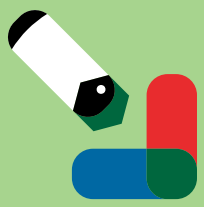
7e à 12e année

La communication sécuritaire en ligne

Adaptation française : Centre franco-ontarien de ressources pédagogiques

ROGERS cybersecure catalyst



Nous utilisons la technologie principalement pour communiquer. Nous passons beaucoup de temps sur nos appareils à parler avec des amies et amis, à commenter des publications, à partager des photos de repas ou de vacances, à utiliser la messagerie instantanée pour communiquer et à créer des groupes de clavardage pour rester en contact avec notre réseau. Mais qu'est-ce qu'on entend par la communication sécuritaire en ligne? Outre les amies et amis et les connaissances, plusieurs plateformes et applications mobiles de médias sociaux permettent de communiquer avec des personnes que l'on n'a jamais rencontrées; il est parfois difficile de savoir qui se cache derrière l'écran et quelles sont ses intentions. La clé pour rester en sécurité en ligne, c'est de restreindre la quantité de renseignements privés que tu partages publiquement, puisque des étrangères et des étrangers pourraient essayer de les utiliser pour te faire du tort. Il peut s'agir d'attaques personnelles; quelqu'un se fait passer pour quelqu'un d'autre dans le but de te manipuler, d'avoir accès à tes données personnelles ou, dans certains cas, de pirater tes comptes.

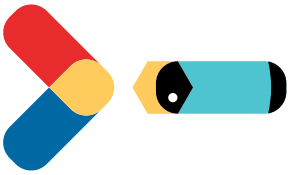
Cette ressource vise à t'outiller en te montrant comment reconnaître les risques potentiels liés à la communication en ligne, et comment communiquer de façon sécuritaire en ligne en faisant des choix plus éclairés.

En ligne, sois attentif à ce qui suit

- **Opportunistes :** Ces personnes essaient souvent de paraître « normales » et honnêtes, mais en réalité, leur intention est de faire du mal. Les opportunistes viennent de tous les milieux et de tous les horizons. À la première interaction, elles et ils peuvent être très difficiles à démasquer. Les opportunistes en ligne veulent généralement quelque chose et tenteront de te manipuler pour l'obtenir.

- **Facteurs de risque pour la sécurité en ligne :** Habituellement, les opportunistes cherchent et ciblent les personnes qui partagent plus ouvertement leurs pensées et leurs sentiments en ligne. Si la vulnérabilité peut être un comportement positif dans la réalité, l'exprimer en ligne peut donner aux opportunistes l'occasion de te manipuler. L'une des façons les plus faciles et efficaces d'être en sécurité en ligne, c'est de garder ta vie privée à l'abri du public. Fais attention à ce que tu partages, et réfléchis à la façon dont ce contenu peut t'exposer, en utilisant les réglages de la plateforme pour gérer qui peut voir ton contenu personnel, et quel contenu peut être partagé publiquement. Ce faisant, tu pourras publier des choses et converser avec des personnes qui respecteront ta vie privée et tes limites, sans que les opportunistes aient accès à tes renseignements personnels.

- **Le preux chevalier :** Les opportunistes peuvent manipuler les autres en utilisant de multiples comptes factices – par exemple, un compte servant à intimider, et l'autre servant à apporter son soutien. Sur les médias sociaux, un compte d'intimidation est utilisé pour harceler, insulter et rabaisser quelqu'un. Le preux chevalier pourrait diffuser publiquement des messages offensants ou des photos et des mèmes blessants, afin d'amener sa cible et les autres à réagir. Elle ou il utilise ensuite un autre compte pour prétendument se porter à la défense de la victime en répondant aux publications de l'intimidatrice ou de l'intimidateur, tout cela dans le but d'avoir de l'attention et de gagner la confiance des autres. Le preux chevalier prétend être aimable et compréhensif, mais son objectif est de se rapprocher de sa victime et de devenir intime avec elle afin de pouvoir la manipuler et avoir accès à ses renseignements personnels, ou pour la convaincre d'organiser une rencontre en personne.



Opportuniste
Personne qui se sert des autres ou de leurs renseignements personnels pour son propre profit ou avantage.

Comment te mets-tu à risque en ligne?

Bien que nous nous retrouvions tous dans les situations suivantes à l'occasion, les opportunistes te cibleront à ce moment si tu :

- **manques d'assurance et de confiance en toi.**
- **te sens seule ou seul, ou si tu as peu d'amies ou d'amis ou de groupes sociaux.**
- **as des relations limitées ou compliquées avec les membres de ta famille, ou si tu ne te confies tout simplement pas beaucoup à eux; les opportunistes peuvent prétendre comprendre ta vie et ta situation.**
- **cherches encore ta voie et ton identité. Les personnes dans cette situation ont tendance à demander de l'aide ou des conseils à d'autres, et les opportunistes en profitent pour prodiguer des « conseils ». Tu ne devrais pas te fier aux paroles et aux intentions de n'importe qui.**

B PERTINENCE

Une fois qu'une ou un opportuniste a trouvé une personne se sentant vulnérable, elle ou il commence à tenter de se lier d'amitié avec elle et de gagner sa confiance. Les opportunistes sont doués pour dénicher les personnes qui passent une mauvaise journée, qui traversent une période difficile, ou qui se sentent seules. Nous nous retrouvons tous dans ces situations à un moment ou un autre, mais les opportunistes remarquent rapidement les changements émotionnels chez les autres et tentent de tirer avantage de la situation. Ce processus peut ne prendre que quelques minutes ou s'étendre sur plusieurs mois.

