www.antifraudcentre-centreantifraude.ca /protect-protegez-fra.htm

Protégez-vous contre les fraudes

Tous les Canadiens et les entreprises canadiennes peuvent devenir la cible de fraudeurs. Voici quelques conseils et trucs pour vous protéger ou protéger votre entreprise contre les fraudes.

N'oubliez pas que si c'est trop beau pour être vrai, ça l'est.

Sur cette page

Particuliers

N'ayez pas peur de dire non

Ne vous laissez pas intimider par les tactiques de vente sous pression.
Si un agent de télémarketing tente de vous convaincre d'acheter quelque chose ou de lui envoyer de l'argent immédiatement :

- Demandez l'information par écrit;
- Raccrochez.

Méfiez-vous des demandes urgentes qui jouent avec vos émotions.

Faites vos recherches

Vérifiez toujours que l'organisation avec laquelle vous faites affaire est légitime avant de prendre toute autre mesure :

- Vérifiez que l'organisme de bienfaisance canadien est enregistré auprès de l'Agence du revenu du Canada.
- Confirmez l'existence de l'agence de recouvrement auprès de l'organisme provincial compétent.

- Faites des recherches en ligne pour trouver les coordonnées de l'entreprise qui vous a apparemment téléphoné et appelez-la pour confirmer.
- Vérifiez la légitimité des appels en composant le numéro de téléphone qui figure au dos de votre carte de crédit.

Si vous recevez un appel ou des nouvelles d'un membre de votre famille qui a besoin d'aide, confirmez la situation en parlant à d'autres proches.

Méfiez-vous des fausses annonces, des annonces trompeuses et des faux courriels. Vérifiez toujours la légitimité de l'entreprise et de ses services avant de communiquer avec elle.

Ne donnez pas de renseignements personnels

Méfiez-vous des appels non sollicités où l'on vous demande des renseignements personnels comme :

- votre nom;
- votre adresse;
- votre date de naissance;
- votre numéro d'assurance sociale;
- votre numéro de carte de crédit ou vos données bancaires.

À moins d'être l'auteur de l'appel, vous ne savez pas à qui vous parlez.

Sachez comment protéger votre numéro d'assurance sociale (NAS).

Sachez à quoi vous attendre lorsque l'Agence du revenu du Canada communique avec vous.

Méfiez-vous des frais initiaux

Bien des fraudeurs vous demanderont de payer des frais avant de recevoir des biens, des services ou un prix.
Il est illégal pour une entreprise de demander des frais initiaux avant de vous accorder un prêt.

Sachez qu'au Canada, il n'y a pas de frais ni de taxes qui s'appliquent aux prix.
Si vous gagnez quelque chose, vous le recevez gratuitement.

Protégez votre ordinateur

Faites attention aux messages qui ont l'air urgents et qui apparaissent pendant que vous naviguez en ligne.
Ne cliquez pas sur ces messages et ne composez pas le numéro fourni.

Aucune entreprise légitime ne vous appellera pour vous informer que votre ordinateur est infecté.

Certains sites Web, comme ceux où il est possible de télécharger de la musique, des jeux, des films ou du contenu réservé aux adultes, peuvent entraîner l'installation de virus ou de programmes malveillants à votre insu.
Méfiez-vous aussi des courriels qui renferment des fautes d'orthographe et des erreurs de mise en forme et abstenez-vous de cliquer sur les pièces jointes ou les liens, car ils peuvent contenir des virus et des logiciels espions.

Assurez-vous d'avoir un logiciel antivirus et de garder votre système d'exploitation à jour.

Ne permettez jamais à quiconque d'accéder à votre ordinateur à distance.
Si vous éprouvez des problèmes avec votre système d'exploitation, apportez-le à un technicien près de chez vous.

Faites attention à qui vous transmettez des photos

Réfléchissez bien avant de transmettre des vidéos ou des images explicites à des personnes.
Ne vous livrez pas à des actes explicites en ligne.

Désactivez votre caméra Web ou tout autre type de caméra branché à Internet lorsque vous ne l'utilisez pas.
Des pirates informatiques sont capables d'accéder à votre ordinateur à distance et d'enregistrer des images à partir de votre appareil.

