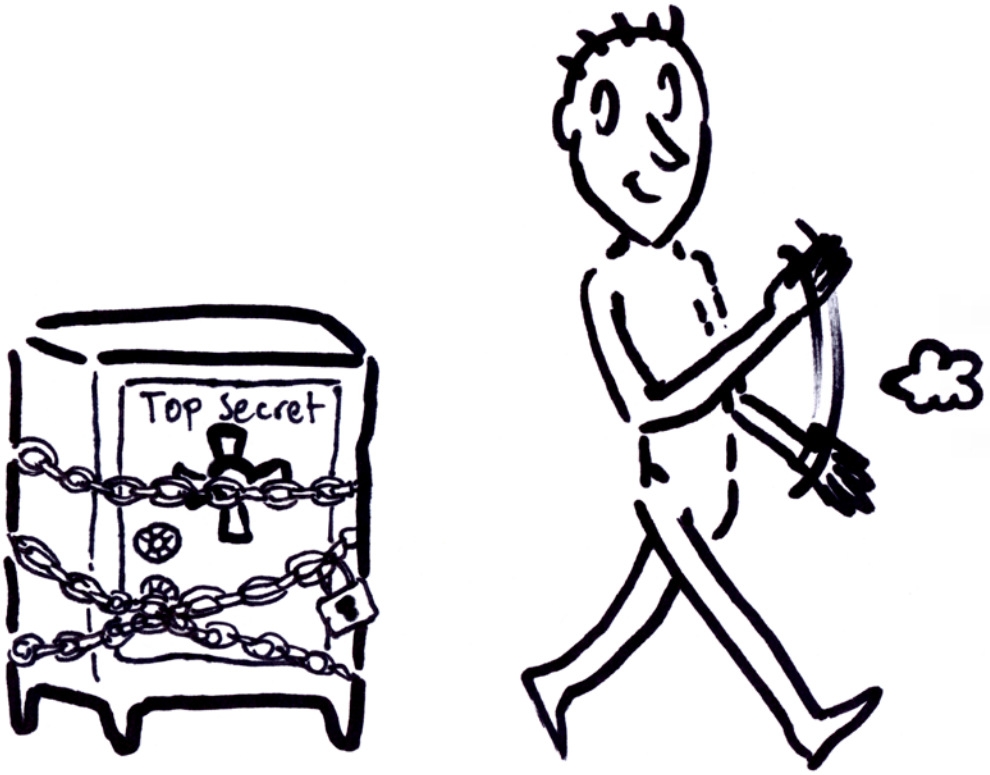
autisme Québec

Série de fiches d'éducation financière

Protéger tes renseignements personnels et ton argent



Idée originale

autisme Québec

Réalisation

Chantale Audet et Amélie Bourret
Autrement dit – www.autrementdit.ca

Collaboration

- Lili Plourde, directrice générale d'Autisme Québec
- Association coopérative d'économie familiale (ACEF) de Québec
- Direction des programmes Déficience intellectuelle et trouble du spectre de l'autisme, et Déficience physique du Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale

Illustrations

Charles-David Laflamme

Révision linguistique

David Rancourt

Graphisme

Stéphanie Rivet – Pulsation graphique

Cette fiche fait partie d'une série de fiches d'éducation financière. Les fiches sont gratuites et libres d'utilisation. Merci de les citer quand vous les utilisez.

Elles ont été rédigées en langage clair et simple pour en faciliter la compréhension et l'utilisation.

Un conseil pratique

Consultez la fiche *Introduction à la série de fiches d'éducation financière*. Elle vous donnera une vue d'ensemble de tous les thèmes abordés.

Comment citer cette publication
Autisme Québec. *Protéger tes renseignements personnels et ton argent. Série de fiches d'éducation financière*. Québec, 2020.

Dépôt légal
Bibliothèque et Archives nationales du Québec, 2020
ISBN 978-2-925115-00-7

Remerciements

Cette série de fiches d'éducation financière a été conçue avec le soutien de nombreuses personnes. Ces personnes ont généreusement accepté de partager leur expérience pour choisir les sujets les plus pertinents, elles ont commenté les nombreuses versions rédigées et elles ont fait part de leurs suggestions tout au long du développement.

