

Guide créatif à l'intention des parents et des enseignant(e)s

Introduction

Si vous fréquentez des jeunes — vos propres enfants, des élèves, neveux et nièces ou des membres d'une équipe —, ce guide s'adresse à vous. Car s'ils ne naviguent pas déjà sur Internet, il y a de fortes chances qu'ils le feront bientôt et qu'ils auront besoin de conseils sur la protection de leur vie privée.

Plus que jamais, les jeunes ont besoin de cette information, puisqu'on compte un nombre croissant de gadgets et de jouets qui offrent des options en ligne; même les jouets en peluche sont désormais munis de codes qui permettent aux enfants de les enregistrer en ligne et de jouer avec leurs pairs! Les jeunes accueillent cette technologie avec enthousiasme; ils naviguent pour entrer en relation avec leurs amis ou pour se faire de nouveaux amis, pour faire des achats, écouter de la musique, regarder des vidéos, jouer à des jeux, apprendre... la liste est infinie!

Selon le Réseau Éducation-Médias, 37 % des jeunes Canadiennes et Canadiens possèdent leur propre ordinateur branché sur Internet et 20 % des élèves de quatrième année accèdent à Internet via leur propre ordinateur personnel — le taux atteint 52 % pour les élèves de secondaire V. Puisque les jeunes font preuve d'un tel enthousiasme envers la technologie, il convient de prendre le temps de leur enseigner la « nétiquette ».

L'information qui suit se veut un guide sur d'importantes questions de protection des données qui concernent tout particulièrement les jeunes. Chaque section débute avec un enjeu important, puis propose des conseils pour lancer le dialogue au sujet de cet enjeu avec les jeunes qui vous entourent.

Les vidéos et autres ressources dont ce guide fait mention sont fournies sous forme de liens — vous pourrez y accéder directement à votre guise. Elles figurent également dans une liste à la fin du document, alors vous pourrez y accéder tout aussi facilement si vous choisissez d'imprimer le guide. Nous avons aussi inclus des liens vers d'autres sites sur la protection de la vie privée à l'intention des jeunes; ils surgissent un peu partout dans le monde, y compris en Norvège, en Australie et à Hong-Kong. Grâce à Internet, les gens peuvent communiquer plus facilement, peu importe où ils habitent, et la protection de la vie privée fait partie des préoccupations des jeunes du monde entier.

ENJEU ET DISCUSSION —N° 1

Réfléchis avant de cliquer!

Les services et les applications en ligne offrent des occasions uniques de création, de réseautage, d'engagement social et d'apprentissage. En ligne, on peut faire des recherches sur les sujets les plus terre-à-terre comme les plus exotiques, communiquer avec ses amis partout dans le monde, regarder des vidéos, jouer à des jeux — les possibilités sont infinies.

Il faut absolument retenir une chose sur les activités en ligne : tout ce qu'on affiche en ligne est public et permanent. On utilise les termes Web et toile pour parler du réseau parce que, comme une toile d'araignée, il a des connexions dans des millions de directions différentes. Quand on affiche un commentaire ou une photo en ligne, ils échappent à notre contrôle; n'importe qui peut les copier ou les envoyer à d'autres. Vous avez des amis sur les sites de réseautage social, vos amis ont des amis, et ainsi de suite. Dès que quelque chose se retrouve sur Internet, on peut l'envoyer à n'importe qui, n'importe où.

Il est aussi très difficile, voire impossible, de supprimer des renseignements affichés en ligne. Une fois qu'ils y sont, ils peuvent être copiés. Ils résident aussi dans les archives et les caches d'autres ordinateurs. Il faut donc faire attention à ce qu'on affiche et bien réfléchir avant d'afficher quoi que ce soit. Posez-vous cette question : « Si ces renseignements se trouvent encore sur Internet dans 5 ou 10 ans, est-ce que je serai mal à l'aise? »

Il suffit de réfléchir avant de cliquer! Assurez-vous que ce que vous affichez est acceptable et ce, avant de l'afficher.

