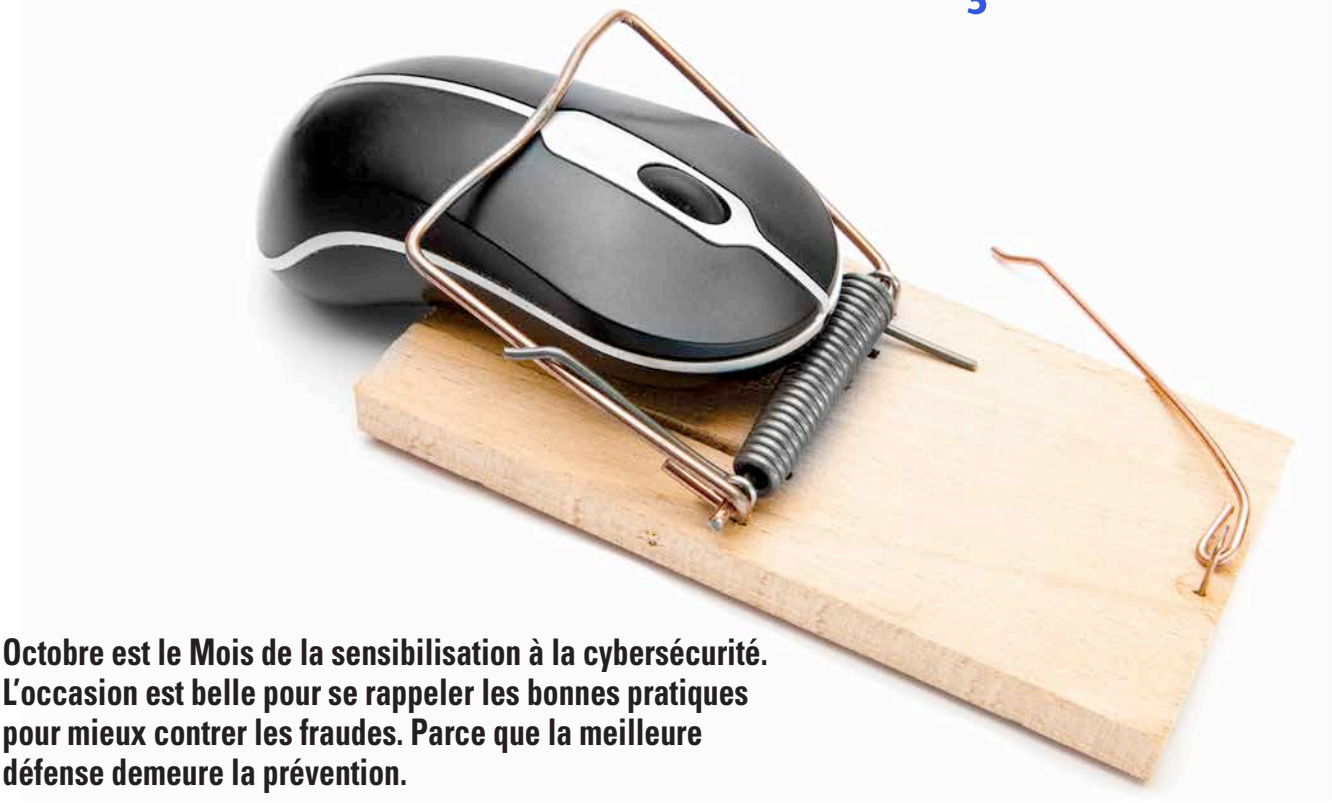
Le bulletin
EspaceD
Des conseils stratégiques pour des épargnants avisés

