Se protéger contre la cybercriminalité

ce que vous devez savoir

BMO

Introduction

Dans une ère de plus en plus axée sur le numérique, la protection des renseignements de nos clients constitue l'une des priorités absolues de BMO. Notre modèle de sécurité est composé de contrôles, de données, de technologies et de talents – pour que vous puissiez faire affaire avec BMO en toute sécurité et en toute con iance.

Notre cadre comprend les investissements que nous avons faits pour que vous puissiez disposer des outils nécessaires pour assurer la confidentialité et la sécurité de vos renseignements à la maison et lorsque vous voyagez. Dans cette brochure, vous trouverez des conseils sur les services bancaires courants et l'utilisation de vos appareils pour vous aider à éviter d'être victime de vol d'identité ou de fraude.

Table des matières

> Nous avons regroupé au sein d'une même équipe des experts de la cybersécurité, de la gestion du risque de fraude, de la sécurité physique et de la gestion de crise pour renforcer notre capacité à détecter les menaces et à améliorer continuellement nos stratégies d'intervention. La cybersécurité est un aspect très important de nos activités – ce travail aide à assurer la sécurité de vos données.
>
> Darryl White
> Chef de la direction, BMO Groupe financier

Comment BMO vous protège

Établissement d'un nouveau point de référence en matière de sécurité

Aujourd'hui, grâce aux puissantes capacités numériques de BMO, nous pouvons offrir l'expérience rapide et commode de services bancaires en ligne à laquelle vous et nos autres clients vous attendez de notre part.

En janvier 2019, BMO a mis sur pied l'Unité Crime financier (UCF) pour regrouper ses équipes de cybersécurité, de gestion du risque de fraude, de sécurité physique et de gestion de crise en une seule organisation interne. Ensemble, nos équipes forment un groupe de travail sur la sécurité entièrement intégré qui solidifie nos capacités en la matière afin de protéger les renseignements des clients et de la Banque.

Nous avons investi dans notre infrastructure technologique en y intégrant des analyses et des capacités avancées, dont l'intelligence artificielle et l'apprentissage machine. Ainsi, nous pouvons détecter et prévenir les menaces à la sécurité de la Banque et de nos clients, y réagir et redresser la situation. L'objectif: favoriser un environnement sûr où vous pouvez épargner des fonds, y accéder et les virer en toute confiance.

Caractéristiques de sécurité de BMO :

- Carrefour de gestion de la sécurité ultramoderne, notre Centre de fusion des données de BMO gère les menaces à la sécurité en tout temps
- Notre modèle opérationnel ajusté aux fuseaux horaires permet à nos équipes du Centre de fusion des données de collaborer avec des équipes de sécurité mondiales en Amérique du Nord, en Europe et en Asie

BMO utilise des contrôles internes sécurisés de pointe pour protéger vos renseignements. Il s'agit notamment de pare-feu et de programmes de renforcement de courriel, ainsi que de logiciels de protection parmi les meilleurs du secteur. Nous avons mis en place des programmes intensifs de sensibilisation et de formation pour que nos employés adoptent les meilleures pratiques en matière de sécurité.

Programmes de sécurité de BMO pour nos clients

En faisant équipe avec des partenaires technologiques de confiance, nous pouvons recommander des logiciels, des services et des applications qui aident à vous protéger en ligne. Pour en apprendre davantage sur les programmes suivants et les télécharger dès aujourd'hui, rendez-vous à l'adresse https://www.bmo.com/securite.

Le **logiciel Trusteer RapportMD* d'IBMMD*** vous protège contre la fraude et le vol d'identité en signalant les sites d'hameçonnage. Offert en téléchargement gratuit et facile à configurer, il vous donnera la certitude d'accéder au site officiel de bmo.com, et non à un faux site.

OnGuard*MC* est un service qui permet de protéger vos renseignements personnels et votre identité en ligne. Il scrute les sites Web publics et clandestins et vous envoie un avis lorsqu'il trouve vos renseignements personnels.

Vérifiez.Moi[MC] est une application qui vous aide à confirmer votre identité rapidement et en toute sécurité au moyen de votre téléphone intelligent.

BMO enverra des codes de vérification en ligne pour confirmer votre identité si nous constatons des activités inhabituelles dans votre compte.

