LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

ESPRIT CRITIQUE (9 À 12 ANS)

****

Il nous semble important d'aborder ce sujet pour plusieurs raisons : les enfants doivent développer un sens de la pensée critique spécifique à leur utilisation d'Internet afin de rester méfiants vis-à-vis des inconnus, de reconnaître les messages frauduleux ou trompeurs et d'adopter des pratiques de navigation et de téléchargement sécuritaires. En outre, nous pensons qu'il est nécessaire de commencer à sensibiliser les enfants aux publicités potentiellement dangereuses et aux contenus trompeurs afin de les préparer à une utilisation autonome et sécuritaire de l'internet.

Suivant les pratiques d'autres initiatives d'éducation à la cyberhygiène, nous avons décidé de créer cette section pour les enfants de 9 ans et plus. Non seulement les enfants plus jeunes sont moins susceptibles de naviguer en ligne ou d'avoir leurs propres appareils, mais ils sont également moins susceptibles de comprendre pleinement les thèmes explorés ici ou de pouvoir les relier à leur expérience en ligne.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QUE L'ESPRIT CRITIQUE ET QUEL EST SON RAPPORT AVEC LA VIE EN LIGNE? QUELS SONT LES RISQUES AUXQUELS LES ENFANTS SONT EXPOSÉS?

Dans nos ressources, nous avons défini l'esprit critique aux enfants en leur disant qu'il consiste à analyser et à évaluer des informations avant de les considérer comme vraies ou valables. Cette affirmation fait référence à plusieurs choses, mais le message général est destiné à leur apprendre qu'ils ne peuvent pas faire confiance à tout ce qu'ils lisent et voient en ligne. Voici quelques-unes des questions en ligne qui nécessitent une réflexion critique :

1. **Discuter avec des inconnus en ligne** : En tant que parents, celui-ci est peut-être le point qui semble le plus menaçant, surtout si vous avez entendu parler de *online grooming* et d'exploitation sexuelle d'enfants en ligne. En parlant aux enfants de la pensée critique et en leur disant de rester vigilants lorsqu'il s'agit des personnes avec lesquelles ils discutent en ligne, nous leur apprenons que les internautes peuvent mentir ou faire des choses qui ne sont pas toujours dans leur intérêt. Nous voulons que les enfants soient conscients de ce fait, non pas pour les effrayer, mais pour leur rappeler qu'ils doivent faire attention à leurs propres émotions face à une situation donnée, surtout lorsque des personnes en ligne pourraient profiter d'eux. Nous abordons ce sujet plus en détail dans une section consacrée aux inconnus en ligne, mais il nous a semblé nécessaire de le mentionner ici aussi.
2. **Prévenir ou éviter le piratage** : Les pirates utilisent diverses méthodes pour tenter de compromettre des systèmes informatiques. Il peut s'agir de courriels d'hameçonnage, de fichiers infectés, de vulnérabilités dans un système ou un réseau existant, de l'envoi de *pop-ups* ou de messages trompeurs, etc. En aidant les enfants à prendre conscience de ces possibilités, nous espérons les inciter à s'arrêter et à réfléchir au lieu d'explorer et de cliquer à l'aveuglette. Cela est d'autant plus vrai puisqu'ils peuvent être influencés par les comportements en ligne de leurs amis, ce qui pourrait les amener à essayer d'accéder à des sites web non sécurisés ou à télécharger des fichiers, en ne pensant qu'au gain ou à l'accès plutôt qu'au danger potentiel auquel ils exposent, leur appareil et celui de leur famille. Même si nous voulons qu'ils soient curieux en ligne, ils doivent commencer à considérer la navigation indépendante sur Internet comme un privilège qui s'accompagne de responsabilités.

