Guide de prévention de la fraude

Terminaux de Solutions aux commerçants TD

AVIS
La Banque Toronto-Dominion se réserve le droit d'apporter des changements aux spécifications en tout temps, sans préavis. La Banque Toronto-Dominion décline toute responsabilité à l'égard de l'utilisation des renseignements fournis dans cette publication par les commerçants clients, notamment quant aux infractions aux droits de propriété intellectuelle ou aux autres droits de tiers résultant de cette utilisation.

Table des matières

Dans quelle mesure votre entreprise est-elle sûre?

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

Informations sur la fraude

- Près de la moitié des fraudes et des vols commis par les employés sont dus à des failles dans les contrôles internes[1].
- Plus de 80 % des entreprises ont signalé avoir été la cible de fraude sur les paiements en 2018[2].
- Bien que les chèques demeurent la source la plus fréquente de fraude sur les paiements, on observe une recrudescence de fraude du courriel d'entreprise compromis. Le pourcentage d'entreprises ciblées par de telles escroqueries est passé de 64 % en 2014 à 80 % en 2018[2].

Faites preuve de vigilance et protégez vos renseignements!

Ne communiquez à personne vos codes d'accès confidentiels. La TD ne vous demandera jamais de fournir des renseignements personnels ou des renseignements d'ouverture de session, comme un code d'accès, un mot de passe, un code de jeton d'authentification ou des numéros de compte, que ce soit par téléphone ou par courriel.

Formation des employés

Votre première ligne de défense, ce sont vos employés. Assurez-vous de les former à reconnaître les opérations ou les comportements suspects. Signalez immédiatement toute activité suspecte à Solutions aux commerçants TD au **1-800-363-1163**.

Comportement suspect

Il y a un certain nombre de comportements frauduleux courants que vous devez connaître :

- le nombre de fois où le NIP a été mal saisi;
- si la carte à puce est mal insérée et que l'appareil demande de glisser la carte;
- la nervosité;
- des produits achetés au hasard;
- l'achat d'un seul article important et coûteux.

Remarque : La liste ci-dessus n'est pas exhaustive. Votre vigilance et votre capacité à détecter les activités inhabituelles constituent également de solides outils de prévention de la fraude.

1 2018 Report to the Nations. Associations of Certified Fraud Examiners.

2 2019 AFP Payments Fraud and Control Survey, Association for Financial Professionals.

Sécurité du terminal

Vous êtes responsable de la sécurité de votre terminal. Nous vous recommandons fortement de :

- Garder votre terminal près de l'endroit où vous travaillez pendant les heures d'ouverture;
- Ranger votre terminal en lieu sûr et hors de vue lorsqu'il n'est pas utilisé (pendant et après les heures d'ouverture);
- Limiter l'accès de tiers à votre terminal (entrepreneurs ou personnel de livraison qui ont accès à votre entreprise); et
- Procéder à une inspection régulière de votre terminal pour vérifier s'il a été altéré.

Inspecter régulièrement votre terminal

Au cours de votre processus d'inspection, vous devez déterminer si les appareils ont été remplacés ou altérés. Pour déterminer si un appareil a été remplacé, vous devez recueillir les renseignements ci-dessous lorsque vous recevez votre terminal afin de les comparer aux éventuels nouveaux renseignements.

- Fabricant de l'appareil (sur l'avant de l'appareil)
- Marque et modèle du terminal (à l'arrière de l'appareil, sur l'étiquette)
- Numéro de série du terminal (à l'arrière de l'appareil, sur l'étiquette)

Nous vous avons fourni une liste de vérification (***Annexe A – Liste de vérification pour l'inspection des terminaux***) qui pourrait vous être utile lors de l'inspection de votre terminal. Si vous repérez des irrégularités, débranchez immédiatement le terminal en question et appelez le Centre de contact de Solutions aux commerçants TD au **1-800-363-1163** pour le signaler et recevoir des instructions sur les étapes à suivre.

Voici certains éléments à surveiller :

- Sceaux inviolables manquants/endommagés/altérés
- Vis manquantes/dépareillées
- Grille de clavier incorrecte
- Fils apparents à l'extérieur du terminal
- Trous percés/découpés dans le terminal
- Nouveaux étiquetages/recouvrements susceptibles de masquer une altération
- Un ***dispositif d'écrémage*** a été ajouté au terminal – les dispositifs d'écrémage sont utilisés par le personnel non autorisé qui tente d'obtenir les données du titulaire de carte avant de lire la carte

Sécurisez le réseau Wi-Fi de votre entreprise

Si vous utilisez un terminal qui fonctionne en Wi-Fi :

- **N'utilisez jamais un réseau Wi-Fi public ou non sécurisé!**
- Changez toujours le mot de passe par défaut fourni avec votre routeur/modem pour un mot de passe fort et complexe qui comprend des lettres, des chiffres et des caractères spéciaux.
- Ne donnez pas le mot de passe aux clients ou aux employés.
- Changez fréquemment votre mot de passe.
- Installez des pare-feu et des logiciels antivirus pour protéger votre réseau Wi-Fi.