Pour lancer la discussion :

As-tu déjà affiché quelque chose en ligne que tu ne voudrais pas que tes parents ou tes profs voient? Ou alors, ton dernier coup de foudre — aimerais-tu que cette personne voie tout ce que tu as affiché? Si tu as affiché des choses qui te mettent mal à l'aise, retire-les d'Internet et, à l'avenir, réfléchis avant de cliquer.

Pense aussi à tes amis. As-tu déjà affiché une photo ou un commentaire qu'un de tes amis n'aurait pas voulu transmettre au grand public? Surveilles-tu ce que tes amis affichent à ton sujet?

ENJEU ET DISCUSSION — N° 2

Es-tu à l'affût des paramètres de confidentialité?

Saviez-vous que Facebook compte plus de 350 000 000 d'utilisateurs actifs qui consultent leur compte au moins une fois par semaine? Saviez-vous que si votre profil Facebook est « ouvert », tous ces utilisateurs peuvent voir ce que contient votre page?

En 2009, MySpace annonçait avoir chassé du site 90 000 personnes inscrites au registre des délinquants sexuels — quand on y est inscrit, c'est parce qu'on s'est fait prendre. D'après vous, combien de délinquants sexuels sont membres d'autres sites de réseautage social? Mais surtout, combien d'individus inquiétants utilisent ces sites, mais n'ont jamais été reconnus coupables pour leurs actes?

Si vous possédez un profil ouvert sur un site de réseautage social, il serait judicieux d'ajuster les paramètres de confidentialité de manière à le « fermer ». Ainsi, seuls ceux qui figurent sur votre liste d'amis auront accès aux détails de votre profil. Les paramètres de confidentialité comprennent plusieurs options; vous pouvez même limiter ce que différentes catégories d'amis verront — par exemple, en ajustant les paramètres de façon à ce que seuls les bons amis puissent tout voir, alors que vos simples connaissances n'auront accès qu'à certains renseignements. Avez-vous inscrit des gens que vous ne connaissez pas du tout sur votre liste d'amis? Consultez l'enjeu n° 3!

Pour lancer la discussion :

Jonathan choisit avec attention les gens qui figurent sur sa liste d'amis sur son site de réseautage social favori, mais il n'a jamais consulté les paramètres de confidentialité. Par défaut, son profil est « ouvert », ce qui veut dire que tous les utilisateurs du site y ont accès. Qu'est-ce que cela implique?

ENJEU ET DISCUSSION — N° 3

Connaissez-vous vos amis?

Il arrive que des gens se joignent à un site de réseautage social comme Facebook ou Bebo et qu'ils découvrent, au moment de la création de leur profil, que quelqu'un en a déjà créé un en leur nom. Ce n'est qu'un autre moyen dont les fraudeurs utilisent Internet à des fins malveillantes.

Si une amie dans la vraie vie vous demande de devenir amis en ligne, assurez-vous qu'il s'agit bien d'elle en lui demandant en personne, tout simplement. Lors de votre rencontre suivante, parlez-lui de son profil. Il y a de bonnes chances que cette personne soit vraiment votre amie en ligne. Mais vous ne perdez rien à le demander. Et on ne sait jamais — vous pourriez ainsi rendre service à votre amie.

Soyez prudents — on n'est jamais sûr à 100 % de savoir à qui on s'adresse en ligne. Alors si, dans le monde réel, vous avez peu ou pas de contact avec vos amis virtuels, faites preuve de prudence. Plus vous aurez de rapports avec vos amis virtuels dans le vrai monde, plus vous pourrez échanger des renseignements avec eux en toute confiance. Bien sûr, vous pouvez envoyer en ligne vos photos de vacances à votre meilleur ami sans hésiter, mais réfléchissez-y à deux fois avant de les envoyer à un ami rencontré en stage de tennis l'été précédent, ou à l'ami d'un ami rencontré en clavardant.

Pour lancer la discussion :

Comment peux-tu confirmer l'identité de tes amis? Joue au détective... Comment pourrais-tu « enquêter » le profil de tes amis? Si l'une de tes amies a deux frères, mais en ligne, elle ne mentionne qu'un frère — est-ce que c'est un faux profil? Cet exercice pourrait t'aider à reconnaître certains imposteurs... ou d'apprendre des choses que tu ignorais jusque-là, comme le fait qu'un de tes amis adore la poutine et les anciens jeux vidéo!

