

## **Texte : Sécurité sur Internet pour les jeunes de 14 à 18 ans**

**\* Les notes de l'animateur apparaissent en italique\***

**Diapositive 1 : Choix.org traite de la sécurité sur Internet : faire face aux réalités du Web**

**Diapositive 2 : Être cyberfuté...**

- *Être prudent en ligne, c'est savoir utiliser Internet. Internet fait maintenant partie du quotidien de la plupart d'entre vous, et les avantages sont nombreux (messagerie instantanée, courriels, moyen de rester en contact avec ses amis, moteurs de recherche efficaces, etc.).*
- *Malheureusement, Internet comporte aussi de nombreux pièges. Vous devez faire preuve de prudence lorsque vous utilisez Internet, tout particulièrement dans les situations où des personnes ou des entreprises vous demandent des renseignements personnels, ou encore des personnes que vous ne connaissez pas veulent vous rencontrer. Vous devez aussi faire attention à ce que vous dites et affichez en ligne.*
- *Cet atelier vous amènera à réfléchir à ce que vous faites sur Internet et vous sensibilisera aux réalités du Web.*

**Diapositive 3: Savez-vous à quoi servent les renseignements que vous donnez sur Internet?**

- *Internet est un moyen facile de collecter et d'emmagasiner des données sur des personnes. Des entreprises peuvent vous inviter à participer à des sondages et à des concours en ligne et à remplir des formulaires d'inscription dans le seul but d'obtenir des renseignements personnels sur vous.*
- *Ces renseignements peuvent, entre autres, servir à organiser des campagnes publicitaires adaptées à des groupes de jeunes bien précis ou être vendus à d'autres entreprises qui vous enverront ensuite des courriels.*
- *Par exemple, certains sites de réseautage social utilisent les renseignements que vous inscrivez dans votre profil pour déterminer quelles annonces apparaîtront dans votre profil et dans les pages que vous visitez.*

**Diapositive 4 : Méfiez-vous des sites Web qui vous demandent :**

- **votre nom complet;**
  - **votre adresse, votre code postal et vos numéros de téléphone à la maison**
  - **votre adresse de courriel**
  - **les adresses de courriel de vos amis**
  - **vos passe-temps et intérêts**
- *Comme toutes les fois où vous donnez des renseignements personnels dans la vraie vie, faites attention aux gens avec qui vous échangez de l'information.*

- *Il est possible d'obtenir vos renseignements personnels et d'en faire une utilisation inappropriée de bien des façons, par exemple :*
  - *quand vous donnez des renseignements pour vous inscrire à des services Internet ou télécharger un logiciel (partage de fichiers, messagerie instantanée, courriel, etc.);*
  - *quand vous créez un profil personnel pour un site de réseautage social ou de jeu en ligne;*
  - *quand vous participez à des sondages en ligne dans l'espoir de gagner des prix;*
  - *quand vous publiez des messages sur le babillard d'un site Web;*
  - *quand vous donnez des renseignements personnels dans un bavardoir ou au cours d'une séance de messagerie instantanée.*
- *Avant de donner tout renseignement personnel en ligne, vous devriez :*
  - *tâcher de savoir pourquoi tant d'information est nécessaire et lire la clause de confidentialité du site pour savoir si vos renseignements resteront confidentiels;*
  - *toujours lire la politique de confidentialité du site Web ou du fournisseur de services avant de donner des renseignements personnels ou d'accepter quoi que ce soit.*
- *Pour protéger le mieux possible vos renseignements personnels en ligne, vous pouvez vous doter d'une autre adresse courriel, créée à partir de faux renseignements, qui sera réservée aux sites Web qui en demandent une. De cette manière, si vous recevez des pourriels à cette adresse, votre adresse personnelle, elle, ne sera pas compromise.*

#### ***Diapositive 5 :***

*Posez les questions suivantes aux élèves. Vous pouvez leur demander de réfléchir à haute voix, ou encore leur donner quelques secondes pour y penser dans leur tête.*

- *Vous recevez ce message instantané de Beaumec\_04. Que feriez-vous? Y répondre en donnant l'information demandée parce que l'avatar semble plutôt gentil? Répondre en donnant des renseignements presque tous faux? Ne pas répondre du tout?*
- *Que feriez-vous si, au centre commercial, une personne qui semble gentille vous posait ces questions? Répondriez-vous de la même façon?*
- *Si vous ne le feriez pas au centre commercial, pourquoi le feriez-vous en ligne?*

