

7 indices pour vous aider à détecter une arnaque



Pour parvenir à leurs fins, les fraudeurs ont recours à une multitude de stratagèmes : [hameçonnage](#), [arnaque amoureuse](#), [arnaque téléphonique](#), arnaque de l'[argent facile](#)... Bien que ces approches diffèrent, elles ont souvent recours à des techniques de manipulation pour déjouer la prudence.

Voici quelques indices à surveiller qui vous aideront à les reconnaître.

Il est facile de penser que la fraude et les arnaques n'arrivent qu'aux autres ou qu'on ne tombera pas dans le panneau.

Pourtant, les fraudeurs perfectionnent continuellement leur approche et savent se montrer habiles et convaincants.

En ayant quelques exemples de fraudes possibles en tête, il peut être plus facile de les reconnaître lorsque celles-ci se produisent.

Sans nécessairement connaître toutes les approches utilisées par les fraudeurs, considérez les signes ci-dessous comme une alerte pour vous **poser des questions et pour vérifier la légitimité du message auprès de sources fiables**.

1. C'est inattendu

Vous avez gagné un concours auquel vous ne vous êtes jamais inscrit?

Vous recevez un avis ou un texto pour un colis que vous n'avez pas commandé?

On vous appelle pour vous dire qu'il y a un problème avec votre ordinateur et qu'il doit être réparé?
Posez-vous la question : « Suis-je à l'origine de cette demande? ».

Desjardins envoie des courriels et des textos

Nous utilisons le courriel et les textos pour communiquer avec vous, mais seulement pour vous fournir de **l'information factuelle**.

Il est possible de recevoir un [message ou une alerte](#) vous avisant, par exemple, que votre relevé de compte est disponible ou que votre solde de carte de crédit est élevé.

Vous pourriez aussi recevoir un [texto](#) vous demandant de confirmer une tentative de connexion à votre compte ainsi que certaines transactions effectuées avec votre carte de crédit.

2. C'est vraiment urgent (et il y a une raison pour ça)

Qu'il soit question d'accepter une offre rapidement, de faire parvenir un paiement ou de fournir des renseignements, le **déla**i demandé est très court et peut faire miroiter des conséquences immédiates si aucune action n'est prise.

Cette pression vise à provoquer la panique et une action rapide, sans vous accorder le recul nécessaire pour vous questionner, pour effectuer vos recherches et pour reconnaître la supercherie.

3. Le ton est menaçant... ou au contraire, particulièrement courtois

Un discours qui joue sur la peur et qui est accompagné d'insultes ou de menaces (ex. : transaction très importante qui pourrait échouer, congédiement professionnel, dénonciation à la police, etc.) cherche à susciter des émotions fortes et à embrouiller l'esprit.

À l'inverse, certaines approches (comme les [arnaques amoureuses](#)) emploient plutôt un langage courtois et affectueux pour exploiter la vulnérabilité émotionnelle.

4. C'est anormal que l'on vous demande ça

Si l'on vous demande de fournir des informations personnelles ou confidentielles (ex. : mot de passe, numéro d'identification personnel [NIP], numéro d'assurance sociale, etc.), questionnez-vous sur l'utilité de cette demande en fonction de votre interlocuteur.

Ne divulguez jamais vos informations si vous n'avez pas fait l'appel.

Il est également anormal que l'on vous demande de remettre votre carte de crédit et de débit à quelqu'un ou de la déposer dans votre boîte aux lettres (comme c'est le cas pour [l'arnaque du faux conseiller et du faux facteur](#)).

Quoi faire en cas de doute?

Dans le cas d'une conversation téléphonique qui vous semble douteuse, prenez en note le nom de votre interlocuteur et **mettez fin à la conversation**.

Ne vous fiez pas à l'afficheur ou au numéro qui vous a été donné.

Communiquez vous-même avec l'entreprise ou l'instance gouvernementale en utilisant les coordonnées

reconnues sur les sites Web officiels ou provenant d'une source externe fiable (ex. : Canada 411, Autorité des marchés financiers, Registre des entreprises, ordre professionnel, etc.).

Si la communication s'avère frauduleuse, dénoncez-la auprès du [Centre antifraude du Canada](#).

5. La provenance du message a l'air louche

Le message est rempli de fautes ou de coquilles?

L'adresse courriel provient d'un service de messagerie gratuit ou ressemble au nom de l'entreprise auquel on a ajouté des caractères superflus?

De tels indices laissent croire que le message est plutôt une [tentative d'hameçonnage](#).

Que ce soit par courriel, sur les réseaux sociaux, par texto ou par téléphone, prenez une pause et questionnez-vous avant de cliquer sur un lien, d'ouvrir une pièce jointe ou de donner suite à des messages provenant de personnes ou d'entreprises que vous ne connaissez pas ou qui présentent d'autres signes d'une arnaque potentielle.

6. Ça a l'air trop beau pour être vrai

À moins qu'il s'agisse d'une enchère, demandez-vous s'il est normal qu'on vous offre beaucoup plus que le prix demandé pour un bien que vous vendez en ligne.

Vous proposer du matériel neuf ou presque neuf hautement recherché (ex. : console de jeu vidéo, vélo de performance, téléphone intelligent, etc.) à un prix ridicule l'est tout autant.

Gagner de « [l'argent facile](#) » ne se fait qu'aux dépens d'une victime.

Lorsqu'une proposition semble trop alléchante pour être vraie, faites confiance à votre instinct.

7. C'est ultrasecret

Un dirigeant de votre entreprise vous annonce en primeur une transaction majeure dont personne ne doit être informé?

Une personne dans le pétrin vous demande de l'argent en insistant sur le fait de ne pas aviser les autorités?

Ces directives visent plutôt à **éviter que vous parliez à quelqu'un** de votre entourage qui pourrait reconnaître le stratagème et vous mettre en garde.

Section Ma sécurité

Cette zone vous renseigne sur le niveau de sécurité de votre compte AccèsD et vous propose des façons de mieux vous protéger.

C'est un outil centralisé pour gérer votre mot de passe, vos questions de sécurité, vos appareils vérifiés ainsi que la validation en deux étapes.

[Découvrez la section Ma sécurité.](#)

Certaines victimes peuvent ressentir de la gêne, voire de la honte, après avoir été dupées et n'osent pas en parler.

Ça ne doit surtout pas être le cas.

Il est important d'en parler à votre entourage et d'aviser les autorités.

Les fraudeurs perfectionnent constamment leurs techniques pour manipuler leurs cibles afin de les prendre au piège.

Vous pouvez également communiquer avec nous si vous désirez obtenir un accompagnement ou préférez en parler en toute confidentialité, en composant le [1 800 CAISSES \(1 800 224-7737\)](tel:1800CAISSES)

Recherche et mise en page par:

Michel Cloutier

CIVBDL

20231013

"C'est ensemble qu'on avance"