Gestion des utilisateurs

En utilisant des types d'utilisateurs, vous pouvez renforcer la sécurité de votre terminal en limitant l'accès à certaines de ses fonctionnalités. Voici les types d'utilisateurs généralement disponibles.

- Administrateur (niveau le plus élevé)
- Directeur/superviseur; et
- Commis (niveau le moins élevé).

Rôle	Description
Administrateur[3]	• Peut accéder à toutes les fonctionnalités, y compris le traitement des opérations financières, les rapports et tous les menus. • Peut configurer des identifiants de directeur, de superviseur et de commis.
Directeur/ superviseur	• Certains terminaux ont un des deux rôles ou les deux (directeur/ superviseur) disponibles. • Peut accéder aux fonctionnalités et fonctions (y compris le traitement des opérations) tous les rapports et tous les menus. • Peut effectuer des opérations financières. • Peut configurer les identifiants de commis.
Commis	• Peut effectuer des opérations financières.

3 Le mot de de passe de l'administrateur correspond aussi au numéro d'accès au terminal.

Lorsqu'un employé quitte votre entreprise :

- Retirez immédiatement son nom d'utilisateur et son mot de passe de tous vos terminaux;
- Changez les mots de passe auxquels il a eu accès; et
- Supprimez tout accès aux comptes bancaires ou retirez ses droits de signataire autorisé.

Propriétaire de l'entreprise à titre d'administrateur

Ce rôle est créé lors de l'installation du terminal, car vous, le propriétaire de l'entreprise, devez avoir accès à tout ce qui se trouve sur le terminal pour exploiter votre entreprise.

Directeur adjoint à titre de directeur/ superviseur

Le directeur/superviseur joue votre rôle pour les activités quotidiennes.

Vous pouvez sélectionner les accès dont il disposera pour les fonctions sensibles du terminal.

Caissiers à titre de commis

Les commis aident les clients à effectuer des opérations financières pour votre entreprise.

Exemple

Vous êtes à la tête d'une entreprise de quatre employés : vous (le propriétaire de l'entreprise), un directeur adjoint et deux caissiers. Vous pouvez configurer les rôles comme suit :

Propriétaire de l'entreprise
Administrateur

Directeur adjoint
Directeur/superviseur

Caissiers
Commis

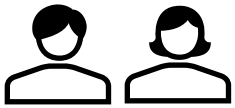
Protection des fonctionnalités du terminal

Il existe différentes façons de protéger votre terminal par un mot de passe, notamment en utilisant des mots de passe et la fonctionnalité du niveau d'utilisateur (administrateur, directeur/superviseur ou commis). Ces paramètres sont utiles pour bloquer des opérations/fonctionnalités spécifiques pour les utilisateurs généraux telles que la vente imposée, le règlement de fin de journée et les fonctions administratives sur le terminal.

Remarque : Vous devez appeler le Centre de contact de Solutions aux commerçants TD pour activer ces paramètres protégés.

Exemple

Il est préférable de partir des rôles d'utilisateurs les moins élevés pour décider des fonctionnalités que vous souhaitez leur accorder. En utilisant le même exemple d'entreprise :



Caissiers
Commis

Si les caissiers de votre entreprise n'effectuent que des ventes, vous pouvez appeler le Centre de contact de Solutions aux commerçants TD et protéger par mot de passe les remboursements, les annulations, les ventes imposées, etc. Comme vous avez protégé ces opérations par mot de passe, vous devez maintenant décider qui peut utiliser son mot de passe pour accéder à ces opérations.

Directeur adjoint
Directeur/superviseur

Si votre directeur adjoint vous représente lorsque vous n'êtes pas sur place, il devrait être autorisé à effectuer les opérations protégées par mot de passe.

S'il n'est responsable que de la gestion des utilisateurs (ajout, modification, suppression), il n'a pas besoin de cette fonctionnalité et la responsabilité vous incomberait en tant que propriétaire de l'entreprise/administrateur.

Pour savoir comment gérer les utilisateurs, consultez le ***Guide du commerçant*** en ligne ou le ***Guide de configuration et de dépannage***.

