Tech Safe BC

Glossaire de sécurité et mauvais usage des technologies destinées aux enfants

Technologies destinées aux enfants



Télécharger le PDF

Dernière mise à jour: Le 12 novembre 2026

Il peut être difficile de se tenir au courant des dernières avancées technologiques, et ceci, sans compter celles qui concernent les enfants. Il faut dire que les nouvelles fonctionnalités et les paramètres de confidentialité semblent évoluer à un rythme effréné. Ce document vise à expliquer les technologies destinées aux enfants et leurs fonctionnalités, ainsi que la manière dont une mauvaise utilisation par un auteur de violence peut compromettre la sécurité.

En consultant ce glossaire, on peut garder à l'esprit que:

- Ce n'est pas la technologie qui est à la source du problème… C'est la violence. (Sécurité technologique Canada, 2025)
- Une expertise en technologie n'est nullement nécessaire pour s'orienter quand celle-ci est utilisée à mauvais escient; des ressources et des réseaux de soutien sont là pour nous aider.
- La sécurité est la priorité.

Si certaines informations contenues dans ce guide ne sont plus à jour ou sont difficiles à comprendre, n'hésitez pas à nous joindre à techsafe@bcsth.ca.

Tech Safe BC

Table des matières:

04 Partage familial

06 Consoles de jeux

08 Médias sociaux

11 Téléphones intelligents et tablettes

13 Montres intelligentes et moniteurs d'activité physique

15 Jouets intelligents

17 Jouets IA

18 GPS et Smart Finders

20 Stalkerware

Partage familial

Ce dont il s'agit:

Le partage familial est une fonctionnalité qui permet aux membres d'un même foyer de partager leurs achats numériques, leurs abonnements et les contrôles parentaux dans le cadre d'un seul forfait, plutôt que de payer séparément pour chaque compte.

Caractéristiques:

- Abonnements partagés (musique, vidéos, espace de stockage, services de jeux, etc.)
- Achats partagés (applications, livres électroniques, films, jeux, etc.)
- Contrôles parentaux (limites de temps d'écran, filtres de contenu, autorisation des achats)
- Outils partagés (calendriers, photos ou localisation)

Risque concernant l'appareil ou le compte d'un enfant:

- Utiliser la localisation partagée pour suivre les déplacements d'un enfant.
- Vérifier quelles applications, quels livres électroniques ou quels contenus multimédias sont utilisés et contrôler l'accès à ces services.
- Si des mots de passe sont partagés ou si des appareils sont synchronisés, l'auteur peut accéder aux messages, aux courriels ou consulter le contenu enregistré.
- Limiter ou surveiller le temps que les enfants passent devant un écran ou leur utilisation d'applications afin d'influencer vos décisions parentales.
- Installer des applications de suivi ou des outils de contrôle parental pour surveiller ou limiter l'utilisation des appareils.
- Effectuer des achats excessifs avec la carte de crédit associée au compte.

- Consulter des comptes pour trouver une nouvelle adresse ou d'autres renseignements personnels.

Stratégies pour reprendre le contrôle de l'appareil:

- Envisagez de créer un nouveau compte distinct pour l'enfant sur un appareil qui n'est pas surveillé par l'auteur de violence. Il peut s'agir, par exemple, d'un compte iCloud ou Google.
- Désactivez les fonctions de partage de position sur tous les appareils et dans toutes les applications.
- Si cela semble sécuritaire, utilisez l'authentification à deux facteurs. De cette manière, même si l'auteur connaît le mot de passe, il lui sera impossible de se connecter.
- Évitez les fonctions de synchronisation automatique sur les nouveaux appareils; utilisez des NIP ou des mots de passe distincts pour chaque appareil.
- Vérifiez régulièrement les paramètres du compte, surtout lorsque l'enfant revient d'une visite chez l'auteur.
- Cherchez de l'aide et du soutien.

