

PRÉVENIR LE VOL D'IDENTITÉ



Le vol d'identité, c'est pas nouveau. Ça existe depuis très longtemps. On en entend plus parler de nos jours parce qu'avec Internet, les techniques se sont multipliées et surtout raffinées.

Le vol d'identité, c'est quelque chose qui se fait souvent à notre insu.

**IL Y A QUAND MÊME DES CHOSES À FAIRE POUR SE PROTÉGER.
VOICI QUELQUES PISTES!**

LE VOL D'IDENTITÉ... C'EST QUOI?

Le vol d'identité c'est lorsqu'une personne obtient et utilise, à votre insu et sans votre consentement, vos renseignements personnels à des fins criminelles.

Exemples de renseignements personnels recherchés par les voleurs:

- Votre nom
- Votre adresse
- Votre courriel
- Votre date de naissance
- Votre numéro d'assurance sociale
- Vos mots de passe
- Vos numéros de permis de conduire et de passeport



Les criminels peuvent utiliser vos renseignements pour :

- 01** Accéder à vos comptes bancaires pour faire des achats ou des retraits
- 02** Faire des demandes de prêts, de cartes de crédit, d'ouverture de comptes bancaires ou même obtenir un prêt hypothécaire
- 03** Obtenir un passeport ou toucher des prestations du gouvernement

COMMENT FONT-ILS?

Pour obtenir vos informations personnelles, les fraudeurs utilisent toutes sortes de techniques.

Ils peuvent :

1

Fouiller dans votre ordinateur à l'aide d'un logiciel espion

2

Voler vos lettres

3

Vous écrire des courriels (hameçonnage)



4

Vous appeler en se faisant passer pour une autre personne

5

Voler des documents dans vos poubelles ou dans votre bac de recyclage

6

Voler votre portefeuille

3

GROS PLAN SUR L'HAMEÇONNAGE

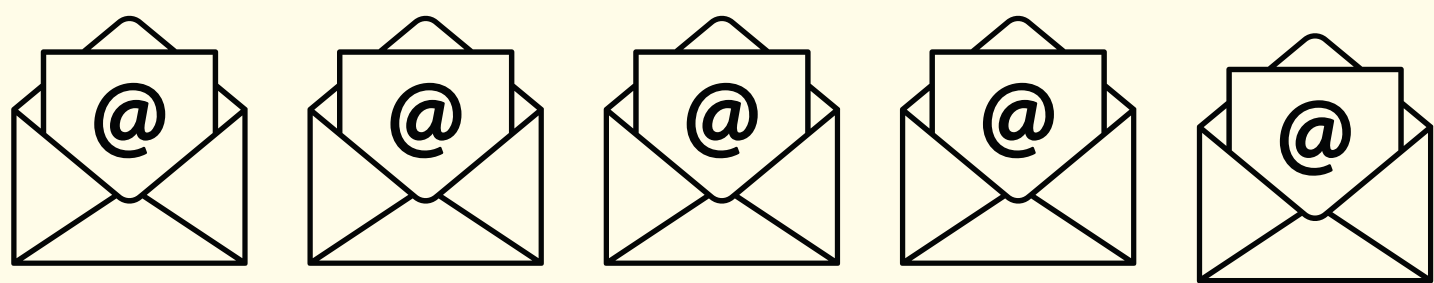
C'est quoi?

C'est une technique qui consiste à envoyer un message (courriel ou texto) en se faisant passer pour une entreprise ou un organisme légitime dans le but de vous amener à donner des renseignements personnels.

Ça peut être votre mot de passe, numéro de carte de crédit, numéro d'assurance sociale, etc.



Une arnaque très répandue



6,4 MILLIARDS

Nombre de courriels d'hameçonnage envoyés chaque jour dans le monde.

Ça fait plus de 2 000 milliards de courriels frauduleux par année

Source : Centre antifraude du Canada



2,46 MILLIONS \$

En 2021, l'hameçonnage a coûté 2,46 millions \$ aux Québécois.e.s et 21 millions \$ aux Canadien.ne.s

ZOOM SUR LES FUITES DE DONNÉES

Une fuite de données, c'est quand des informations confidentielles ou sensibles ont été consultées sans permission.