1. **Gérer les messages des fraudeurs** : Même avec un accès limité à l'internet, les enfants peuvent être exposés à des arnaques et à des messages frauduleux. Sur les plateformes de jeux en ligne, il n'est pas rare que des fraudeurs envoient des messages d'hameçonnage ou des instructions pour gagner de la monnaie de jeu qui s'avèrent finalement être un stratagème pour s'emparer de leurs comptes. Même si l'enfant ne perd pas toujours réellement de l'argent, le temps et l'énergie qu'il a consacrés à ses jeux en ligne lui sont précieux, et le fait de les perdre aux mains de fraudeurs peut être particulièrement dévastateur. En outre, il faut apprendre aux enfants que les fausses promesses, les offres d'enrichissement rapide et d'autres types d'arnaques sont courantes en ligne, afin qu'ils soient moins susceptibles de tomber dans le panneau une fois qu'ils auront accès à leur propre argent ou qu'ils commenceront à vouloir plus d'autonomie en ligne. Cela est d'autant plus vrai alors qu'ils approchent l'âge où ils commencent à ouvrir des comptes sur les réseaux sociaux et peuvent donc être plus facilement approchés par des personnes mal intentionnées.
2. **Consommer du contenu en ligne trompeur ou frauduleux** : Tout comme les fraudeurs qui ciblent directement les individus en ligne, de nombreuses entreprises et annonceurs ont recours à des pratiques frauduleuses ou trompeuses pour gagner de l'argent - pensez aux entreprises de *dropshipping* qui vendent des chaussures prétendument certifiées orthopédiques sans aucune preuve de leurs bienfaits médicaux réels, ou bien aux boutiques en ligne qui prétendent vendre des bijoux en or ou en argent véritables, mais dont les produits se ternissent dès le premier usage. Alors que les enfants commencent à consommer du contenu, non seulement sur les réseaux sociaux mais aussi sur des plateformes libres d'usage à tous comme YouTube, ils seront bientôt également confrontés à des influenceurs qui créent des contenus trompeurs sponsorisés, ou qui font la publicité d'un style de vie qui les incitent à se procurer les produits les plus à la mode et les plus récents. Tout contenu publié sur l'internet peut être frauduleux ou inciter les gens à dépenser de l'argent inutilement : il faut donc que les enfants commencent à s'en méfier tôt pour ne pas se faire prendre.
3. **Être confronté à du contenu généré par l'intelligence artificielle (IA)** : Avec le développement des contenus générés par l'IA, il peut être difficile de savoir si ce que l'on nous vend donne des résultats authentiques ou s'il a été maquillé pour y donner cette impression. Le contenu généré par l'IA peut également être utilisé pour falsifier des faits pour alimenter la désinformation ou de contenu hypertruqué. Étant donné la rapidité avec laquelle la qualité de ce type de contenu augmente, les enfants doivent être conscients de la possibilité que ce qu'ils consomment puisse être faux. Au lieu de fonder leurs convictions sur ce qu'ils trouvent en ligne uniquement sur la qualité d'un élément de contenu, nous souhaitons qu'ils prennent plutôt l'habitude et la responsabilité de faire leurs propres recherches.

QUEL SOUTIEN PEUT-ON OFFRIR AUX ENFANTS?

Il est important de promouvoir l'esprit critique dans tous les aspects de la vie des enfants, et pas seulement en ce qui concerne la vie en ligne. La fraude existe aussi bien hors ligne qu'en ligne, et nous ne voulons pas donner aux enfants l'impression que les gens ne mentent qu'en ligne. Mais en plus de cela, nous devrions également adopter des habitudes de navigation en ligne sûres et critiques afin de leur donner un bon modèle et de normaliser la recherche d'affirmations et de faits en ligne.

Nos ressources vidéo donnent aux enfants quelques exemples de questions qu'ils peuvent se poser lorsqu'ils consomment du contenu en ligne. En tant que leur réseau de soutien et leurs adultes de confiance, il est aussi important de laisser la porte ouverte aux discussions sur ces questions. Nous voulons qu'ils n'aient pas peur de nous contacter si quelque chose les met mal à l'aise, mais nous voulons aussi qu'ils parlent ouvertement de tout contenu qu'ils rencontrent afin que la question de savoir s'il est trompeur ou non puisse faire l'objet d'une conversation continue. Les contenus trompeurs bernent même les adultes les plus renseignés, il ne faut donc pas s'attendre à ce que les enfants soient capables de faire la différence immédiatement. Nous devons éviter qu'ils se sentent jugés s'ils parlent avec enthousiasme d'accepter une offre frauduleuse pour obtenir rapidement des pièces de jeu, par exemple, et leur expliquer calmement pourquoi cette offre n'est peut-être pas vraie et ce qu'il faut faire à partir de là.

