MARS 2023 | VOL.3

CAHIER SPÉCIAL POUR LA PRÉVENTION DE LA FRAUDE

Mars, mois de la prévention de la fraude

Voyez comment vous pouvez prévenir la fraude financière.

Plus vous serez informé, moins les fraudeurs pourront vous arnaquer!

EN MARS, ON PARLE DE PRÉVENTION

Les conseils d'Otonom Solution

On entend de plus en plus parler de fraude, de vols de données ou d'identité. Il ne se passe pas un mois sans qu'on reçoive un courriel nous avisant de fuite de données, qu'on entende aux nouvelles qu'une entreprise a été fraudée ou qu'il y a eu un vol massif de données. C'est tellement devenu fréquent que cela en paraît malheureusement presque banal.

Le mois de mars, désigné comme le mois de la prévention de la fraude, vient nous rappeler collectivement que la fraude est tout sauf banale et que la prévention est l'affaire de tous.

Chaque année, Otonom Solution se donne pour mission d'aider sa clientèle et ses partenaires avec de judicieux conseils en matière de prévention de la fraude en paiement.

COMMENT SE PROTÉGER CONTRE LES FRAUDEURS?

Une affaire de tous

L'avènement des nouvelles technologies a ouvert le monde à des possibilités qu'on aurait jugé impossibles il n'y a pas si longtemps. Ce progrès qui nous rend la vie si facile, a également contribué à créer de nouvelles avenues d'arnaques et de tentatives de fraude.

Les entreprises de toutes tailles ainsi que les individus, peuvent faire l'objet d'une tentative de fraude. La question n'est pas de savoir si on fera face à une tentative de fraude, mais plutôt quand cela arrivera.

Le meilleur moyen de se prémunir contre la fraude est de se tenir informé et de partager ses connaissances autour de soi. En entreprise, on insistera jamais assez sur la notion de prévention.

- Ne confiez pas toutes les tâches à la même personne.
- Mettez en place des politiques et des normes et ce, même si vous êtes une petite entreprise de quelques employés.
- N'hésitez pas à investir dans de la formation en matière de prévention de la fraude pour vos employés.
- Révisez annuellement votre plan et vos stratégies en matière de prévention de la fraude. Les fraudes évoluent, votre plan doit aussi évoluer.
- Révisez et testez votre plan d'intervention dans le cas d'une fraude. Soyez préparé pour réagir plus rapidement.

ASSUREZ-VOUS QUE VOUS AVEZ DES PROCÉDURES EN PLACE ET QUE VOS EMPLOYÉS LES APPLIQUENT.

LA MAJORITÉ DES FRAUDES SONT DIFFICILES À DÉCELER AVANT QU'IL NE SOIT TROP TARD.

SOYEZ PRÉVENTIF AVANT DE DEVOIR ÊTRE RÉACTIF!

FRAUDE À LA LOCATION D'UN LOGEMENT

Une arnaque qui fait mal

Les médias sociaux offrent une belle vitrine pour les propriétaires qui mettent leurs logements à louer. On ajoute une description, quelques photos et le tour est joué. Il en va de même pour les condos à vendre. La visibilité est grande et les réponses sont nombreuses.

Les fraudeurs ont vu l'opportunité de monter une arnaque facile. On prend les photos et la description d'un condo à vendre et on fait une annonce de condo à louer avec un prix très attractif sur une autre plateforme.

Le faux propriétaire explique par exemple que le condo à louer était occupé par son enfant lors de ses études et qu'il n'est pas prêt à le vendre tout de suite. Comme la visite doit être faite par l'enfant maintenant déménagé dans une autre ville, il demande un dépôt de garantie par virement en précisant que la réponse à la question ne sera donnée qu'à la signature du bail.

Les locataires potentiels sont enchantés par les photos et le prix. Ce qu'ils ne savent pas c'est que la fonction "dépôt automatique" offerte par certaines institutions financières a été activée du côté du fraudeur. Lors du virement, le locataire potentiel est avisé par un message que le destinataire recevra les fonds sans besoin de répondre à la question de sécurité, mais ça peut facilement passer inaperçu dans la précipitation et l'excitation d'avoir trouvé la perle rare. Une fois l'argent envoyé, c'est trop tard. Le locataire potentiel est tombé dans le panneau et le faux propriétaire coupe les communications et passe au suivant.

