LA CYBERSÉCURITÉ POUR LES ÉLÈVES D'ÂGE SCOLAIRE

UN GUIDE À L'INTENTION DES PARENTS

Table des matières

Introduction à la cybersécurité : un monde numérique, de nouveaux défis

À l'ère numérique, l'accès à Internet enrichit considérablement notre vie et celle de nos enfants. Le numérique se veut une porte d'accès à une connaissance illimitée et à une socialisation innovante, ouvrant des horizons d'apprentissage fascinants. L'utilisation d'Internet chez les jeunes est une aventure riche et positive, remplie de découvertes et de possibilités d'épanouissement personnel et éducatif. Cependant, comme toute puissante ressource, Internet présente des risques qu'il ne faut pas ignorer. Il est donc important d'outiller les jeunes avec des habiletés et des compétences pour naviguer sur le web de manière sécuritaire, avisée et confiante. C'est dans cette perspective que la cybersécurité entre en jeu.

D'entrée de jeu, dans le présent livret portant sur la cybersécurité, il convient de préciser la définition des termes « Internet » et « web ».

Selon les littératures consultées, « Internet » signifie un réseau international informatique de communications, tandis que le terme « web » se traduit par un système permettant l'accès à des ressources trouvées sur Internet.

La cybersécurité ne concerne pas seulement la protection de nos systèmes informatiques et de nos données personnelles contre les cyberattaques. Elle englobe également une série de pratiques, de connaissances et d'habiletés essentielles pour naviguer en toute sécurité sur Internet. Les jeunes de tous âges utilisent Internet pour une multitude de raisons : recherches scolaires, jeux, réseaux sociaux et plus encore. Chacune de ces activités, bien qu'enrichissante, cache des risques, tels que l'exposition à des contenus inappropriés, le cyberharcèlement, le vol d'identité et la manipulation par de fausses informations. Sans une compréhension adéquate de la cybersécurité, les jeunes sont vulnérables.

Ceci dit, loin de craindre l'usage d'Internet, nous célébrons son potentiel à façonner une génération innovante, informée et connectée, tout en faisant preuve de vigilance et de proactivité face à sa sécurité. En guidant les jeunes à comprendre les principes de la cybersécurité, nous les préparons à devenir non seulement des internautes compétentes et compétents, mais aussi des citoyennes et citoyens responsables à l'ère numérique. Internet est un atout incroyable pour l'apprentissage et la croissance et, avec une éducation réfléchie en cybersécurité, nos enfants peuvent en tirer le meilleur parti tout en se protégeant des risques.

LE RÔLE DES PARENTS DANS L'ÉDUCATION NUMÉRIQUE

En tant que parents, notre rôle ne se limite pas à fournir un accès à la technologie. Il s'étend à l'éducation de nos enfants sur la manière de l'utiliser de façon efficace, responsable et sécuritaire. Voici quelques-unes des actions les plus importantes que vous pouvez entreprendre pour guider vos enfants dans l'univers numérique.

Dialogue ouvert : Créez un environnement familial où les sujets numériques sont discutés librement. Encouragez vos enfants à partager leurs expériences en ligne, leurs découvertes, mais aussi leurs doutes et leurs inquiétudes.

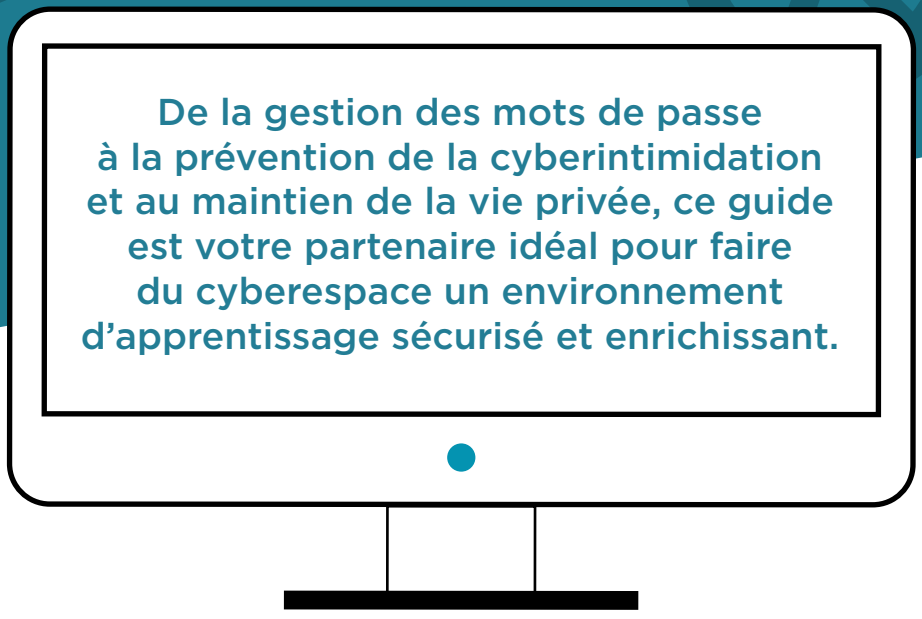
Éducation et sensibilisation : Informez-vous et informez vos enfants des risques en ligne. Expliquez l'importance de la confidentialité, les raisons pour lesquelles il est crucial de ne pas partager d'informations personnelles, et enseignez-leur à reconnaître les comportements en ligne dangereux ou suspects. Des ressources, telles ECNO Cyber sensibilisation et les ressources répertoriées par le Centre franco, vous seront certainement utiles. L'école a aussi de la documentation pour inspirer vos discussions.

Supervision et paramètres de confidentialité : Faites preuve de proactivité dans la supervision de l'utilisation d'Internet par vos enfants. Utilisez les paramètres de confidentialité et les contrôles parentaux disponibles sur la plupart des plateformes et appareils pour protéger vos enfants des contenus inappropriés.

Pratiques de sécurité en ligne : Enseignez à vos enfants l'importance des mots de passe forts difficiles à pirater, de la vérification en deux étapes et des mises à jour régulières de logiciels. Montrez-leur par l'exemple en sécurisant vos propres appareils et comptes.

Citoyenneté numérique : Encouragez vos enfants à montrer du respect et de la bienveillance en ligne, tout comme elles et ils le feraient dans la vie réelle. Discutez des conséquences du cyberharcèlement et de l'importance de signaler tout comportement inapproprié.

La cybersécurité, loin d'être un sujet réservé aux personnes expertes, est une habileté de vie essentielle à développer dans notre monde connecté. En tant que parents, nous avons le devoir non seulement de saisir les enjeux de la cybersécurité, mais également d'être une boussole fiable pour aider nos enfants à naviguer en toute confiance dans cet environnement numérique. Ce livret de cybersécurité a été spécialement conçu pour fournir aux parents les connaissances et les outils nécessaires pour protéger la sécurité numérique de leurs enfants, qu'elles ou ils soient à l'élémentaire ou au secondaire.



Risques liés à la sécurité en ligne

CE QUE TOUT PARENT DEVRAIT SAVOIR

Dans l'univers numérique où nos enfants naviguent chaque jour, les risques de sécurité en ligne sont d'autant plus variés qu'omniprésents. Comprendre ces risques est le premier pas vers le soutien de nos enfants dans cet espace où le réel et le virtuel se confondent. Face à des défis, tels que la cyberintimidation, les arnaques et l'exposition à des contenus inappropriés, leur capacité à naviguer en sécurité sur Internet devient de plus en plus essentielle. Cette section vous expose un aperçu des risques les plus communs et vous offre quelques conseils pratiques pour éduquer vos enfants et les aider à naviguer dans les espaces numériques de manière plus sûre.

Maliciels, virus et hameçonnage : les intrus numériques

Les logiciels malveillants, ou maliciels, et les virus informatiques sont conçus pour s'infiltrer et parfois endommager les appareils sans le consentement de l'utilisatrice ou de l'utilisateur. Ils peuvent voler des informations personnelles, causer des dysfonctionnements des appareils ou même les verrouiller jusqu'à ce qu'une rançon soit payée. L'hameçonnage, quant à lui, est une technique utilisée pour tromper les utilisatrices et utilisateurs afin de divulguer des informations confidentielles, comme des mots de passe ou des détails de carte de crédit, souvent par le biais de courriels et de messages textes qui semblent provenir de sources légitimes.

STRATÉGIES DE PRÉVENTION

Logiciel antivirus

Installez un logiciel antivirus[1] de confiance sur tous les appareils et configurez-le pour qu'il se mette à jour automatiquement.