Ressources supplémentaires:

- Partage familial d'Apple: Quitter un groupe familial
- La famille Google: Page d'assistance

Consoles de jeux

Ce dont il s'agit:

Un appareil conçu pour jouer à des jeux vidéo sur un téléviseur ou un écran d'ordinateur. Les consoles modernes permettent également la lecture numérique de flux vidéo ou audio et facilitent la communication.

Caractéristiques:

- **Bibliothèque de jeux**: Choisir et jouer à des jeux numériques que vous pouvez acheter dans la boutique de la console.
- **Jeu en ligne**: Plusieurs joueurs s'y rassemblent par l'entremise d'Internet.
- **Outils de communication**: Chat vocal, messagerie ou listes d'amis.
- **Services d'abonnement**: Accès à des collections de jeux
- **Contrôle parental**: Possibilité de limiter le temps de jeu, l'accès à certains contenus ou les dépenses sur les comptes des enfants.
- **Médias**: Regarder des films et écouter de la musique en continu, par le biais de services comme Netflix, YouTube, Spotify, etc., ou simplement sur Internet.
- **Sauvegardes et services infonuagiques:** Sauvegarder la progression d'un jeu en ligne pour y accéder depuis plusieurs consoles.

Risques liés à une console utilisée par un enfant:

- Suivi des jeux auxquels l'enfant ou l'adolescent joue, de la durée de ces sessions et des personnes qui l'entourent dans les espaces virtuels.
- Accès à des messages privés ou aux listes d'amis.
- Contrôler les achats ou les abonnements et restreindre l'accès.
- Manipuler les mesures de contrôle parental afin de nuire à la personne survivante et à sa relation avec son enfant.

- Utiliser la fonction de jeu à distance ou des appareils connectés pour surveiller ou limiter l'utilisation de la console.
- Créer un faux compte et envoyer une demande d'ami à un enfant ou à un adolescent pour renouer le contact.

Stratégies pour reprendre le contrôle de l'appareil:

L'utilisation d'une console de jeux à des fins néfastes peut se produire par le biais du contrôle parental, des comptes partagés ou de l'accès aux identifiants de connexion, des appareils associés ou de la fonction de jeu à distance, de l'accès aux achats ou aux abonnements partagés, ainsi que par des flux d'activité de la console ou des paramètres de notification de celle-ci.

Par conséquent, pour sécuriser l'appareil, il faut:

- Penser à créer un compte de jeu distinct vous permettant l'accès aux fonctions de contrôle parental.
- Utiliser des mots de passe forts et uniques.
- Activer l'authentification à deux facteurs.
- Vérifier et supprimer les appareils associés, puis vous déconnecter de tous les appareils inutilisés.
- Si possible, utiliser des comptes de paiement distincts.
- Modifier les paramètres de confidentialité sur la console pour masquer votre statut en ligne, l'historique de vos jeux et votre liste d'amis; vérifier régulièrement ces paramètres pour vous assurer qu'ils n'ont pas été modifiés.

Un important rappel: L'utilisation des consoles de jeux pour manipuler ou exercer un contrôle constitue de la violence, et cela n'est pas acceptable. Selon la situation familiale, certaines des stratégies mentionnées ci-dessus peuvent ne pas s'appliquer. Il est toutefois important de comprendre comment la technologie peut être utilisée à mauvais escient afin d'élaborer des stratégies adaptées aux besoins des personnes survivantes.

Guides concernant différentes consoles de jeu:

- **Nintendo**: Sécurité en ligne
- **PlayStation**: Outils et conseils de sécurité
- **Xbox**: Sécurité en ligne et paramètres de confidentialité

Ressources:

- **Sécurité Technologique Canada**: Jeux en ligne: Risques et stratégies en matière de protection de la confidentialité.

Médias sociaux

Ce dont il s'agit:

Les médias sociaux désignent les plateformes en ligne et les applications qui permettent de créer et de partager du contenu, tout en interagissant avec d'autres personnes par le biais de profils, de messageries et de communautés.