Un sincère merci à toutes ces personnes, donc, personnes autistes, parents, intervenants et spécialistes de la gestion des finances personnelles.

Plus spécifiquement :
Mathieu Bérubé-Le May, Christophe Comeau, Brigitte Coutu, Léonie Dancause, Madeleine Gagne, Francine Hamel, Charles-David Laflamme, Marie Lambert, Lucie Latour, Élizabeth Le May, Justin Matte, Andrée Paradis, Jean-François Picard, Laurent Rainville, Alain Rheault, Jacinthe Rochette, Anne Seigneur

Aussi, nous souhaitons remercier d'autres personnes qui ont jeté leur regard sur les fiches de façon ponctuelle. Elles se reconnaîtront sûrement !

Merci à l'Office des personnes handicapées du Québec (OPHQ) pour la subvention accordée dans le cadre du Programme de soutien aux organismes de promotion.

Ce projet a été réalisé grâce au soutien de l'Autorité des marchés financiers. Les informations, opinions et avis exprimés n'engagent que la responsabilité d'Autisme Québec. Un merci tout spécial à Camille Beaudoin, Nathalie Depocas et Valérie Sauvé.

AUTORITÉ DES MARCHÉS FINANCIERS

Office des personnes handicapées Québec

Protéger tes renseignements personnels et ton argent

Cette fiche te sensibilisera à l'importance de bien t'occuper de tes renseignements personnels et de ton argent.

Tu y trouveras de l'information sur les sujets suivants :

1. **Tes renseignements personnels**
2. **Pourquoi prendre soin de tes renseignements personnels**
3. **Quelle information fournir, quand le faire et à qui**
4. **Conseils pour protéger tes renseignements personnels**
5. **Conseils pour protéger ton argent**
6. **Conseils pour assurer ta sécurité en ligne**
7. **Quoi faire en cas de fraude**

La protection des renseignements personnels fait partie des habiletés à acquérir pour gérer ses finances personnelles.

Bon à savoir

Tu trouveras dans cette fiche plein de conseils pour développer de bonnes habitudes afin d'éviter des situations fâcheuses.

L'idée n'est pas de te faire peur, mais plutôt de t'outiller pour que tu demeures alerte face à des situations de fraude qui surviennent souvent.

1
Tes renseignements personnels

Tes renseignements personnels sont des renseignements qui servent à t'identifier. Voici les renseignements personnels les plus courants :

- Ton nom
- Ta date de naissance
- Ton adresse
- Ton adresse courriel
- Ton numéro d'identification personnel (NIP)
- Ton numéro de compte
- Ton numéro d'assurance sociale (NAS)
- Tes identifiants et mots de passe pour des sites Web

Bon à savoir

Le NAS est un renseignement personnel à part car il donne accès à une grande quantité d'information à ton sujet.

Certains de ces renseignements personnels sont aussi confidentiels, c'est-à-dire qu'ils ne doivent pas être révélés sauf dans des situations bien précises. Tu dois donc les garder secrets et les protéger.

Il est important de prendre de bonnes habitudes avec tous tes documents importants, comme ta carte d'assurance maladie, tes cartes de débit et de crédit, ton permis de conduire, les lettres et les documents que tu reçois de ton institution financière ou du gouvernement.

Plus loin, tu trouveras plusieurs trucs pour t'aider à bien prendre soin de tes renseignements personnels.

2
Pourquoi prendre soin de tes renseignements personnels

Chaque année, plusieurs personnes sont victimes de vols d'identité parce qu'un individu malveillant a réussi à obtenir leurs renseignements personnels. C'est plus fréquent qu'on ne l'imagine.

Savais-tu ?

Un vol d'identité se produit quand quelqu'un vole et utilise des renseignements personnels. En utilisant les renseignements personnels d'une personne, le voleur se fait passer pour elle.

C'est souvent en obtenant plus d'un renseignement personnel (par exemple, le nom d'une personne, sa date de naissance et un mot de passe) que les voleurs réussissent à voler l'identité de quelqu'un.