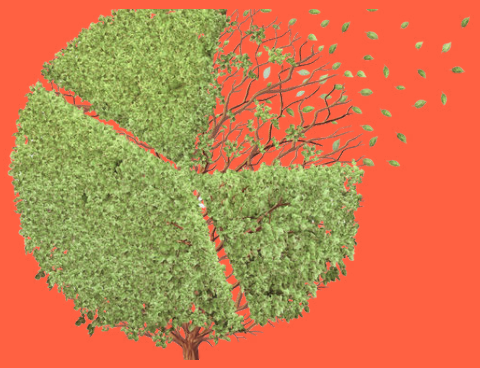
Trucs et conseils

- Attention si les photos sont incroyables et que le prix du loyer est vraiment bas. Quand c'est trop beau pour être vrai...
- Faites une recherche web avec l'adresse du logement.
- Les dépôts de garantie sont interdits au Québec.

FAUX TEXTO OU FAUX COURRIEL DE VOTRE PATRON

Il est de plus en plus facile de modifier l'affichage d'un numéro de téléphone pour faire croire qu'il vient d'une agence reconnue ou de votre patron. Même chose pour les courriels.

Méfiez-vous de toute demande urgente pour fournir des documents confidentiels, de faire un paiement urgent ou d'acheter des cartes cadeaux. Prenez le temps de vérifier cette demande, surtout si elle sort de l'ordinaire. On ne le répètera jamais assez, la vigilance peut vous empêcher d'être victime de fraude. Dans le pire des cas, votre patron verra que vous prenez la prévention de la fraude au sérieux et dans le meilleur des cas, vous aurez empêché l'entreprise d'être victime d'une fraude.



EN DATE DU 31 JANVIER 2023

SIGNALEMENTS DE FRAUDE:
6 610
(91 190 EN 2022)

VICTIMES DE FRAUDE:
3 923
(57 055 EN 2022)

EN PERTES FINANCIÈRES LIÉES AUX FRAUDES :
43.6 M$
(531 M$ EN 2022)

Source
Centre antifraude du Canada
https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

FRAUDE AUX PAIEMENTS DES FOURNISSEURS

Jamais deux... sans trois

Pour la troisième année consécutive, la fraude aux paiements des fournisseurs tient une place importante dans notre cahier spécial. Cela tient du fait que cette fraude est toujours très active et fait malheureusement encore des victimes.

Le stratagème est simple, se faire passer pour le fournisseur de façon à faire modifier les coordonnées bancaires pour le paiement d'une facture, afin de détourner celui-ci. En plus d'usurper l'identité d'un fournisseur, le fraudeur ajoute la notion d'urgence, afin que le paiement se fasse rapidement, diminuant ainsi les chances de se faire prendre.

Comment se protéger contre ce type de fraude? Avoir un plan établi pour le paiement de vos fournisseurs et s'y tenir!

Même si les points suivants sembleront être l'évidence même, sachez que dans l'action, on peut vite devenir déstabilisé. Le plan devient donc important, afin de ne pas se faire entraîner malgré nous dans une fraude.

- Ne modifiez jamais les coordonnées de paiement sous simple réception d'un courriel ou d'un appel. Prenez le temps d'appeler le fournisseur en utilisant les coordonnées présentes à vos dossiers.
- Ne modifiez jamais l'adresse ou le courriel d'un fournisseur sans vérification préalable que la demande vient bien de votre fournisseur.
- Soyez attentif aux incohérences. Par exemple, un texte dans un français douteux, de nombreuses fautes, un changement de gabarit de facture ou de courriel.
- Toute demande d'ajustement de facture à la hausse après la réception de celle-ci devrait vous alerter.
- Demandez l'avis d'un/une collègue.
- Prenez le temps AVANT de perdre de l'argent.
- En cas de doute.. il n'y a pas de doute. Vérifiez avec votre fournisseur.

NE NÉGLIGEZ PAS LA FORMATION DE VOS EMPLOYÉS CONCERNANT LES RISQUES LIÉS À LA FRAUDE.

ON N'EST JAMAIS ASSEZ PRÉPARÉ ET OUTILLÉ QUAND ON EFFECTUE DES TRANSACTIONS FINANCIÈRES.

VOUS NE SAVEZ PAS PAR OÙ COMMENCER?

DEMANDEZ DE L'AIDE. DE NOMBREUX OUTILS SONT DISPONIBLES ET DES FIRMES SE SPÉCIALISENT DANS CE GENRE DE FORMATION.

LE FAUX TECHNICIEN RÉINVENTÉ

Une arnaque qui se raffine.