Caractéristiques:

- Les utilisateurs disposent de «profils» comprenant certains renseignements personnels tels que le nom, des photos, une biographie et l'historique des activités.
- Amis ou abonnés: réseau de personnes qui se connaissent et les personnes célèbres ou influentes que l'on peut suivre.
- Le partage de contenu consiste à publier des photos, des vidéos, des liens et permet la diffusion en direct. Cela comprend également la création de «stories» qui sont des contenus numériques éphémères.
- Les outils de communication comprennent la messagerie directe (MD), les appels vocaux, les appels vidéo et les discussions de groupe.

- Possibilité de commenter ou de répondre aux publications.
- Possibilité de réagir aux publications à l'aide d'émojis, de partages et de republications.

Risques liés aux comptes de médias sociaux pour enfants:

- **Harcèlement ou humiliation publique**: Commentaires ou réponses inappropriés sur un profil, visibles par la communauté en ligne reliée au compte. Utiliser la fonction de messages éphémères pour envoyer un message blessant qui s'efface automatiquement au bout d'un délai choisi par l'expéditeur.
- **Usurpation d'identité et manipulation**: Créer un ou plusieurs faux profils et envoyer une ou plusieurs demandes d'ami dans le but de contrôler, de harceler ou de nuire.
- **Suivi ou surveillance**: Utiliser des renseignements diffusés en ligne de manière malveillante ou dans le but d'exercer un contrôle.

Stratégies pour reprendre le contrôle du compte:

- Créez un nouveau compte pour votre enfant en choisissant un nom d'utilisateur difficile à trouver (à l'aide de la barre de recherche de la plateforme) sur un appareil sécurisé.
- Choisissez une photo de profil générique, qui ne représente ni la survivante ni son enfant.
- Supprimez ou désactivez le compte.
- Bloquez ou mettez en sourdine la ou les personnes malveillantes, si vous pouvez le faire en toute sécurité.
- Conservez les preuves de la violence numérique en effectuant une capture d'écran ou un enregistrement vidéo de l'écran (cela s'applique aux messages éphémères).

- Consignez les faits de l'auteur et signalez-les à la plateforme.
- Limitez les renseignements partagés sur la plateforme.
- Communiquez avec vos amis et vos proches en qui vous avez confiance par messagerie directe (MD).
- Évitez de publier des vidéos, des stories ou des snaps qui révèlent votre emplacement ou des renseignements personnels visibles à l'arrière-plan (p. ex., des panneaux de rue, des noms d'écoles ou des points de repère reconnaissables).
- Vérifiez régulièrement vos paramètres de confidentialité. Rendez vos profils «privés» et surveillez qui peut voir vos publications, les mentions ou les messages qui vous sont adressés.
- Désactivez la fonction de géolocalisation.
- Passez en revue votre liste d'amis et d'abonnés, puis bloquez ou supprimez toute personne suspecte.
- Déconnectez-vous de tous les appareils que vous n'utilisez pas.

Ressources supplémentaires:

- **Tech Safe BC**: Ressources sur les médias sociaux
- **Sécurité technologique Canada**: Conseils sur la sécurité et la confidentialité sur les médias sociaux
- **Sécurité technologique Canada**: Documenter la violence technologique
- **Sécurité technologique Canada**: Sécurité et confidentialité technologiques: Une trousse d'outils pour les survivantes
- **Commissaire à la sécurité en ligne (gouvernement de l'Australie)**: Bibliothèque vidéo: Protégez vos technologies (anglais)
- **Comprendre la fonctionnalité des messages éphémères**: Snapchat (anglais), Instagram (anglais), WhatsApp (anglais, Facebook Messenger (anglais), Signal (français).

Téléphones intelligents et tablettes

Ce dont il s'agit:

Les appareils mobiles et les tablettes font désormais partie intégrante du quotidien des enfants et des jeunes; ils leur permettent de demeurer connectés avec leur entourage, de faire leurs devoirs et d'accéder à des ressources et à de l'information. Les fonctionnalités de ces appareils sont similaires à celles d'un ordinateur, mais leur format les rend plus faciles à transporter.

