

Ressource pour le programme d'études

Cybersécurité : partie 1

Alignement avec le CLAO

Compétence	Groupe de tâches	Niveau
Compétence D – Utiliser la technologie numérique	s. o.	1
Choisir un élément.	s. o.	1
Choisir un élément.	Choisir un élément.	Choisir un élément.
Choisir un élément.	Choisir un élément.	Choisir un élément.
Choisir un élément.	Choisir un élément.	Choisir un élément.

Voies de transition (cochez toutes les cases qui s'appliquent)

- | | |
|---|---|
| <input checked="" type="checkbox"/> Emploi | <input type="checkbox"/> Études postsecondaires |
| <input type="checkbox"/> Formation en apprentissage | <input checked="" type="checkbox"/> Autonomie |
| <input type="checkbox"/> Études secondaires | |

Compétences pour réussir intégrées (cochez toutes les cases qui s'appliquent)

- | | |
|--|--|
| <input type="checkbox"/> Adaptabilité | <input type="checkbox"/> Calcul |
| <input type="checkbox"/> Collaboration | <input checked="" type="checkbox"/> Résolution de problème |
| <input type="checkbox"/> Communication | <input checked="" type="checkbox"/> Lecture |
| <input type="checkbox"/> Créativité et innovation | <input type="checkbox"/> Rédaction |
| <input checked="" type="checkbox"/> Compétences numériques | |

Notes : Les ressources *Cybersécurité : partie 1* et *Cybersécurité : partie 2* portent sur des questions plus élémentaires et plus complexes en matière de cybersécurité et visent respectivement les niveaux de compétence 1 et 2.

Cybersécurité : partie 1

Qu'est-ce que la cybersécurité?

Les ordinateurs et les téléphones intelligents sont utiles dans la société moderne, et ils peuvent être très divertissants. Toutefois, leur utilisation comporte des risques. La cybersécurité consiste à gérer ces risques.

La cybersécurité consiste à se protéger contre les risques liés à l'utilisation d'un ordinateur ou d'un téléphone intelligent.



Objectifs de cette ressource

Cette ressource présente une introduction aux éléments ci-après :



- ✓ la **protection de vos mots de passe** afin d'éviter qu'ils soient oubliés ou volés;
- ✓ la gestion de vos **renseignements** et de votre **présence** en ligne;
- ✓ le repérage des sites Web et des liens douteux afin d'éviter les **virus** et les **pourriels**;
- ✓ des **conseils** et des **astuces** pratiques en matière de cybersécurité;

En plus de :

- ✓ *quelques activités pratiques pour vous assurer que vous êtes sur la bonne voie.*

Table des matières

<i>Qu'est-ce que la cybersécurité?</i>	1
<i>Objectifs de cette ressource</i>	1
<i>1. Introduction : à quoi sert la cybersécurité?</i>	3
Quels sont les risques?.....	3
<i>2. Mots de passe</i>	4
Quels sont les risques?.....	4
Que pouvez-vous faire?	5
Conseils pour la création de mots de passe robustes	5
Activité 1.....	6
<i>3. Protégez votre vie privée et vos renseignements personnels</i>	8
Quels sont les risques?.....	8
Que pouvez-vous faire?	9
Protégez votre vie privée sur votre téléphone intelligent :.....	9
Protégez votre vie privée sur Facebook :	10
<i>4. Sauvegardez vos données</i>	12
Quels sont les risques?.....	12
Que pouvez-vous faire?	12
<i>5. Pourriels et virus</i>	13
Qu'est-ce qu'un pourriel ?	13
Qu'est-ce qu'un virus?	14
Que pouvez-vous faire?	14
Activité 2.....	18
<i>6. Gérez votre présence en ligne</i>	19
Que pouvez-vous faire?	19
<i>7. Survol</i>	20

1. Introduction : à quoi sert la cybersécurité?

Il n'y a pas lieu d'avoir peur d'utiliser un ordinateur, un téléphone intelligent ou Internet. Il convient toutefois de faire preuve de **vigilance** et de **prudence** afin d'éviter les risques réels.

