PRÉVENTION DE LA FRAUDE EN LIGNE

Naviguer en sécurité

Nous ne serons jamais complètement à l'abri des gens malveillants qui veulent usurper notre identité ou nos comptes en banque. Par contre, nous pouvons leur rendre la tâche plus difficile. Voici donc nos conseils pour mettre les chances de votre côté !

Ne faites jamais de transactions sur des sites web non sécurisés. Assurez-vous de repérer l'icône de cadenas dans la barre de recherche ou que l'URL débute par HTTP**S**.

option-consommateurs.org

Ne transigez jamais via un ordinateur ou un réseau wifi public. Le wifi public est non sécurisé, il est donc beaucoup plus facile pour des gens mal intentionnés d'intercepter vos transactions et d'avoir accès à vos informations en ligne. Que ce soit pour acheter des vêtements ou pour vous connecter à votre banque, attendez donc d'être de retour à la maison !

Ayez des mots de passe sécuritaires.

1. Variez vos mots de passe. En utilisant toujours le même, vous facilitez la tâche des gens malveillants.

2. Évitez les mots de passe de type 1111, 1234, dates de fête (la vôtre ou celle de vos enfants), nom de votre animal de compagnie, adresse, numéro de téléphone…

3. Employez les suggestions du navigateur lorsque vous créez un nouveau mot de passe. Elles sont très robustes et vous évitent de recourir à votre imagination pour créer un mot de passe sécuritaire.

4. Les phrases en guise de mot de passe, une bonne idée ! Utilisez des trucs mnémotechniques et transformez-les en mots de passe. Par exemple, « Hier, j'ai acheté 2 baguettes chez l'épicier à Notre-Dame-de-Grâce ! » = Hja2bcéàNDG !

Vous craignez d'oublier vos mots de passe ?

- Considérez l'utilisation d'un gestionnaire de mots de passe. Cela permet d'enregistrer tous vos mots de passe dans un seul système et de les entrer automatiquement dans les champs requis au besoin. Vous n'avez qu'à en créer et retenir qu'un seul.

- Si vous souhaitez noter vos mots de passe sur un document papier, assurez-vous que vous le laisserez dans un endroit caché et sécurisé de la maison.

Activez l'authentification à 2 facteurs autant que possible. Oui, c'est une étape supplémentaire pour vous connecter à vos comptes, mais vous serez bien contents lorsque cela vous sauvera d'une fraude ou du piratage de vos réseaux sociaux !

Ne négligez pas l'importance d'un antivirus. Installez-le et mettez-le à jour lorsqu'il le faut.

Restreignez le plus possible le partage de vos renseignements personnels. Pour en savoir plus à ce sujet, cliquez ici !

OPTION consommateurs

Avec la participation financière de :

Justice Québec