Quelle fonctionnalité puis-je protéger?

- Amorcer une vente, retour, annulation, vente imposée et saisir manuellement des opérations effectuées par carte de crédit
- Amorcer et effectuer des opérations préautorisées
- Exécuter un règlement/la fermeture de journée
- Réimprimer des reçus
- Imprimer des rapports
- Passer d'un mode semi-intégré à un mode autonome (terminaux semi-intégrés seulement)
- Accéder à divers menus

Comment est-elle protégée?

- La fonctionnalité du terminal est protégée par le type d'utilisateur (administrateur, directeur/superviseur ou commis), et non par le code d'utilisateur.
- Pour utiliser une fonctionnalité protégée, l'utilisateur doit ouvrir une session avec son code d'utilisateur. Si le niveau de son type d'utilisateur est insuffisant, l'accès lui sera refusé.

Registre des activités

Certains terminaux disposent d'un registre des activités qui affiche/imprime un rapport de toutes les activités protégées auxquelles on a accédé sur le terminal. Le rapport recueille le code d'utilisateur associé à la fonctionnalité protégée par un mot de passe qui a été exécutée.

Seul l'administrateur a accès à ce rapport.

Pour savoir comment récupérer le registre des activités, consultez le ***Guide du commerçant*** en ligne ou le ***Guide de configuration et de dépannage*** de votre terminal.

Sécurité des opérations

Quel que soit votre type d'entreprise, vous n'êtes pas à l'abri d'opérations frauduleuses. Il est possible de reconnaître ce risque et de le réduire. Bien qu'il n'y ait aucune solution précise pour éliminer la fraude, voici quelques conseils pour vous aider à la prévenir.

Opérations avec présentation de la carte

- L'utilisation de la technologie des cartes à puce (p. ex. opération par carte à puce et NIP, sans contact) pour traiter les opérations avec présentation de la carte est l'un des moyens les plus efficaces pour protéger votre entreprise contre des pertes.
- Saisir manuellement les renseignements d'une carte de crédit dans un terminal en présence du titulaire de la carte augmente considérablement le risque d'opérations frauduleuses et de subir des pertes liées aux débits compensatoires. Pour plus de renseignements, consultez Risques liés à la saisie manuelle des renseignements sur les cartes de crédit.
- Les commerçants sont responsables de l'entretien et du contrôle de leurs terminaux en tout temps. Il faut notamment être présent pendant que le client utilise l'appareil. Les fraudeurs tenteront d'effectuer des opérations frauduleuses de différentes façons. Voici les méthodes couramment utilisées :
    - Endommager la bande magnétique de la carte de crédit et insérer la carte incorrectement pour forcer la saisie manuelle de l'opération.
    - Modifier le mode d'acceptation initialement programmé par le commerçant (p. ex. passer d'une opération par carte à puce et NIP à la saisie manuelle), ce qui expose les commerçants à des fraudes potentielles et à des débits compensatoires.

Les opérations saisies manuellement présentent un risque élevé de fraude

Si vous saisissez manuellement une opération par carte de crédit qui est considérée comme frauduleuse, vous serez responsable de tout débit compensatoire qui pourrait en résulter. Les opérations par carte de crédit saisies manuellement comprennent les opérations relatives à des commandes postales ou téléphoniques.

Vérifications de carte

Assurez-vous de former les 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) https://www.pcisecuritystandards.org/lang/fr-fr/.

Que dois-je vérifier?

- Vérifier que la carte est signée.
- Si une signature est requise pour le reçu, vérifier que la signature correspond à celle figurant au dos de la carte.
- Vérifier que la date d'expiration n'est pas dépassée.
- N'oubliez pas : Seulement **vous** pouvez saisir manuellement les renseignements de la carte sur le terminal.

Les vérifications ci-dessus n'éliminent pas le risque de fraude.

Opérations par carte de crédit saisies manuellement

Si vous êtes mal à l'aise à l'idée d'effectuer une vente imposée, vous avez le droit, en tant que propriétaire d'entreprise, de demander un autre mode de paiement (débit, espèces, etc.).

Si vous traitez une opération par carte de crédit saisie manuellement, consultez les vérifications de carte à la page précédente. Ces opérations peuvent être protégées par un mot de passe pour s'assurer qu'elles ne sont pas effectuées par des employés non autorisés.

Pour en savoir plus, consultez la section ***Protection des fonctionnalités du terminal***.