ENJEU ET DISCUSSION — N° 4

Choisis le mot de passe parfait et protège-le

La sécurité de vos renseignements dépend de celle de votre mot de passe. Sans mot de passe solide, vos renseignements en ligne sont vulnérables — d'autres pourraient y accéder.

Le mot de passe idéal devrait :

- Être **solide** (on recommande un minimum de 8 caractères). Plus le mot de passe comprend de caractères, plus il sera solide.
- Être composé de caractères **divers**. En combinant des lettres, des chiffres et des symboles, le mot de passe est plus complexe et, donc, plus difficile à deviner.
- Être **modifié** régulièrement pour réduire le risque que quelqu'un accède à vos renseignements personnels.

Voici quelques erreurs souvent commises en ce qui a trait aux mots de passe :

- Recourir à des **séquences** ou à des répétitions de caractères. Le mot de passe est alors plus facile à deviner.
- Utiliser des **renseignements personnels**, comme une partie de votre nom, date de naissance, numéro d'assurance sociale ou les renseignements similaires de vos proches.
- Utiliser le **même** mot de passe pour plusieurs systèmes.
- **Dévoiler** votre mot de passe à d'autres pour des raisons quelconques.
- Taper votre mot de passe sur un ordinateur qui ne vous appartient pas ou qui échappe à votre contrôle — d'autres pourraient réussir à extraire votre mot de passe de l'ordinateur après que vous l'aurez utilisé.

Pour lancer la discussion :

Katherine est folle de joie d'avoir reçu un téléphone cellulaire pour ses 14 ans. Elle doit choisir un mot de passe et choisit le 141414. Elle donne son mot de passe à tous ses amis pour qu'ils puissent utiliser son téléphone. En rentrant chez elle, elle modifie le mot de passe de son ordinateur; elle choisit le 141414 de façon à ne pas mélanger les mots de passe. Que penses-tu du choix de mot de passe de Katherine, de sa décision de le communiquer à ses amis et d'avoir le même mot de passe pour son téléphone et son ordinateur?

ENJEU ET DISCUSSION — N^o 5

Assure-toi que tes renseignements personnels restent privés — et protège ton identité

Êtes-vous à risque de vol d'identité? Voici quelques questions essentielles à vous poser :

- 1) Conservez-vous votre numéro d'assurance sociale dans votre portefeuille?
- 2) Jetez-vous vos relevés bancaires et vos reçus aux poubelles?
- 3) Avez-vous révélé votre NIP à des amis?
- 4) Choisissez-vous des mots de passe simples et faciles à deviner?

Si vous avez répondu « oui » à au moins une de ces questions, vous courez le risque d'être victime de vol d'identité!

Voici quelques statistiques sur le vol d'identité, tirées d'un récent sondage¹ :

- 1,7 million de Canadiennes et Canadiens ont été touchés par le vol d'identité en 2008.
- Si plus de 45 % des cas de vol d'identité sont reliés à l'utilisation d'Internet, la plupart des voleurs d'identité ne recourent pas au cyberspace pour acquérir des renseignements.
- 40 % des contrevenants sont des femmes — cela s'explique peut-être par l'absence de violence associée à ce crime et la possibilité de le commettre sans l'aide d'un complice.
- L'âge moyen des voleurs d'identité est de 33 ans.
- 64,6 % des contrevenants agissent seuls dans la plupart des cas.
- 53,4 % des incidents impliquent le vol de portefeuilles, de sacs à main, puis la fraude.

Il appert que plusieurs personnes choisissent de voler des identités simplement parce que c'est facile. Le vol d'identité est l'un des crimes connaissant la plus forte hausse depuis quelques années.

Pour lancer la discussion :

Les élèves de l'école John F. Ross CVI, à Guelph, ont participé à notre concours de vidéo 2008; la vidéo soumise, intitulée « C'est votre vie... et votre vie privée », plonge les spectateurs dans les pensées d'un voleur d'identité et démontre à quel point il est facile de duper les gens pour leur faire dévoiler leurs renseignements personnels sur Internet. Cette vidéo a gagné le 3^e prix – visionnez-la [ici](#). Discutez avec les jeunes de la vidéo et des réalités du vol d'identité.

