Se protéger à l'ère numérique:
Conseils de sécurité de l'Unité Crime financier de BMO

BMO MD

Unité Crime financier de BMO – Établir un nouveau point de référence en matière de sécurité financière

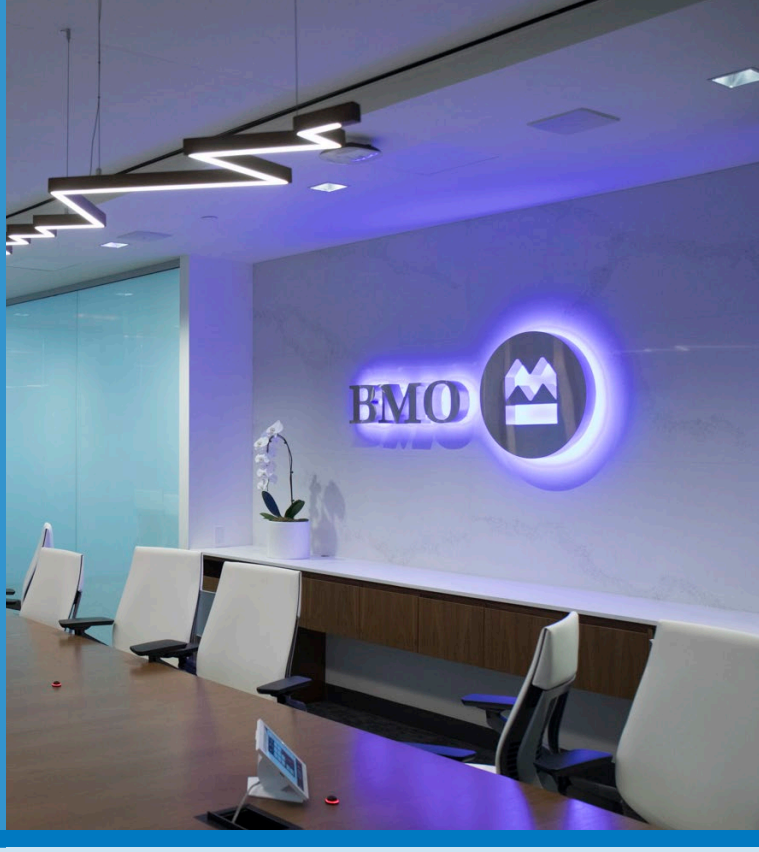
Pour en apprendre davantage, consultez le site bmo.com/securite

Table des matières

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 confiance.

Notre cadre comprend également des outils de partage avec les clients et nos communautés, pour vous aider à protéger votre vie privée et votre sécurité. Dans ce bref guide, vous trouverez des con-seils simples pour vous aider à protéger vos comptes et éviter d'être victime de vol d'identité ou de fraude.



Unité Crime financier de BMO

Établir un nouveau point de référence en matière de sécurité.

