Le bulletin
EspaceD

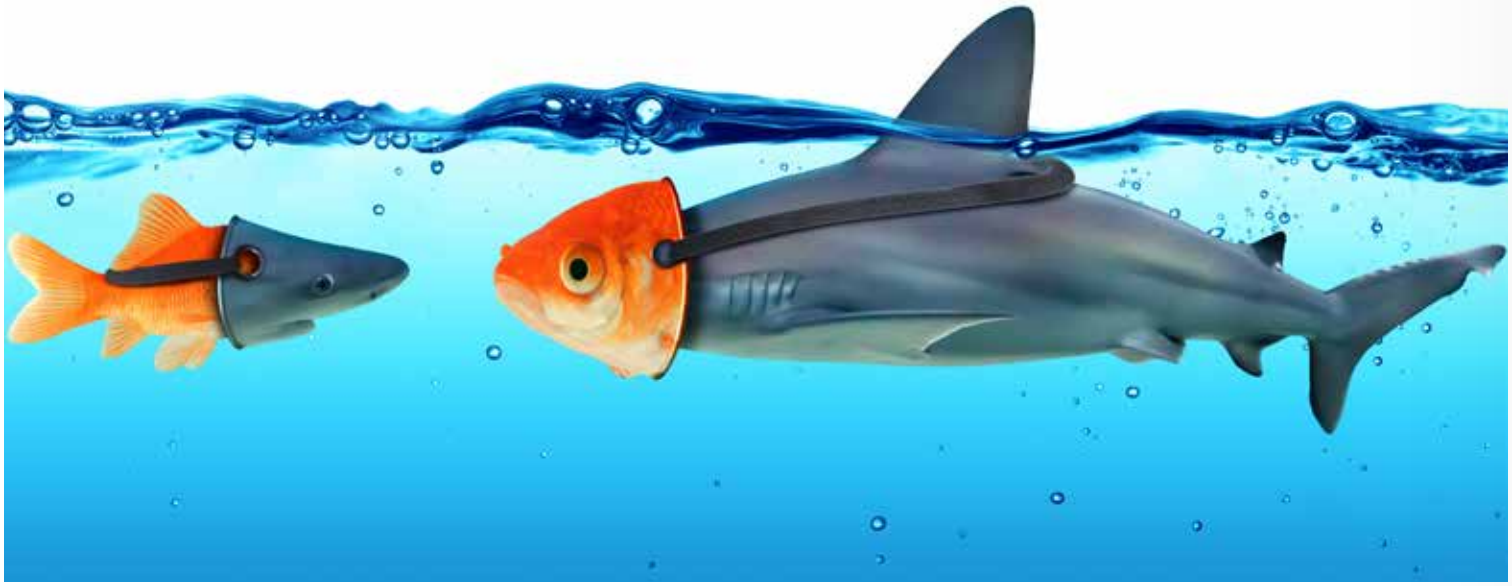
Desjardins
Caisse du Sud
de la Matawinie

Des conseils stratégiques pour des épargnants avisés

Quatrième trimestre 2017

3 cyberfraudes à surveiller

POUR ÉVITER D'ÊTRE LE PROCHAIN POISSON, APPRENEZ À DÉMASQUER LES PRINCIPALES FRAUDES SUR LE WEB.



Évitez de vous faire hameçonner

1 geste simple à adopter

desjardins.com/securite/hameconnage

1. Courriel

Vous avez sûrement déjà reçu un courriel frauduleux…

COMMENT AVEZ-VOUS RÉAGI ?

Bien que 97 %* des gens pensent être en mesure de reconnaître un tel piège, les fraudeurs réussissent malgré tout à déjouer la vigilance de plusieurs internautes. Étonnant, non ?

Scrutez à la loupe la raison invoquée pour vous faire réagir de manière impulsive.

POURQUOI CLIQUONS-NOUS ?

Un sentiment d'urgence, un problème que vous voulez régler au plus vite ou une promesse de gain alléchante sont des prétextes susceptibles de vous faire tomber dans le panneau.

COMMENT AGIR ALORS ?

Aussi étrange que cela puisse paraître, la première chose à faire, c'est de ne rien faire… le temps de prendre le recul nécessaire avant de réagir à un courriel inattendu. Ensuite, si la communication semble douteuse, effectuez les vérifications ci-dessous afin de valider sa légitimité.

Rappelez-vous que, dans le doute, il vaut mieux s'abstenir pour déjouer les plans des fraudeurs que de venir gonfler leurs statistiques de réussite.

6 VÉRIFICATIONS RAPIDES POUR ÉVITER DE VOUS FAIRE PRENDRE

1. Vérifiez si l'adresse de courriel de l'expéditeur vous semble connue et conforme aux standards habituels, notamment après l'arobas (@).
2. Regardez s'il s'agit d'une adresse d'entreprise ou personnelle.
3. Déplacez votre curseur sur le lien hypertexte, sans cliquer sur le lien, afin de vérifier si l'adresse du lien correspond à l'entreprise de l'expéditeur, s'il se présente comme tel.
4. Méfiez-vous puisque, souvent, l'adresse suspecte ressemble à s'y méprendre à une adresse connue, mis à part une seule lettre.
5. Scrutez à la loupe la raison invoquée pour vous faire réagir de manière impulsive afin d'éviter de fournir des informations confidentielles.
6. Méfiez-vous du contenu du courriel, puisque les fautes d'orthographe n'y sont pas toujours présentes.

