Comportement d'autrui

GUIDE DU FORMATEUR

Le présent document sert de guide de référence et de préparation pour le formateur, ainsi que de complément au plan de leçon.

Les connaissances que l'apprenant doit avoir acquises au terme du module se trouvent dans la section « Objectifs d'apprentissage ».

La section « Contexte et détail pour le formateur » contient quant à elle une description du contenu ainsi que des liens vers des références permettant au formateur d'en apprendre plus sur le sujet. Il pourra ainsi mener les discussions et répondre aux questions avec assurance, sans être limité par la matière. Par ailleurs, chaque élément de la section « Contexte et détail pour le formateur » vient étayer une partie du scénario.

Objectifs d'apprentissage

- Connaître les caractéristiques du harcèlement et de l'intimidation en ligne.
- Être sensibilisé à la présence de prédateurs sexuels sur le Web.
- Savoir que la fraude en ligne existe et connaître les principaux types de fraudes.
- Savoir trouver de l'aide et dénoncer les fraudes faites en ligne.

Contexte et détail pour le formateur

1 Harcèlement et intimidation en ligne

1.1 En bref

L'intimidation en ligne est un comportement inacceptable, de par ses effets négatifs, et difficile à cerner. Le fait de reconnaître l'intimidation et d'en parler peut être la première étape pour contrer ce comportement.

1.2 En détail

- En pratique, il n'y a aucune différence entre le harcèlement en ligne et l'intimidation en ligne, aussi appelée cyberintimidation.
  - Ces termes sont souvent utilisés de manière interchangeable, bien que l'intimidation soit plus fréquemment associée aux environnements scolaires et professionnels[1].
  - La cyberintimidation se définit comme « un méfait intentionnel et répété commis à partir d'ordinateurs, de téléphones cellulaires ou de tout autre appareil électronique ».
    - Le harcèlement criminel consiste en la répétition d'actes qui amène les personnes visées à légitimement craindre pour leur sécurité[2].
- Il est impossible de connaître le nombre exact de cas de cyberintimidation chez les adolescents, mais on estime qu'au moins 20 à 30 % d'entre eux en auraient été victimes[3].
  - Vous entendrez que l'intimidation est fréquente et répandue, mais il faut faire attention.
    - Cela pourrait donner l'impression que l'intimidation est normale ou « sans grande importance ».
  - Un seul cas d'intimidation, peu importe sa nature, est un cas de trop.
  - Les actes qui créent des préjudices sont variés et difficiles à catégoriser ou à cibler[4].
  - Leur répétitivité est l'aspect le plus important et le plus facile à percevoir[5].
    - La nature permanente de ces actes crée un climat d'insécurité pour la victime qui se demande continuellement quel sera le prochain coup de son agresseur; à lui seul ce climat peut constituer un méfait.
    - Être victime de mauvais traitements jour après jour, aussi anodins soient-ils, finit par prendre le dessus.

1 Sur Internet : <http://www.cchst.ca/oshanswers/psychosocial/cyberbullying.html>.
2 Sur Internet : <http://www.justice.gc.ca/fra/pr-rp/jp-cj/vf-fv/har/part1.html>.
3 Sur Internet : <http://www.prevnet.ca/fr/intimidation/faits-et-solutions>.
4 Consulter la partie 1.6 du site : <http://www.justice.gc.ca/fra/pr-rp/jp-cj/vf-fv/har/part1.html>.
5 Sur Internet : <http://www.pensezcybersecurite.gc.ca/cnt/cbrbllng/prnts/cbrbllng-fr.aspx>.

- Les torts causés par la cyberintimidation ne sautent pas toujours aux yeux. Par contre, ils sont beaucoup plus graves que si on était simplement maltraité, bousculé ou ridiculisé.
- L'intimidation n'a jamais été admissible ou bénéfique.
  - Il est faux de croire à certaines idées véhiculées :
    - « C'est ainsi qu'agissent les garçons. »
    - « Ça va l'endurcir. »
    - « Ça va l'aider à se faire une carapace. »
    - « Ce qui ne tue pas rend plus fort. »
  - Ces phrases sont souvent utilisées pour amenuiser, normaliser ou gérer les comportements nocifs ou intimidateurs.

Les leçons de la vie peuvent toutes être enseignées d'une manière plus humaine et appropriée que par l'intimidation.

