Gestion du risque de fraude liée aux paiements :

Conseils et signaux avertisseurs

Toute entreprise s'expose à des risques de fraude. Nous nous engageons à vous fournir tout le soutien nécessaire pour vous aider à minimaliser les risques de fraude auxquels votre compte bancaire de BMO[MD] pourrait être exposé. Le présent document, intitulé **Conseils et signaux avertisseurs concernant la fraude** – Liste de vérification, contient un un certain nombre de meilleures pratiques à appliquer pour prévenir la fraude liée aux paiements et vous protéger contre la violation de données. Nous vous recommandons fortement de lire et de mettre en pratique les mesures qu'elle contient, puis de les communiquer aux autres membres de votre organisation.

Besoin d'aide?

Si vous avez des questions sur le contenu de la liste de vérification, adressez-vous à votre représentant de BMO ou envoyez un courriel à bmo.tps@bmo.com.

BMO[MD] Banque de Montréal

Ici, pour vous.[MC]

Conseils et signaux avertisseurs concernant la fraude

Logiciels malveillants	Conseils et signaux avertisseurs
Maliciels, alias logiciels malveillants Le maliciel s'insinue dans votre système informatique et y exécute des activités et des opérations non autorisées. En voici des exemples : • Prise de contrôle de la messagerie électronique • Prise de contrôle ou vol d'identité de compte de grande entreprise • Violation et vol de données • Déni de service	✓ Téléchargez Rapport de Trusteer[MD*] IBM, un logiciel gratuit accessible à partir de la page d'ouverture de session des Services bancaires en ligne pour entreprises de BMO du site bmo.com[1]. Fonctionnant avec les pare-feu et logiciels antivirus existants, il constitue une mesure de sécurité supplémentaire. ✓ Mettez régulièrement à jour vos logiciels antivirus et antimaliciels. ✓ Vérifiez toujours d'où proviennent les demandes de transfert de fonds. ✓ Assurez-vous que vous êtes bien sur un site Web légitime. En cas de doute, entrez l'adresse URL que vous connaissez. ✓ Prenez conscience de tout changement à votre expérience des Services bancaires en ligne pour entreprises, notamment à l'affichage d'adresses URL inhabituelles dans la fenêtre de votre navigateur, aux demandes de validation des identifiants d'ouverture de session, au ralentissement inhabituel de votre session en ligne ou aux demandes de saisie des identifiants d'ouverture de session sur une page autre que la page d'identification. ⚑ Méfiez-vous des courriels dans lesquels on vous demande de communiquer des renseignements relatifs à votre compte ou vos identifiants de connexion bancaire (noms d'utilisateur et mots de passe) ou on vous offre d'effectuer la vérification de votre compte. BMO ne communiquera jamais avec vous par téléphone, par courriel ou par message texte pour vous demander votre code d'utilisateur, votre mot de passe, votre NIP, votre numéro d'assurance sociale ou d'autres renseignements hautement confidentiels.

Conseils et signaux avertisseurs concernant la fraude

Hameçonnage

Hameçonnage et hameçonnage ciblé
L'*hameçonnage* est l'une des techniques les plus souvent utilisées pour infecter un système informatique en y introduisant un maliciel.

Manifestations de l'hameçonnage
En général, la technique consiste à envoyer des courriels non sollicités qui ont l'apparence de courriels légitimes et portent les noms et logos de vraies sociétés comme des banques et des compagnies d'assurance.

Dans ces courriels, on peut vous demander vos renseignements personnels ou financiers, vous inviter à cliquer sur un lien ou vous diriger vers un site Web.

Hameçonnage réussi : maliciel introduit
Si vous divulguez les renseignements demandés, le maliciel peut infecter vos comptes de courriel, ainsi que les adresses courriel et le réseau de votre entreprise. L'opération peut aboutir à un vol d'identité et à la prise de contrôle de la messagerie électronique de l'entreprise, et faciliter le piratage de bases de données.