Voici des exemples de ce qu'un voleur pourrait faire s'il obtenait tes renseignements personnels :

- Avoir accès à ton compte
- Encaisser un chèque qui t'appartient
- Faire des achats avec ton argent
- Louer un appartement avec ton argent ou en utilisant ton nom
- Prendre un contrat de téléphone cellulaire
- Obtenir une carte de crédit en ton nom

Le vol d'identité est très grave et peut avoir des conséquences sérieuses pour toi. Parmi les conséquences possibles, tu pourrais :

- Te faire voler de l'argent
- Être relié à une fraude que tu n'as pas commise
- Avoir des problèmes pour obtenir un permis de conduire ou un prêt dans une institution financière

Ce ne sont que quelques exemples de problèmes que rencontrent les personnes qui se font voler leur identité.

Il est souvent possible de trouver des solutions à ces problèmes, mais le mieux reste de faire tout ce que tu peux pour prévenir le vol de ton identité.

En apprenant à prendre soin de tes renseignements personnels, tu risqueras moins de te faire voler ton identité ou d'être victime de fraude.

Savais-tu ?

Une fraude est une activité malhonnête et illégale qui vise à tromper les gens.

3
Quelle information fournir, quand le faire et à qui

Ce ne sont pas tous les types de renseignements personnels qui sont ultrasecrets. Par exemple, tu peux bien sûr révéler ta date d'anniversaire ou ton adresse courriel à certaines personnes sans t'inquiéter. Tu ne dois jamais, cependant, révéler des renseignements comme ton NIP.

De façon générale, il te faut prendre des précautions. Quand on te demande des renseignements personnels et que tu n'es pas certain de devoir les fournir, ne les fournis pas immédiatement. Informe-toi d'abord auprès d'une personne de ton entourage pour t'assurer que c'est acceptable.

Pour ce qui est du NAS, il y a des situations où tu dois le fournir et d'autres où ce n'est pas nécessaire.

S'il n'est pas absolument nécessaire de fournir ton NAS, ne le fais pas.

Attention !

À lui seul, ton NAS peut permettre le vol d'identité ou la fraude.

Comment protéger ton NAS ? Ne garde pas sur toi ta carte ou le document où ton NAS est écrit. Fournis-le seulement si tu dois le faire.

Quand dois-tu fournir ton NAS ?

Il peut arriver qu'on te demande ton NAS et que tu ne comprennes pas pourquoi.

Selon Services Canada, un certain nombre de situations nécessitent que tu donnes ton NAS.

Si tu n'es pas certain de devoir fournir ton NAS, pose la question à quelqu'un de confiance. Dans le doute, attends et informe-toi. Tu pourras fournir ton NAS plus tard.

Exemples de situations où il est nécessaire de donner ton NAS :

- Quand tu obtiens un emploi
- Pour faire ton rapport d'impôts
- À ton institution financière, si tu veux ouvrir un compte qui donne des intérêts comme un compte d'épargne, un REER, un CELI ou un REEI
- Pour demander la plupart des prestations gouvernementales, par exemple d'assurance emploi, d'aide sociale et de solidarité sociale

Exemples de situations où il n'est pas nécessaire de donner ton NAS :

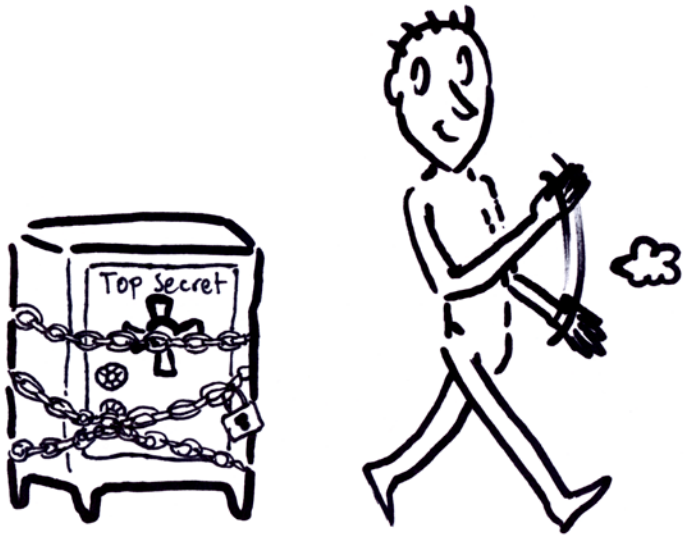
- Pour confirmer ton identité (sauf pour des programmes gouvernementaux)
- Pour remplir un formulaire de demande d'emploi
- Pour remplir un formulaire pour louer un logement
- Pour négocier un bail
- Pour remplir une demande de carte de crédit
- Pour remplir un questionnaire médical
- Pour louer une auto

Savais-tu ?

