



Sécurité en ligne

Qu'est-ce que la sécurité en ligne?

Le concept de sécurité en ligne intervient lorsque des personnes essaient d'assurer leur sécurité pendant qu'elles utilisent leur téléphone ou leur ordinateur en ligne. Pour plus de sécurité en ligne, les gens ont non seulement besoin de connaître les risques liés à l'Internet, mais ils ont également besoin de savoir comment réduire ces risques afin de se protéger.



Les médias sociaux peuvent être utilisés dans le but de se sentir heureux, fier, excité et aimé. Cependant, ils peuvent également provoquer des sentiments de tristesse, de souffrance, de honte chez les gens et les blesser. Il est important que chacun apprenne à mieux se protéger lorsqu'il est en ligne. Si vous apprenez à utiliser les médias sociaux de façon plus sécurisée, vous pourrez augmenter vos opportunités en termes d'expériences positives sur les médias sociaux et limiter les risques d'être blessé.





Sécurité en ligne

Harcèlement, discrimination et vol d'identité en ligne

Harcèlement et discrimination

Le harcèlement et la discrimination peuvent revêtir plusieurs formes sur Internet. Les formes les plus courantes sont le **cyberharcèlement** et la **cyberintimidation**.

- Le **cyberharcèlement** consiste à donner à une personne ou à recevoir d'une personne une attention répétée et importune en ligne ou sur le téléphone sans son autorisation.
- La **cyberintimidation** consiste à utiliser l'Internet pour intimider les gens. Il s'agit de la publication et du partage de renseignements désobligeants, préjudiciables et faux sur une personne.



Le fait d'être harcelé ou intimidé en ligne provoque souvent chez les gens un sentiment de gêne et d'insécurité. Le cyberharcèlement et la cyberintimidation peuvent être considérés comme des pratiques illégales.

Vol d'identité

On parle de vol d'identité lorsqu'une personne utilise les renseignements personnels d'une autre sans sa permission. Le fait de partager votre numéro de téléphone personnel, des informations sur votre lieu de résidence, sur votre établissement scolaire et même le nom de votre animal familier peut permettre à une personne de vous pirater, prendre votre identité et prétendre être vous!



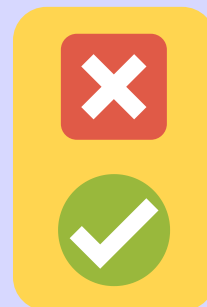


Sécurité en ligne

Prendre des décisions plus sûres en ligne

Consentement

Si une personne publie quelque chose (p. ex. une photo) concernant une autre en ligne, elle doit obtenir le consentement préalable de cette personne (elle doit demander à la personne l'autorisation de publier dans les médias sociaux quelque chose qui la concerne). Par exemple, si vous publiez une photo, une vidéo, une capture d'écran, etc. qui appartiennent à une autre personne ou qui contiennent des informations sur cette autre personne, vous devez alors demander et obtenir son autorisation avant la publication dans les médias sociaux.



Partage de renseignements

Tout ce qui est publié sur Internet y reste pour toujours! Le partage de renseignements personnels en ligne peut permettre à une personne d'avoir accès à vos comptes de médias sociaux, votre compte bancaire ou votre courrier électronique et de recueillir vos renseignements sans votre autorisation et à votre insu. Cela est également considéré comme du piratage de vos comptes en ligne.



Gestion des relations en ligne

Le fait de savoir à qui vous parlez sur les médias sociaux peut vous aider à vous protéger contre le cyberharcèlement et la cyberintimidation. Il est important d'être très prudent lorsqu'on échange avec des personnes étrangères en ligne. Une personne peut facilement créer un faux compte avec de fausses photos et prétendre être une autre personne en ligne. Ceci est également connu comme du « catfishing ». Lorsqu'on connaît avec qui l'on parle et avec qui l'on échange des informations sur les médias sociaux, on est capable de se protéger contre les prédateurs, la cyberintimidation et le vol d'identité.



Sécurité en ligne

Utilisation des médias sociaux

Les gens utilisent les technologies numériques et de communication, notamment les cellulaires, les téléphones intelligents, l'Internet et les médias sociaux pour montrer des choses dont ils sont fiers, pour se faire des amis et pour apprendre. Ces technologies peuvent également servir à l'imagination et être utilisées comme outils de communication, de mise en relation et/ou pour créer des communautés.

La cyberintimidation, le cyberharcèlement et le harcèlement sont courants sur Internet, notamment par le biais des médias sociaux, d'où l'importance d'apprendre à utiliser les médias sociaux de façon plus sécurisée.



Agir avec précautions



La majorité des applications pour médias sociaux disposent de directives de sécurité qui décrivent comment utiliser ces applications de façon plus sécurisée. Ces directives se retrouvent normalement dans la section paramètres de l'application du média social.

