Trousse pour nouveaux arrivants

Fraude

Feuilles de travail

Ottawa Community Loan Fund • Fonds d'emprunt Communautaire d'Ottawa
22 O'Meara St., Causeway Work Centre, Ottawa, ON K1Y 4N6 Tel: 613-594-3535 Fax: 613-594-8118
www.oclf.org

Table des matières

Fraude

Frauder c'est mentir ou voler pour obtenir de l'argent.
Les fraudeurs vous mentiront pour que vous leur donnez ou envoyez de l'argent.
Ils peuvent voler vos renseignements personnels pour prendre votre argent.

Il y a plusieurs types de fraudes.
Certaines arrivent lorsque l'on vous fait croire un mensonge.
Certaines arrivent sans que vous ayez rien fait.

Les fraudeurs inventent pleins de choses pour vous tromper.
Ils sont habituellement polis et amicaux.
Ils insisteront jusqu'à ce que vous disiez oui.

Le vol d'identité

Le vol d'identité arrive quand quelqu'un d'autre se fait passer pour vous.

Le voleur d'identité peut aller chercher un prêt, faire un retrait de votre compte de banque ou faire demande pour une carte de crédit en utilisant votre nom.
Il utilise vos renseignements comme votre numéro d'assurance sociale (NAS) ou votre numéro de carte de crédit pour se faire passer pour vous.
Plusieurs années peuvent être nécessaires pour rebâtir votre historique de crédit si vous êtes victime d'un vol d'identité.

Habituellement, les voleurs d'identité obtiennent leurs renseignements directement de vous.
A l'aide de mensonges ou de pratiques trompeuses, ils réussissent à obtenir votre numéro de carte de crédit et sa date d'expiration, votre numéro de compte bancaire, vos mots de passe ou votre NAS.
Ils se font passer pour votre banque, le gouvernement, un magasin, un site d'enchères en ligne comme eBay ou votre compagnie de carte de crédit.
Si vous êtes à la recherche d'un emploi, ils peuvent se faire passer pour un employeur.

Les voleurs d'identité peuvent cacher leur vrai numéro de téléphone et se faire passer pour un représentant d'une vraie compagnie ou d'un bureau du gouvernement.
Le numéro qui apparaît à l'afficheur semble vrai.
Ils peuvent vous appeler ou laisser un message (**l'hameçonnage vocal** ou « vishing »).
Ils vous demanderont vos renseignements personnels ou d'utiliser votre téléphone pour entrer votre NAS, votre numéro de carte de crédit ou votre numéro d'identification personnel (NIP).
Ils peuvent vous envoyer une lettre ou un courriel (**l'hameçonnage par courriel** ou *phishing*).
Ils peuvent fonctionner avec un faux site web qui ressemble beaucoup à un vrai site.
Ils peuvent mettre une annonce dans le journal ou un site web.

Un courriel d'un voleur d'identité peut proposer un lien.
Lorsque vous cliquez sur le lien, vous serez dirigé vers un autre site web qui vous demande des renseignements personnels.
Il peut y avoir une invitation à signaler un numéro de téléphone.
Souvent, ces faux courriels vous disent que votre compte sera fermé ou que quelqu'un tente de se servir de votre compte.
Ils peuvent vous promettre un remboursement ou de l'argent si vous répondez.
Ils font souvent des fautes d'orthographes.
Les logos peuvent sembler étranges.

Les voleurs d'identité prennent vos lettres de votre boîte aux lettres comme votre relevé de carte de crédit ou des nouveaux chèques envoyés par votre banque.
Ils peuvent prendre des papiers comme des offres de crédit « pré-approuvé » dans votre recyclage.
Ils peuvent voler votre sac à main ou votre portefeuille.
Ceci arrive fréquemment dans les milieux de travail, dans les foules ou dans les moyens de transports publics.
Ils utilisent parfois une glaneuse, une machine électronique qui relève les renseignements personnels de votre carte de crédit lorsque vous l'utilisez au restaurant ou au guichet automatique, par exemple.
Ils utilisent les renseignements pour faire une fausse carte de crédit.
Ils vous surveillent pour saisir votre NIP.

Ils peuvent changer votre adresse avec vos créditeurs ou services publiques pour avoir de l'information sur vous.
Ils peuvent se faire passer pour vous et vendre votre maison ou prendre une hypothèque sur votre maison ou une autre propriété (titre acquis par déchéance ou par fraude).