« Déclaration de revenus » est l'expression officielle pour parler d'un rapport d'impôts.

Tu peux aussi visiter le site de Services Canada, qui contient beaucoup d'information à ce sujet :

Protéger votre numéro d'assurance sociale
www.canada.ca/fr/emploi-developpement-social/programmes/numero-assurance-sociale/proteger.html



Une bonne façon de protéger ton NAS, c'est de garder ta carte ou le document sur lequel se trouve ton numéro en sécurité chez toi.

4
Conseils pour protéger tes renseignements personnels

Tu peux protéger tes renseignements personnels de plusieurs façons. Ce n'est pas très difficile, il suffit de prendre de bonnes habitudes et de rester prudent quand on te demande de l'information.

Gare aux fausses demandes d'information

Ne révèle pas de renseignements personnels au téléphone quand tu reçois des appels qui t'en demandent, à moins d'être absolument certain que la demande est justifiée ou que tu connais la personne à qui tu parles.

Si tu reçois un appel que tu n'attendais pas d'une institution financière, ou encore de l'Agence du revenu du Canada ou de Revenu Québec (les organismes qui s'occupent des impôts), réponds que tu vas rappeler. Ainsi, tu pourras savoir si l'appel provient véritablement d'eux.

Si tu rappelles pour vérifier, n'utilise pas le numéro que la personne te donnera au téléphone. Utilise plutôt le numéro officiel de l'institution, de l'organisation ou de la compagnie, que tu pourras facilement trouver sur Internet.

Aussi, ne réponds jamais à un courriel ou à un texto qui te demande de fournir des renseignements personnels ou de confirmer de l'information. Les institutions financières et les organismes gouvernementaux fonctionnent rarement de cette façon. Si tu reçois un tel courriel, il s'agit très probablement d'une demande qui n'est pas vraie.

Protège tes documents et tes cartes

Tu dois prendre certaines précautions avec tes documents importants et avec tes cartes de débit et de crédit. Tu ne dois pas les laisser traîner n'importe où.

Range tous les documents que tu reçois de ton institution financière et des organismes gouvernementaux, ainsi que tes factures, dans une chemise ou un cartable, par exemple.

Jette de façon adéquate tous tes documents qui contiennent des renseignements personnels. Par exemple, déchire tes factures et tes lettres importantes, puis mets-les à la poubelle. Ne les mets pas au recyclage. Si tu as accès à une déchiqueteuse, c'est encore mieux. Surtout, ne les jette pas dans une poubelle publique !

Si tu perds ta carte de débit ou ta carte de crédit, appelle immédiatement ton institution financière pour l'aviser. Celle-ci pourra alors s'assurer qu'aucune transaction ne se fera avec ta carte. Il existe habituellement une ligne téléphonique accessible 24 heures sur 24, 7 jours par semaine pour ce type d'urgence.

Après avoir utilisé une de tes cartes, prends le temps de bien la ranger dans ton portefeuille. Ne la laisse pas n'importe où ni dans tes poches. C'est une bonne habitude à prendre !

Attention aux pièges pour s'emparer de tes renseignements personnels

Malgré toutes les précautions qu'il est possible de prendre, il est tout de même facile de tomber dans des pièges ou d'accorder sa confiance à quelqu'un qui a des idées malveillantes. Plusieurs personnes se font prendre. En fait, tout le monde est vulnérable.

Les voleurs d'identité et les fraudeurs utilisent plusieurs méthodes pour s'emparer de renseignements personnels. Ils peuvent être rusés.

Certains d'entre eux, habiles en informatique, peuvent même réussir à accéder à des bases de données qui contiennent des renseignements personnels.

Attention !

Tu reçois un courriel ou un texto d'une institution financière qui te demande d'accéder à ton compte ou de cliquer sur un lien pour fournir certains renseignements ?

