



## PARLONS DE CYBER SÉCURITÉ

- Étrangers et bonbons virtuels
- Paramètre des comptes
- Choix des amis
- Autorisations de publications
- Mots de passe

**Internet est partout, il faut donc se méfier, mais il est aussi important de montrer l'exemple à nos enfants.**

1- Savez-vous vraiment sur quels sites naviguent vos enfants?

Voir la campagne publicitaire contre les dangers d'Internet sur les enfants et les adolescents via le lien suivant : <https://youtu.be/aimMh80QNlk>.

2- Les enfants tombent facilement dans le piège.

Voir la vidéo « Action innocence - Le Masque – 1 » via le lien suivant : <https://youtu.be/ppbxgbjmaSo>.

3- Les informations personnelles telles qu'une photographie, une publication, un personnage dans un jeu en ligne, etc.

Voir la vidéo « Com'Infinie - Et si un voyant vous révélait les dangers d'Internet » via le lien suivant : <https://youtu.be/kbVBOQ0J5w>.

4- Demandez à votre enfant de vous aviser avant de publier une photo de famille prise à Noël, une photo de lui avec son costume d'Halloween ou encore une photo de lui devant l'autobus lors de sa première journée d'école. Ainsi, il apprendra qu'il est important d'avoir le consentement de ses parents avant de publier quoi que ce soit sur Internet.

5- Il est facile de faire confiance à un étranger lorsqu'il semble te comprendre et te connaître rapidement.

Voir la vidéo « The dangers of social media (child predator experiment) » via le lien suivant : <https://youtu.be/6jMhMVEjEQg>.



- 6- Sur les réseaux sociaux, il est souvent question de concours de popularité. Et oui, plus on a d'amis virtuels et plus on obtient de « J'aime ».

Invitez-vous tous les élèves fréquentant la même école que votre enfant à son anniversaire afin qu'il reçoive plus de cadeaux?

- 7- Une fois publiée sur les réseaux sociaux, une photographie ne nous appartient plus.

Voir la vidéo « Think before you post » via le lien suivant : <https://youtu.be/M8dzxgYwhrl>.

- 8- Il est important de faire attention aux faux concours auxquels on désire participer et à tous les liens sur lesquels on clique.

<https://www.danslescoulisses.com/fr/un-individu-aurait-pirate-le-telephone-de-plusieurs-joueurs-du-canadien/>.

Voir le vidéo « Espionner quelqu'un via son cellulaire : horriblement plus facile qu'on ne le croit | Corde sensible » via le lien suivant : <https://youtu.be/cjcha7fwitc>.

- 9- Il est important de créer des mots de passe robustes sur Internet. Par exemple, si mon chien se nomme Jack, il est plus sécuritaire d'inscrire *J1cisnK!* ou si je me nomme Nancy, il est également possible de choisir *J3\_5u1s\_N@n(y* comme mot de passe.

- 10- Voir le nouveau vidéoclip de sensibilisation d'Action innocence Monaco via le lien suivant : <https://youtu.be/SpeG5rVuUVM> Mai 2019.

- 11- Pornographie juvénile (SEXTO) :

- Production;
- possession;
- diffusion.

- 12- Voir le vidéoclip officiel de la chanson de Stromae intitulée Carmen via le lien suivant :

<https://youtu.be/UKftOH54iNU>.



## POUR EN SAVOIR UN PEU PLUS

Voir les pages suivantes :

- Les commentaires sur Internet – Vérités et conséquences avec Louis T. :  
<https://youtu.be/FP9rnf9uHSM>
- Le jeu interactif pour les élèves de 3e et 4e année :  
<http://habilomedias.ca/jeux/pirates-de-la-vie-privee>
- La vie privée : cette fille peut foire basculer votre vie en une heure | Corde sensible :  
<https://youtu.be/bS5h0uC4bAg>
- The dangers of snapchat (child predator experiment) :  
<https://youtu.be/fg-LhgZLB8M>
- Photoshop has gone too far :  
<https://youtu.be/Hnvoz91k8hc>
- <https://tefaispassextorquer.ca/#home>
- AidezMoiSVP.ca – Ne laisse personne écrire ton histoire à ta place :  
<https://youtu.be/4S-UknlHbSc>
- AidezMoiSVP.ca – Manifeste du pouvoir de #changerlhistoire :  
<https://youtu.be/4GytsCa8iZQ>



# CONTRAT D'UTILISATION D'INTERNET

## PROMESSE DE L'ENFANT :

- Mes informations personnelles (nom et prénom, adresse, numéro de téléphone, mot de passe, photographie, etc.) ne seront jamais divulguées sans l'accord de mes parents.
- J'informerai mes parents de toute situation qui me dérange.
- Je respecterai les limites d'utilisation d'Internet et des appareils électroniques établies par mes parents.
- Mes messages et paroles seront toujours respectueux.
- Je ne rencontrerai jamais quelqu'un sans l'accord de mes parents.
- Je m'assurerai que mes parents sont d'accord avant de télécharger, acheter ou participer à un concours.
- Je me souviendrai que tout étranger présent sur Internet n'est peut-être pas celui qu'il prétend être et que je dois rester méfiant et vigilant même s'il semble gentil.
- Mes parents auront toujours accès à ce que je fais sur Internet.