- Qu'est-ce qu'un intimidateur?
  - Les cyberintimidateurs :
    - peuvent être des personnes contrariées, en colère ou autrement tourmentées qui se servent des technologies auxquelles elles ont accès pour se défouler;
    - peuvent vouloir se venger, se faire justice ou donner une leçon à quelqu'un;
    - peuvent être eux-mêmes des victimes d'intimidation;
    - peuvent être incapables de faire le lien entre leurs actes dans le monde virtuel et les conséquences dans le monde réel;
      - Ces agresseurs sont souvent considérés comme des cyberintimidateurs par inadvertance, car bien que leurs actes soient intentionnels, ils ne cherchent pas à causer du tort.
    - ne sont pas nécessairement des personnes qui sont méchantes envers les autres dans la vie de tous les jours (mais c'est souvent le cas).
- Quelles sont les répercussions sur les victimes?
  - Les victimes peuvent ressentir : colère, tristesse, frustration, gêne, stress, peur, solitude, impuissance, inquiétude et dépression.
  - Selon la personne et les circonstances, les effets de l'anonymat, de l'absence d'un refuge, d'un flot constant de messages blessants et de la gêne due à un grand nombre de témoins peuvent être considérables.
  - Les victimes peuvent aussi intérioriser leurs blessures, ce qui peut les mener à penser à l'automutilation ou au suicide.

- Soyez proactif
  - Servez-vous de la technologie à votre avantage.
    - Empêchez certaines personnes de communiquer avec vous en ligne.
    - Changez de mots de passe, de noms d'utilisateur ou d'adresses courriel.
    - Supprimez les messages texte anonymes sans même les lire.
  - Délaissez la technologie.
    - Cette stratégie est irréaliste et inefficace à long terme.
      - La technologie est partout et fait partie intégrante de tous les aspects de notre vie.
      - Les communications électroniques sont le principal moyen de communication des adolescents; elles sont même parfois plus utilisées que les discussions en personne.
      - La technologie est un outil de socialisation et d'éducation important ainsi qu'une source de soutien des pairs.
      - Personne ne devrait être privé des avantages de la technologie à cause de l'intimidation.
  - Soyez au courant de ce que font vos enfants ou vos adolescents en ligne.
    - Un logiciel de surveillance et de filtrage de contenu peut s'avérer efficace pour les jeunes enfants, mais pourrait avoir l'effet inverse auprès des plus vieux.
      - Vous pouvez trouver des ressources adaptées à l'âge de votre enfant sur le site Web de PREVNet au www.prevnet.ca.
    - Parlez avec eux des technologies qu'ils utilisent pour mieux les comprendre ainsi que pour connaître les enjeux et les configurations liés à la protection de la vie privée.
    - Contribuez à l'utilisation de ces technologies. Par exemple, regardez des vidéos sur YouTube avec eux ou faites du clavardage vidéo avec les membres de la famille.
    - Ayez des discussions familiales sur le comportement à adopter en ligne, et faites savoir à vos enfants qu'ils n'ont pas à craindre de se confier s'ils se sentent harcelés.
  - Sachez que de nombreuses victimes n'osent pas faire part de leur situation à des adultes.
    - Les jeunes garçons et les victimes plus âgées se montrent d'ailleurs plus réfractaires à se confier. Lorsqu'ils le font, ce sera le plus souvent à un ami, un parent ou un tuteur. Certains en parlent aussi à un membre du personnel de leur école.

- Peu de victimes vont chercher de l'aide auprès des autres. Si elles le font, elles se tournent d'abord vers un ami, ensuite un parent et en dernier lieu un enseignant. Plus la victime vieillit, moins elle sera portée à en parler au personnel de l'école ou à un parent.

– Le Web regorge de bonnes ressources qui offrent des renseignements, des conseils et des outils spécifiques pour en apprendre sur la cyberintimidation et savoir comment y faire face.

- Le Web regorge de bonnes ressources qui offrent des renseignements, des conseils et des outils spécifiques pour en apprendre sur la cyberintimidation et savoir comment y faire face.
- Nous vous recommandons tout particulièrement le site Web de PREVNet (http://www.prevnet.ca/fr/intimidation/cyberintimidation), un réseau canadien qui offre d'excellentes ressources.
- http://www.thedoorthatsnotlocked.ca/app/fr/
- https://protectchildren.ca/app/fr/index
- http://habilomedias.ca/sur-droit-chemin-enseigner-enfants-comportement-%C3%A9thique-s%C3%A9curitaire-ligne-page-portail
- http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/bullres-resinti-fra.htm
- http://www.pensezcybersecurite.gc.ca/cnt/cbrbllng/index-fr.aspx
- http://www.pensezcybersecurite.gc.ca/cnt/cbrbllng/tns/index-fr.aspx
- http://jeunessejecoute.ca/Teens/InfoBooth/Bullying/Cyberbullying.aspx?lang=fr-ca
- http://www.spvm.qc.ca/fr/jeunesse/ado-Cyberintimidation.asp

1.3 En pratique

Prenez le harcèlement en ligne et la cyberintimidation au sérieux.

