



Contribuez à protéger votre organisation contre la **fraude**

À BMO, nous sommes guidés par notre raison d'être, **Avoir le cran de faire une différence *dans la vie, comme en affaires***, donc nous sommes déterminés à protéger nos clients. Notre Unité Crime financier travaille jour et nuit pour vous protéger, vous avez toutefois également un rôle important à jouer afin d'assurer la sécurité de vos renseignements financiers. Vous trouverez ci-dessous des conseils pour aider votre organisation à éviter d'être victime de fraude.

 Protégez votre organisation contre ces fraudes financières courantes

Type de fraude	Comment protéger votre organisation
Escroquerie au faux ordre de virement (FOVI) et fraude liée aux paiements Une forme de piratage psychologique qui se produit souvent lorsqu'un fraudeur envoie un courriel qui semble provenir d'une source connue, comme un dirigeant ou un représentant des comptes fournisseurs, dans lequel il fait une demande qui semble authentique. Les escroqueries FOVI entraînent fréquemment des fraudes liées aux paiements.	- Établissez un processus de rappel pour tout changement apporté aux paiements ou aux numéros de compte, en particulier les instructions électroniques. - Mettez en place des contrôles internes, comme un approuvateur secondaire. - Limitez ce que vous publiez sur les médias sociaux, en particulier si vous occupez un poste de nature délicate.
Fraude par carte de crédit Transaction par carte de crédit qui n'est pas effectuée par le titulaire de la carte, notamment en cas de perte ou de vol, d'altération de terminaux de commerçants et de vol d'identité.	- Signalez la perte ou le vol d'une carte dès que possible. - Dans la mesure du possible, utilisez la technologie de carte à puce plutôt que la bande magnétique. - Surveillez vos comptes pour repérer les transactions que vous ne reconnaissez pas. - Ne divulguez jamais de renseignements permettant d'identifier une personne lors d'un appel non sollicité. - Installez un logiciel de protection qui surveille vos renseignements sur le Web caché.
Fraude par chèque La fraude la plus courante touchant les entreprises à l'heure actuelle. Des chèques sont souvent volés dans la poste et modifiés, falsifiés par lavage ou reproduits (chèques contrefaits).	- Envisagez plutôt d'utiliser les paiements électroniques. - Mettez en place des contrôles : désactivez les chèques dormants, fermez les comptes inutiles, passez en revue le rapport sur les comptes et effectuez la concordance des comptes. - Tirez parti des Services technologiques de BMO, notamment de l'option de confirmation de paiement. - Conservez les chèques dans un endroit sûr et détruisez ceux qui sont inutiles.
Prises de contrôle de compte Ce type de fraude se produit lorsqu'un malfaiteur obtient un accès non autorisé à un compte de client et y effectue des transactions frauduleuses. Cette fraude se fait principalement en ligne, mais peut aussi se faire en personne ou par téléphone.	- Limitez ce que vous publiez sur les médias sociaux. - Établissez un processus selon lequel les paiements doivent être approuvés par un approuvateur actif, différent de l'initiateur (double approbation). - Supprimez les courriels contenant des renseignements personnels relatifs aux SBLE, comme le code de client et d'utilisateur. - Assurez-vous que la barre d'adresse de tout site sensible affiche un cadenas fermé. - Faites une distinction entre la technologie utilisée à des fins professionnelles et celle utilisée à des fins personnelles et installez et tenez à jour un logiciel antivirus. - Mettez en place l'authentification multifactorielle.



Conseils pour protéger votre organisation

Suivez ces conseils afin de protéger votre organisation contre la fraude

Supervision efficace

- ✓ Mettez en œuvre un logiciel de surveillance des transactions et l'authentification multifactorielle.
- ✓ Créez une liste de vérification indiquant quoi faire en cas de fraude.
- ✓ Éduquez les employés sur les stratagèmes courants de piratage psychologique et les méthodes de cyberattaque et de fraude.
- ✓ Établissez soigneusement les procédures et les contrôles pour les fournisseurs avec lesquels vous faites affaire.

Séparation des tâches

- ✓ Exigez que les paiements soient approuvés par un approbateur actif, différent de l'initiateur.
- ✓ Encouragez les congés obligatoires pour les postes de nature délicate.
- ✓ Créez des postes d'administrateurs remplaçants pour les congés ou les urgences et formez-les.
- ✓ Discutez avec BMO de la désignation d'une personne-ressource pour les cas de fraude.

