

Freiner la fraude à la source.

Protégez votre clavier NIP,
protégez vos clients





Protéger votre commerce contre la fraude par carte de débit.

Techniques de fraude par carte de débit

Les pertes subies en raison de la fraude par clonage des cartes de débit *Interac* ont baissé au taux le plus faible jamais enregistré, passant de 142 millions de dollars en 2009 à 16,2 millions de dollars en 2014. En 2014, seulement 20 % des pertes, ou 3,2 millions de dollars, sont liés à l'exploitation frauduleuse au Canada. Grâce à la combinaison de saines politiques, à des investissements en technologie, ainsi qu'à une collaboration remarquable avec les institutions financières, les acquéreurs ou fournisseurs de services de paiement, les commerçants et les corps policiers, le système *Interac* est un réseau de paiement de calibre mondial.

Même si les statistiques témoignent clairement du succès du système *Interac* en ce qui a trait à la réduction de la fraude par carte de débit *Interac*, il est important que les commerçants connaissent les méthodes que les malfaiteurs utilisent pour mener des activités frauduleuses par carte de paiement pour éviter que leur commerce en soit victime.

Clonage de bande magnétique

Pour recueillir le NIP et les données enregistrées sur la bande magnétique à l'insu du titulaire de la carte, le criminel 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 de débit à bande magnétique qui, avec le NIP approprié, permet de retirer de l'argent du compte bancaire du titulaire par l'entremise des guichets automatiques et des appareils aux points de vente dépourvus de la technologie à puce.

Claviers NIP trafiqués

Les malfaiteurs volent les claviers NIP, les trafiquent et les replacent aux points de vente. Ils peuvent ainsi récupérer les données stockées sur la bande magnétique et le NIP des cartes de débit quand leur titulaire s'en sert. Les malfaiteurs remplacent les claviers NIP par des modèles identiques, mais frauduleux, pour que le commerçant ne remarque pas l'absence des claviers originaux; 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 carte.

Restez à l'affût



- Un malfaiteur peut distraire un 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.
- Les malfaiteurs tenteront aussi de trafiquer les appareils laissés sans surveillance sur le comptoir.

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 que l'Association 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.

Votre clavier NIP est aussi précieux que de l'argent



Pour un criminel, 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.

Ce que vous devriez faire



Si un malfaiteur vous aborde et vous demande de l'aider à installer un appareil trafiqué ou de fermer les yeux sur cette installation :

- refusez poliment et informez-le que vous ne participerez pas à ses activités illégales;
- recueillez autant d'information sur lui que possible (comme une description physique, le véhicule qu'il conduisait ou sa plaque d'immatriculation);
- avertissez sur-le-champ la police et votre acquéreur ou fournisseur de services de paiement;
- ne vous mettez pas en danger.

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 criminel peut se faire embaucher par votre entreprise si des mesures de vérification des antécédents ne sont pas en place. Dans d'autres cas, un malfaiteur peut payer ou menacer un de vos employés pour qu'il commette des actes illégaux, comme installer de l'équipement clandestin. Voici des mesures que vous pouvez prendre à ce sujet.

- 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.

Quoi 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 et votre acquéreur ou fournisseur de services 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.

L'Association Interac peut vous aider



- Une vidéo de formation se trouve à l'adresse interac.ca/videofraude.
- Sceaux de sécurité – Communiquez avec votre acquéreur ou fournisseur de services de paiement pour commander des sceaux de sécurité GRATUITS.
- La liste de vérification de l'intégrité du point de vente se trouve à l'adresse <http://www.interac.ca/fr/securite/tools-resources-fr>.

Pour en savoir plus, veuillez communiquer avec nous en envoyant un courriel à dcfprevention@interac.ca.

Interac et le logo *Interac* sont des marques déposées d'Interac Inc., utilisées sous licence.