Soyez au courant de ce que font vos enfants sur Internet.

Allez chercher de l'aide si vous êtes inquiet pour une personne de votre entourage.

2 Présence de prédateurs sexuels sur le Web

2.1 En bref

L'exploitation sexuelle est un des dangers du Web, et les jeunes sont plus à risque d'en être victimes. En sachant ce que les jeunes font sur Internet et en contribuant de façon positive à leur utilisation du Web, on peut exercer une bonne influence.

2.2 En détail

- L'Internet offre un moyen facile aux prédateurs de communiquer avec les personnes vulnérables et d'en abuser. Ils peuvent donc viser les jeunes.
  - La victime peut se faire convaincre ou être contrainte :
    - d'envoyer ou de publier des photos sexuellement explicites d'elle;
    - de prendre part à des activités sexuelles par caméra Web ou sur un téléphone intelligent;
    - d'avoir des conversations à caractère sexuel par messagerie texte ou en ligne;
    - de rencontrer l'agresseur en personne.
  - Les conséquences de l'agression (p. ex., des images ou des vidéos) peuvent continuer de circuler sur Internet longtemps après ladite agression.
    - C'est exactement ce qui rend le harcèlement sexuel en ligne particulièrement nocif : les torts perdurent.
- Il n'y a pas qu'un facteur de risque qui mène aux agressions.
  - Il s'agit plutôt d'une combinaison complexe de facteurs de risque et de l'absence de facteurs de protection qui peuvent diminuer la capacité de résilience d'un jeune et le rendre vulnérable aux agressions.
  - Les adolescents sont plus susceptibles de se faire solliciter que les enfants ou les adultes.
    - C'est la nature humaine, les adolescents sont inexpérimentés, impulsifs, à la recherche de sensations et enclins à prendre des risques.
    - Ces caractéristiques, jumelées au désir d'explorer leurs pulsions sexuelles, les rendent particulièrement vulnérables sur le Web.
- Les prédateurs développent des relations avec les jeunes sur une période étendue et de différentes façons.
  - Ce processus peut prendre quelques secondes comme des années.
  - La manipulation peut se présenter sous différentes formes, mais la plupart du temps, les agresseurs utilisent les flatteries, posent des questions sur les parents et l'horaire du jeune et abordent rapidement le sujet de la sexualité.
    - L'agresseur peut séduire le jeune par des flatteries pour qu'il se sente spécial et pour exploiter son besoin naturel de se sentir aimé et important.
      - La victime n'aura pas nécessairement le sentiment de se faire abuser et se sentira en confiance.
    - À l'inverse, l'agresseur peut jouer la carte de l'intimidation et de la peur pour contrôler la victime, par exemple en faisant du chantage.

- Il peut la menacer d'envoyer des photos, des vidéos ou des copies de leurs conversations à ses amis ou à sa famille si elle refuse d'avoir des relations sexuelles.

- Ces moyens visent à désensibiliser la victime et à la préparer psychologiquement jusqu'à ce qu'elle soit plus encline à avoir une relation sexuelle.

- Un parent qui s'intéresse aux comportements de son enfant sur Internet et qui exerce une surveillance peut agir comme une protection contre ce type d'agression.
  - Les enfants dont les parents surveillent leur utilisation d'Internet ont moins d'expériences négatives sur le Web que les autres jeunes.
  - Un jeune qui sait que ses parents surveillent son utilisation d'Internet et y participent, et qui entretient une bonne relation avec eux et ses proches, est moins susceptible de devenir une victime du Web.