#### ***Diapositive 6: Vol d'identité***

- **Un vol d'identité consiste à obtenir et utiliser de façon frauduleuse l'identité d'une autre personne dans le but de commettre des fraudes ou d'autres activités criminelles, habituellement pour en profiter financièrement.**
- **On peut en payer le prix pendant des années.**
- **Soyez toujours prudents. Pensez-y bien avant de transmettre des renseignements personnels en ligne et prenez les mesures voulues pour les protéger!**

*Si une personne obtient des renseignements personnels comme votre date de naissance, votre adresse, votre numéro d'assurance sociale et des renseignements au sujet de votre emploi, elle peut s'en servir pour se faire passer pour vous. Elle peut demander des cartes de crédit en votre nom à votre insu! Elle peut aussi prendre le contrôle de vos comptes bancaires ou en ouvrir de nouveaux, effectuer des transferts de solde, demander des prêts ou acheter des biens et des services. Vos renseignements peuvent également servir à obtenir des passeports, des visas et d'autres documents importants.*

*On peut en payer le prix pendant des années. Si une personne obtient une carte de crédit en votre nom, elle pourrait entacher votre dossier de crédit pendant une période allant jusqu'à dix ans! Il vous sera pratiquement impossible d'obtenir un prêt d'une institution financière, d'acheter une voiture ou de contracter une hypothèque le jour où vous voudrez acheter une maison.*

*Pour vous aider à minimiser vos risques de vol d'identité, pensez-y bien avant de communiquer des renseignements en ligne. Si vous jugez bizarre qu'on vous demande certains renseignements, eh bien ne les fournissez pas! Faites confiance à votre intuition lorsqu'il s'agit de fournir des renseignements personnels en ligne – si vous ne vous sentez pas à l'aise de divulguer certains détails, ne le faites pas!*

*Si vous effectuez des transactions sur des sites bancaires ou d'autres sites pour lesquels vous devez entrer des renseignements confidentiels, n'utilisez pas d'ordinateurs accessibles dans les endroits publics et assurez-vous de fermer votre session lorsque vous avez terminé. Il sera ainsi plus difficile pour les autres de voler vos renseignements personnels.*

#### **Diapositive 7 : Hameçonnage**

- **L'hameçonnage est une méthode utilisée pour obtenir des renseignements illégalement. Pour ce faire, on envoie à une personne de faux courriels qui semblent provenir d'une entreprise légitime (p. ex. une banque ou un site d'enchère en ligne).**
- **N'OUBLIEZ pas qu'une entreprise légitime ne vous demandera jamais de lui fournir votre mot de passe!**

*Ces courriels redirigent la personne à un faux site Web qui semble être exploité par la même entreprise et sur lequel on lui demande de fournir des renseignements personnels comme des numéros de compte et des mots de passe. Si la personne acquiesce à la demande, ces renseignements sont directement transmis aux escrocs responsables de la combine.*

*Exemple : En juin 2004, [des fraudeurs ont lancé un hameçon aux clients de la Banque Royale](#). Des messages électroniques frauduleux provenant soi-disant de la banque ont été envoyés aux clients. Dans ces messages, on demandait aux clients de confirmer leurs numéros de compte et leurs numéros d'identification personnels (NIP) à l'aide du lien*

fourni. Le message frauduleux indiquait que si le destinataire ne cliquait pas sur le lien pour inscrire ces renseignements, il ne pourrait plus accéder à son compte.

