

La sécurité sur Internet pour les personnes autistes



ASD Cyber Safe

Cyber-Sécurité



**CENTRE DE RESSOURCES
ET DE FORMATION
RESOURCE AND
TRAINING CENTRE**

Copyright © 2021

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, email the author, addressed “Attention: Permissions Coordinator,” at the email below:

reception@giantstepsmontreal.com

Canada

Titre: La sécurité sur Internet pour les personnes autistes

Écrit par K.Bron Johnson pour L'École À Pas de Géant, Montréal,
QC

Format: eBook

This publication has been assigned:

ISBN: 978-0-9780305-4-4

First Edition

INTRODUCTION



En premier lieu, ce programme vise à donner aux personnes autistes qui utilisent Internet des moyens d'atteindre leurs objectifs, qu'ils soient sociaux, ludiques, professionnels, scolaires ou financiers (opérations bancaires, impôts, magasinage), tout en protégeant leurs renseignements personnels et en prenant de bonnes décisions de façon autonome.

En deuxième lieu, le programme vise à renseigner les parents ou aidant-es et les enseignant-es sur les différentes façons dont les personnes autistes utilisent Internet, parfois avec des objectifs différents de ceux de la majorité, ainsi qu'à les aider à honorer ces différences et à les comprendre. Globalement, l'essentiel est de trouver un équilibre bénéfique en assurant la sécurité de la personne tout en respectant son agentivité.

ASD Cyber Security Curriculum

Les textes s'adressent directement aux personnes autistes.
Des notes pour les aidant-es et les enseignant-es sont ajoutées en complément.

TABLE DES MATIÈRES



Introduction	iii
table des matières	vi
Vie privée, confidentialité et renseignements personnels	1
Sécurité et mots de passe	3
Qu'est-ce qui fait qu'un site est sécuritaire?	6
Hameçonnage (phishing)	8
Conversations en ligne et applications de messagerie	10
Amitiés et relations amoureuses	14
La sexualité et la loi	19
Intimidation et cyberintimidation	21
Recrutement extrémiste et racisme	22
Ressources supplémentaires (en anglais)	25

VIE PRIVÉE, CONFIDENTIALITÉ ET RENSEIGNEMENTS PERSONNELS



Certaines informations doivent rester privées. À certains moments et à certains endroits, on doit partager ses renseignements personnels. Mais sur Internet, on n'est pas obligé de partager des renseignements à notre sujet et souvent, on ne devrait pas. Pourquoi? C'est parce que des gens peuvent voler des renseignements et les utiliser pour voler notre argent en ligne.

Quand on accède à des services en personne, par exemple quand on va à la banque ou chez le médecin ou le dentiste, on donne nos renseignements personnels sans problème. Par exemple, à la clinique, on pourrait te demander ton adresse et ta carte d'assurance-maladie, ou encore ta carte bancaire pour payer. Dans ces situations, tout va bien.

Mais sur Internet, il y a des renseignements qu'on ne doit pas donner, même si la personne qui nous les demande semble honnête : adresse à la maison, numéro de téléphone, mots de passe, renseignements bancaires, numéro d'assurance sociale et renseignements financiers. Si une banque ou un autre service a besoin de ces renseignements, tu recevras la demande dans une lettre ou pendant un rendez-vous en personne.

Ne dis pas le nom de ton école. Parfois, c'est même préférable de ne pas dire ton vrai nom, pour toi et les autres membres de ta famille.

Tu peux créer une identité en ligne avec un surnom et l'utiliser pour t'inscrire sur un groupe de discussion ou avec une application. Quel nom aimerais-tu utiliser en ligne?

SÉCURITÉ ET MOTS DE PASSE



Beaucoup de sites demandent un nom d'utilisateur et un mot de passe pour ouvrir une session. Un compte de courriel et un compte en banque sont des exemples.

C'est important que ton mot de passe reste secret pour que personne d'autre ne puisse l'utiliser pour accéder à ton compte. Si ton mot de passe est très simple, par exemple si c'est un mot du dictionnaire, un pirate informatique pourrait cambrioler ton compte avec un ordinateur qui peut deviner des milliers de mots de passe par seconde. La meilleure façon de déjouer les pirates est d'utiliser un mot de passe qui est long (au moins 12 caractères) et qui contient des majuscules, des minuscules et des caractères spéciaux (comme !@#\$.). De plus, il ne faut pas utiliser de renseignements personnels dans le mot de passe, comme ta date de naissance ou ton adresse à la maison.

