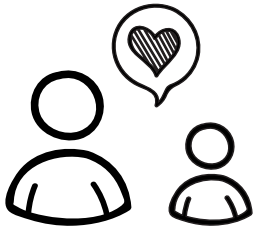
Faire Attention :

S'arrêter.
Réfléchir.
Se connecter.

FRENCH



Pour aider les enfants de votre entourage à être en sécurité en ligne, *Faire Attention : S'arrêter. Réfléchir. Se connecter.* propose quelques idées pour vous aider à entamer une conversation avec eux. Choisissez une section et lisez-la ensemble pour découvrir comment partager avec précaution, être gentil en ligne, résister au cyberharcèlement et protéger leurs (et vos) informations personnelles en ligne. Ces outils peuvent vous aider à montrer aux enfants comment faire de bons choix et utiliser la technologie de manière responsable. Et, en parlant avec eux, vous les amenez à comprendre qu'un adulte digne de confiance est là pour les aider quand ils commettent des erreurs.

To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

Être en ligne fait partie de votre vie. Vous regardez et créez du contenu, publiez des photos et des vidéos, jouez à des jeux et partagez avec vos amis et votre famille votre localisation et ce que vous faites. Mais publier, jouer et se connecter en ligne n'est pas sans risque. Certaines personnes et situations que vous rencontrez ne sont pas toujours ce qu'elles semblent être.

Quelle que soit la rapidité de vos doigts sur un clavier, un téléphone ou une tablette, les meilleurs outils dont vous disposez pour éviter les risques en ligne sont votre cerveau et votre temps. Arrêtez-vous et réfléchissez aux situations qui vous aideront à vous protéger, ainsi que vos amis et votre famille, vos comptes et vos appareils. Sinon vous risquez de partager trop d'informations, de vous rendre ridicule, d'embarrasser d'autres personnes, d'endommager votre ordinateur ou de parler à des personnes qui ne sont pas ce qu'elles prétendent être.

- ✓ PARTAGER AVEC PRÉCAUTION
- ✓ C'EST SUPER D'ÊTRE GENTIL
- ✓ RÉSISTER AU CYBERHARCÈLEMENT
- ✓ LA CONNEXION DE PROTECTION

PARTAGER AVEC PRÉCAUTION

Réfléchissez avant de partager

Ce que vous faites en ligne a des conséquences dans le monde réel. Les photos, vidéos et messages que vous partagez ont une incidence sur vous, votre vie privée, votre réputation et celles des personnes qui vous entourent, maintenant et dans l'avenir. Arrêtez-vous et réfléchissez avant de publier.

Ce que vous publiez pourrait avoir une « cible » plus importante que vous ne le pensez.

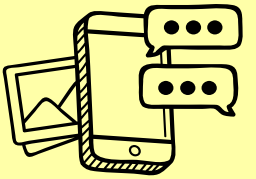
Vous ne pouvez pas totalement contrôler qui voit votre profil, vos photos, vos vidéos ou vos textes, même si vous utilisez des paramètres de confidentialité ou des applications qui suppriment votre contenu après sa visualisation ou dans les 24 heures suivantes. Tous ceux qui voient vos publications peuvent en faire une capture d'écran ou un enregistrement. Posez-vous la question : « Est-ce que je voudrais que quelqu'un se lève en plein déjeuner et partage cette photo ou cette vidéo avec toute la cafetéria ? »

Ce que vous partagez peut avoir une incidence sur les autres. Il peut être embarrassant, injuste et même dangereux d'envoyer ou de publier des photos et des vidéos sans avoir obtenu l'autorisation des personnes qui y figurent. Obtenez d'abord l'accord de chaque personne. Avant de faire une publication, demandez : « Es-tu d'accord si je publie ça sur les réseaux sociaux ? » Si la personne refuse, ne publiez pas ce contenu.

