

Contact

Idées d'affaires pour les clients des Services aux commerçants TD

Cinq excellentes raisons de penser à la sécurité des données

Selon les spécialistes, les Canadiens utilisent leurs cartes de crédit presque autant que le comptant¹.

Plus ils le font, plus les données sur leur compte seront utilisées et potentiellement stockées.

Dans le dernier numéro de *Contact*, nous avons expliqué comment le programme Sécurité de l'information concernant les comptes (SIC) de Visa Canada vous aide à prévenir le vol de ces renseignements confidentiels.

Le programme SIC exige des commerçants qu'ils se conforment à la Norme de sécurité des données de l'industrie des cartes de paiement (ICP) à l'échelle internationale (pour obtenir une liste détaillée de ces exigences et des critères de conformité, visitez le site www.visa.ca/sic). La protection des données comporte d'importants avantages pour votre entreprise.

Dans ce numéro

2 / Requinquez vos affaires

- Conseils pour la protection des données

3 / Gérez votre entreprise

- Dernières nouvelles sur la carte à puce
- Des changements dans

l'industrie des cartes de paiement

4 / Prévention des fraudes

- Aide-mémoire pour la prévention des fraudes
- Préparez-vous : voici MasterCard
- Besoin de papier?

REQUINQUEZ VOS AFFAIRES



1. Accroître le sentiment de confiance chez le consommateur

Bien des consommateurs recherchent un détaillant de confiance et ont tendance à lui rester fidèle, en plus de le recommander à leurs connaissances. Dans une

étude commanditée par Visa en 2006 et s'étendant sur douze pays, les répondants ont classé la sécurité des renseignements personnels et financiers au premier rang de leurs préoccupations. Ils ont également laissé entendre que les pratiques des détaillants, dans ce domaine, pouvaient les inciter à se procurer des biens ou des services chez eux.

Si vous respectez les normes du secteur, vous démontrez aux clients votre engagement à protéger leurs données de paiement. C'est un moyen essentiel d'obtenir leur confiance et de la renforcer.

Suite à la page 2

5 excellentes raisons de penser à la sécurité des données

Suite de la page 1

2. Mettre la sécurité en vedette

Le principal objectif du programme SIC et de la Norme de l'ICP en matière de sécurité des données consiste à protéger les renseignements confidentiels en tout point du système de paiement. Il en résulte une meilleure prise de conscience qui vous incitera à renforcer vos mesures afin de contrer toute attaque éventuelle.

3. Prévenir les dépenses inutiles

Une solide politique de sécurité des données vous aidera à prévenir les infractions à la sécurité qui pourraient

coûter cher à votre entreprise, en termes de réputation et de bénéfices.

Une atteinte à la protection des données en raison de lacunes dans les pratiques de sécurité risque d'engendrer pour l'entreprise des frais importants : vérifications, litiges et amendes, sans compter une exploitation sensiblement compromise.

La mise en application de normes efficaces prévient toutes ces dépenses et protégera votre bonne réputation.

4. Conserver une image positive

Faire l'effort de respecter la Norme de l'ICP en matière de sécurité des données vous aidera considérablement à préserver votre réputation auprès

des consommateurs et des médias, car le public accorde de plus en plus d'importance à la protection des données personnelles.

5. Obtenir un avantage concurrentiel

Une excellente politique de sécurité des données peut vous aider à acquérir une réputation de détaillant honnête et fiable. Si vos clients savent que vous protégerez les données confidentielles associées à leur compte, ils reviendront vous voir, votre chiffre d'affaires augmentera, et vous vous démarquerez de vos concurrents.

