

# PROTÉGEZ VOS OPÉRATIONS FINANCIÈRES



Caisses populaires  
acadiennes

*plus haut, plus loin, ensemble*



[www.acadie.com](http://www.acadie.com)

C'est une série de moyens pour renforcer la sécurité de vos opérations financières.



En mettant en place des mesures simples à appliquer pour réduire les fraudes. En freinant les fraudeurs pour limiter les victimes. En prenant plus de précautions. Et moins de risques. Renforcer votre sécurité en ligne, c'est agir ensemble dans un même but : protéger vos avoirs et vos données. Voilà pourquoi nous vous recommandons quelques consignes et mesures de sécurité à suivre. Voilà pourquoi vous devriez les appliquer. Parce que nous faisons tout en notre pouvoir pour vous protéger. Parce que vous aussi, vous avez le pouvoir et la responsabilité de vous protéger.

# TABLE DES MATIÈRES

<b>Les Caisses populaires acadiennes prennent les grands moyens .....</b>	<b>4</b>
<b>Carte La Populaire .....</b>	<b>5</b>
ABC de la sécurité lorsque vous utilisez votre carte.....	5
<b>Au guichet automatique et chez les marchands .....</b>	<b>6</b>
Les fraudeurs convoitent votre NIP... et vos avoirs.....	6
Comment vous protéger? .....	6
Mesures à prendre pour vous assurer une protection accrue.....	7
<b>AccèsD Internet: pour une sécurité optimale .....</b>	<b>8</b>
Comment les fraudeurs s’y prennent-ils?.....	8
Vos moyens de défense .....	8
Les Caisses populaires acadiennes contre-attaquent.....	9
<b>Courriel frauduleux.....</b>	<b>11</b>
Les escrocs se modernisent eux aussi .....	11
Ne mordez pas à l’hameçon .....	12
<b>Sollicitation par téléphone .....</b>	<b>13</b>
Le cas classique.....	13
Vos meilleures armes .....	13
<b>Ressources importantes .....</b>	<b>14</b>

## LES CAISSES POPULAIRES ACADIENNES PRENNENT LES GRANDS MOYENS

Nous ne négligeons aucun effort pour vous assurer sécurité et confidentialité lors de vos opérations, que ce soit à votre caisse, au guichet automatique, par Internet ou chez les marchands lorsque vous utilisez le paiement direct.

Nos services transactionnels en ligne répondent aux plus hauts standards de sécurité de l'industrie financière et sont conformes à la Loi sur la protection des renseignements personnels et des documents électroniques. Des technologies solides et éprouvées ont été mises à contribution pour que vos données soient protégées advenant altération, perte ou accès non autorisé.

Aussi robuste soit-il, tout système de protection exige de l'utilisateur un minimum de comportements sécuritaires pour que les mesures en place donnent leur plein bénéfice. Les consignes à suivre sont le plus souvent simples et peu exigeantes. Il suffit d'en être informé comme vous le serez en parcourant les quelques pages qui suivent. Vous y apprendrez notamment comment éviter que des fraudeurs se fassent passer pour vous auprès de marchands, de votre Caisse et d'autres institutions financières.

**En tant que membre de l'Association Interac, les Caisses populaires acadiennes participent aux mesures de sensibilisation visant la protection du NIP associé aux cartes de débit. D'où les nouvelles étiquettes portant la mention « Protégez votre NIP ».**

# CARTE LA POPULAIRE

## ABC de la sécurité lorsque vous utilisez votre Carte La Populaire

Les règles de base à respecter pour protéger votre argent sont des plus simples :

- 1) Ne prêtez votre Carte La Populaire à personne.
- 2) Si votre carte est perdue, volée ou retenue par un guichet automatique, avisez immédiatement votre caisse ou le Centre d'assistance au 1 800 361-5121.
- 3) Vérifiez régulièrement vos relevés et vos soldes pour vous assurer que toutes les transactions ont bien été faites par vous. Si vous y voyez des écritures frauduleuses, communiquez rapidement avec votre caisse ou le Centre d'assistance au 1 800 361-5121.
- 4) Ne révélez jamais ni votre NIP (numéro d'identification personnel pour utilisation au guichet automatique et aux terminaux de paiement direct) ni vos mots de passe (vos codes d'entrée pour vos transactions AccèsD Internet) à qui que ce soit. **Aucune institution financière, aucun agent de police, aucun représentant de Desjardins ou de votre Caisse populaire acadienne, ni aucun commerçant n'est autorisé à vous demander votre NIP ou vos mots de passe AccèsD. Ces derniers n'appartiennent qu'à vous.**
- 5) N'utilisez pas de NIP ou de mot de passe faciles à découvrir comme votre adresse, votre numéro de téléphone ou votre date de naissance.
- 6) Mémorisez votre NIP et vos mots de passe; ne les écrivez nulle part, surtout pas sur votre carte.
- 7) Soyez discret: cachez le clavier avec la main ou le corps lorsque vous composez votre NIP.

