Prêt à prévenir la fraude?

Conseils pour protéger votre entreprise contre la fraude

TD On est prêts pour vous

Reconnaître et prévenir la fraude

Votre entreprise est-elle à l'abri?

Quel que soit le type d'entreprise, le risque de fraude est en constante évolution et bien présent.

Faits sur la fraude

- 33 % de toutes les défaillances ou faillites d'entreprise sont causées par le vol ou la fraude[1].
- Près des trois quarts des entreprises ont signalé être la cible de fraude sur les paiements en 2016[2].
- Bien que les chèques demeurent la source la plus fréquente de fraude sur les paiements, les fraudeurs utilisent de nouvelles techniques en recourant au courrier électronique, aux médias sociaux et aux logiciels malveillants pour cibler les paiements électroniques[2].

[1] Source : i-sight.com, accès le 13 septembre 2017.
[2] 2016 AFP Payments Fraud and Control Survey, Association for Financial Professionals.

Soyez vigilant et ne divulguez pas vos renseignements personnels. La TD ne vous demandera pas de fournir des renseignements personnels ou des codes d'accès comme vos identifiants, mots de passe, codes d'authentification ou numéros de compte par téléphone ou par courriel.

Manœuvres électroniques frauduleuses courantes

- **Hameçonnage par courriel/ Hameçonnage par texto/ Hameçonnage vocal :** courriel, texto ou appel téléphonique en apparence authentique qui semble provenir d'une entreprise légitime et qui demande au destinataire de confirmer son numéro de compte ou une activité frauduleuse, d'agir pour prévenir la suspension de son compte, etc. Généralement, le courriel ou le texto contient un lien ou un document menant à un faux site Web où l'on demande de fournir les codes d'accès ou d'autres renseignements confidentiels. N'ouvrez aucune pièce jointe et ne cliquez sur aucun lien contenu dans un courriel provenant d'un expéditeur inconnu.
- **Courriel d'imposteur :** courriel de quelqu'un qui se fait passer pour une personne connue du destinataire (chef de la direction, directeur des Finances, fournisseur, etc.). Ces courriels demandent souvent un virement interbancaire ou un transfert électronique de fonds ou ils peuvent fournir de nouvelles directives ou de nouveaux numéros de compte pour un paiement à faire. Comme il est relativement facile d'usurper une identité dans un courriel, vous devriez toujours confirmer les instructions de paiement en personne ou par téléphone en composant les numéros de téléphone que vous avez en dossier.

- **Logiciel malveillant :** programme malveillant utilisé pour perturber le fonctionnement d'un ordinateur, recueillir de l'information sensible ou accéder à des systèmes informatiques. Le logiciel malveillant peut être caché dans une pièce jointe à un courriel que l'utilisateur a ouverte ou dans une macro-instruction sur laquelle il a cliqué.
- **Rançongiciel :** type de logiciel malveillant qui infecte un ordinateur en chiffrant ses fichiers et données jusqu'à ce que la victime paie une rançon.

Même si vous ne pouvez pas prédire quand et pourquoi votre entreprise peut devenir une cible, vous pouvez prendre de nombreuses mesures pour réduire le risque de fraude.

Meilleures pratiques pour prévenir la fraude

Il existe plusieurs meilleures pratiques conçues pour protéger vos opérations financières et réduire les risques liés à la fraude. Lisez les conseils ci-dessous et intégrez-les dans votre plan de prévention de la fraude au quotidien. **En éliminant les possibilités de fraude, vous aurez déjà fait beaucoup pour la prévenir.**

Liste de vérification de la sécurité en ligne

Services bancaires

Il est primordial pour la TD de garantir la sécurité des renseignements personnels de ses clients. Ne partagez avec personne vos codes d'accès confidentiels aux services bancaires en ligne. **Le Groupe Banque TD ne vous demandera jamais de fournir des renseignements personnels, des codes d'accès ou des renseignements sur votre compte par courriel ou téléphone.**