Il s'agit d'une tactique couramment utilisée par les fraudeurs pour voler ton identité ou ton argent. Mieux vaut donc supprimer le message et ne pas y répondre.

Si tu crois que le message provient vraiment de ton institution financière, prends le temps de l'appeler avant de faire quoi que ce soit.

N'utilise pas le numéro de téléphone qui se trouve dans le courriel ou dans le texto. Utilise plutôt le numéro que tu trouveras sur le vrai site Web de ton institution financière.

Voici quelques pièges courants que les voleurs d'identité et les fraudeurs utilisent. Si tu sais les reconnaître, tu seras en mesure d'en éviter plusieurs.

Des exemples de pièges courants :

- Certains voleurs vont trouver d'anciennes factures, ou encore des documents contenant des renseignements personnels qui ont été laissés dans une poubelle ou au recyclage.
- D'autres vont être subtils et prétendre travailler pour ton institution financière ou une compagnie avec qui tu fais affaire. Ils te contacteront par téléphone ou par courriel et ils te demanderont alors quelques renseignements personnels.
- Quelqu'un t'annoncera que tu as gagné un prix, mais que tu dois donner quelques renseignements pour le recevoir.
- On t'informera par texto ou par courriel que tu as reçu un virement Interac de quelqu'un que tu connais ou du gouvernement, et on t'invitera à cliquer sur un lien pour l'accepter.
- On t'enverra par courriel une facture pour un achat que tu n'as pas fait, et on te proposera de cliquer sur un lien pour avoir plus d'information ou pour contester cette facture.

5
Conseils pour protéger ton argent

De la même façon que tu peux protéger tes renseignements personnels, il existe des façons simples pour protéger ton argent.

Fais attention à ton NIP

Tu as la responsabilité de protéger ta carte de débit ainsi que ton NIP pour éviter de te les faire voler.

Il est nécessaire que tu apprennes ton NIP par cœur et surtout que tu ne le révèles à personne.

Voici quelques bonnes habitudes à prendre pour protéger ton NIP :

- Ne donne pas ton NIP à quelqu'un d'autre.
- N'écris jamais ton NIP.

Si tu choisis de l'écrire quand même, assure-toi de garder le document où il est écrit dans un endroit qui n'a rien à voir avec ta carte de débit ou ton portefeuille.

Prends des précautions quand tu utilises ta carte de débit

Ta carte de débit donne un accès direct à ton compte. C'est pourquoi il faut toujours la protéger et protéger ton NIP quand tu l'utilises.

Concrètement, voici ce que tu peux faire :

- Protège le clavier chaque fois que tu composes ton NIP.
  - Mets ta main libre au-dessus du clavier.
  - Mets-toi bien droit devant le guichet ou l'appareil pour cacher l'écran et le clavier.
- Surveille autour de toi pour t'assurer que personne n'essaie de voir les chiffres que tu composes quand tu entres ton NIP.
- Ne te laisse pas distraire, et n'accepte pas d'aide si quelqu'un t'en offre.
- Range immédiatement ton argent et ta carte de débit dans ton portefeuille.
- Range le bordereau de guichet automatique. Ne le laisse pas au guichet ou dans la poubelle sur place.

Bon à savoir

Toutes ces précautions s'appliquent aussi quand tu utilises une carte de crédit.

Savais-tu ?

Le bordereau, c'est le papier que tu reçois du guichet automatique.

Attention aux pièges pour s'emparer de ton argent

Sans même avoir accès à tes renseignements personnels, les fraudeurs peuvent aussi utiliser divers moyens pour te demander de l'argent. Ils sont parfois convaincants.

Il peut être difficile de savoir si l'offre qu'on te fait est honnête ou malhonnête.

Des exemples de pièges courants :

- On peut te demander directement de l'argent : pour aider quelqu'un dans une situation difficile dans un autre pays, ou parfois même pour aider quelqu'un que tu connais.
- On peut t'appeler au téléphone ou t'écrire un courriel pour te proposer une offre qui paraît hyper-alléchante, une offre vraiment intéressante, trop belle pour être vraie.
- On veut te vendre un produit, on fait pression sur toi pour que tu te décides rapidement et que tu payes sur-le-champ.

Il existe plusieurs exemples comme ceux-ci. Il te faut être vigilant.