- 8)** Ne composez pas votre NIP une seconde fois sans d'abord vérifier l'annulation et avoir obtenu le relevé de cette opération.
- 9)** Ne perdez jamais votre carte de vue durant une transaction.
- 10)** Récupérez votre carte et le relevé à la fin de la transaction.
- 11)** Changez votre NIP et vos mots de passe immédiatement si vous soupçonnez qu'on vous a observé lors de la composition.

## AU GUICHET AUTOMATIQUE ET CHEZ LES MARCHANDS

### Les fraudeurs convoitent votre NIP... et vos avoirs.

Les grands fraudeurs ne manquent ni de culot, ni d'imagination. Comment s'y prennent-ils ?

Le clonage de carte peut se faire dans un guichet automatique ou directement chez le marchand par un employé malveillant lors d'une transaction. Le fraudeur tente ensuite de subtiliser votre NIP lorsque vous le saisissez sur le clavier numérique.

### Comment vous protéger ?

Les trois meilleures protections contre le clonage de votre Carte La Populaire sont simples :

- Protégez votre NIP en suivant les règles de base énoncées plus haut.
- Ne perdez jamais votre carte de vue pendant une transaction.
- Récupérez votre carte et votre relevé après chaque transaction.

## Mesures à prendre pour vous assurer une protection accrue

Pour réduire les sommes qui pourraient être retirées frauduleusement de votre compte, les solutions suivantes ont été mises en place :

- Le montant total pour vos retraits effectués auprès **d'autres institutions financières au Canada** est fixé par défaut à **300 \$ CAN\* par jour**. Pour des retraits additionnels, vous pouvez vous rendre à un guichet des Caisses populaires acadiennes\*\*.
- Le montant total pour vos retraits effectués auprès **d'autres institutions financières hors Canada** est fixé par défaut à **500 \$ CAN\* par jour**.
- La limite d'achat par **paiement direct** (incluant les retraits) chez les marchands est fixée par défaut à **1 000 \$ CAN\* par jour**.
- Vous devrez, lors de certaines opérations – retrait, dépôt, virement – au guichet automatique, confirmer votre identité en entrant le jour et le mois de votre date de naissance.

Pour obtenir un complément d'information sur ces limites, contactez directement votre caisse.

**NE DIVULGUEZ JAMAIS VOTRE NIP,  
MÊME À UN EMPLOYÉ DES CAISSES  
POPULAIRES ACADIENNES.**

\* Peut être changé sans préavis.

\*\* À moins d'une entente contraire avec votre caisse.

# ACCÈSD INTERNET : POUR UNE SÉCURITÉ OPTIMALE

Lorsque vous utilisez AccèsD Internet, vous naviguez en sécurité. Nos services transactionnels et nos formulaires de demande en ligne répondent aux plus hauts standards de sécurité. Demeurez vigilant. Malgré ces précautions, l'utilisateur pourrait créer une faille dans le système de sécurité en ayant omis de compléter les actions nécessaires pour sécuriser son poste. Voici quelques conseils pour encore mieux vous prémunir contre les principaux attaquants qui s'intéressent trop aux renseignements confidentiels vous concernant et qui convoitent vos avoirs.

## Comment s'y prennent-ils ?

Les fraudeurs utilisent différents moyens pour vous soutirer des renseignements confidentiels :

- Courriel ou site frauduleux affichant un faux logo ou un visuel d'une entreprise de confiance ou avec laquelle vous faites déjà affaire.
- Échanges dans un forum de discussion.
- Virus informatique et logiciel espion.
- Attaque de pirates informatiques.

Les données recueillies sur la victime peuvent être des mots de passe, des numéros de cartes de crédit ou de débit, le numéro d'assurance sociale, la date de naissance et des renseignements personnels. Ces renseignements sont alors vendus à des criminels ou utilisés pour accéder entre autres à des comptes de crédit, de chèques ou d'épargne.