#### **Diapositive 8 : Achats et transactions bancaires en ligne**

- **Faites uniquement affaire avec des entreprises dignes de confiance.**
- **Assurez-vous qu'il y a l'icône d'un cadenas verrouillé ou d'une clé intacte dans le coin inférieur droit de la fenêtre de votre navigateur au moment d'effectuer des achats ou des transactions bancaires en ligne.**
- **Prenez soin de bien fermer votre session quand vous avez terminé.**
- **Pour vos transactions bancaires, n'utilisez jamais un mot de passe dont vous vous servez pour un autre site.**

*L'icône d'un cadenas verrouillé ou d'une clé intacte dans le coin inférieur droit de la fenêtre de votre navigateur indique qu'il s'agit d'un site sécuritaire et qu'il est peu probable que des imposteurs puissent voir vos renseignements.*

*Pour fermer correctement une session, cliquez toujours sur le bouton « Fermer la session » ou « Fin de la session » plutôt que sur le X dans le coin supérieur droit de la fenêtre.*

*Utiliser plusieurs mots de passe est le meilleur moyen de protéger vos renseignements personnels. Ne révélez à personne votre mot de passe bancaire. Si vous devez le prendre en note, ne l'emmagasinez pas dans votre ordinateur.*

#### **Diapositive 9 : Utilisation des cartes de crédit en ligne**

- **Consultez les politiques du commerçant et conservez vos reçus.**
- **Utilisez uniquement des systèmes de transfert de paiement sécurisés (p. ex. protocoles SSL).**
- **Ne faites affaire qu'avec les commerçants fiables : assurez-vous qu'ils ont une adresse et un numéro de téléphone vérifiables et consultez les commentaires formulés par les autres acheteurs à leur sujet.**

*Toute entreprise qui vous autorise à régler vos achats à l'aide de transferts ou de paiements par carte de crédit devrait utiliser un protocole sécurisé pour coder toutes les données transmises. Cette technologie rend les données pratiquement impossibles à déchiffrer par une tierce partie. L'adresse des sites Web munis d'un protocole sécurisé qui servent à régler des transactions devrait débiter par « https » plutôt que « http ».*

*La plupart des sites d'enchère comportent un système qui permet aux acheteurs de coter les vendeurs. Consultez les commentaires formulés par les autres acheteurs pour établir si le vendeur est fiable.*

#### **Diapositive 10 : Concours en ligne**

**Ce sont les prix à gagner qui rendent ces concours si intéressants! Mais dans bien des cas, vous devez fournir une tonne de renseignements personnels. Que faire?**

*Laissez les élèves répondre à cette question. Il est utile de leur rappeler que, même s'il y a des prix à gagner, il y a de nombreuses escroqueries sur Internet.*

*Avant de participer à un concours en ligne, posez-vous les questions suivantes :*

- *Le concours est-il organisé par une entreprise que vous connaissez?*
- *Donne-t-on un numéro où vous pouvez appeler pour obtenir des détails, ou un site Web que vous pouvez visiter?*
- *Que devez-vous faire pour gagner? Répondre à une question facile ou donner des renseignements personnels?*
- *Rappelez aux élèves que même s'ils suivent toutes les règles de sécurité lorsqu'ils participent à un concours ou magasinent en ligne, ils peuvent être victimes d'une escroquerie en ligne. Les cyberescrocs peuvent créer de faux sites Web et courriels pratiquement impossibles à distinguer des vrais.*

*Surtout, cela semble-t-il trop beau pour être vrai?*

***Diapositive 11 : Si cela semble trop beau pour être vrai... alors ça l'est sans doute! Pour obtenir plus d'information ou pour signaler une escroquerie ou une fraude, allez à l'un des sites suivants :***

- [www.recol.ca](http://www.recol.ca)
- [www.phonebusters.com](http://www.phonebusters.com)

*Fiez-vous à votre instinct dans ce genre de situation. Si cela semble trop beau pour être vrai, alors ça l'est sans doute! Pour obtenir plus d'information ou pour signaler une escroquerie ou une fraude, rendez-vous sur le site de RECOL (Signalement en direct des crimes) à [www.recol.ca](http://www.recol.ca) ou au site du Centre d'appel antifraude du Canada à [www.phonebusters.com](http://www.phonebusters.com).*

***Diapositive 12 : L'histoire de Michel***

*Présentez l'histoire de Michel (ci-dessous) et laissez les élèves répondre à la question suivante : « Que peut-il arriver une fois que Michel a divulgué ces renseignements? »*