Protégez votre identité

Vous pouvez protéger votre identité.

Gardez le nombre de documents avec vos renseignements personnels au minimum dans votre sac à main ou votre portefeuille.
Ne gardez pas sur vous les cartes de crédit supplémentaires, votre carte NAS, votre certificat de naissance ou votre passeport à moins d'en avoir besoin ce jour là.
Gardez-les dans un endroit sécuritaire.
Donnez votre NAS seulement quand c'est nécessaire.
Offrez d'autres sources d'identification si vous le pouvez.

NIP

N'utilisez pas des numéros qui sont faciles à deviner pour votre NIP.
N'écrivez pas votre NIP.
Changez votre NIP et vos mots de passe souvent.
Utilisez votre main ou votre corps pour cacher les numéros quand vous entrez votre NIP au guichet automatique, lorsque vous utilisez le paiement direct ou une carte d'interurbain.
Si vous pensez que quelqu'un connaît votre PIN, changez-le.

Cartes de débit ou de crédit

Signez votre nouvelle carte à l'endos dès que vous la recevez.
Lorsque vous utilisez votre carte de débit ou de crédit, regardez la personne qui fait la transaction.
Assurez-vous que la carte que l'on vous remet est bien la vôtre.
Les fraudeurs peuvent garder votre carte et vous en remettre une fausse.
Lorsque vous voyagez, gardez vos cartes avec vous ou dans le coffre-fort de l'hôtel.

Reçus et relevés

Prenez toujours les relevés de vos cartes de crédit ou de guichet automatique.
Mettez-les dans votre sac à main ou portefeuille.
Ne les mettez pas dans vos sacs où ils peuvent tomber facilement.

Vérifiez bien vos relevés de banque et de carte de crédit à chaque mois.
Si vous voyez des transactions dont vous ne vous souvenez pas, avertissez la compagnie de carte de crédit ou la banque immédiatement.

Vérifiez votre dossier de crédit chez Equifax et TransUnion au moins une fois par an.
Examinez votre dossier pour voir si quelqu'un a demandé de le vérifier **sans votre permission**.

Déchiquetage

Avant de jeter à la poubelle les documents qui contiennent des renseignements personnels tels que votre signature, votre nom et adresse, les relevés, les reçus, les factures des services publics, les demandes de cartes de crédit, et les formulaires d'assurance, déchiquetez-les (détruisez le papier en le déchirant en petits morceaux).
Lorsque vous recevez un nouveau document qui contient des renseignements personnels (comme un permis de conduire ou l'immatriculation de votre automobile) déchiquetez l'ancien.
Si vos factures n'arrivent pas au moment habituel, communiquez avec la compagnie pour vous assurer qu'elle a la bonne adresse.

Appels téléphoniques

Ne donnez pas de renseignements personnels au téléphone.
Dites à celui qui vous appelle que vous voulez vérifier le numéro et que vous allez rappeler.
Donnez seulement ces renseignements si vous composez **vous-même** le numéro de téléphone qui apparaît sur votre facture, à l'endos de votre carte bancaire ou de votre carte de crédit ou dans le bottin de téléphone.

Si la banque, le gouvernement ou une compagnie de carte de crédit vous téléphonent, ils devraient connaître votre nom, votre NAS et les renseignements sur votre compte.
Ils ne demanderont **jamais** votre NAS, numéro de compte, mot de passe, NIP, numéro de carte de crédit, la date d'expiration ou le code de sécurité à l'endos de votre carte de crédit.
Ils vous demanderont peut-être des questions pour s'assurer que vous êtes bien leur client.

En ligne

Soyez prudent lorsque vous faites des achats en ligne.
Achetez de magasins que vous connaissez et à qui vous pouvez faire confiance.

Assurez-vous de voir le symbole du cadenas ou de la clé au bas de l'écran. Un cadenas ouvert ou une clé brisée indiquent que d'autres personnes sur internet ont accès à vos renseignements personnels.
Après avoir donné vos renseignements personnels, assurez-vous de bien fermer votre session, d'effacer votre cache navigateur et de fermer votre fenêtre de navigateur.
Installez des logiciels anti-pourriel et antivirus et un pare-feu informatique sur votre ordinateur.
Assurez-vous de faire vos mise-à-jour.

