# Concepts de sécurité

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

- Acquérir de nouvelles connaissances pour se défaire des mythes et des idées préconçues sur la sécurité.
- Comprendre la valeur des renseignements.
- Adopter un mode de pensée axé sur la sécurité.
- Connaître les comportements malveillants en ligne.

# Contexte et détail pour le formateur

## 1 Se protéger, ça vaut la peine

### 1.1 En bref

Tout le monde peut gérer sa sécurité sur Internet, il suffit d'adopter de saines habitudes.

### 1.2 En détail

- Certaines excuses répandues sont parfois utilisées afin de justifier l'absence d'efforts en sécurité informatique. Une discussion sur ces idées préconçues peut s'avérer pertinente.
- « Ce n'est pas à moi de m'occuper de ça. »
  - La sécurité, c'est l'affaire de tous.
    - À la maison, vous verrouillez la porte d'entrée; dans les endroits publics, vous surveillez vos biens de valeurs.
    - De la même façon, avec votre ordinateur, vous devez garder vos mots de passe confidentiels et vérifier que la sécurité est activée.
- « C'est pénible. »
  - Vaut mieux prévenir que guérir.
    - Au départ, les gens trouvaient que les ceintures de sécurité des voitures étaient gênantes; aujourd'hui, on n'y pense plus et elles permettent de sauver des vies.
    - Une fois que vous aurez pris l'habitude, ce sera un automatisme et vous vous éviterez bien des soucis à long terme.
- « C'est trop compliqué. »
  - Avec un peu de formation et quelques bons trucs, n'importe qui peut appliquer les principes de sécurité de base.
    - Prenez votre temps et posez des questions; s'il y a lieu, déléguez les tâches plus techniques à une personne-ressource de confiance.
  - Veiller à ce que ***quelqu'un*** s'occupe de la sécurité.
- « Je ne suis pas à risque. »
  - L'automatisation expose tout le monde au crime.
    - Les gens sont ciblés de façon arbitraire.
    - Cela n'a rien à voir avec ce qu'ils ont à perdre. Même les personnes moins fortunées peuvent se faire voler leur identité ou pirater leur ordinateur dans un dessein pernicieux.

- « Je vais me faire pirater de toute façon. »
  - Il est possible de réduire au minimum les risques liés à la sécurité, mais pas de les éliminer complètement.
  - Par contre, les bonnes habitudes et la vigilance peuvent aider à éviter qu'un petit problème prenne des proportions démesurées et en entraîne de plus gros.
  - Vous pouvez réduire au minimum les risques d'être touché par un problème et, advenant le cas où il en surviendrait un, vous pouvez en amenuiser les répercussions.

### 1.3 En pratique

Voyez la cybersécurité comme quelque chose que vous pouvez prendre en charge en y consacrant un peu de temps.

## 2 Vos renseignements et les ressources de votre ordinateur ont de la valeur

### 2.1 En bref

Vos renseignements, personnels ou autres, ont une valeur sur Internet : faitesles circuler prudemment. Votre connexion Internet et les ressources de votre ordinateur peuvent aussi profiter à certains.

### 2.2 En détail

- Les renseignements sont la monnaie d'échange d'Internet.
  - Les vôtres ont une valeur pour d'autres.
  - Les organisations et les personnes cherchant à s'enrichir veulent en savoir plus sur vous.
    - Elles pourraient dépasser les limites et violer votre vie privée.
    - D'autre part, vos renseignements (comme ceux de votre carte de crédit) pourraient être subtilisés par des criminels[1].
  - Soyez vigilant lorsque vous fournissez des renseignements.
    - Que ce soit dans des formulaires en ligne ou par téléphone.
    - Demandez-vous si le site Web ou votre interlocuteur en a réellement besoin.
    - Si vous avez un doute, pensez-y à deux fois avant de le faire, ou alors, donnez de faux renseignements. Il n'y a pas de règle qui vous oblige à remplir chaque formulaire avec précision sur le Web.
    - Lorsque vous entrez des renseignements sur une page Web, laissez les champs non obligatoires vides (les champs obligatoires sont habituellement identifiés au moyen d'un astérisque).