Vigilance pour les courriels et messages textes

Encouragez la vigilance et la vérification en demandant des informations personnelles, même s'ils semblent provenir d'organismes ou de sources connues. Apprenez à vos enfants à vérifier l'authenticité des demandes en contactant directement l'entreprise ou l'organisation via un canal officiel (par exemple, appeler l'école si le courriel prétend en provenir). Ne jamais répondre à des courriels non sollicités et toujours vérifier l'adresse de l'expéditeur.

Mises à jour régulières

Assurez-vous que le système d'exploitation de vos appareils électroniques et de toutes vos applications sont régulièrement mis à jour. Cette pratique corrige et évite souvent des failles de sécurité qui pourraient être exploitées par des personnes malveillantes.

Signes d'un message ou site web suspect

Apprenez à vous enfants à reconnaître les signes d'un message. Les fautes d'orthographe, les offres trop alléchantes et les demandes non sollicitées d'informations personnelles sont des signaux qui inspirent le doute. Enseignez à vos enfants à ne jamais cliquer sur des liens ou télécharger des pièces jointes dans des courriels de sources inconnues.

1 Exemples d'antivirus de confiance : Norton Antivirus, McAfee, Kaspersky, Bitdefender, Avast.

Applications et sites web non sécurisés : naviguer avec prudence

Les enfants peuvent facilement naviguer sur des applications et des sites web non sécurisés qui ne protègent pas adéquatement leurs informations personnelles ou qui sont truffés de logiciels malveillants.

STRATÉGIES DE PRÉVENTION

- **Apprenez-leur à reconnaître un site sécurisé**, notamment par la présence du « https » dans l'URL et le symbole du cadenas.
- **Installez des outils de contrôle parental**[2] pour bloquer l'accès aux sites web non sécurisés ou inappropriés.
- **Sélectionnez rigoureusement vos applications à partir de sources officielles**, comme le Google Play Store et l'Apple App Store, et lire les avis et les permissions demandées avant l'installation.
- **Sensibilisez vos enfants aux critères de sécurité** qui rendent une application et un site sûrs, comme les politiques de confidentialité claires et les options de paramètres de sécurité.

2 Exemples d'outils de contrôle parental : Qustodio, Norton Family, Kaspersky Safe Kids, Net Nanny, Circle Home Plus, Google Family Link, Screen Time.

Contenu inapproprié et accès non désiré : garder un œil ouvert

Internet offre une vaste gamme de contenus et il est important de guider nos enfants vers des ressources qui sont adaptées à leur âge et à leur développement personnel. En les accompagnant activement, nous pouvons les aider à tirer le meilleur parti de cet espace tout en les protégeant des contenus qui ne leur conviennent pas.

STRATÉGIES DE PRÉVENTION

- **Discutez des différents types de contenu que vos enfants peuvent consulter en ligne** et dialoguez ensemble sur les raisons pour lesquelles certains contenus sont inappropriés ou potentiellement dangereux. Utilisez des exemples généraux sans exposer les enfants à du contenu réellement inapproprié.

- **Apprenez-leur à reconnaître des publicités trompeuses.** Expliquez la façon dont certaines publicités en ligne peuvent être conçues pour tromper et que cliquer dessus pourrait les rediriger vers des sites malveillants. Aidez-les à reconnaître et à ignorer les publicités qui semblent « trop belles pour être vraies ».

- **Installez des filtres de contenu et des bloqueurs de publicité**[3] pour minimiser les chances d'exposition à des contenus inappropriés. Vous pouvez même faire de la recherche et installer un logiciel de filtrage web en famille. Explorez ensemble les fonctionnalités et configurez les paramètres pour bloquer les sites web inappropriés. Discutez de l'importance de ces outils tout en reconnaissant qu'aucun système n'est parfait et que la communication ouverte reste essentielle.

- **Parlez régulièrement avec vos enfants de ce qu'elles et ils voient en ligne** et encouragez-les à venir vers vous si elles et ils lisent du contenu dérangeant ou questionnable. Sans envahir leur intimité, portez attention à l'utilisation d'Internet de vos enfants. Convenez ensemble, en incluant les sœurs et frères, de règles d'utilisation d'Internet, y compris les heures et les lieux permis.

3 Exemples d'applications de filtrage de contenus web : OpenDNS FamilyShield, Net Nanny, Norton Family, SafeDNS, Qustodio.

Rencontres avec des personnes inconnues en ligne : établir des limites saines

L'anonymat d'Internet ouvre la porte à des interactions diverses, et il est essentiel d'éduquer les jeunes sur la manière de naviguer sûrement dans cet espace. En les guidant sur la façon d'établir des connexions sûres, notamment dans les jeux en ligne, nous pouvons les aider à profiter de leurs interactions tout en les sensibilisant aux risques et en leur apprenant à éviter les situations potentiellement dangereuses.

Par exemple, Maxime, 15 ans, passionné de jeux vidéo, a reçu une invitation à rejoindre un groupe privé de joueuses et joueurs en ligne. Malgré que les membres du groupe puissent avoir de bonnes intentions, il se peut aussi qu'elles et ils cherchent à manipuler des jeunes joueuses et joueurs pour obtenir des informations personnelles, pour les soumettre à du harcèlement en ligne ou même pour distribuer des maliciels *(malwares)* ou des liens vers des sites web frauduleux. Maxime pourrait, sans le savoir, compromettre la sécurité de son appareil et de ses données personnelles en cliquant sur des liens ou en téléchargeant des fichiers vérolés.

STRATÉGIES DE PRÉVENTION

- **Créez une liste de contrôle portant sur les rencontres et collaborations en ligne** pour évaluer si une interaction en ligne avec une personne inconnue est sûre. Par exemple, « Cette personne demande-t-elle des informations personnelles? », « Connaissons-nous cette personne dans la vie réelle? », « Avons-nous un sentiment de malaise dans cette interaction? ».

- **Restez au courant des jeux et des plateformes** que vos enfants utilisent et des personnes avec qui elles et ils interagissent.

Vérifiez l'identité des personnes rencontrées en ligne :

- **Effectuez une recherche croisée :** effectuez une recherche dans un navigateur en ligne, par exemple, Google sur le nom ou le pseudonyme pour voir si les informations fournies correspondent à ce qui est disponible en ligne; utilisez la recherche par image inversée de Google pour vérifier l'authenticité des photos de profils.
- **Vérifiez les profils sur les réseaux sociaux :** examinez si la personne possède des profils cohérents sur différents réseaux sociaux. Vérifiez l'historique des publications, les commentaires et les interactions avec d'autres utilisatrices et utilisateurs. Un profil authentique aura souvent un historique d'engagement significatif avec d'autres personnes.
- **Demandez des preuves en temps réel :** proposez un appel vidéo rapide comme moyen efficace de confirmer l'identité de la personne.
- **Posez des questions spécifiques :** demandez à connaître des détails qui seraient connus uniquement de la personne concernée ou difficiles à inventer sur-le-champ. Par exemple, si la personne prétend être quelqu'un qui vous connaît, vous pourriez lui demander : « Peux-tu me parler d'un souvenir spécifique que nous avons partagé lors d'un événement passé? »

En armant vos enfants des connaissances et des outils pour naviguer en ligne en toute sécurité, vous les aidez à développer des habiletés et compétences essentielles pour leur avenir à l'ère numérique. L'objectif est de créer un environnement numérique où les jeunes se sentent à l'aise pour discuter de leurs expériences et préoccupations en ligne avec leurs parents ou tuteurs, tout en étant équipées et équipés pour prendre des décisions éclairées et sécuritaires.

La communication est l'outil le plus puissant dont disposent les parents pour naviguer avec leurs enfants dans le monde numérique.

Il est essentiel d'instaurer tôt un dialogue ouvert sur l'utilisation efficace, responsable et sécuritaire d'Internet, en créant un environnement où l'enfant se sent à l'aise de partager ses expériences et ses inquiétudes.

- Commencez par raconter vos propres expériences en ligne, les bons comme les mauvais côtés.
- Posez des questions ouvertes sur ce que vos enfants aiment faire en ligne, leurs applications et sites préférés, et si elles et ils ont vécu ou entendu des situations inconfortables ou des comportements inappropriés.
- Programmez des moments réguliers pour explorer ensemble le monde numérique.

Ces moments peuvent aussi être des occasions d'apprentissage mutuelles pour découvrir de nouveaux intérêts ou discuter des dernières tendances en ligne.