Soyez prudent lorsque vous ouvrez un courriel avec une pièce jointe ou que vous téléchargez un dossier ou un programme en ligne.
N'envoyez pas de courriel avec vos renseignements personnels ou financiers.
D'autres personnes peuvent avoir accès à vos courriels.
Ne donnez pas vos renseignements personnels à un lien contenu dans un courriel.

Poste

Si vous partez pour quelques jours, demandez à un voisin de ramasser votre poste.
Si vous ne connaissez pas personne, vous pouvez aussi demander au bureau de poste de retenir votre poste. Vous devrez payer pour ce service.

Identifiez la fraude

Voici deux exemples de courriels frauduleux qui prétendent être de la Banque nationale du Canada.
Les courriels ressemblent à des vrais courriels de la Banque nationale.
Comment pouvez-vous savoir que ce sont des courriels frauduleux?

BANQUE NATIONALE DU CANADA

Cher(e) membre Bank National. Vous avez gagner 5000$ dans le concour de bank national.

Pour dŏposer votre prix , veuillez cliquez sur ce lien sécurisé si dessus :

https://bvi.bnc.ca/index/bnc/indexfr.html/

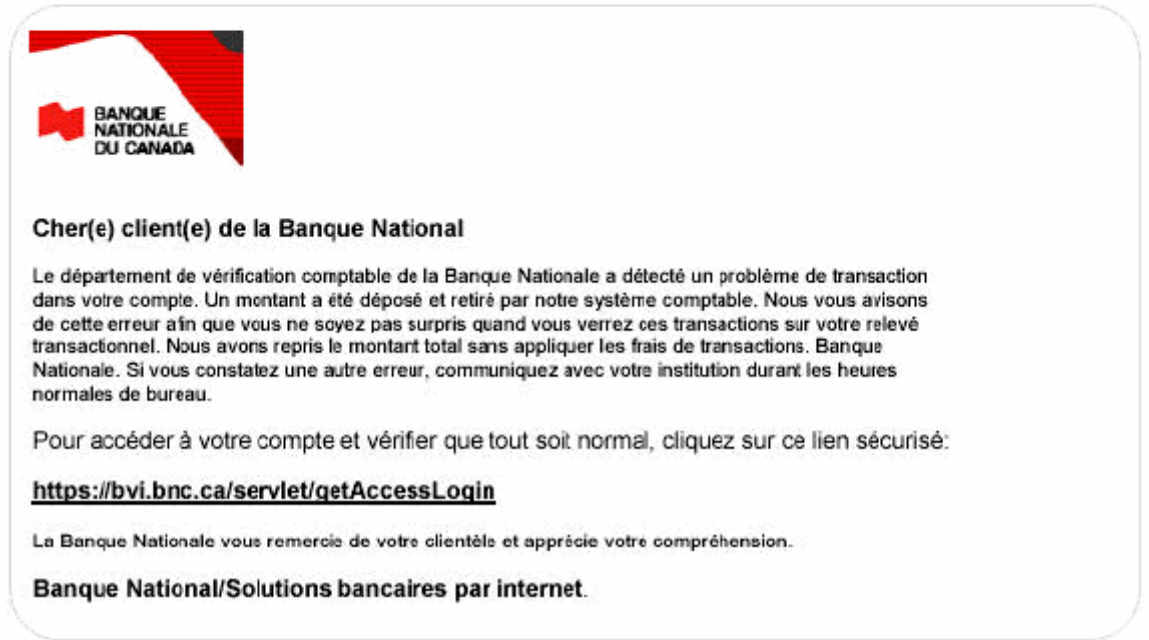
Soyez assuré que Bank National met tout en oeuvre pour rĕcompencer les utilisateurs de ses services internet.

Le Groupe Bank National vous remercie de votre clientèle et apprécie votre compréhension.

Bank National

Svp ne repondez pas a ce courriel car c'est seulement un avis. Le courrier envoyee a cette adresse ne peut pas etre repondu

Copyright © 2007 Mouvement des Bank National. Tous droits rĕservĕs.



BANQUE NATIONALE DU CANADA

Cher(e) client(e) de la Banque National

Le département de vérification comptable de la Banque Nationale a détecté un problème de transaction dans votre compte. Un montant a été déposé et retiré par notre système comptable. Nous vous avisons de cette erreur afin que vous ne soyez pas surpris quand vous verrez ces transactions sur votre relevé transactionnel. Nous avons repris le montant total sans appliquer les frais de transactions. Banque Nationale. Si vous constatez une autre erreur, communiquez avec votre institution durant les heures normales de bureau.