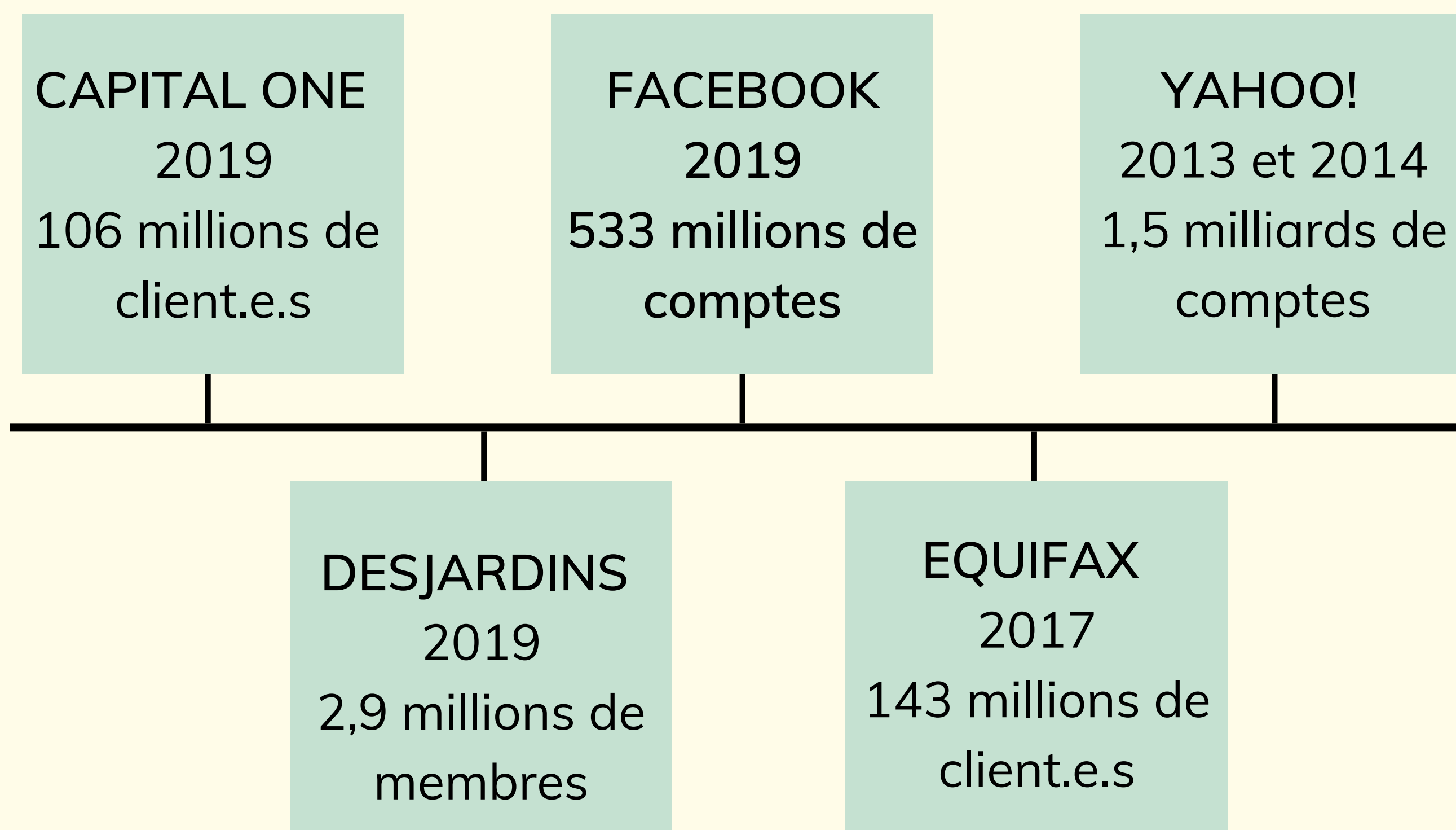
Le piratage ou les attaques de logiciels malveillants sont les principales causes de fuites de données dans les entreprises.

Elles peuvent aussi être le résultat d'une fuite interne (un employé qui vend des données, par exemple), de la perte ou du vol d'un disque dur physique contenant des fichiers, ou simplement d'erreur humaine.



Les fuites de données se sont multipliées dans le monde au cours des 10 dernières années.

Voici quelques exemples célèbres que vous connaissez peut-être...



Attention aux courriels et textos frauduleux!