*McAfee

2. SMS

Fraude par SMS, par texto, smishing… peu importe le nom donné à ce stratagème, l'objectif demeure le même: obtenir des informations personnelles.

Voici les prétextes les plus courants pour tenter de vous faire tomber dans le panneau.

PROBLÈMES D'ACCÈS

Les fraudeurs sont susceptibles de vous faire réagir en prétextant l'existence de problèmes. Par exemple: on vous avise que vos accès (à votre compte, au site transactionnel de votre institution financière, etc.) sont bloqués ou suspendus et que, pour résoudre le problème, vous devez cliquer sur un lien inclus dans le SMS reçu.

À ne pas confondre avec un SMS légitime provenant de votre institution financière. En effet, Desjardins offre un service de prévention de la fraude par message texte. Vous pourriez être contacté pour que soient validées des transactions effectuées par carte de crédit. Il vous sera alors demandé de communiquer au numéro inscrit au revers de votre carte. Desjardins ne vous demandera toutefois jamais d'informations personnelles par SMS.

VIREMENT INTERAC

Lorsque vous recevez un virement Interac d'une personne que vous connaissez, un courriel ou un SMS vous est automatiquement envoyé pour vous en aviser et le nom de la personne qui vous envoie l'argent est clairement indiqué.

Vous devez ensuite cliquer sur un lien qui vous mènera vers la page de connexion du site transactionnel de votre institution financière. Les fraudeurs utilisent ce moyen pour vous faire tomber dans le panneau. Ils envoient un courriel d'hameçonnage prétextant la réception d'un virement. Le hic, c'est que celui-ci est quasi identique à un courriel légitime!

Différence importante: le nom de l'expéditeur est celui d'une personne que vous ne connaissez pas nécessairement. Avant de cliquer, il est important de vous demander si vous attendez vraiment de l'argent par virement Interac d'une personne que vous connaissez… car l'argent ne tombe pas du ciel.

REMBOURSEMENT D'IMPÔT

Durant la période des impôts, les fraudeurs en profitent. Ils se font passer pour l'Agence de revenu du Québec ou du Canada et vous informent que vous avez reçu un remboursement d'impôt.

Dans quelques mois, soyez vigilants! Ne tentez pas de contacter l'Agence du revenu au numéro fourni. Contactez-la plutôt au numéro de téléphone inscrit sur son site Internet officiel pour valider la véracité de cette information.

Avant de cliquer, il est important de vous demander si vous attendez vraiment de l'argent par virement Interac.

- Pour plus de détails, visitez la **section Sécurité du site Web de Desjardins.**
- Si vous recevez un SMS ou un courriel frauduleux, acheminez-le à l'adresse courriel **protection@desjardins.com** et supprimez-le.
- Pour tout savoir sur la fraude et les risques de vol d'identité en ligne, découvrez le site **Je garde ça pour moi,** une initiative contre la fraude en ligne du Mouvement Desjardins en collaboration avec la Banque Nationale et la Banque Laurentienne.

3. Arnaque du faux technicien

Voici comment reconnaître un stratagème de fraude très en vogue et la manière de s'en protéger.

Un stratagème de fraude très en vogue par les temps qui courent.

LE SCÉNARIO TYPE

Un «technicien» informatique communique avec vous par téléphone. Il prétend devoir faire, par exemple, la mise à jour d'un logiciel, la décontamination ou la réparation de votre ordinateur. Pour vous convaincre, ce «technicien» affirme que la version de votre logiciel est désuète (ou contaminée) et qu'elle ne sera bientôt plus accessible. Il demande ensuite de se connecter à distance à votre ordinateur pour effectuer une «mise à jour».

CE QUI SE PASSE EN RÉALITÉ

Le fraudeur souhaite plutôt avoir accès à votre ordinateur afin d'y faire un «balayage» pour recueillir vos identifiants et vos mots de passe. En ayant en main vos informations personnelles, il sera ensuite en mesure de procéder à des transferts de fonds.

À SAVOIR ABSOLUMENT

Le technicien d'une entreprise ne vous appellera jamais pour effectuer de telles mises à jour ou réparations sur votre ordinateur. La vigilance est votre meilleure alliée dans ce type de situation.

4 CONSEILS UTILES

1. N'acceptez jamais qu'un inconnu prenne le contrôle à distance de votre ordinateur.
2. N'exécutez jamais d'action à la demande de quiconque.
3. Ne fournissez jamais vos informations personnelles (numéro de carte de débit ou de crédit, mot de passe Accès D, NIP).
4. En cas de doute, mettez fin à la conversation et communiquez avec l'entreprise pour laquelle ce «technicien» prétend travailler à un numéro de téléphone obtenu d'une source externe fiable (ex.: Canada 411).

QUE FAIRE SI VOUS AVEZ PERMIS AU FRAUDEUR D'AVOIR ACCÈS À VOTRE ORDINATEUR?

Communiquez rapidement avec :

- Les Services de cartes Desjardins au numéro qui figure au revers de votre carte de débit ou de crédit
- Le **Centre antifraude du Canada** au 1 888 495-8501

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, poste 5523733 ou 1 866 835-8444, poste 5523733.

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