Pour accéder à votre compte et vérifier que tout soit normal, cliquez sur ce lien sécurisé:

https://bvi.bnc.ca/servlet/getAccessLogin

La Banque Nationale vous remercie de votre clientèle et apprécie votre compréhension.

Banque National/Solutions bancaires par internet.

Est-ce que le courriel est personnalisé?
Les courriels sont adressés au client de la Banque nationale, pas à vous personnellement.

Est-ce que le courriel parle d'un problème qui peut être réglé en cliquant sur un lien?
Le premier courriel vous invite à cliquer sur un lien pour gagner votre prix.
Le deuxième courriel vous invite à cliquer sur un lien pour accéder à votre compte.

Est-ce que le courriel demande des renseignements personnels que l'organisme devrait connaître?
Aucun site web ne devrait vous demandez des renseignements personnels tels que votre NAS pour y accéder.

Est-ce qu'il y a des fautes dans le courriel?
Dans le premier courriel on parle de la Bank national (au lieu de la Ban**que** nationa**l**e) et il y a plusieurs autres fautes.
Dans le deuxième courriel on parle de la Banque National (au lieu de Banque nationa**l**e).

Arnaque

Une **arnaque** ou une escroquerie est lorsque quelqu'un essaye de vous tromper.
Les arnaqueurs promettent souvent quelque chose qui est trop beau pour être vrai.
Si on vous propose quelque chose qui est trop beau pour être vrai, méfiez-vous.
Si vous répondez à une lettre, un courriel, un appel téléphonique ou une publicité, l'arnaqueur vous demande des frais, un paiement anticipé ou des renseignements financiers.
L'arnaqueur prend votre argent et vous n'avez jamais ce qu'il vous a promis.

Prix

Certains arnaqueurs vous feront croire que vous avez gagné un gros prix et que vous devez payer des frais ou des taxes pour l'obtenir.
Si vous gagnez un prix ou une loterie, vous n'aurez **jamais** à payer des taxes ou des frais sur l'argent que vous avez gagné.
Vous pourriez remplir un billet de tirage qui peut être une fraude.
Les renseignements sur le billet de tirage peuvent servir à communiquer avec vous.

Occasions en Or

Les fraudeurs peuvent vous proposer un prêt garanti à un bas taux d'intérêt même si vous avez un mauvais historique de crédit ou pas d'historique de crédit.
Ils peuvent vous faire croire que quelqu'un a besoin d'argent pour une bonne affaire.
Ils peuvent vous faire croire qu'ils ont beaucoup d'argent à transférer au Canada.
Ils peuvent vous faire croire que vous pouvez faire un investissement sans risque qui vous rapportera beaucoup.

Emploi

Les fraudeurs peuvent vous offrir un emploi.
Une partie de votre travail est de passer de l'argent dans votre compte de banque.
Si l'on vous demande de passer de l'argent dans votre compte de banque, il y a de bonnes chances que cet argent provienne du milieu du crime organisé.

Les fraudeurs peuvent vous dire que vous ferez un « coup d'argent » et que vous deviendrez riche en un rien de temps.
Ils peuvent vous offrir beaucoup d'argent à travailler à la maison.
Ils peuvent vous faire croire que vous ferez beaucoup d'argent en faisant du porte-à-porte ou en vendant à vos amis et aux membres de votre famille.
Méfiez-vous si vous devez acheter beaucoup d'**inventaire** (choses à vendre) pour commencer.
Méfiez-vous si on vous fait croire que vous ferez de l'argent en convaincant d'autres personnes à se joindre au groupe.
Il y a des gens qui vous diront qu'ils ont fait beaucoup d'argent mais méfiez-vous car ils font partie de l'arnaque.

Faux chèques

Si vous recevez un paiement pour quelque chose que vous avez vendu ou loué, acceptez seulement un chèque pour le montant exact.
Les fraudeurs peuvent vous donner un chèque pour un plus gros montant et vous demander de redonner l'argent supplémentaire en argent comptant ou en envoyant l'argent par mandat ou par virement.
Si le chèque est sans provision, vous perdrez votre argent.
Si le chèque est faux, votre argent sera parti avant que vous vous apercevez que c'est un faux.
Lorsque vous déposez le faux chèque à la banque, vous devenez **redevable** à la banque pour le montant du chèque.
Vous devrez alors rembourser la banque.