Quels sont les risques?

- Si vous **oubliez** ou **perdez** vos mots de passe, l'**accès** à votre téléphone intelligent et à des sites Web importants, comme votre institution bancaire, risque d'être **bloqué**.



- Si vous ne vous souciez pas de votre **vie privée**, des entreprises peuvent **repérer** vos renseignements et votre emplacement.



- Si vous ne **sauvegardez** pas vos données, vous risquez de perdre des éléments importants comme des photos et des vidéos.



- Si vous ne vous **souciez** pas des renseignements que vous publiez en ligne, cela pourrait avoir des conséquences négatives sur vos relations ou vos possibilités d'emploi.



- Si vous cliquez sur des **liens douteux** ou visitez des **sites Web à risque**, vous pourriez vous exposer à un **virus** informatique ou même vous faire voler vos renseignements.



2. Mots de passe

De nos jours, nous devons souvent avoir **plusieurs** mots de passe. Des mots de passe pour les téléphones intelligents, les courriels, les services bancaires en ligne, etc. C'est pourquoi il est **si important d'assurer la sécurité de vos mots de passe**.

Voici ce que vous devez savoir :



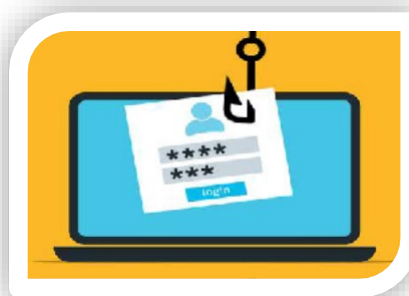
Quels sont les risques?

a. Si vous **oubliez** ou **perdez** votre mot de passe, vous pourriez :

- ne plus avoir accès à votre ordinateur ou à votre téléphone;
- ne plus avoir accès à votre adresse de messagerie électronique;
- ne plus avoir accès à vos services bancaires en ligne;
- ne plus avoir accès à d'autres applications importantes.

b. Mais pire encore, si une personne **devine** ou **découvre** votre mot de passe, elle peut :

- accéder à vos renseignements;
- fouiner dans votre adresse de messagerie;
- voler de l'argent dans votre compte bancaire;
- voler vos renseignements et votre identité.



Que pouvez-vous faire?

Il existe trois étapes clés pour protéger vos mots de passe :

- a. créez des mots de passe ROBUTES;
- b. conservez-les par écrit dans un endroit sûr auquel vous seul avez accès;
- c. ne révélez à PERSONNE vos mots de passe;
- d. n'utilisez pas le même mot de passe pour toutes les applications.



La première étape est la plus difficile : ***comment créer un mot de passe robuste?***

Conseils pour la création de mots de passe robustes

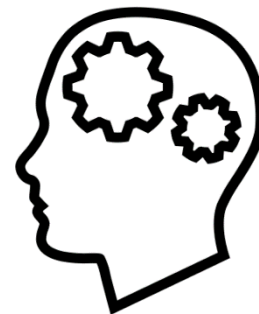
*Un mot de passe robuste est **facile à retenir pour vous**, mais **difficile à deviner pour les autres**.*

- **N'UTILISEZ PAS** votre nom, votre date de naissance ou d'autres renseignements personnels comme votre adresse ou le nom de votre chien.
- **N'UTILISEZ PAS** le même mot de passe plusieurs fois pour des applications différentes.
- **UTILISEZ** un mot de passe long d'au moins huit caractères. Les caractères sont des lettres, des chiffres et des symboles.
- **UTILISEZ** des chiffres et des symboles, ainsi que des lettres majuscules et minuscules.

Activité 1

Voici trois mots de passe différents :

- Encerclez les mots « **robuste** » ou « **faible**. »
- Expliquez pourquoi et comment chaque mot de passe pourrait être amélioré.