- Prenez connaissance des fonctions de sécurité offertes pour les produits et services de la TD et mettez-les en œuvre, y compris celles qui permettent la séparation des tâches et la vérification de l'identité en double et qui améliorent l'administration et le contrôle.
- Tapez toujours l'adresse du site Web de la banque. N'utilisez pas les liens compris dans les courriels, les fenêtres contextuelles ou les moteurs de recherche.
- Fixez des limites de paiement appropriées à chaque utilisateur.
- Assurez-vous que votre navigateur est connecté de façon sécuritaire à tous les sites bancaires en utilisant le protocole HTTPS (c'est-à-dire que « https:// » doit faire partie de l'adresse). De cette façon, l'information circulant entre votre ordinateur et le site Web de la banque est chiffrée.

- N'accédez jamais aux sites Web des banques en utilisant un ordinateur public ou partagé susceptible de contenir un logiciel non autorisé.
- N'utilisez pas les réseaux WI-FI publics pour accéder aux services bancaires en ligne, car ils ne sont pas sécurisés.
- Observez la présentation des écrans des services bancaires en ligne. Si elle diffère de ce que vous voyez habituellement, il se pourrait que votre navigateur soit compromis. Mettez fin immédiatement à votre opération et signalez la situation à la TD.
- Fermez la session quand vous avez fini ou si vous laissez votre ordinateur sans surveillance.
- Utilisez un ordinateur autonome et pourvu de la fonction de verrouillage exclusivement pour effectuer des opérations bancaires en ligne, avec lequel il est impossible d'accéder au courriel et de naviguer sur Internet.
- Soyez prudent quand vous visitez d'autres sites Web sur l'ordinateur que vous utilisez pour effectuer vos opérations bancaires, car des logiciels malveillants peuvent être téléchargés à votre insu à partir de sites Web non fiables.

Ordinateurs

- Installez un pare-feu pour protéger votre ordinateur contre les pirates informatiques.
- Utilisez uniquement les logiciels avec licence d'utilisation légale et mettez-les à jour.

- Utilisez le logiciel antivirus le plus récent sur le marché. Les logiciels gratuits peuvent ne pas protéger contre les menaces les plus récentes.
- Choisissez des mots de passe uniques comprenant une combinaison de lettres, de chiffres et de symboles.
- N'utilisez pas les mêmes mots de passe pour les applications personnelles et professionnelles.
- Assurez-vous de désactiver la fonction d'entrée automatique du mot de passe de votre navigateur.
- N'enregistrez jamais vos mots de passe sur votre ordinateur, dans Internet ou dans un logiciel.

Courriel

- N'indiquez pas de renseignements bancaires dans un courriel envoyé à la TD ou à quiconque, à moins qu'il ne soit chiffré.
- N'ouvrez pas les fichiers joints dans les courriels provenant d'expéditeurs inconnus.
- Ne cliquez pas sur les liens contenus dans un courriel pour accéder à une page Web. Si vous doutez de l'authenticité du message, appelez pour vérifier ou tapez l'adresse du site Web directement dans votre navigateur.

- Méfiez-vous des courriels qui semblent provenir d'un expéditeur fiable (par exemple, une banque ou un organisme gouvernemental) et qui vous demandent de fournir ou de confirmer des renseignements sur votre compte ou des codes d'accès comme un identifiant, un mot de passe ou un code d'authentification en suivant un hyperlien. Signalez immédiatement les courriels suspects à la TD à phishing@TD.com.
- Si vous croyez avoir répondu à un courriel suspect et que vous avez partagé vos codes d'accès aux services bancaires en ligne, veuillez signaler la situation immédiatement.
    - Pour les Services bancaires par Internet aux entreprises, veuillez communiquer avec le Centre de soutien, Gestion de trésorerie au 1-800-567-4455.
    - Pour les services de BanqueNet, communiquez avec un spécialiste de BanqueTel au 1-800-895-4463.
- Vérifiez toujours les directives de paiement par téléphone ou en personne même si elles semblent provenir d'une source connue. Ne suivez pas les directives de paiement envoyées par courriel, car le courriel peut être frauduleux.