Les pirates peuvent aussi voler des mots de passe sur des sites Web qu'ils ont cambriolés. C'est donc important d'utiliser des mots de passe différents pour chaque compte, surtout les comptes très importants comme les comptes en banque et de cartes de crédit. Si le mot de passe est le même partout, les pirates pourraient voler ton mot de passe sur un site moins important et l'utiliser pour ouvrir une session dans un compte important sur un autre site.

Il peut être difficile de se souvenir de plusieurs mots de passe compliqués pour chacun de ces sites Internet. Un gestionnaire de mots de passe peut être utile. Plusieurs navigateurs Internet, comme Chrome ou Firefox, ont un gestionnaire de mots de passe intégré. Ou encore, on peut ajouter une extension comme LastPass ou 1Password. Un gestionnaire de mots de passe crée un mot de passe aléatoire pour chaque site et l'enregistre pour qu'on n'ait pas besoin de le mémoriser. Il suffit de se souvenir du mot de passe du gestionnaire de mots de passe.

Si tu reçois un avertissement d'une entreprise ou d'un site Web que ton mot de passe ou tes renseignements personnels ont été piratés, c'est important de suivre les instructions et de changer tout de suite le mot de passe du compte. Vérifie ton compte pour voir si quelque chose a

changé. En cas de problème, communique avec l'administration du site Web.

QU'EST-CE QUI FAIT QU'UN SITE EST SÉCURITAIRE?

Dans l'ensemble, il faut se fier à son jugement pour décider si un site est sécuritaire. C'est surtout comment on agit en ligne qui permet de se protéger. C'est comme marcher sur le trottoir : ça peut être sécuritaire ou dangereux. Si on regarde avant de traverser la rue et qu'on respecte la signalisation, on évite les dangers. Voici quelques conseils sur les éléments à surveiller pour décider si un site est sécuritaire ou non :

- Sur un site d'achat de produits en ligne ou sur le site d'une institution financière comme une banque, il devrait y avoir les lettres https: dans l'adresse URL du site (dans le haut du navigateur) et un symbole de cadenas (🔒).
- Le site devrait être facile à regarder. Il ne devrait pas y avoir beaucoup de publicités clignotantes ou

de fenêtres contextuelles (pop-up) qui compliquent l'accès.

HAMEÇONNAGE (PHISHING)

L'hameçonnage, ça fait penser à la pêche, avec raison! C'est une approche où des criminels cherchent à attraper des victimes... comme on attrape des poissons. Ces personnes tentent d'attirer les gens dans leurs pièges pour leur voler de l'argent. Les criminels tentent d'obtenir des renseignements personnels, comme les renseignements bancaires ou un numéro d'assurance sociale. Par exemple, on peut recevoir un courriel suspect qui nous demande d'ouvrir une session pour une vérification. C'est préférable d'aller directement au site Web en tapant soi-même l'adresse dans le navigateur pour vérifier si cette organisation tente vraiment de nous joindre. On peut signaler ces courriels suspects en tant que pourriels pour arrêter de les voir dans la boîte de réception.

C'est très important de se rappeler que les gouvernements et les institutions financières ne demanderont jamais de numéro d'assurance sociale ou de renseignements bancaires

ASD Cyber Security Curriculum

par courriel ou message texte. Si ces organisations doivent absolument nous communiquer quelque chose, ce sera avec une lettre ou de vive voix au téléphone.

CONVERSATIONS EN LIGNE ET APPLICATIONS DE MESSAGERIE



Les conversations en ligne peuvent se dérouler sur des sites Internet dédiés, mais aussi dans des jeux ou des applications ou lors de visionnements en ligne. Les conversations sur Internet peuvent se faire par texte, par voix ou par vidéo. Des exemples d'applications de conversation en temps réels sont Skype, Google Hangouts, Facebook Messenger, Signal, WhatsApp et HouseParty. Toutes ces applications permettent aussi les conversations vidéo, au lieu de taper au clavier.

D'autres plateformes de médias sociaux comme Twitter ou Instagram permettent de publier des idées sous forme de texte, de vidéo et d'images. Les autres personnes peuvent interagir avec le contenu en laissant un commentaire. Ce sont des interactions beaucoup plus lentes et qui ne reçoivent pas toujours de réponse, et parfois pas tout de suite. Ces plateformes permettent aussi aux gens d'envoyer

des messages privés (MP) ou messages directs. Dans ce cas, la conversation se passe directement entre deux personnes.