Mot de passe 1 :

Steve choisit un mot de passe pour une nouvelle adresse de messagerie. Il choisit l'adresse de son domicile, pensant qu'elle sera facile à retenir. Il écrit donc : **ruemaple22**.

Ce mot de passe est-il :

ROBUSTE ou **FAIBLE**

Expliquez pourquoi et comment il pourra être meilleur :

Mot de passe 2 :

Anna choisit un mot de passe pour un nouveau compte bancaire. Elle choisit le nom de ses enfants et leur âge. Elle écrit donc : **max10amber6**.

Ce mot de passe est-il :

ROBUSTE ou **FAIBLE**

Expliquez pourquoi et comment il pourra être meilleur :



Mot de passe 3 :

Steve choisit un mot de passe pour un nouveau compte Google. Il choisit son aliment préféré, avec un numéro facile à retenir. Il écrit donc : **banane123**.

Ce mot de passe est-il :

ROBUSTE ou **FAIBLE**

Expliquez pourquoi et comment il pourra être meilleur :

**Mot de passe 4 :**

Anna choisit un code d'accès pour son nouveau téléphone intelligent. Elle choisit l'année de sa naissance, en pensant qu'il sera facile de s'en souvenir. Il écrit donc : **1985**.

Ce mot de passe est-il :

ROBUSTE ou **FAIBLE**

Expliquez pourquoi et comment il pourra être meilleur :

3. Protégez votre vie privée et vos renseignements personnels

Nous ne divulguons pas nos renseignements personnels à des inconnus dans la rue, mais nous publions **beaucoup** d'information à notre sujet en ligne. Il est donc **très important de protéger vos renseignements personnels**.

Voici ce que vous devez savoir :

Quels sont les risques?

a. *Si vous ne protégez pas votre vie privée, il est possible pour des entreprises ou des individus de :*

- **prendre** vos renseignements personnels, comme vos photos, et les utiliser;
- **prendre** vos renseignements personnels pour essayer de vous vendre quelque chose;
- **suivre** votre position.



b. *Mais pire encore, des personnes mal intentionnées peuvent :*



- ✓ **voler** vos renseignements;
- ✓ **voler** de l'argent dans votre compte bancaire;
- ✓ **voler** votre identité.


Que pouvez-vous faire?

La première chose à faire est de vous **DÉCONNECTER** et de **vérifier vos paramètres de confidentialité** chaque fois que vous utilisez un nouvel appareil ou un nouveau compte de médias sociaux. Habituellement, vous accédez aux paramètres en cliquant sur l'**icône de votre profil** dans le coin supérieur droit, puis en cliquant sur **Paramètres et confidentialité**.

Voici quelques exemples :


Protégez votre vie privée sur votre téléphone intelligent :

Protégez vos photos :

- Cliquez sur **Réglages**  et défilez vers le bas jusqu'à **Confidentialité et sécurité**.
- Cliquez sur **Confidentialité** puis sur **Photos**.
- Vous verrez la liste des applications souhaitant accéder à vos photos.
- Cliquez sur les applications auxquelles vous souhaitez retirer l'accès, puis sélectionnez **Aucune**.



Protégez votre position :

- Cliquez sur **Réglages**  et défilez vers le bas jusqu'à **Confidentialité et sécurité**.
- Cliquez sur **Confidentialité** puis sur **Service de localisation**.
- Vous pouvez désactiver cette fonctionnalité pour **empêcher le suivi de votre position**, mais dans ce cas, des applications comme **Cartes** et **Localiser** ne fonctionneront pas tant que vous ne l'aurez pas réactivée.
- Plutôt, défilez les applications auxquelles vous ne voulez pas avoir accès et appuyer sur **Jamais**.

Protégez votre vie privée sur Facebook :**a. Contrôlez vos Réglages de confidentialité.**

- Cliquez sur le petit cercle avec votre photo de profil dans le coin supérieur droit.
- Cliquez sur **Paramètres et confidentialité**.
- Cliquez à nouveau sur **Paramètres**.
- Cliquez à nouveau sur **Confidentialité** à gauche.

