

Texte: La cybersécurité 11-13 ans

Les notes du présentateur sont en italiques

Diapo 1: Choix.org traite de la sécurité sur Internet : faire face aux réalités du Net

Diapo 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 Net.*

Diapo 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 pourriels.*
- *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.*

Diapo 4: Méfiez-vous des sites Web qui vous demandent :

- **Votre nom complet**
- **Votre adresse, votre code postal et votre numéro de téléphone à la maison**
- **Votre adresse courriel**
- **Les adresses 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.*

Diapo 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 un 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?*

Diapo 6: Les concours en ligne

Ils sont si attrayants car vous pourriez gagner quelque chose!! Mais ils demandent souvent plein d'informations personnelles. Que devriez-vous 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?

Diapo 7: 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 aux sites suivants :

- www.recol.ca
- 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, allez au site du Centre RECOL (Signalement en direct des crimes) à www.recol.ca ou au site du Centre d'appel antifraude du Canada à www.phonebusters.com.

Diapo 8: 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^e 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](#))

Diapo 9: 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 penser à d'autres avantages du clavardage.

Diapo 10: L'histoire de Michel

Présentez l'histoire de Michel 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 se trouvait dans son bavardoir préféré lorsqu'il a reçu un message privé d'ill_skillz. Ill_skillz et Michel ont clavardé pendant quelques minutes, et ill_skillz a parlé à Michel d'une nouvelle application fantastique pour un site de réseautage social

populaire qui permettrait à Michel de voir toutes les personnes qui ont regardé son profil. Michel voulait vraiment cette application et a demandé à ill_skillz comment il pouvait se la procurer. Ill-skillz a dit à Michel que c'était très compliqué et que ça lui prendrait beaucoup de temps à lui expliquer. Il a dit à Michel de lui donner son nom d'utilisateur et son mot de passe, et qu'il ajouterait rapidement l'application à son système pour lui. Michel n'était pas vraiment à l'aise avec cette idée, mais ill_skillz l'a rassuré en expliquant que Michel pourrait changer son mot de passe dès que l'application serait installée.

Michel a donné à ill_skillz son nom d'utilisateur et son mot de passe, et attendait de ses nouvelles avec anxiété. Après avoir attendu ce qui lui semblait une éternité, Michel a tenté d'envoyer un message à ill_skillz pour savoir comment les choses se passaient, mais il s'est rendu compte que celui-ci avait quitté le bavardoir. Michel a alors essayé d'entrer dans son compte de réseautage social mais a découvert que son mot de passe ne fonctionnait plus. Michel ne pouvait pas croire qu'il avait donné son nom d'utilisateur et son mot de passe si rapidement, même si l'idée le mettait mal à l'aise.

Voici quelques réponses possibles à la question :

- Un inconnu pourrait maintenant connaître des détails personnels comme son adresse, à quelle école il va et où il travaille.
- Sa photo pourrait être utilisée à d'autres fins.
- Des messages méchants pourraient être envoyés à ses amis à partir de son compte.
- Des renseignements personnels concernant ses amis pourraient être utilisés à d'autres fins.

Lorsque les élèves ont terminé de répondre à la question, rappelez-leur ce qui suit :

- Donner votre mot de passe, c'est comme donner la combinaison de votre casier.
- Ne révélez jamais votre mot de passe, même pas à vos amis. Dès que vous donnez accès à vos renseignements, vous n'avez aucun contrôle sur la façon dont ils seront utilisés!

Diapo 11: 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 (vous finirez peut-être par passer plus de temps à clavarder que vous l'auriez voulu).**
- **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 au harcèlement, à la violence verbale ou à la cyberintimidation.**

Demandez aux jeunes s'ils peuvent penser à d'autres aspects négatifs du clavardage

Diapo 12: Les sites de réseautage social

- **Ajoutez seulement les amis que vous connaissez personnellement.**
- **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 qu'elle est 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.

- *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!*

Diapo 13: Des conseils sur le clavardage

- **Utilisez un pseudonyme qui ne révèle pas trop à votre sujet**
 - Exemples: BelleAbeille, Champion_22, *hyper_1*
- **Ne donnez pas vos informations personnelles (la ville où vous habitez, l'école que vous fréquentez, les équipes sportives auxquelles vous appartenez etc.)**
- **N'envoyer pas de photos de vous – surtout pas à des personnes que vous ne connaissez pas personnellement**
- **Ne rencontrez pas en personne des gens dont vous avez fait la connaissance en ligne – surtout pas tout(e) seul(e) ou sans informer quelqu'un où vous allez et qui vous rencontrez**
- **Si quelqu'un à qui vous parlez en ligne vous met mal à l'aise, parlez-en à un parent ou à un adulte de confiance.**

Voici quelques conseils à garder en tête 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! 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 faire 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 maintenant 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 retracer 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. Cela peut être tentant de rencontrer une personne avec qui vous vous êtes lié d'amitié 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.*

Diapo 14: 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.