L'*hameçonnage* ciblé est une technique par laquelle des criminels cherchent dans les réseaux sociaux (Facebook[MD†], Twitter[MD‡], LinkedIn[MD#]) des personnes qui ont le pouvoir d'autoriser des paiements. Ces personnes reçoivent ensuite des courriels qui contiennent des maliciels.

Conseils et signaux avertisseurs

- Méfiez-vous des demandes de renseignements confidentiels par courriel ou par message texte, qu'elles arborent le logo d'une entreprise véritable ou portent un en-tête.
- Ne communiquez jamais vos données d'identification personnelles ni vos renseignements financiers (renseignements sur un compte, noms d'utilisateur, mots de passe et numéros d'identification personnels). Ne communiquez jamais votre jeton de sécurité ni le mot de passe qui y est associé. À noter que BMO ne vous demandera jamais ce type de renseignement.
- Ne cliquez jamais sur un lien dans un courriel suspect, car il se pourrait que vous soyez dirigé vers un site frauduleux ou que votre clic active un maliciel (par exemple, un logiciel espion) qui surveillera vos frappes afin d'accéder à vos renseignements financiers.
- Prenez garde de rendre publics dans les sites de médias sociaux trop de renseignements sur votre travail, puisque cela peut faire de vous et de votre entreprise des cibles d'hameçonnage.

Fenêtres contextuelles dans l'Internet

Fenêtres contextuelles et faux logiciels antivirus dans l'Internet
Ce type de fenêtre contextuelle contient souvent un message urgent, par exemple une « alerte de sécurité » ou un avis de « risque élevé de menaces ». On l'appelle également faux logiciel antivirus.

La fenêtre vous dirige vers un site qui vous invite à acheter un soi-disant programme de sécurité, sauf qu'en réalité le site est bidon, et votre numéro de carte de crédit et vos autres renseignements sont communiqués directement aux fraudeurs.

Conseils et signaux avertisseurs

Gestion des fenêtres contextuelles

- ✓ Assurez-vous que votre entreprise a mis en place des mesures pour contrôler les fenêtres contextuelles dans Internet.
- ✓ Apprenez aux utilisateurs à ne pas autoriser l'affichage des fenêtres contextuelles et à ne pas répondre aux messages qu'elles contiennent.

Conseils et signaux avertisseurs concernant la fraude

Programmes gratuits clones

Programmes gratuits également appelés programmes sosies
Le sosie est un programme censé reproduire la présentation, l'impression générale et même le code d'un logiciel authentique, et le fait qu'il soit « gratuit » donne envie aux utilisateurs de le télécharger.

Le logiciel est faux et télécharge un maliciel dans le système informatique.

Conseils et signaux avertisseurs

Quand la gratuité n'a rien d'une aubaine

✓ Veillez toujours à télécharger des logiciels à partir d'un site officiel.

⚑ Méfiez-vous de la publicité pour des programmes gratuits dans les fenêtres contextuelles dans Internet, même si les logos arborés sont authentiques. Ne téléchargez des programmes qu'à partir de sites Web de confiance, et vérifiez l'adresse URL fournie.

Sites Web compromis

Sites Web faux ou compromis
Ces sites semblent légitimes, mais il n'en est rien. On pourrait vous demander de valider vos données d'identification, même après que vous aurez ouvert une session. Il se peut également que des adresses URL inhabituelles s'affichent dans la fenêtre de votre navigateur. Vous pourriez être dirigé vers un site Web tout à fait différent et être invité à y saisir des renseignements personnels ou financiers.

Conseils et signaux avertisseurs

Accès aux sites Web

✓ Entrez l'adresse URL du site dans la fenêtre de votre navigateur; par exemple : www21.bmo.com.

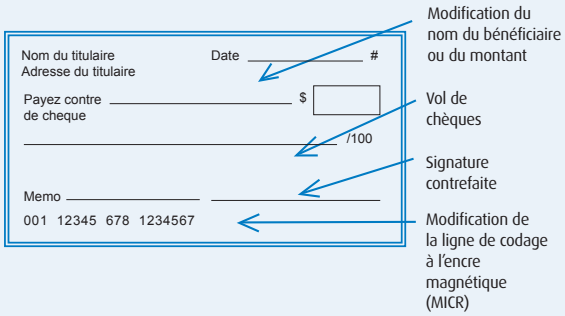
✓ Dans l'onglet Ouvrir une session du site bmo.com, cliquez sur Services bancaires en ligne.