À première vue, les messages d'hameçonnage ressemblent à n'importe quel autre courriel ou message texte.

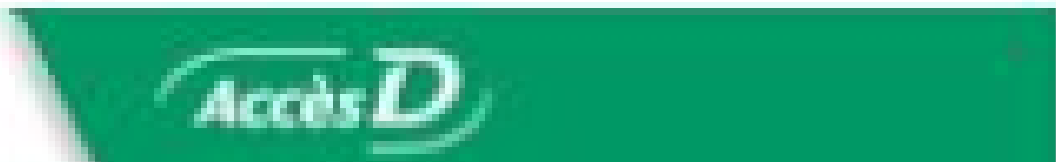
Mais certains signes ne trompent pas!

Mauvaise adresse courriel

Message non personnalisé

Présence de fautes d'orthographe

From: Service de securite Desjardins [flapadmi@flap.asso.fr]
Sent: 23 janvier 2007 03:11
To: [REDACTED]
Subject: Information Importante

A nos membres des caisses populaire Desjardins :

Nous avons remarqué que plusieurs tentatives d'accès à votre compte en ligne ont été commises dernièrement de sécurité, nous vous demandons de confirmer certaines informations et de vérifier vos transactions. Cette vérification doit être faite avant le 26 janvier 2007. Passé cette date, nous serons obligés de suspendre pour une période indéterminée afin d'éviter qu'une tierce personne puisse accéder à votre compte.

Pour accéder à votre compte et vérifier vos transactions, cliquez sur le lien :
<https://accesd.desjardins.com/>

Nous vous remercions de votre compréhension et coopération dans cette situation pour protéger votre identité.

Desjardins / AccèsD
Cojoigner avoirs et être

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

Copyright © 2007 Mouvement des caisses Desjardins. Tous droits réservés.

[Sécurité](#) | [Confidentialité](#) | [Con](#)