*L'histoire de Michel :*

*Michel parcourait un site de petites annonces en ligne (un site sur lequel on peut annoncer des articles à vendre, comme Craigslist et Kijiji) à la recherche d'un jeu vidéo rare qu'il voulait se procurer. Il a fini par le trouver à un prix très raisonnable sur la page d'un vendeur nommé ill\_skillz. Michel a envoyé un message à ill\_skillz pour lui dire qu'il souhaitait acheter le jeu. Plus tard cette journée-là, Michel a reçu un courriel d'ill\_skillz. Ill\_skillz expliquait à Michel qu'il était en vacances et que ce dernier pouvait communiquer avec son frère pour conclure la transaction. Il a demandé à Michel d'acheminer son nom complet, son adresse postale et son numéro de carte de crédit à son frère à l'adresse électronique inscrite dans le courriel. Michel n'était pas vraiment à l'aise avec cette idée, mais ill\_skillz l'a rassuré en lui expliquant que son frère n'avait besoin du numéro de carte de crédit que pour réserver le jeu vidéo à Michel et garantir qu'il ne serait pas vendu à une autre personne.*

*Michel a fait parvenir le courriel demandé et a attendu impatiemment qu'ill\_skillz ou son frère lui donne des nouvelles. Quelques jours plus tard, il n'avait toujours pas reçu de confirmation de l'envoi du jeu vidéo. Lorsqu'il a reçu son relevé de carte de crédit à la fin du mois, il a découvert que la limite de sa carte de crédit avait été atteinte le jour même où il avait envoyé le courriel.*

*Rappelez aux élèves ce qui suit :*

- *Vous ne devez jamais donner des renseignements personnels ou des numéros de carte de crédit à une personne ou une entreprise si vous n'êtes pas persuadé qu'il s'agit d'une transaction légitime.*
- *Réglez vos achats en ligne uniquement si les sites sont dotés d'un système de paiement sécurisé.*
- *Une fois qu'une personne détient des renseignements personnels comme votre adresse et votre numéro de carte de crédit, il est facile pour elle de voler votre identité et de compromettre votre crédit (si le concept de crédit est nouveau pour les élèves, expliquez-le).*

### ***Diapositive 13 : Le clavardage***

*La majorité des jeunes font du clavardage tous les jours, que ce soit grâce à la messagerie instantanée ou aux sites de réseautage social.*

*- 86 % des élèves de 11<sup>e</sup> année ou de secondaire 5 utilisent la messagerie instantanée pendant un jour moyen.*

*- 86 % des élèves disent avoir des comptes de courriel. ([Media Awareness Network, Key Findings, « Young Canadians in a Wired World - Phase 2 », 2005](#))*

### ***Diapositive 14 : Les avantages du clavardage***

- ***On peut rester en contact avec des camarades d'école ou avec des amis qui ont déménagé.***
- ***On peut clavarder tout en naviguant sur le Web.***
- ***On peut se faire de nouveaux amis partout dans le monde.***
- ***On peut utiliser des logiciels de clavardage pour collaborer à des projets scolaires ou pour transférer des fichiers.***

*Demandez aux jeunes s'ils peuvent trouver d'autres avantages.*

**Diapositive 15 : Les aspects négatifs du clavardage**

- **Le ton et les émotions ne se communiquent pas facilement par écrit (ce qui provoque parfois des malentendus).**
- **On devient vite accro.**
- **On risque d'utiliser des formes abrégées et des expressions trop familières dans son langage de tous les jours et dans les textes qu'on rédige.**
- **On ne sait pas toujours si on devrait converser ou non avec les gens qu'on rencontre sur Internet**
- **Les gens peuvent mentir sur leur âge, sur l'endroit où ils se trouvent et sur leurs intentions.**
- **Vous vous exposez à du harcèlement, à de la violence verbale ou à de la cyberintimidation.**

*Demandez aux jeunes s'ils peuvent trouver d'autres aspects négatifs.*

**Diapositive 16: Sites de réseautage social**

- **Ajoutez seulement vos amis dans la vraie vie.**
- **Réglez vos paramètres de sécurité, sinon pratiquement n'importe qui peut voir ce que vous affichez en ligne!**
- **Respectez les autres en ligne : s'ils ne veulent pas que leur nom ou leurs photos apparaissent sur votre page, respectez leur volonté!**

**N'oubliez pas : aucune information ne reste privée une fois publiée en ligne! Vous n'avez aucun contrôle sur la façon dont elle sera utilisée.**