## Vos moyens de défense

Voici les mesures à prendre pour réduire les risques de devenir une victime des fraudeurs sur Internet :

- N'utilisez jamais les fonctions de saisie automatique et de mémorisation des mots de passe disponibles dans les navigateurs.
- Changez de mot de passe régulièrement – tous les mois et IMMÉDIATEMENT si vous soupçonnez que quelqu'un le connaît.

- Équipez votre ordinateur d'un logiciel antivirus, d'un logiciel anti-espion et d'un pare-feu reconnus, et tenez-les à jour.
- Assurez-vous de voir le sceau de sécurité à l'écran (cadenas fermé) et de **taper manuellement l'adresse du site d'AccèsD** (<https://accesd.acadie.com>).
- Quittez bien votre session en cliquant sur **Quitter** en haut de l'écran et fermez le navigateur; vous détruisez alors toutes les copies des pages Internet emmagasinées sur votre disque dur et prévenez ainsi toute intrusion inopportune ou accidentelle dans vos comptes.
- Videz la mémoire cache (voir [www.acadie.com](http://www.acadie.com) pour en savoir plus) et évitez d'utiliser un poste public ou partagé.
- Lorsque vous devez vous débarrasser de documents contenant des informations personnelles et confidentielles, comme vos relevés de comptes ou vos relevés de carte de crédit, assurez-vous de bien détruire vos documents.

## Les Caisses populaires acadiennes contre-attaquent

Les Caisses populaires acadiennes font appel aux technologies les plus avancées pour assurer votre sécurité sur AccèsD Internet :

- Chiffrement des transactions  
Toutes les opérations effectuées dans nos services transactionnels en ligne sont chiffrées selon les meilleures pratiques du marché afin d'assurer la confidentialité pendant la circulation entre notre site sécurisé et le navigateur de votre micro-ordinateur ou de votre appareil mobile. C'est pourquoi l'utilisateur d'AccèsD ne peut accéder à ce service qu'avec les versions les plus récentes des navigateurs qui acceptent le protocole de sécurité SSL.2.0 à 128 bits (Netscape - 4.6 et plus, sauf Netscape - 6.0, Microsoft Explorer - 5.0 et plus, et Safari).  
SSL signifie Secure Sockets Layer soit « couches de connexion protégées ». Ce protocole permet le chiffrement des données échangées et garantit l'identité de nos serveurs. Il fait en sorte que les données échangées ne peuvent être visualisées que par des personnes autorisées.

- Sécurité des transactions en ligne

Les transactions que vous effectuez électroniquement avec le réseau des Caisses populaires acadiennes sont hébergées sur nos serveurs. Elles sont donc sécurisées et aucune des informations qui y sont contenues ne peut être interceptée par une tierce personne.

- Sceau de sécurité

Assurez-vous de toujours naviguer dans un environnement sécuritaire lorsque vous transmettez des renseignements confidentiels. Si vous n'apercevez pas le sceau de sécurité à l'écran (cadenas fermé), ou si vous apercevez un sceau brisé (cadenas ouvert), la sécurité de la transmission de votre transaction par Internet n'est pas garantie; une tierce partie pourrait alors l'intercepter.

L'emplacement du sceau de sécurité diffère selon le navigateur utilisé. Visitez le [www.acadie.com](http://www.acadie.com) pour en savoir plus.

Une fois le cadenas localisé, cliquez sur ce dernier pour obtenir à l'écran le certificat attestant la sécurité du site. Vous devez pouvoir y lire le nom du propriétaire du site (pour AccèsD : <https://accesd.acadie.com>) ainsi que la période de validité du certificat.

- Numéro de confirmation

Un numéro de confirmation est émis après chaque transaction, ce qui confirme que votre opération a été effectuée et que votre demande a bien été reçue.

- Enregistrement automatique de toutes les transactions

Toutes les transactions que vous effectuez dans AccèsD Internet sont enregistrées et se retrouvent sur votre relevé de compte. Vous pouvez ainsi garder un œil sur les activités passées à votre compte.

**NE DIVULGUEZ JAMAIS VOS MOTS DE PASSE ACCÈSD À QUI QUE CE SOIT, MÊME À UN AGENT DE POLICE.**

# COURRIEL FRAUDULEUX

## Les escrocs se modernisent eux aussi...

Les fraudeurs ont vite compris la puissance du courriel. C'est même devenu la tactique préférée pour inciter des internautes à dévoiler des renseignements personnels et confidentiels.

