Connected Canadians
Canadiens Branchés

Outils de sécurité numérique : Construire votre boîte à outils personnelle en cybersécurité

Créer des mots de passe forts

Votre mot de passe est la première ligne de défense. Ne réutilisez jamais le même mot de passe sur plusieurs sites.

FAIBLE — Facile à déchiffrer	FORT — Difficile à déchiffrer
❌ password123	✅ Au moins 12 caractères de long
❌ John1952	✅ Mélanger les lettres, les chiffres et les symboles
❌ Fluffydog!	✅ Pas de noms, de dates ou de noms d'animaux
❌ qwerty	✅ Utiliser une phrase de passe (quatre mots aléatoires)
❌ 123456	✅ Un mot de passe unique pour chaque site

💡 Essayez https://bitwarden.com/fr-fr/password-strength/ pour tester votre mot de passe. Une phrase de passe comme "railcar shamrock routine crate" prendrait des siècles à déchiffrer!

Vous pouvez également utiliser useapassphrase.com (anglais) ou proton.me/fr/pass/passphrase-generator (français) pour générer une phrase de passe ou tester la solidité de votre mot de passe.

Utiliser un gestionnaire de mots de passe

Pensez à votre trousseau de clés. Vous avez une clé pour votre porte d'entrée, votre voiture, peut-être votre boîte aux lettres, peut-être un casier de rangement. Vous ne mémorisez pas quelle clé correspond à quoi, vous prenez simplement la bonne au moment où vous en avez besoin.

Connected Canadians
Canadiens Branchés

Un gestionnaire de mots de passe, c'est exactement la même chose, mais pour vos comptes en ligne. Il stocke tous vos mots de passe en toute sécurité. Vous n'avez besoin de vous souvenir que d'une seule chose, votre mot de passe principal, et il s'occupe du reste.

Voici comment cela fonctionne:

1. Vous créez UN seul mot de passe principal fort
2. L'application génère un mot de passe unique pour chaque site
3. Il remplit automatiquement vos informations de connexion chaque fois que vous visitez ce site
4. Si un site est piraté, aucun autre compte n'est en danger

Parmi les gestionnaires de mots de passe populaires, on trouve : Bitwarden, Google Password Manager et Apple Passwords.

⚠️ Notez votre mot de passe principal et conservez-le en lieu sûr chez vous. Il n'y a aucune récupération possible si vous l'oubliez.

Vérifiez si vos données ont été divulguées

Visitez haveibeenpwned.com et entrez votre adresse courriel pour voir si elle est apparue dans une violation de données connue.

Types de résultats	
✅ Bonne nouvelle : "Aucune compromission trouvée!"	⚠️ Action requise : "Oh non — compromis!"
Vous êtes hors de danger.	Changez ces mots de passe immédiatement.

Connected Canadians
Canadiens Branchés

💡 Inscrivez-vous aux alertes courriel gratuites sur haveibeenpwned.com afin d'être informé immédiatement si vos données sont compromises lors de futures violations.

Repérer les arnaques et l'hameçonnage

Les arnaqueurs misent sur la **panique**. Le moment où vous vous sentez pressé, menacé ou confus est exactement celui où vous devez ralentir.

Utilisez cette règle en trois étapes chaque fois:

- **ARRÊTEZ.** Ne cliquez pas, ne payez pas et ne donnez aucune information. Raccrochez ou fermez le navigateur. Les arnaqueurs créent de fausses échéances (« Agissez dans les dix prochaines minutes ! ») pour vous empêcher de réfléchir correctement.
- **RESPIREZ.** Posez-vous les questions suivantes : est-ce moi qui ai initié ce contact? Me demandent-ils quelque chose d'inhabituel, comme des cartes-cadeaux, un virement bancaire ou un accès à distance à mon ordinateur? Serais-je mal à l'aise d'en parler à un membre de ma famille? Si quelque chose vous semble bizarre, faites confiance à votre intuition. Vous aurez presque toujours raison.
- **RAPPELEZ.** Raccrochez et rappelez l'organisation en utilisant un numéro que vous trouvez vous-même sur leur site Web officiel ou au dos de votre carte bancaire. N'utilisez jamais un numéro fourni par l'appelant. S'il s'agit d'un vrai organisme, vous le joindrez lorsque vous rappellerez. S'il s'agit d'une arnaque, le numéro ne correspondra pas.

