CAISSE DESJARDINS DES RAMÉES

© Desjardins

HAMEÇONNAGE : COMMENT LE DÉTECTER, LE SIGNALER ET LE PRÉVENIR

CAISSE DESJARDINS DES RAMÉES

Cette technique de fraude est basée sur de fausses intentions, menées sous une fausse identité. Souvent, elle consiste à envoyer un message par courriel, par texto ou par l'entremise des réseaux sociaux en se faisant passer, entre autres, pour une institution financière ou une entreprise renommée. En lançant un maximum de lignes à l'eau, les voleurs souhaitent voir certains destinataires mordre à l'hameçon en leur faisant révéler certaines informations ou en cliquant sur un lien. L'objectif demeure toujours le même : soutirer de l'argent!

DÉTECTER LES SIGNES D'HAMEÇONNAGE

Une demande par courriel, par texto ou via les réseaux sociaux vous semble étrange? Attention : le stratagème ne consiste pas toujours à demander de l'argent. L'objectif est de vous inciter à poser un geste impulsif et immédiat pour ainsi obtenir vos informations personnelles.

1. Parfois, le piège débute en évoquant un **problème**, y compris en vous disant victime d'hameçonnage! On vous conseille alors de régler la situation, en entrant vos renseignements personnels.
2. Un **profit**, petit ou grand, semble tout à coup à votre portée. Par exemple, en laissant croire à un gain, un avantage ou un prix. Les fraudeurs tentent ensuite de vous soutirer des renseignements personnels.
3. Une **urgence** vous poussant à agir rapidement est un autre signe d'hameçonnage. Les fraudeurs jouent avec vos sentiments, dont la peur ou l'empathie pour vous inciter à l'action.
4. On pique votre **curiosité**? Vous avez envie de cliquer sur un lien ou d'ouvrir un fichier qu'on vous a envoyé? La plupart du temps, les fraudeurs piratent des comptes ou des profils pour se faire passer pour une personne que vous connaissez.

QUOI FAIRE (OU NE PAS FAIRE) SI VOUS AVEZ DES DOUTES SUR UN MESSAGE REÇU?

1. Prenez une pause et questionnez-vous. Si vous avez le moindre doute :

- Ne cliquez pas sur l'hyperlien d'un texte ou d'une image
- N'ouvrez pas les pièces jointes
- Ne téléchargez pas les images
- Abstenez-vous de répondre à l'expéditeur

2. Examinez ce que vous avez reçu :

- Reconnaissez-vous des signes mentionnés plus haut?
- Reportez-vous également au centre antifraude Canada.

Rappelez-vous : comme toute bonne histoire de pêche, quand c'est trop beau pour être vrai, c'est rarement vrai!

3. Signalez la fraude

Si vous avez cliqué sur un hyperlien, téléchargé ou ouvert une pièce jointe, communiquez avec le Centre antifraude du Canada, puis avec votre institution financière, en utilisant les coordonnées officielles.

✓ Pour les membres Desjardins : transférez le courriel ou le texto à : protection@desjardins.com

✓ Pour un texto, transférez-le au numéro : **7726**. Ceci vous permettra de signaler la fraude à vos fournisseurs de services.

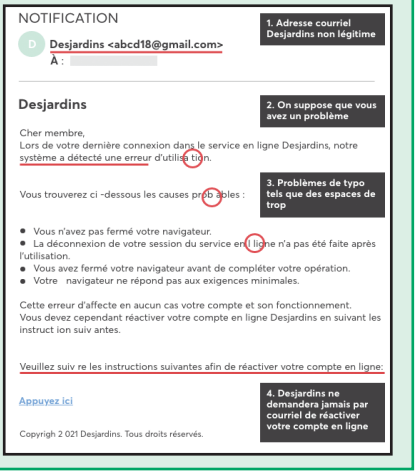
4. Supprimez ensuite le message frauduleux sans avoir interagi avec celui-ci.

EXEMPLE DE COURRIEL D'HAMEÇONNAGE

Vous recevez un courriel ou un texto demandant un changement de votre mot de passe ou la mise à jour de votre compte. Il peut vous inviter à cliquer sur un lien ou à ouvrir une pièce jointe. L'exemple ci-joint présente différents indices qui vous permettent de déterminer qu'il s'agit bien d'un courriel d'hameçonnage.

Il est important de se rappeler de prendre une pause afin de faire les vérifications appropriées avant de poser une quelconque action.

Pour plus d'information sur l'hameçonnage, visitez le www.desjardins.com/securite/hameconnage.



PRÉVENIR LA FRAUDE EN REHAUSSANT VOTRE PROTECTION

Desjardins redouble sans cesse d'efforts pour déployer les ressources nécessaires à la tranquillité d'esprit des membres.

- Rehaussez le niveau de sécurité de la connexion de vos comptes, en ajoutant un code de sécurité à votre mot de passe afin de limiter le risque de fraudes. **Activez la validation en deux étapes**: www.desjardins.com/securite/validation-2-etapes.

- Confirmez une tentative de connexion à votre compte ainsi que certaines transactions effectuées avec votre carte de crédit. C'est simple, vous n'avez qu'à répondre « Oui » ou « Non », selon ce qui est demandé. Activez le service gratuit d'**alertes de sécurité** en mettant à jour votre numéro de cellulaire dans AccèsD: www.desjardins.com/securite/alertes-securite-prevenir-fraude.