Lien douteux

Sentiment d'urgence

Menace

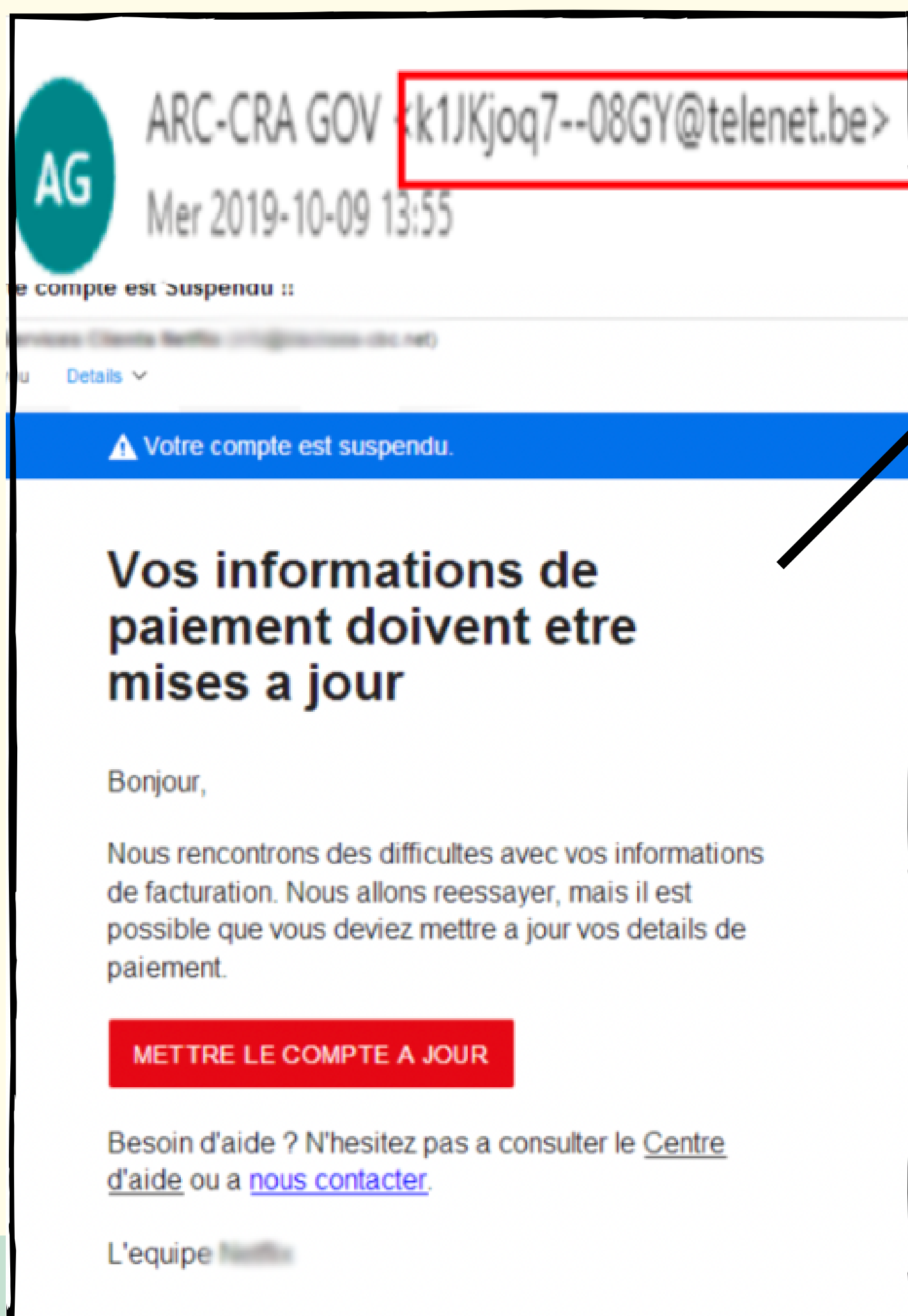
Reconnaître un message frauduleux

Pour vous inciter à donner vos informations personnelles, les fraudeurs utilisent toutes sortes de stratégies.

Voici quelques exemples :

SUSCITER UN SENTIMENT D'URGENCE

Les menaces de fermer vos comptes ou d'en limiter l'accès si vous ne répondez pas rapidement sont les signes d'une fraude par hameçonnage

