Meilleures pratiques de prévention de la fraude

24 façons de protéger votre entreprise

Votre entreprise est-elle bien protégée?

Quel que soit le type d'entreprise, le risque de fraude est toujours présent. Bien qu'il soit impossible de prédire pourquoi ou quand votre entreprise deviendra la cible d'une fraude, il y a beaucoup à faire pour en réduire le risque.

Nous avons réuni quelques-unes des meilleures pratiques auxquelles nos clients ont recours pour protéger leurs opérations financières et leurs rapports avec nous. Nous vous invitons à passer en revue les conseils qui suivent pour déterminer dans quelle mesure votre entreprise est protégée contre la fraude et pour vous aider à élaborer un plan de prévention. Vous constaterez que nombre de ces pratiques peuvent être adoptées aisément et à peu de frais. Éliminez les occasions de fraude et vous ferez déjà beaucoup pour vous protéger!

Nos spécialistes de la gestion de trésorerie seront ravis de collaborer avec vous. Nous pouvons vous aider à cerner vos besoins et vous fournir de l'information sur les produits et services que nous pouvons offrir à votre entreprise pour l'aider à se protéger contre la fraude.

Conciliation

1. **Conciliation quotidienne :** Conciliez toutes vos opérations bancaires chaque jour. Vous pouvez rapidement et facilement accéder à ces données en ligne.
2. **Concordance paie-bénéficiaire :** Transmettez-nous une copie de votre registre de chèques comportant les renseignements sur les bénéficiaires. Les chèques reçus chaque jour peuvent être contrôlés, et les éléments qui ne concordent pas, notamment les modifications du nom des bénéficiaires, vous seront signalés afin que vous puissiez prendre des mesures immédiates.
3. **Relevés bancaires de fin de mois :** Examinez chaque élément de votre relevé, y compris les images de chèques. Si un élément de votre relevé ne correspond pas à vos dossiers, vous devez nous en aviser dans un délai de 30 jours.

Chèques

4. **Émission de chèques centralisée :** Ne laissez pas de chèques entre les mains d'employés non autorisés.
5. **Mise sous clé des chèques :** Mettez sous clé, dans des endroits distincts et sûrs, tous les chèques non émis, les timbres de signature et les bons de commande de chèques.
6. **Renforcement des mesures de sécurité :** Contrôlez votre stock de chèques, depuis l'impression et l'émission jusqu'à la signature et à l'envoi. En outre, vérifiez le stock de chèques fréquemment et à l'improviste.
7. **Papier d'impression de chèque :** Le choix du papier est important. Insistez pour obtenir un papier de qualité afin de maximiser la protection contre la fraude. Notre fournisseur de chèques, Davis + Henderson[MD], offre de nombreuses caractéristiques graphiques de pointe en matière de sécurité, notamment :
   - les microcaractères
   - la protection contre les agents chimiques
   - les fibres fluorescentes et les messages à l'encre de sécurité
   - les hologrammes
   - l'icône de cadenas
   - un motif métallisé
8. **Numéros de série imprimés à l'encre magnétique (MICR) :** Utilisez les numéros de série MICR obligatoires sur tous les chèques de comptes commerciaux.
9. **Impression de chèques :** À l'impression et au traitement des chèques :
   - utilisez des caractères de 10 points ou plus
   - évitez d'utiliser les enveloppes à fenêtre

Substituts aux chèques

10. **Paiement de factures :** Payez vos comptes réguliers par voie électronique. Les services bancaires par Internet peuvent faciliter les paiements postdatés.
11. **Paiement des taxes :** Payez la TPS, la TVQ et la TVH, et effectuez d'autres paiements complexes de taxes au moyen d'un service de production de déclaration et de paiement par Internet.
12. **Cartes de crédit :** Encouragez les fournisseurs à accepter les cartes de crédit pour tout montant inférieur à 5 000 $ afin d'éliminer les chèques à faibles montants. De plus, certaines cartes vous permettent d'accumuler des récompenses.
13. **Chèques de paie :** Reliez votre logiciel de traitement de la paie à un service de transfert électronique de fonds (TEF) afin de déposer la paie directement dans le compte des employés. Ou encore, informez-vous au sujet de Ceridian[MD]. Cette entreprise peut s'occuper

de l'ensemble des fonctions de paie et de dépôt direct à votre place.

