Arnaques téléphoniques et comment les reconnaître

Ces dernières années, divers facteurs ont contribué à créer un contexte particulièrement propice pour les fraudeurs, qui ont su profiter de la situation.
La personne mal intentionnée au bout du fil peut se faire passer, entre autres, pour un employé de votre institution financière, du gouvernement ou d'un corps policier, pour un proche ou encore un organisme à but non lucratif.
Son objectif ultime est de récolter de l'information confidentielle ou de recevoir de l'argent. Voici des conseils qui vous aideront à distinguer les appels légitimes des arnaques téléphoniques.

Deux exemples courants d'arnaques téléphoniques :

- Arnaque du faux conseiller et du faux facteur
- Arnaque du faux technicien

Arnaque du faux conseiller et du faux facteur

Une personne qui se dit être un conseiller de votre institution financière vous téléphone.
Il vous mentionne que vous avez été victime d'une fraude par carte de crédit ou de débit et que votre carte actuelle doit être remplacée.

Après vous avoir demandé le numéro de votre carte, le faux conseiller, parfois remplacé par un message enregistré, vous invite à lui donner votre NIP (numéro d'identification personnel) sous prétexte de bloquer la

carte pour empêcher d'autres transactions frauduleuses.
Il peut vous demander de le fournir de vive voix, à l'aide de votre clavier téléphonique ou en l'inscrivant sur un morceau de papier à joindre dans une enveloppe avec votre carte.

Puis, le faux conseiller vous offre de venir chercher votre carte, pour vous éviter de vous déplacer.
Il vous indique donc de simplement déposer la carte dans votre boîte aux lettres. Un facteur viendra ensuite la chercher.
Vous suivez ses indications et vous remarquez qu'une personne vêtue comme un employé de Poste Canada ou d'une autre entreprise de courrier vient récupérer votre carte.
Même si vous démontrez des doutes, la personne au bout du fil sait se montrer convaincante afin de gagner votre confiance.

De cette façon, les fraudeurs s'emparent de votre carte et de votre NIP et peuvent ensuite effectuer des transactions, notamment des retraits d'argent.

Développez les bons réflexes!

- En cas de doute, notez le nom de la personne qui vous appelle et mettez fin à la conversation.
  Appelez au numéro de téléphone indiqué au dos de votre carte de débit ou de crédit.
- Ne communiquez jamais votre NIP à qui que ce soit.
  C'est un numéro que seul vous devriez connaître.

Quelles sont les pratiques de Desjardins lors d'un appel?

Il est possible que nous communiquions avec vous à propos de nos produits et services, mais nous avons en place des pratiques pour assurer votre sécurité.

Si vous recevez un appel de Desjardins

Nous **ne vous demanderons jamais de donner :**

- vos **informations personnelles et confidentielles** (date de naissance, numéro de carte, NIP, numéro d'assurance sociale);
- vos **questions et réponses de sécurité** en lien avec vos comptes Desjardins;
- vos **identifiants, codes, informations ou mots de passe** pour vous authentifier;
- le code à usage unique que vous avez peut-être reçu pendant l'appel.

Ceci s'applique aussi dans le cas d'un **courriel** ou d'un **texto légitime**.