Caractéristiques:

- Communication: Appels et textos, appels vidéo et vocaux, messagerie instantanée et courriels.
- Internet et connectivité via le Wi-Fi, les données cellulaires, le Bluetooth et les points d'accès Hotspot.
- Possibilité de télécharger des applis, par exemple des applis de médias sociaux, de communication, éducatives et des jeux en ligne, etc.
- Localisation et navigation.

Risques liés à l'appareil d'un enfant:

- Recevoir des appels, des vidéos ou des textos perturbants de la part de l'auteur.
- Utiliser la fonction de messages éphémères d'une application pour envoyer des messages blessants.
- Suivi ou surveillance de l'emplacement de l'appareil.
- Installation d'applications de suivi de localisation sur l'appareil.
- Utilisation des paramètres de contrôle parental en vue de nuire à l'autre parent.

Stratégies pour reprendre le contrôle de l'appareil:

- Si cela peut se faire en toute sécurité, bloquez le contact ou empêchez l'accès à l'appareil et à l'emplacement, par exemple à l'aide de la fonction «Localiser» de Apple.
- Prenez immédiatement une capture d'écran ou une vidéo d'enregistrement d'écran du message violent afin de conserver des preuves.
- Sur un iPhone, utilisez la fonction Vérification de sécurité pour voir qui a accès à l'appareil, à sa localisation et à ses applications. Vérifiez les renseignements personnels du compte ainsi que les paramètres de confidentialité et de sécurité de l'appareil.
- Vérifiez si votre appareil contient des applis inconnues ou nouvelles.
- Consultez la section «Notre plan de sécurité technologique» pour prendre connaissance du plan de sécurité.
- Découvrez d'autres façons de sécuriser votre appareil grâce à: Guide des téléphones pour les survivantes, par Sécurité technologique Canada.

Ressources supplémentaires:

- **Sécurité technologique Canada**: Page d'accueil
- **Comprendre la fonctionnalité des messages éphémères**: Snapchat (anglais), Instagram (anglais), WhatsApp (anglais, Facebook Messenger (anglais), Signal (français).

Montres intelligentes et moniteurs d'activité physique

Ce dont il s'agit:

Les montres intelligentes et les moniteurs d'activité physique ont peut-être l'apparence d'une montre, mais fonctionnent comme un mini-ordinateur. Elles se connectent à un téléphone intelligent (via Wi-Fi ou Bluetooth) et transmettent des données liées à la santé ou à l'activité physique, tout en permettant une connexion à un téléphone intelligent.

De nombreuses montres intelligentes destinées aux enfants nécessitent une connexion à une application parentale.

Caractéristiques:

- Communication, comme les appels vocaux et messageries
- Localisation et suivi
- Un moniteur d'activité physique compte les pas, mesure la fréquence cardiaque, etc.
- Peut être associé au service «Partage familial», selon le modèle.

Risques liés à la montre intelligente d'un enfant:

- Utilisation malveillante de fonctions de communication pour entrer en contact avec l'enfant ou l'autre parent.
- Suivi de la localisation: Il se peut que l'auteur suive les déplacements de l'enfant grâce à une application parentale ou aux fonctions de partage familial de la montre.
- Accès au compte: L'auteur pourrait avoir accès aux comptes liés à l'appareil.
- Le suivi des données relatives à la santé d'un enfant comme forme de surveillance.

Stratégies pour reprendre le contrôle de l'appareil:

- Vérifiez les appareils ou les comptes associés: Assurez-vous que la montre ne se connecte qu'à des appareils ou comptes de confiance.
- Vérifiez les autorisations de l'appli: Vérifiez ce qui est partagé et avec qui à l'aide de l'appli.
- Sur un iPhone, utilisez la fonction Vérification de sécurité pour voir qui a accès à l'appareil, à sa localisation et aux applis.
- Assurez-vous que la fonction GPS ou de partage de position est désactivée.
- Envisagez d'effectuer une réinitialisation d'usine, car cela supprime toutes les connexions cachées et permet de créer une nouvelle connexion avec des téléphones ou des comptes sécuritaires.
- Nous vous invitons à consulter le site Web officiel de l'appareil en cas de problèmes et à communiquer avec son centre d'aide.