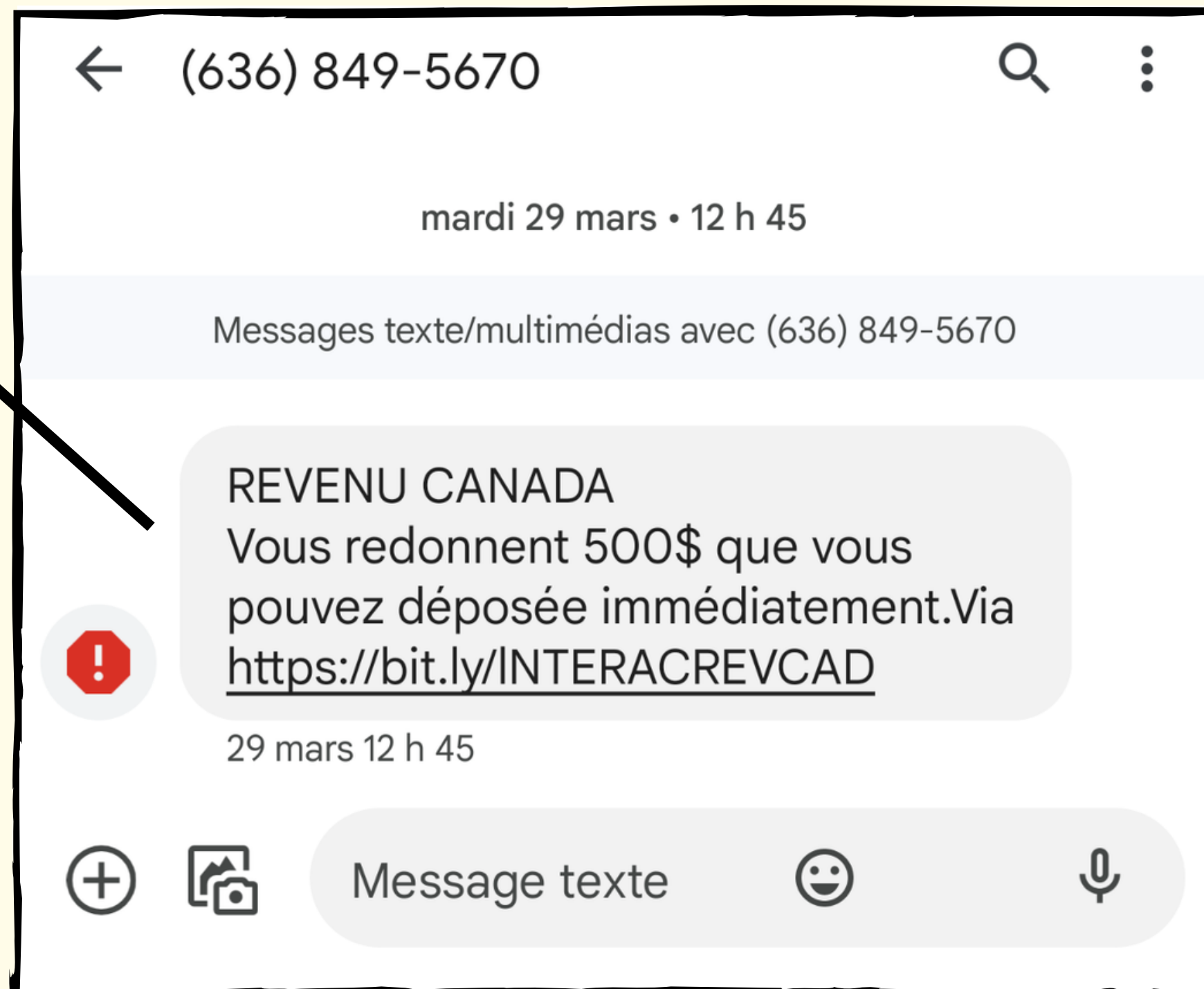


FAIRE CROIRE QU'IL Y A UN PROBLÈME

Tout message qui présente une situation obligeant à divulguer ses informations personnelles afin de résoudre un problème devrait être considéré comme suspect.

FAIRE MIROITER UN PROFIT

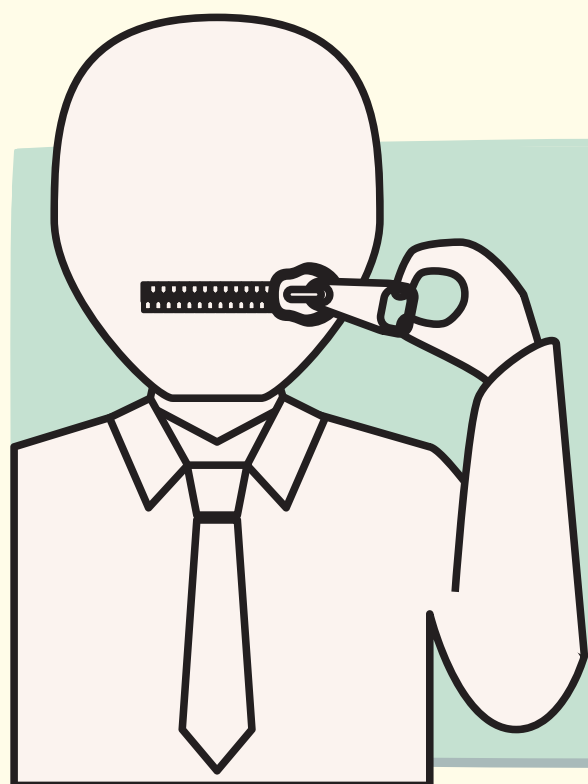
Les fraudeurs utilisent souvent cette stratégie pour vous inciter à donner vos renseignements personnels



PIQUER LA CURIOSITÉ
Dans le but de vous inciter à cliquer sur un lien ou d'ouvrir une pièce jointe.

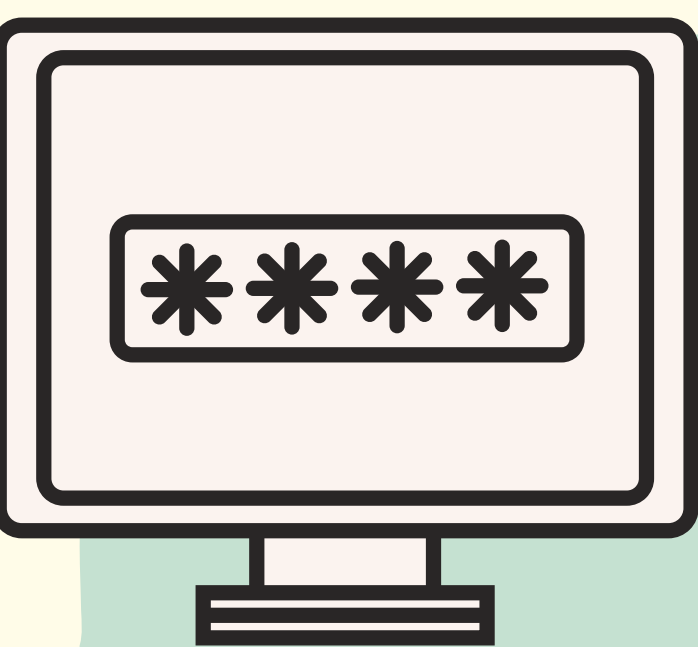
COMMENT SE PROTÉGER?