1 Exemple : <https://www.priv.gc.ca/cf-dc/incidents/2015/009_150710_f.asp>.

    - Si vous croyez qu'une personne ou une organisation n'a pas de besoin véritable ou justifié pour obtenir une information, vous n'êtes pas obligé de la leur fournir.
    - Les criminels pourraient tenter de vous soutirer des renseignements pour accéder à votre compte bancaire ou demander du crédit en votre nom.
  - Soyez vigilant aussi lorsque vous publiez des renseignements personnels sur les médias sociaux.
    - Publier de l'information sur votre date de naissance, votre adresse, les membres de votre famille ou vos animaux de compagnie, par exemple, pourrait donner des outils aux criminels.
    - Cette information peut leur offrir des indices au sujet de vos mots de passe ou celui de vos parents et amis. Elle peut aussi indiquer le contenu de votre domicile ou permettre de savoir quand vous serez absent.
- Les ressources de votre ordinateur – mémoire, capacité à calculer, connexion Internet – ont aussi une valeur pour les criminels.
  - Peut-être pensez-vous que votre ordinateur ne contient aucun renseignement intéressant. Eux ne sont pas de cet avis. Vous devez faire preuve de vigilance en matière de sécurité.
  - L'ordinateur lui-même pourrait être ce qu'ils recherchent. Ils pourraient l'utiliser pour attaquer d'autres ordinateurs ou pour masquer leur identité.

### 2.3 En pratique

Soyez vigilant lorsque vous fournissez des renseignements en ligne.

Prenez les précautions nécessaires pour protéger votre ordinateur.

## 3 Un mode de pensée axé sur la sécurité

### 3.1 En bref

Envisager la sécurité du point de vue d'un criminel peut vous aider à prendre les bonnes décisions concernant les risques et la sécurité.

### 3.2 En détail

- Les professionnels de la sécurité font souvent référence au mode de pensée axé sur la sécurité.
  - Il s'agit d'adopter un point de vue qui permet de voir les failles dans la sécurité. Plutôt que de penser à la facilité d'utilisation, ils pensent à la facilité de ***mauvaise*** utilisation. Ils procèdent ainsi pour trouver les brèches par lesquelles les criminels pourraient s'immiscer. Vous pouvez aussi utiliser cette méthode pour identifier les sources de risques. Par exemple :
    - Pratique > Ce mot de passe est-il facile à retenir?
      - Sécurité -> Ce mot de passe est-il facile à deviner?

- Pratique > Est-il facile d'ouvrir mon compte?
  - Sécurité -> Est-il facile pour quelqu'un d'autre d'ouvrir mon compte?
- Pratique > De quels renseignements dois-je disposer pour accéder à mon compte bancaire?
  - Sécurité -> De quels renseignements une autre personne doit-elle disposer pour accéder à mon compte bancaire?

- Ce point de vue peut vous aider à mieux comprendre les risques liés aux actions et à agir en conséquence.
  - Par exemple, si vous créez un compte qui ne contient aucune donnée personnelle, ne perdez pas de temps à maximiser la sécurité. Si quelqu'un y accède, il ne pourrait pas causer beaucoup de dommages.
  - Par contre, dans le cas d'un compte bancaire, les dommages pourraient être considérables. Vous devez donc porter une plus grande attention à la sécurité.
- La prudence se situe à mi-chemin entre pratique et sécurité.
  - Parfois, l'option la plus facile est la meilleure (faible risque).
  - D'autres fois, l'option la plus difficile est la meilleure (haut risque).
  - Il est irréaliste de croire que l'on peut prendre les mesures les plus sécuritaires en tout temps. On peut toutefois y être sensibilisé et faire des choix éclairés sur le niveau de sécurité nécessaire pour chaque situation.

### 3.3 En pratique

Pensez à la sécurité avant de choisir l'option la plus facile.

## 4 Les risques en ligne

### 4.1 En bref

Les cybercriminels tentent de piéger les gens pour leur soutirer de l'argent ou des renseignements personnels, ou utilisent des programmes malveillants pour le faire de façon automatisée. Les services de sécurité (détecteur de programme malveillant, pare-feu), le chiffrement et un esprit critique peuvent aider à se protéger de ces attaques.

### 4.2 En détail

- Les cybercrimes se divisent en deux catégories : visant les personnes (en les piégeant ou en leur faisant du mal directement) ou visant les ordinateurs (vol de ressources ou de renseignements).
  - Contre une personne
    - Les communications et les publications sur Internet peuvent servir à léser, à frauder ou à voler une personne.

        - Le tout se fait à distance de partout dans le monde sans même devoir rencontrer la personne, ce qui facilite la tâche aux criminels.

    - Soyez méfiant lorsque vous faites des affaires sur Internet; l'informatique facilite l'usurpation et la fabrication de faux documents et de fausses photos.
    - Soyez toujours vigilant, les criminels peuvent se servir de tous les renseignements que vous publiez sur la toile pour voler votre identité.
    - Hameçonnage : Activité qui consiste à leurrer une personne pour y soutirer des renseignements.
        - Vous pourriez vous faire duper en visitant un faux site Web qui ressemble à un autre auquel vous avez confiance (comme celui d'une banque).