Ressources supplémentaires:

- **Apple Watch**: Guide de sécurisation de l'appareil (Anglais)
- **Fitbit:** Paramètres relatifs aux données et à la confidentialité de Fitbit

Jouets intelligents

Ce dont il s'agit:

Les jouets intelligents offrent des fonctionnalités supplémentaires grâce à leur connexion à Internet ou à des applis, et permettent d'interagir d'une manière qui était impossible auparavant. Selon le jouet, celui-ci peut être équipé de capteurs, de microphones, de caméras, Bluetooth, Wi-Fi ou de fonctionnalités d'IA (intelligence artificielle).

Caractéristiques:

Bien que chaque jouet intelligent soit différent, les caractéristiques suivantes peuvent se présenter:

- Possibilité de se connecter à un autre appareil, comme un téléphone, à une tablette ou à Internet.
- Peut s'activer par la voix, le mouvement ou le toucher.
- Peut se souvenir du nom de l'enfant, de ses préférences, etc.
- Jouer un rôle pédagogique ou éducatif, comme pour les mathématiques, les langues, etc.
- Divertir par des jeux, des histoires, des vidéos ou de la musique.

Risques liés au jouet:

- Surveillance des conversations à partir des enregistrements stockés par le jouet.
- Suivi de la localisation si le jouet intelligent est équipé d'un GPS ou si les paramètres de localisation sont activés.
- Surveillance de l'appli liée au jouet intelligent.
- Communiquer avec l'enfant ou l'autre parent grâce aux fonctions de communication du jouet.

Stratégies pour reprendre le contrôle de l'appareil:

- Chaque modèle de jouet intelligent est différent. Pour bien comprendre ses caractéristiques, il est important de consulter les détails de ce jouet en particulier sur le site du fabricant, surtout si l'enfant a remarqué quelque chose d'inhabituel.
- Est-ce que ce jouet peut être connecté à une appli?
- Faut-il une connexion Bluetooth ou Wi-Fi pour le faire fonctionner?
- Privilégiez la sécurité immédiate; n'abordez pas la question du jouet avec l'auteur.
- Considérez-le comme un appareil d'enregistrement potentiel, éteignez-le (si vous pouvez le faire en toute sécurité) ou déplacez-le dans une autre pièce en invoquant une raison neutre, comme «il faut nettoyer cette pièce».
- Placez le jouet dans quelque chose qui empêcherait tout enregistrement, par exemple à l'intérieur de serviettes.
- Signalez tout cas présumé d'utilisation fautive et communiquez avec votre intervenante pour trouver ensemble une solution.
- Vérifiez si le jouet enregistre des données sur le nuage. Si possible, désactivez les fonctionnalités des services infonuagiques.
- Désactivez les paramètres de localisation ou le GPS sur le jouet.
- Désactivez l'accès à tous les microphones.
- Désactivez les fonctions Wi-Fi ou Bluetooth du jouet lorsque vous ne l'utilisez pas.
- Envisagez de réinitialiser l'appareil et de le jumeler à nouveau à un compte de confiance, si possible.
- Préparez un plan de sécurité avec votre enfant grâce à notre programme «Safe Tech».

Ressources supplémentaires:

- **Sécurité technologique Canada**: Préoccupations liées à la sécurité des jouets intelligents
- **Projet *Safety Net***: Jouets intelligents et localisation (Anglais)

Jouets IA

Ce dont il s'agit:

Les jouets dotés d'IA (intelligence artificielle) utilisent les capacités des robots conversationnels pour interagir avec les enfants. Cette IA tente d'apprendre, en quelque sorte, à reconnaître les émotions et les sentiments humains pour jouer avec les enfants. Cette fonctionnalité peut être intégrée à des jouets tels que des poupées, des peluches, des figurines ou encore des jouets technologiques pour enfants, comme les robots.