*Les sites de réseautage social offrent un autre moyen de rester en contact avec ses amis et sa famille. Même s'il est très pratique d'avoir un blogue, un site personnel ou un espace sur un site public, il faut faire attention à ce qu'on affiche sur ces sites. Vous devez aussi bien réfléchir à qui vous ajoutez comme amis, à ce que vous dites et faites sur ces sites, et à qui vous donnez accès à vos renseignements.*

*Basic rule of thumb: Do not post or do anything you would not want your parents or grandparents to see!*

- *Voici une bonne règle de base : N'affichez ou ne faites rien que vous ne voudriez pas que vos parents ou vos grands-parents voient!*

**Diapositive 17 : Des conseils sur le clavardage**

- **Utilisez un pseudonyme impersonnel.**
  - **Ex. : BelleAbeille, Champion\_22, \*hyper\_1\*.**
- **Ne donnez jamais de renseignements personnels (la ville dans laquelle vous habitez, le nom de votre école, les équipes sportives desquelles vous faites partie, etc.).**
- **N'envoyez jamais de photos de vous, surtout aux gens que vous ne connaissez pas personnellement.**

- **N'acceptez jamais de rencontrer des personnes que vous avez connues en ligne, surtout si vous êtes seule ou seul ou que personne ne sait où vous allez et qui vous rencontrez.**
- **Si quelqu'un à qui vous parlez en ligne vous met mal à l'aide, parlez-en à un parent ou à un adulte de confiance.**

*Voici quelques conseils à suivre pour que le clavardage demeure une activité amusante :*

- *Utilisez un pseudonyme impersonnel. Le pseudonyme parfait n'évoque en rien votre identité réelle. Votre nom en ligne est la première chose que les autres voient et détermine la première impression qu'ils auront de vous.  
Ex. : BelleAbeille, Champion\_22, \*hyper\_1\*.*
- *Ne donnez jamais de renseignements personnels. Les « renseignements personnels », ce sont des renseignements que vous ne donneriez pas volontiers à un inconnu dans l'autobus ou dans une file d'attente à l'épicerie.*
- *N'envoyez jamais de photos de vous. Transmettre une photo paraît peut-être anodin, mais dès qu'elle est partie, vous ne contrôlez plus qui la verra et à quoi elle servira. Vous ne savez jamais où votre photo peut aboutir ni entre les mains de qui elle peut tomber. Imaginez l'effet que ça vous ferait de voir votre photo sur [www.jeunesfous.com](http://www.jeunesfous.com)! À partir du moment où vous envoyez votre photo sur Internet, des gens peuvent s'en servir, la modifier, la diffuser, et vous ne pouvez rien pour les en empêcher.*
- *Par ailleurs, la personne à qui vous envoyez votre photo n'est peut-être pas qui elle prétend être, mais elle sait exactement de quoi vous avez l'air. Si vous lui avez aussi donné des renseignements sur vous, il peut être très facile pour elle de vous retrouver sans votre permission.*
- *N'acceptez jamais de rencontrer des personnes que vous avez connues en ligne, surtout si vous êtes seule ou seul ou que personne ne sait où vous allez et qui vous rencontrez. Vous aurez peut-être envie de rencontrer une personne connue sur Internet, mais le fait est que vous ne saurez jamais à qui vous avez vraiment affaire. Posez-vous la question suivante : avez-vous déjà menti à quelqu'un en ligne? Probablement. Cela signifie qu'il est probable qu'on vous ait aussi menti. La personne que vous rencontrez pourrait ne pas être qui elle prétend être ou avoir menti sur ses intentions.*
- *Si quelqu'un à qui vous parlez en ligne vous met mal à l'aide, parlez-en à un parent ou à un adulte de confiance.*

### **Diapositive 18 : La cyberintimidation**

*La cyberintimidation est l'utilisation des technologies de communications comme Internet, les sites de réseautage social, les sites Web, les courriels, la messagerie texte et la messagerie instantanée pour continuellement intimider ou harceler les autres.*

### **Diapositive 19 : Exemples de cyberintimidation**

- **Envoyer des courriels ou des messages textes ou instantanés méchants ou menaçants.**
- **Afficher des photos gênantes de quelqu'un en ligne.**