✓ Ajoutez le site officiel à vos favoris.

Fraude par chèque

Fraude par chèque
La fraude par chèque touche à la fois les organisations qui émettent les chèques et celles qui reçoivent et déposent les paiements par chèque.

La fraude par chèque demeure le type de fraude le plus courant auquel les entreprises sont confrontées. Elle englobe le vol et l'utilisation de renseignements sur des chèques véritables, la contrefaçon, la modification de données de chèques et même le remplacement de données de chèque par des données falsifiées



Conseils et signaux avertisseurs

✓ **Utilisez l'encre magnétique**
Elle facilite la détection des photocopies.

✓ **Utilisez des chèques hautement sécurisés**
Ils sont dotés d'un certain nombre de caractéristiques (encre liante et cercles thermoréactifs) qui les rendent plus difficiles à falsifier.

✓ **Vérification des chèques**
Vérifiez si la signature est authentique, si des mots sont mal orthographiés et si le montant, le bénéficiaire et les autres renseignements sont exacts.

Conseils et signaux avertisseurs concernant la fraude

Fraude liée aux paiements électroniques	Conseils et signaux avertisseurs
Fraude par virement automatique ou par virement télégraphique Un stratagème de fraude classique consiste à compromettre un compte en utilisant des données d'identification et des renseignements recueillis par hameçonnage ou par d'autres moyens.	✓ Prenez l'habitude de valider les demandes de paiement par virement électronique par courriel et par télécopieur; à cette fin, communiquez avec le demandeur et assurez-vous que la personne à qui vous parlez est bel et bien le demandeur. Pour ce faire, vous pouvez comparer le numéro de téléphone qui vous a été donné à celui qui figure dans vos dossiers ou poser des questions auxquelles seul le véritable demandeur connaît les réponses. ✓ Faites en sorte que les employés du service à la clientèle posent aux appelants des questions d'authentification supplémentaires, pour être certains qu'ils sont bien les personnes qu'ils prétendent être. ✓ Séparez la fonction d'exécution du paiement et celle de l'approbation aux fins de double validation. Par exemple, l'employé qui effectue un paiement électronique ne sera pas autorisé à le transmettre. Pour que les instructions de paiement soient exécutées, il faut qu'un second employé examine et approuve la transaction, et qu'il vérifie notamment les instructions du client. Si un transfert frauduleux est effectué, les données d'identification du premier employé ne pourront être utilisées pour transmettre le paiement. ✓ Examinez régulièrement les demandes de paiement électronique pour établir les habitudes normales des demandeurs (fourchette en dollars, nombre de demandes de paiement faites par mois, etc.). Ainsi, toute demande qui semble inhabituelle sera détectée et fera l'objet d'une enquête. ⚑ Si votre expérience des Services bancaires en ligne pour entreprises de BMO vous paraît insolite, par exemple, on ne cesse de vous demander le mot de passe associé à votre jeton de sécurité, ne communiquez pas l'information demandée.

[1] Le téléchargement et l'utilisation du logiciel sont assujettis aux conditions de la convention de droits d'utilisation qui accompagne le logiciel Trusteer Rapport. En téléchargeant et en installant le logiciel Rapport de Trusteer, vous consentez à respecter toutes les modalités dudit logiciel. La Banque de Montréal n'est pas responsable de ce logiciel ni des autres produits ou services associés au logiciel Rapport de Trusteer, ni du site Web du logiciel Trusteer Rapport, et elle ne peut s'en porter garante. La Banque de Montréal n'est pas responsable des difficultés, des conséquences, des coûts, des demandes d'indemnisation, des dommages ni des pertes pouvant découler de quelque façon que ce soit du téléchargement ou de l'utilisation du logiciel. Les problèmes, questions et préoccupations concernant le logiciel Rapport de Trusteer doivent être soumis à Trusteer.