Diapo 15: 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 personnes.**

Diapo 16: David Knight

Partagez l'histoire de David (ci-dessous). On vous demandera peut-être des précisions sur l'histoire de David. 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 créé un site Web diffamatoire à son sujet.*

- 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 a 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 de l'Internet.

Diapo 17:

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

Que pouvez-vous faire si vous êtes victime de cyberintimidation?

Posez les questions 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 pas 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 courriel et des noms fictifs. Souvent, le cyberintimidateur connaît la victime, mais la victime ne sait pas qui est le cyberintimidateur.

2) Que pouvez-vous 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 il est possible que vous aurez besoin d'une copie si vous décidez de dénoncer le cyberintimidateur.
- 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, communiquez 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, une enquête est nécessaire.

Diapo 18: 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?

Diapo 19: 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 les faire penser à ces deux points.

Diapo 20: Le leurre par Internet

La plupart d'entre vous ont 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.

Diapo 21:

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, ou la cyberprédation, et est un crime au Canada.

Diapo 22: Signaux d'alarme

- L'interlocuteur vous offre des cadeaux ou un emploi;
- Il est très affectueux et vous fait beaucoup de compliments;
- Il 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 se donne du mal 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](#)).*

Diapo 23:

Cela dit, 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.

Diapo 24: Si quelqu'un en ligne vous met mal à l'aise...

- **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 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 pour signaler tout comportement en ligne offensif ou qui vous met mal à l'aise.**

Diapo 25: Nathalie

Lisez le scénario de Nathalie aux élèves, puis posez-leur les questions fournies. Laissez les élèves répondre aux questions et ajoutez les réponses présentées ci-dessous si les élèves n'y pensent pas.

Nathalie, qui a 12 ans, vient de s'inscrire à un site de réseautage social populaire. Elle veut que son profil présente une bonne image d'elle, alors elle y ajoute plusieurs photos d'elle en shorts et en gilet débardeur. Elle remplit les sections où on demande à quelle école elle va et quels sont ses passe-temps. Comme elle veut que les personnes qui voient son profil soient capables d'entrer en contact avec elle, elle ajoute aussi son adresse courriel et son numéro de cellulaire.

1) Afficheriez-vous en ligne le genre de photos et de renseignements que Nathalie a affichés?

- Il s'agit d'une question purement rhétorique; laissez les jeunes y réfléchir.

2) Qu'est-ce que les gens peuvent découvrir au sujet de Nathalie à partir des renseignements qu'elle a fournis?

- Quelqu'un pourrait faire une recherche à partir du nom de son école pour découvrir dans quelle ville elle habite.

- Quelqu'un pourrait faire une recherche à partir de son nom pour trouver d'autres renseignements sur elle sur Internet. Cela pourrait comprendre des renseignements dont elle ignore l'existence, comme des articles de journaux dans lesquels son nom apparaît ou des photos dont la légende contient son nom.

- À partir des photos qu'elle a fournies, quelqu'un pourrait se rendre à son école et la reconnaître.

- Même si tout ça semble très improbable, plus vous affichez de renseignements en ligne, plus il sera facile pour les autres d'avoir accès à votre vie privée.

3) Qu'est-ce que Nathalie peut faire pour être plus en sécurité en ligne?

- Utiliser un pseudonyme dans son profil.

- Retirer les renseignements personnels comme le nom de son école et son numéro de cellulaire.

- Régler ses paramètres de sécurité pour que seuls ses amis puissent voir ses renseignements et ses photos. (Aussi, ajouter seulement ses amis dans la vraie vie.)

Diapo 26: Chris

Lisez le scénario suivant 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 vous avez trouvé ce site.

- Signaler le site Web à www.cyberaide.ca.

Diapo 27: Signalez toute information illégale que vous trouvez 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 déroutant ou qui vous met mal à l'aise. La GRC recommande d'alerter la police si vous observez l'une des activités illégales mentionnées ci-haut.

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.

Diapo 28: La RÉALITÉ

**Si vous ne le feriez pas en personne, pourquoi le feriez-vous en ligne ?
Pensez 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. Si vous ne feriez pas quelque chose en personne, ne le faites pas en ligne.

Diapo 29: Vous voulez plus d'information?

Visitez www.choix.org et on vous montrera comment vous pouvez vous impliquer dans vos écoles et vos communautés!

Jetez un coup d'œil à ces sites Web:

www.cyberaide.ca

www.bewebaware.ca/french

www.media-awareness.ca/francais

www.jeunessejecoute.ca (1-800-668-6868)

www.thinkuknow.com (anglais seulement)

*N'hésitez pas à communiquer avec moi si vous avez encore des questions sur ce qui a été présenté aujourd'hui. Vous pouvez aussi visiter **choix.org** ou envoyer un courriel à 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 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!*