- **Créer un site Web pour se moquer des autres.**
- **Se faire passer pour une autre personne en utilisant son nom.**
- **Tromper une personne pour lui faire révéler des renseignements personnels ou de l'information gênante et les envoyer à d'autres.**

**Diapositive 20 : David Knight**

*Racontez l'histoire de David (ci-dessous). On vous demandera peut-être des précisions à ce sujet. Nous vous suggérons de répondre que les détails de cette affaire sont sans importance et que ce qu'il faut surtout retenir, ce sont les dommages que cause l'intimidation, en ligne ou en personne.*

David Knight

*Tel que relaté par la [CBC, 2005](#) :*

- *Pour David Knight, l'école était un enfer.*
- *Il ne savait absolument pas pourquoi il se faisait agacer, ridiculiser et tabasser depuis des années.*
- *L'humiliation a franchi les limites du tolérable lorsque quelqu'un a ouvert un site diffamatoire à son endroit.*
- *Le site contenait des propos vulgaires à caractère sexuel qui portaient atteinte à la réputation de David. Il recevait aussi des courriels méchants contenant des messages semblables.*
- *Dans le cas de David, il ne s'agissait plus d'une trentaine d'élèves qui disaient des choses à son sujet dans la cafétéria : ce qui était écrit en ligne pouvait être vu par 6 milliards de personnes.*
- *Se sentant pris au piège, David a abandonné l'école et fini sa dernière année d'études à la maison.*
- *Sept mois plus tard, David et sa famille ont finalement réussi à faire retirer le site Web blessant d'Internet.*

**Diapositive 21 :**

**En quoi la cyberintimidation est-elle différente de l'intimidation traditionnelle?**

**Que faire si vous êtes victime de cyberintimidation?**

*Posez la question au groupe et écrivez leurs réponses sur le tableau noir ou sur un tableau à feuilles. S'ils ont du mal à répondre à la question, donnez quelques exemples parmi les suivants pour encourager la participation. Dès que la discussion s'achève, passez à la diapositive suivante.*

1) *En quoi la cyberintimidation est-elle différente de l'intimidation traditionnelle?*

- *Elle n'a pas de limite : la cyberintimidation peut suivre un élève à la maison après l'école ou à tout endroit où des technologies de communications sont accessibles.*
- *Elle peut être plus dure : on dit souvent des choses en ligne qu'on ne dirait pas normalement en personne parce qu'on ne peut voir la réaction de l'autre.*

- Elle a une plus grande portée : une personne peut se moquer d'une autre personne dans un courriel ou un site Web destiné à toute la classe ou au monde entier. Personne n'est à l'abri de la cyberintimidation, pas même les professeurs, les directeurs et d'autres adultes.
  - Elle peut être anonyme : on utilise souvent des adresses de courriel et des noms fictifs. Souvent, le cyberintimidateur connaît la victime, mais la victime ne sait pas qui est le cyberintimidateur.
- 2) *Que faire si vous êtes victime de cyberintimidation?*
- Ne répondez pas aux messages ou aux affichages des cyberintimidateurs. Si possible, bloquez l'expéditeur des courriels ou messages.
  - Gardez une copie des messages. Vous n'avez pas à les lire, mais vous aurez besoin d'une copie si vous décidez de dénoncer la cyberintimidation.
  - Parlez-en à quelqu'un, comme un parent, un enseignant, un agent de la paix ou un adulte de confiance.
  - Si les messages sont sur un site ou une page Web, il faut communiquer avec le fournisseur de services Internet (FSI). La plupart des FSI ont des politiques sur l'utilisation de leur service et sur les mesures qu'il est possible de prendre si ces politiques ne sont pas respectées. Un grand nombre de sites Web contiennent un lien ou un bouton pour signaler un contenu inapproprié. Dans certains cas, les propriétaires des sites Web peuvent eux-mêmes retirer le contenu ou avertir la personne qui l'a affiché, mais dans d'autres cas, il faut faire enquête.

### **Diapositive 22 : Premières impressions ?**

*Demandez aux élèves de vous donner leurs premières impressions de l'avatar de gauche, puis leurs premières impressions de l'avatar de droite. Demandez-leur ce qu'ils penseraient si vous leur disiez que l'avatar de gauche appartient en réalité à :*

- une adolescente de 15 ans,
- qui vit dans une communauté rurale en Alberta,
- qui fait partie de la chorale de son école et qui fait du bénévolat dans une maison de retraite locale.