On peut aussi créer des conversations de groupe. Chaque fois qu'on entre dans une conversation, c'est important de regarder qui fait partie du groupe de la conversation. S'il y a une personne dans le groupe que tu ne reconnais pas, demande-lui de se présenter. Si tu ne connais pas cette personne, tu peux décider quelle information tu vas partager. Et si tu n'es pas à l'aise, tu peux quitter la conversation de groupe.

Les espaces en ligne peuvent sembler sécuritaires et privés, mais parfois, ils ne le sont pas. Ça dépend des règles du site au sujet de qui peut entrer et du niveau d'anonymat. Imagine que tu es dans ta chambre : tu peux inviter une personne à entrer, puis fermer la porte. C'est une conversation privée entre toi et une autre personne. Dans une conversation de groupe, plusieurs personnes partagent la même conversation. C'est comme s'il y avait plusieurs personnes dans ta chambre. Et dans une conversation publique, tout le monde est dans ta chambre. La porte est ouverte et d'autres personnes peuvent entrer et écouter ou commenter.

Quand on est sur Internet, c'est important de faire attention à ce qu'on dit ou ce qu'on commente, et de savoir qui est dans la chambre et si la porte est verrouillée ou ouverte. La différence entre la vraie vie et Internet, c'est que ce qui arrive sur Internet peut rester là pour toujours.

Donc même si c'est agréable de discuter avec des amis, on doit quand même garder certaines choses importantes pour soi. Comme dans la vraie vie, on ne montre pas les parties privées du corps (les parties du corps couvertes par les sous-vêtements comme les seins, les fesses, le pénis ou la vulve). Quand on est sur Internet, on ne doit pas envoyer des images du corps nu (déshabillé) ou des parties privées du corps à personne, jamais! Si tu en reçois une, ne la partage pas et ne la montre pas à d'autres personnes. Parles-en à un de tes parents ou à une personne à qui tu fais confiance.

Il y a des choses qui ne doivent pas être sur Internet.

Pour les enseignant-es et aidant-es : Il est important de lire les conditions de service de chaque application ou site Web qu'un enfant utilise. Pour de nombreux comptes de médias sociaux, par exemple Facebook et Instagram, l'âge minimum des utilisateurs est de 13 ans. Même si cette règle

peut être contournée par une personne adulte, c'est préférable de respecter les limites d'âge imposées par l'entreprise.

AMITIÉS ET RELATIONS AMOUREUSES



Certaines applications (**hiki**, par exemple) ont été créées pour les personnes autistes pour leur permettre de trouver des amis ou des partenaires amoureux. Mais il faut quand même être prudent. Les gens peuvent mentir et prétendre être quelqu'un qu'ils ne sont pas. Par exemple, une personne pourrait mentir à propos de son âge. Une personne pourrait te faire croire qu'elle est un homme, mais en fait, c'est une femme. Quelqu'un pourrait dire qu'il ou elle a beaucoup d'argent ou de cadeaux et veut t'en donner. Ou encore, une personne pourrait mentir en disant qu'elle est autiste comme toi, mais en fait, ce n'est pas vrai. On ne peut pas se fier à un site Internet ou à une application pour savoir si chaque personne dit la vérité.

Il y a des gens qui trouvent beaucoup de plaisir à tromper les personnes qui croient leurs mensonges. On les appelle les « arnacœurs », ou les arnaqueurs du cœur. Ces gens tentent de séduire quelqu'un en faisant semblant d'être une

personne qu'ils ne sont pas. Ils pourraient même t'envoyer de fausses photos pour te faire croire leurs mensonges. Pourquoi est-ce que les gens font ça? Parfois, c'est parce qu'ils ou elles souffrent de solitude ou croient que personne n'aimera leur vraie personnalité. Ils ou elles manquent de confiance en soi. Il y a aussi des gens qui ne peuvent pas se retenir de mentir.

C'est important de te respecter et de respecter ton temps. Si tu crois qu'il y a quelque chose qui ne va pas à propos d'une personne ou d'une situation, ou si tu poses des questions et que l'histoire de l'autre personne change tout le temps, c'est peut-être une situation où de l'aide extérieure pourrait être utile. Dans une situation « spéciale »* comme celle-là, on peut se tourner vers une personne de confiance pour avoir des conseils.

* Voir les ressources suivantes : *Les situations spéciales et Partenaires de confiance*

On peut développer beaucoup d'amitié et de sentiments envers les personnes qu'on rencontre en ligne et avec qui on discute souvent. Il peut aussi arriver qu'on commence à ressentir un sentiment amoureux ou du désir sexuel. C'est important de prendre son temps et de ne pas aller trop vite.