- Les réactions des victimes face aux agressions sont variées.
  - Elles peuvent tenter de faire face à la situation en tentant de l'oublier, en la niant ou en modifiant la réalité.
  - Elles peuvent tenter de trouver du réconfort auprès de leur cercle social, se plonger dans le travail, s'inquiéter, croire à la pensée magique, se blâmer, s'investir dans une activité physique ou tout garder pour eux.
  - Les jeunes ont besoin de soutien pour pouvoir parler de l'exploitation sexuelle qu'ils ont subie.
    - Les jeunes victimes d'agressions sexuelles graves et répétées ont tendance à se confier sur le tard, de façon hésitante et indirecte, ou sont honteuses et ont peur de la réaction de leurs parents.
      - Les jeunes qui croient que leurs parents auront une réaction négative tardent à en parler et ont plus tendance à se confier à quelqu'un d'autre.
      - Les enfants ont de la difficulté à parler de choses secrètes, troublantes et angoissantes, car les occasions d'aborder ce genre de sujets en famille sont peu fréquentes.
      - Ils sont aussi attentionnés aux besoins de leurs proches et ont peur des conséquences pour leur famille et leur agresseur.
    - Quand les jeunes victimes se confient, elles le font dans des situations où le thème de l'exploitation sexuelle est amené par quelqu'un d'autre.
      - Certaines d'entre elles sentent qu'il est difficile de trouver un moment suffisamment privé pour parler de ce qu'elles ont vécu.
      - Il leur devient plus facile de se confier lorsque le sujet est déjà abordé et que le moment est propice à la discussion.

- Pour dénoncer une agression sexuelle ou pour en savoir plus sur le sujet, rendez-vous à l'adresse https://www.cybertip.ca/app/fr/report.

- Plusieurs outils et ressources sont offerts à l'adresse https://www.protectchildren.ca/app/fr/index.

2.3 En pratique

Soyez au courant de ce que font vos enfants sur Internet.

Définissez ce qui est et ce qui n'est pas un comportement acceptable.

Soutenez vos enfants et offrez-leur un environnement propice à la confidence.

3 Fraude en ligne

3.1 En bref

Il y a de la fraude en ligne. Pour repérer les risques et ne pas se faire prendre, il est important de connaître les attrapes les plus courantes. Vous pourrez alors identifier une fraude en ligne, la signaler et l'enrayer.

3.2 En détail

- La facilité avec laquelle on peut communiquer sur Internet permet aux fraudeurs et aux escrocs d'atteindre un grand nombre de personnes facilement.

- Les fraudeurs se servent notamment d'appels téléphoniques, de faux sites Web, de courriels et de la messagerie en ligne pour tenter de convaincre les gens de leur fournir leurs renseignements personnels ou ceux d'autres personnes, ou encore de leur donner de l'argent.

- Il est important d'être à l'affût des fraudes, de prendre son temps et de se méfier des personnes suspectes.

- Certes, connaitre les principales arnaques peut vous aider à repérer les escrocs, mais il existe une tonne de façons de frauder.

  - Demandes d'argent

  - Fausses situations d'urgence

    - Les arnaqueurs se servent des médias sociaux, d'Internet et des journaux pour cibler les personnes âgées.

      - Une personne qui prétend être un membre de la famille ou un ami proche appelle à propos d'une situation d'urgence nécessitant l'envoi immédiat de fonds. Il est souvent question d'un membre de la famille qui a été arrêté ou qui a eu un accident pendant un voyage à l'étranger. Le fraudeur invoque des frais d'hospitalisation, d'avocat ou de cautionnement. Généralement, il demande à la victime potentielle de recourir à une entreprise de transfert de fonds (p. ex. Western Union, MoneyGram).

- Comment se protéger
  - Vérifiez où se trouve votre proche auprès de votre famille ou de vos amis.
  - Sachez que jamais un policier, un juge ou une entité juridique ne vous demandera de lui envoyer de l'argent par l'intermédiaire d'une entreprise de transfert de fonds.
  - Ne donnez jamais le nom ou les coordonnées d'un membre de votre famille à un appelant inconnu.
  - Méfiez-vous toujours des demandes d'argent urgentes.