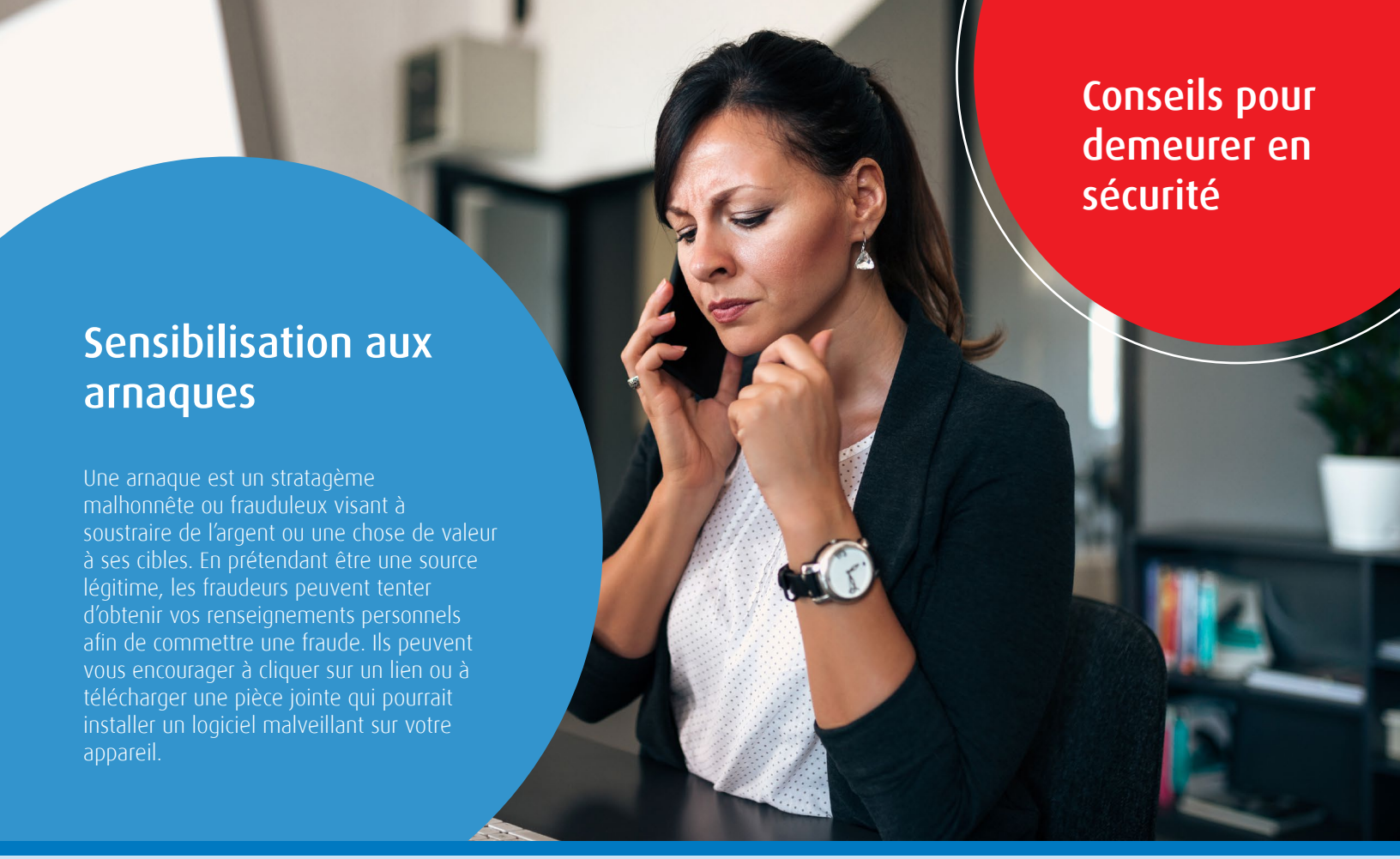
Aujourd'hui, grâce aux puissantes capacités numériques de BMO, nous pouvons offrir l'expérience rapide et commode de services bancaires en ligne à laquelle vous et nos autres clients vous attendez de notre part.

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 for-ment 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.

Autres caractéristiques de sécurité de BMO:

- Carrefour de gestion de la sécurité ultramoderne, le Centre de fusion des données de BMO gère les menaces à la sécurité en tout temps.
- Le modèle opérationnel « ajusté aux fuseaux horaires » permet à nos équipes de travailler avec des équipes de sécurité du monde entier,
- en Amérique du Nord, en Europe et en Asie.
- Des contrôles internes à plusieurs niveaux assurent la sécurité des données des clients.
- Une formation fréquente permet aux employés de se tenir au courant des meilleures pratiques en matière de sécurité.



Conseils pour demeurer en sécurité

Sensibilisation aux arnaques

Une arnaque est un stratagème malhonnête ou frauduleux visant à soustraire de l'argent ou une chose de valeur à ses cibles. En prétendant être une source légitime, les fraudeurs peuvent tenter d'obtenir vos renseignements personnels afin de commettre une fraude. Ils peuvent vous encourager à cliquer sur un lien ou à télécharger une pièce jointe qui pourrait installer un logiciel malveillant sur votre appareil.