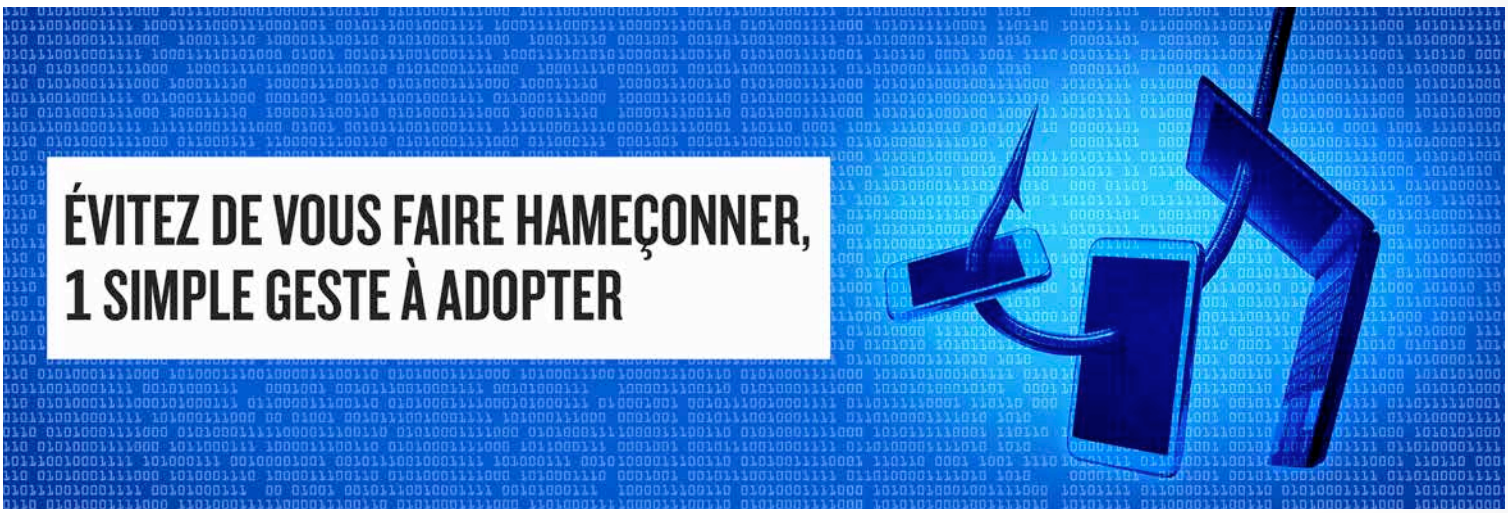
Desjardins
Caisse populaire Trillium

Quatrième trimestre 2016

ÊTES-VOUS À L'ABRI D'UNE TENTATIVE D'HAMEÇONNAGE?



Octobre est le Mois de la sensibilisation à la cybersécurité. L'occasion est belle pour se rappeler les bonnes pratiques pour mieux contrer les fraudes. Parce que la meilleure défense demeure la prévention.



Stéphanie Gohier-Coulombe et Karine Benoit | Mouvement Desjardins

Que faites-vous lorsque vous recevez un courriel ou un texto ? La plupart des gens l'ouvrent systématiquement et, sans trop porter attention, cliquent sur les fichiers joints ou les liens insérés. Cette habitude, les fraudeurs l'ont bien comprise et l'exploitent à fond !

Chaque jour, des milliers de tentatives de vol d'informations confidentielles à des utilisateurs sont envoyées par courriel et par message texte (SMS) d'hameçonnage. Ces courriels se présentent sous divers prétextes, mais la caractéristique principale est qu'ils ne sont pas sollicités.

La vigilance demeure la meilleure des protections puisque les conséquences potentielles sont importantes : la prise de contrôle à distance de son ordinateur par un cybercriminel, la perte de données, de fichiers ou d'images ainsi que le vol d'informations personnelles et bancaires en vue de commettre une fraude.

98 COURRIELS SONT REÇUS OU ACHEMINÉS PAR PERSONNE CHAQUE JOUR EN MOYENNE

Une simple habitude qui joue des tours !