14. **Paiement des fournisseurs :** Un outil de consolidation des comptes créditeurs peut servir à payer, par voie électronique, les fournisseurs qui exigent l'envoi d'une preuve de paiement par télécopieur, par courriel ou par échange de données informatisées (EDI).
15. **Traites bancaires :** Les traites bancaires perdues peuvent être remplacées, mais l'original reste toujours valide. Pour les paiements en dollars US ou autre devise, songez plutôt à utiliser le virement par câble.
16. **Virements par câble manuels :** Utilisez un service de virement en ligne comportant des fonctions de sécurité, notamment les dispositifs d'authentification et les gabarits pour paiements préautorisés, plutôt qu'un service par téléphone ou télécopieur.
17. **Paiement préautorisé :** En autorisant vos créanciers à débiter automatiquement votre compte, vous pouvez gérer votre trésorerie puisque vous savez exactement quand les paiements seront effectués.

Dépôts

18. **Comptes de dépôt locaux :** Songez à éliminer les comptes de dépôts locaux utilisés par vos bureaux régionaux. Utilisez plutôt le dépôt direct dans un compte central et vérifiez-en l'activité chaque jour.
19. **Boîte postale scellée :** Demandez à vos clients de poster leurs paiements à une boîte postale gérée par une banque afin de centraliser et d'automatiser le processus de perception des comptes clients.
20. **Effets retournés :** Utilisez des tampons d'endossement qui permettent de diriger précisément les effets retournés vers le compte de votre choix.
21. **Services aux commerçants :** Apprenez à vos employés à reconnaître les pratiques frauduleuses et établissez un processus de transmission à une instance supérieure qui leur permettra de vous signaler ces situations. Assurez-vous de respecter la Norme de sécurité des données de l'industrie des cartes de paiement, qui protège les renseignements confidentiels de vos clients et, en fin de compte, votre marque. Assurez-vous, en tout temps, de ranger vos factures dans un endroit sûr et d'exercer un contrôle vigilant sur le matériel de point de vente, qui peut aussi faire l'objet d'une utilisation frauduleuse.

Comptabilité

22. **Séparation des fonctions :** Les responsables de la préparation et de la signature des chèques doivent être différents de ceux qui s'occupent de la conciliation avec le relevé bancaire.
23. **Comptes spéciaux :** Ouvrez des comptes distincts pour séparer notamment les virements entrants et les nombreux chèques à faible montant.
24. **Vérification de sécurité :** Nous recommandons de faire faire une vérification complète, y compris un examen approfondi de vos mesures de sécurité, par un comptable professionnel.

    Éliminez les occasions de fraude et vous ferez déjà beaucoup pour vous protéger. Vu les pertes financières, l'interruption du cours normal de vos activités et la perte de confiance des clients que peut occasionner une fraude, la mise en œuvre des meilleures pratiques est bien peu chère payée pour se protéger. Communiquez avec votre directeur des relations-clients, Services bancaires commerciaux TD dès aujourd'hui pour vous renseigner sur les nombreux services qui peuvent vous aider à vous protéger contre la fraude.

Sécurité informatique

Protection de votre ordinateur personnel

Il existe de nombreuses façons de protéger vos renseignements personnels sur Internet.

- Assurez-vous de détenir une licence légale pour votre système d'exploitation et votre navigateur et téléchargez les mises à jour de sécurité et les versions de vos logiciels les plus récentes.
- N'oubliez pas de fermer votre session lorsque vous avez terminé vos opérations bancaires ou si vous laissez votre ordinateur sans surveillance.
- Protégez votre nom d'utilisateur, votre mot de passe et vos renseignements d'ouverture de session. Le Groupe Banque TD ne vous demandera jamais de fournir des renseignements personnels ou d'ouverture de session, comme votre nom d'utilisateur, votre mot de passe, votre NIP ou vos numéros de compte.
- Choisissez des mots de passe peu communs dont vous vous souviendrez et que vous n'aurez donc pas à prendre en note. Utilisez une combinaison de lettres et de chiffres afin d'en assurer une meilleure protection.
- N'utilisez pas de mots de passe faciles à deviner, comme une date d'anniversaire, un nom de famille ou un numéro de téléphone.
- Assurez-vous de désactiver la fonction de remplissage automatique ou toute autre fonction de mémorisation des mots de passe de votre navigateur.
- Il vaut mieux ne pas sauvegarder vos mots de passe dans votre ordinateur, Internet ou un logiciel, car toute personne qui obtiendrait ces renseignements serait en mesure d'usurper votre identité.
- Ne divulguez jamais vos mots de passe, particulièrement en ligne, même à la police, à

votre institution financière ou à votre fournisseur de service Internet.