¹ Statistiques provenant du 2^e rapport de Benoît Dupont et Guillaume Louis (*Les voleurs d'identité : profil d'une délinquance ordinaire*), de la Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal.

ENJEU ET DISCUSSION — N° 6

Sois prudents lorsque tu visites des sites Web de jeux vidéo

Quels genres de sites Web de jeux vidéo connaissez-vous?

Certes, les jeux vidéo en ligne sont amusants et divertissants, mais si vous ne faites pas preuve de prudence, vous risquez de compromettre votre identité et vos renseignements personnels.

Les gens accèdent de plus en plus aux renseignements personnels des autres via les sites de jeux en réseau. Si une personne malveillante obtient des renseignements à votre sujet à partir des profils que vous avez créés pour ces jeux, elle pourrait s'en servir pour ouvrir un compte à votre nom et le revendre, ou pour accéder à vos comptes financiers existants.

Lorsque vous visitez des sites de jeux :

- Vérifiez si votre ordinateur est en mode « administrateur ». Certains jeux règlent automatiquement l'ordinateur à ce mode et c'est problématique, puisqu'un pirate informatique pourrait alors obtenir un contrôle absolu de l'ordinateur au niveau « administrateur ».

L'un des moyens d'éviter ce problème est de naviguer depuis un compte « utilisateur ». Bien que cela n'assure pas la sécurité totale de l'ordinateur, c'est plus sécuritaire que de naviguer en mode administrateur.

Lorsqu'on joue en ligne, il est important de s'assurer que des **pare-feu** sont en place pour mieux protéger l'ordinateur. Les jeux multijoueurs exigent parfois une exception dans les règles touchant ces pare-feu. Les pare-feu servent à protéger les ordinateurs des virus. Si vous les désactivez, vous et vos renseignements devenez extrêmement vulnérables.

Pour lancer la discussion :

Pense aux profils que tu as créés pour les jeux vidéo en ligne. As-tu donné ton nom au complet? Ta date de naissance? Ton adresse ou tout autre renseignement personnel qui pourrait intéresser un malfaiteur? Pense à tes camarades de jeux — les connais-tu tous dans la vraie vie? Si l'un d'entre eux était un pirate informatique, voudrais-tu qu'il ait accès à tous les renseignements de ton profil ?

ENJEU ET DISCUSSION — N° 7

Méfie-toi des courriels et des messages instantanés provenant d'inconnus

Connaissez-vous le terme « hameçonnage »? Il s'agit d'une tentative criminelle d'accès à des données privées et sensibles, comme les mots de passe Internet et les numéros de cartes de crédit, par quelqu'un qui se fait passer pour une organisation légitime et digne de confiance. Ces tentatives sont souvent effectuées par courriel ou message instantané.

Les sites de réseautage social sont devenus la cible des hameçonneurs. Plusieurs criminels :

- créent des sites Web quasi identiques à la page d'accueil d'un site de réseautage social pour vous induire à entrer votre nom d'utilisateur et votre mot de passe;
- utilisent les renseignements obtenus pour pirater votre compte et accéder à tous vos renseignements.
- insèrent un lien dans un message au sein du système de messagerie interne du site de réseautage social.

Ce que vous pouvez faire :

- **Ne répondez pas aux courriels** qui demandent des renseignements personnels bancaires. Les entreprises authentiques n'envoient pas de courriels à leurs clients pour demander leur nom d'utilisateur ou leur mot de passe.
- Faites preuve de **prudence** avec les courriels et les messages personnels. Si vous ne connaissez pas l'expéditeur, tentez de savoir s'il est légitime avant de répondre.
- **Protégez** votre ordinateur avec des filtres anti-pourriel et des logiciels antivirus et assurez-vous que votre pare-feu est activé.
- **Faites attention** et porter un regard critique sur les messages qui proviennent de personnes que vous ne connaissez pas ou en qui vous n'avez pas confiance. N'entrez jamais de renseignements personnels en ligne à moins d'être certain à 100 % qu'il s'agit d'un site Web légitime et authentique. En cas de doute, on ne doit pas hésiter à demander de l'aide.