- Arnaques amoureuses
  - Les arnaques amoureuses impliquent un criminel qui séduit sa victime au moyen de fausses intentions pour avoir accès à son argent.
  - Ce type de fraude a de graves répercussions sur la victime et entraine de très lourdes conséquences financières. En 2014 seulement, 13 millions de dollars ont été volés à des Canadiens de cette façon.
    - Les fraudeurs utilisent de fausses photos sur les sites de rencontre et les médias sociaux pour leurrer les victimes et leur subtiliser leur argent sous différents prétextes.
    - Ils sont prêts à entretenir des relations sur de longues périodes pour gagner la confiance de leurs victimes et pouvoir leur soutirer plus d'argent.
    - Le fraudeur gagne la confiance de sa victime en lui démontrant de l'affection; il peut même lui envoyer des cadeaux, des fleurs ou des preuves d'amour pour lui faire croire que ses sentiments sont sincères. Souvent, le fraudeur réside dans un autre pays que sa victime; à un moment de la relation, il lui fait croire qu'il veut la rencontrer, mais qu'il n'a pas l'argent nécessaire pour payer le voyage. Il demande alors à la victime de couvrir les frais. Parfois aussi, les fraudeurs simulent des situations d'urgence, comme la maladie d'un proche, ou demandent une aide financière à la victime pour différentes raisons.
  - Comment se protéger
    - Méfiez-vous des personnes qui prétendent résider au Canada ou aux États-Unis mais travailler à l'étranger.
    - Méfiez-vous des personnes qui se proclament amoureuses très rapidement.
    - Méfiez-vous si elles disent vouloir venir vous rencontrer, mais qu'une situation quelconque les en empêche.
    - Si vous êtes sur un site de rencontre, quittez le site. Le fraudeur vous demandera probablement de poursuivre les échanges par un système de messagerie instantanée ou par courriel.

- N'encaissez aucun chèque et n'envoyez jamais d'argent pour quelque raison que ce soit!

- Une entreprise entre soudainement en contact avec vous.
  - Faux services
    - ***Technicien Microsoft ou Windows***
      - L'arnaqueur se fait passer pour le représentant d'une entreprise bien connue, comme Microsoft, et prétend que l'ordinateur de la victime transmet des virus ou a été piraté et qu'il doit être nettoyé.
      - L'arnaqueur obtient ainsi un accès à l'ordinateur à distance et peut exécuter des programmes ou modifier des paramètres.
      - Il explique ensuite à la personne qu'elle doit payer des frais pour le service et lui demande un numéro de carte de crédit.
      - Dans certains cas, l'arnaqueur fait un virement à partir de l'ordinateur de la victime au moyen d'une entreprise de transfert de fonds comme Western Union ou MoneyGram.
      - La victime se retrouve alors à payer pour un service dont elle n'avait pas besoin puisque son ordinateur n'était pas infecté.
    - ***Faible taux d'intérêt***
      - L'arnaqueur offre à la victime une réduction du taux d'intérêt de sa carte ou de sa marge de crédit.
      - Il lui demande des renseignements personnels comme son numéro d'assurance sociale, le nom de jeune fille de sa mère, sa date de naissance, son numéro de carte de crédit et la date d'expiration de la carte.
    - ***Service d'entretien***
      - L'arnaqueur se fait passer pour le représentant d'un fournisseur de services d'électricité, d'eau ou de gaz de la région et fait croire qu'une facture est en souffrance et qu'un paiement est requis sur-le-champ sans quoi les services seront interrompus.
      - Il demande à ce que le paiement soit effectué par carte prépayée, comme celles de Green Dot. Ces cartes ne sont pas comme celles des comptes bancaires; elles ne requièrent aucune identification avec photo et sont difficiles à retracer.
    - Comment se protéger
      - De grandes entreprises comme Microsoft ne vous appelleront jamais.

- Les fournisseurs de services publics appellent parfois leur client, mais ils ne demanderont jamais un paiement par carte prépayée au téléphone. Les paiements en souffrance sont plutôt reportés à la facture suivante.

- Appelez le service à la clientèle du fournisseur au numéro inscrit sur votre facture. Vous aurez ainsi la certitude de parler à un vrai employé.

- Ne fournissez jamais de renseignements personnels par téléphone.

- Ne craignez pas de poser des questions.

- Si vous sentez qu'on vous force la main, n'hésitez pas à raccrocher.

- Vous gagnez un prix auquel vous ne vous attendiez pas.

  - Faux prix

    - L'arnaqueur prétend représenter Reader's Digest ou la loterie Set for life. La personne se fait annoncer qu'elle a gagné un prix et que pour le réclamer, elle doit fournir son numéro de carte de débit et sa date de naissance, et parfois même entrer son NIP sur le pavé numérique du téléphone.

    - Les arnaqueurs ciblent des gens qui n'utilisent pas les services bancaires en ligne et se servent de ces renseignements pour s'approprier leur compte et blanchir de l'argent et le produit d'autres arnaques par marketing de masse.

    - Pour pouvoir recevoir son prix, la victime doit d'abord acquitter des frais d'avance. Elle ne recevra jamais de prix.