Aucun vrai organisme gouvernemental, banque, entreprise technologique ou service public ne demandera jamais un paiement par carte-cadeau, cryptomonnaie ou virement électronique, **jamais**.

Ce mode de paiement est le signe le plus révélateur d'une arnaque. **Une fois qu'un virement électronique ou un numéro de carte-cadeau est envoyé, l'argent ne peut pas être récupéré.**

Connected Canadians
Canadiens Branchés

Quatre signaux d'alarme	Principales arnaques au Canada
Urgence / Menaces « Payez maintenant ou vous serez arrêté »	**Faux appels de l'ARC** Vérifiez : 1-800-959-8281
Cartes-cadeaux ou virement électronique Les gouvernements et les banques n'exigent jamais cela	**Arnaque aux grands-parents** Appelez directement le petit-enfant
On vous demande de cliquer sur un lien Allez directement sur le site Web - ne cliquez jamais!	**Arnaque au soutien technique** Microsoft ne vous appelle jamais
Trop beau pour être vrai On ne peut pas gagner un prix auquel on n'a jamais participé!	**Romance / virement électronique** Aucune protection contre la fraude une fois l'argent transmis

Activer l'authentification à deux facteurs (2FA)

Authentification à deux facteurs (2FA) est une étape de sécurité supplémentaire qui aide à protéger vos comptes, comme le courriel ou les services bancaires en ligne.

Normalement, vous vous connectez avec **une seule chose : votre mot de passe.**

Avec la 2FA, vous avez besoin de **deux choses** pour prouver que c'est vraiment vous.

Une façon utile de s'en souvenir est :

1. **Quelque chose que vous savez**
   Il s'agit de votre **mot de passe ou NIP**. Vous seul devriez le connaître.

2. **Quelque chose que vous possédez**
   Il s'agit généralement de votre **téléphone où un code spécial vous est envoyé**. Par exemple, après avoir entré votre mot de passe, votre banque pourrait vous envoyer par texto un **code à six chiffres** que vous saisissez pour terminer votre connexion.

Connected Canadians
Canadiens Branchés

Ainsi, même si quelqu'un devine votre mot de passe, il **ne peut toujours pas accéder à votre compte sans votre téléphone.**

Vous pouvez y penser comme **une carte de guichet automatique et un NIP :**

- La **carte** est quelque chose que vous possédez
- Le **NIP** est quelque chose que vous savez

Vous avez besoin **des deux** pour accéder à votre argent.

Voici pourquoi cela aide :
Cela rend beaucoup plus difficile pour les arnaqueurs ou les pirates informatiques d'accéder à vos comptes.