Pour lancer la discussion :

Annie a récemment ouvert un compte bancaire à la banque du centre commercial de la région. Un jour, elle reçoit un courriel de l'institution qui souhaite vérifier son mot de passe en ligne. Une banque procéderait-elle ainsi pour vérifier le mot de passe d'un client? Si le courriel semble provenir de la banque (les logos, les couleurs, etc. sont ceux de la banque, et le président de la banque a signé le courriel), qu'est-ce qu'Annie devrait faire? Qu'est-ce qui pourrait arriver si elle répond au courriel et procède à la vérification de son mot de passe en ligne?

ENJEU ET DISCUSSION — N° 8

Les parents sur Facebook

VOS parents sont-ils sur Facebook?

Peu importe qu'il s'agisse de vos parents, de vos collègues, de votre patron ou d'un entraîneur — les renseignements qu'on affiche en ligne sont publics et y restent en permanence, et il est bel et bien possible que tout le monde puisse les voir. Si vous êtes mal à l'aise à l'idée que certaines photos ou informations soient exposées aux yeux de tous, vous ne devriez probablement pas les afficher en ligne. Évaluez bien ce que vous choisissez de télécharger vers le Web. Réfléchissez avant de cliquer pour vous éviter des soucis éventuels!

Et même si vous faites attention à ce que vous affichez, qu'en est-il si vous n'êtes pas très à l'aise de compter vos parents parmi vos amis Facebook? Peut-être écrivent-ils toujours des messages sur votre mur ou font des commentaires sur tous vos agissements. Cela pourrait vous inciter à vous tourner vers les paramètres de confidentialité. Est-il possible de limiter leur accès à vos renseignements? Si vous souhaitez vous apitoyer sur votre sort avec d'autres adolescents qui sont dans la même galère, consultez la page suivante : [Oh Crap. My Parents Joined Facebook](#) (en anglais seulement). Le site a été créé par deux filles dans la vingtaine qui s'entretiennent des relations parents-enfants sur Facebook et donnent des exemples à ce sujet.

Pour lancer la discussion :

En Norvège, un [site Web](#) consacré à la protection de la vie privée des jeunes présente des vidéos qui expliquent aux jeunes à quel point il est facile pour d'autres de savoir ce qu'ils font sur Internet. Cette vidéo-ci se déroule pendant une conférence élèves-enseignants; l'enseignante discute de ce qu'elle a découvert simplement après avoir googlé le nom de l'élève.

ENJEU ET DISCUSSION — N° 9

Les applications sur iPhone et autres

Combien d'entre-vous possèdent un téléphone cellulaire? Et combien de ces appareils vous donnent accès à Internet? Grâce à certains appareils comme le iPhone et le BlackBerry, vous pouvez télécharger des applications assez géniales qui vous permettent, par exemple, de connaître des restaurants recommandés, d'obtenir les horaires de cinéma et plus encore.

Par contre, vous ignorez peut-être qu'avec certaines de ces applications, vos données de localisation sont diffusées sur l'ensemble de votre réseau de données cellulaires. Bien qu'on avance que ces serveurs sont sécuritaires, il n'y a aucun moyen de savoir qui accède à vos renseignements de localisation.

Il est important d'utiliser ces applications de manière sécuritaire et de vous assurer de savoir ce qu'elles impliquent. Vous ignorez si une application diffuse vos renseignements? Informez-vous!

Pour lancer la discussion :

Est-ce que toi ou un de tes amis a déjà utilisé un téléphone cellulaire muni d'un dispositif GPS pour savoir où se trouve quelqu'un d'autre ou pour diffuser votre propre emplacement? L'information de localisation est un renseignement très délicat; si tu permets à une personne dangereuse d'y accéder, tu pourrais t'exposer à des risques.

ENJEU ET DISCUSSION — N° 10

Sites de rencontres en ligne

Ce n'est pas facile de faire des rencontres amoureuses, peu importe son âge. C'est pour cette raison que certaines personnes se tournent vers les sites de rencontres en ligne. Si c'est quelque chose que vous envisagez, rappelez-vous qu'Internet :

- est complètement anonyme et qu'il n'y a aucun moyen de savoir à qui on s'adresse en ligne.