Pour en savoir plus sur la protection du compte de vos clients, visitez le site www.visa.ca/sic ■

Conseils pour la protection des données

Il est normal que l'on désire conserver les données personnelles de sa clientèle à l'abri des pirates informatiques. Voici quelques conseils à ce sujet, qui vous aideront à protéger les renseignements confidentiels de vos clients et votre entreprise :

- Ne conservez que le nécessaire en matière de données sur les titulaires de carte et ne sauvegardez jamais le contenu de la bande magnétique d'une carte de débit ou de crédit.
- Détruisez les données de compte dont vous n'avez plus besoin selon la méthode reconnue. Ne sauvegardez jamais le CVV, le CVV2 ou le NIP.
- Certains logiciels enregistrent automatiquement les données. Examinez les vôtres et actualisez vos préférences pour éviter que des données sur les comptes soient sauvegardées sans avertissement.
- Faites les vérifications de sécurité associées aux normes ICP (pour en savoir plus, consultez le site www.pcisecuritystandards.org).
- Utilisez des pare-feu efficaces.
- Changez les mots de passe de système et les codes de sécurité fournis à l'origine par le concepteur de logiciels.
- Chiffrez toutes les données relatives aux cartes de paiement qui sont enregistrées dans les systèmes de l'entreprise de traitement.
- Chiffrez toutes les données sur les cartes, qui vous sont transmises par Internet ou par un autre réseau public ouvert.
- Activez votre logiciel antivirus et obtenez toutes les mises à niveau.
- Assurez la protection des autres logiciels, notamment les systèmes d'exploitation, et obtenez les plus récentes versions.
- Ne donnez accès aux données sur les clients qu'aux employés qui en ont besoin. Assurez-vous que chaque employé utilisant un ordinateur possède son propre code d'accès.
- Contrôlez l'accès aux données de carte de paiement sur support papier.
- Mettez vos systèmes de sécurité à l'épreuve régulièrement.
- Adoptez une politique de sécurité décrivant clairement les règles que doivent respecter les employés qui ont accès aux données et renforcez-la régulièrement.
- Exigez que tous les tiers ayant accès aux données sur les titulaires de carte se conforment aux exigences de sécurité de l'ICP.



Dernières nouvelles sur la carte à puce

Les membres de l'industrie canadienne des paiements – soit Visa Canada Corporation, MasterCard Canada, Inc. et l'Association Interac – travaillent de concert pour étendre la technologie de la carte à puce au marché canadien dans les prochaines années.

C'est pourquoi ils ont lancé à l'automne 2007 un projet pilote d'un an comportant le lancement de cartes de débit et de crédit dotées d'une puce dans un marché regroupant 200 000 consommateurs de la région de Kitchener-Waterloo. On a confié à des détaillants locaux 2 300 terminaux de point de vente compatibles, et les guichets automatiques bancaires ont été mis à niveau dans une proportion de 65 %.

« Les commerçants et les consommateurs ont beaucoup à gagner du passage à la technologie de la carte à puce, a déclaré Tracey Black, directrice du projet. Les cartes à puces et leurs terminaux renforcent encore davantage la sécurité d'un système de paiement. »

Résultats positifs. Une enquête réalisée récemment auprès de 200 commerçants et employés de première ligne ayant participé au projet pilote a donné des résultats positifs, par exemple :

- **Mémoire du NIP.** La plupart des répondants ont constaté que les clients, dans une proportion variant entre 70 % et 80 %, se souvenaient de leur NIP au moment d'effectuer une opération sur carte de crédit à puce.
- **Convivialité des messages-guides dans les terminaux.** La plupart des commerçants et des employés de première ligne ont déclaré que les messages des terminaux conçus pour guider les titulaires de carte lors d'une opération étaient faciles à lire et intelligibles et qu'ils ne causaient guère de difficultés pour l'essentiel de la clientèle.
- **Appui à une amélioration de la sécurité.** Les clients ont exprimé une

opinion positive; les titulaires de carte sont heureux de constater que le recours à un NIP (plutôt qu'à une signature) avait pour effet d'accroître la sécurité.

- **Aucun effet sur le temps nécessaire.** Les répondants, dans une mesure pouvant atteindre 88 %, ont constaté que l'utilisation d'une carte à puce plutôt qu'une autre carte prenait le même temps ou moins à la caisse.

