

# Prévention de la fraude par carte et par chèque



Les entreprises de toute taille peuvent être la cible de fraude par carte. Apprenez à reconnaître les différents types de fraudes afin de protéger votre entreprise et vous-même contre les fraudeurs.

## LA FRAUDE PAR CARTE

Chaque fois qu'une personne utilise votre carte de crédit ou le numéro de votre carte sans votre autorisation, elle commet une fraude par carte. Voici cinq des types de fraudes les plus courants :

1

### **Contrefaçon :**

Des criminels obtiennent les numéros de cartes de crédit par le biais de terminaux piratés ou du vol de données. Ils utilisent les numéros volés pour **créer de fausses cartes de crédit et s'en servir** comme si elles étaient vraies.

2

### **Arnaque et utilisation inappropriée :**

Un criminel gagne la confiance de sa victime en lui envoyant un courriel qui semble légitime, puis il obtient les renseignements de la carte de crédit de cette personne.

3

### **Carte perdue ou volée**

Un fraudeur utilise une **carte perdue ou volée** pour effectuer des achats.

4

### **Prise de contrôle d'un compte :**

Un criminel **prend le contrôle d'un compte** et l'utilise pour réaliser ses achats.

5

### **Opération sans carte :**

Un fraudeur **se sert du numéro d'une carte de crédit pour effectuer des achats** en ligne, par téléphone ou par la poste.

## PROTÉGER VOTRE ENTREPRISE DE LA FRAUDE PAR CARTE

### Nos mesures de protection :

- **Surveillance de vos opérations par carte** en ligne et en personne.
- **Examen de tous les achats** effectués au moyen de votre carte à un terminal.
- **Détection d'activités qui semblent suspectes**, par exemple, un achat particulièrement dispendieux ou plusieurs achats effectués dans un court laps de temps.
- **Possibilité de refuser les opérations** particulièrement suspectes.
- **Émission de nouvelles cartes** quand vous en avez besoin.

## LES MESURES À PRENDRE POUR VOUS PROTÉGER

### Surveillez l'utilisation de vos cartes

- **Vérifiez quotidiennement vos opérations par carte de crédit.** Si vous remarquez quelque chose d'inhabituel, appelez-nous immédiatement.
- **Établissez une alerte sur vos comptes de carte de crédit** pour recevoir un avis lorsque vos cartes sont utilisées.
- **Choisissez l'option sans papier pour recevoir des relevés électroniques** afin de protéger les renseignements sur vos comptes.

### Protégez vos cartes

- **Ne laissez jamais vos cartes de crédit sans surveillance.**
- **Ne divulguez jamais votre NIP** à qui que ce soit et n'en gardez jamais une note près de votre carte.
- **Ne fournissez jamais de renseignements confidentiels** par téléphone ni par courriel. Rappelez-vous que la Banque Scotia ne vous contactera jamais par téléphone ni par courriel pour obtenir les numéros de votre carte de crédit ou votre mot de passe.
- **Apposez votre signature au verso de toute nouvelle carte de crédit**, dès que vous la recevez.
- Si l'une de vos opérations est refusée ou si votre carte est perdue ou volée, **appelez-nous immédiatement** pour réduire le risque de fraude.
- Lorsqu'une carte de crédit n'est plus valide, **détruisez-la en la découpant en petits morceaux.**

VOUS AIMERIEZ EN SAVOIR PLUS?

### Protégez-vous contre les escroqueries

Obtenez plus d'information sur la fraude par courriel et par téléphone.

### Pensez cybersécurité

Découvrez comment améliorer la cybersécurité à la maison et au travail.

### Centre antifraude du Canada

Restez au fait des derniers types de fraudes pour éviter d'en être victime.

## LA FRAUDE PAR CHÈQUE

La personne qui utilise illégalement un chèque pour obtenir des fonds commet une fraude par chèque. Il existe trois types de fraudes par chèque.

- 1 Contrefaçon :**  
Un chèque qui semble être authentique, mais qui est faux.
- 2 Falsification :**  
Le fraudeur change le montant du chèque, le nom du bénéficiaire ou les deux.
- 3 Endossement frauduleux/bénéficiaire visé non payé :**  
Le criminel imite la signature du signataire ou endosse le chèque sans autorisation.

## PROTÉGEZ VOTRE ENTREPRISE DE LA FRAUDE PAR CHÈQUE

### Nos mesures de protection

La Banque Scotia offre trois [services de détection des fraudes](#) : *Relevé des effets payés*, *Rapprochement et Rapprochement des bénéficiaires*. Ces services permettent :

- **de repérer les chèques** qui n'ont pas été émis par votre entreprise;
- **de détecter des changements** apportés au nom du bénéficiaire, au montant ou au numéro de série d'un chèque;
- **d'obtenir des images des chèques** compensés dans le compte.

### LES MESURES À PRENDRE POUR VOUS PROTÉGER

- **Vérifiez** les opérations et les retraits de votre compte quotidiennement.
- Si un chèque est manquant, **appelez la Banque** pour qu'elle bloque le paiement.
- **Mettez sous clé vos chèques** et tout matériel servant à émettre des chèques.
- **Restreignez l'accès aux chèques et au matériel connexe.** Seuls les employés autorisés devraient avoir accès aux chèques et pouvoir les traiter et les poster.
- **Séparez les tâches.** L'employé qui émet les chèques ne doit pas être celui qui en fait le rapprochement