Protéger son clavier NIP, c'est protéger ses clients

puceInterac.ca

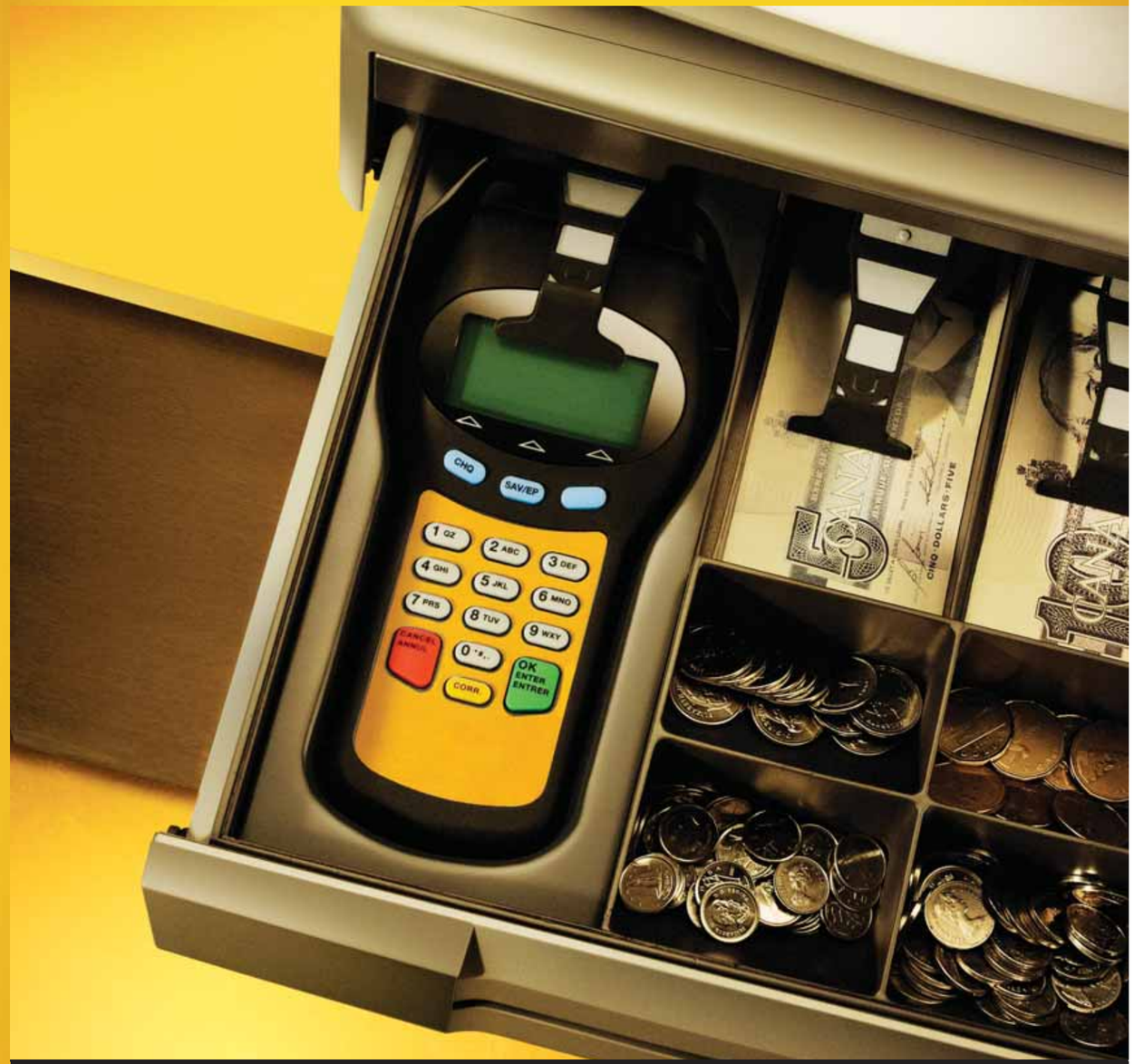
Migration à la technologie de la carte à puce

Au cours des prochaines années, les cartes de débit, les guichets automatiques et les dispositifs aux points de vente vont passer à la technologie de la carte à puce, une nouvelle génération de carte de paiement qui rend le système de paiement encore plus sécuritaire. Une puce informatique est désormais intégrée aux nouvelles cartes de débit, ce qui leur confère la puissance d'un ordinateur. Elles peuvent ainsi emmagasiner et traiter des données ainsi que communiquer avec le guichet ou le dispositif de point de vente, ce qui augmente leur niveau de sécurité. Pour en savoir plus, consultez le site www.puceinterac.ca.

Tous les jours, tout simplement.MC

À propos de l'Association Interac

L'Association Interac est responsable de la conception et de l'exploitation du réseau national de paiement par carte de débit, qui permet aux Canadiens d'avoir accès à leur argent aux guichets automatiques et aux terminaux de point de vente partout au pays. Pour en savoir plus, consultez le site www.interac.ca.



Prévention de la fraude par carte de débit

Chaque jour, des millions de Canadiens règlent leurs achats au moyen du service Paiement direct *Interac*. Les Canadiens figurent même parmi les plus grands utilisateurs mondiaux de la carte de débit, et le service Paiement direct *Interac* est le mode de paiement préféré d'un Canadien sur deux.