Menaces

Les fraudeurs vous diront que vous devez décider maintenant sinon vous perdrez votre chance.
Ils diront que vous perdrez votre compte si vous ne répondez pas.
Quelquefois, ils peuvent vous faire croire qu'ils ont besoin de l'argent pour aider quelqu'un qui est malade.

Conseils de sécurité

Ne cliquez jamais sur un lien d'un courriel frauduleux.
Votre ordinateur pourrait être attaqué par un site web frauduleux.

Ne répondez pas à un fraudeur.
S'il tente de vous rejoindre par téléphone, raccrochez.

N’envoyez **jamais** d’argent ou des objets de valeur.
Ne remplissez pas de billet de tirage pour un concours si vous ne connaissez pas la compagnie.

Soyez prudents lorsque vous rencontrez des gens sur l’internet.
Vous ne savez pas vraiment qui ils sont.

Si vous pensez avoir un chèque frauduleux, donnez-le à la police.
Si quelqu’un, par exemple, vous envoie un chèque et vous demande de lui renvoyer de l’argent par mandat-poste ou par virement, donnez le chèque à la police.

Ne signez pas un contrat en vitesse.
Prenez le temps d’y penser.

Victime de fraude

Si vous êtes une victime de fraude ou de vol d'identité, communiquez tout de suite avec votre banque et votre compagnie de carte de crédit.

Vous pouvez aussi communiquer avec les agences d'évaluation du crédit qui pourront mettre un avertissement de fraude à votre dossier.
Communiquez avec la police.

Écrivez ce qui est arrivé.
Gardez une liste des gens qui doivent être avisés de la fraude.
Gardez tous les documents reliés à la fraude.
Si la banque ou la compagnie de crédit disent que vous êtes responsable, communiquez avec l'Agence de la consommation en matière financière du Canada au 1-866-461-2232.

Si vous recevez un courriel ou un appel frauduleux, avertissez la compagnie ou l'organisme et la police.
Vous pouvez rejoindre la Gendarmerie royale du Canada (GRC) au 1-888-495-8501ou au www.phonebusters.com.
Vous pouvez aussi avertir la police locale ou provinciale.
Si c'est une fraude internationale, vous pouvez avertir RECOL, une initiative qui fait appel à un partenariat intégré des services de police canadiens et internationaux à www.recol.ca.

Si vous recevez un courriel ou appel téléphonique douteux, vous pouvez vérifier si l'organisme a émis un avis de fraude sur son site web.
Ouvrez une nouvelle fenêtre de votre navigateur et mettez-y le nom de l'organisme ou une adresse d'un site web provenant de votre relevé, entente, facture ou les Pages jaunes.
L'organisme aura peut-être des exemples d'hameçonnage vocal ou par courriel.
Le site web vous dira aussi quoi faire si vous avez donné vos renseignements personnels à un fraudeur.

Protéger mon identité

1. Je laisse les cartes d'identité non-essentielles à la maison. ☐
2. Je donne mon NAS seulement quand c'est essentiel. ☐
3. J'ai un NIP difficile à deviner. ☐
4. Je n'ai pas mis mon NIP par écrit. ☐
5. J'utilise ma main pour empêcher que les autres voient mon NIP. ☐
6. Je signe l'endos de mes cartes tout de suite. ☐
7. Je regarde ma carte lorsque je l'utilise pour le débit ou le crédit. ☐
8. Je garde les reçus de mes transactions de cartes de crédit et de débit et du guichet automatique. ☐
9. Je vérifie mes relevés de banque et de cartes de crédit. ☐
10. Je vérifie mon dossier de crédit une fois par an. ☐
11. Je déchiquette les documents qui contiennent des renseignements personnels. ☐
12. Je ne donne pas de renseignements personnels au téléphone à moins que ce soit moi qui fais l'appel. ☐
13. Je vérifie pour voir si le site web a le symbole du cadenas fermé et de la clé entière. ☐
14. Je ferme ma session, j'efface mon cache navigateur et je ferme ma fenêtre de navigateur. ☐
15. J'ai un anti-pourriel, un logiciel antivirus et un pare-feu. ☐
16. Je n'envoie pas de renseignements personnels par courriel. ☐

17. Je fais attention à l'hameçonnage vocal ou par courriel. ☐

18. Je demande à quelqu'un de s'occuper de ma poste lorsque je suis parti. ☐