- Protégez votre ordinateur contre les pirates informatiques et autres fraudeurs en installant un pare-feu.
- Passez en revue et appliquez les protocoles d'authentification associés à nos produits et services, notamment la séparation des tâches, les procédures d'autorisation et d'authentification ainsi que les droits d'administrateur.
- Utilisez toujours un système informatique autonome et verrouillé pour effectuer vos opérations bancaires.
- Restez au courant des mesures de sécurité de l'information et de prévention.
- Les logiciels antivirus et anti-logiciels espions sont conçus pour détecter et supprimer les virus et les programmes malveillants qui infectent votre ordinateur. Gardez toujours ces logiciels à jour.
- Effacez toujours la mémoire cache de votre navigateur après chaque utilisation de services bancaires en ligne. Vous supprimerez ainsi toutes les pages, les fichiers et les rapports que votre navigateur pourrait avoir sauvegardés temporairement sur votre disque dur.
- Les courriels ne sont pas un canal de communication sûr et peuvent facilement être interceptés, de la même manière que peuvent l'être vos conversations par téléphone cellulaire. Vous ne devriez donc jamais inclure de renseignements bancaires dans un courriel, qu'il nous soit destiné ou non. Seules des questions d'ordre général devraient être envoyées par courriel. Les renseignements personnels qui ne devraient pas être transmis par courriel comprennent, sans s'y limiter, les numéros de compte, les noms d'utilisateur et les mots de passe.

Hameçonnage

L'hameçonnage survient quand un fraudeur envoie des courriels d'apparence légitime qui semblent provenir de sociétés établies dans le but de « pêcher » des renseignements personnels et financiers. Ces courriels frauduleux amènent les destinataires à cliquer sur des liens qui les redirigent vers de faux sites Web. Ceux-ci sont conçus pour donner l'impression aux clients qu'ils se trouvent sur un site d'entreprise légitime. Sur le faux site, on demande à la personne d'entrer des renseignements personnels ou financiers qui serviront à commettre des fraudes.

Le Groupe Banque TD n'enverra jamais de courriels à ses clients pour leur demander des renseignements personnels, leur nom d'utilisateur, leur mot de passe ou leur NIP.

Comment éviter les fraudes par hameçonnage

Bien que les services en ligne soient une façon sûre d'effectuer ses opérations bancaires, en règle générale, vous devriez faire preuve de prudence lorsque vous transmettez des renseignements personnels ou financiers sur Internet.

- Méfiez-vous des courriels vous pressant de transmettre des renseignements personnels ou financiers. Les courriels d'hameçonnage contiennent le plus souvent des messages alarmants (mais faux) qui ont pour but de faire réagir immédiatement le destinataire. Ils vous demandent généralement des renseignements comme votre nom d'utilisateur et votre mot de passe.
- Les courriels d'hameçonnage NE sont habituellement PAS personnalisés, bien qu'ils peuvent parfois l'être. Les vrais messages de votre banque sont généralement personnalisés, mais n'hésitez pas à appeler votre institution financière si vous avez le moindre doute.
- Ne cliquez pas sur les liens que contiennent un courriel pour vous rendre à une page Web. Si vous doutez de l'authenticité du message ou si vous ne connaissez pas l'expéditeur, appelez-nous ou ouvrez une session sur notre site Web en saisissant l'adresse Web dans la barre d'adresse de votre navigateur.
- Prenez l'habitude de saisir vous-même l'adresse Web des institutions bancaires, des sites de magasinage ou d'encan ainsi que des sites d'opérations financières plutôt que d'utiliser les liens qui s'affichent automatiquement.

Pour en apprendre davantage sur la prévention de la fraude, veuillez communiquer avec votre directeur des relations-clients, Services bancaires commerciaux TD.

Pour en savoir plus sur les services de gestion de trésorerie ou trouver le Centre bancaire commercial TD de votre région, visitez le www.servicesbancairescommerciauxtd.com ou communiquez avec votre directeur des relations-clients, Services bancaires commerciaux TD.

web_591329 (0312)