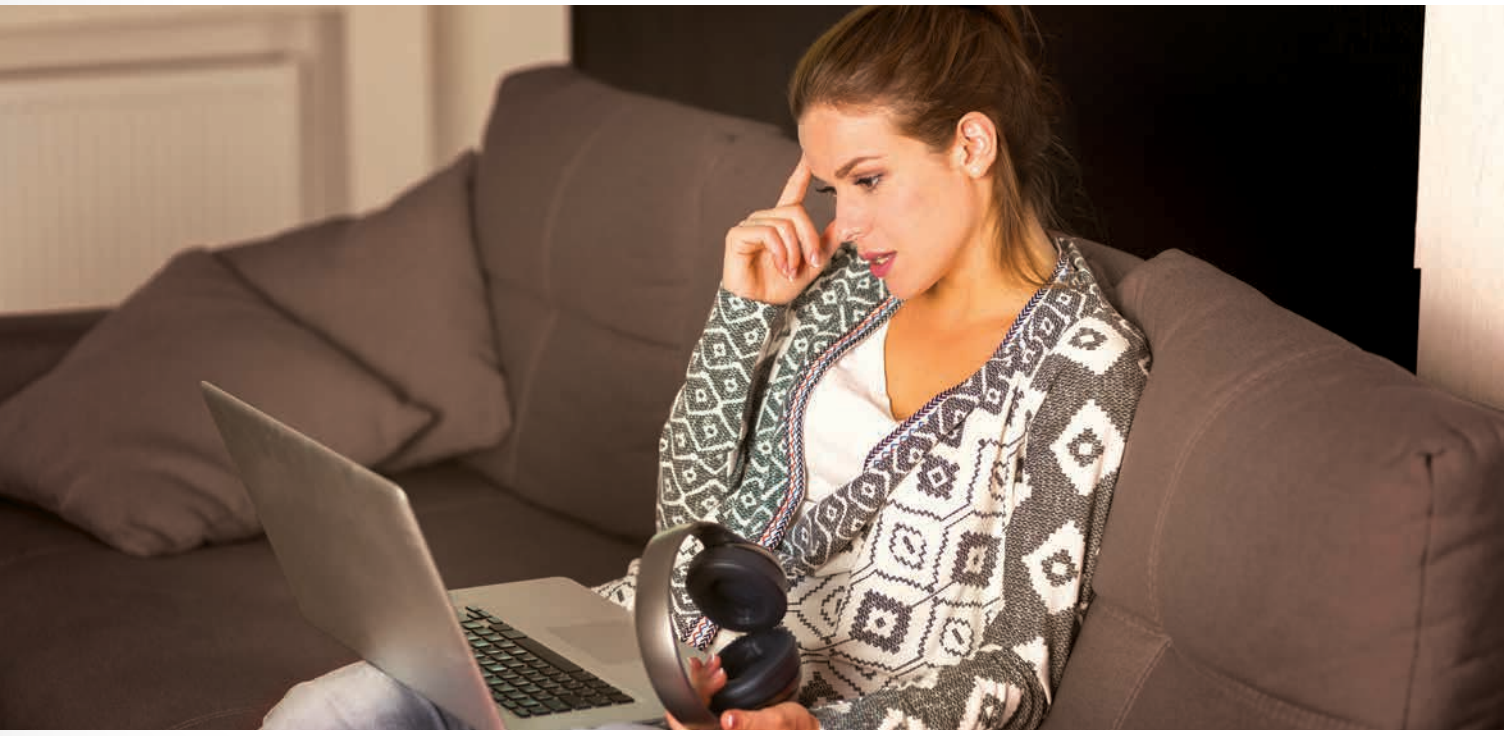
Les fraudeurs ont raffiné leurs techniques pour piéger les utilisateurs, ce qui complexifie la recherche d'indices pour détecter les courriels et les messages textes (SMS) d'hameçonnage. Ils sont devenus de véritables spécialistes en marketing et en psychologie, sachant trouver le bon prétexte pour vous faire réagir. Comme ce stratagème de fraude est évolutif, les attaques des fraudeurs portent davantage sur des situations comme l'urgence, le profit et le problème.

Votre curiosité, votre pire ennemi

Misez sur la vigilance, la patience et la réflexion pour bien reconnaître un courriel d'hameçonnage. En cas de doute :

- Ne cliquez pas sur le lien hypertexte d'un texte ou d'une image ;
- N'ouvrez pas le fichier joint ;
- Ne téléchargez pas le fichier ou n'autorisez pas l'affichage d'une image ;
- Ne répondez pas à l'expéditeur puisque cela confirme la validité de votre adresse de courriel ;
- Détruisez le courriel.

Le service Assistance vol d'identité est offert gratuitement aux membres particuliers de Desjardins.



3 QUESTIONS POUR ÉVALUER VOS RÉFLEXES SUR LE WEB

1. ÊTES-VOUS ASSEZ MÉFIANT ?

Contrairement à la croyance populaire, l'hameçonnage existe aussi sur les réseaux sociaux. Les fraudeurs misent sur le fait que les gens partagent facilement des pages qui demandent vos informations (pour participer à certains concours ou voir des vidéos par exemple). Bref, les fraudeurs misent sur la nature même des médias sociaux, soit le visionnement et le partage, pour obtenir certaines informations personnelles.