Éviter les arnaques et se protéger

✓ Évitez les demandes ou les offres « urgentes » ou « trop belles pour être honnêtes ».

✓ Passez attentivement en revue les courriels et les adresses URL. Les courriels et les sites Web peuvent sembler émaner de sociétés de confiance, mais en examinant attentivement le texte et l'URL, vous remar querez une petite différence, comme une lettre supplémentaire, un point ou un .net au lieu d'un .com.

✓ Refusez les appels et les courriels non sollicités. Si vous ne connaissez pas l'appelant ou l'expéditeur, faites preuve de prudence, voire évitez-le complètement.

✓ Méfiez-vous des personnes qui demandent des cartes-cadeaux, des mandats, des chèques ou des virements télégraphiques. Si une personne demande ce type de paiement, le risque de fraude peut être plus élevé.

Remarque: BMO ne communiquera jamais avec vous par courriel, texto ou appel non sollicité pour vous demander des renseignements sensibles, des mots de passe ou des NIP. Si vous recevez un appel, un message vocal, un courriel ou un texto douteux d'une personne prétendant être de BMO, communiquez immédiatement avec nous en utilisant les renseignements au verso de votre carte.

Magasinage en ligne

Alors que le commerce en ligne poursuit sa progression, les fraudeurs trouvent toujours de nouvelles façons de profiter des acheteurs en ligne. Vous pouvez prendre certaines mesures pour vous protéger, notamment:

✓ Effectuez vos achats en ligne uniquement auprès de commerçants connus et fiables. La présence d'une icône de cadenas verrouillé et de la mention « https » dans l'URL est un signe positif. Si vous êtes sur un site qui ne comporte pas ces deux éléments dans la barre d'adresse, le risque est plus grand que vos données soient communiquées à une entité malveillante.

✓ Interrogez-vous sur les trop bonnes affaires. Si le prix semble trop beau pour être vrai, c'est probablement qu'il l'est. Recherchez aussi ces signaux avertisseurs : le site vous demande de payer à l'avance pour débloquer la transaction ou recevoir un bon de réduction; vous ne pouvez pas payer avec un moyen sécurisé comme votre carte de débit, votre carte de crédit ou vos applications de paiement; la politique de retour ou de remboursement du site est vague ou inexistante.

✓ Évitez les réseaux Wi-Fi publics. Ils sont le meilleur ami des fraudeurs. En effectuant des achats en ligne alors que vous êtes connecté à un réseau public, vous vous exposez à un risque, car vous ne pouvez absolument pas savoir qui l'utilise et qui peut y accéder (et accéder ainsi à vos données!).

✓ Utilisez les applications de paiement mobile. Elles sont jugées plus sûres pour les achats en ligne que le fait de saisir directement les données de votre carte.

✓ Vérifiez régulièrement vos relevés bancaires. Si vous remarquez une transaction que vous n'avez pas effectuée sur votre relevé bancaire, communiquez immédiatement avec votre banque.

Hameçonnage

C'est l'un des moyens les plus efficaces et les plus utilisés par les cybercriminels pour approcher les gens au quotidien, que ce soit par courriel, par message texte ou par téléphone. En 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:

- Lisez attentivement les courriels. Les salutations impersonnelles ou génériques et les fautes d'orthographe ou de grammaire sont autant de signaux avertisseurs d'un potentiel hameçonnage par courriel.
- 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 répondez pas aux courriels, aux messages texte ou aux appels qui proviennent d'entreprises ou de personnes que vous ne connaissez pas.
- 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.