Modification du processus de paiement. La plupart des détaillants ont affirmé n'avoir guère d'expérience des opérations effectuées à l'aide des cartes à puce et des NIP, où la carte doit rester dans le terminal pendant qu'on entre le NIP et que l'opération se termine.

En effet, dans une opération avec carte

à puce, le client insère sa carte dans le terminal, qui affiche alors le montant de l'achat et demande l'entrée du NIP. Après confirmation de ce dernier, l'achat est approuvé et le reçu est imprimé. Quand l'opération est terminée, un message invite le client à retirer sa carte.

« Toutes les cartes à puce conserveront une piste magnétique au verso, » a ajouté M^{me} Black, afin que les commerçants équipés d'un terminal PDV compatible uniquement avec ce type de carte puissent recevoir des paiements comme d'habitude.

Dans nos prochains numéros, nous vous tiendrons au courant des événements entourant la conversion à la carte à puce; visitez également le site www.tdcanadatrust.com/francais/merchant ■

Des changements dans l'industrie des cartes de paiement

À la nouvelle carte à puce (voir l'article précédent) s'ajoute toute une série de mesures de promotion de la sécurité dans l'industrie de traitement des cartes de paiement. Voici un avant-goût de deux autres de ces améliorations.

Cartes de paiement sans contact

Les nouvelles cartes sans contact – comme la solution de paiement payWave* de Visa – offrent à la fois les avantages de la technologie de la carte à puce sur le plan de la sécurité et la commodité d'un paiement sans l'insertion de la carte et sans l'entrée du NIP. C'est une technique idéale pour les opérations en service express et d'un montant peu élevé, comme dans les cafés, les cinémas et les kiosques à journaux.

Le titulaire de la carte n'a qu'à passer sa carte – qui est dotée d'une antenne et d'un microcircuit – devant un lecteur sans contact, et le paiement se fait rapidement et sans risque.

Révision de la Norme de sécurité des données de l'ICP

En octobre, le PCI Security Standards Council (conseil de normalisation pour la sécurité des données de l'ICP) diffusera la version 1.2 de la Norme de l'ICP (voir notre premier article). Les douze exigences de base actuelles de la Norme de l'ICP en matière de sécurité des données resteront en vigueur, mais la nouvelle version en donnera une description plus claire et la rendra plus facile à appliquer. La version 1.2 :

- expliquera plus en détail les exigences techniques de la Norme de l'ICP;
- décrira plus précisément la manière de soumettre des rapports sur la sécurité;
- recommandera de nouvelles pratiques exemplaires;
- comprendra une rubrique traitant du processus de sécurité, avec une liste de questions et de réponses et un glossaire.

Aide-mémoire sur la prévention des fraudes

Le temps des Fêtes approche à grand pas; compte tenu du regain d'activité qui l'accompagne, le moment est bien choisi pour revoir les méthodes de prévention des fraudes avec votre personnel de première ligne. Votre entreprise pourra certainement profiter des conseils suivants pendant cette période de pointe.

Adoption des pratiques exemplaires

Lors du traitement d'opérations sur carte de crédit, obtenez toujours les autorisations appropriées et vérifiez les aspects suivants :

- La signature au bas du reçu doit toujours correspondre à celle qui figure au verso de la carte.
- Le code à quatre caractères apparaissant sous le numéro imprimé en relief doit être identique aux quatre premiers caractères de celui-ci.
- L'hologramme en forme de colombe doit être en trois dimensions, et non pas un dessin sans perspective.
- La date d'expiration ne doit pas être passée.

Si l'opération est entrée manuellement, assurez-vous d'obtenir une impression claire et lisible de la carte *Visa* du client sur toutes les copies de la facture. Si votre terminal électronique ne permet pas de glisser une carte, entrez les données de l'opération manuellement. Faites une impression manuelle de la carte, en vous assurant que la plaque du commerçant est fixée à la presse à carte. Veillez aussi à ce que tous les renseignements pertinents (signature du client, date, numéro d'autorisation, montant, etc.) figurent sur la facture, en cas de litige.

