifier votre identité lorsque vous ouvrez une session.

## Ce que nous ne faisons pas

Nous ne vous demandons jamais par courriel de nous communiquer des renseignements sur vous ou sur vos comptes (c.-à-d. hameçonnage). Si vous recevez un courriel qui semble provenir de Portefeuille futé BMO et qui vous demande des renseignements personnels, communiquez immédiatement avec nous.

## Ce que vous pouvez faire

- Assurez-vous que les plus récents pare-feu et anti-logiciels espions sont installés sur vos appareils.
- Ne communiquez votre code d'utilisateur et votre mot de passe à personne.
- Gardez à l'esprit que les courriels ne sont pas chiffrés et qu'ils peuvent donc être interceptés et lus par des tiers. Veuillez ne pas nous envoyer de renseignements confidentiels par courriel.
- N'utilisez pas d'ordinateur public pour vous connecter à votre compte Portefeuille futé BMO. Utilisez toujours votre propre connexion sécurisée.

• Inscrivez-vous à la vérification en deux étapes aussitôt qu'on vous y invitera.

Pour de plus amples renseignements sur la sécurité chez BMO Groupe financier visitez le http://www.bmo.com/accueil/a-propos-de-bmo/services-bancaires/confidentialite-securite/comment-nous-vous-protegeons

* Certaines conditions s'appliquent.

# Modalités de la garantie de sécurité

## 1. Garantie de sécurité

Conformément aux sections 2 et 3 ci-dessous, BMO Nesbitt Burns vous indemnisera pour les pertes pécuniaires directement liées à des transactions non autorisées effectuées dans votre compte Portefeuille futé BMO. Cela exclut les pertes pécuniaires directement liées à des transactions non autorisées effectuées dans votre compte bancaire BMO Banque de Montréal. Nous nous réservons le droit de modifier les modalités de cette garantie de sécurité, ou de la révoquer en tout temps, sans préavis. Aux fins de cette garantie de sécurité, une « transaction non autorisée » désigne une transaction effectuée, sans votre permission, votre autorisation ou à votre insu, dans votre compte Portefeuille futé BMO par l'intermédiaire du portail en ligne et où il peut être démontré que vous avez été victime de fraude, de vol ou que vous avez dû la faire à la suite d'une supercherie, de l'utilisation de la force ou d'une intimidation. Il est entendu que les « transactions non autorisées » excluent toute transaction effectuée dans votre compte par une personne ayant été autorisée à effectuer des transactions dans votre compte, ou autrement à agir en votre nom.

## 2. Vos responsabilités

BMO Nesbitt Burns ne vous indemnisera pas et refusera toute demande de compensation en lien avec cette garantie de sécurité si vous ne prenez pas les mesures ci-dessous :

a) nous informer immédiatement lorsque vous découvrez qu'une transaction non autorisée a été effectuée, ou alors dans les cinq jours ouvrables après la réception du relevé de compte mensuel suivant la date de la transaction non autorisée;

b) nous informer immédiatement si vous savez ou soupçonnez que votre numéro de compte Portefeuille futé BMO ou votre code d'utilisateur a été obtenu par quelqu'un d'autre ou si des opérations suspectes ont eu lieu dans votre compte;

c) apporter votre entière coopération lors de l'enquête sur une transaction non autorisée présumée, et répondre à toutes les demandes raisonnables en fournissant les renseignements nécessaires et en prenant les mesures indiquées;

d) autoriser BMO Nesbitt Burns à faire appel à un tiers qui procédera à l'enquête et vérifiera les virus qui se trouvent sur votre ordinateur ou votre appareil mobile;

e) vous conformer aux modalités de la convention de gestion de placements Portefeuille futé BMO, ainsi qu'à celles des ententes qui régissent vos comptes bancaires de particuliers ou d'entreprises ou vos comptes de courtage, ou d'autres produits ou services financiers que nous offrons.

## 3. Limitations

BMO Nesbitt Burns ne vous indemnisera pas et refusera toute demande de compensation en lien avec cette garantie de sécurité si nous avons des motifs de croire que :

a) vous ne possédiez pas la version la plus récente des pare-feu et logiciels antivirus;

b) vous avez commis, seul ou de concert avec d'autres personnes, un acte criminel, malhonnête ou frauduleux en lien avec la transaction non autorisée;

c) vous avez communiqué votre code d'utilisateur, votre numéro de compte ou votre mot de passe de Portefeuille futé BMO à une autre personne, y compris, sans s'y limiter, à un fournisseur de services de regroupement d'information sur les comptes en ligne, ou encore vous avez négligé de protéger la confidentialité de votre code d'utilisateur, de votre numéro de compte ou de votre mot de passe de Portefeuille futé BMO;

d) vous avez accédé au portail en ligne en utilisant un ordinateur ou un appareil pour lequel il y avait des raisons de croire qu'il contenait un logiciel en mesure de communiquer des renseignements à un tiers ou de compromettre votre code d'utilisateur, votre numéro de compte ou votre mot de passe de Portefeuille futé BMO; ou

e) vous avez omis de prendre des précautions raisonnables pour empêcher une transaction non autorisée (par exemple, vous avez omis de fermer la session et le navigateur Internet à la fin de votre session Portefeuille futé BMO).

Limite de responsabilité : BMO Nesbitt Burns ne vous indemnisera ou ne vous fournira de compensation en aucunes circonstances autres que celles précisées dans la Section 1 ci-dessus ou ne sera tenu responsable de tous dommages indirects, consécutifs, spéciaux, majorés, punitifs ou exemplaires, en tout ou en partie (y compris, sans se limiter à toute interruption des opérations, perte de profits, occasion manquée, perte de marché, ou toute autre perte commerciale ou financière) découlant d'une transaction non autorisée dans votre compte, même si nous avons été avisés que des dommages pouvaient survenir.