On ne doit pas se sentir sous pression de rencontrer quelqu'un. Si tu n'es pas à l'aise, peu importe quand, tu peux toujours dire non.

Si tu décides de rencontrer en personne quelqu'un que tu as seulement connu en ligne, voici quelques conseils pour te protéger :

- Organise la rencontre dans un lieu public où vous serez visibles, comme un restaurant ou une librairie.
- Dis à tes amis et à ta famille où tu vas et qui tu vas rencontrer.
- Si vous changez de lieu, dis-le à quelqu'un.
- Emmène un ou une amie et dis à la personne que tu vas rencontrer d'amener quelqu'un et faites-en une sortie de groupe.
- Assure-toi d'avoir un moyen de transport pour revenir à la maison ou de pouvoir le faire par toi-même. Ne te fie pas à la personne que tu rencontres pour te ramener chez toi.
- Prépare un plan de sortie au cas où la rencontre se passe mal.

Le rapprochement et l'intimité qu'on peut ressentir quand on développe des liens en ligne peuvent aussi être un moyen d'exprimer notre sexualité. Mais il y a des lois qu'on doit connaître. C'est illégal d'avoir des images, vidéos ou fichiers audio de nudité ou à contenu sexuel d'une personne de moins de 18 ans. Même si la personne a menti et a dit qu'elle avait plus de 18 ans quand elle t'a envoyé ces fichiers, tu peux quand même avoir des problèmes, c'est-à-dire une arrestation par la police, un procès et la prison (parfois pendant des années). C'est pour ça que c'est si important de ne jamais prendre ni envoyer à personne des photos de nudité ou de sexualité.

Pour les enseignant-es et aidant-es :

De nombreuses personnes autistes ont plus de succès et se sentent plus à l'aise dans les relations amoureuses en ligne que dans la vraie vie. La communication par écrit permet à chacun et chacune de prendre le temps de réfléchir avant de répondre et d'éviter le jugement qui peut accompagner un comportement social maladroit. Des amitiés proches peuvent se former avec des personnes autistes et non autistes, même s'il n'y a eu aucune rencontre en personne.

C'est important de ne pas contrer ces liens, car ils permettent de briser l'isolement que beaucoup de personnes autistes peuvent ressentir. Le soutien mutuel, l'acceptation et le partage des expériences et des intérêts peuvent créer un lien dont la valeur dépasse souvent ce qui est vécu dans le cadre des amitiés en personne. Même si ce type de lien n'est pas conforme aux attentes neurotypiques, il est quand même valide et précieux. Se voir interdire l'accès à Internet ou à un appareil de communication peut donc avoir des effets très négatifs sur la santé mentale. Avec les pratiques de distanciation physique qui deviennent peu à peu la norme, tout le monde commence à apprécier les amitiés en ligne à leur juste valeur.

Cela dit, il faut être extrêmement vigilant pour ce qui est des relations interpersonnelles en ligne.

LA SEXUALITÉ ET LA LOI



Pour les enseignant-es et aidant-es :

Les forums en ligne sont parfois les seuls endroits où on peut trouver des gens qui comprennent notre identité de genre ou notre orientation sexuelle. Par contre, les enfants peuvent y découvrir des concepts que vous ne leur avez pas encore expliqués. De plus, comme il n'est pas toujours possible de confirmer l'âge des personnes avec qui on interagit, c'est une source de danger. Il faut dire que les personnes autistes sont très à l'aise dans leurs amitiés avec des personnes qui sont dans un groupe d'âge différent du leur. Leur niveau de maturité émotionnelle peut différer de la norme.

Il est très important d'éviter qu'un ou une jeune autiste se trouve en possession de [pornographie juvénile](#), que ce soit intentionnellement ou pas. C'est pourquoi nous recommandons d'éliminer complètement le partage d'images de nudité ou à caractère sexuel.

Même si la personne souhaite explorer sa sexualité avec des images ou des vidéos, par prudence, il est préférable d'enseigner que l'Internet, c'est « pour toujours » – même les photos ou vidéos supprimées peuvent être retrouvées.