Si vous appelez Desjardins

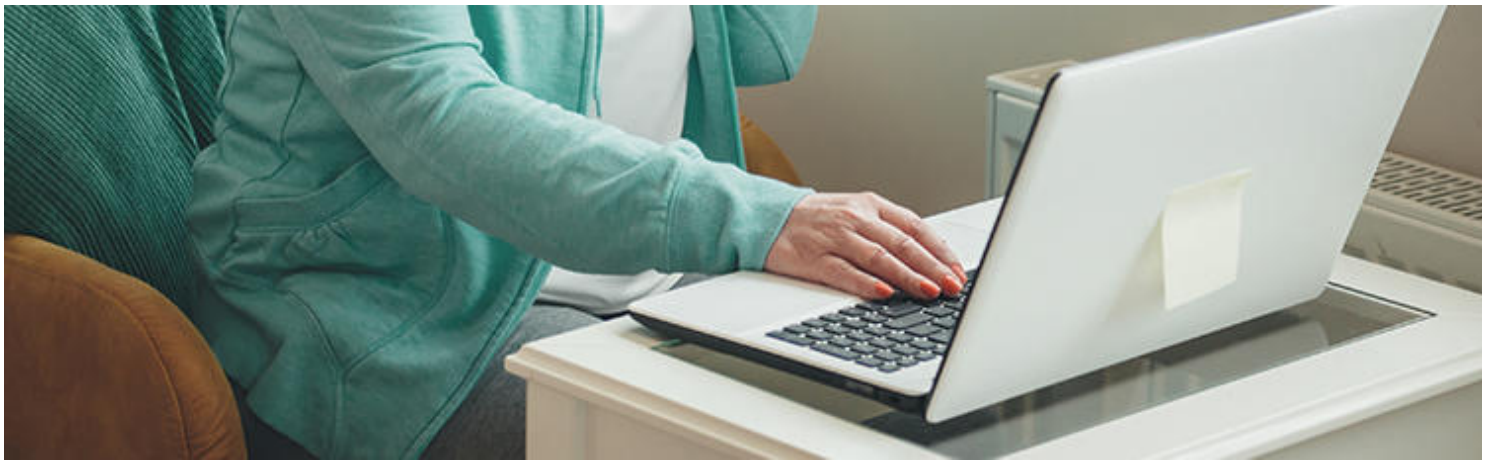
Lorsque c'est vous qui faites l'appel, pour vous authentifier, il est possible que le conseiller Desjardins vous demande de :

- fournir un code à usage unique reçu par notification poussée* ou par texto;
- répondre à des questions de sécurité.

Carte volée? Suspendez-la!

Si vous n'arrivez pas à mettre la main sur votre Carte d'accès Desjardins ou sur votre carte de crédit ou que vous pensez qu'elle a été volée, vous pouvez bloquer son utilisation temporairement via AccèsD.
C'est simple et rapide, et les risques d'utilisation frauduleuse sont de cette manière minimisés.

Une fois la carte retrouvée, il vous suffit de la réactiver.
Si la perte ou le vol de votre carte est confirmé, contactez-nous pour l'annuler et en obtenir une nouvelle.
Il est également possible de demander son remplacement dans l'application Services mobiles Desjardins et sur le Web.
Vous la recevrez par la poste dans un délai de 5 à 10 jours ouvrables.



Arnaque du faux technicien

Un autre stratagème utilisé par les fraudeurs afin d'obtenir vos informations personnelles, c'est une personne qui vous appelle et se fait passer pour un technicien en informatique (ex. : Windows, AccèsD, etc.) d'une entreprise reconnue.

