Le bulletin
EspaceD

Desjardins
Caisse populaire Trillium

Des conseils stratégiques pour des épargnants avisés

Quatrième trimestre 2018

Armez-vous contre la fraude

Maîtres dans l'art d'utiliser les émotions pour tromper leurs cibles, les fraudeurs raffinent sans cesse leurs techniques. Mais quelques dénominateurs communs devraient vous mettre la puce à l'oreille. Comme la prémisse qui dit que, si quelque chose est trop beau pour être vrai, c'est que c'est probablement faux!

Les fraudeurs utilisent les émotions pour tromper leurs victimes.

Vous recevez un appel téléphonique, un message texte ou un courriel qui provoque chez vous un sentiment d'urgence ou de peur, ou qui vous fait miroiter un gain facile à votre portée. Méfiez-vous! Les stratagèmes qui s'appuient sur les émotions sont nombreux. En voici 4 parmi les plus courants.

1. Vous recevez un appel, en anglais, de ce qui semble être l'Agence de revenu du Canada vous mentionnant que vous devez de l'argent et que, faute d'agir sur-le-champ, votre dossier sera remis aux autorités et vous serez passible d'une accusation criminelle. Envahi par la peur, vous avez peut-être comme premier réflexe de suivre les consignes et d'appeler au numéro laissé dans votre boîte vocale.

CONSEIL

Surtout, ne rappelez pas, car il s'agit bel et bien d'une arnaque. Si vous avez des doutes, communiquez plutôt directement avec l'agence dont il est question en utilisant un numéro de téléphone officiel publié sur le site Web du gouvernement du Canada par exemple. Sachez que les organismes gouvernementaux n'utilisent pas de telles pratiques et que, si votre dossier faisait l'objet d'un quelconque litige, vous en seriez avisé par la poste. Bloquez plutôt le numéro de téléphone de l'appelant et, si la situation se reproduit, signalez-le aux autorités.

2. Vous recevez un message texte de votre petit-fils vous expliquant qu'il est à l'étranger, qu'il s'est fait voler son argent et son passeport et qu'il est incapable d'utiliser son téléphone pour communiquer avec vous de vive voix. Il vous demande de lui transférer une importante somme d'argent afin de revenir au pays. L'inquiétude s'installe et vous sentez le besoin de lui venir en aide.

CONSEIL

Ne faites rien avant d'avoir procédé à certaines vérifications. Communiquez d'abord avec un proche parent pour corroborer les faits. Il s'agit le plus souvent d'un stratagème visant à vous escroquer.

3. Vous recevez un courriel de votre institution financière qui vous informe que votre compte a été la cible d'une tentative de fraude. On vous invite à cliquer sur un lien afin de fermer rapidement votre compte. Paniqué devant l'urgence de la situation, vous êtes tenté de suivre les consignes mentionnées et de fermer votre compte sur-le-champ.

CONSEIL

Ne cédez pas à la panique! Ne cliquez pas sur les liens affichés et n'ouvrez pas les pièces jointes. Les institutions financières ne communiquent jamais avec leurs membres et clients par courriel ou par texto pour valider une authentification sur une page de connexion, et encore moins pour obtenir des informations

personnelles. Toutefois, par mesure de sécurité, en cas de doute sur des transactions faites dans votre compte, votre institution financière pourrait communiquer avec vous par téléphone. Le cas échéant, vous auriez simplement à répondre par oui ou par non à quelques questions concernant ces transactions.

N'accédez pas non plus au site de votre institution financière à partir d'un lien transmis par courriel ou issu d'un résultat dans un moteur de recherche (Google, Yahoo, Bing, etc.). Tapez toujours l'adresse (www.desjardins.com, par exemple), puis cliquez sur le lien permettant de faire des opérations en ligne. Assurez-vous que cette adresse sécurisée commence bien par https://.

Si vous avez répondu ou croyez avoir répondu par erreur à un courriel frauduleux, modifiez vos mots de passe sans tarder dans tous les sites transactionnels que vous utilisez.

4. Vous recevez un message vous informant que vous êtes l'heureux bénéficiaire de la fortune d'un étranger récemment décédé qui vous aurait choisi comme seul héritier de sa succession. Pour mettre la main sur votre butin, vous devez transmettre vos informations personnelles et financières. Bien que vous doutiez de la véracité de cette nouvelle, l'idée d'une petite fortune tombée du ciel suscite chez vous de la joie et de l'excitation. Et si c'était vrai?

CONSEIL

Faites des vérifications approfondies avant de divulguer une quelconque information. Nombreux sont ceux qui ne peuvent résister à des occasions apparemment si alléchantes. C'est pourquoi les fraudeurs utilisent l'appât du gain pour piéger leurs victimes. Retenez qu'une méfiance bien placée vous évitera bien des soucis.