Fraudes sur les médias sociaux

Un vol d'identité peut survenir là où vous ne vous y attendez pas forcément, par exemple parmi vos « amis » ou « abonnés » sur les réseaux sociaux. Bien que ces communautés puissent sembler comme un espace où nous pouvons publier les détails de notre vie en toute sécurité, il se pourrait que vous partagiez plus que vous ne le pensez. Voici quelques conseils pour vous aider à protéger vos renseignements sur les réseaux sociaux:

- Évitez de partager trop de renseignements personnels, comme votre date de naissance, vos projets de vacances, etc. Ces renseignements pourraient fournir des indices sur vos mots de passe ou questions de sécurité. Publier des renseignements sur vos vacances en temps réel peut vous exposer à des cambriolages en votre absence.
- Ne répondez pas aux questionnaires qui demandent des renseignements « amusants ». Ils pourraient être utilisés pour accéder à vos comptes. N'oubliez pas que, lorsque vous fournissez des renseignements pour quelque chose de « gratuit » en ligne, vous les communiquez probablement à des tiers.
- Soyez prudent avec les personnes que vous ne connaissez pas, lorsque vous acceptez de nouveaux amis et de nouveaux abonnés sur les réseaux sociaux. Ne divulguez pas de renseignements personnels à une personne avant d'avoir fait sa connaissance dans la vie réelle.
- Passez en revue vos paramètres de confidentialité sur tous vos appareils et sur chacun de vos comptes de réseaux sociaux pour vous assurer que vous ne partagez vos publications qu'avec le public visé.

Liste de vérification en matière de cybersécurité

Voici quelques mesures de base que vous pouvez prendre pour vous assurer que vos renseignements demeurent protégés:

Correctifs (mises à jour du système) – Améliorez la sécurité de votre appareil et/ou de ses fonctionnalités en installant les mises à jour de votre micrologiciel ou de vos logiciels dès qu'elles sont disponibles. Utilisez un logiciel antivirus réputé pour une protection supplémentaire et créez régulièrement des sauvegardes de vos données, en particulier les renseignements que vous jugez essentiels.

Mots de passe – Créez des mots de passe forts et complexes pour vos comptes. Les mots de passe complexes comptent plus de huit caractères et comprennent des lettres, des chiffres et des sym-boles. Ne communiquez vos mots de passe à personne, modifiez-les régulièrement, utilisez des mots de passe différents pour les différents comptes et changez toujours les mots de passe par défaut fournis par un fabricant.

Autorisations – Limitez l'accès à vos données personnelles en restreignant l'accès à vos applications, navigateurs Web, appareils photo et microphones (en augmentant les paramètres de confidentialité). Il est important que vous désactiviez les droits d'accès aux sites Web de partage de fichiers que vous ne connaissez pas ou n'utilisez pas.

Protégez votre identité – Évitez de communiquer des renseignements personnels. Ne donnez aucun renseignement qui n'est pas nécessaire, surtout s'il s'agit d'un renseignement non accessible au public. Limitez aussi vos publications sur les réseaux so-ciaux. Les fraudeurs peuvent cibler les réseaux sociaux pour découvrir des renseignements personnels et les utiliser contre vous (p. ex. en répondant aux questions de réinitialisation d'un mot de passe).

Parents (tuteurs), enfants et personnes âgées – Protégez vos amis et les membres de votre famille en leur expliquant les conseils ci-dessus et en les informant qu'ils peuvent communiquer avec vous s'ils ont des doutes ou des problèmes en lien avec la cybersécurité. Les personnes âgées sont parmi les plus ciblées par les fraudeurs. Maintenez un dialogue ouvert avec celles que vous connaissez au sujet de la cybersécurité et de leur activité en ligne.

Conseils pour les enfants:

✓ Assurez-vous que vos enfants ne téléchargent que des applications provenant de sources fiables, comme Google Play ou l'App Store, et passez en revue les paramètres de confidentialité de toute application avant de la télécharger.

✓ La plupart des navigateurs offrent des fonctionnalités de recherche sécurisée pour vous aider à bloquer les sites Web au contenu douteux. Pensez à ajouter un logiciel de contrôle parental qui vous permet de filtrer les catégo-ries de sites Web, d'empêcher le partage de renseignements personnels et de planifier les horaires de navigation des enfants sur Internet.

✓ Apprenez à vos enfants à éviter les contenus douteux qu'ils trouvent en ligne. D'une manière générale, les enfants doivent éviter d'interagir avec les publicités intempestives, les sites Web demandant des renseignements personnels et les téléchargements provenant de personnes ou de sites inconnus.