Quand tu sens de la pression, ou si tu sens qu'on cherche à te faire prendre une décision ou à te faire agir rapidement, questionne-toi. C'est probablement louche. Le mieux est souvent de prendre le temps pour y penser.

Tu peux aussi en parler avec ton entourage et même appeler l'Autorité des marchés financiers pour vérifier s'il s'agit d'une fraude financière.

Autorité des marchés financiers
1 877 525-0337

On te fait une offre qui ne t'intéresse pas ou qui est trop belle pour être vraie ? Tu n'es pas obligé de l'accepter. C'est correct de dire non !

6
Conseils pour assurer ta sécurité en ligne

Il est facile et très pratique de gérer son compte ou encore de faire des achats en ligne. Mais il faut aussi être vigilant, car plusieurs cas de fraudes sont rapportés.

Encore une fois, il s'agit de prendre de bonnes habitudes, en t'assurant que tu fais tes transactions sur un ordinateur sécuritaire placé dans un endroit sécuritaire et sur des sites sécurisés.

- Assure-toi qu'un antivirus est installé sur ton ordinateur.
- Garde ton ordinateur à jour en téléchargeant les mises à jour de ton système d'exploitation.
- Utilise des sites sécurisés. Les institutions financières ont des sites sécurisés. Des compagnies comme PayPal, par exemple, offrent aussi des services de paiements sécurisés en ligne.
- Avant d'inscrire tes renseignements personnels ou de faire des transactions, assure-toi que l'adresse du site que tu visites correspond bien à l'adresse officielle de ton institution financière, de la compagnie ou de l'organisation.

Bon à savoir

Comment savoir si un site est sécurisé ?
Regarde si tu vois un cadenas dans la barre d'adresse et si l'adresse commence par https.

Aussi, assure-toi de ne pas faire de transactions sur un ordinateur que tu ne connais pas. Il te serait difficile de savoir s'il est sécuritaire.

Quand tu fais des transactions en ligne, il est préférable de ne pas les faire dans un lieu public. Tu ne sais jamais, quelqu'un pourrait voir tes renseignements personnels.

Finalement, assure-toi de toujours quitter correctement les sites Web que tu as utilisés pour faire tes transactions. Ce n'est pas assez de cliquer sur le « x ». Il est préférable de cliquer à l'endroit prévu sur la page Web pour se déconnecter.

Faire des achats ou des transactions en ligne est pratique. Assure-toi toutefois que tu prends des précautions pour éviter de te faire voler tes renseignements personnels ou ton argent.

Attention !

Les réseaux Wi-Fi publics ne sont pas sécuritaires et peuvent facilement être piratés. Évite de faire des transactions ou d'écrire des renseignements personnels en ligne si tu utilises un réseau public.

Si tu dois absolument le faire, assure-toi de prendre les bons moyens pour protéger tes données.

7
Quoi faire en cas de fraude

Si tu penses avoir été victime d'une fraude, il y a quelque chose à faire. Il est important de dénoncer les fraudes afin de limiter les dommages pour toi et d'éviter qu'il y ait d'autres victimes.

Pour dénoncer :

- Communique avec l'Autorité des marchés financiers au 1 877 525-0337.
- Contacte ton poste de police local.

L'Autorité des marchés financiers suggère aussi de changer tout de suite tes mots de passe si tu sais que tu les as donnés à un fraudeur.

Écris tout ce qui s'est passé. Tu peux faire la liste des renseignements personnels ou de l'argent qui t'ont été volés.

Tu devrais également rassembler tous les documents qui indiquent que tu es victime d'une fraude, par exemple tes relevés de compte.

Garde aussi des notes de toutes tes démarches.

À retenir

Assure-toi de bien protéger tes renseignements personnels et ton argent :

- En rangeant tes documents et tes cartes de façon sécuritaire
- En ne révélant jamais tes mots de passe ni ton NIP
- En communiquant seulement tes renseignements personnels, comme ton NAS, quand tu es certain que la personne a raison de te les demander

Reste vigilant en ligne en t'assurant de faire tes transactions sur des sites sécurisés.

Si tu te retrouves dans une situation où on a volé ton argent ou tes renseignements personnels, ne reste pas seul. Tu peux obtenir de l'aide pour résoudre la situation.