Signature de l'enfant

## PROMESSE DES PARENTS :

- Je m'engage à prendre les mesures nécessaires pour qu'Internet soit utilisé en toute sécurité par tous les membres de la famille à la maison.
- Je prendrai connaissance de toute utilisation Internet de mon enfant sur Internet et m'engage à connaître le fonctionnement des sites, programmes ou applications qu'il utilise.
- J'établirai des règles d'utilisation d'Internet et je limiterai le temps passé sur les écrans.
- Je comprends qu'un appareil électronique n'est pas une garderie ou un éducateur et que ma présence est donc nécessaire lorsque mon enfant navigue sur Internet.
- Je m'intéresserai aux amis réels et virtuels de mon enfant.
- Je m'engage à être présent pour aider mon enfant s'il vit une situation difficile.
- Je m'assurerai que tout appareil électronique de la maison reste dans une pièce commune en tout temps (par exemple : cuisine, salon, etc.).
- J'aiderai mon enfant à protéger ses informations personnelles (par exemple : pseudonyme, mot de passe, courriel, etc.).

Signature des parents

# TÉLÉPHONE ET SÉCURITÉ



Pour les parents et les ados, le téléphone est utile à la fois comme moyen de communication et comme dispositif de sécurité. Or, comme la plupart des technologies, le téléphone présente aussi des risques pour la sécurité de son utilisateur. Pour la sécurité de votre enfant, il est important que vous connaissiez les mesures à prendre pour qu'il en fasse une utilisation prudente.

## CONSIGNES DE SÉCURITÉ IMPORTANTES

1. Prenez le temps de vous renseigner sur les fonctions de l'appareil. Est-il muni d'applis préinstallées (comme Instagram<sup>MD</sup> et Facebook<sup>MD</sup>) ou de jeux avec lesquels vous devriez vous familiariser? Comprenez-vous le fonctionnement des services de géolocalisation et pourquoi il peut être important de les désactiver pour les photos et certaines applis?
2. D'emblée, dites à votre ado que vous exercerez un droit de regard sur la manière dont il utilise son téléphone. Ne manquez surtout pas à votre parole; faites des vérifications de temps à autre et au besoin, et imposez des conséquences pour tout écart ou comportement inapproprié.
3. Voyez s'il est possible de paramétrer l'appareil de façon à bloquer l'accès à certains sites (dont les sites pornographiques) ou si cela peut se faire au moyen d'applis de contrôle parental ou par l'entremise de l'opérateur de téléphonie cellulaire.
4. Imposez un couvre-feu pour l'usage des appareils électroniques (y compris les téléphones) dans votre foyer. Établissez aussi des règles pour les textos et les jeux (choix des correspondants de vos ados, de leurs partenaires de jeu, des sites et des applis qu'ils utilisent).
5. Dites à votre ado de ne pas répondre à des appels ou à des messages harcelants, hostiles ou inattendus et de conserver ce genre de messages. Montrez-lui comment bloquer les appels ou les messages venant d'utilisateurs indésirables et rappelez-lui l'importance de parler à un adulte de confiance s'il reçoit de tels messages.

**Le téléphone de votre enfant et l'information qu'il contient peuvent s'avérer utiles en situation de danger (p. ex. si votre enfant venait à disparaître). Tâchez de connaître les fonctions de géolocalisation offertes par l'appareil. Comme propriétaire du contrat, vous avez accès au registre des appels entrants et sortants ainsi qu'à l'information sur l'heure de la dernière utilisation connue de l'appareil. Certains appareils permettent aussi d'être localisés sur une carte moyennant un code; assurez-vous de connaître ce code.**

**Il est normal qu'un ado fasse des erreurs. Avertissez-le lorsqu'il omet d'utiliser son téléphone de façon responsable et rappelez-lui souvent qu'il peut vous parler sans crainte de tout ce qu'il vit.**



# TU AS PERDU LE CONTRÔLE??

**TEL-JEUNES**

[www.teljeunes.com](http://www.teljeunes.com)

**1 800 263-2266**



**AidezMoISVP.ca**

**cyberaide!ca**  
[www.cyberaide.ca](http://www.cyberaide.ca)

Besoin d'en parler?  
On est ouvert.  
24/7/365

Jeunesse. J'écoute   
1-800-668-6868  
[JeunesseJecoute.ca](http://JeunesseJecoute.ca)



# 5 MOYENS PRATIQUES DE RENFORÇER VOTRE CYBERSÉCURITÉ



## STOCKEZ VOS DONNÉES DE FAÇON SÉCURITAIRE ET SACHEZ COMMENT RÉCUPÉRER LES COPIES DE SAUVEGARDE

Utilisez uniquement des clés USB neuves que vous ou une personne que vous connaissez avez achetées. Ne les branchez jamais à un ordinateur non fiable.

