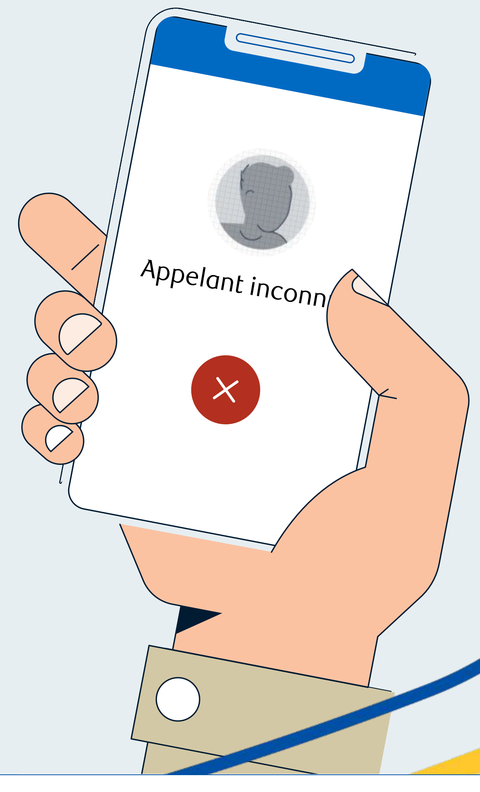
Escroquerie par usurpation d'identité bancaire

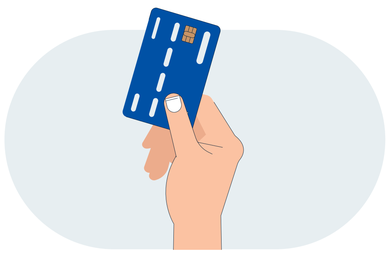
L'usurpation d'identité bancaire se produit lorsqu'un fraudeur communique avec vous en se faisant passer pour un employé de la Banque.

Le fraudeur tentera de vous tromper de diverses façons pour récolter des renseignements sur votre compte ou effectuer des opérations non autorisées.

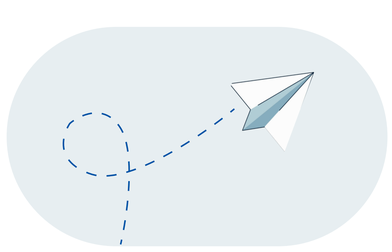
Lisez ce qui suit pour savoir comment reconnaître les signaux d'alerte, comprendre ce que RBC ne demandera JAMAIS et savoir comment protéger vos renseignements.



Attention aux signaux d'alerte

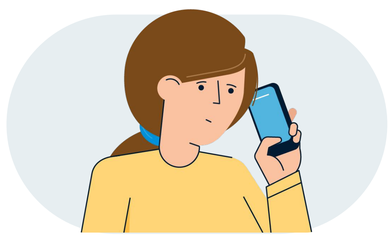


Vous recevez un appel, un courriel ou un message texte vous demandant de fournir les renseignements sur votre carte, votre mot de passe, votre code d'accès unique, votre numéro de référence de virement électronique ou d'autres renseignements sensibles.

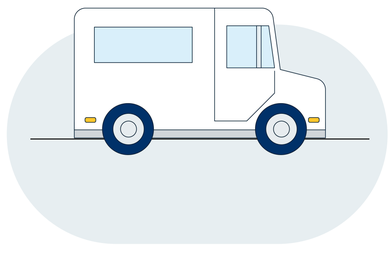


On vous demande de prendre des mesures pour « sécuriser votre profil », notamment :

- Faire un virement à RBC
- Vous envoyer des fonds à vous-même
- Effectuer n'importe quel autre type d'opération



Un appelant prolonge la conversation, utilise des moyens détournés et crée un faux sentiment d'urgence pour vous pousser à faire ce qu'il demande et vous inciter à révéler des renseignements sensibles.



Vous recevez un appel vous demandant de mettre votre carte de débit ou de crédit dans une enveloppe avec votre NIP ou votre mot de passe, et on vous dit de placer l'enveloppe quelque part ou de la remettre à un représentant de l'entreprise de messagerie qui viendra la chercher chez vous.

Vous avez reçu un appel de RBC concernant des opérations non autorisées, mais lorsque vous appelez au numéro figurant au verso de votre carte, on vous informe qu'il n'y a pas de notes ou d'indicateurs à cet effet dans nos systèmes.

Ce que RBC ne vous demandera <u>jamais</u> de faire:

- ✕ Effectuer n'importe quel type d'opération en son nom.
- ✕ Fournir un code d'accès à usage unique envoyé par message texte, courriel ou messagerie vocale pour vous identifier par téléphone ou en personne.
- ✕ Télécharger une application d'accès à distance.
- ✕ Divulguer votre NIP.
- ✕ Effectuer un virement de fonds pour quelque raison que ce soit.
- ✕ Effectuer n'importe quel type d'authentification numérique à deux facteurs pour les appels sortants (notamment : vérification de l'identité ou vérification du NIP à l'aide d'un code d'accès à usage unique).
- ✕ Créer un nouveau mot de passe dans Banque en direct avec le conseiller ou communiquer votre mot de passe à quiconque.

Façons de vous protéger

- ☐ Si vous recevez un appel suspect, raccrochez immédiatement et communiquez avec RBC au numéro figurant au verso de votre carte.
- ☐ Ne cliquez sur aucun lien ou ne fournissez aucune information si vous ne pouvez confirmer avec certitude l'identité de la personne qui communique avec vous.
- ☐ Signalez les messages textes suspects à votre fournisseur de services de télécommunications en les transférant au 7726 sur votre appareil mobile.
- ☐ Utilisez la fonctionnalité de verrouillage en libre-service des Services bancaires mobiles et de Banque en direct pour protéger vos cartes jusqu'à ce que vous puissiez communiquer avec RBC.
- ☐ Faites preuve de prudence lorsque vous recevez des messages non sollicités par téléphone, par courriel ou dans les médias sociaux. Ils ne sont probablement pas légitimes.
- ☐ Prenez le temps de vous renseigner sur les offres ou sur ce qu'on vous dit. Ne laissez jamais quelqu'un vous pousser à prendre une décision, à divulguer des renseignements ou à agir immédiatement.
- ☐ Consultez régulièrement les alertes de fraude de RBC à l'adresse www.rbc.com/cyberfute/alertes.

Soyez cyberfuté RBC
rbc.com/cyberfute