L'objectif est de préparer vos enfants à naviguer sur Internet de manière informée et sécuritaire, tout en renforçant le dialogue familial autour de ces enjeux cruciaux.

Communication sécuritaire en ligne

PROMOUVOIR UNE CULTURE DE CONFIDENTIALITÉ

La communication en ligne fait partie intégrante de la vie de nos enfants. Que ce soit à travers les forums de clavardage, les réseaux sociaux ou les jeux en ligne, les jeunes interagissent continuellement avec le monde extérieur. Cette ouverture, bien qu'enrichissante, les expose à des risques. Chaque clic, chaque partage et chaque connexion laisse une trace indestructible dans l'océan du cyberespace. La confidentialité devient donc un pilier fondamental à notre intégrité numérique. Face à la collecte incessante de nos données personnelles par des entités souvent invisibles, la maîtrise des paramètres de confidentialité devient non seulement une compétence essentielle, mais une nécessité absolue pour protéger notre identité et notre espace numérique.

C'est dans ce contexte que la présente section aborde des stratégies concrètes pour renforcer la confidentialité en ligne, depuis l'ajustement des paramètres de confidentialité jusqu'à l'inculcation d'une réflexion critique sur le partage d'informations personnelles.

PARAMÈTRES DE CONFIDENTIALITÉ : NAVIGUER AVEC ASSURANCE

Prenez le temps d'explorer et d'ajuster les paramètres de confidentialité des comptes sur les réseaux sociaux et autres plateformes en ligne avec vos enfants. Cette démarche comprend la personnalisation de l'accès aux publications, la gestion des contacts et la compréhension de l'utilisation des données personnelles. Encouragez vos enfants à adopter une approche critique avant de partager des informations en ligne en se questionnant sur qui peut voir leurs publications et les conséquences potentielles de ces partages.

PLUS PRÉCISÉMENT

Explorez les paramètres de confidentialité des comptes de vos enfants sur les réseaux sociaux et les autres plateformes en ligne. Faites attention aux paramètres de confidentialité par défaut, qui peuvent être plus permissifs que vous ne le souhaitez. Apprenez-leur à les ajuster pour renforcer la sécurité. Cette pratique inclut la personnalisation des personnes qui peuvent voir leurs publications ou les contacter et de la manière dont leurs données sont utilisées. Discutez de la différence entre rendre un compte totalement public, le restreindre aux amies et amis et le configurer en mode privé en utilisant le menu déroulant du navigateur pour sélectionner les réglages.

Encouragez vos enfants à se poser les bonnes questions avant de partager des informations en ligne. Qui peut les voir? Est-ce de l'information que je serais à l'aise de voir publiée sur Internet? La publication pourrait-elle me nuire dans l'avenir?

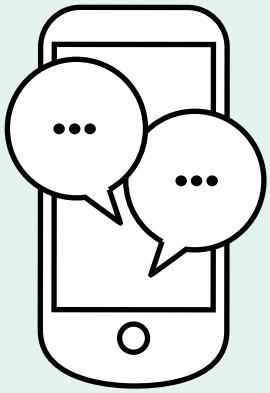
LA SÉCURITÉ PAR LE DESIGN : UTILISER LES OUTILS À NOTRE DISPOSITION

Les plateformes en ligne offrent une gamme d'outils conçus pour améliorer la sécurité et la confidentialité des utilisatrices et utilisateurs. Savoir s'en servir est un pas vers une expérience en ligne plus sécurisée.

EN PRATIQUE

Familiarisez-vous et vos enfants avec les outils et applications qui favorisent une communication sécuritaire. Par exemple, des applications de messagerie telles que Signal, WhatsApp et Telegram, qui se spécialisent dans le cryptage de données et permettent de contrôler l'accès à leurs profils.

Discutez des implications de l'utilisation des médias sociaux, y compris de la permanence des publications en ligne et de la façon dont elles peuvent impacter la réputation et l'empreinte numérique à long terme.



RÈGLES FAMILIALES POUR ASSURER LA COMMUNICATION SÉCURITAIRE EN LIGNE

Une liste de règles claires concernant le temps passé en ligne et les types de communication acceptables est une bonne pratique pour renforcer la sécurité en ligne tout en favorisant un environnement familial où la communication et la confiance sont préconisées. Voici des exemples de règles, avec des explications pour chacune d'elles, qui pourront vous guider dans la définition de vos propres règles familiales :

EXEMPLE

Pas plus de deux heures d'écran pour les loisirs en ligne par jour lors des jours d'école et pas plus de trois heures les fins de semaine et les jours fériés.

POURQUOI?

Cette règle aide à promouvoir un équilibre sain entre le temps passé en ligne et d'autres activités, comme les devoirs, la lecture, l'activité physique, le sport et le temps en famille. Cette pratique contribue aussi à prévenir la surutilisation d'Internet et sa dépendance.

2e RÈGLE : Périodes sans écran

EXEMPLE

Aucun écran pendant les repas et une heure avant de se coucher.

POURQUOI?

Les périodes sans écran encouragent la communication et l'interaction en face à face pendant les repas et aident à améliorer la qualité du sommeil en réduisant l'exposition à la lumière bleue avant le coucher.

3e RÈGLE : Communications avec des personnes de connaissance seulement

EXEMPLE

Ne communiquez en ligne qu'avec des personnes que vous connaissez et en qui vous avez confiance dans la vie réelle.

POURQUOI?

Cette règle vise à protéger contre les dangers potentiels de parler à des personnes inconnues en ligne, qui peuvent inclure des prédatrices et prédateurs en ligne ou des personnes cherchant à exploiter les jeunes utilisatrices et utilisateurs.

4e RÈGLE : Partage d'informations personnelles

EXEMPLE

Ne partagez pas d'informations personnelles (adresse, numéro de téléphone, nom de l'école) sur Internet sans permission parentale.

POURQUOI?

Le partage d'informations personnelles peut exposer les jeunes à des risques de sécurité, y compris le vol d'identité, le harcèlement en ligne ou pire. Cette règle vise à protéger leur vie privée et leur sécurité.

5e RÈGLE : Utilisation des paramètres de confidentialité

EXEMPLE

Utilisez les paramètres de confidentialité sur tous les réseaux sociaux et toutes les plateformes de communication pour contrôler qui peut voir vos informations et publications.

POURQUOI?

Activer et maintenir des paramètres de confidentialité appropriés protège contre le partage non intentionnel d'informations avec un public plus large qu'attendu et aide à maintenir un contrôle sur l'empreinte numérique personnelle.

Vie privée en ligne et codes d'accès

LES CLÉS DE LA FORTERESSE NUMÉRIQUE

Dans un monde connecté, où la vie privée et la sécurité en ligne sont essentielles, maîtriser la création et la gestion des mots de passe devient une habileté précieuse. Cela nous sert à protéger efficacement nos informations personnelles tout en tirant pleinement parti des possibilités qu'offre Internet. Les mots de passe agissent comme les gardiens de nos informations personnelles, protégeant l'accès à nos courriels, à nos réseaux sociaux et à nos autres plateformes numériques contre les intrusions non autorisées. De même, notre navigation sur le web, marquée par l'utilisation inévitable de témoins et de traceurs, requiert une attention particulière pour maintenir notre confidentialité face à la collecte incessante de données. Cette section vise à vous fournir des directives claires et pratiques pour que vous puissiez aider vos enfants à bien créer et gérer leurs mots de passe ainsi qu'à contrôler l'accès des témoins et traceurs.

MOTS DE PASSE : PLUS QU'UNE SIMPLE COMBINAISON

Les mots de passe sont la première ligne de défense contre l'accès non autorisé à vos informations personnelles et à celles de vos enfants. Cependant, leur efficacité repose sur leur complexité et la manière dont ils sont gérés.

Par exemple, si vous utilisez un même mot de passe simple comme Soleil123, pour tous vos comptes, de vos courriels à vos réseaux sociaux en passant par d'autres plateformes de multimédia, vous risquez qu'une ou un pirate devine facilement votre mot de passe, prenne le contrôle de vos comptes et accède à vos courriels personnels. Vous risquez ainsi d'exposer vos informations personnelles et privées, voire même vos informations financières et bancaires.

Quelques conseils pratiques sont présentés ci-dessous à l'égard de la création de mots de passe, de la gestion de ces derniers ainsi que de la vérification en deux étapes.

1er CONSEIL

Utiliser ces critères pour la création de mots de passe forts

- Contient au moins 12 caractères.
- Combine lettres, chiffres et symboles et varie les caractères (majuscules, minuscules, chiffres, symboles).
- Évite les informations personnelles, comme les anniversaires et les noms de famille.
- Est unique pour chaque compte.