Un vol d'identité, ça peut nous coûter très cher.
Il est donc très important de protéger le plus possible nos renseignements personnels



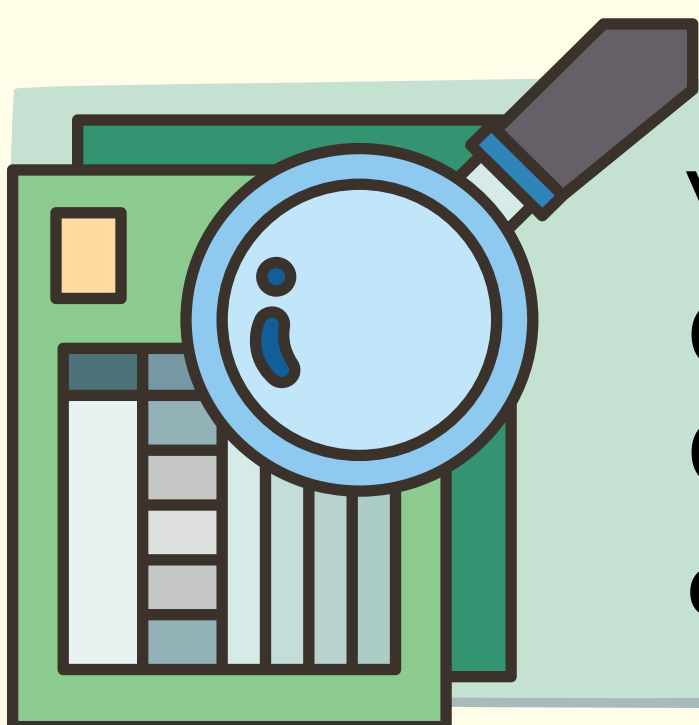
PROTÉGEZ VOS INFORMATIONS PERSONNELLES

Donnez-les juste si vous avez confiance en la personne qui vous les demande



CHOISISSEZ UN MOT DE PASSE FORT

Modifiez le souvent, n'utilisez pas toujours le même et gardez le secret



VÉRIFIEZ VOS RELEVÉS DE COMPTE ET DE CARTE DE CRÉDIT RÉGULIÈREMENT

Consultez votre dossier de crédit une fois par année et assurez-vous qu'il n'y a pas d'erreurs



GARDER LES DOCUMENTS IMPORTANTS DANS UN ENDROIT SÉCURITAIRE

Ne traînez pas votre carte d'assurance sociale avec vous et déchiquetez vos documents personnels



PROTÉGEZ VOTRE ORDINATEUR

Assurez-vous d'avoir un logiciel antivirus et de garder votre système d'exploitation à jour
Fermez toujours vos sessions

QUE FAIRE SI VOUS ÊTES VICTIME DE VOL D'IDENTITÉ?



RESTEZ CALME

Ça ne sert à rien de paniquer. Respirez et commencez les démarches!

RASSEMBLEZ TOUTE L'INFORMATION

Par exemple : documents, reçus, copies de courriels ou de messages textes



CONTACTEZ EQUIFAX ET TRANSUNION

Demandez qu'un avis de fraude soit inscrit à votre dossier de crédit



APPELEZ LA POLICE

Demandez le numéro du rapport et conservez-le précieusement.
Les informations volées pourraient être utilisées des années après le vol.



