LA LIBERTÉ
Depuis 1913

Clinique de
Cyber-Criminologie

GÉNÉRATION CYBER-SMART

PARLER AUX INCONNUS ***

La communication des enfants avec des inconnus sur internet est, d'après nos recherches, la principale source d'inquiétude des parents en ce qui concerne les problèmes auxquels leurs enfants peuvent être confrontés en ligne. Par exemple, un enfant peut réagir à un commentaire publié sous une vidéo YouTube ou se retrouver à jouer avec quelqu'un à l'autre bout du monde. En fait, la recherche montre que rencontrer des inconnus en ligne est une chose majoritairement positive pour les enfants, qui peuvent tirer un grand profit des interactions avec des personnes de tous horizons. Il est donc important de donner les clés aux enfants afin que ces échanges se déroulent en toute sécurité.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QUELS SONT LES RISQUES LIÉS AUX INTERACTIONS AVEC DES INCONNUS EN LIGNE?

Les menaces dont les parents sont généralement le plus conscients sont les **menaces sociales** que représentent les prédateurs en ligne. En raison des nombreux moyens de communication et de connexion actuels, la possibilité que l'enfant soit en contact avec un prédateur augmente. Pourtant, nous pouvons vous assurer que ce n'est pas toujours le cas : les jeunes sont en ligne à un niveau égal, voire supérieur, à celui des adultes, et il est très probable que même les jeunes enfants jouent à des jeux vidéo en ligne ou discutent de leurs passions communes avec quelqu'un de leur âge.

Cela dit, la navigation en ligne comporte certains risques, et il existe des individus dont le but est de trouver et d'exploiter les enfants. Les prédateurs peuvent souvent mentir sur leur identité pour se lier d'amitié avec des personnes afin de gagner leur confiance et d'établir une relation avec elles, tout en ayant des motifs sexuels ou financiers cachés. Même lorsqu'ils disent la vérité sur leur identité, les prédateurs en ligne peuvent complimenter et envoyer des cadeaux aux victimes qu'ils espèrent séduire pour essayer de les manipuler, parfois dans l'espoir de les éloigner de leur famille et de leurs amis afin d'exercer un plus grand contrôle sur elles - c'est ce qu'on appelle le *grooming*.

Avec assez de détails personnels sur l'école d'un enfant ou les endroits qu'il fréquente souvent, un prédateur peut avoir assez d'informations pour le trouver en personne, l'exposant ainsi à des menaces telles que l'agression, le harcèlement ou le trafic. Et avec l'essor des outils d'intelligence artificielle, un prédateur peut créer des contenus sexuels hypertruqués d'enfants en utilisant simplement des vidéos anodines que ces derniers ou leurs parents ont partagé en ligne.

Au-delà des risques sociaux, les inconnus en ligne peuvent également exposer les enfants à des risques de cybersécurité. Les enfants peuvent être victimes d'arnaques en ligne, de tentatives d'hameçonnage ou de manœuvres frauduleuses qui les incitent à révéler des informations sensibles ou à faire des achats non autorisés. Ils peuvent également être amenés à télécharger des logiciels malveillants ou des virus lorsqu'ils naviguent sur Internet ou lorsqu'ils jouent à des jeux en ligne, compromettant la sécurité de leurs appareils et de leurs informations personnelles.

COMMENT SOUTENIR LES ENFANTS DANS LEURS RELATIONS AVEC DES INCONNUS EN LIGNE?

Il est tout d'abord important d'éduquer les jeunes sur ce qu'est une relation saine. Il est important de mettre l'accent sur le fait qu'il n'est pas normal que des adultes ou des personnes beaucoup plus âgées soient amis avec des enfants, même s'ils pensent qu'ils s'entendent bien, et de leur expliquer ce à quoi ils devraient s'attendre dans leurs relations interpersonnelles avec leurs amis et les personnes qui les intéressent. Selon les études, les comportements à risque (drogues, relations sexuelles, etc.) en ligne et dans le monde physique sont très fortement corrélés, et c'est pourquoi il est nécessaire de donner aux enfants de fortes bases sur ce que sont des relations saines et un système de soutien solide, afin qu'ils puissent reconnaître les comportements malsains ou manipulateurs lorsqu'ils les rencontrent et éviter de plus gros ennuis plus tard.

N'oubliez pas non plus que la majorité des prédateurs que les enfants rencontrent et avec lesquels ils interagissent en ligne sont des personnes qu'ils connaissent hors ligne, comme des connaissances familiales, des voisins, etc. Le lien hors ligne avec l'enfant est souvent ce qui donne au prédateur le niveau de confiance nécessaire pour entamer et maintenir une relation avec l'enfant. En d'autres mots, tous les étrangers sur internet ne sont pas dangereux, et toutes les personnes qui peuvent être dangereuses sur l'internet ne sont pas forcément des étrangers, ce qui réaffirme l'importance de donner aux enfants les outils sociaux appropriés pour reconnaître quand quelqu'un, même des personnes qu'ils connaissent , les mettent mal à l'aise.

Encouragez aussi vos élèves à parler de leurs relations en ligne sans leur porter de jugement. Il est important de ne pas leur donner l'impression que les rencontres en ligne sont fondamentalement dangereuses ou anormales : c'est la réalité de leur monde, et s'ils se sentent jugés, il est peu probable qu'ils s'ouvriront s'ils rencontrent des problèmes.