2e CONSEIL

Bien gérer les mots de passe

Un gestionnaire de mots de passe, tel que 1Password et Bitwarden, gère, stocke et remplit automatiquement des mots de passe uniques et complexes pour chaque site que vous utilisez. Les gestionnaires éliminent le besoin de mémoriser ou de noter plusieurs mots de passe, rendant l'accès à vos comptes rapide et facile.

3e CONSEIL

Activer la vérification en deux étapes

La vérification en deux étapes ajoute une couche de sécurité supplémentaire en exigeant une deuxième forme d'identification, souvent un code temporaire envoyé par SMS ou généré par une application.

En général, voici la procédure pour activer l'authentification à deux facteurs (2FA) sur les comptes les plus sensibles, tels que les courriels, les réseaux sociaux et les plateformes de jeux.

- Accédez à votre compte.
- Accédez aux paramètres de sécurité.
- Trouvez l'option « Validation en deux étapes » et activez-la.
- Suivez les directives.

TÉMOINS ET TRACEURS : NAVIGUER AVEC DISCERNEMENT

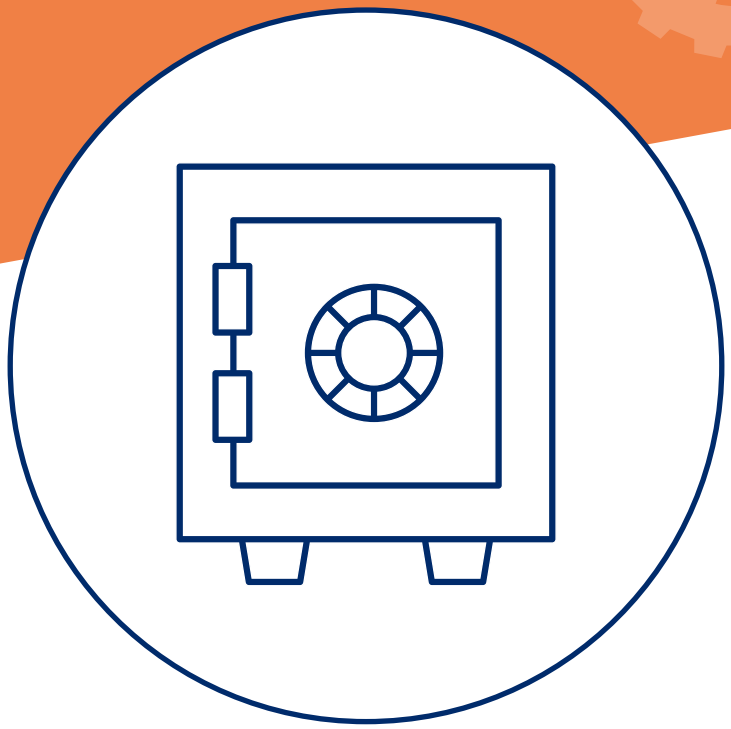
Les témoins (*cookies*) et les traceurs peuvent suivre notre activité en ligne et collecter des informations sur nos habitudes de navigation, nos intérêts et parfois même nos informations personnelles. Ce sont de petits fichiers stockés sur votre appareil par les sites web que vous visitez. Ils sont utilisés pour mémoriser vos préférences et activités en ligne. Bien qu'utiles pour une expérience personnalisée sur le web, ils peuvent aussi poser des risques pour la vie privée en permettant le suivi de vos activités en ligne. Ces quelques conseils pratiques s'avèrent utiles pour gérer et limiter l'activité des témoins et traceurs pour vous et vos enfants :

- **Ajustez les paramètres de confidentialité du navigateur** concernant la gestion des témoins. Certaines options permettent de bloquer les témoins tiers ou de les supprimer automatiquement après chaque session de navigation.
- **Utilisez le mode de navigation privée sur votre navigateur** afin d'éviter le stockage des témoins lors de sessions spécifiques.
- **Déconnectez-vous de vos comptes** lorsque vous avez terminé de les utiliser, particulièrement si ces comptes sont partagés entre plusieurs appareils.
- **Contrôlez la publicité ciblée** dans vos paramètres de confidentialité des comptes en ligne en limitant la collecte et l'utilisation des données.
- **Installez des extensions de navigateur dédiées au blocage des traceurs**[4] pour réduire le suivi en ligne.

4 Exemples d'extensions de navigateurs dédiées aux blocages des traceurs : uBlock Origin, Privacy Badger, DuckDuckGo Privacy Essentials, Ghostery, Disconnect.

La gestion sécuritaire de la vie en ligne de vos enfants commence par une compréhension et une application rigoureuse des principes de sécurité, en particulier en ce qui concerne les mots de passe et la navigation sur Internet.

Encouragez une culture de sécurité en ligne à la maison en expliquant que la protection de l'espace numérique de vos enfants est la responsabilité de toutes et tous. En mettant en pratique ces conseils, vous ferez un pas de plus vers une expérience en ligne plus sûre et plus respectueuse de votre vie privée ainsi que de celle de vos enfants.



Vérification de l'information et discernement

NAVIGUER ENTRE VRAI ET FAUX

Dans notre monde dynamique où l'information est à portée de clics, il est primordial que nos enfants apprennent à naviguer sur Internet avec réflexion et discernement. En tant que parents, nous jouons un rôle essentiel en ouvrant des discussions enrichissantes sur les contenus en ligne, en mettant en lumière l'importance des biais médiatiques et en démystifiant l'influence des algorithmes des réseaux sociaux.

Il est également crucial d'encourager nos enfants à adopter une approche critique de l'information. Cette approche inclut la vérification des sources, l'analyse de la date de publication et la distinction entre les faits et les opinions.

Promouvoir un comportement éthique en lien à l'information et encourager un partage responsable en ligne est tout aussi vital. Apprendre à nos enfants à réfléchir aux conséquences de partager des informations, en considérant l'impact potentiel sur autrui et la société, est essentiel pour limiter la diffusion de fausses nouvelles et pour favoriser un espace numérique plus respectueux et conscient.

Développer un esprit critique chez nos jeunes internautes les prépare à devenir des citoyennes et citoyens avertis et responsables, capables de distinguer le contenu de qualité et de contribuer positivement à la communauté en ligne. Cette section vous propose des conseils pratiques pour guider vos enfants dans l'apprentissage du discernement numérique, la reconnaissance de fausses nouvelles et la vérification des faits et des sources.

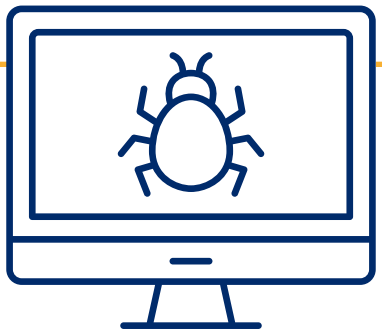
RECONNAÎTRE LES FAUSSES NOUVELLES : DÉMYSTIFIER LES INFORMATIONS TROMPEUSES

Éduquer vos enfants à reconnaître les différents angles sous lesquels une histoire peut être racontée est le premier pas vers la compréhension du concept de biais médiatiques. Cette pratique les aide à comprendre que les reportages et les articles peuvent présenter différents points de vue influencés par les perspectives et intentions de l'auteure ou de l'auteur.

Il est tout aussi important de discuter des rouages invisibles des algorithmes des réseaux sociaux qui peuvent inconsciemment nous enfermer dans des « bulles de filtres », où nous ne voyons que des informations qui renforcent nos croyances préexistantes, réduisant ainsi la diversité des perspectives auxquelles nous sommes exposées et exposés.

En tant que parents, vous pouvez aider vos enfants à comprendre cette dynamique et à encourager une exploration plus large du monde numérique. Cette pratique comprend l'importance de diversifier les sources d'information pour enrichir leur compréhension et développer une perspective plus équilibrée.

En discutant ouvertement de la manière dont les informations sont présentées et en encourageant la curiosité au-delà de leur fil d'actualité habituel, vous les aidez à devenir des consommatrices et consommateurs d'informations plus critiques et informés. Ce genre de discussion les prépare à naviguer de manière plus consciente et réfléchie dans le paysage numérique, tout en contribuant positivement à leur développement personnel et éducatif.



Il est également important de comprendre la différence entre ce qui est **une opinion** et ce qui est **un fait**, ainsi que d'apprendre à reconnaître un **langage subjectif**, c'est-à-dire des mots et des manières de s'exprimer qui montrent une opinion ou un biais. Cette sensibilité linguistique est la clé pour lire entre les lignes et reconnaître les intentions de l'auteure ou de l'auteur.