Une fenêtre s’ouvrira afin de vous permettre de gérer l’accès à **votre compte**. Vous saurez qui peut voir vos futures publications :

Votre activité	Qui peut voir vos futures publications ?	Ami(e)s
----------------	--	---------

Vous pouvez modifier ces paramètres afin de vous sentir plus en sécurité.



b. Empêchez les applications malveillantes d'accéder à vos renseignements personnels afin de prévenir que **personne ne les vole**.

- Trouvez la flèche dans le coin supérieur droit et cliquez dessus.
- Cliquez sur **Paramètres et confidentialité** dans le menu.
- Cliquez à nouveau sur **Paramètres**.
- Défilez vers le bas jusqu'à **Applications et sites Web**.

Applications et sites Web

Il s'agit des applications et des sites web que vous avez associés à votre compte Facebook soit en vous y connectant avec Facebook, soit en associant un de leurs comptes à votre profil Facebook. Vous pouvez examiner et gérer les informations non publiques auxquelles chaque application a l'autorisation d'accéder, ou supprimer ces accès.

Informations auxquelles une application peut accéder

Public	Certaines informations à votre sujet font partie de votre public profile ou ont été rendues publiques par une action de votre part. Une application peut accéder à ces informations publiques à tout moment.
Non public	Les autres informations ne sont pas publiques. Une application ne peut y accéder via cette connexion que si vous choisissez de les partager lorsque vous vous connectez à l'aide de votre compte Facebook. S'il apparaît que vous ne vous êtes pas connecté à une application à l'aide de votre compte Facebook au cours des 90 derniers jours, l'accès de l'application à vos informations non publiques via cette connexion expire automatiquement. Lorsque cette situation se produit, l'application passe du statut « Active » à « Expired ». Veuillez noter que, même si une application n'a plus accès à vos informations non publiques, elle peut toujours posséder les informations non publiques que vous avez partagées précédemment lorsqu'elle était Active. En savoir plus



iPiccy Photo Editor
Ajoutée le 5 avr 2022 • **Active**

[Voir et modifier](#)
[Supprimer](#)



Adobe
Ajoutée le 17 jan 2022 • **Expirée**

[Voir et modifier](#)
[Supprimer](#)

Consultez cette page pour supprimer les applications qui ne devraient pas être autorisées à accéder à vos renseignements.

c. Choisissez bien vos amis ou vos amies!

Malheureusement, **toutes les personnes** qui vous envoient une demande d'amitié ne sont pas dignes de votre confiance.

- N'acceptez que les demandes d'amitié des personnes que vous connaissez réellement.
- NE COMMUNIQUEZ JAMAIS vos renseignements personnels à des personnes que vous ne connaissez pas.
- NE COMMUNIQUEZ JAMAIS vos renseignements personnels à partir d'un ordinateur.



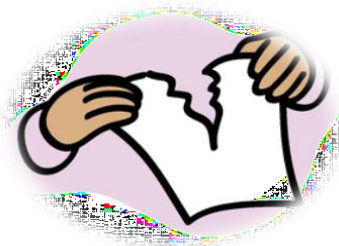
4. Sauvegardez vos données

Autrefois, nous conservions nos photos et nos lettres importantes dans des **boîtes à chaussures**, mais aujourd'hui, beaucoup de choses qui comptent pour nous sont enregistrées en ligne. C'est pourquoi il est ***si important de veiller à ne pas perdre nos données les plus précieuses.***

Voici ce que vous devez savoir :

Quels sont les risques?

- a. La perte de **photos**, de **vidéos**, de **lettres**, de documents professionnels (comme des **CV**) et d'autres **souvenirs de valeur**.



Que pouvez-vous faire?