Bien que le réseau *Interac* soit l'un des systèmes les plus sécuritaires du monde, la fraude par carte de débit, aussi connue sous le nom de « clonage », peut se produire.

Qu'est-ce que la fraude par carte de débit ?

La fraude par carte de débit est le transfert non autorisé des données de la bande magnétique d'une carte à celle d'une carte contrefaite. Elle permet de retirer les fonds d'un compte bancaire à l'insu de son titulaire. Pour contrefaire une carte, les fraudeurs ont besoin de deux types de données : les données enregistrées sur la bande magnétique, et le NIP.

Techniques de fraude par carte de débit

1 Clonage

Pour recueillir le NIP et les données enregistrées sur la bande magnétique à l'insu du titulaire de la carte, le fraudeur utilise de l'équipement clandestin, comme des lecteurs de cartes et des minicaméras installées à des guichets automatiques ou à des points de vente. Les renseignements ainsi obtenus sont ensuite utilisés pour contrefaire une carte qui, avec le NIP approprié, permet de retirer de l'argent du compte bancaire du titulaire.

Ce qu'il faut rechercher :

- Petits orifices dans les plafonds, les cloisons, les plaques et les affiches.
- Fils dont la fonction est inconnue et lecteur de cartes supplémentaire.

2 Claviers NIP trafiqués

Les fraudeurs remplacent les claviers NIP par des modèles identiques mais frauduleux pour que personne ne constate leur absence; ils en modifient les composantes et les replacent à leurs points de vente d'origine. Ils peuvent alors télécharger par réseau sans fil les données stockées sur la bande magnétique des cartes de débit et le NIP quand leur titulaire s'en sert.

Ce qu'il faut rechercher :

- Un fraudeur distrait l'employé en poste en achetant des produits de grande taille ou en détournant son attention pendant que son complice a le clavier NIP en main.
- Pièces ou sceaux de sécurité brisés.

Caméra clandestine dans le plafond pouvant filmer, par un orifice, les clients qui entrent leur NIP.

Les dispositifs utilisés pour le clonage des cartes sont très petits, donc facilement portables.

Fraudeur utilisant des rouleaux de papier hygiénique et un bristol pour cacher son complice qui échange un clavier NIP.

Sceau de sécurité brisé.

Chacun peut contribuer à prévenir la fraude

La fraude nous touche tous, y compris les commerçants. Si la sécurité de l'information des cartes de débit de vos clients est compromise ou si un clavier NIP est volé dans votre commerce, votre marque ou vos ventes peuvent en souffrir. La valeur de la marque que votre entreprise a mis du temps à bâtir peut être rapidement détruite, la réaction des médias et du public étant habituellement rapide et négative.

Bien qu'*Interac*, les institutions financières et les organismes d'application de la loi collaborent pour assurer la sécurité des services *Interac*, les commerçants ont aussi un rôle primordial à jouer dans la lutte contre la fraude, ne serait-ce qu'en inspectant régulièrement l'espace adjacent aux caisses et aux terminaux.

Comment empêcher la fraude par carte de débit dans votre établissement :

1 Votre clavier NIP est aussi précieux que de l'argent

Pour un fraudeur, un clavier NIP est comme de l'argent comptant.

- Rangez vos claviers NIP hors de vue lorsqu'ils ne servent pas.
- Mettez votre terminal sous clé durant les heures de fermeture s'il n'est pas intégré à la caisse.

2 Faites une inspection quotidienne

Les fraudeurs utilisent plusieurs techniques pour installer des dispositifs clandestins dans un commerce. L'inspection régulière des lieux est une pratique exemplaire qui vous permet de détecter immédiatement les appareils douteux et de prévenir d'éventuelles activités frauduleuses.

- Vérifiez le numéro de série de votre clavier NIP pour vous assurer que celui-ci n'a pas été volé.
- Examinez l'espace adjacent à la caisse pour y déceler des fils dont la fonction est inconnue ou d'éventuelles caméras cachées derrière les panneaux du plafond, les murs ou les affiches.
- Recherchez les indices de contrefaçon : pièces et sceaux de sécurité brisés, autocollants ajoutés, dos du clavier NIP semblant être une pièce neuve, etc.

3 Renseignez-vous sur vos employés et collègues

Un processus d'embauche qui suit des procédures strictes est une étape importante pour prévenir la fraude. Dans certains cas, un fraudeur peut se faire embaucher par votre entreprise si des mesures de vérification des antécédents ne sont pas en place. Dans d'autres cas, un fraudeur peut payer ou menacer un de vos employés pour qu'il commette des actes illégaux, comme installer de l'équipement clandestin.

- Demandez une pièce d'identité avec photo émise par un gouvernement.
- Prenez une photo de chaque employé à son embauche et gardez-en une copie.
- Vérifiez les antécédents de chaque nouvel employé.

Que faire dans des circonstances suspectes ou si votre clavier NIP ou terminal de point de vente se fait voler ?

- Ne dérangez rien sur la scène d'un éventuel crime.
- Ne touchez pas aux appareils concernés.
- Avertissez sur-le-champ la police ou votre fournisseur de service de paiement.
- Coopérez avec les enquêteurs ou la police en leur permettant d'inspecter les lieux; fournissez-leur les horaires de travail, les renseignements sur les employés et les enregistrements des caméras de surveillance.

Pour en savoir plus sur la prévention de la fraude, écrivez à l'Association Interac, à dcfprevention@interac.ca ou communiquez avec votre fournisseur de services de paiement.