Une fois que vous avez publié un contenu en ligne, il est impossible de revenir en arrière

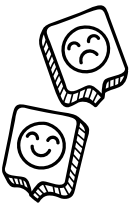
Même si vous supprimez un contenu que vous avez publié, ou si la publication expire, cette photo ou ce commentaire que vous ne voulez plus que les gens voient pourrait être sauvegardé, partagé et demeurer quelque part en ligne, définitivement.

Sextage : Ne faites pas ça



Vous avez peut-être entendu des histoires, à l'école ou dans les journaux, à propos de personnes qui s'adonnent au « sextage », qui envoien des photos de « nudes » à partir de leurs téléphones. Ne faites pas ça. Point. La création, la transmission ou même la sauvegarde de photos, de vidéos ou de messages sexuellement explicites mettent en péril vos amitiés et votre réputation. Pis encore, vous pourriez enfreindre la loi.

Remarque sur les médias sociaux



D'après l'administrateur de la santé publique des États-Unis, l'utilisation des médias sociaux peut vous nuire, en fonction du temps que vous passez sur les plateformes, du type de contenu que vous voyez et de la façon dont cela perturbe des activités essentielles pour votre santé comme le sommeil ou l'exercice physique.

C'EST SUPER D'ÊTRE GENTIL

Il est important d'être poli

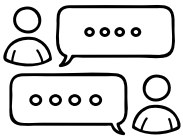
Lorsque vous ne pouvez pas voir les expressions faciales, le langage corporel ou d'autres signaux visuels d'une personne en ligne, vous pouvez vous sentir libre de publier ou de dire des choses que vous ne diriez pas en face. Mais lorsque vous envoyez des textos, des messages directs, des e-mails, que vous publiez ou jouez à des jeux vidéo, c'est comme si vous parliez à quelqu'un en personne. Songez à la manière dont vous communiquez et réfléchissez avant de parler ou de publier.

Ralentissez. Il est facile d'avoir des malentendus en ligne. Avant d'envoyer un message, demandez-vous : « Comment les autres personnes se sentiront-elles face à ce message ? »

Prenez en compte et respectez les points de vue et les sentiments des autres en ligne, comme vous le feriez en face. N'oubliez pas : de vraies personnes se trouvent derrière les avatars et noms de profil.

Soyez modéré. Évitez d'écrire tout en MAJUSCULES, d'utiliser de longues séries de points d'exclamation ou de gros caractères gras. C'est la même chose que de crier.

Ne mettez pas tout dans la discussion de groupe. Avant d'envoyer un message de groupe ou d'appuyer sur Répondre à tous, arrêtez-vous et réfléchissez : Qui a besoin de voir ce message ?



Ne vous faites pas passer pour autrui

Il est répréhensible et potentiellement blessant de créer des profils, des commentaires ou des messages qui semblent provenir de quelqu'un d'autre, par exemple d'un camarade de classe ou d'un professeur.

Parlez franchement

Si vous voyez un ami publier quelque chose d'irréfléchi ou de dangereux, dites-le-lui. Vous pouvez éviter à votre ami d'avoir des ennuis et de se couvrir de ridicule. Si vous voyez quelque chose d'indécent en ligne, signalez-le et parlez-en à un adulte de confiance. La plupart des applications et plateformes proposent un moyen de signaler un comportement menaçant ou indécent.

RÉSISTER AU CYBERHARCÈLEMENT

Chaque personne a le droit de se sentir en sécurité dans ses interactions de tous les jours avec les autres, que ce soit en ligne ou en personne.

Si quelqu'un publie des commentaires méchants, des mèmes blessants, des photos embarrassantes ou envoie des conversations ou des messages privés à votre sujet, il s'agit de harcèlement. Ce n'est pas acceptable. Adressez-vous à un adulte de confiance pour obtenir de l'aide et décider de la manière dont vous devez réagir.

