LA FRAUDE PAR COURRIEL OU TEXTO

Voici des informations importantes à connaître concernant la fraude par courriel ou texto. L'hameçonnage est un stratagème de fraude qui consiste à envoyer massivement des courriels ou des textos semblant provenir d'une institution financière ou d'une entreprise connue.

Ces courriels et textos sont utilisés par des personnes mal intentionnées pour voler vos informations personnelles ou installer un logiciel malveillant sur votre ordinateur, en vous incitant à cliquer sur des liens ou à ouvrir des fichiers joints.

Les conséquences potentielles de ce type d'attaque peuvent s'avérer importantes : perte de vos données, accès non autorisés ou vol de vos informations confidentielles dans le but de commettre des fraudes.

La vigilance et la reconnaissance des courriels et des textos d'hameçonnage permettent de vous protéger de ces conséquences. Un courriel ou un texto d'hameçonnage peut prendre plusieurs formes, mais sa caractéristique principale est d'être non sollicité.

Gestes simples à adopter pour éviter de vous faire hameçonner

Avant de cliquer :

1. Vérifiez que le courriel ou le texto est attendu et sollicité.
2. Portez attention aux différentes situations qui tentent de vous faire réagir :
    - **Urgence**
      L'objectif est de vous inciter à **poser un geste rapide et irréfléchi** en misant sur le sentiment d'urgence.
    - **Profit**
      L'objectif est de vous faire croire que vous avez **reçu un gain ou un avantage sans l'avoir demandé**. Les fraudeurs misent sur l'appât du gain pour vous pousser à divulguer vos renseignements personnels.
    - **Problème**
      L'objectif est de vous informer qu'un **problème est survenu** dans votre compte. Cette situation vous oblige à divulguer vos renseignements personnels pour résoudre le problème.

Exemples de situations déclenchant une réaction impulsive		
URGENCE	**PROFIT**	**PROBLÈME**
Demande de mise à jour des coordonnées bancaires ou des renseignements personnels	Achat, remboursement ou transfert de fonds porté à votre compte	Problème ou mise à jour d'une application ou de votre système d'exploitation (Windows, Mac OS, etc.), expiration de votre mot de passe, dépassement de l'espace disponible sur le disque dur, etc.
Somme due à une agence fiscale	Prix reçu, voyage gagné, etc.	Problème de livraison d'un colis
Collecte de fonds après une catastrophe naturelle, un évènement tragique ou autre demande d'argent	Rabais important	Problème, suspension, opérations frauduleuses ou frais non autorisés sur votre Carte d'accès Desjardins, votre carte de crédit ou dans votre compte AccèsD

3. Vérifiez si l'adresse courriel de l'expéditeur vous semble connue et légitime, notamment après l'arobas (@) : est-ce une adresse d'entreprise ou personnelle?
4. Déplacez votre curseur sur le lien hypertexte (sans cliquer dessus) pour vérifier que l'adresse du lien est légitime et correspond à l'entreprise de l'expéditeur (attention aux adresses similaires).
5. Évaluez la pertinence et la vraisemblance du courriel ou du texto. Soyez sur vos gardes! Posez-vous des questions : avez-vous vraiment participé à un concours? Attendez-vous un colis? Est-ce une procédure habituelle? Est-ce « trop beau pour être vrai »?
6. Ne fournissez jamais d'informations confidentielles permettant de vous authentifier par courriel ou texto (par exemple : numéro d'assurance sociale, numéro de carte de crédit, date de naissance, mot de passe, etc.).
7. Évitez d'être trop curieux et d'être distrait par des identités visuelles ou des logos connus qui peuvent être facilement copiés et prendre l'apparence d'un courriel, d'un texto ou d'un site Web authentique.

Soyez vigilant!

Quoi faire si vous recevez un courriel ou un texto frauduleux?

Si vous recevez un courriel ou un texto que vous croyez frauduleux :

1. Ne cliquez pas sur l'hyperlien d'un texte ou d'une image.
2. N'ouvrez pas le fichier joint et n'activez pas les macros d'un document.
3. Ne téléchargez pas d'image et n'autorisez pas l'affichage d'une image.
4. Ne répondez pas à l'expéditeur pour ne pas confirmer la validité de votre adresse courriel.

En cas de **courriel frauduleux**:

1. Transférez-le à protection@desjardins.com. Vous recevrez une réponse automatisée.
2. Supprimez ensuite le courriel frauduleux.

En cas de **texto frauduleux**:

1. Transférez-le à protection@desjardins.com. Vous recevrez une réponse automatisée.
2. Transférez-le à **7726**. Vous recevrez une réponse automatisée.
3. Supprimez ensuite le texto frauduleux.

Quoi faire si vous avez cliqué sur un lien ou ouvert une pièce jointe dans un courriel ou un texto frauduleux?

Vous n'avez pas fourni vos informations confidentielles

- Modifiez sans tarder votre mot de passe pour ce site.
  - Simplement en cliquant sur le lien d'un courriel ou message texte frauduleux, votre ordinateur peut avoir été infecté par un logiciel malveillant permettant aux fraudeurs de recevoir tous vos nouveaux mots de passe. Avant de modifier votre mot de passe, assurez-vous que votre ordinateur ne contient aucun virus ou utilisez temporairement un autre ordinateur.
- Appliquez la même procédure pour tous vos accès confidentiels.

Vous avez fourni vos informations confidentielles?

- Communiquez avec l'équipe de sécurité pour investigation: 1 866 335-0338

Source : Caisse Desjardins de Rimouski – Septembre 2021