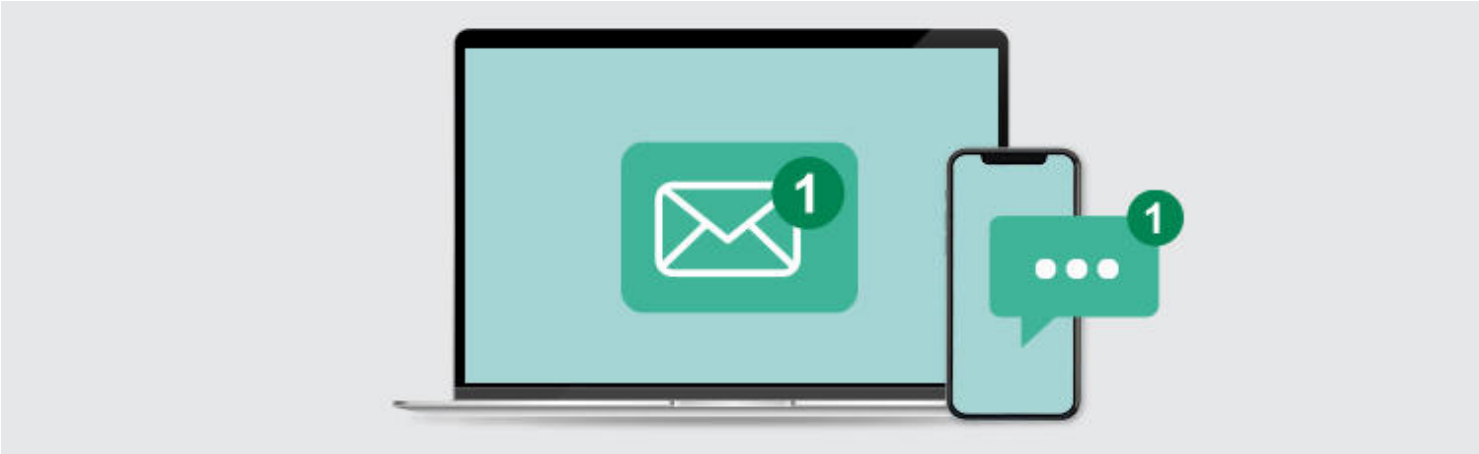
Le technicien vous dit qu'il doit procéder à une mise à jour d'un programme sur votre ordinateur.
Vous le laissez faire en pensant que c'est nécessaire, mais dans les faits, il profite de cet accès pour installer un programme qui viendra capter votre identifiant et votre mot de passe lors de votre prochaine connexion à AccèsD.

Dans certains cas, le fraudeur peut même pousser l'audace à vous demander de lui fournir vos codes d'accès.
Avec vos codes en main, il peut avoir accès à vos comptes et à vos données personnelles et commettre des fraudes.

Développez les bons réflexes!

- Gardez en tête qu'aucun professionnel ou entreprise **ne vous contactera personnellement pour vous aider à régler**, par exemple, un problème avec votre ordinateur.
- N'acceptez pas qu'un inconnu **prenne le contrôle à distance** de votre ordinateur.

- **N’exécutez jamais d’action** à la demande de quiconque.
  Surtout pour régler un problème pour lequel vous n’avez jamais demandé de soutien.
- Ne fournissez jamais **vos informations personnelles** (numéro de carte de débit ou de crédit, mot de passe AccèsD, NIP, etc.).
- Si vous avez un doute que votre ordinateur a été infecté, contacter rapidement votre institution financière et **faites nettoyer votre ordinateur** par un fournisseur de service reconnu.



Desjardins envoie des courriels et des textos

Nous utilisons le courriel et les textos pour communiquer avec vous, mais seulement pour vous fournir de **l’information factuelle**.
Il est possible de recevoir un message ou une alerte vous avisant, par exemple, que votre relevé de compte est disponible ou que votre solde de carte de crédit est élevé.

Desjardins vous protège grâce aux alertes de sécurité

Vous pourriez aussi recevoir un texto vous demandant de confirmer une tentative de connexion à votre compte ainsi que certaines transactions effectuées avec votre carte de crédit.
C’est simple, aucun lien à cliquer et vous n’avez qu’à répondre « Oui » ou « Non », selon ce qui est demandé.

Assurez-vous que votre numéro de cellulaire et votre adresse de courriel soient à jour dans la section « Ma sécurité », et sous « Gestion du dossier » de votre carte de crédit, puis choisissez « Changement d’adresse ».

Soyez alerte, sachez reconnaître les indices et ayez toujours de bons réflexes avant de fournir de l’information ou de transférer des sommes d’argent.
Si vous croyez ou vous avez été victime de fraude, communiquer avec le Centre antifraude du Canada puis avec votre institution financière le plus rapidement possible.

Pour plus de sécurité

Pour connaître l’ensemble de nos outils et conseils, consultez la page desjardins.com/securite et, surtout, n’hésitez pas à nous contacter en cas de doute.

* Une notification poussée est un message envoyé directement par une application mobile sur un téléphone ou sur une tablette.
Dans le cas d’une authentification auprès d’un conseiller, la notification poussée serait envoyée par l’application Accès D.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231013
"C'est ensemble qu'on avance"