Les opérations saisies manuellement présentent un risque élevé de fraude

Si vous saisissez manuellement une opération par carte de crédit qui est considérée comme frauduleuse, vous serez responsable de tout débit compensatoire qui pourrait en résulter. Les opérations par carte de crédit saisies manuellement comprennent les opérations relatives à des commandes postales ou téléphoniques.

Vente/opérations imposée

La fonctionnalité Vente/opérations imposée permet de saisir manuellement les numéros d'autorisation antérieurs. Pour votre protection, cette fonctionnalité est désactivée par défaut sur votre terminal.

Si vous souhaitez effectuer une vente imposée, communiquez avec le Centre de contact de Solutions aux commerçants TD au **1-800-363-1163** pour activer la fonctionnalité après la vérification de votre identité. Nous vous recommandons vivement de protéger la fonctionnalité de vente imposée par un mot de passe.

Pour en savoir plus, consultez la section Protection des fonctionnalités du terminal.

Remboursements (crédit et débit)

Si vous avez peur que des remboursements inappropriés soient effectués (que ce soit en raison d'erreurs, d'une fraude commise par un employé, etc.), nous vous recommandons d'ajouter un mot de passe de superviseur à ces opérations.

Pour faire ajouter un mot de passe de superviseur aux opérations de remboursement, veuillez communiquer avec le Centre de contact de SCTD au **1-800-363-1163**.

Pour en savoir plus, consultez la section ***Protection des fonctionnalités du terminal***.

Opérations sans présentation de la carte

- La saisie du code de vérification de la carte (CVC) est obligatoire pour les opérations sans présentation de la carte. Le CVC est le code de sécurité à trois ou quatre chiffres figurant au verso de la carte de crédit.
- Le Service de vérification d'adresse est un outil offert aux commerçants en ligne pour faciliter la détection des opérations douteuses effectuées par carte de crédit et comparer l'adresse de facturation soumise par l'acheteur à l'adresse de facturation du titulaire de carte au dossier de la banque émettrice.

Les vérifications du Service de vérification d'adresse **n'éliminent pas** le risque de fraude.

Appel pour autorisation

Parfois, en raison d'un problème de communication ou de sécurité, une opération ne peut pas ou ne doit pas être traitée. Vous trouverez ci-dessous la liste des messages et des événements qui vous obligeront à appeler pour demander une autorisation.

Quand...

- vous effectuez une vente ou une opération de préautorisation imposée.

  OU

- le numéro de carte à l'écran ne correspond pas au numéro en relief sur la carte.

  OU

- la signature du titulaire de carte sur le reçu ne correspond pas à celle figurant au dos de la carte.

OU

- vous doutez de la validité d'une carte ou d'une opération.

Vous devez...

1. Appeler immédiatement pour obtenir une autorisation vocale.
2. Demander une autorisation CODE 10. Dans cette situation, il se peut que la carte soit frauduleuse et un CODE 10 en alertera l'institution financière.

Les autorisations **n'éliminent pas** le risque de fraude. Si vous saisissez manuellement une opération par carte de crédit qui est considérée comme frauduleuse, vous serez responsable de tout débit compensatoire qui pourrait en résulter.

Conserver les reçus du titulaire de carte

Il incombe aux commerçants de conserver tous les reçus pour répondre aux questions des titulaires de carte, comme les contestations ou les débits compensatoires. Voici les directives de conservation pour en assurer l'intégrité. Veuillez conserver vos reçus :

- ***Dans un endroit sombre, frais et sûr pendant au moins 18 mois***
- ***Tant que vous conservez les bandes de caisse pour les opérations de paiement direct***
    - Si la TD a besoin d'une copie du reçu, veuillez l'envoyer dans les huit (8) jours et en conserver une copie pour vos dossiers.
    - Ces délais de conservation et de réponse requis sont ceux de Solutions aux commerçants TD uniquement et peuvent varier selon l'institution financière.
    - Vos reçus pourraient devenir illisibles s'ils sont conservés dans des contenants enduits de plastique ou exposés à des sources directes de chaleur ou de froid.
- ***Classez les reçus dans des enveloppes, disposées par date, dans un classeur sécurisé/verrouillé.***
- Si vous avez plusieurs terminaux, utilisez une enveloppe différente pour chacun d'entre eux.

Renseignements sur le titulaire de carte

Les fraudeurs peuvent utiliser des reçus pour assembler les renseignements de la carte.

Cela comprend également tous les rapports que vous pouvez imprimer avec les renseignements sur le titulaire de carte. Ils doivent être conservés en lieu sûr ou détruits.