Inscrivez-vous au service Alertes BMO pour recevoir un avis par courriel ou messagerie texte si nous détectons des activités douteuses dans vos comptes.

La **Messagerie** est un moyen simple et gratuit de chiffrer vos courriels et vos renseignements confidentiels lorsque vous travaillez avec un représentant de BMO. Visitez simplement le site bmo.com/securite pour accéder à notre guide de configuration de la Messagerie.

Notre engagement envers vous

BMO offre une Garantie totale des services bancaires électroniques aux clients des Services bancaires aux particuliers. Conformément à celle-ci, nous vous rembourserons la totalité des pertes découlant de transactions non autorisées effectuées dans vos comptes bancaires personnels au moyen des Services bancaires en ligne et des Services mobiles BMO.

Pour obtenir un remboursement dans le cadre de cette garantie, vous devez suivre quelques étapes, qui sont expliquées dans notre Convention relative aux services bancaires électroniques. Nous vous recommandons également de protéger votre ordinateur.
Pour en savoir plus, allez à bmo.com/securite.

CONSEILS!

Nous vous recommandons de lire notre Convention relative aux services bancaires électroniques, que vous pouvez obtenir à n'importe quelle succursale de BMO, ou en ligne à bmo.com/conventions.

Pour assurer votre protection dans le cadre de notre garantie, suivez les étapes décrites dans la Convention, notamment :

- Préservez la confidentialité de votre mot de passe en tout temps
- Conservez votre mot de passe en lieu sûr, séparé de vos numéros de carte de débit et de crédit
- Si vous souhaitez utiliser la technologie Touch ID ou la reconnaissance faciale à partir de votre appareil mobile pour ouvrir une session dans les Services mobiles BMO, vous devez être la seule personne dont les empreintes digitales ou l'image faciale sont enregistrées dans votre appareil afin que personne d'autre ne puisse accéder à vos renseignements bancaires personnels
- Veuillez nous aviser dans les 24 heures dès que vous constatez la perte ou le vol de votre carte de débit ou de crédit ou du téléphone intelligent que vous utilisez pour accéder aux Services bancaires mobiles, ou dès que la confidentialité de votre mot de passe est compromise

Protection de votre identité

De nos jours, votre identité constitue l'un de vos actifs les plus précieux. Si des fraudeurs mettent la main sur vos renseignements personnels, ils peuvent accéder à vos comptes, obtenir des cartes de crédit ou faire des achats en votre nom, et bien plus encore. Nous devons travailler ensemble pour protéger ces renseignements.

Quels renseignements devez-vous protéger?

Vous devez protéger tout renseignement qui peut être utilisé pour vous identifier. En voici quelques exemples: votre numéro d'assurance sociale (NAS), vos numéros d'identification personnels (NIP) qui vous permettent d'utiliser vos cartes bancaires ou vos cartes de crédit, ainsi que les questions et réponses de vérification.

Les seules organisations auxquelles vous devriez transmettre votre NAS sont votre employeur, le gouvernement fédéral et votre institution financière.

CONSEIL!

Ces organisations ne vous demanderont jamais de divulguer vos renseignements personnels, vos NIP ou vos mots de passe par courriel, par téléphone ou dans des fenêtres contextuelles sur des sites Web.

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

Les NIP et les mots de passe visent à protéger votre argent et vos comptes. Ils permettent de confirmer que vous êtes l'utilisateur autorisé de vos comptes (carte de débit, carte de crédit, services bancaires en ligne, services bancaires par téléphone, etc.) et vous donnent accès à votre argent. Il est essentiel que vous établissiez des NIP et des mots de passe forts, et que vous ne les divulguiez à personne.