AYEZ DES RÉFLEXES SÉCURITAIRES

Vous croyez que vous ne serez jamais victime d'un fraudeur et que vous savez éviter les pièges? Détrompez-vous et restez vigilant, car les arnaques sont de plus en plus raffinées et difficiles à détecter. Pour vous prémunir adéquatement contre la fraude, voici 5 réflexes à adopter.

Ne donnez aucun renseignement personnel par courriel, téléphone ou texto! Sauf s'il s'agit d'un membre de votre famille ou d'un ami proche avec qui vous êtes totalement en confiance.

Ne cliquez sur aucun lien qui vous semble douteux. Vérifier l'adresse. Comporte-t-elle des caractères étranges? Est-ce bien celle de l'institution financière dont il est question? Vérifiez si le message contient des fautes d'orthographe, fréquentes dans les communications frauduleuses.

N'ouvrez aucune pièce jointe, à moins de connaître personnellement l'émetteur ou l'institution qui vous l'envoie.

Ne téléchargez pas d'images, elles peuvent contenir des virus qui infecteront votre appareil.

Que faire si vous recevez un courriel ou un texto frauduleux au nom de Desjardins?
S'il s'agit d'un courriel: Transférez-le à protection@desjardins.com et vous recevrez une réponse automatisée. Supprimez ensuite le courriel frauduleux.

S'il s'agit d'un message texte: Transférez-le par courriel à protection@desjardins.com et par message texte à 7726. Les experts en sécurité de Desjardins recommandent d'utiliser non pas l'un de ces moyens de transmission, mais bien les deux. Une réponse automatisée vous sera ensuite envoyée. Il ne vous restera plus qu'à supprimer le message frauduleux de vos appareils.

Vos renseignements confidentiels sont-ils bien protégés?

Pour s'emparer de votre argent, voire de votre identité, les fraudeurs tentent d'obtenir vos informations personnelles comme vos numéros de comptes bancaires ou de cartes de crédit, vos mots de passe ou votre numéro d'assurance sociale. Assurez-vous donc que vos renseignements confidentiels sont bien protégés.

DISPOSEZ DE VOS DOCUMENTS DE FAÇON SÉCURITAIRE

Plusieurs des documents que vous recevez par la poste, comme les factures, contiennent des renseignements personnels dont les escrocs sont friands. Pour vous prémunir contre le vol d'identité, utilisez une déchiqueteuse pour les détruire avant de les mettre au recyclage. Certains commerces offrent d'ailleurs ce service à un prix abordable. Sinon, il mieux vaut les mettre à la poubelle que dans votre bac bleu.

Changez fréquemment vos mots de passe et créez-en des complexes!

VARIEZ VOS MOTS DE PASSE

Si vous utilisez toujours le même mot de passe et que des personnes malveillantes réussissent à le saisir, vous ouvrez la porte à des fraudes dans tous vos comptes. Changez fréquemment vos mots de passe et créez-en des complexes! Utilisez des lettres, des chiffres et des symboles dont vous vous souviendrez facilement, mais qui n'ont aucun lien avec vos informations confidentielles.

INSTALLEZ UN LOGICIEL DE SÉCURITÉ SUR VOTRE ORDINATEUR

Assurez-vous que votre ordinateur est muni d'un logiciel de sécurité avec mises à jour automatiques et comprenant les éléments suivants: antivirus, anti-espion, anti-pourriel et pare-feu. Effectuez aussi des mises à jour fréquentes de votre système d'exploitation (Windows, macOS ou Linux) et de votre navigateur.

UTILISEZ VOS PROPRES DISPOSITIFS ÉLECTRONIQUES POUR EFFECTUER VOS TRANSACTIONS

Évitez d'utiliser des ordinateurs publics pour effectuer vos transactions confidentielles. Servez-vous toujours de vos propres appareils. Lors d'achats en ligne, assurez-vous que vous êtes sur un site sécurisé. Le «http» de l'adresse du site devrait contenir un «s», donc s'écrire «https». De même, quand vous êtes sur le point d'entrer vos coordonnées et vos informations de paiement, vous devriez voir apparaître l'icône d'un cadenas dans la barre d'adresse. Enfin, si un site vous semble suspect, éviter d'y faire des affaires.

Ce bulletin est publié quatre fois l'an par la direction Design graphique, Publicité et Médias sociaux, vice-présidence Marketing, Mouvement Desjardins.

Information: 418 835-8444 ou 1 866 835-8444

Rédactrice en chef: Marie-Christine Daignault. **Conception graphique:** Design graphique, Publicité et Médias sociaux – Mouvement Desjardins.