

# Méfiez-vous des escroqueries : faites les recherches et protégez-vous!

## 1. L'auteur du courriel, du message texte ou du message téléphonique automatisé que vous avez reçu prétend-il représenter l'ARC?

L'ARC ne communique jamais avec vous par message texte et ne vous demande jamais de renseignements financiers par courriel. Elle n'utilise jamais non plus un vocabulaire intimidant et ne menace jamais de vous faire arrêter ou de vous dénoncer. Elle peut vous demander, au téléphone, certains renseignements, sans toutefois jamais vous obliger à agir ou à payer tout de suite. Ne laissez pas les escrocs vous effrayer!

## 2. Une entreprise vous demande-t-elle des renseignements personnels au téléphone ou en ligne?

On reçoit souvent des courriels ou des appels téléphoniques prétendument envoyés ou passés par des entreprises de grande notoriété, par exemple une banque ou une compagnie de téléphone. On peut par exemple vous demander votre nom et votre prénom ou votre numéro d'assurance sociale. Ne donnez jamais d'information par courriel ni au téléphone, à moins que l'on vous appelle d'un numéro que vous connaissez et qui est digne de confiance. En cas de doute, raccrochez, faites des recherches, et communiquez vous-même avec l'entreprise afin de confirmer la raison pour laquelle on vous a appelé(e).

## 3. Le courriel ou le message texte vous est-il prétendument adressé par un organisme authentique, et vous invite-t-on à cliquer sur un lien pour vérifier des renseignements personnels?

Les organismes authentiques ne vous demandent jamais de vérifier de l'information en ligne. Ne cliquez pas sur les liens proposés, même si c'est pour vous désabonner ou vous désinscrire. Communiquez avec l'organisme sur son site Web ou en personne pour confirmer qu'il y a effectivement des renseignements à vérifier.

## 4. Restez sur vos gardes quand vous faites des emplettes en ligne. Faites des vérifications pour savoir si un lien vous mène à un autre site Web avant d'acheter un produit.

N'achetez jamais un produit en cliquant sur un lien qui n'est pas associé à un site Web authentique, par exemple eBay. En cas de problème de paiement ou si vous ne recevez jamais le produit, ce site Web ne vous protège pas. Pour savoir si un site Web est sécurisé, assurez-vous que le lien porte le préfixe « https », précédé du symbole du cadenas.

## **5. Un site Web vous invite-t-il à taper les renseignements sur votre carte de crédit pour un essai « gratuit »?**

Des entreprises affirment qu'elles ne commencent à prélever les fonds sur votre carte que si vous n'annulez pas le service à la fin de la période de l'essai gratuit. Or, en tapant les renseignements sur votre carte de crédit, vous vous engagez souvent à payer. Assurez-vous de lire le texte en petits caractères et la politique sur l'annulation avant de donner ces renseignements. Consultez les critiques portant sur l'entreprise et le produit.

## **6. Une publicité fait-elle valoir qu'on peut vous envoyer des compléments alimentaires ou des médicaments sans ordonnance?**

Les produits offerts sur les sites Web qui s'affichent comme des pharmacies en ligne ne sont sans doute pas authentiques ou pourraient même être nocifs pour votre santé. Rappelez-vous qu'il faut quand même une ordonnance pour commander des produits auprès de pharmacies en ligne authentiques. Assurez-vous de faire des vérifications sur l'entreprise avant d'acheter des produits.

## **7. Une publicité vous invite-t-elle à prendre une décision précipitée?**

Le libellé de certaines publicités, souvent diffusées en ligne ou par courriel, vous invite à acheter tout de suite un produit. Ces publicités font souvent valoir que le prix ou l'offre est valable « pour une durée limitée seulement ». Ne vous inscrivez pas ou n'achetez pas le produit offert sans d'abord lire les critiques sur l'entreprise ou le produit.

## **8. Une publicité propose-t-elle un remède qui permet de se rétablir rapidement d'un grave ennui de santé?**

Les publicités proposent souvent des produits qui permettent soi-disant de corriger un problème de santé ou de donner des résultats rapides. Il peut s'agir de compléments pour maigrir et de traitements capillaires. N'achetez jamais lorsqu'on vous presse de le faire, surtout s'il s'agit d'une vente à tempérament qui s'étend sur une longue durée. Et rappelez-vous que les traitements « miracles » n'existent pas. Faites des recherches!

## **9. Un vendeur itinérant vous presse d'acheter un service ou un produit le jour même?**

Les artistes de la fraude font souvent appel à des tactiques très insistantes pour vous convaincre de faire des achats importants le jour même. Il peut s'agir d'un chauffe-eau ou d'autres produits dont le prix est élevé. Il se peut qu'on ne vous livre jamais ce que vous avez acheté ou qu'on vous livre des produits de qualité inférieure. Les vendeurs authentiques n'insistent pas pour que vous achetiez. Prenez la peine de noter le nom du vendeur et celui de l'entreprise. Ne donnez jamais, à un vendeur itinérant, de documents renfermant des renseignements personnels, par exemple des copies de facture. Prenez le temps de faire des recherches sur les produits offerts avant de les acheter.



## 10. Quelqu'un, que vous avez connu sur un site de rendez-vous, vous demande-t-il de lui envoyer de l'argent?

Certaines personnes sont parfois très convaincantes quand vient le temps de vous exprimer leurs sentiments, surtout en ligne. Restez sur vos gardes : il pourrait s'agir d'imposteurs. Ces personnes pourraient par exemple vous dire qu'elles ont besoin d'argent de toute urgence ou qu'elles veulent prendre l'avion pour vous rendre visite. N'envoyez jamais d'argent à quelqu'un que vous ne connaissez qu'en ligne.

## 11. Une personne avec laquelle vous communiquez prétend-elle être le PDG de l'entreprise pour laquelle vous travaillez?

Cette manœuvre frauduleuse est répandue et s'adresse aux employés qui ont accès aux fonds de l'entreprise. Si vous recevez un courriel qui vous est prétendument adressé par un cadre supérieur ou le PDG et qu'on vous demande d'envoyer des fonds à un tiers pour conclure une affaire ou un contrat, méfiez-vous. Confirmez la transaction en personne. Invitez votre employeur à adopter un protocole normalisé pour les virements de fonds, afin de pouvoir dépister facilement ces fraudes.



### POUR EN SAVOIR PLUS

Pour en savoir davantage sur les différents types d'escroqueries ou de fraude, sur les moyens à prendre pour vous protéger et sur ce qu'il faut faire pour dénoncer les cas de fraude, nous vous invitons à consulter le site [Le petit livre noir de la fraude](#), le site du [Centre antifraude du Canada](#) ou le site de [l'Agence du revenu du Canada](#).