Norme de sécurité de l'industrie des cartes de paiement (PCI DSS)

Les mesures de cette norme sont conçues pour vous aider à prévenir le vol de données confidentielles des titulaires de cartes en évaluant la sécurité de ces données au sein de votre entreprise et, si nécessaire, en améliorant votre niveau de sécurité pour respecter ou dépasser les normes du secteur.

La norme PCI DSS exige de toute organisation qui recueille, traite, transmet ou stocke les données des titulaires de carte qu'elle respecte et maintienne les normes de sécurité des données établies par le secteur des paiements dans le monde entier et gérées par le Conseil des normes de sécurité des données de l'industrie des cartes de paiement.

Tous les commerçants gérant les données des titulaires de carte doivent se conformer à cette norme et aux programmes de conformité des réseaux de cartes de paiement. Ceux qui ne s'y conforment pas peuvent être soumis à des amendes, frais ou cotisations et/ou à la cessation de leurs services de traitement.

Pour en savoir plus, consultez les sites https://www.td.com/ca/fr/entreprises/comment-faire/solutions-aux-commercants/norme-de-securite-pci et https://www.pcisecuritystandards.org/lang/fr-fr/.

Annexe A – Liste de vérification pour l'inspection des terminaux

Imprimez cette liste de vérification pour chaque terminal et inspectez-les pour vous assurer qu'ils n'ont pas été altérés.[4]

Date de l'inspection : _____

Fabricant de l'appareil : _____ (sur l'avant du terminal)

Marque et modèle : _____ (à l'arrière du terminal, sur l'étiquette)

Numéro de série : _____ (à l'arrière du terminal, sur l'étiquette)

Votre terminal comporte-t-il l'un des éléments suivants?

Condition	Oui	Non
Sceaux inviolables manquants, endommagés ou altérés	☐	☐
Vis manquantes ou dépareillées	☐	☐
Touches dépareillées	☐	☐
Grille de clavier incorrecte	☐	☐
Fils apparents à l'extérieur du terminal	☐	☐
Trous percés ou découpés dans le terminal	☐	☐
Ajout de nouveaux étiquetages/recouvrements susceptibles de masquer une altération	☐	☐
Un ***dispositif d'écrémage*** a été ajouté au terminal[5]	☐	☐
Quelque chose qui n'est pas abordé dans les points ci-dessus et qui semble inhabituel ou inapproprié	☐	☐

Si vous avez coché Oui à l'une des cases ci-dessus :

- Débranchez immédiatement le terminal en question; et
- Appelez le Centre de contact de Solutions aux commerçants TD au **1-800-363-1163** pour le signaler et recevoir des instructions sur les étapes à suivre.

4 Nous vous recommandons fortement d'inspecter vos terminaux attentivement et fréquemment.

5 Les dispositifs d'écrémage sont utilisés par le personnel non autorisé qui tente d'obtenir les données du titulaire de carte avant de lire la carte. Les dispositifs d'écrémage peuvent être insérés dans le lecteur de bande magnétique ou le lecteur de puce, ou superposés sur l'appareil lui-même.

Annexe B – Conseils de prévention de la fraude informatique

- Installez un pare-feu pour protéger votre ordinateur.
- 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 d'entreprise.
- Assurez-vous de désactiver la fonctionnalité de saisie automatique du mot de passe de votre navigateur.
- N'enregistrez jamais vos mots de passe sur votre ordinateur, dans Internet ou dans un logiciel.

Annexe C – Conseils de prévention de la fraude par 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.
- N'utilisez pas de liens dans un courriel pour accéder à une page Web. Si vous soupçonnez que le message n'est pas authentique, appelez pour le vérifier ou entrez l'adresse 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 de jeton 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 (SBIE), veuillez communiquer avec le Centre de soutien des Services de gestion de trésorerie au 1-800-567-4455.
    - Pour BanqueNet, appelez 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.

Coordonnées

Veuillez communiquer avec le Centre de contact de Solutions aux commerçants TD au 1-800-363-1163. Nous serons heureux de répondre à toutes vos questions.

Authorisation :

24 heures sur 24, 7 jours sur 7

Demandes de terminal :

24 heures sur 24, 7 jours sur 7

Questions générales des commerçants :

Du lundi au vendredi, de 8 h à 20 h (HE)

Fournitures d'imprimantes et rouleaux de papier :

Du lundi au vendredi, de 8 h à 17 h (HE)

Centre de ressources

Ce guide contient les renseignements les plus importants pour commencer à utiliser votre appareil. Votre terminal dispose de fonctionnalités et de fonctions supplémentaires présentées dans notre portail de documentation à l'adresse www.solutionsauxcommercantstd.com/centrederessources.

Resource Centre