Voici quelques précieux conseils à prendre en considération lorsqu'on visite des sites de rencontres en ligne :

- **Fiez-vous** à votre instinct. Si votre intuition vous dit que quelque chose cloche chez quelqu'un ou si cette personne dégage une « énergie négative », cessez toute communication.
- Faites preuve de **prudence** en communiquant vos renseignements personnels.
- Il est conseillé d'ouvrir un compte de courriel **anonyme** pour poursuivre les interactions avec quelqu'un en dehors de la communauté de rencontres en ligne. Ainsi, vos renseignements personnels et d'identification demeureront anonymes et il vous sera beaucoup plus facile de rompre toute communication si nécessaire.
- Si vous choisissez d'intégrer le monde virtuel au monde réel, ne rencontrez **JAMAIS** cette personne seul à seul. Si vous avez moins de 18 ans, demandez la permission à vos parents avant de rencontrer en personne un ami virtuel ou une amie virtuelle. Et rappelez-vous : cette personne n'est peut-être pas qui elle prétend être.

Pour lancer la discussion :

Le site Web de la [Norvège](#) sur la protection de la vie privée des jeunes illustre qu'on peut faire des rencontres amoureuses en ligne avec quelqu'un qui n'est pas qui il affirme être. Le scénario présenté décrit une situation particulière : « Es-tu tombée amoureuse de ton petit frère? »

ENJEU ET DISCUSSION — N° 11

Le sexto

Dans un [rapport de recherche](#) du Pew Research Center à ce sujet, on apprend que 4 % des jeunes de 12 à 17 ans ont déjà envoyé un sexto et 15 % en ont déjà reçu un.

Il faut se rappeler que :

- Tout ce qui est affiché sur Internet est **public** et **permanent**. Dès qu'on envoie une photo, elle risque de devenir **publique**.
- Tout ce qui est affiché sur Internet peut laisser une **trace documentaire** — vos pairs, votre famille et de futurs employeurs pourraient le retracer.
- Toute photo d'une personne de moins de 18 ans nue est considérée être de la **pornographie juvénile**. Ceux ou celles qui prennent les photos — et même si vous vous photographiez vous-même — sont assujettis à la loi. De plus, ceux qui reçoivent les photos pourraient être inculpés de possession de pornographie juvénile.

Il importe aussi que vous réfléchissiez aux **conséquences** de vos actions. Envoyer une photo privée via un téléphone cellulaire peut donner lieu à une situation terriblement humiliante.

Posez-vous ces questions avant d'afficher des photos sur Internet :

- Qui peut trouver des photos ou des vidéos de vous en ligne? Vos parents? Vos amis? Des membres de votre famille? Vos enseignants?
- S'ils les trouvaient, est-ce que ça vous mettrait dans l'embarras?
- Si ça ne vous met pas dans l'embarras aujourd'hui, qu'en serait-il dans 5 ou 10 ans?
- Comment quelqu'un pourrait-il utiliser vos photos, vos vidéos et vos renseignements personnels?
- Que feriez-vous si quelqu'un de votre école tombait sur vos photos/vidéos?
- Que voulez-vous que les autres sachent à votre sujet?

Pour lancer la discussion :

Le [site Web](#) norvégien sur la protection de la vie privée des jeunes a produit une vidéo sur le sexto. Deux adolescents discutent de l'humiliation que peut subir une personne à cause d'une photo sur Internet... pour finir par télécharger une photo plutôt révélatrice — tous pourront la voir en ligne.

ENJEU ET DISCUSSION — N^o 12

La cyberintimidation

Qu'est-ce que la cyberintimidation?

La cyberintimidation est très différente des autres types d'intimidation qui impliquent un face-à-face. Les personnes qui s'adonnent à la cyberintimidation recourent à la technologie (des téléphones cellulaires ou Internet, par exemple) pour harceler quelqu'un ou lui faire du mal. Un sondage effectué en 2008 indique que près d'un élève sur cinq est victime d'intimidation en ligne.