Établissement d'un NIP et d'un mot de passe forts

- Utilisez un mot de passe ou un NIP différent pour chaque compte
- Créez des mots de passe contenant au moins huit caractères, dont des caractères spéciaux et des chiffres
- Modifiez fréquemment vos NIP et vos mots de passe
- N'utilisez pas de simples mots du dictionnaire, des noms de saison, des dates tirées du calendrier ou des expressions courantes
- N'utilisez pas de dates qui ont une signification pour vous et qui sont faciles à deviner (p. ex. date de naissance ou d'un anniversaire)

Protection de vos NIP et mots de passe

La protection de vos mots de passe et de vos NIP est l'une des meilleures façons de vous protéger contre la fraude et le vol d'identité. Voici quelques conseils à ce sujet:

- Ne divulguez vos mots de passe à personne
- Évitez de conserver vos mots de passe dans des endroits facilement accessibles, comme votre bureau, votre voiture, votre portefeuille ou sous votre clavier
- Lorsque vous entrez votre NIP à un guichet automatique ou dans un magasin, cachez le pavé numérique à l'aide de votre main
- De même, lorsque vous entrez votre mot de passe à l'ordinateur ou sur votre téléphone intelligent, assurez-vous que personne ne vous regarde

Protection de vos comptes

Documents papier

Bon nombre d'entre nous utilisent encore des documents papier (chèques, relevés de compte en format papier, etc.) pour effectuer des transactions ou en faire le suivi. Voici quelques conseils pour vous aider à protéger votre identité et à éviter que des transactions frauduleuses soient effectuées dans votre compte :

- Conservez vos chèques et tout autre document contenant des données bancaires en lieu sûr
- Rédigez vos chèques à l'encre indélébile et de manière lisible, et évitez d'y laisser des espaces où les fraudeurs pourraient ajouter des chiffres ou des mots
- Déchiquetez tout document dont vous n'avez pas besoin, y compris les chèques sur lesquels vous avez fait une erreur
- Ne laissez jamais la ligne « Payez à l'ordre de » en blanc, et évitez d'émettre des chèques « au porteur »
- Soyez toujours à l'affût de toute irrégularité dans vos comptes et vos transactions (en ligne, dans vos livrets bancaires ou vos relevés de compte). Si vous repérez une activité suspecte, signalez-la immédiatement à BMO
- Soyez prudent lorsque vous acceptez d'échanger de l'argent contre un chèque d'une personne que vous ne connaissez pas bien. Le chèque pourrait ne pas être compensé, et vous serez tenu responsable des fonds perdus

CONSEIL!

N'oubliez pas de vérifier régulièrement vos relevés bancaires à la recherche de transactions suspectes, que ce soit au moyen des Services bancaires en ligne ou de l'application mobile. Si vous remarquez quelque chose d'inhabituel, téléphonez-nous au 1-844-837-9228 ou rendez-vous dans une succursale de BMO pour nous le signaler.

Protection et sécurité des cartes

Les cartes de débit et de crédit nous permettent d'accéder à notre argent et de l'utiliser au moment et de la manière qui nous conviennent, ce qui nous procure une grande souplesse. Il est important que vous protégiez vos cartes et les renseignements qui y sont liés pour éviter de devenir victime de fraude.

Voici quelques conseils pour protéger vos cartes :

- Conservez toujours vos cartes en lieu sûr; ne les laissez jamais à la vue de tous et ne les prêtez pas
- Annulez et détruisez toute carte que vous n'utilisez plus (p. ex. une carte expirée ou annulée)
- Signez et activez vos nouvelles cartes dès que vous les recevez
- Lorsque vous faites un achat, vérifiez toujours que la carte qu'on vous remet est bien la vôtre
- Déchiquetez ou détruisez tout document papier (reçus, relevés, etc.) contenant des renseignements relatifs à vos cartes
- Insistez pour glisser vous-même votre carte dans le lecteur lorsque vous faites un achat. Si ce n'est pas possible et que le caissier doit le faire pour vous, ayez toujours l'œil sur votre carte
- Lorsque vous faites des achats, vérifiez que le montant est exact avant d'entrer le NIP de votre carte ou de taper votre carte sur le terminal. Vérifiez également le reçu dès que la transaction est terminée
- Cachez votre NIP lorsque vous faites une transaction à un guichet automatique ou que vous payez vos achats dans un magasin
- Évitez de donner votre numéro de carte de crédit par téléphone, sauf si c'est vous qui faites l'appel. Ne donnez pas votre numéro de carte de crédit par téléphone dans un endroit public

Ce que BMO fait pour vous protéger :