Vous pouvez également avoir recours à un conseiller pédagogique de confiance ou à une autorité pour vous assister dans l'utilisation des médias sociaux de façon plus sécurisée.



Sécurité en ligne

Utilisation des médias sociaux

Conseils pour une utilisation plus sécurisée des médias sociaux

- Ajoutez, suivez et parlez uniquement à des personnes que vous connaissez sur les médias sociaux
- Ne publiez aucun renseignement personnel vous concernant sur les médias sociaux
 - **Ne partagez pas** votre numéro de téléphone, des informations sur votre établissement scolaire, sur votre domicile, vos renseignements bancaires, etc.
- Gardez les informations relatives à vos comptes de médias sociaux confidentiels
 - Les gens peuvent garder les informations relatives à leurs **comptes de médias sociaux confidentiels**. Pour ce faire, ils peuvent aller dans les paramètres de confidentialité et protéger leurs comptes. Lorsque le compte d'une personne est paramétré comme étant privé, cela signifie que des personnes étrangères ne peuvent ni entrer en contact avec elle ni voir son compte ou quoi que ce soit qu'elle publie ou partage sur ce compte. Les personnes autorisées à suivre une personne sur les médias sociaux (ex. les amis et la famille) sont les seules à voir ses informations et ses photos sur son compte.





Sécurité en ligne

Utilisation des applications de rencontre

Les applications de rencontre telles que Tinder, Bumble, Hinge, et Grindr favorisent les rencontres et la création de relations entre les individus. **Vous devez être âgé de 18 ans et plus pour utiliser les applications de rencontre!**

Lorsque vous parlez à des personnes sur des applications de rencontre, ne partagez pas de renseignement personnel tel que votre adresse, votre numéro de téléphone ou des informations sur vos comptes de médias sociaux.

Lorsque vous créez un profil sur une application de rencontre, ajoutez une photo de vous qui ne contient aucune information pouvant vous identifier en arrière-plan. Par exemple, n'ajoutez aucune photo de vous qui révèle :

- l'adresse de votre domicile
- votre quartier
- votre lieu de travail



Lorsque vous rencontrez pour la première une personne que vous avez connue sur une application de rencontre :

- dites à un ami où vous allez et quand vous comptez être de retour
- chargez votre cellulaire et emportez-le avec vous
- rencontrez la personne dans un lieu public (ex. café, restaurant, cinéma, etc.)
- Arrangez-vous afin de disposer de votre propre moyen de transport à l'aller et au retour du lieu de rendez-vous



Sécurité en ligne

Points importants à retenir

Si le compte d'une personne ne contient aucune information sur elle, si elle n'a pas plusieurs ami(e)s/abonné(e)s et que le nombre de ses publications est insignifiant, cela signifie que le **compte est faux**. Ce ne serait pas une bonne idée de lui parler, de la suivre ou de l'ajouter en tant qu'ami en ligne.



Parfois, ce qu'on voit (photos) et ce qu'on lit (faits et informations) **en ligne n'est pas toujours vrai**. Il est important que les gens remettent en question ce qu'ils voient en ligne et qu'ils se renseignent auprès des amis ou des adultes lorsqu'ils ne sont pas sûrs de la véracité ou de la réalité de quelque chose.

Gardez les renseignements personnels tels que votre numéro de téléphone, vos renseignements bancaires et votre adresse **confidentiels** et ne les partagez pas avec d'autres personnes en ligne. Assurez-vous que tous vos comptes sont **protégés par des mots de passe**.





Sécurité en ligne

Points importants à retenir



Les gens qui utilisent les médias sociaux **doivent uniquement ajouter des personnes qu'ils connaissent et qu'ils souhaitent ajouter**. Les personnes que vous ajoutez dans les médias sociaux seront en mesure de voir tout ce que vous publiez et partagez sur votre compte. Il est donc important d'ajouter uniquement des personnes en qui vous avez confiance. Ce qui pourrait signifier que vous ne souhaitez pas ajouter ou « être ami(e) avec » des personnes que vous ne connaissez pas sur les médias sociaux.

Ne cliquez sur aucun lien qui vous redirige vers un site Web ou vers tout autre compte en ligne envoyé par une personne que vous ne connaissez pas. Parfois, les gens reçoivent des liens et des messages en ligne de personnes ou d'organisations qu'ils ne connaissent pas. Dans d'autres cas, le message est envoyé par une personne que vous connaissez, mais il est inapproprié. Si vous ne savez pas si vous devez cliquer sur le lien ou non, demandez alors à une personne de confiance autour de vous telle qu'un leader communautaire, un parent, un conseiller ou un enseignant.