AVISEZ VOTRE INSTITUTION FINANCIÈRE ET VOTRE COMPAGNIE DE CARTE DE CRÉDIT

Demandez leur de mettre une alerte



COMMUNIQUEZ AVEC LE CENTRE ANTIFRAUDE DU CANADA

Pour signaler la fraude :
1-888-495-8501



PARLEZ À VOS AMIS ET À VOTRE FAMILLE

Parlez de votre expérience
aux gens autour de vous.
Ça leur évitera peut-être
de se faire avoir aussi.



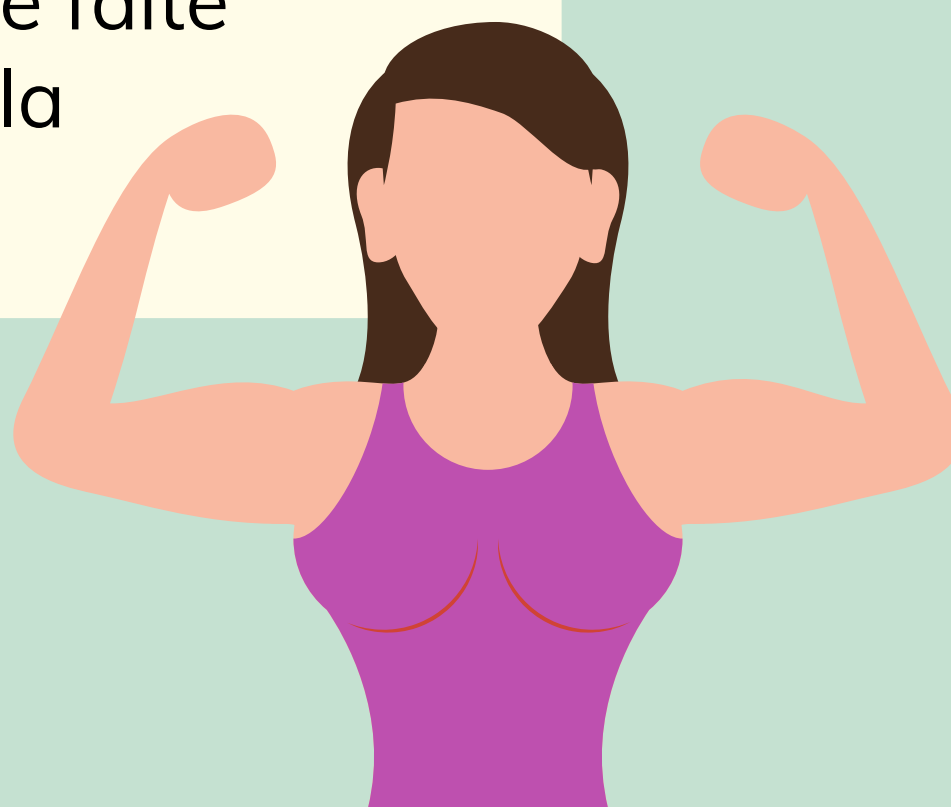
ÉVITER D'ÊTRE VICTIME À NOUVEAU

Nettoyez votre ordinateur et
changez vos mots de passe, s'il
s'agit d'une fraude en ligne.
Changez le NIP de vos cartes de
débit et de crédit



IL VOUS RESTE DE L'ÉNERGIE?

Contactez la compagnie au
nom de qui la fraude a été faite
pour les informer de la
situation



L'ACEF DU NORD DE MONTRÉAL EST LÀ POUR VOUS!

Vous avez des doutes sur une situation?

Vous avez été victime de vol d'identité et vous avez besoin d'aide pour faire vos démarches?



Pour éviter de vous retrouver dans une situation difficile ...

APPELEZ-NOUS!