Les caractéristiques peuvent inclure:

- Audio.
- Vidéo.
- Microphone
- Reconnaissance faciale ou gestuelle.

Risques liés à l'utilisation:

- Les jouets peuvent comprendre un «mode de surveillance parentale», donnant accès à l'historique des conversations ou permettant de surveiller un enfant en temps réel.
- Un parent peut également allumer le jouet à l'aide de l'appli qui lui est associée.

Stratégies:

- Chaque modèle de jouet est différent. Pour bien comprendre ses caractéristiques, il est important de consulter la fiche descriptive du jouet en question sur le site du fabricant, surtout si vous ou votre enfant avez remarqué quelque chose d'inhabituel.
    - Est-ce que ce jouet peut être connecté à une appli?

    - Faut-il une connexion Bluetooth ou Wi-Fi pour faire fonctionner le jouet?
- Privilégiez la sécurité immédiate; n'abordez pas la question du jouet avec l'auteur.
- Considérez-le comme un appareil d'enregistrement potentiel, éteignez-le (si vous pouvez le faire en toute sécurité) ou déplacez-le dans une autre pièce en invoquant une raison neutre, comme «il faut nettoyer cette pièce».
- Placez le jouet dans quelque chose qui peut atténuer tout bruit susceptible d'être enregistré, par exemple à l'intérieur de serviettes.
- Signalez tout cas présumé d'utilisation malveillante et communiquez avec votre intervenante pour gérer la situation ensemble.

GPS et Smart Finders

Ce dont il s'agit:

Un GPS est un système qui permet à un appareil ou une application de suivre en temps réel les déplacements d'une personne sur de longues distances. Un Smart Finder est un appareil muni d'un Bluetooth ou d'une connexion à bande ultra-large (UWB) qui peut être dissimulé dans des effets personnels afin de suivre les déplacements d'une personne.

Remarque: La technologie UWB permet d'obtenir une précision de 30 à 100 mètres, selon l'appareil.

Caractéristiques:

- **GPS**: Conçu pour le suivi en temps réel sur de vastes zones.
- **Smart Finder**: Conçu pour le suivi de localisation à courte portée.

Risques liés à la mauvaise utilisation:

- Suivi de la localisation dans le but de harceler ou de contrôler les déplacements de l'enfant ou d'un des parents.

Stratégies:

- En cas de danger immédiat, composez le 911 ou le numéro des services d'urgence de votre région.
- Pour obtenir de l'aide auprès d'un organisme local, communiquez avec Victim Link BC au 1-800-563-0808.
- Désactivez le partage de la localisation lorsque vous ne l'utilisez pas.
- Documentation: Prenez des captures d'écran ou des photos afin de conserver des preuves de la surveillance (p. ex., en prenant des captures d'écran d'une alerte de localisation suspecte, d'un message ou d'une application qui semble inhabituelle, ou en prenant une photo d'un dispositif de surveillance physique) avant de retirer l'auteur du service.
- Il convient également de consigner par écrit la date, l'heure et les détails relatifs à la découverte du dispositif de suivi (voir Registre des actes de violence facilités par la technologie de la BCSTH) (anglais).
- Désactivez le Bluetooth ou tout partage de position dans les paramètres de l'appareil.
- Inspectez les effets personnels de l'enfant (en particulier après une visite chez l'auteur): les jouets, l'intérieur des souliers, la doublure des manteaux, les valises ou les sacs à dos sont autant d'endroits où un dispositif de repérage pourrait être dissimulé.
- S'il s'agit d'un traceur physique, évitez de le manipuler plus que nécessaire. Si vous devez l'enlever, prenez-en une photo et mettez-le dans une poche Ziploc à titre de preuve.
- Selon la situation, communiquez avec les professionnels concernés (services de soutien, intervenante PEACE, défenseure juridique, avocate spécialisée en droit de la famille, etc.) pour les informer de cette infraction.