Sécurisez les données stockées dans le nuage ou en ligne en activant toutes les mesures de sécurité disponibles.

Faites des copies de sauvegarde de l'information personnelle importante et sachez où elles se trouvent.

Exercez-vous au moins une fois à récupérer vos copies de sauvegarde. Vous saurez ainsi quoi faire si jamais vous êtes victime d'une attaque par rançongiciel.

*Les Canadiens sont la cible de cybercrimes de toutes sortes. Voici cinq moyens pratiques à mettre en œuvre dès maintenant afin de protéger vos appareils contre les atteintes à la cybersécurité.*

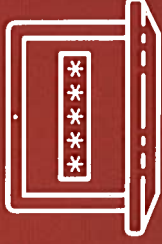
Consultez le [www.cyber.gc.ca](http://www.cyber.gc.ca) pour en savoir plus sur les mesures présentées ci-dessous.



## METTEZ À JOUR VOS APPAREILS MOBILES, VOS ORDINATEURS ET VOS APPLICATIONS

Les mises à jour sont essentielles à la sécurité, car elles contiennent les correctifs de sécurité. Ne les ignorez jamais.

Assurez-vous d'appliquer les mises à jour non seulement aux systèmes d'exploitation, mais aussi aux applications mobiles. Optez pour les mises à jour automatiques.



## ASSUREZ LA SÉCURITÉ DE VOS MOTS DE PASSE

Optez pour des phrases de passe uniques et des mots de passe complexes.

Ne dévoilez jamais vos mots de passe. N'utilisez pas le même mot de passe pour différents comptes, sites Web ou appareils.

Utilisez l'authentification à deux facteurs lorsqu'elle est offerte.



## SÉCURISEZ VOS COMPTES DE MÉDIAS SOCIAUX ET DE COURRIEL

Activez tous les paramètres de sécurité offerts dans chacun de vos comptes de médias sociaux et de courriel.

N'utilisez pas vos comptes de médias sociaux pour ouvrir des sessions dans d'autres comptes en ligne (p. ex. sites de magasinage, banque en ligne, médias sociaux ou autres comptes personnels).



## SOYEZ À L'AFFÛT DES MESSAGES D'HAMEÇONNAGE ET DE HARPONNAGE

Sachez reconnaître les messages qui sont des tentatives d'hameçonnage ou de harponnage.

Méfiez-vous des liens suspects, ne cliquez jamais dessus.

Utilisez un logiciel antivirus ou antimaliciel sur vos ordinateurs.

Se comporter en Cyber Héros suppose d'être futé, vigilant, secret, sympa et courageux. Afin de faire preuve de ces qualités, tous les membres de notre famille s'engagent à respecter les règles suivantes :



## Faites attention à votre image

Nous réfléchissons bien à ce que nous partageons, et avec qui – et donc à l'impact que ces informations sont susceptibles d'avoir pour nous et pour autrui (p. ex. adresse du domicile, emplacement actuel, informations concernant d'autres personnes).



## Ne tombez pas dans le panneau

Nous nous méfions des tentatives de phishing et autres arnaques et nous tiendrons mutuellement au courant de toute activité suspecte.



## Gardez votre identité secrète

Nous prendrons nos responsabilités afin de protéger les informations sensibles en créant des mots de passe forts et uniques comportant des lettres, des chiffres et des symboles.



## Faites le bien autour de vous

Nous répandrons la positivité et le respect et bloquerons et signalerons les comportements en ligne malveillants . Si nous sommes témoins de harcèlement en ligne, nous réagissons en protecteurs et pas en spectateurs.



## Appelez un adulte à l'aide

Nous prendrons position pour défendre nos intérêts et ceux d'autrui si nous observons des comportements malveillants ou inappropriés en ligne. Nous parlerons ouvertement des situations qui nous mettent mal à l'aise, en famille.

Ainsi, nous pourrons explorer le Net de manière sûre et confiante.

Signature,

\_\_\_\_\_



\_\_\_\_\_



\_\_\_\_\_



\_\_\_\_\_