Le courriel frauduleux, qui a l'apparence d'un courriel légitime, vous suggère d'abord de cliquer sur un lien ou sur une pièce jointe pour l'une ou l'autre de ces raisons. Par exemple :

- Changement ou mise à jour des renseignements personnels
- Concours
- Suspension possible de la carte client ou du compte
- Formulaire de demande d'un produit ou d'un service
- Expiration du compte

Après avoir accepté cette invitation, l'utilisateur est ensuite dirigé sur un faux site Web où on lui demande des renseignements tels que :

- Numéro de carte de guichet
- Mot de passe
- Numéro de compte
- Numéro d'identification personnel (NIP)
- Numéro d'assurance sociale
- Autres renseignements personnels ou confidentiels
- Date de naissance

## Ne mordez pas à l'hameçon

- Ne divulguez jamais vos numéros d'identification personnels (NIP), mots de passe AccèsD, numéro d'assurance sociale, date de naissance ou tout autre renseignement personnel lié ou non à votre dossier AccèsD.
- Pour accéder au service AccèsD, tapez manuellement l'adresse de notre site (<https://accesd.acadie.com>) dans votre fureteur.  
**Ne cliquez jamais sur un lien contenu dans un courriel.**

**RAPPEL : VOS MOTS DE PASSE ET VOS NUMÉROS D'IDENTIFICATION PERSONNELS VOUS APPARTIENNENT, NE LES DIVULGUEZ À PERSONNE.**

# SOLLICITATION PAR TÉLÉPHONE

Lorsqu'on vous sollicite par téléphone, soyez aux aguets et méfiez-vous des gens qui se disent représentants d'une entreprise avec qui vous faites affaire ou d'un organisme connu que vous estimez ou appuyez.

Il se peut très bien qu'un agent de télécommercialisation de Desjardins communique un jour avec vous pour vous faire profiter des avantages de l'un de nos produits. Suivez les recommandations ci-dessous pour rester aux aguets et pour ne laisser aucune chance aux fraudeurs

## Le cas classique

Les fraudeurs par téléphone maîtrisent l'art de se faire passer pour quelqu'un d'autre. Certains poussent l'audace jusqu'à utiliser le numéro de téléphone d'une entreprise de confiance sur l'afficheur ! Ils évoquent une urgence financière, un concours gagné par la victime ou des données manquantes à son dossier pour lui soutirer des renseignements personnels. Munis de ces informations, ils tenteront et réussiront bien souvent quelque escroquerie.

## Vos meilleures armes

- En aucun temps l'agent ne vous demandera de divulguer votre numéro d'identification personnel (NIP), vos mots de passe AccèsD (Internet) ou d'autres renseignements personnels tels que votre date de naissance et votre numéro d'assurance sociale.

**Petit rappel :** aucune institution financière, aucun agent de police, aucun représentant de Desjardins ni aucun commerçant n'est autorisé à vous demander votre NIP ou vos mots de passe AccèsD.

Dans le doute, contactez le Centre d'appel antifraude du Canada au 1 888 495-8501 ou visitez le [www.phonebusters.com](http://www.phonebusters.com).

## RESSOURCES IMPORTANTES

- Le Centre d'assistance au Canada, 1 800 361-5121 et à l'extérieur du Canada, appels à frais virés au (514) 281-9289
- Le Bureau de la concurrence, 1 800 348-5358, [www.bc-cb.gc.ca](http://www.bc-cb.gc.ca)
- GRC – Signalement en direct des délits économiques, 1 888 495-8501, [www.recol.ca](http://www.recol.ca)
- Le Centre d'appel antifraude du Canada, 1 888 495-8501, [www.phonebusters.com](http://www.phonebusters.com)

Ces bureaux de crédit et autres organisations inscriront un indicateur de fraude à votre dossier :

- Equifax : 1 800 465-7166
- TransUnion : 1 877 525-3823
- Les autorités policières locales, les sociétés émettrices de cartes de crédit, les banques et les archives provinciales.



si...

Vous perdez votre Carte  
La Populaire...

Vous êtes victime de vol d'identité  
ou de fraude...

Vous êtes victime d'un cas  
d'hameçonnage...

**Appelez sans tarder votre caisse  
ou le Centre d'assistance au  
Canada : 1 800 361-5121,  
à l'extérieur du Canada à frais  
virés : (514) 281-9289.**

N'oubliez pas: les fraudeurs se  
montrent souvent bien gentils  
et s'empressent de créer des liens  
de confiance. Soyez vigilant.



**Protégez votre NIP**



**Caisses populaires  
acadiennes**

*plus haut, plus loin, ensemble*