Aussi, n'oubliez pas que [70 % des personnes autistes s'identifient comme étant LGBTQ+](#). Une conversation au sujet du vocabulaire qui permet de décrire l'orientation sexuelle et le genre – homosexualité, transgenre, gai, aromantique, asexuel, etc. – aidera la personne autiste à mieux décrire ce qu'elle ressent. Ce ne serait pas étonnant de voir une personne autiste qui socialise en ligne dans un site de discussion ou une application de rencontres LGBTQ+. Qu'il ou elle soit LGBTQ+ ou pas, c'est très possible que ses amis autistes le soient et ce peut être plus facile de socialiser dans ce type d'environnement.

INTIMIDATION ET CYBERINTIMIDATION



Qu'est-ce qu'une bonne amitié, ou de bons comportements d'amitié?

Les bons amis t'acceptent comme tu es. Ils ou elles ne te disent pas de changer, que ce soit tes vêtements, tes cheveux, tes croyances religieuses ou ton orientation sexuelle. Au lieu, ils et elles te soutiennent et t'encouragent à être exactement toi-même. Ça ne veut pas dire ne jamais te faire de suggestions pour t'améliorer! Mais ce doit être fait en privé et en respectant tes émotions. Quelqu'un qui te prend à part et te murmure à l'oreille : « Hé, ta braguette est baissée! » veut t'épargner de la gêne. Mais quelqu'un qui te crie devant tout le monde: « Hé, tu fais dur et tes souliers sont quétaines! » vise à te faire du mal.

Les bons amis sont ceux à qui on peut faire confiance.

Si tu dis quelque chose à un ou une amie et que c'est un secret, il ou elle ne le racontera pas à d'autres personnes. Et tu feras la même chose. Même si l'amitié se termine, vous continuerez à garder vos secrets.

Si un ou une amie te dévalorise, te dit des méchancetés ou des insultes, te dit de faire des choses illégales ou qui te causeront des problèmes ou raconte des mensonges à ton sujet, ce n'est pas une amitié saine et tu peux demander de l'aide à une de tes personnes de confiance. Tu mérites d'avoir de bons amis qui te valorisent.

Recrutement extrémiste et racisme

Certains groupes extrémistes nationalistes et racistes ciblent parfois les personnes vulnérables pour les recruter, et en particulier les jeunes hommes autistes. Ces groupes « font la cour » à des gens isolés socialement ou qui se sentent seuls et renforcent leur confiance en eux en leur disant que le reste du monde est contre eux et que tous leurs problèmes vont disparaître s'ils adoptent leurs croyances et deviennent membres du groupe. Pour certains, c'est la première fois qu'ils se sentent vraiment acceptés et ces croyances peuvent commencer à leur sembler intéressantes. Le besoin d'appartenance et la pression sociale peuvent être si forts qu'ils peuvent commencer à faire des choses qu'ils ne

feraient pas normalement. Les sites de discussion et même les plateformes de jeu peuvent être des endroits où les extrémistes vont tenter de se lier d'amitié avec eux et de les recruter.

Pour les enseignant-es et aidant-es : C'est important de parler ouvertement avec les enfants de vos valeurs et de nommer les enjeux dans les domaines de la sexualité et du racisme avec des mots simples, mais exacts et explicites. S'ils regardent la télévision ou vont sur Internet, les enfants entendent et lisent beaucoup de vocabulaire, peut-être plus que vous l'imaginez. Si vous ne leur en parlez pas, ils ne connaîtront pas vos valeurs et opinions. Ils essaieront de deviner et se feront leurs propres idées. Par exemple, si vous ne parlez jamais d'homosexualité, ils pourraient croire que le sujet est tabou et le cacher. Si vous ne leur parlez pas de racisme, ils pourraient croire que certains groupes de personnes valent plus que d'autres. Vous pourriez croire que vos enfants connaissent vos opinions, mais de nombreuses personnes autistes ne tirent pas de conclusions et ne perçoivent pas les subtilités quand il y a des non-dits.

Même si ces conversations peuvent être difficiles pour les adultes, c'est possible qu'elles vous permettent de vous rapprocher et même d'avoir des éclaircs de compréhension. Elles peuvent aussi avoir un rôle de prévention du suicide.

RESSOURCES SUPPLÉMENTAIRES (EN ANGLAIS)



<https://www.getsafeonline.org/>

<https://www.common sensemedia.org/>

<https://www.wbez.org/shows/wbez-news/cps-teacher-develops-toolkit-to-fight-white-nationalism/11ba8fdb-ef4b-4f40-866f-60fc30831b98>

<https://www.wizcase.com/blog/internet-safety-guide-for-people-with-autism-spectrum-disorders/>