*Demandez aux élèves ce qu'ils penseraient si vous leur disiez que l'avatar de droite appartient en réalité à :*

- un homme de 52 ans,
- qui vit avec sa famille dans une maison en rangée dans une grande ville,
- qui travaille pour une entreprise d'édition.

*Après avoir donné ces descriptions aux élèves, demandez-leur s'ils sont surpris. Leurs premières impressions étaient-elles différentes de la description de la personne?*

### **Diapositive 23 : Réfléchissez à ce qui suit :**

- 1) **Les premières impressions en ligne sont importantes.**
  - **Demandez aux jeunes de réfléchir aux impressions que pourraient donner d'eux les images (réelles ou fausses) qu'ils affichent en ligne.**
- 2) **Les gens ne sont pas toujours ce qu'ils prétendent être.**

- **Avez-vous déjà menti en ligne (au sujet de votre âge, d'où vous venez, etc.)?**

**Si vous pouvez mentir, d'autres le peuvent aussi. Ne croyez pas tout ce que quelqu'un vous dit en ligne!**

*Expliquez aux jeunes que cet exercice était fictif et qu'il a été créé pour leur amener à réfléchir à ces deux choses.*

#### **Diapositive 24 : Le leurre par Internet**

*La plupart d'entre vous avez probablement déjà inventé des choses en ligne, comme votre âge ou la ville où vous vivez. Il est donc possible que quelqu'un avec qui vous avez parlé n'était pas tout à fait honnête non plus. Malheureusement, les personnes qui inventent des choses en ligne n'ont pas toutes de bonnes intentions.*

#### **Diapositive 25 :**

*Certaines personnes que vous rencontrez en ligne pourraient vous contacter dans un but sexuel, et non par amitié sincère. Utiliser Internet pour attirer un jeune à une rencontre pour des motifs sexuels s'appelle le leurre d'enfant et est un crime au Canada.*

#### **Diapositive 26 : Signaux d'alarme**

- **L'interlocuteur vous offre des cadeaux ou un emploi.**
- **Il est très affectueux et vous fait beaucoup de compliments.**
- **Il vous offre de vous aider à faire vos devoirs ou à régler des problèmes personnels.**
- **Il prétend qu'il se trouve dans une situation urgente et que vous devez lui venir en aide immédiatement.**
- **Il tente de vous menacer, de vous intimider ou de vous donner des ordres.**
- **Il fait l'impossible pour se lier d'amitié avec vous.**
- **Il introduit graduellement un contenu à caractère sexuel dans les conversations.**

**N'oubliez pas : Les gens ne sont pas nécessairement qui ils prétendent être. Ce n'est pas parce que quelqu'un semble avoir à peu près votre âge qu'il ou elle a votre âge en réalité. Les adultes peuvent faire semblant en ligne d'être plus jeunes. Parfois, des adultes apparemment dignes de confiance sont mal intentionnés.**

*- Voici l'expérience vécue par une jeune Canadienne qui a rencontré quelqu'un en ligne, telle que relatée par la CBC :*

- *Cette histoire est basée sur des faits vécus; toutefois, pour protéger l'identité de la victime, nous l'appellerons simplement « Katrina ». En 2003, Katrina, alors âgée de 12 ans, a rencontré dans un bavardoir un garçon qui disait avoir 17 ans. Ils ont eu deux conversations à caractère sexuel, puis ont échangé leurs coordonnées. Le garçon a appelé Katrina pour lui faire des avances sexuelles. Elle a raccroché le téléphone et son père a appelé la police. ([CBC, 2003](#)).*

#### **Diapositive 27 :**

**Les internautes n'ont pas tous de mauvaises intentions. Internet peut être un excellent moyen de rencontrer des gens et de se faire de nouveaux amis!**

*Le but de cette leçon est de vous sensibiliser et de vous amener, je l'espère, à réfléchir de façon critique à ce que vous faites en ligne.*

**Diapositive 28 : Si quelqu'un vous met mal à l'aise en ligne :**

- Cessez tous contacts avec la personne et bloquez ses messages, si possible.
- Sauvegardez le message et son contenu, si possible (y compris le pseudonyme et l'adresse de courriel de la personne) au cas où les autorités doivent faire enquête.
- Parlez-en à un adulte de confiance (parent, enseignant, agent de la paix, etc.).
- Vous pouvez également contacter [www.cyberaide.ca](http://www.cyberaide.ca) pour signaler tout comportement en ligne choquant ou qui vous met mal à l'aise.