Sauvegardez vos données sur un ordinateur

Si vous utilisez un ordinateur, sauvegardez toujours vos documents sur une clé **USB**. Celle-ci peut être branchée sur **n'importe quel ordinateur** et achetée dans un commerce de proximité à un **prix relativement abordable**.

À partir de **MS Word** ou de **Google Docs** :

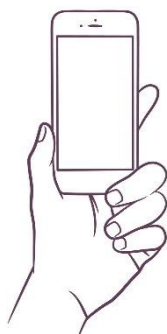
- cliquez sur Fichier;
- cliquez sur Enregistrer sous;
- cliquez sur Ce PC;
- le nom de la clé USB devrait apparaître à gauche parmi les options;
- cliquez dessus, puis enregistrez votre document.



Sauvegardez vos données sur votre iPhone

Il est important de **sauvegarder** toutes les données enregistrées sur votre iPhone, **en particulier vos photos et vos vidéos**. Pour vous assurer que vous effectuez une sauvegarde :

- Cliquez sur **Réglages**  puis tapez sur votre **nom**.
- Tapez sur **iCloud**, puis sur **Stockage iCloud**.
- Activez** la fonctionnalité.



Cela vous permettra d'accéder à vos données au moyen d'iCloud depuis Internet.

5. Pourriels et virus

La plupart des sites Web que nous visitons et des courriels que nous recevons sont surs, mais certaines personnes mal intentionnées ont créé des sites Web ou des liens qui peuvent nuire à votre ordinateur ou votre téléphone intelligent. C'est pourquoi il est **si important d'éviter les pourriels et les virus et de savoir quoi faire si vous n'y parvenez pas**.

Voici ce que vous devez savoir :

Qu'est-ce qu'un pourriel ?

- On appelle « pourriel » tout type de **courriel ou de texte ennuyeux et non désiré que l'on vous envoie**.



Parfois, il s'agit simplement de publicités, mais il arrive aussi qu'elles contiennent un virus.

Qu'est-ce qu'un virus?

- Un virus est un type de « code » informatique qui peut **endommager votre ordinateur ou votre téléphone**.
- Il peut également être utilisé pour **voler** vos renseignements personnels.

Comment obtient-on des pourriels ou des virus?

La manière la plus courante d'obtenir des pourriels ou des virus est la suivante :

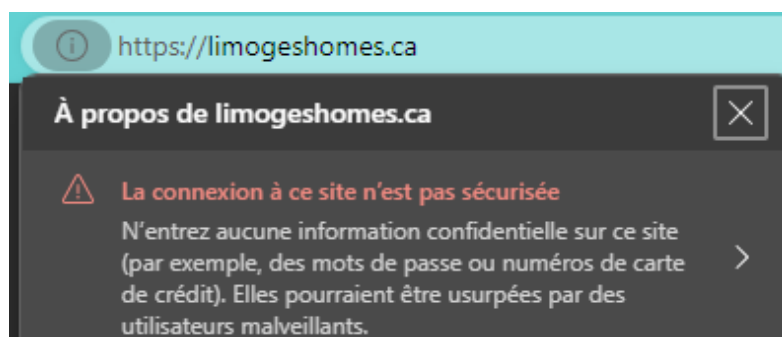
- en consultant des **sites Web peu fiables**;
- ou :
- en cliquant sur des **liens peu fiables**.

Que pouvez-vous faire?

Sites Web peu fiables

La première chose est de reconnaître les sites Web qui sont dignes de confiance.

- Les sites Web les plus populaires, comme YouTube, Facebook et Amazon, sont **très sûrs** et vous n'avez pas à vous inquiéter.
- Mais vous devez être prudent lorsque vous consultez des sites Web qui vous sont moins familiers.
- Si vous visitez un site Web et que vous voyez l'avertissement « **Non sécurisé**, », vous devriez quitter la page immédiatement.