L'arnaque du faux technicien informatique existe depuis déjà longtemps. Presque tout le monde a déjà reçu un appel d'un technicien tenace au français douteux, qui nous informe que notre ordinateur est infecté et qu'il doit intervenir immédiatement.

Peut-être un peu essoufflée parce qu'on en a beaucoup parlé, cette arnaque a évolué. Le centre antifraude du Canada nous avise qu'une variante est apparue dans laquelle les fraudeurs envoient une fausse facture de renouvellement à un abonnement d'anti-virus. Le courriel comporte un numéro de téléphone pour annuler le service ou pour régler le problème de non-paiement. C'est en composant le numéro que le faux technicien entre en scène et vous demande d'accéder à votre ordinateur à distance pour vous aider avec votre problème et par la même occasion, tenter de voler vos données.

- N'acceptez les demandes de support à distance que des personnes ou entreprises que vous connaissez.
- N'accédez à aucune information personnelle (courriel, compte bancaire etc.) durant une session de support à distance ou lorsque vous partagez votre écran.
- **Ne cédez pas sous la pression du faux technicien.**

FONDS RÉCUPÉRÉS GRÂCE À L'AIDE DU CAFC EN 2022

2 883 792$

Source
Centre antifraude du Canada
https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

MOTS DE PASSE

Ne faites pas de recyclage. N'utilisez pas le même mot de passe pour tous vos comptes.

Utilisez des mots de passe complexes et même des phrases de passe. 8 caractères MINIMUM.

Utilisez un gestionnaire de mots de passe.

Mélangez des chiffres, lettres majuscules, lettres minuscules et caractères spéciaux.

Si vous devez changer votre mot de passe à cause d'un bris de sécurité, ne vous contentez pas d'ajouter un caractère. Changez complètement le mot de passe.

Soyez créatif et non prévisible dans votre choix de mot de passe.

QUIZ

TESTEZ VOS CONNAISSANCES

10 questions sur la cybersécurité.
Quiz du Gouvernement du Canada.

GO

Otonom Solution est une entreprise canadienne dûment accréditée par les autorités réglementaires et qui est au cœur de vos opérations depuis 2008. Elle propose une solution de paiement sécurisée innovante qui joint divers outils de productivité à son approche unique de gestion de comptes et d'institutions financières multiples par un seul et même accès.

4 Place Ville-Marie, 3e étage
Montréal, QC, H3B 2E7
1 855 OTONOM1
info@otonomsolution.com

Rédaction et design graphique
Caroline Brodeur, CISA

Révision
Jean Salvador
Lyne Sylvain
Sylvie Robitaille

Traduction
Dianne Shea

Communication
Wafia Kanzari

L'ACCRÉDITATION EN TRANSFERT DE FONDS PAR REVENU QUÉBEC

Un permis à vérifier

Revenu Québec émet un permis aux entreprises dûement certifiées en matière de transfert d'argent. Ne vous fiez pas aux belles paroles qu'on vous dit et vérifiez!

C'est simple, facile et gratuit. Vous n'en serez que gagnant de le faire!

Otonom Solution est fier de pouvoir affirmer être pleinement accrédité. Vérifiez ici

LE CENTRE ANTIFRAUDE DU CANADA (CAFC)

Un site à garder dans ses favoris

Le Centre antifraude du Canada est géré conjointement par la GRC, le Bureau de la concurrence et la Police provinciale de l'Ontario.

On y trouve beaucoup d'informations sur les fraudes qui circulent et sur les moyens de s'en prévenir. Le meilleur moyen de se protéger est de s'informer.

VOUS PENSEZ AVOIR ÉTÉ VICTIME DE FRAUDE ?

- Restez calme. Paniquer ne vous aidera pas.
- Rassemblez le plus de preuves possibles: documents, courriels, textos, relevés d'appels, témoignages d'employés, etc.
- En cas d'hameçonnage, changez immédiatement vos mots de passe et activez l'authentification à deux facteurs.
- En cas de fraude du président (haut dirigeant) avisez vos employés que quelqu'un se fait passer pour vous et changez vos mots de passe.

EN CAS DE FRAUDE FINANCIÈRE, VOUS DEVEZ AUSSI CONTACTER

- Votre institution financière ET/OU VOTRE FOURNISSEUR DE PAIEMENT.
- Le Centre antifraude du Canada au 1 888 495-8501 ou en ligne au www.antifraudcentre-centreantifraude.ca.
- Votre poste de police local afin de dénoncer la fraude.