2. ÊTES-VOUS TROP GÉNÉREUX DE VOS INFORMATIONS ?

Même sans concours, la plupart d'entre nous dévoilent facilement quelques bribes de vie sur les médias sociaux. Il n'y a pas que nos amis qui verront la photo de la nouvelle maison. Les fraudeurs aussi peuvent voir et recueillir vos informations affichées volontairement sur vos réseaux sociaux.

Bien que la majorité des gens soient sensibles à ne pas afficher leur date de naissance, il existe bien d'autres informations qui en disent long sur vous, tels que vos liens de parenté avec les membres de votre famille, votre numéro de cellulaire, etc.

3. AVEZ-VOUS DE BONNES HABITUDES ?

- Limitez-vous l'accès de vos médias sociaux à vos amis ?
- Remettez-vous en question la pertinence de certains de vos statuts ?
- Doutez-vous des messages qui demandent des informations personnelles ?
- Hésitez-vous devant un site qui demande un accès à vos informations personnelles ?

Cette année, Desjardins s'est uni à la Banque Nationale et à la Banque Laurentienne pour créer le site **jegardecapourmoi.com,** une expérience interactive pour apprendre à se prémunir de la fraude bancaire en gardant ses informations personnelles pour soi. Avez-vous de bons réflexes ? Testez vos habitudes à **jegardecapourmoi.com.**

RANÇONGICIEL :
UN STRATAGÈME D'EXTORSION DE PLUS EN PLUS RÉPANDU

Stéphanie Gohier-Coulombe et Karine Benoit | Mouvement Desjardins

Les attaques par des logiciels de rançon se caractérisent par l'intrusion dans votre ordinateur d'un logiciel malveillant qui chiffre toutes vos données. Pour les récupérer, les fraudeurs vous demandent de payer une rançon. Ce qu'ils veulent, c'est votre argent.

2 PERSONNES SUR 5 VONT SE FAIRE PRENDRE

Bien que la grande majorité des compagnies s'engagent à protéger les adresses de courriel de leurs clients, il arrive que ces listes se retrouvent entre les mains de fraudeurs. Dès lors, installer le rançongiciel sur l'ordinateur de quiconque se fait piéger par un courriel d'hameçonnage devient un jeu d'enfant pour ces fraudeurs.

En effet, les fraudeurs utilisent l'envoi de courriels d'hameçonnage qui incluent des fichiers Office Word (.doc et .rtf), des fichiers PDF ou un hyperlien qui, lorsqu'ils sont ouverts, permettent de chiffrer les données de votre ordinateur et de le verrouiller.

Trop tard… Comment réagir ?

Selon Jean-Yves Riverin, conseiller en sécurité au Centre de surveillance de la sécurité du Mouvement Desjardins, il est préférable de ne jamais payer la rançon aux fraudeurs pour récupérer ses données, car il arrive souvent, malgré un paiement, que les fraudeurs ne vous rendent jamais la clé de déchiffrement. C'est une roue sans fin qui vous obligera à donner de plus en plus d'argent sans nécessairement récupérer vos données.

Bien qu'il soit trop tard pour récupérer toutes vos données, Jean-Yves Riverin conseille de retirer dès que possible le câble réseau, de préparer votre ordinateur à un reformatage ou de repartir d'une copie de sauvegarde. D'où l'importance de faire des copies de sauvegarde régulièrement sur un support externe à l'ordinateur et de maintenir les logiciels à jour sur votre poste de travail.

6 CONSEILS POUR ÉVITER LES PIÈGES ET LES ATTAQUES

1. Assurez-vous que tous les logiciels (y compris Windows, les navigateurs, Java et Adobe) sont tenus à jour et que tous les correctifs sont installés.
2. Sauvegardez régulièrement vos données, préférablement sur un autre appareil et non dans votre ordinateur lui-même.
3. Ne cliquez pas sur des liens et n'ouvrez pas de fichiers contenus dans des courriels provenant de sources inconnues ou peu fiables.
4. Assurez-vous de tenir à jour votre logiciel antivirus.
5. Ne téléchargez pas et n'installez pas de logiciels provenant de sources inconnues ou peu fiables.
6. Ne cliquez jamais dans une fenêtre contextuelle qui affirme que votre ordinateur est infecté par un virus.

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 : Direction Design graphique et Publicité – Mouvement Desjardins.