  - Fausses vacances

    - La personne reçoit un appel lui annonçant qu'elle a gagné un voyage. Le nom d'une entreprise réelle est parfois nommé, comme Expedia, Air Miles, Air Canada ou WestJet. La personne au bout du fil dit à la victime qu'elle est un client privilégié et qu'elle mérite un crédit voyage ou un rabais si elle réserve son voyage sur-le-champ.

    - L'interlocuteur utilise des tactiques de vente sous pression pour convaincre la victime de donner son numéro de carte de crédit afin de payer des frais, par exemple les taxes.

    - Le voyage ou le vol s'avère être une supercherie.

    - Comment se protéger

      - Tout appel vous annonçant que vous avez gagné un concours auquel vous n'avez pas participé est faux. On ne peut participer à une loterie étrangère qu'en se rendant dans le pays en question et en achetant un billet en personne. On ne peut pas acheter un billet en votre nom.

      - Les entreprises de loterie ou de tirage connues (p. ex. Reader's Digest, Publishers Clearing House) ne demandent jamais au gagnant d'effectuer un paiement pour réclamer son prix.

- Tous frais demandés pour réclamer un prix ne seront jamais acquittés au moyen d'une entreprise de transfert de fonds comme Western Union ou MoneyGram, ou de cartes prépayées comme celles de Green Dot. Si un inconnu vous appelle pour vous annoncer que vous avez gagné un concours auquel vous n'avez pas participé, raccrochez.
- Si vous recevez un appel pour vous annoncer que vous avez gagné un voyage, mais que vous devez payer des frais par carte de crédit, raccrochez.
- Consulter les sites Web d'entreprises reconnues; elles publient habituellement des mises en garde concernant ce type de sollicitation.
- Ne fournissez jamais de renseignements personnels ou de numéro de carte de crédit par téléphone.
- Si ça semble trop beau pour être vrai… c'est sans doute le cas.

- Achat et vente en ligne
  - Achat en ligne
    - Chaque année, il y a des articles populaires en rupture de stock dans les magasins, que ce soit des consoles de jeu vidéo ou des jouets. Les arnaqueurs en profitent pour faire semblant de vendre ces produits sur des sites Web de leur création, dans les petites annonces ou sur des sites d'enchères. Le consommateur paie pour l'article convoité, sans jamais le recevoir.
    - Indices
      - L'article en question est vendu à un prix ridiculement bas.
      - Le prix est vraiment plus bas que ceux des autres articles semblables en vente.
      - La description du produit est très générique (donne l'impression d'être du copier-coller), par exemple le mot article est utilisé à la place du nom réel du produit.
      - La publicité ou la description comporte des fautes d'orthographe.
      - Il est seulement possible de communiquer avec le vendeur par courriel.
    - Comment se protéger
      - Vérifiez l'évaluation du vendeur de qui vous achetez. N'achetez pas d'un nouveau vendeur ou d'un vendeur qui a reçu des évaluations négatives.
      - Validez l'existence de l'entreprise; recherchez son adresse et son numéro de téléphone.
      - Achetez d'entreprises ou de personnes reconnues ou avec qui vous avez déjà fait affaire.

- Ne faites aucune transaction hors du site d'enchères.
- Lisez les modalités et assurez-vous de comprendre les modes de paiement, la politique de retour et la garantie du produit.
- Vérifiez la protection contre la fraude offerte pour le mode de paiement que vous utilisez. L'option la plus sécuritaire est souvent de payer par un service de paiement en ligne ou par carte de crédit.
- Si le prix demandé pour un article semble trop beau pour être vrai… c'est sans doute le cas.

- Vente en ligne
  - Vous devez savoir que si vous vendez un article en ligne, il se peut que vous receviez des offres d'achat malhonnêtes.
    - Habituellement, le vendeur reçoit une réponse d'un arnaqueur prétendant vouloir acheter l'article mis en vente. L'arnaqueur fera un ou plusieurs faux paiements au moyen d'une carte de crédit volée ou de faux chèques. Dans certains cas, la victime perd non seulement son article, mais aussi de l'argent à cause du remboursement d'un trop-perçu ou des frais d'expédition de l'article.
  - Indices
    - Les arnaqueurs n'essaient pas de négocier; ils pourraient même vous offrir de payer plus si vous retirez votre annonce sur-le-champ.
    - Les arnaqueurs font un paiement trop gros et vous demandent d'envoyer le remboursement à un agent d'expédition.
    - Ils ne demandent pas à voir le produit et n'hésitent pas avant d'acheter.
    - Ils utilisent le mot article plutôt que le nom réel du produit (propos très génériques qui donnent l'impression d'être du copier-coller).
    - Ils paient par chèque ou par transfert de fonds (PayPal, e-Transfer).
  - Comment se protéger
    - Demandez l'opinion d'une personne de confiance.
    - Faites des recherches sur l'acheteur.
    - Authentifiez le paiement avant d'envoyer l'article.
    - Si possible, faites l'échange en personne (endroit public, en présence d'autres personnes, de jour, etc.).
    - Ne communiquez pas seulement par courriel; demandez un numéro de téléphone (si l'acheteur ne veut pas vous en donner un, c'est mauvais signe).