Si vous êtes victime de harcèlement en ligne, voici ce qu'il faut faire :

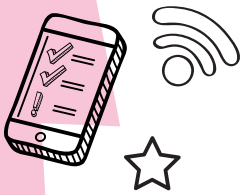
- **Ignorez** la personne ou bloquez-la afin de l'empêcher de vous contacter à nouveau.
- **Sauvegardez l'historique** et demandez l'aide d'un adulte de confiance.
- **Signalez-le.** De nombreuses applications et plateformes disposent des outils permettant de signaler un comportement indécent ou menaçant.

Le harcèlement amène souvent la victime à se sentir mal, et donne une mauvaise image de l'intimidateur.

Harceler quelqu'un peut également vous causer des ennuis avec votre école ou la police.

Si vous êtes témoin de harcèlement en ligne, trouvez des moyens de devenir un « défenseur », c'est-à-dire quelqu'un qui intervient, interrompt ou prend la parole pour y mettre fin. Les comportements méchants cessent généralement assez rapidement lorsque quelqu'un prend la défense de la personne victime de harcèlement.

La connexion de protection



Protégez votre vie privée

Quoi que vous fassiez en ligne, vous laissez une trace. Prenez les mesures suivantes pour vous assurer que cette trace ne mène pas à des informations que vous n'aviez peut-être pas l'intention de partager.

Utilisez les paramètres de confidentialité. Découvrez comment activer les paramètres de confidentialité pour les appareils, les applications et les comptes de médias sociaux, puis activez-les. Cela vous permet de limiter les personnes qui peuvent voir votre localisation, vos publications, et qui peuvent communiquer avec vous.

Vérifiez vos paramètres de localisation. Certaines applications vous permettent de voir la localisation de vos amis. Elles partagent également la vôtre. Réfléchissez aux circonstances dans lesquelles il est judicieux de communiquer votre localisation. Lorsque cela n'est

pas le cas, désactivez le partage de votre localisation. Les fonctionnalités de vos appareils, comme l'appareil photo, peuvent contenir des informations sur l'endroit où vous vous trouviez lorsque vous avez pris une photo. Si vous ne voulez pas indiquer où vous étiez à chaque selfie, désactivez votre localisation sur l'appareil photo de votre téléphone. Demandez-vous toujours : « Cette application a-t-elle besoin de savoir où je me trouve ? »

Vos amis en ligne doivent uniquement être les personnes que vous connaissez réellement. Cela peut être amusant de communiquer avec des amis par le biais de messages écrits, médias sociaux ou jeux vidéos, mais certaines personnes ne sont pas ce qu'elles prétendent être en ligne. Et si vous ne faites pas attention, vous pourriez partager vos informations personnelles avec un parfait inconnu.

Protégez vos informations

Une fois que vous donnez vos informations personnelles, telles que votre numéro de sécurité sociale, vos mots de passe ou vos coordonnées bancaires, à une personne que vous ne connaissez pas, vous n'avez aucun moyen de revenir en arrière.

Voici quelques conseils pour protéger vos informations en ligne :

Ne répondez pas aux messages qui demandent des informations personnelles. Même si le message semble venir d'un ami, d'un membre de la famille ou d'une entreprise que vous connaissez, ou s'il indique que quelque chose de grave

se produira si vous ne répondez pas. Il est fort probable qu'il s'agisse d'un message mensonger, envoyé pour voler vos informations. Demandez à un adulte de confiance de vous aider à le signaler comme indésirable ou spam.

Vérifiez les informations auxquelles une application veut avoir accès, avant de la télécharger. Certaines applications demandent l'autorisation d'accéder à des informations ou à des fonctionnalités dont elles n'ont pas besoin, comme votre liste de contacts, votre appareil photo, votre espace de stockage, votre localisation et votre microphone. Demandez à un adulte de confiance de vous aider à lire la politique de confidentialité de l'application pour savoir comment vos données seront utilisées et si elles seront partagées. Décidez ensuite si ce jeu de mots a vraiment besoin d'accéder à vos photos.

Discutez avec un adulte de confiance avant d'effectuer des achats intégrés, surtout si le service est payant.