Protégez vos comptes en ligne

En prenant les mesures suivantes, vous pourrez mieux protéger vos comptes en ligne contre la fraude et les fuites de données :

- Créez des mots de passe difficile à deviner :
  - utilisez un mot de passe comportant au moins huit caractères (lettres majuscules et minuscules) et au moins un chiffre et un symbole.
  - créez des mots de passe uniques pour chaque compte en ligne, y compris les comptes des réseaux sociaux, de courriel, financiers et autres.
  - utilisez une combinaison de phrases passes faciles à retenir pour vous, mais difficiles à deviner pour les autres.
- Activez l'authentification multifacteur.
- Accédez à vos comptes qu'à partir de sources fiables.
- Ne révélez pas de renseignements personnels dans les médias sociaux.

Pour en savoir plus sur les façons de protéger vos comptes, consultez le site de Pensez cybersécurité.

Reconnaître la mystification

La mystification est utilisée par les fraudeurs pour tromper les victimes et les convaincre qu'elles communiquent avec des personnes honnêtes ou des entreprises ou des organisations légitimes.

Voici les principales variations de cette technique utilisées par les fraudeurs :

Falsification des données de l'appelant
: Les fraudeurs peuvent manipuler le numéro de téléphone apparaissant sur l'afficheur (que ce soit par appel téléphonique ou par texto). Ils peuvent faire en sorte que s'affichent des numéros de téléphone légitimes d'organismes d'application de la loi, d'institutions financières, d'organismes gouvernementaux ou de fournisseurs de service.

Faux courriel
: Un peu comme ils le font avec les données de l'appelant, les fraudeurs peuvent manipuler l'adresse de courriel de l'expéditeur afin de faire croire à la victime qu'elle reçoit un courriel d'une source légitime.

Faux site Web
: Les fraudeurs créent de faux sites Web qui semblent légitimes.
Il peut s'agir de faux sites Web d'institutions financières, d'entreprises offrant des emplois, de sociétés de placement ou d'organismes gouvernementaux.
Dans bien des cas, les fraudeurs utilisent un nom de domaine ou une adresse URL de site Web semblable à celui d'une organisation ou d'une entreprise légitime, avec une différence mineure dans l'orthographe.

Pour vous protéger

- Ne présumez jamais que les numéros de téléphone qui apparaissent sur votre afficheur sont authentiques.
- Si vous recevez un appel d'une personne affirmant travailler pour votre institution financière, un organisme d'application de la loi ou un fournisseur de services, raccrochez et appelez vous-même l'organisme ou l'entreprise.
- Si vous recevez un texto ou un courriel, communiquez directement avec l'entreprise ou l'organisme en question.
  Assurez-vous de vérifier leurs coordonnées et n'utilisez pas l'information fournie dans le premier message reçu.
- Ne cliquez jamais sur des liens reçus par texto ou par courriel.
- Au moment de consulter un site Web, vérifiez toujours l'adresse URL et le domaine pour vous assurer qu'il s'agit du site Web officiel.

Entreprises

Sachez à qui vous avez affaire

Gare aux factures sur lesquelles figurent le nom d'entreprises légitimes.
Les fraudeurs utilisent des noms de véritables entreprises comme les Pages jaunes pour que les factures semblent authentiques.
Examinez soigneusement les factures avant d'effectuer un paiement.

Dressez une liste des entreprises avec qui vous faites généralement affaire pour aider les employés à distinguer les vrais contacts des faux.

Ne donnez pas de renseignements lors d'appels non sollicités

Apprenez aux employés de tous les échelons à se méfier des appels non sollicités.
S'ils ne sont pas l'auteur de l'appel, ils ne devraient pas fournir ni confirmer :

- l'adresse de l'entreprise;
- le numéro de téléphone de l'entreprise;
- des numéros de compte;
- des renseignements au sujet du matériel de bureau (p. ex. marque et modèle de l'imprimante).

Limitez les pouvoirs de vos employés

N'autorisez que quelques employés à approuver les achats et à régler les factures.

Surveillez les anomalies

Méfiez-vous :

- des commandes plus grosses que la normale;
- des commandes multiples du même produit;
- des commandes de gros achats.

Ces commandes pourraient être frauduleuses.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230819
"C'est ensemble qu'on avance"