LA SÉCURITÉ SUR INTERNET

10 trucs et astuces pour te protéger sur Internet

Voici quelques conseils qui te permettront de naviguer sur Internet de façon sécuritaire. Si tu rencontres des problèmes sur Internet, n'hésite pas à en parler à un adulte de confiance. Plusieurs ressources gratuites et confidentielles sont également à ta disposition pour t'aider, te guider et répondre à tes questions. Tu trouveras ces ressources à la fin du guide.

INFORMATIONS EN LIGNE

Ce qui est mis en ligne sur Internet ne disparaît jamais. Il y a toujours moyen de retrouver ce qui était sur un site ou ce qu'un utilisateur a écrit ou partagé. Même le contenu qui est effacé par l'utilisateur laisse des traces dur Internet et peut être récupéré.

TES INFORMATIONS PERSONNELLES

Personne ne devrait partager ses informations personnelles sur Internet via un compte ou des échanges avec d'autres internautes. Voici des données qu'on ne devrait jamais mettre en ligne :

- Ton adresse
- Ton numéro de téléphone
- Ta date de naissance
- Le nom de ton école
- Tes numéros de compte bancaire
- Tes mots de passe
- Autres

COMPTE PUBLIC ET PRIVÉ

Lorsque ton compte est « public », tout le monde peut y avoir accès et consulter les informations et le contenu que tu y partages. Même si tu ne lui as pas donné ton autorisation.

Pour se protéger des personnes malintentionnées et pour sécuriser les informations et le contenu que tu y partages, il est plus prudent de mettre ton compte « privé ». Tu diminues les risques de rencontrer des problèmes.

MOT DE PASSE

Pour éviter que des gens malintentionnés accède à tes informations personnelles, assure-toi de sécuriser tes appareils électroniques à l'aide de mot de passe.

Ne partage pas tes mots de passe avec tes ami·es, même si tu as confiance en eux·elles.

Les compagnies (Facebook, Instagram, TikTok, Snapchat, etc.) ne demandent jamais ton mot de passe par courriel, SMS ou chat. Méfie-toi de ce type de demande.

N'utilise pas un seul mot de passe pour te connecter à tous tes appareils et applications. Si quelqu'un accède à un mot de passe, il accède à toutes tes informations et données personnelles.

Il est beaucoup plus prudent d'utiliser une authentification à double sens lorsque disponible. Exemple : confirmation avec son téléphone ou code unique par courriel ou sms.

APPLICATIONS

Télécharge toujours tes applications via pour téléphone ou tablette via ton Apple Store, Amazon Store ou Google Play Store. Surtout, il est recommandé de télécharger des applications de compagnies connues et reconnues.

Ne télécharge pas tes applications via un courriel que tu reçois. Par exemple, une compagnie communique avec toi par courriel pour te proposer son nouveau produit et t'invite à cliquer sur un lien à même le courriel. Rends-toi plutôt dans ton Apple Store, Amazon Store ou Google Play Store pour télécharger l'application.

FAUX COMPTES

Communiquer avec les gens que tu connais est plus sécuritaire. Plusieurs personnes se présentent sous de faux comptes via les réseaux sociaux. Leurs motivations sont très variées et peuvent être mal intentionnées. Il est toujours préférable de communiquer avec des personnes que tu connais.

BLOQUER UN COMPTE

Que ce soit sur ton cellulaire ou sur tes comptes, tu peux bloquer un utilisateur pour l'empêcher de communiquer avec toi et de consulter ton profil.

Tu peux également signaler anonymement des comptes lorsque des actions inadéquates sont posées.

FAKE NEWS

Vérifie toujours la source de tes informations. Les « fake news » sont très fréquentes et nombreuses sur Internet. Ce n'est pas parce qu'une information est sur Internet qu'elle est valide. Méfie-toi de ce que tu lis!

HAMMEÇONNAGE

Les hackers utilisent toutes sortes de stratégies pour obtenir nos informations personnelles. Nous devons être vigilant·es.