514 277-7959

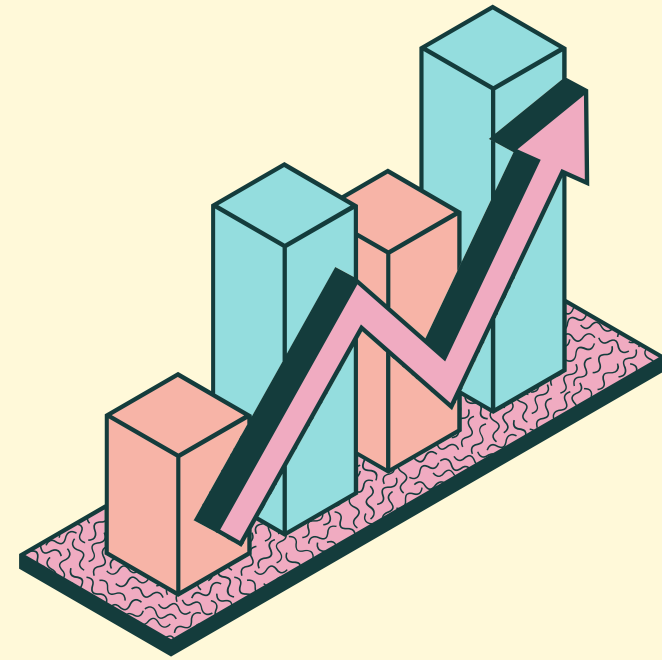
info@acefnord.org



COMMENT SAVOIR QU'ON EST VICTIME DE VOL D'IDENTITÉ?

START INVESTING EARLY

Un rappel d'Engie



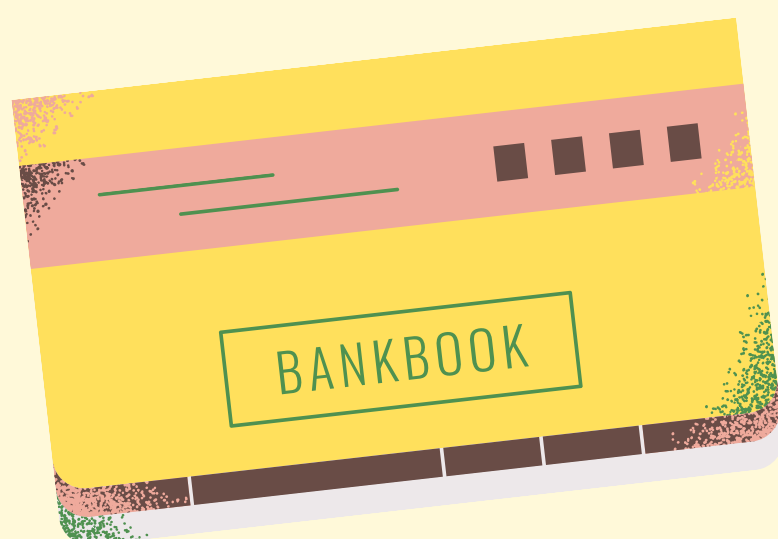
MAKE A LIST OF GROCERY ITEMS

Make a grocery list so that when you go grocery shopping, you won't buy things that are not on the list.



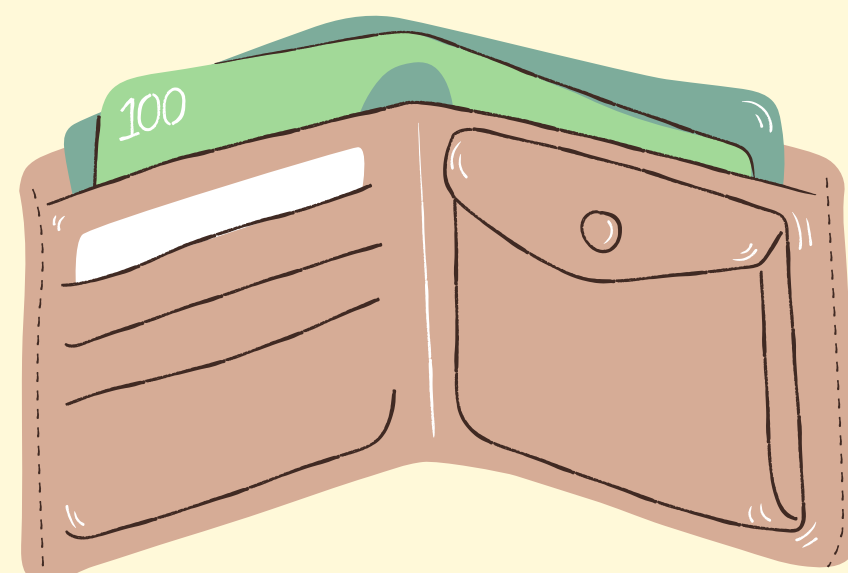
SAVE FIRST, SPEND LATER

Consommez moins d'électricité pour aider l'environnement.



SAVE EARLY

Éteignez la lumière quand vous ne l'utilisez pas.



AVOID DEBT

Pour plus de conseils, allez sur reduirelaconso.fr