- Contre un ordinateur
    - Les criminels peuvent voler (copier sans autorisation) des données personnelles à partir de votre ordinateur ou les voler à un tiers. Ils peuvent aussi manipuler ces données pour vous frauder.
    - Les renseignements peuvent être volés lorsqu'ils sont stockés sur un ordinateur ou qu'ils circulent sur Internet.
    - La plupart des vols se font par l'entremise de programmes automatisés implantés ou créés par les criminels eux-mêmes.
    - Programme malveillant : ces activités illicites sont automatisées au moyen de ce qu'on appelle des programmes malveillants.
        - Ces programmes peuvent servir à :
            - voler des renseignements sur un ordinateur (p. ex. copier des fichiers, enregistrer l'historique d'utilisation d'Internet ou ce que l'utilisateur écrit);
            - manipuler les données d'un ordinateur (p. ex. verrouiller l'ordinateur et demander une rançon);
            - manipuler les renseignements envoyés (p. ex. envoyer un courriel au nom de quelqu'un);
            - manipuler les renseignements reçus (p. ex. modifier les résultats d'une recherche).
        - Dès que les renseignements se trouvent sur Internet, ils passent par d'autres ordinateurs qui, eux, peuvent comporter des programmes malveillants pour copier ou manipuler lesdits renseignements.
        - Certains programmes malveillants peuvent se servir de votre ordinateur pour en attaquer d'autres ou pour attaquer des sites Web. Le contrôle de plusieurs ordinateurs permet aux cybercriminels d'automatiser un plus grand nombre de processus et de se distancer davantage des activités criminelles.

        - Les ordinateurs piratés fonctionnant à l'insu de leurs propriétaires sont appelés zombies.
        - Le rassemblement de plusieurs ordinateurs de ce type est appelé réseau de zombies.
    - Les logiciels de sécurité peuvent aider à protéger un ordinateur, mais ne sont pas une protection absolue.
        - Ils peuvent détecter les programmes malveillants.
        - Un pare-feu peut aider à bloquer les programmes malveillants.
        - Le chiffrement peut empêcher un programme malveillant de lire ou de manipuler les communications.
            - Par exemple, dans un navigateur, le « s » dans les adresses commençant par « https*://* » indique que la connexion est chiffrée.
    - La meilleure protection contre la fraude est la méfiance et l'information. Si vous croyez avoir été leurré, arrêtez tout et parlez-en à une personne de confiance.

### 4.3 En pratique

Soyez à l'affût des criminels.

Gardez votre service de sécurité à jour et utilisez des services chiffrés pour le traitement de renseignements confidentiels.

## 5 Bonnes habitudes

### 5.1 En bref

Sans trop d'efforts, vous pouvez grandement réduire les risques. Puis, si vous éprouvez des problèmes, vous pouvez toujours demander de l'aide.

### 5.2 En détail

- Dans le monde réel, les discussions sur la santé et la sécurité sont chose commune. Nous prenons soin de notre santé et évitons d'être victimes d'un crime en prenant les précautions nécessaires selon le contexte.
    - Nous nous faisons vacciner avant de voyager à l'étranger, mais pas pour se rendre chez un ami.
    - Rien ne nous garantit d'être protégé à cent pour cent, mais ça aide.
- De la même façon, nous devons protéger notre ordinateur avant d'aller sur Internet en le configurant correctement, en appliquant les correctifs nécessaires et en gardant le logiciel de sécurité à jour et fonctionnel.

- Prenez les bonnes habitudes :
    - Pensez avant de cliquer;
    - Recherchez les indicateurs de sécurité;
    - Soyez méfiant dans vos transactions en ligne.
- Vous pouvez demander de l'aide à des amis ou à des personnes-ressources comme votre fournisseur de services financiers ou de services de sécurité, les autorités gouvernementales ou encore les services de police.

### 5.3 En pratique

Voyez la cybersécurité comme de saines habitudes qui peuvent vous aider à réduire les risques.

## Glossaire

| | |
|---|---|
| **Chiffrement** | Processus de conversion de l'information en format illisible par les entités non sécurisées, mais lisible par le destinataire désigné. |
| **Média social** | Technologie du Web conçue pour l'interaction sociale et le partage de contenu, par exemple Facebook et Twitter. |
| **Mode de pensée axé sur la sécurité** | Façon d'envisager les ordinateurs d'un point de vue axé sur les failles de sécurité. |
| **Pare-feu** | Barrière de sécurité entre des réseaux ou entre un ordinateur et un réseau. |
| **Programme malveillant** | Logiciel créé dans un mauvais dessein. |
| **Réseau de zombies** | Regroupement d'ordinateurs contrôlés à distance. |
| **Zombie** | Ordinateur infecté par un programme malveillant et contrôlé à distance; fait partie d'un réseau de zombies. |