Prenez le temps de bien expliquer à vos élèves pourquoi il vaudrait mieux qu'ils respectent les seuils minimums d'âges d'utilisation des plateformes en ligne. Ce conseil ne s'applique pas seulement aux réseaux sociaux, mais aussi à certaines plateformes comme Wizz ou d'autres plateformes similaires à Chatroulette qui mettent les utilisateurs en contact avec n'importe qui dans le monde. Même après avoir dépassé la limite d'âge minimale, les jeunes peuvent être exposés à des personnes avec lesquelles ils ne sont pas assez matures pour avoir des conversations ou avec lesquelles ils ne sont pas préparés à communiquer. Les plateformes de vidéochat comme Wizz permettent aux utilisateurs de discuter avec n'importe qui plutôt qu'avec des personnes qu'ils connaissent ou qui ont des amis ou des intérêts communs, ce qui réduit considérablement les chances que le jeune utilise ces plateformes pour nouer des amitiés sérieuses. En plus du risque d'être mis en contact avec des prédateurs à travers ces plateformes, l'enfant pourrait tout simplement être exposé à des contenus ou des sujets inappropriés, ce qui pourrait aussi être très bouleversant.

QUE FAIRE SI UN ÉLÈVE RENCONTRE UN PROBLÈME?

Si un élève vient vous voir pour vous parler d'un problème lié à un étranger ou un inconnu en ligne, ne paniquez pas et laissez-le exprimer ses émotions. Si le problème est lié à des propos qui le rendent mal à l'aise, mais qui ne semblent pas soulever de problèmes graves, accompagnez-le pour signaler, puis bloquer l'autre personne. Les plateformes disposent généralement d'un moyen accessible pour signaler des comptes ou des messages abusifs, que vous devriez utiliser pour aider votre élève à se sentir plus en sécurité. Bloquer un utilisateur empêchera ensuite votre élève de voir les activités de l'autre personne sur la plateforme et vice versa.

Si vous pensez que l'interaction est plus grave et pourrait nécessiter un recours légal, par exemple si un inconnu lui demande des photos intimes, menace de divulguer des informations sensibles ou de faire du mal à votre élève, assurez-vous de tout enregistrer et de prendre des captures d'écran des messages abusifs, que vous pourrez transmettre aux parents afin qu'ils puissent décider s'ils souhaitent contacter les autorités à propos de la situation.

RESSOURCES

Signaler quelqu'un sur Discord :
https://discord.com/safety/360044103651-reporting-abusive-behavior-to-discord

Comment signaler une publication ou un profil sur Instagram?
https://help.instagram.com/192435014247952?cms_id=192435014247952

Signaler un profil Facebook :
https://www.facebook.com/help/171757096241231/?helpref=uf_share

Signaler les comportements inappropriés sur X :
https://help.twitter.com/fr/safety-and-security/report-abusive-behavior

Signaler un problème sur YouTube :
https://support.google.com/youtube/topic/9387085?hl=fr&ref_topic=2803138&sjid=11240297009758357308-NA

Signaler un problème sur TikTok :
https://support.tiktok.com/fr/safety-hc/report-a-problem

Signaler des violations de règles sur Roblox :
https://en.help.roblox.com/hc/fr/articles/203312410-Comment-signaler-des-violations-de-r%C3%A8gles

Signaler un problème de sécurité sur Snapchat :
https://values.snap.com/fr-FR/safety/safety-reporting

Article de La Presse sur la sextorsion sur la plateforme Wizz :
https://www.lapresse.ca/actualites/wizz/alertes-contre-une-appli-de-rencontre-pour-ados/2024-02-13/la-sextorsion-sur-wizz-est-omnipresente.php

GLOSSAIRE

- **Forum** : Un forum est une plateforme qui permet aux utilisateurs d'engager des discussions, de partager des informations, de poser des questions et de communiquer avec d'autres personnes sur divers sujets d'intérêt.
- **Exploitation sexuelle en ligne** : L'exploitation sexuelle en ligne fait référence à l'utilisation de l'internet et des plateformes de communication numérique pour exploiter sexuellement, groomer, manipuler ou contraindre des enfants à des fins d'abus sexuel, de harcèlement, de trafic ou d'exploitation.
- **Conditionnement ou *grooming*** : Le grooming désigne le processus par lequel un prédateur établit une relation, une confiance et un lien émotionnel avec un enfant dans le but de l'abuser sexuellement, de l'exploiter ou de le manipuler. Les comportements de «grooming» sont généralement effectués sur une longue période de temps et impliquent des tactiques de manipulation visant à désensibiliser la victime, à réduire ses inhibitions et à établir un contrôle sur elle.

- **Restriction d'âge** : Une restriction d'âge sur une plateforme en ligne fait référence à une politique ou à un mécanisme mis en œuvre par la plateforme pour limiter l'accès aux utilisateurs en dessous d'un certain seuil d'âge.
- **Hameçonnage** : L'hameçonnage est un type de cyberattaque où les auteurs tentent de tromper des individus et de leur faire divulguer des informations sensibles, telles que des noms d'utilisateur, des mots de passe, ou des numéros de carte de crédit, en se faisant passer pour une entité digne de confiance dans le cadre d'une communication électronique.
- **Hypertrucage** : L'hypertrucage fait référence à la manipulation de contenu média (souvent audio ou vidéo) à l'aide d'outils d'intelligence artificielle (IA) pour leur donner une apparence réaliste alors que ce contenu est fictif.

Balayez ce QR code à l'aide de votre caméra pour visionner nos vidéos