Tendances en matière de fraude

Les experts des Services aux commerçants TD constatent une hausse des cas de fraude lors d'opérations par téléphone, par la poste et par Internet; ils recommandent la plus grande prudence lorsque la carte n'est pas présentée.

- Si les adresses de livraison et de facturation sont différentes, demandez au client de vous donner un numéro de téléphone à composer le jour et un autre pour le soir. Vérifiez ces numéros dans l'annuaire ou sur le site www.canada411.ca, puis rappelez le client pour confirmer la commande.
- Si le client doit passer prendre les articles, demandez-lui de présenter sa carte *Visa* et glissez-la dans le lecteur (ou faites une impression manuelle), puis priez-le de signer la facture.
- Si la commande a été faite par Internet, songez à utiliser *Vérifié par Visa**, un service en ligne qui permet d'authentifier l'identité d'un client à l'aide d'un mot de passe. Pour en savoir plus, visitez www.visa.ca/fr/merchant/products/vbv/

Rappelez-vous que le numéro d'autorisation confirme uniquement la présence des fonds nécessaires; il ne constitue pas un assentiment du titulaire de la carte à l'égard de l'opération, ni ne prévient les débits compensatoires.

Indices à surveiller

Voici quelques comportements inhabituels méritant une surveillance :

- Des achats considérables (surtout s'ils sont faits par téléphone, par télécopieur ou par Internet);

- Achat de plusieurs modèles différents d'un produit très coûteux, surtout avec une carte de crédit nouvellement validée;
- Client insistant pour apporter avec lui un article de grande valeur (un téléviseur, une chaîne stéréo, etc.), même si la livraison est comprise dans le prix.

Le site www.tdcanadatrust.com/francais/merchant contient des précisions supplémentaires sur la prévention de la fraude dans les entreprises; vous pouvez également consulter le Centre d'assistance des Services aux commerçants, en composant le 1-800-363-1163, pour demander un exemplaire de notre dépliant sur la prévention de la fraude par carte de crédit. ■

Préparez-vous : voici MasterCard

Nous pouvons vous aider dans votre préparation à l'acceptation de la carte MasterCard^{MD}. Commencez en communiquant avec First Data, en composant le 1-866-306-7847 ou en envoyant un courriel à merchantservicescanada@firstdata.com

Besoin de papier?

Les entreprises suivantes sont les fournisseurs de papier privilégiés pour les terminaux point de vente des Services aux commerçants TD.

- MainTech Industries, 1-800-268-5120
- Maxwell Media Products, 1-800-561-6406
- Papier Parfait Inc., 1-877-745-5163

Le bulletin *Contact* est publié périodiquement par les Services aux commerçants TD. Tous les efforts ont été faits pour que l'information contenue dans le présent bulletin soit exacte. Cependant, les Services aux commerçants TD n'assument aucune responsabilité quant aux erreurs ou aux omissions que comporterait cette information ou quant aux pertes découlant de ces erreurs ou omissions.

Pour obtenir plus d'information, vous pouvez nous écrire à Bulletin Contact, Service du marketing des Services aux commerçants TD,

100 Wellington St. W., 29th Floor, Canadian Pacific Tower, Toronto (Ontario) M5K 1A2, nous téléphoner sans frais au 1-800-363-1163 ou consulter le site www.tdcanadatrust.com/francais/merchant

1. Interac Association 2007.



Sources Mixtes
Cert no. SW-COC-001700
© 1996 FSC

* Visa International Service Association/Utilisée sous licence.
^{MD} Marque déposée de MasterCard International Incorporated.
© 2008 La Banque Toronto-Dominion. Tous droits réservés.



Services aux Commerçants