**Diapositive 29 : Chris**

*Lisez le scénario aux élèves, puis posez-leur les questions suivantes. Fournissez les réponses suivantes si les élèves ne les mentionnent pas.*

*Dans le cadre de son cours de sciences sociales, Chris effectuait des recherches sur les agressions sexuelles lorsqu'il est tombé sur un site Web pornographique qui disait présenter d'authentiques photos de viols. Chris a conclu que ce site ne représentait probablement pas la réalité, mais il se sentait néanmoins mal à l'aise vis-à-vis du fait que ce site existait sur Internet.*

1) *Qu'auriez-vous fait si vous aviez été à la place de Chris?*

- *En parler à un adulte de confiance.*
- *Noter l'adresse du site Web et l'heure et la date auxquelles on a trouvé ce site.*
- *Signaler le site Web à [www.cyberaide.ca](http://www.cyberaide.ca).*

**Diapositive 30 : Signalez toute activité illégale observée en ligne à la police :**

- **Cyberharcèlement**
- **Escroqueries ou fraude par Internet**
- **Activités dangereuses et illégales, comme la fabrication de bombes, le terrorisme ou le commerce d'armes non enregistrées**
- **Menaces physiques**
- **Crimes haineux**
- **Piratage informatique (fait de pénétrer illégalement un ordinateur ou un réseau informatique)**

*Dites ce qui suit aux élèves : Lorsque vous naviguez sur Internet, vous pouvez toujours tomber par hasard sur quelque chose de dérangentant ou qui vous met mal à l'aise. La GRC recommande d'alerter la police si vous observez l'une des activités illégales suivantes sur Internet :*

*Si vous observez un acte illégal qui ne constitue pas un cas d'urgence, signalez-le à votre fournisseur de services Internet (FSI) et à la police. La plupart des FSI ont une « charte de bon usage » qui énonce clairement les droits de leurs abonnés, les règles à suivre et les conséquences du non-respect de ces règles.*

**Diapositive 31 : La RÉALITÉ**

**Pourquoi faire en ligne ce que vous ne feriez pas en personne?  
Réfléchissez de façon critique à ce que vous faites en ligne!**

*Terminez la présentation en disant ce qui suit aux élèves : tout ce que vous faites en ligne a des conséquences dans la vraie vie. Ne faites pas en ligne ce que vous ne feriez pas en personne.*

**Diapositive 32 : Souhaitez-vous obtenir plus d'information?**

**Rendez-vous sur le site [www.choix.org](http://www.choix.org) pour en apprendre davantage sur ce que vous pouvez faire pour sensibiliser votre école et votre collectivité!**

**Et visitez ces sites web :**

**[www.cyberaide.ca](http://www.cyberaide.ca)**

**[www.webaverti.ca](http://www.webaverti.ca)**

**[www.thinkuknow.com](http://www.thinkuknow.com) (site en anglais)**

**[www.media-awareness.ca](http://www.media-awareness.ca)**

**[www.jeunessejecoute.ca](http://www.jeunessejecoute.ca) (1-800-668-6868)**

*N'hésitez pas à communiquer avec moi si vous n'avez pas obtenu réponse à toutes vos questions aujourd'hui. Vous pouvez aussi visiter **choix.org** ou envoyer un courriel à [deal-choix@rcmp-grc.gc.ca](mailto:deal-choix@rcmp-grc.gc.ca) pour vous renseigner davantage. Si vous désirez faire une campagne de sécurité en ligne dans votre école ou votre collectivité, consultez la boîte à outils sur le site [choix.org](http://choix.org) pour connaître les ressources à votre disposition! Je vous ai fourni plusieurs autres sites que vous pouvez consulter pour obtenir plus d'information. Merci de m'avoir invité à venir vous parler aujourd'hui!*