Sois vigilant lorsqu'une personne inconnue...

- répond, à toi ou à tes publications avec des commentaires élogieux, ou commence à poser des questions qui semblent inoffensives. Tes réponses pourraient potentiellement donner à l'opportuniste des détails pouvant lui servir à en apprendre plus sur toi, ou à accéder à des renseignements de nature délicate.

- affirme partager tous tes intérêts et opinions ou beaucoup d'entre eux.

- essaie de normaliser une relation qui serait autrement considérée comme étrange compte tenu des circonstances (p. ex. : la personne est beaucoup plus âgée que toi, ou essaie de nouer une relation amoureuse rapidement). Souviens-toi de ces indices, et n'oublie pas que de tels comportements peuvent être douteux.

- te pousse à prendre part à des conversations qui commencent à être trop personnelles, ou te demande de faire quelque chose qui te rend mal à l'aise. C'est inacceptable, et tu ne devrais pas te sentir obligé de répondre.

- demande à te voir, d'abord en demandant des photos, puis en faisant un appel vidéo. Éventuellement, elle peut même insister pour te rencontrer en personne. N'oublie pas que cela peut être très dangereux et que tu dois faire preuve d'une prudence extrême. Si tu as un doute, demande conseil à un parent, à une tutrice ou à un tuteur ou à une ou un adulte de confiance.

Qu'as-tu appris?

Pourquoi est-il dangereux de publier des renseignements personnels et privés en ligne? Comment les opportunistes peuvent-ils utiliser ces renseignements d'une façon négative et malveillante?

Cyberprédatrices et cyberprédateurs à garder à l'œil

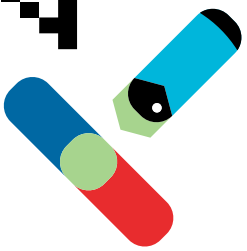
Cyberprédation
Situation où une personne communique avec une autre, généralement plus jeune, par le biais de la technologie (comme les messages textes ou privés) avec l'intention de lui faire du tort.

- Une personne inconnue qui essaie de profiter de ta générosité.
- Une personne inconnue qui te fait des promesses trop belles pour être vraies.
- Une personne inconnue qui affirme te connaître ou connaître l'une ou l'un de tes amis ou un membre de ta famille, même si ce n'est pas le cas. C'est pourquoi il est important d'être consciente ou conscient de ce que tu partages en ligne – et avec qui!

Cyberharcèlement

Que quelqu'un te suive sur les médias sociaux, ce n'est pas considéré comme du cyberharcèlement. Cependant, si cette personne utilise ces renseignements pour surveiller d'autres aspects de ta vie – virtuelle ou réelle – cela peut être dangereux. Sois à l'affût de ces deux méthodes couramment utilisées par les harceleuses et harceleurs :

Cyberharcèlement
Pratique qui consiste généralement à surveiller les activités en ligne d'une personne, à utiliser des appareils connectés pour maintenir la communication avec l'intention de harceler ou d'intimider, de causer de l'inconfort ou même de susciter la peur.



• Arnaque : Les arnaqueuses et arnaqueurs prétendent souvent être quelqu'un d'autre et créent de multiples fausses identités en ligne, en utilisant de faux noms, de fausses photos, de fausses affiliations, etc. Elles et ils se servent de ce déguisement pour tromper leur victime, qui croit avoir affaire à quelqu'un d'autre. Une fois qu'elles et ils ont accès à toi, elles et ils pourraient commencer à suivre tes mouvements en ligne.

• Hameçonnage : Tentative frauduleuse ou fraude visant une utilisatrice ou un utilisateur d'Internet dont le but est d'obtenir des renseignements personnels à des fins illégales. Les cyberprédatrices et cyberprédateurs peuvent poser des questions qui semblent anodines à première vue afin d'avoir accès à des renseignements qu'elles et ils peuvent utiliser pour obtenir encore plus de renseignements personnels. C'est ainsi que tes itinéraires de voyage, les personnes avec qui tu voyages, et même le lieu précis où tu vas pourraient être révélés.