Gestion de l'accès

- ✓ Passez régulièrement en revue les privilèges d'accès des employés pour en vérifier la convenance et tenir compte des départs.
- ✓ Limitez l'accès aux fichiers principaux du personnel.
- ✓ Contrôlez les fichiers de fournisseurs et les fichiers principaux et les droits de tirer des chèques.
- ✓ Communiquez l'importance d'utiliser la technologie de l'entreprise pour le travail uniquement.

Éviter les sites Web frauduleux

- ✓ N'accédez pas au site Web des SBLE de BMO au moyen d'un moteur de recherche; en cas de doute, rendez-vous directement sur bmo.com.
- ✓ Assurez-vous que la barre d'adresse de tout site sensible affiche un cadenas fermé ou l'icône permettant d'afficher les renseignements d'un site.
- ✓ Ajoutez le site bmo.com à vos favoris pour y accéder ultérieurement.
- ✓ Installez [Trusteer Rapport](#).



Travail à distance

Suivez ces conseils lorsque vous travaillez de la maison afin de protéger votre organisation.

- ✓ Modifiez le mot de passe du Wi-Fi de votre domicile, et établissez un réseau distinct pour les visiteurs.
- ✓ Gardez à jour le micrologiciel de votre routeur.
- ✓ Connectez les appareils de l'Internet des objets (IdO) à un réseau distinct, comme un réseau d'invités.
- ✓ Envisagez de désactiver le micro des assistants virtuels comme Alexa et Google Home, de les débrancher lorsque vous travaillez ou de les tenir loin de votre espace de travail.
- ✓ Soyez conscient de la nature confidentielle de ce que vous dites lors d'une conversation en lien avec le travail.
- ✓ Verrouillez toujours votre ordinateur lorsque vous quittez votre bureau.
- ✓ Séparez vos appareils personnels et de travail.



Conseils pour protéger également vos

- ✓ Ne divulguez jamais votre mot de passe, y compris à votre banque.
- ✓ Utilisez l'authentification multifactorielle.
- ✓ Tenez vos coordonnées à jour.
- ✓ Inscrivez-vous aux alertes des services bancaires.
- ✓ Utilisez des mots de passe forts et uniques.
- ✓ Faites en sorte de pouvoir reconnaître [les fraudes et les signaux d'avertisseurs courants](#) pour être en mesure de les éviter.
- ✓ Soyez à l'affût des tentatives d'hameçonnage.
- ✓ Sécurisez vos appareils.
- ✓ Passez en revue d'autre contenu de sensibilisation à la fraude sur BMO.com. ([Canada](#) | [États-Unis](#)).

Pour en savoir plus, consultez bmo.com/securite.

Les renseignements sont fournis à titre informatif seulement et ne visent pas à fournir des conseils juridiques, financiers, de placement ou autres conseils professionnels et ne doivent pas être utilisés à cet égard.

Signaler un incident de fraude

Élaborez un plan de signalement de la fraude et transmettez-le à vos employés.

1. Obtenez tous les renseignements pertinents.
2. Communiquez avec votre équipe Gestion relationnelle, votre équipe Service à la clientèle ou le Soutien technique de BMO : ils recueilleront les renseignements nécessaires, amorceront un processus d'enquête et de recouvrement (s'il y a lieu) et vous fourniront des conseils.
3. Si vos systèmes sont potentiellement compromis :
 - Demandez à ce que votre accès aux SBLE soit temporairement verrouillé.
 - Contactez un professionnel de la cybersécurité local réputé.
4. Si votre compte des SBLE fait l'objet d'une transaction non autorisée ou est compromis :
 - Fournissez tous les renseignements à votre représentant BMO dès que possible.
5. Produisez un rapport de police contenant le plus de renseignements possible.
6. Contactez votre assureur pour lui signaler tout incident pouvant entraîner une perte de fonds ou de données.
7. Effectuez une analyse judiciaire de la cybersécurité pour procéder à une vérification et à un nettoyage de vos systèmes.
8. Communiquez avec votre représentant BMO pour rétablir l'accès aux SBLE et aux services.