Foire aux questions

Proposez-vous d'utiliser un gestionnaire de mots de passe?

Il n'y a pas de réponse absolue à cette question, car les avis des experts en sécurité divergent généralement à ce sujet, selon le contexte et l'application. Voici toutefois une liste des avantages et des inconvénients des gestionnaires de mots de passe :

Avantages :

Un mot de passe pour tout – La caractéristique la plus avantageuse est que, au lieu de devoir mémoriser des dizaines, voire des centaines de mots de passe pour vos comptes en ligne, il suffit d'en retenir un.

Génération de mots de passe puissants – L'un des avantages du gestionnaire de mots de passe est qu'il peut créer des mots de passe complexes, générés automatiquement pour vous.

Inconvénients :

Un point de défaillance unique – Si vous oubliez votre mot de passe, vous risquez de ne plus avoir accès aux différents comptes ou services gérés par votre gestionnaire de mots de passe. À l'inverse, si quelqu'un parvient à obtenir votre mot de passe principal, il pourra accéder à vos comptes.

Les programmes de gestion de mots de passe sont une cible pour les pirates informatiques – puisqu'ils n'ont qu'un seul mot de passe à trouver pour accéder à l'ensemble de vos données de connexion privées.

Comment établir que votre appareil a été piraté?

Voici quelques signes qui peuvent indiquer que votre appareil a été compromis :

Diminution notable de la durée de vie de la batterie

Un appareil qui a été compromis peut afficher une durée de vie de la batterie considérablement réduite, car le logiciel malveillant peut utiliser des ressources supplémentaires. Un appareil qui a été compromis peut afficher une durée de vie de la batterie considérablement réduite, car le logiciel malveillant peut utiliser des ressources supplémentaires.

Gel/performance médiocre

Une performance médiocre ou lente peut être causée par un logiciel malveillant qui utilise vos ressources ou entre en conflit avec d'autres applications de votre système.

Utilisation élevée des données

Une utilisation excessive des données peut être causée par un logiciel malveillant qui utilise votre connexion Internet pour renvoyer des renseignements vers son serveur.

Fenêtres contextuelles mystérieuses

Des alertes contextuelles constantes et inattendues pourraient indiquer que votre appareil a été infecté par une forme de logiciel malveillant qui oblige les appareils à afficher certaines pages générant des revenus pour les pirates grâce à des clics. Ce type de logiciel malveillant est connu sous le nom de logiciel publicitaire.

Activité inhabituelle liée à l'appareil

Si l'auteur de cybermenaces parvient à accéder à votre appareil (en particulier à votre téléphone), il peut également avoir accès à vos comptes. Surveillez les activités inhabituelles sur vos comptes, comme la réinitialisation des mots de passe, l'envoi de courriels et la réception de courriels de vérification pour de nouveaux comptes que vous n'avez pas ouverts.

Que dois-je faire si je pense que mon appareil a été compromis?

Voici quelques mesures à prendre si vous pensez que votre appareil a été compromis :

- Téléchargez une application de sécurité vérifiée qui peut analyser la présence de logiciels malveillants sur votre appareil et les supprimer de votre ordinateur ou de votre téléphone.
- Réinitialisez vos mots de passe et les renseignements sur votre compte pertinents.
- Parcourez votre liste d'applications et supprimez celles que vous ne reconnaissez pas ou dans lesquelles vous n'avez pas entièrement confiance.
- Mettez systématiquement à jour votre système d'exploitation et les applications. Cela garantira que toutes les vulnérabilités connues sont corrigées et ne peuvent pas être utilisées contre votre appareil.

Comment puis-je modifier mes paramètres de confidentialité pour mieux me protéger?

Regardez de quelle manière les données de localisation sont utilisées – Ces renseignements permettent de déterminer votre localisation et de vous suivre tout au long de la journée. Vérifiez et modifiez les paramètres de géolocalisation pour chaque application que vous utilisez.

Ne permettez pas aux applications d'accéder à votre téléphone – Les applications peuvent demander l'accès à vos contacts, à votre calendrier, à vos appareils photo, à vos photos et à votre microphone. Désactivez ces options dans les paramètres de l'appareil si elles ne sont pas nécessaires.