APPEL À L'ACTION

Fie-toi à ton instinct

Se fier à son instinct, c'est avoir confiance en son intuition ou en sa compréhension immédiate d'une situation – on entend souvent les gens dire « tu le sais, c'est tout ». La plupart des gens, malheureusement, ont vécu des rencontres bizarres ou effrayantes avec quelqu'un en public. Peut-être que la personne t'a fixé des yeux trop longtemps, s'est tenue trop près de toi ou t'a souri d'une drôle de façon. Des situations semblables peuvent avoir lieu en ligne, mais sous une forme différente. Quelqu'un peut complimenter une photo de toi de façon très personnelle, publier des commentaires sur ton profil régulièrement ou se lier d'amitié avec tes amies et amis. À l'occasion, les opportunistes peuvent te demander d'éviter de donner des renseignements sur eux aux autres; elles et ils peuvent aussi te demander de leur révéler tes secrets, sans en parler à ta famille et à tes amies et amis. Cela devrait être un signal d'alarme que quelque chose ne va pas.

Lorsque tu communiques avec d'autres personnes en ligne, tu dois faire attention aux situations dans lesquelles tu te places. Les réelles intentions d'une personne sont plus difficiles à décerner dans un message texte qu'en personne. Si la situation te semble un peu étrange, tu dois prendre du recul et examiner ce qui se passe réellement.

À ne pas oublier

À tout moment où tu as peur ou tu te sens inconfortable, tu dois...

Arrête de parler à la personne immédiatement, sans te sentir obligé d'expliquer pourquoi.

Bloque l'utilisatrice ou l'utilisateur, mais NE supprime PAS les messages qui ont été envoyés. Montre-les à une ou un adulte de confiance.

Parles-en immédiatement à un parent, à une tutrice ou un tuteur ou à une ou un adulte de confiance. Elle ou il sera en mesure de t'aider à évaluer si les intentions et les actions de la ou du possible opportuniste sont acceptables.

Paramètres de localisation

Ton appareil mobile enregistre ton emplacement précis lorsque tu prends une photo ou une vidéo, et peut révéler où tu es lorsque tu publies un commentaire ou une image. Lorsque la localisation est activée, tes comptes de médias sociaux et tes publications peuvent révéler des détails délicats sur ton emplacement à quelqu'un qui y a accès. Ce ne sont pas toutes les plateformes de médias sociaux qui suppriment les données de localisation; la meilleure façon de ne pas révéler où tu te trouves est donc de désactiver les services de localisation sur tes appareils.

Le savais-tu?

Les images, les vidéos et les fichiers contiennent des renseignements ou des descriptions supplémentaires en arrière-plan, appelés métadonnées; cela peut inclure ton nom et ton emplacement! Lorsque tu envoies directement ces fichiers à une autre utilisatrice ou un autre utilisateur, tu lui envoies aussi ces renseignements.

ACTIVITÉ 1

Les activités sont une bonne façon de t'exercer et de mettre en pratique tes connaissances sur le sujet abordé dans la ressource.

Évaluation de l'état de préparation

Pose-toi les questions suivantes, ou discutes-en avec tes camarades de classe, ta famille ou tes amies et amis. Que ferais-tu si...?

Outre tes parents ou tes tutrices et tuteurs, à qui pourrais-tu demander de l'aide? Utilise cette liste pour nommer d'autres adultes à qui tu peux faire confiance.

1. Exemple : Mon entraîneur de soccer, M. Graham
2. _____
3. _____
4. _____
5. _____

ACTIVITÉ 2

Vie privée 101

Jette un œil au profil de médias sociaux plus bas; c'est l'exemple d'un profil lorsqu'il est public (que l'on trouve facilement en effectuant une recherche sur Google). Selon ce que tu as appris dans cette ressource, encercle les renseignements qui pourraient aider une ou un opportuniste à nouer une fausse amitié.

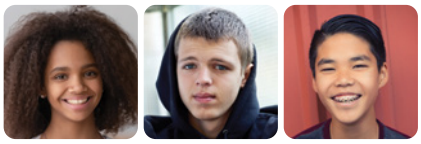
Kiara Reddy

À propos

- Habite à **Mississauga, Ontario**
- Étudie à **Cawthra Park Secondary School**
- Travaille chez **PetSmart**
- En couple avec **Tom Parker**
- Née le **11 juillet 2003**

Amis (127)

Voir tout



Simone Jones | Matthew Miller | William Min

Kiara Reddy est à **Lakefront Promenade Park**
18 octobre à 8:12

J'adore marcher le matin avec Lucy!

46 | 9 Commentaires

Kiara Reddy se sent triste.
14 octobre à 19:12

Je m'ennuie de ma meilleure amie. On se voit bientôt, **Amber Foster**!

28 | 7 Commentaires

Kiara Reddy **soupe** au **Thyme Ristorante**.
12 octobre à 18:24

POUR EN SAVOIR PLUS

Pour en savoir plus sur la cybersécurité ou pour poursuivre la conversation et l'apprentissage, consultez le site du Centre canadien pour la cybersécurité : https://www.cyber.gc.ca/fr/.

Jeunesse, J'écoute

Pour de l'aide, envoyez un message texte au 686868 ou téléphonez au 1-800-668-6868 partout au Canada, 24 heures sur 24, 7 jours sur 7, ou accédez aux ressources en ligne sur jeunessejecoute.ca.

ROGERS
cybersecure
catalyst

Adaptation française : Centre franco-ontarien de ressources pédagogiques