

# Concepts de sécurité



## AIDE-MÉMOIRE

### 1. Se protéger, ça vaut la peine

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

- 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

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

- 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

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

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

### 4. Les risques en ligne

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.

- 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

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

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

## Glossaire

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