Ce type d'intimidation peut mener :

- à la dépression
- à l'isolement
- à des troubles de l'alimentation
- au suicide

Le cyberintimidateur peut être sévèrement puni si on fait appel à la police. Si vous ou vos amis êtes victime de cyberintimidation, le [Réseau Éducation-Médias](#) recommande une action en quatre étapes :

- **STOP!** — quittez immédiatement l'environnement ou l'activité virtuelle où se produit l'intimidation.
- **BLOQUEZ** les courriels ou les messages instantanés envoyés par l'intimidateur. **NE LUI RÉPONDEZ JAMAIS.**
- **SAUVEGARDEZ** tous les messages de harcèlement et faites-les parvenir à votre fournisseur de messagerie électronique (Yahoo, Hotmail, etc.). La plupart des fournisseurs ont établi des politiques contre le harcèlement sur leur serveur.
- **PARLEZ-EN** à un adulte en qui vous avez confiance. Alerte la police si des menaces de violence physique ont été faites.

Il est très important de dénoncer les incidents de cyberintimidation pour que l'intimidateur cesse de harceler la victime.

Pour lancer la discussion :

Partout sur la planète, de nombreuses personnes ont été victimes de cyberintimidation. Dans certains cas, MySpace et Facebook étaient concernés : des utilisateurs ont créé de faux profils pour harceler d'autres utilisateurs. On note aussi la création de faux sites Web avec contenu blessant ou dégradant. Quelle est la différence entre l'intimidation traditionnelle et la cyberintimidation? Comment les outils en ligne peuvent-ils aggraver une telle situation?

Ressources citées dans ce document (par ordre de mention) :

Vidéo : « C'est votre vie... et votre vie privée » (élèves de John F. Ross CVI, à Guelph, troisième prix du concours de vidéo 2008 viepriveedesjeunes.ca.). Lien : <http://www.youthprivacy.ca/fr/contest.html>

Site Web : *Oh Crap. My Parents Joined Facebook*. Lien : <http://myparentsjoinedfacebook.com/>

Vidéo : « La conférence parent-enseignant-élève s'est bien déroulée... mais ç'a été la catastrophe quand mon enseignante a googlé mon travail ! » [Traduction]; (site Web norvégien sur la protection de la vie privée et les jeunes). Lien : <http://www.dubestemmer.no/The+parent-teacher-student+conference+went+ok....9UFRnU4L.ips>

Vidéo : « Es-tu tombée amoureuse de ton PETIT FRÈRE ?! » [Traduction]; (site Web norvégien sur la protection de la vie privée et les jeunes). Lien : <http://www.dubestemmer.no/Did+you+fall+in+love+with+your+LITTLE+BROTHER%3F.9UFRzSWw.ips>

Rapport de recherche : *Teens and Sexting* (« Les ados et le sexto »); (Pew Research Center). Lien : <http://pewresearch.org/assets/pdf/teens-and-sexting.pdf>

Vidéo : « Ce n'était qu'une blague... mais voilà que j'ai appuyé sur la touche " Entrée " » [Traduction]; (site Web norvégien sur la protection de la vie privée et les jeunes). Lien : <http://www.dubestemmer.no/It+was+just+a+joke....9UFRnWWg.ips>

Ressources sur la cyberintimidation : Réseau Éducation-Médias. Lien : http://www.media-awareness.ca/english/tools/main_search/search_results.cfm

Autres liens utiles :

Site Web jeunesse sur la protection de la vie privée — Australie. Lien : <http://www.privacy.gov.au/topics/youth>

Site Web jeunesse sur la protection de la vie privée — Hong-Kong. Lien : http://www.youth.gov.hk/en/info_centre/civic/600E.htm

Site Web jeunesse sur la protection de la vie privée — Norvège. Un outil génial pour que les élèves (et les enseignants) apprennent à « réfléchir plus en profondeur à la relation entre la protection de la vie privée, l'anonymat et l'identité dans un monde en réseau ». Lien : <http://www.dubestemmer.no/en/>

Le Réseau Éducation-Médias. Une façon épatante de découvrir la culture des médias et de l'information. Lien : <http://www.media-awareness.ca/francais/index.cfm>

Œil pour œil. Lien : <http://www.idtrail.org/InYourI/>

Commissariat à la protection de la vie privée du Canada. Pour les adultes — renferme des tonnes d'information sur la protection de la vie privée et vos droits. Lien : <http://www.priv.gc.ca/>