Ressources supplémentaires:

- **Sécurité technologique Canada**: Guide de la survivante pour la surveillance des déplacements

Stalkerware

Ce dont il s'agit:

Un «stalkerware» comprend les outils, logiciels, applications ou tout dispositif qui permettent à une autre personne de surveiller et d'enregistrer secrètement des renseignements provenant d'un appareil qui ne lui appartient pas. Bien que chaque «stalkerware» permette à la personne qui en traque une autre d'accéder à différents niveaux de fonctionnalités du téléphone (p. ex., textos, agenda, contacts), il peut être difficile de déterminer si l'appareil a été compromis.

Les signaux concernant l'appareil peuvent inclure:

- La batterie se décharge rapidement.
- Des pics inattendus dans la consommation de données.
- Augmentation inattendue du temps passé devant les écrans chaque semaine.
- Des avis ou des textos étranges ou inconnus.
- Baisse soudaine du rendement de l'appareil.
- Modifications inattendues des paramètres de l'appareil.
- Des appels inexpliqués sur votre facture téléphonique.
- Surchauffe importante de l'appareil.
- Il est difficile d'éteindre l'appareil.
- Bruit de fond pendant les appels téléphoniques.

Stratégies pour reprendre le contrôle de l'appareil:

- **Document**: Si un logiciel de surveillance est détecté sur l'appareil, consignez toutes les preuves avant de supprimer quoi que ce soit. Au Canada, il est illégal d'installer un logiciel sur l'appareil d'une autre personne sans son consentement, y compris des logiciels espions comme les Stalkerware.
- **Réinitialisation aux paramètres d'usine**: Si possible, envisagez de réinitialiser l'appareil aux paramètres d'usine; cela effacera toutes les données. Avant d'envisager cette option, assurez-vous de sauvegarder toutes vos données importantes en les enregistrant ou en les téléchargeant sur un appareil fiable (p. ex., photos, contacts, etc.).
- **Faites confiance à votre instinct**: Si l'utilisation de l'appareil ne justifie pas que ce dernier soit devenu instable ou ne réponde plus, il se peut qu'il ait été compromis. Il serait peut-être judicieux de le faire examiner par un spécialiste.
- **Nouvel appareil temporaire**: Un nouvel appareil pourrait permettre de créer de nouveaux comptes et d'en limiter l'accès aux seules personnes de confiance.
- **Utilisez une protection antivirus couvrant les logiciels espions**: Selon l'appareil, il est possible qu'une application de sécurité puisse être téléchargée sur celui-ci. Des analyses régulières de l'appareil (en particulier après qu'un enfant a été en contact avec l'auteur) permettraient de déterminer si l'appareil a été compromis et, le cas échéant, à quel moment.
- **Pour découvrir d'autres stratégies, consultez le site de Sécurité technologique Canada**: Guide de sécurité: Stalkerware pour téléphones.

Ressources supplémentaires:

- **Sécurité technologique Canada**: Logiciels espions pour appareils mobiles: Identification, suppression et prévention.

Autres ressources utiles:

- Glossaire technologique: Glossaire complet des termes et du vocabulaire technologiques (anglais).

Commentaires: Cette ressource est en constante évolution; aidez-nous à l'améliorer. N'hésitez pas à nous faire savoir s'il manque quelque chose ou si vous avez des suggestions qui pourraient aider d'autres jeunes au cas où la technologie serait utilisée à leur encontre par un membre de la famille. *Veuillez remplir ce court formulaire*. Merci beaucoup.

Si vous êtes victime de violence liée aux technologies, il existe de l'aide. Trouvez du soutien au sein de votre communauté en communiquant avec un *programme membre de la BC Society of Transition Houses* ou consultez nos autres ressources en matière de sécurité à l'adresse *techsafebc.bcsth.ca*.

©BC Society of Transition Houses, projet Tech Safe BC, 2026. Nous encourageons le partage de ce contenu, à condition que la BC Society of Transition Houses soit mentionnée.