- Prenez votre temps; ne précipitez pas la transaction.
- Ne vous sentez pas obligé de faire une transaction dont vous n'êtes pas certain.
- Faites confiance à votre instinct.

- Contrefaçons
  - Vous pourriez vous faire arnaquer en achetant en ligne sur des sites qui semblent authentiques, mais qui sont en fait des imitations de ceux d'entreprises connues.
    - Les contrefacteurs sont très habiles pour reproduire l'apparence des sites Web connus.
    - Les produits contrefaits sont de qualité nettement inférieure aux originaux et, dans de nombreux cas, peuvent être très dangereux. Par exemple, on a déjà trouvé des bactéries, des champignons et de la moisissure dans des vestes contrefaites.
  - Indices
    - Des articles semblables mais de marques différentes sont vendus sur un même site.
    - Le prix de l'article est extrêmement réduit (de 75 %, 80 % ou même 90 %).
    - Le site Web ou les hyperliens comportent des fautes d'orthographe.
    - Les coordonnées se résument à une adresse courriel.
    - Les communications sont génériques et semblent être du copier-coller, et la qualité de la langue est approximative.
    - L'adresse courriel provient d'un compte Gmail, Hotmail ou Yahoo (les fabricants ont habituellement leur propre domaine).
  - Comment se protéger
    - Faites des recherches avant d'acheter quoi que ce soit (politique de retour, évaluations du vendeur, etc.).
    - Appelez au numéro sans frais de l'entreprise; n'hésitez pas à poser des questions.
    - Payez au moyen de votre carte de crédit et vérifiez votre relevé.
    - Évitez de cliquer sur les fenêtres publicitaires et les liens annonçant de « super aubaines ».
    - Si ça semble trop beau pour être vrai… c'est sans doute le cas.

3.3 En pratique

Faites preuve d'esprit critique.

Méfiez-vous des demandes d'argent pressantes et des aubaines improbables.

Ne craignez pas de communiquer avec une entreprise pour faire des vérifications.

4 Obtenir de l'aide

4.1 En bref

Des organisations peuvent vous aider si vous croyez que vous ou un proche avez été victime de fraude. Si vous croyez être à risque, avez perdu une carte ou avez été victime d'hameçonnage, vous pouvez prendre certaines mesures, notamment en appelant votre institution financière et vos fournisseurs de services.

4.2 En détail

- Nous sommes tous continuellement confrontés à la fraude en ligne.
- Vous rendre compte que vous avez été victime d'une fraude est un bon début, mais vous pouvez aussi prendre certaines mesures.
- Personne n'est à l'abri d'une erreur; il n'y a donc aucune raison d'avoir honte.
- Il y a beaucoup de choses que vous pouvez faire pour amenuiser les conséquences.
- Modifiez vos mots de passe, vérifiez vos relevés de compte et faites des appels pour confirmer que tout est normal.
- Il est important de toujours signaler une fraude.
- Le Centre antifraude du Canada est résolu à vous aider à « identifier, signaler et enrayer la fraude ».
  - Si vous croyez que vous ou un proche êtes victime de fraude, communiquez avec le Centre antifraude du Canada, par téléphone au 1 888 495-8501, ou en ligne à l'adresse http://www.antifraudcentre.ca.
- Si vous soupçonnez une tentative de fraude en lien avec un compte bancaire ou une carte de crédit, communiquez sans tarder avec l'institution financière en question. Leurs coordonnées se trouvent habituellement sur leur site Web. En voici quelques-unes qui pourraient vous être utiles.
  - Banque de Montréal
    - Perte ou vol de la carte de débit BMO : 1 877 225-5266
    - Perte ou vol de la carte MasterCard BMO (Canada et États-Unis) : 1 800 361-3361
    - https://www.bmo.com/principal/contactez-nous