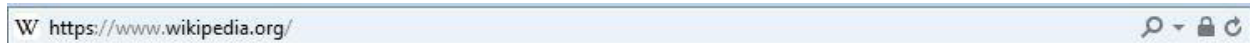


Vous pouvez savoir que le site Web sur lequel vous vous trouvez est sécurisé de deux manières différentes :

a. Le cadenas

Observez le cadenas **verrouillé** sur les trois principaux navigateurs :

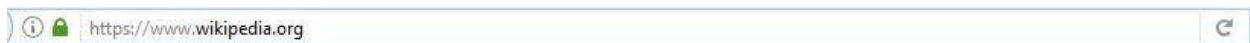
GOOGLE CHROME



INTERNET EXPLORER

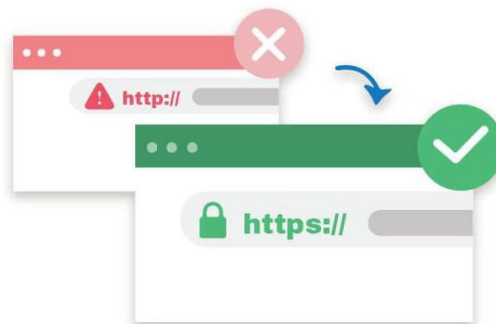


MOZILLA FIREFOX



b. La lettre « s » :

L'hyperlien des sites Web sécurisés commence par <https://>, mais celui des sites Web non sécurisés ne contient pas lettre « s » qui signifie **SÉCURISÉ**.



Liens peu fiables

La deuxième chose est de reconnaître les liens qu'il ne faut pas ouvrir.

Les **liens** sont des éléments d'un courriel, d'un message texte ou d'un site Web sur lesquels vous pouvez **cliquer** pour obtenir un résultat.

- Vous pouvez détecter un lien en recherchant des mots **soulignés** ou **écrits en bleu**.
- Lorsque vous défilez un lien, votre pointeur passe **de la flèche à la main**.
- Lorsque vous cliquez sur un lien, une nouvelle **fenêtre** ou **page Web** s'ouvre.

Sécurisé ou non sécurisé?



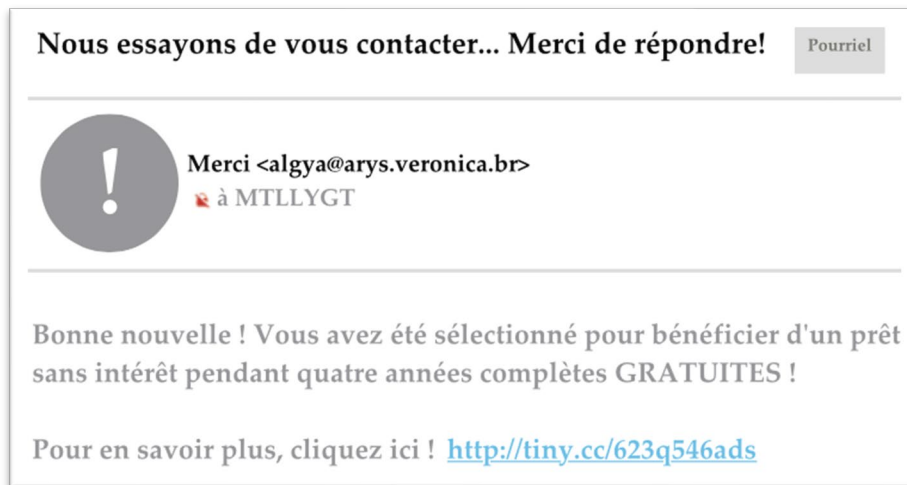
- Les liens figurant sur des sites Web sécurisés sont **surs**.
- Les liens contenus dans les courriels ou les textes qui vous sont envoyés directement par des amis ou des amies ou des employeurs ou employeuses de confiance **devraient être surs**.
- Les liens figurant dans des courriels provenant d'adresses électroniques que vous ne connaissez pas **peuvent être dangereux** :





Si vous cliquez sur ce lien, votre ordinateur sera probablement infecté par un virus!