Liste de vérification de la sécurité des chèques

Protection contre la fraude : inscrivez-vous à un service de protection contre la fraude par chèques qui gère la compensation de chèques tirés sur vos comptes en dollars canadiens et américains.

Centralisez l'émission des chèques : ne laissez pas les chèques à la portée d'employés non autorisés.

Gardez les chèques en lieu sûr : gardez sous clé les chèques non émis, les chèques numérisés aux fins de dépôt, les timbres de signature et les formulaires de commande de chèques. Vérifiez le nombre de chèques fréquemment et sans préavis.

Sécurité de la poste : évitez d'envoyer les chèques par la poste dans des enveloppes à fenêtre ou transparentes.

Utilisez des chèques de grande qualité : utilisez des chèques de qualité comprenant une ligne de codage magnétique et les plus récentes caractéristiques de sécurité.

Conseils pour réduire davantage le risque de fraude par chèque

- **Paiements de factures :** payez les factures courantes électroniquement. Si vous utilisez les Services bancaires par Internet aux entreprises, vous pouvez réduire les risques davantage en restreignant l'accès aux paiements de factures afin que seuls les bénéficiaires inscrits puissent être payés.

- **Paiement préautorisé :** réduisez le nombre de chèques que vous émettez en permettant aux créanciers de débiter les paiements récurrents automatiquement de votre compte.
- **Cartes de crédit :** réglez par carte de crédit si possible pour réduire l'utilisation de chèques.
- **Chèques de paie :** connectez votre logiciel de paie maison à un service de transfert électronique de fonds pour déposer directement la paie dans le compte des employés. Nous pouvons aussi vous renseigner sur les fournisseurs de services de paie qui peuvent gérer tous les aspects de la paie et du dépôt direct pour votre entreprise.
- **Traites bancaires :** remplacez les traites bancaires par des virements interbancaires.

Liste de vérification de la sécurité des dépôts

Coffrets postaux : si vous recevez beaucoup de paiements par chèque, envisagez de vous inscrire à un service de coffret postal géré par une banque pour centraliser et automatiser la perception des comptes clients.

Effets retournés : utilisez des timbres d'endos qui imputent clairement les effets retournés au compte de votre choix. Les chèques déposés en utilisant le service de traitement de dépôts à distance comprennent un endossement virtuel, numérisé au dos du chèque.

Cartes de paiement : si vous acceptez les cartes de crédit ou de débit de vos clients, apprenez aux employés à reconnaître les opérations ou les comportements suspects. Signalez immédiatement toute activité suspecte à Solutions aux commerçants TD au 1-800-363-1163. Assurez-vous également de vous conformer à la Norme de sécurité des données de l'industrie des cartes de paiement (norme PCI DSS).

Liste de vérification de la sécurité de la comptabilité

Rapprochement quotidien : rapprochez chaque jour toutes les opérations bancaires de votre entreprise et signalez immédiatement les opérations inhabituelles.

Fonctions distinctes : assurez-vous que des personnes différentes sont responsables de l'émission des chèques et de la conciliation du relevé bancaire.

Comptes distincts : envisagez d'ouvrir des comptes différents pour séparer les paiements, comme les virements interbancaires entrants et les nombreux chèques de faible montant.

Audit de sécurité : faites effectuer une vérification complète, avec examen approfondi de vos procédures de sécurité, par un professionnel en comptabilité.

On est prêts à vous conseiller sur la prévention de la fraude.

Nous pouvons vous fournir de l'information sur les produits et services que nous offrons pour vous aider à protéger votre entreprise contre la fraude.

Si vous êtes un client des Services bancaires commerciaux ou des Services bancaires aux grandes entreprises, veuillez communiquer avec votre directeur des relations-clients pour en savoir plus.

Si vous êtes un client des Services bancaires aux PME, composez le **1-800-895-4463** pour parler à un spécialiste des Services bancaires aux entreprises.

MD Le logo TD et les autres marques de commerce sont la propriété de La Banque Toronto-Dominion.
591329(1117)