- Banque Laurentienne
    - 514 252-1846 ou 1 800 252-1846 (sans frais)
- Banque Nationale
    - 1 888 TelNat 1 (1 888 835-6281)
    - Région métropolitaine de Montréal : 514 281-3159
    - Canada et États-Unis : 1 800 361-0070 (sans frais)
    - Ailleurs dans le monde : 514 281-3159 (à frais virés)
- Mouvement des caisses Desjardins
    - Montréal et les environs : 514 397-8649
    - Canada et États-Unis : 1 866 335-0338
    - Autre pays : 514 397-4610 (à frais virés)
- RBC Banque Royale
    - 1 800 769-2511;
    - 1 800 769-2555 (services en ligne)
    - 1 800 769-2535 (Soutien aux clients des services bancaires en ligne RBC Express)
    - RBC Bank (Géorgie), Amérique du Nord : 1 800 769-2553
    - ATS : 1 800 661-1275
- Banque Scotia
    - 1 800 575-2424 : faites le 3, puis le 1 si vous êtes un client de la Banque Scotia et croyez avoir été victime d'une fraude en ligne.
- Servus Credit Union
    - 1 877 378 8728
- Tangerine
    - 1 888 723-3304
- TD
    - https://www.td.com/francais/confidentialite-et-securite/confidentialite-et-securite/signaler-une-fraude-en-ligne/reportfraud.jsp
        - TD Canada Trust : 1 866 222-3456
        - Placements directs TD : 1 800 465-5463
        - TD Assurance : 1 877 397-4187
        - Services bancaires par Internet aux entreprises : 1 800 668-7328

- Numéros de téléphone des émetteurs de cartes en cas d'urgence, de perte ou de vol :
    - ATB Financial : 1 800 661-2266
    - Banque Canadian Tire : 1 800 459-6415
    - Banque HSBC Canada : 1 866 406-4722
    - Banque Nationale du Canada : 1 888 622-2783
    - Banque Royale du Canada: 1 800 361-0152
    - Banque Walmart Canada : 1 888 925-6218
    - BMO Banque de Montréal : 1 800 361-3361
    - Bridgewater Bank : 1 866 398-4404
    - Capital One : 1 800 481-3239
    - CIBC : 1 800 663-4575
    - Citibank Canada : 1 800 305-7259
    - Compagnie de Fiducie Peoples : 1 866 452-1138
    - CUETS Financial : 1 800 567-8111
    - Direct Cash Bank : 1 888 466-4043
    - MBNA : 1 800 379-2744
    - Sears Canada : 1 800 288-9965
    - Services financiers le Choix du Président : 1 866 246-7262
    - TD : 1 888 347-3261
- American Express
    - Carte perdue ou volée
    - Toronto : 905 474-0870
    - Amérique du Nord : 1 800 668-2639
    - Ailleurs (à frais virés) : 905 474-0870
- Visa
    - Canada : 1 800 847-2911
    - http://www.visa.ca/fr/aboutcan/contacts/index.jsp

4.3 En pratique

Signalez les cas de fraude au Centre antifraude du Canada.

Communiquez avec votre institution financière si vous soupçonnez une fraude en lien avec votre compte bancaire ou votre carte de crédit.

Glossaire

Arnaque	Procédé malhonnête ou trompeur créé à des fins criminelles.
Arnaqueur	Personne qui commet des arnaques.
Caméra Web	Caméra vidéo capable de transmettre un signal vidéo par Internet.
Centre antifraude du Canada	Organisme central canadien recevant les plaintes de fraude en ligne.
Cyberintimidation	Méfait intentionnel et répété commis à partir d'ordinateurs, de téléphones cellulaires ou de tout autre appareil électronique.
Entreprise de transfert de fonds	Entreprise permettant d'envoyer de l'argent à une autre personne peu importe où elle est dans le monde.
e-Transfer	Méthode pour envoyer ou recevoir de l'argent en ligne par Interac.
Fenêtre publicitaire	Publicité s'ouvrant dans une nouvelle fenêtre du navigateur, souvent au premier plan.
NIP	Numéro d'identification personnel.
PayPal	Entreprise de transfert de fonds en ligne.
Téléphone intelligent	Téléphone fonctionnant comme un ordinateur et avec lequel il est possible de naviguer sur Internet et d'installer des applications.
YouTube	Site Web hébergeant du contenu vidéo (youtube.com).