IMPORTANT : En cas de doute, n'ouvrez JAMAIS de liens douteux!

Cherchons des indices sur les virus en examinant un autre courriel :



De nombreux indices montrent que le lien figurant dans le courriel n'est pas sûr.

- Gmail a signalé qu'il pouvait s'agir d'un **pourriel** dans le coin supérieur droit.
- Gmail a joint un **panneau d'arrêt** en guise d'avertissement supplémentaire : 
- Gmail a également fourni un symbole de cadenas **non verrouillé** : 
- L'**adresse électronique** de l'expéditeur est inconnue et étrange.
- Le **lien** (souligné en bleu) est inconnu et étrange.
- Le courriel est très insistant et vise à vous faire **presser le pas!**
- Dans le courriel, on vous promet de GRANDES CHOSES de sorte que vous ne vous arrêtiez pas pour réfléchir.

Activité 2

Encerclez autant d'indices que vous le pouvez afin de démontrer que ce lien **n'est pas sûr** :

NOTIFICATION DU PAIEMENT FINAL Pourriel

 MR. JEAN RACINE <info.jracine@adb.org>
 à ▼

À L'ATTENTION DU BÉNÉFICIAIRE,

Je souhaite humblement vous informer que le département de crédit et de contrôle télex de la Banque Africaine de Développement (A.D.B.) a reçu une instruction à l'effet de vous transférer immédiatement votre fonds approuvé de CAD 10,850,000.00 MILLIONS.

Je vous demande donc de reconfirmer de toute urgence le numéro de compte HSBC tel qu'il est indiqué ci-dessous ([cliquez ici](#) pour confirmer maintenant) pour ce compte a été soumis par votre avocat Barrister Godson Gabriel de (GODSON & CO. LAW CHAMBERS) pour le paiement.

6. Gérez votre présence en ligne

Dans la vie réelle, nous n'agissons pas de manière **inappropriée** au travail ou ne disons pas de grossièretés à nos proches, mais nos employeurs et employeuses et notre famille peuvent être exposés à des propos inappropriés que nous publions en ligne. C'est pourquoi il est **si important de maintenir une présence en ligne solide et respectueuse**.

Voici ce que vous devez savoir : **Quels sont les risques?**

Si vous publiez des messages ou des photos inappropriés en ligne, vous risquez de :

- nuire à vos relations avec vos amis ou vos amies et votre famille;
- perdre votre emploi;
- avoir du mal à trouver un nouvel emploi.

Que pouvez-vous faire?

La meilleure manière de conserver une présence en ligne solide et respectueuse est de :

- se souvenir que votre profil et vos publications pourraient être **vus** par de nombreuses personnes, y compris vos **enfants**, vos **grands-parents** et les employeurs.
- Alors, **PENSE** avant de publier un message en ligne.

PENSE AVANT DE PUBLIER!

P – Est-ce positif?

E – Est-ce exact?

N – Est-ce nécessaire?

S – Est-ce sage?

E – Est-ce enrichissant?

*Assurez-vous que votre **contenu est de bon goût** afin que tous puissent l'apprécier et qu'il ne vous cause pas d'ennuis!*

7. Survol

*Vous connaissez maintenant les **risques** que comporte l'utilisation d'un ordinateur, d'un téléphone intelligent ou des médias sociaux.*

- Vous avez appris à protéger vos mots de passe et vos renseignements personnels.
- Vous avez appris à **éviter** les pourriels et les virus.
- Vous avez également appris à **gérer** votre présence en ligne.
- Vous pouvez vous référer à ce guide à tout moment pour revoir les renseignements sur la cybersécurité et les moyens de se protéger en ligne.



Ce projet Emploi Ontario est financé en partie par le gouvernement du Canada et le gouvernement de l'Ontario.

Les opinions exprimées à même cette ressource représentent celles de Community Literacy of Ontario et ne sont pas forcément celles de nos bailleurs de fonds.