Aidez vos enfants à reconnaître les caractéristiques trompeuses des fausses nouvelles, telles que les titres sensationnalistes conçus pour générer des clics ou des réactions émotionnelles, qui sont souvent disproportionnés par rapport au contenu réel de l'article. Par exemple :

« Les médecins sont stupéfaits : Une mère de trois enfants découvre le remède contre le vieillissement! »

« Économie en chute libre : on prédit le prochain krach boursier dans quelques mois! »

« Le gouvernement cache-t-il des villes souterraines? Les théories deviennent réalité! »

- Apprenez à vos enfants à reconnaître ces titres qui utilisent l'hyperbole, soit une figure de style démesurée, l'émotion et la curiosité pour inciter le lectorat à cliquer ou à acheter le magazine ou le journal en version numérique.
- Expliquez-leur que les titres ou sous-titres sont souvent accompagnés d'articles qui n'ont pas nécessairement la substance ou les preuves pour étayer les affirmations extraordinaires du titre.

SENSIBILISATION À L'INTELLIGENCE ARTIFICIELLE : ATTENTION AUX « DEEPFAKES »!

L'intelligence artificielle (IA) joue un rôle de plus en plus influent dans notre manière de créer et de diffuser des informations sur Internet, ouvrant la porte à des innovations fascinantes, telles que les articles générés par machine, les œuvres d'art créées par l'IA et les hypertrucages (*deepfakes*). Ces derniers, qui utilisent des algorithmes d'apprentissage en profondeur (*deep learning*) pour modifier des images et des vidéos, peuvent enrichir des domaines comme l'éducation et le divertissement en rendant l'apprentissage plus créatif, interactif et engageant, tout comme ils peuvent aussi être utilisés pour tromper et manipuler.

Comme toute technologie puissante, l'IA nécessite une utilisation consciente et responsable. En tant que parents, il est essentiel de guider nos enfants à travers le paysage numérique complexe de l'IA. Nous pouvons les aider à comprendre à la fois les potentiels positifs et les défis éthiques associés à ces technologies, tels que le problème du consentement des personnes dont les images et les voix sont utilisées pour créer des contenus qui pourraient être nuisibles ou trompeurs et les problèmes et risques de désinformation.

En tant que parents, nous avons la responsabilité de soutenir nos enfants en leur apprenant à distinguer les sources fiables d'information, à repérer les contenus douteux et à utiliser des outils de vérification des faits, et ce particulièrement avec la venue de l'IA.

En faisant ainsi, nous les aidons à développer les habiletés et compétences essentielles pour devenir des citoyennes et citoyens responsables, capables de naviguer de manière éclairée à l'ère numérique dans un monde où l'IA joue un rôle croissant.

SOURCES VÉRIFIÉES ET DE QUALITÉ

Il est important d'encourager une approche sceptique et curieuse de l'information retrouvée en ligne pouvant provenir de fausses nouvelles ou d'hypertrucages créés par l'IA. Ces habiletés comprennent des stratégies telles que la prise en compte de la date de publication, l'actualité du sujet et la vérification de l'information afin de savoir si elle est soutenue par des sources fiables.

Encouragez vos enfants à utiliser des sources d'information diversifiées pour obtenir un spectre plus large d'opinions et de faits. Montrez-leur à utiliser les outils de recherche des bibliothèques en ligne et les bases de données scolaires pour accéder à des informations vérifiées et de qualité.

En plus des sites gouvernementaux, des conseils scolaires ainsi que des musées, voici quelques exemples de ressources et de bibliothèques en ligne accessibles en français, qui peuvent servir de références fiables pour des recherches approfondies et équilibrées :

ÂGE DE L'ÉLÉMENTAIRE

- **Le Centre franco :** offre des activités d'apprentissage et des ressources pédagogiques pouvant être utilisées à l'école et à la maison. (https ://www.lecentrefranco.ca/)
- **Les Débrouillards :** s'adresse aux jeunes scientifiques. On leur explique les comment et pourquoi de la vie quotidienne à travers des expériences, des défis et des démonstrations. (https ://www.lesdebrouillards.com/)
- **Lumni :** offre des contenus éducatifs gratuits pour les élèves de toutes les années d'étude. Cette ressource présente des vidéos, des jeux et des articles couvrant de nombreux sujets éducatifs pour les élèves de l'élémentaire et du secondaire. (https ://www.lumni.fr/)
- **National Geographic Kids (FR) :** propose des jeux éducatifs qui stimulent la curiosité des enfants sur le monde naturel, la science et les différentes cultures. (https ://www.nationalgeographic.fr/)
- **TFO :** est la télévision franco-ontarienne qui offre aux personnes en apprentissage, aux parents et aux pédagogues des contenus éducatifs et culturels d'avant-garde. (https ://www.tfo.org/)
- **Universalis Junior :** est une encyclopédie en ligne adaptée aux enfants et aux jeunes adolescentes et adolescents. Elle propose des articles, des médias et des ressources pédagogiques dans une variété de domaines. (https ://junior.universalis.fr/)

ÂGE DU SECONDAIRE

- **BanQ numérique (bibliothèque et archives nationales du Québec) :** propose une vaste collection numérique qui inclut des livres, des journaux, des magazines ainsi que des documents d'archives et des collections patrimoniales du Québec. (https ://numerique.banq.qc.ca/)
- **CAIRN.info :** est une plateforme spécialisée dans les domaines des sciences humaines et sociales, proposant des articles de revues universitaires, des livres et des encyclopédies majoritairement en français. (https ://www.cairn.info/)
- **Érudit :** est une plateforme diffusant des revues savantes francophones en sciences humaines et sociales et en sciences naturelles, offrant un accès à une riche documentation scientifique. (https ://www.erudit.org/fr/)
- **Gallica :** est une bibliothèque numérique de la Bibliothèque nationale de France qui offre un accès gratuit à des millions de documents, incluant des livres, des manuscrits, des cartes et des images, couvrant une vaste gamme de sujets historiques et culturels. (https ://gallica.bnf.fr/)
- **Le Centre franco :** offre des activités d'apprentissage et des ressources pédagogiques pouvant être utilisées à l'école et à la maison. (https ://www.lecentrefranco.ca/)
- **Lumni :** offre des contenus éducatifs gratuits pour les élèves de toutes les années d'étude. Cette ressource présente des vidéos, des jeux et des articles couvrant de nombreux sujets éducatifs pour les élèves de l'élémentaire et du secondaire. (https ://www.lumni.fr/)
- **TFO :** est la télévision franco-ontarienne qui offre aux personnes en apprentissage, aux parents et aux pédagogues des contenus éducatifs et culturels d'avant-garde. (https ://www.tfo.org/)

OUTIL DE VÉRIFICATION DES FAITS ET DES SOURCES

Afin d'aider vos enfants à naviguer avec discernement dans l'océan d'informations en ligne, il est essentiel de leur fournir des outils adéquats pour évaluer la crédibilité et l'exactitude de ce qu'elles et ils trouvent sur Internet. C'est dans cette optique qu'un outil de vérification des faits est proposé ci-dessous. Il est recommandé de l'adapter selon les besoins de vos enfants.

Évaluer la crédibilité des sources

- Quelles sont les compétences de l'auteure ou de l'auteur? Son expérience dans le domaine est-elle documentée et évidente?
- Quel est l'objectif du site?

Croiser les informations, consulter plusieurs sources

D'autres sources fiables rapportent-elles la même information? Sinon, pourquoi? Si une information est vraie, elle sera également rapportée par plusieurs médias ou sources fiables.

Analyser le ton et la formulation

- Le texte utilise-t-il un ton alarmiste ou sensationnel?
- Le texte présente-t-il des faits de manière neutre ou contient-il des mots chargés émotionnellement qui semblent vouloir influencer le lectorat?
- Le texte pose-t-il des questions provocatrices sans apporter de réponses claires?

Vérifier les dates et les contextes

Certaines fausses nouvelles utilisent des événements réels, mais les déforment ou les appliquent dans d'autres contextes.

- Quelle est la date de parution de l'article? Quelle est la date de rédaction? Est-ce normal?
- Est-il évident que le texte fait référence à une information dans son contexte intentionné?

Finalement, il est recommandé d'utiliser une application ou un site web dédié à la vérification des faits avec vos enfants, tels que Snopes ou FactCheck.org. Ces sites, et d'autres similaires, éduquent les lectrices et lecteurs sur la manière d'identifier les fausses nouvelles et d'analyser de manière critique les informations lues.