Protégez vos comptes

Vous conservez beaucoup d'informations personnelles sur vos comptes en ligne. Voici quelques mesures à prendre pour empêcher d'autres personnes d'accéder à vos comptes.

Créez des mots de passe forts.
Plus votre mot de passe est long, plus il est difficile à pirater. Utilisez au moins 12 caractères avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Envisagez d'utiliser une phrase de passe composée de mots aléatoires pour la rendre

plus facile à mémoriser. Mais n'utilisez pas d'expressions courantes, de paroles de chansons ou de citations de films faciles à deviner.

Soyez unique. Créez différents mots de passe pour vos différents comptes. Ainsi, si quelqu'un obtient le mot de passe de l'un de vos comptes, il ne pourra s'en servir pour accéder à vos autres comptes. Vous pouvez utiliser un gestionnaire de mots de passe pour garder une trace de tous vos différents mots de passe.

Gardez-les confidentiels. Ne partagez vos mots de passe avec personne, même pas votre meilleur ami ou quelqu'un avec qui vous sortez.

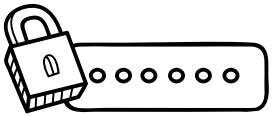
Soyez pointilleux pour ce qui est des questions de sécurité.

Essayez de choisir des questions de sécurité auxquelles vous seul pouvez répondre. Sautez les questions dont les réponses pourraient être trouvées en ligne, comme votre code postal, votre lieu de naissance ou le nom de jeune fille de votre mère. Si vous ne pouvez pas éviter ces questions, alors faites preuve de créativité ! Considérez-les comme les mots de passe, et utilisez des réponses assez longues et difficiles à deviner. Assurez-vous simplement de vous souvenir de vos réponses.

Utilisez l'authentification multifacteur. De nombreux comptes offrent une protection supplémentaire à vos comptes au moyen d'une « authentification multifacteur », ce qui exige autre chose qu'un simple mot de passe.

L'authentification multifacteur associe quelque chose que vous connaissez (comme un mot de passe) à quelque chose que vous avez (comme un code d'accès généré par une application) ou qui vous identifie intrinsèquement (comme une empreinte digitale).

En cas de violation, changez rapidement les mots de passe. Si une entreprise vous informe que des données ont été violées et qu'un pirate informatique aurait pu obtenir votre mot de passe, modifiez directement le mot de passe que vous utilisez pour ce compte. Changez-le également pour tout compte utilisant un mot de passe similaire.



Protégez vos appareils

La meilleure façon de profiter des activités en ligne ? S'assurer que vos appareils sont sûrs et sécurisés. Commencez par ces points :

Paramétrez la mise à jour automatique des logiciels de sécurité pour tous vos appareils, navigateurs internet et systèmes d'exploitation. Cela vous aide à vous protéger contre les nouvelles menaces de sécurité.

Ne cliquez pas sur des liens et n'ouvrez pas des pièces jointes. Si vous recevez un texte, un e-mail ou un message inattendu en ligne qui vous demande de cliquer sur un lien ou d'ouvrir une pièce jointe, ne le faites pas, même s'il s'agit d'une offre d'avantages gratuits. Les liens et les pièces jointes peuvent cacher des virus ou des logiciels espions qui pourraient endommager votre téléphone, votre ordinateur ou votre tablette.

Protégez vos appareils par un mot de passe. Vous éviterez ainsi que vos photos, messages et comptes ne se retrouvent entre de mauvaises mains.

Conservez-les en lieu sûr. Ne laissez jamais votre téléphone, votre ordinateur portable ou votre tablette devant tout le monde, même pas pendant une minute.

En savoir plus en suivant le lien

This booklet helps kids socialize safely online. There's help on how to share with care, be kind online, stand up to cyberbullying, and protect their personal information. Get free copies in English or Spanish at

ftc.gov/bulkorder

FEDERAL TRADE COMMISSION

Août 2023