Lorsque tu n'es pas certain de la provenance du courriel, il est toujours plus prudent d'écrire toi-même l'URL du site dans ton navigateur de recherche que de cliquer le lien qu'il t'envoie.

Voici quelques astuces à valider pour ne pas te faire avoir :

- Vérifier l'expéditeur·trice : N'ouvre pas les liens d'expéditeur·trices inconnu·es.
- Vérifier le lien URL : Les hackers modifient légèrement l'URL pour te faire croire que tu seras redirigé·e sur une page Web sécurisée. Par exemple : instagram.com pourrait devenir « instagra.com » ou « insta.com ».
- S'assurer que l'URL commence par « https » : Une page "http" (sans le S) n'est pas une page Web sécurisée.
- Observer la qualité des images: Les infographies ont tendance à être de moins bonne qualité lorsqu'il s'agit de tentative d'hameçonnage.
- Observer Le ton du message : Les hackers écrivent des messages insistants et créent une "urgence" pour que tu cliques rapidement (ex. « Dans 2h, tout s'effacera! », « Tu pourras uniquement télécharger cette appli aujourd'hui. »)
- Observer l'infographie : Les plates-formes de hackers sont légèrement différentes des plateformes réelles.
- Être à l'écoute de ton feeling : Si quelque chose te chicotte, ne cliques pas!

COMPORTEMENTS À ÉVITER

IMAGES INTIMES :
Le fait de produire, envoyer, partager et conserver des images intimes de personnes mineures (18 ans et moins) est interdit, même si toi et l'autre personne êtes consentant·es. Il s'agit d'actes criminels pouvant conduire à des accusations criminelles.

INSULTES, MENACES ET RUMEURS :
Il est interdit de produire ou partager du contenu comportant des insultes, des propos haineux ou incitant à la haine, des rumeurs et/ou des menaces. Même si la personne visée n'est pas clairement identifiable, il s'agit d'actes criminels pouvant conduire à des accusations criminelles.

DES RESSOURCES À TA DISPOSITION AU BESOIN

GÉNÉRALE

Tel-Jeune https://www.teljeunes.com	1 800 263-2266	514 600-1002
Jeunesse, j'écoutes https://www.jeunessejecoute.ca	1 800 668-6868	Texte PARLER au 686868
Le Regroupement québécois des centres d'aide et de lutte contre les agressions à caractère sexuel (RQCALACS) https://www.rqcalacs.qc.ca	1 888 933-9007	
Prévention suicide https://suicide.ca	1 866 APPELLE 1 866 277-3553	
Info-Social **(Réseau de la santé)**	811 option 2	
Centre de crise https://www.centredecrise.ca/listecentres		
Deuil jeunesse https://www.deuil-jeunesse.com/services-professionnels	418-624-3666	

CYBERDÉPENDANCE

À l'abris du gameur https://www.twitch.tv/abrisdugameur		
Le grand chemin https://legrandchemin.qc.ca/services-gratuits/adolescents/	1 877 381-7075	
Jeu: aide et référence https://aidejeu.ca/	1 800 461-0140	

VIOLENCE

SOS violence conjugale
https://sosviolenceconjugale.ca/fr
1 800 363-9010

Violence info
https://www.violenceinfo.com
418 667-8770

Le centre de prévention de la radicalisation menant à de la violence
https://info-radical.org/fr/historique
Montréal : 514-687-7141 #116
Ailleurs au Québec :
1-877-687-7141 #116

TROUSSE D'OUTILS PÉDAGOGIQUES

Habilo médias
https://habilomedias.ca/

Centre québécois d'éducation aux médias et à l'information
https://www.cqemi.org/fr/outils-pedagogiques

Atelier d'autodéfense numérique
https://www.bienetrenumerique.com/

Pause
https://pausetonecran.com

Fondation jeunes en tête
https://fondationjeunesentete.org/trousse-jeunes/

Réfléchis quand tu publies
http://www.reflechisquandtupublies.ca/