Ces outils de vérification des faits examinent les déclarations, les histoires et les rumeurs pour déterminer leur exactitude. Ils font également l'analyse des propos portant sur des personnalités publiques, des politiciennes et politiciens, des chaînes de courriels, des publications sur les réseaux sociaux et d'autres sources d'information qui peuvent être sujettes à des interprétations erronées ou à la diffusion de fausses nouvelles.

En conclusion, en éduquant vos enfants à reconnaître les biais médiatiques, à percer les « bulles de filtres » des algorithmes des médias sociaux et à discerner les faits des opinions, vous les outillez à devenir des consommatrices et consommateurs d'informations avertis.

De plus, en les sensibilisant à reconnaître les fausses nouvelles et les hypertrucages générés par l'intelligence artificielle, vous les préparez à faire face à la désinformation de manière proactive.

Encouragez-les à utiliser des outils de vérification des faits. La consultation de diverses sources fiables enrichira leur discernement numérique.

En appliquant ces habiletés et compétences, vos enfants pourront aborder l'espace numérique avec confiance et prudence, en valorisant la vérité et en apportant une contribution positive à la société de demain. Cette éducation les positionne non seulement comme consommatrices et consommateurs d'informations avertis, mais aussi comme des citoyennes et citoyens actifs et responsables dans un monde de plus en plus connecté.

Empreinte numérique et image en ligne

CONSTRUIRE UNE PRÉSENCE POSITIVE

Notre empreinte numérique, composée de tout ce que nous partageons, aimons et commentons en ligne, peut influencer profondément notre quotidien. Pour les jeunes d'aujourd'hui qui évoluent dans un monde où la séparation entre la vie privée et la vie publique s'estompe, il est crucial de leur apprendre à contrôler leur présence en ligne. Les informations qu'elles et ils publient peuvent rester accessibles indéfiniment, même après avoir tenté de les retirer. Ce contenu, susceptible d'être enregistré, redistribué ou utilisé de manières inattendues, peut influencer leur réputation et leurs occasions futures.

Face à un environnement où des employeurs et des institutions scolaires scrutent les profils numériques lors de leurs processus de sélection, il est essentiel d'enseigner à nos enfants à gérer leur empreinte numérique de manière prudente. En les guidant soigneusement avant de partager du contenu en ligne, nous les aidons à construire une présence numérique qui valorise leur personnalité et leurs valeurs de manière positive.

Nous vous proposons ici des conseils pratiques pour vous aider, en tant que parents, à accompagner vos enfants dans la création et la gestion de leur identité numérique. En adoptant ces recommandations, vous les équipez à naviguer avec assurance et responsabilité dans le monde numérique, optimisant ainsi leurs chances pour l'avenir tout en protégeant leur intégrité personnelle.

GÉRER SON IMAGE EN LIGNE

Commencez par inculquer la prudence et la réflexion. Encouragez vos enfants à prendre une pause avant de publier et à se poser des questions telles que la suivante : « Me sentirais-je à l'aise si cette information ou image était vue par n'importe qui, y compris des personnes inconnues ou les gens de mon futur milieu professionnel? » Expliquez-leur que toute publication devient une extension de leur réputation et peut être perçue comme un reflet de leur caractère et de leurs valeurs.

Aidez-les à assurer un audit régulier des paramètres de confidentialité sur tous leurs comptes de médias sociaux. Montrez-leur à ajuster les paramètres pour contrôler les personnes qui ont accès à leurs informations et publications. Assurez-vous qu'elles et ils comprennent les implications de chaque réglage de confidentialité et la différence entre une publication publique et une publication privée.

Finalement, soyez un modèle pour vos enfants en gérant votre propre image numérique avec soin et en montrant de bons exemples de comportements en ligne. L'apprentissage par l'exemple est souvent le plus efficace; en voyant leurs parents prendre des décisions réfléchies en ligne, les enfants sont plus susceptibles de reproduire ce comportement responsable. Ainsi, en accompagnant vos enfants à travers ces étapes, vous les aiderez à développer un sens de responsabilité numérique qui leur servira tout au long de leur vie.

CONSTRUIRE UNE PRÉSENCE POSITIVE

Pour aider vos enfants à établir une présence positive sur Internet, commencez par les encourager à partager leurs passions, talents et accomplissements de manière constructive. Les plateformes numériques peuvent être utilisées comme des portfolios où montrer leurs projets d'école, leurs participations à des événements, leurs réussites sportives ou artistiques et toute autre activité qui met en lumière leur engagement et leurs compétences. Invitez-les à partager les aspects positifs de leur vie pour que leur présence en ligne devienne un atout puissant, reflétant leur identité et leurs valeurs de manière authentique et inspirante.

Il est important d'accompagner nos enfants et de les aider à comprendre que leur comportement en ligne doit refléter leur véritable personnalité, tout comme dans la vie réelle. Cette cohérence est essentielle pour construire une présence numérique qui soit à la fois positive et authentique.

En les guidant à être elles-mêmes et eux-mêmes en ligne, vous les aidez non seulement à devenir des citoyennes et citoyens responsables à l'ère numérique, mais aussi à exploiter pleinement les possibilités qu'offre Internet. Parmi ces contributions, Internet inclut la création de relations saines, la participation à des projets collaboratifs enrichissants ainsi que l'accès à des ressources éducatives et professionnelles précieuses.

En conclusion, lorsque nos enfants apprennent à aligner leur comportement en ligne avec leur personnalité réelle, elles et ils se construisent une réputation qui est juste et respectable, et qui leur servira bien dans le futur. En leur enseignant à réfléchir avant de partager et en leur montrant l'exemple avec de bonnes pratiques numériques, vous leur donnez les outils nécessaires pour naviguer avec succès et intégrité dans le paysage numérique d'aujourd'hui et de demain. Ainsi, nos enfants seront mieux équipés pour profiter de tout ce que le monde numérique a à offrir, de manière sûre et responsable.

Cyberrespect et bienveillance

CITOYENNETÉ ET EMPATHIE NUMÉRIQUE

L'hyperconnectivité à laquelle sont exposées et exposés les jeunes d'aujourd'hui offre des occasions incroyables d'apprentissage et de connexion, enrichissant leur expérience éducative et sociale. Elle introduit également des occasions d'enseigner le respect et la bienveillance en ligne afin de s'assurer qu'elles et ils apprennent, comprennent les normes de comportement acceptable sur Internet et y adhèrent.

En tant que parents, vous avez une occasion unique de servir de modèle sur la manière de communiquer respectueusement en ligne, de respecter la vie privée des autres et de partager de manière réfléchie. En guidant vos enfants à naviguer de manière positive et responsable dans le monde numérique, vous les aidez non seulement à se comporter de manière éthique en ligne, mais également à interagir socialement de manière constructive et respectueuse.

CULTIVER L'EMPATHIE NUMÉRIQUE ET LE CYBERRESPECT

L'empathie numérique, ou la capacité à gérer ses émotions en ligne, à comprendre et à faire preuve d'empathie pour les autres à travers les plateformes numériques, est une habileté essentielle pour naviguer dans les interactions en ligne. Les quelques astuces suivantes vous aideront à cultiver l'empathie numérique et le cyberrespect chez vos enfants.

- **Encouragez-les à se mettre à la place de l'autre** et à réfléchir à la façon dont leurs messages et commentaires pourraient affecter les autres avant de les publier.
- **Proposez des exercices de perspective** dans lesquels elles et ils doivent réfléchir à ce qu'une personne pourrait ressentir en recevant un certain message ou un commentaire en ligne. Rappelez-leur que la personne qui reçoit le message ne voit pas les expressions faciales, par exemple, le sourire, les tremblements, le désintérêt et le rougissement.
- **Encouragez-les à nommer leurs émotions.** Apprenez-leur à reconnaître le moment où une conversation en ligne les affecte négativement et à prendre du recul. En parlant ouvertement de leurs émotions, elles et ils s'outillent de savoir-faire pour répondre de manière plus mesurée et réfléchie.
- **Encouragez les actions positives en ligne**, comme laisser des commentaires encourageants et positifs sur les publications de leurs amies et amis et partager des histoires inspirantes. Ces pratiques contribuent à créer une culture numérique où l'empathie et le soutien mutuel sont valorisés.
- **Outillez-les à gérer les désaccords.** Apprenez à vos enfants des stratégies pour gérer les désaccords en ligne de manière constructive en évitant les réponses impulsives et en cherchant à comprendre les points de vue opposés.