- Pour prévenir l'écrémage des cartes de débit et l'espionnage par-dessus l'épaule, nous avons équipé nos guichets automatiques de volets protecteurs pour le clavier, d'écrans encastrés munis de panneaux de protection, ainsi que de dispositifs anti-écrémage
- Si nous soupçonnons que votre carte de débit ou de crédit est à risque, nous bloquerons immédiatement l'accès à vos fonds et nous vous en informerons par l'intermédiaire de notre programme d'appels automatisé ou de notre Centre contact clientèle. BMO vous aidera ensuite à configurer l'accès à vos cartes de débit ou de crédit dès que possible

Transactions électroniques

En cette ère numérique, nous pouvons effectuer nos opérations bancaires au moyen d'un appareil mobile, en ligne ou par téléphone. Bien que ces solutions soient rapides, simples et très pratiques, elles peuvent également faciliter la vie aux fraudeurs. Voici des conseils pour vous aider à effectuer des opérations bancaires en ligne de manière sécuritaire et en toute confiance.

- Gardez vos logiciels d'exploitation à jour. Les fraudeurs ciblent souvent les anciennes versions des logiciels pour lancer des programmes malveillants. Assurez-vous d'utiliser des logiciels de sécurité qui comprennent un pare-feu, un antivirus, un antipourriel et un anti-logiciel espion
- Lorsque vous effectuez des opérations bancaires en ligne, assurez-vous d'accéder au vrai site Web de BMO en vérifiant que la barre d'adresse affiche une icône de cadenas verrouillé. De plus, l'adresse du site Web doit commencer par « https »
- Évitez d'utiliser des ordinateurs publics, comme ceux que l'on trouve dans les bibliothèques et les cafés Internet. Ils peuvent contenir des logiciels malveillants capables d'enregistrer vos renseignements
- Supprimez fréquemment vos témoins (« cookies »), car les fraudeurs peuvent s'en servir pour accéder à vos renseignements confidentiels
- Vérifiez que votre connexion sans fil à la maison est chiffrée et protégée par un mot de passe. Ainsi, personne ne pourra l'utiliser sans votre permission
- Protégez vos appareils mobiles et vos tablettes. Assurez-vous que personne ne peut lire les renseignements affichés à l'écran de vos appareils. N'utilisez pas les réseaux Wi-Fi publics pour effectuer des transactions bancaires ni ne conservez vos mots de passe sur votre appareil
- Veillez à protéger vos appareils mobiles au moyen d'un mot de passe et à les verrouiller lorsque vous ne les utilisez pas. De cette manière, vos renseignements seront protégés si votre appareil est perdu ou volé

Ce que BMO fait pour vous protéger :

- Si vous oubliez de fermer une session en ligne sécurisée, nous y mettrons fin automatiquement après dix minutes d'inactivité afin d'éviter que quelqu'un d'autre accède à vos renseignements financiers
- BMO utilise un processus de vérification qui détecte l'appareil utilisé et pose des questions de sécurité. Cette caractéristique de sécurité permet à BMO de poser d'autres questions de vérification lorsqu'un outil inconnu, comme un nouvel appareil mobile ou un nouveau navigateur, tente d'accéder à votre compte

Services bancaires par téléphone sécurisés

BMO propose maintenant le système Empreinte vocale, une méthode sûre qui permet de confirmer votre identité à l'aide de votre voix lorsque vous utilisez les Services bancaires par téléphone. Le système Empreinte vocale, qui est notre principale méthode d'authentification des clients, accélère et simplifie les opérations bancaires par téléphone et les rend plus sûres.

Lorsque vous utilisez les Services bancaires par téléphone, rappelez-vous les conseils suivants :

- Faites attention à ce que vous dites à l'agent
- Assurez-vous que personne ne peut entendre vos renseignements personnels

Escroqueries courantes

Vous trouverez ci-dessous des exemples d'escroqueries couramment utilisées pour accéder à des renseignements personnels et financiers, ainsi que des mesures que vous pouvez prendre pour vous.

CONSEIL!

Visitez régulièrement le site bmo.com/securite pour vous tenir informé des nouvelles escroqueries commises par les fraudeurs.