Cela signifie également qu'il ne faut pas punir les enfants s'ils se font piéger par des offres d'argent rapide ou d'autres types de manœuvres frauduleuses. Ce sont des occasions d'apprentissage importantes pour eux, même s'ils finissent par perdre de l'argent ou par se faire pirater un compte. C'est pourquoi il est important de maintenir d'autres habitudes de navigation sûres, comme l'utilisation de mots de passe uniques pour chaque compte, l'installation d'un bon logiciel antivirus et l'utilisation d'une carte de crédit prépayée pour les achats qu'ils effectuent en ligne, afin de limiter les dégâts et d'éviter que le reste de la famille ne soit affecté. Il n'en reste pas moins qu'il ne faut pas contribuer à la honte qu'ils peuvent ressentir de commettre des erreurs que même des adultes avertis commettent.

Si vous souhaitez aborder le sujet avec votre enfant, mais ne savez pas comment l'approcher, asseyez-vous avec votre enfant et accompagnez-le dans une séance où vous passez ensemble à travers votre fil d'actualité sur les réseaux sociaux par exemple. Demandez-lui d'identifier les messages frauduleux, les contenus qui le mettent mal à l'aise ou qui attirent son attention, puis évaluez ces contenus ensemble. Posez-lui des questions sur la véracité de ce que vous trouvez, sur les intentions qui se cachent derrière le contenu exploré, et aidez-le à faire des recherches pour vérifier certaines informations. Vous apprendrez peut-être quelque chose sur vos propres habitudes de navigation en faisant cet exercice, et cela lui permettra de comprendre en temps réel ce à quoi il pourrait être exposé lorsqu'il commencera à acquérir plus d'autonomie en ligne.

RESSOURCES

Clinique de cyber-criminologie: https://www.clinique-cybercriminologie.ca/

Centre antifraude du Canada: https://antifraudcentre-centreantifraude.ca/index-fra.htm

Finances avisées Manitoba: https://financesaviseesmanitoba.ca/preservation-and-risk-mitigation/escroqueries-et-fraudes/

Article par Innovation, Sciences et Développement économique Canada sur le marketing d'influence: https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr/recueil-pratiques-commerciales-trompeuses-volume-4#sec01

Article de Radio-Canada sur l'hypertrucage: https://ici.exploratv.ca/blogue/pub-deepfake-youtube-aniston-macbook-fraude-techno-ia/

GLOSSAIRE

- **Publicité en ligne** : La publicité en ligne désigne la pratique consistant à promouvoir des produits, des services ou des marques sur internet à l'aide de divers canaux et plateformes numériques.
- **Influenceur** : Un influenceur est une personne qui a la capacité d'influencer les opinions, les comportements et les décisions d'achat d'un public spécifique en raison de l'expertise, de l'authenticité ou de l'autorité qu'il perçoit dans un créneau ou un secteur particulier. Les influenceurs ont généralement une audience importante et engagée sur les plateformes de réseaux sociaux, les blogs ou d'autres canaux en ligne. Ils utilisent leur présence en ligne pour partager du contenu, promouvoir des produits et s'engager auprès de leur public.
- **Créateur de contenu** : Un créateur de contenu est une personne ou une entité qui produit, conçoit et publie un contenu créatif et original sur diverses plateformes médiatiques, généralement dans un but publicitaire ou promotionnel.
- **Intelligence artificielle** : L'intelligence artificielle (IA) est le développement de systèmes informatiques ou de logiciels capables d'effectuer des tâches qui requièrent généralement l'intelligence humaine, comme l'apprentissage, le raisonnement, la résolution de problèmes, la compréhension du langage naturel, la reconnaissance vocale et la perception visuelle.
- **Piratage** : Au sens général, le piratage informatique désigne l'obtention d'un accès non autorisé à des systèmes ou réseaux informatiques, impliquant souvent la manipulation, l'exploration ou l'exploitation de la technologie pour atteindre cet objectif.
- **Fraude** : La fraude est la tromperie intentionnelle ou la déformation des faits dans le but d'obtenir un avantage injuste ou malhonnête, souvent à des fins financières. Elle implique l'utilisation de pratiques trompeuses pour amener des individus, des organisations ou des systèmes à croire ou à agir sur la base de fausses informations.

- **Contenu généré par l'IA** : Le contenu généré par l'IA fait référence au matériel créatif ou informatif produit avec l'aide des technologies de l'intelligence artificielle (IA). Dans ce contexte, les algorithmes d'IA, en particulier ceux basés sur l'apprentissage automatique, le traitement du langage naturel et d'autres techniques avancées, sont utilisés pour générer du contenu écrit, visuel ou audio sans implication humaine directe dans le processus de création de contenu.
- **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