ACTIVITÉ PRATIQUE : SIMULATION DE SCÉNARIOS

Mettez en scène des scénarios de cyberinteraction où les jeunes peuvent pratiquer la réaction à diverses situations, de la réception d'un message inapproprié au partage de rumeurs, en appliquant les principes de la citoyenneté numérique et de l'empathie numérique. Discutez de la façon dont ces situations devraient être gérées de manière respectueuse.

Par exemple, si quelqu'un publie un commentaire négatif sur leur photo, décidez ensemble s'il est préférable de répondre calmement, de prendre du recul pour un moment, de ne pas répondre ou de signaler le commentaire aux administratrices et administrateurs du site.

Pour chaque scénario, envisagez plusieurs options de réponse et évaluez leurs conséquences potentielles. Soulignez l'importance de ne pas agir impulsivement en ligne et de prendre le temps de réfléchir à la réponse la plus respectueuse et appropriée. Ce genre de réponses peut inclure l'emploi d'un langage poli, le choix de ne pas répondre aux provocations et l'adoption d'une approche empathique en essayant de comprendre la perspective de l'autre personne.

Enfin, soulignez que le respect en ligne inclut également le respect de la vie privée d'autrui. Cela signifie obtenir le consentement avant de partager des informations ou des photos d'autres personnes et respecter leurs choix et opinions, même lorsqu'ils diffèrent des leurs.

CHARTE FAMILIALE DU CYBERRESPECT

La charte proposée ci-dessous vise à établir des lignes directrices pour un comportement en ligne respectueux et responsable au sein d'une famille. Elle incite les personnes à encourager une présence positive sur Internet et à fournir un cadre pour la gestion des comportements négatifs.

NORMES DE CYBERRESPECT

Communication positive
Nous nous engageons à communiquer de manière positive et constructive, en évitant les mots blessants, les sarcasmes mal placés et les jugements hâtifs.

Confidentialité et consentement
Nous respectons la vie privée d'autrui et demandons toujours le consentement avant de partager des informations et des photos qui ne nous appartiennent pas personnellement.

Empathie et compréhension
Nous faisons l'effort de comprendre les situations du point de vue des autres avant de réagir en rappelant que chaque personne a ses propres défis ou contraintes.

RESPECT DES DIFFÉRENCES

Tolérance
Nous acceptons et respectons les différences, que ce soit les opinions, les intérêts ou les origines, et nous nous opposons à toute forme de cyberintimidation et de discrimination.

Dialogue ouvert
Nous promouvons le dialogue et la discussion ouverte sur des sujets controversés tout en faisant preuve de politesse et de respect.

GESTION DES COMPORTEMENTS NÉGATIFS

Signalement de discussion
En cas d'une situation en ligne où des comportements négatifs sont adoptés, nous en discutons en famille et, si nécessaire, signalons ces comportements aux plateformes concernées.

Soutien familial
Nous offrons un soutien familial à toute personne confrontée à des comportements négatifs en ligne en prenant le temps de discuter de l'incident et des émotions suscitées.

CONSÉQUENCES

Tout manquement aux normes établies dans cette charte entraînera une discussion familiale et des mesures éducatives appropriées pour comprendre et corriger le comportement.

Une possibilité pourrait être de faire signer la charte à l'ensemble des membres de la famille adhérant à l'énoncé suivant.

« En adhérant à cette charte, nous nous engageons collectivement à maintenir un environnement numérique sain, soutenant et respectueux, qui reflète les valeurs de notre famille. Nous nous soutenons mutuellement dans l'apprentissage et l'adaptation à l'évolution constante de notre environnement numérique en restant unies et unis face aux défis et en célébrant ensemble les possibilités qu'il nous offre. »

Éduquer les jeunes sur le cyberrespect et la bienveillance est un processus continu qui nécessite engagement et patience. En mettant l'accent sur le comportement positif, la citoyenneté numérique, l'empathie, et en discutant ouvertement des conséquences des actions négatives, les parents peuvent équiper leurs enfants des outils nécessaires pour naviguer dans le monde numérique de manière respectueuse et bienveillante. Cet apprentissage contribue à la création d'un espace en ligne plus sûr et plus accueillant pour toutes et tous.

Cyberintimidation

RECONNAÎTRE ET RÉAGIR

Internet offre d'innombrables possibilités pour apprendre, créer des liens et s'exprimer. Avec les bonnes stratégies, les jeunes peuvent exploiter ces occasions favorables de manière sûre et positive, notamment en ce qui concerne le développement de leurs relations interpersonnelles. Malgré ces aspects positifs, la cyberintimidation est un problème grandissant qui touche un grand nombre de jeunes aujourd'hui et duquel il est important de s'informer continuellement.

La cyberintimidation peut prendre diverses formes, allant du harcèlement en ligne aux menaces, en passant par la diffusion de rumeurs et le partage non consenti d'informations personnelles. Elle peut avoir des conséquences profondes sur le bien-être émotionnel et physique des jeunes. Toutefois, cette section est conçue pour vous équiper de manière positive et vous fournir des outils efficaces pour aider vos enfants à naviguer avec confiance et résilience dans leurs interactions en ligne.

Les méthodes proposées ci-dessous aideront vos enfants non seulement à gérer et à contrer la cyberintimidation, mais aussi à renforcer leur capacité à se tenir debout avec assurance et intégrité dans l'environnement numérique parfois tumultueux. En développant ces compétences, elles et ils pourront transformer les défis en occasions de croissance personnelle et de développement de la résilience, ouvrant la voie à un avenir plus sûr et plus positif en ligne.

SIGNES DE LA CYBERINTIMIDATION

Les signes de la cyberintimidation ne sont pas toujours évidents. Voici quelques indicateurs de cyberintimidation dont vos enfants pourraient être victimes :

- **Changement de comportement –** recherche de solitude, irritabilité accrue, changements d'humeur.
- **Réactions émotionnelles –** tristesse ou colère après l'utilisation d'Internet ou des appareils mobiles.
- **Évitement –** refus d'aller à l'école ou d'utiliser des appareils électroniques.
- **Symptômes physiques –** troubles du sommeil, maux de tête, perte d'appétit.
- **Performances scolaires –** baisse notable des performances scolaires.

COMMENT RÉAGIR EN TANT QUE PARENT?

Si vous suspectez ou découvrez que vos enfants sont victimes de cyberintimidation, voici quelques conseils que vous pourriez privilégier :

- **Écoutez sans juger –** encouragez vos enfants à parler de leurs expériences. Écoutez attentivement sans minimiser leurs sentiments.
- **Ne répondez pas –** conseillez à vos enfants de ne pas répondre à l'intimidatrice ou à l'intimidateur. Souvent, ne pas réagir diminue l'intérêt de la personne qui intimide.
- **Offrez du soutien émotionnel ou professionnel –** offrez un soutien émotionnel constant. Dans les cas de cyberintimidation graves, il peut être nécessaire de chercher l'aide de professionnelles et professionnels, tels que le personnel enseignant et la direction d'école, qui pourront effectuer les démarches nécessaires auprès du conseil scolaire, ou bien de demander de l'aide d'une ou d'un psychologue ou des organismes spécialisés dans la lutte contre la cyberintimidation.

PLAN D'ACTION CONTRE LA CYBERINTIMIDATION

Afin de vous outiller à soutenir vos enfants en cas de cyberintimidation, voici un exemple de plan d'action que vous pourriez adapter selon vos besoins. Il vise non seulement à fournir des réponses immédiates en cas de cyberintimidation, mais également à inculquer une approche proactive et préventive pour assurer la sécurité et le respect de soi en ligne.

ÉTAPE 1 Documenter

Gardez des captures d'écran et des enregistrements des incidents de cyberintimidation comme preuves.

ÉTAPE 2 Réagir immédiatement de manière appropriée

Répondre de manière constructive peut transformer une situation négative en une occasion d'apprentissage et d'affirmation de soi. Quelques exemples de réponses :

- Affirmation de soi : « Je vois que ton commentaire est blessant et il n'est pas apprécié. Si tu as un problème avec moi, parlons-en respectueusement ou discutons-en avec une médiatrice ou un médiateur pour le résoudre. »
- Réponse éducative : « Je ne sais pas si tu le sais, mais ce que tu dis en ligne peut vraiment blesser les gens. Je t'invite à réfléchir aux impacts de tes écrits sur les autres. »
- Redirection vers un comportement positif : « Je sais que nous pouvons toutes et tous avoir de mauvais jours, mais utilisons nos plateformes pour encourager et soutenir les autres au lieu de les dénigrer. »

Ceci dit, parfois, la réponse la plus constructive est de ne pas s'engager directement dans un discours avec l'intimidatrice ou l'intimidateur et de ne pas répondre à ses provocations. Les personnes qui intimident cherchent souvent une réaction; ne pas leur en donner peut les décourager de continuer.