Hameçonnage : C'est l'un des moyens les plus efficaces et les plus utilisés par les cybercriminels pour s'attaquer aux gens ordinaires, que ce soit par courriel, par message texte ou par téléphone. Se faisant passer pour une source légitime, les cybercriminels essaient d'obtenir vos renseignements personnels ou vous incitent à cliquer sur un lien ou à télécharger une pièce jointe qui peut installer un logiciel malveillant sur votre appareil. Voici quelques conseils pour vous aider à éviter l'hameçonnage :

- Vérifiez les liens dans les courriels en plaçant le curseur sur le lien
- Lisez attentivement les courriels. Les salutations impersonnelles ou génériques et les fautes d'orthographe ou de grammaire sont autant de signaux avertisseurs d'une escroquerie potentielle
- Ne répondez pas aux courriels, aux messages texte ou aux appels qui proviennent d'entreprises ou de personnes que vous ne connaissez pas
- Si vous recevez un courriel, un message texte ou un appel vous demandant d'urgence de répondre ou de cliquer sur un lien, de vérifier votre compte ou de modifier votre mot de passe, faites une vérification auprès de l'entreprise avant d'agir. Ne vous sentez pas forcé de répondre à une demande urgente
- Ne cliquez pas sur des pièces jointes provenant de sources inconnues
- N'entrez pas de renseignements personnels ou financiers dans une formule intégrée à un courriel ou accessible par un lien dans le courriel. Si le courriel semble légitime, appelez l'entreprise ou consultez son site Web, puis ouvrez une session sécurisée avant d'entrer les renseignements demandés

Arnaques amoureuses : Les sites de rencontre en ligne sont populaires auprès des fraudeurs qui cherchent à tromper leurs victimes en les amenant à leur envoyer de l'argent. Méfiez-vous des personnes qui veulent agir rapidement, qui refusent de vous rencontrer en personne, ou qui vous demandent de l'argent pour quelque raison que ce soit. Évitez d'être victime de fraude : ne communiquez pas vos renseignements personnels (y compris des photos), et refusez d'envoyer ou de recevoir de l'argent.

Fraudes liées aux mules : Une mule est une personne qui transfère de l'argent volé d'un compte bancaire à un autre. Des criminels la recrutent, souvent à son insu, pour transférer de l'argent qu'ils ont tiré de leurs activités criminelles. Les autorités ont ainsi plus de difficulté à retracer ces criminels. Ceux-ci pourraient vous proposer des offres alléchantes sur les médias sociaux, dans un courriel, par la poste ou par téléphone. Méfiez-vous des offres d'emploi qui semblent trop belles pour être vraies, ou des personnes qui vous demanderaient d'ouvrir un compte bancaire pour elles.

Faux organismes de bienfaisance : Les fraudeurs peuvent se présenter comme des organismes de bienfaisance légitimes pour convaincre les victimes compatissantes de donner généreusement pour leur cause. Demandez à l'organisation en question de vous envoyer une formule de promesse de don, et faites des recherches en ligne à son sujet pour vous assurer de sa crédibilité.

Fraudes sur les médias sociaux : Surveillez les fausses demandes d'amis ou les adresses URL masquées menant à des jeux-questionnaires « gratuits ». Interagissez seulement avec des gens que vous connaissez. Sachez que, lorsque vous fournissez des renseignements pour quoi que ce soit qui est « gratuit » en ligne, vous les communiquez probablement à des tiers.

CONSEIL!

Souvenez-vous que nous ne communiquerons jamais avec vous de façon non sollicitée par téléphone, courriel ou messagerie texte pour vous demander de nous confirmer ou de nous fournir votre mot de passe, ou de nous transmettre des renseignements personnels ou relatifs à votre compte.

Coordonnées

Signalement d'un courriel d'hameçonnage

Si vous pensez qu'un courriel représente une tentative d'hameçonnage, envoyez-le en pièce jointe à l'adresse **hameconnage@bmo.com**, puis supprimez-le.

Signalement d'une activité suspecte dans votre compte

Si vous remarquez une activité suspecte dans l'un de vos comptes de BMO, veuillez nous en faire part au **https://www.bmo.com/principal/contactez-nous**.

Signalement d'une carte perdue ou volée

Pour signaler une carte de crédit perdue, composez le **1-800-361-3361** ou le **514-877-0330** (appel à frais virés depuis l'étranger).

Pour signaler une carte de débit perdue, composez le **1-877-225-5266**.

5118600 (06/20) 06/20 - 1153

BMO