Restreignez l'accès à vos comptes – Les applica-tions peuvent demander l'accès à vos autres comptes, comme Facebook, Twitter ou Google. Lorsque vous n'utilisez plus une application, sup-primez-la et dissociez-la de vos comptes et de votre appareil dans les paramètres.

Comment puis-je utiliser les applications de réseaux sociaux en toute sécurité tout en protégeant ma vie privée?

Comprenez les renseignements recueillis

Avant de vous inscrire à un service en ligne ou de télécharger une application de réseaux sociaux, découvrez les renseignements personnels recueillis et les mesures de protection de la confidentialité proposées. Si vous n'appréciez pas la façon dont un service traite les renseignements personnels, ne vous y inscrivez pas.

Ajustez les paramètres de confidentialité

Avant de publier des renseignements ou des images sur les sites de réseautage social, passez en revue et modifiez les paramètres de confidentialité par défaut. Définissez vos préférences afin que les ren-seignements ne soient partagés qu'avec les per-sonnes désirées.

Désactivez la géolocalisation

Désactivez ou restreignez votre géolocalisation si elle est activée automatiquement. Nombre d'applications ou de services vous demanderont d'activer la géolocalisation. Déterminez si ces renseignements sont essentiels au service avant de prendre une décision.

Quelles applications mobiles puis-je utiliser en toute sécurité sur mon appareil?

Déterminez votre source et téléchargez des appli-cations auprès d'acteurs fiables.

Les applications figurant dans Google Play et l'App Store d'Apple sont soumises à un contrôle de légitimité, de qualité, de sécurité et à de nombreux autres facteurs. Les applications proposées par d'autres acteurs sont plus susceptibles d'être infectées par des programmes malveillants. Assurez-vous que la source de votre application est sûre et légitime.

Comprenez le fournisseur ou le développeur de l'application

Les développeurs d'applications de renom sont faciles à rechercher et de nombreuses applications renvoient au site Web de leur fournisseur, ce qui vous permet d'en apprendre davantage sur lui.

Inspectez les autorisations

Les applications ne doivent pas demander trop d'autorisations, et celles-ci doivent avoir un rap-port avec l'application.

Lisez les commentaires

Prêtez attention au nombre de téléchargements et à la note de l'application. La lecture des commentaires sur l'application peut également vous aider à comprendre ses avantages et ses inconvénients.

Rappels importants

✓ Inscrivez-vous aux alertes de votre banque. Grâce aux Alertes BMO, il est facile de faire le suivi des activités de votre compte et de surveiller les transactions douteuses. Vous pouvez vous inscrire par l'intermédiaire des Services bancaires en ligne ou de l'application BMO.

✓ Gardez vos coordonnées à jour. Ainsi, les employés de BMO peuvent communiquer avec vous immédiatement s'ils détectent une activité inhabituelle à votre compte.

✓ Veillez à utiliser l'ouverture de session à sécurité accrue dans la mesure du possible. Elle uti-lise plusieurs renseignements pour confirmer l'identité d'un client. Une combinaison de facteurs peut être utilisée, par exemple, un élément connu du client (comme un mot de passe) et un élément qu'il possède (comme un jeton matériel) ou de son identité (comme une empreinte digitale, ses traits faciaux ou sa voix, pratique aussi appelée biométrie).

Coordonnées

Visitez le site bmo.com/securite pour en savoir plus sur l'Unité Crime financier de BMO et sur les autres moyens de se protéger en ligne.

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 phishing@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 bmo.com/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 (au Canada).

Vous pensez avoir été victime d'un vol d'identité ou de la cybercriminalité?
Rendez-vous sur le site du Centre antifraude du Canada pour faire un signalement, obtenir un plan de rétablissement de l'identité personnalisé étape par étape et trouver des ressources utiles.

BMO MD

Unité Crime financier de BMO – Établir un nouveau point de référence en matière de sécurité financière

Pour en apprendre davantage, consultez le site bmo.com/securite