ÉTAPE 3 **Bloquer l'auteure ou l'auteur de la cyberintimidation**

Utilisez les fonctionnalités de blocage sur les plateformes pour empêcher la personne qui intimide de poursuivre ses actions. Modifiez les paramètres de confidentialité pour restreindre qui peut voir et interagir avec les publications et profils de vos enfants.

ÉTAPE 4 **Signaler l'incident**

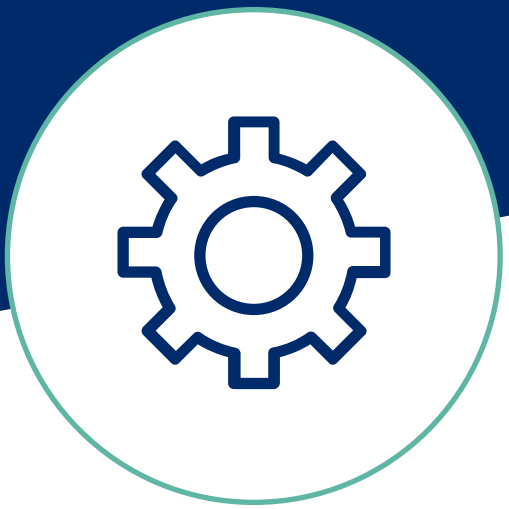
Signalez l'incident aux plateformes concernées et, si nécessaire, à l'école ou aux autorités. Expliquez clairement la raison pour laquelle le contenu est considéré comme de la cyberintimidation lors du signalement.

ÉTAPE 5 **Chercher du soutien**

Encouragez fortement vos enfants à parler à une personne adulte de confiance immédiatement. Cette personne peut, par exemple, être une ou un parent, un autre membre de la famille, une enseignante ou un enseignant ou une direction d'école. Discuter de l'incident et de ses sentiments avec une ou un adulte peut grandement aider à traiter l'expérience émotionnelle et à décider des prochaines étapes.

La cyberintimidation est un défi complexe nécessitant une approche proactive et informée de la part des parents. En éduquant vos enfants sur les signes et les réactions appropriées ainsi qu'en fournissant les outils et les ressources nécessaires, vous pouvez les aider à naviguer dans l'espace numérique de manière plus sûre et confiante.

Le soutien, l'écoute et la communication ouverte sont essentiels pour bâtir la résilience de vos enfants face à la cyberintimidation.



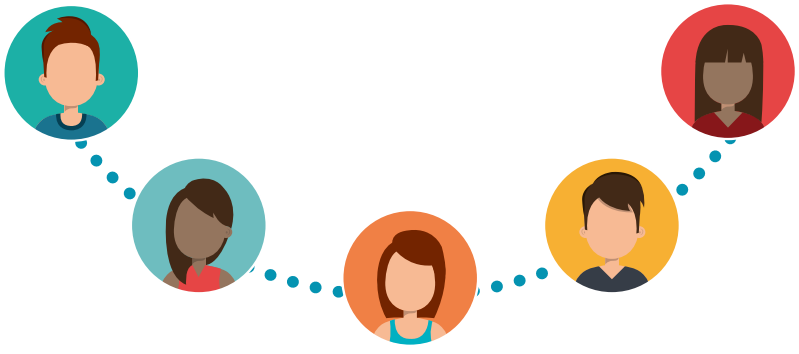
Pour conclure

Nous terminons ce livret en rappelant l'importance vitale d'une éducation numérique complète et empathique. En équipant nos jeunes avec des stratégies ciblées et efficaces, nous les préparons, non seulement à reconnaître et à contrer la cyberintimidation, mais aussi à établir une présence en ligne à la fois positive et respectueuse. Leurs interactions en ligne, lorsqu'elles sont guidées par l'empathie et le respect, peuvent enrichir l'expérience éducative et sociale.

Ce livret vous a fourni des outils pratiques pour aider vos enfants à naviguer avec assurance dans le monde numérique en valorisant et en développant une citoyenneté numérique responsable. En apprenant à aligner leur comportement en ligne avec leurs valeurs et leur identité réelle, elles et ils posent les bases d'une réputation en ligne authentique et respectée, qui les servira bien dans l'avenir.

Enfin, comme parents, notre rôle ne s'arrête pas à fournir un accès technologique, mais aussi à être des modèles pour encourager nos enfants à adopter de saines habitudes à long terme (par exemple : publication réfléchie et modérée de photos, temps d'utilisation). Nos enfants nous observent et cherchent à nous imiter. Notre rôle implique aussi de guider, de soutenir et de participer activement à l'éducation numérique de nos enfants. Continuer d'apprendre et d'adapter les conseils de ce guide à vos besoins familiaux renforcera, non seulement la sécurité numérique de vos enfants, mais également vos liens familiaux, en faisant de l'espace numérique un lieu d'apprentissage et de croissance partagée.

Ainsi, ensemble, nous pouvons façonner un avenir numérique sûr et enrichissant pour nos jeunes en les guidant vers une utilisation d'Internet à la fois responsable, sécuritaire, éthique et éclairée.



Références

COMMUNICATION SÉCURITAIRE EN LIGNE : PARAMÈTRES DE SÉCURITÉ

Commissariat à la protection de la vie privée. (2019). *Règles à la maison à élaborer vous-même pour la protection des renseignements personnels en ligne*. https ://www.priv.gc.ca/biens-assets/youth-plan/index2_f

Pensez cybersécurité. (s. d.). Sécurisez vos appareils. Gouvernement du Canada. https ://www.pensezcybersecurite.gc.ca/fr/securisez-vos-appareils

CYBERINTIMIDATION

Éducaloi. https ://educaloi.qc.ca/?s=cyberintimidation

HabiloMédias et Telus. (2018). *Aider nos enfants à composer avec la cyberintimidation*. https ://habilomedias.ca/sites/default/files/guides/guide_aider_nos_enfants_composer_avec_cyberintimidation.pdf

CYBERRESPECT

Sécurité publique Canada et HabiloMédias. (2017). *Guide de la civilité en ligne à l'intention des parents*. https ://habilomedias.ca/sites/default/files/guides/guide-civilite-en-ligne.pdf

RISQUES LIÉS À LA SÉCURITÉ EN LIGNE : CE QUE TOUT PARENT DEVRAIT SAVOIR

Commissariat à la protection de la vie privée du Canada. (le 8 mars 2024). *12 conseils pratiques en matière de protection de la vie privée à l'usage des parents.* https ://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/campagnes-et-activites-de-sensibilisation/sensibilisation-des-enfants-a-la-vie-privee/fs-fi/tips/

Cyberaide.ca. https ://cyberaide.ca/fr/

HabiloMédias et Telus Averti. (2018). *Aider nos enfants à naviguer notre monde numérique : Guide pour les parents de TELUS Averti.* https ://habilomedias.ca/sites/default/files/guides/guide_aider_nos_enfants_naviguer_notre_monde_numerique.pdf

Le Centre franco et Toronto Metropolitan University. (s. d.). *La sécurité en ligne : comprendre les risques.* https ://cybersecurite.lecentrefranco.ca/

Pensez cybersécurité. (s. d.). La cyber sécurité simplifiée pour les enfants. Gouvernement du Canada. https ://www.pensezcybersecurite.gc.ca/fr/blogues/la-cyber-securite-simplifiee-pour-les-enfants

Pensez cybersécurité. (2022). Les menaces à la cybersécurité que toute la famille doit surveiller. Gouvernement du Canada. https ://www.pensezcybersecurite.gc.ca/fr/blogue/surveiller-cybermenaces-famille

Verreault, L. et Cadets Canada. (2022). Transmettez la cyberprudence de génération en génération. Gouvernement du Canada. https ://www.pensezcybersecurite.gc.ca/fr/blogues/transmettez-la-cyberprudence-de-generation-en-generation

VÉRIFICATION DES FAITS ET DES SOURCES

HabiloMédias. (s. d.). *Comment savoir ce qui est vrai (et ce qui ne l'est pas) sur Internet*. Un guide Au-delà des faits. https ://habilomedias.ca/sites/default/files/guides/guide_au_dela_des_faits.pdf