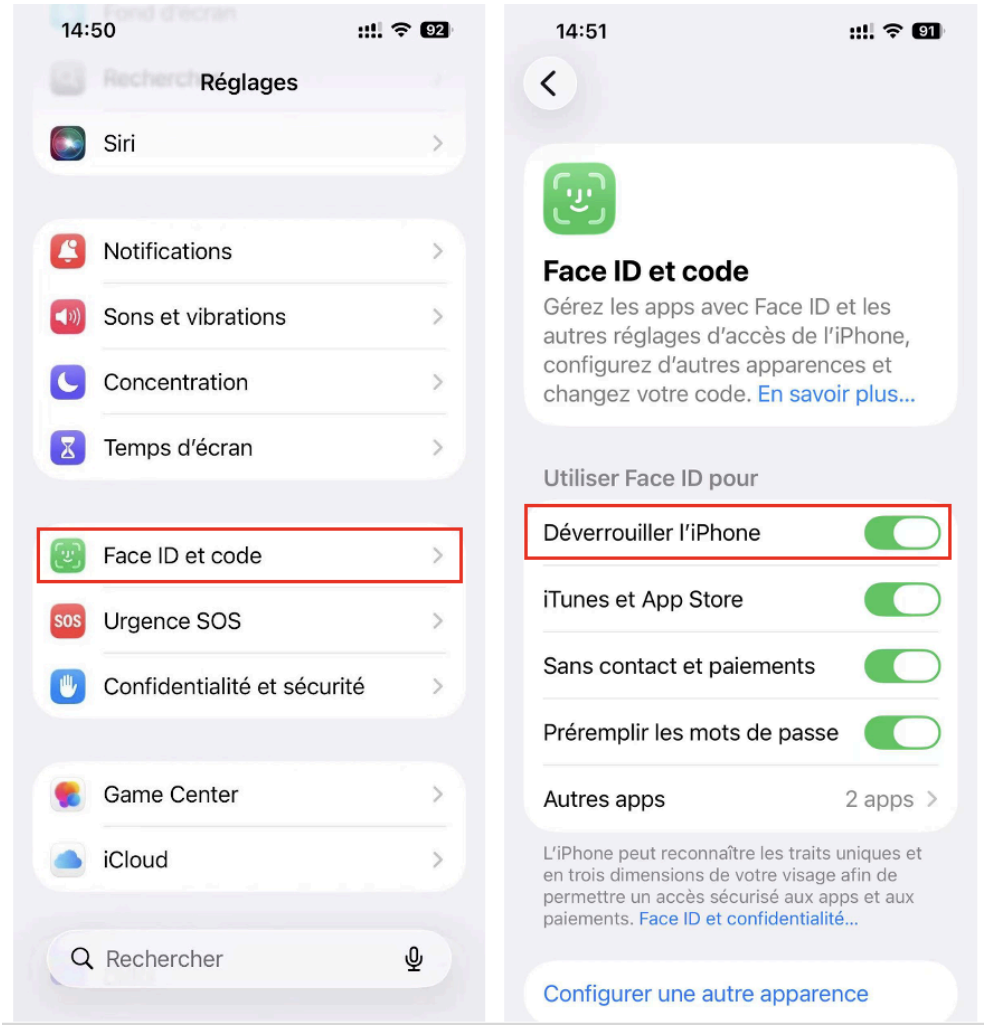
Sécurisez vos appareils

Étape 1 - Vérifiez le verrouillage de votre écran

Ouvrez vos Paramètres et assurez-vous d'avoir configuré un NIP ou un verrouillage biométrique, comme une empreinte digitale ou Face ID.

Connected Canadians
Canadiens Branchés

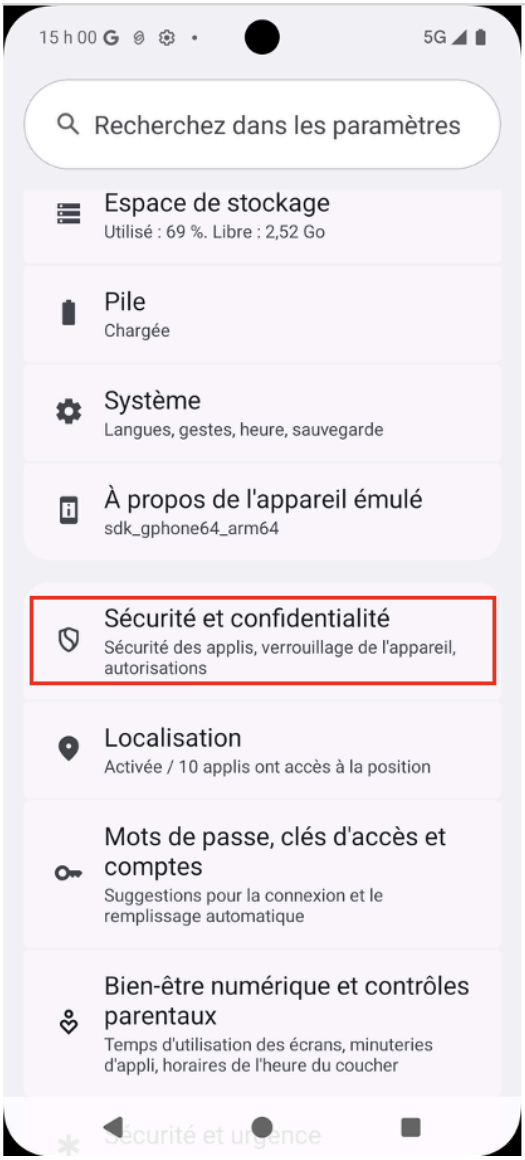
iPhone : Paramètres → Face ID et code

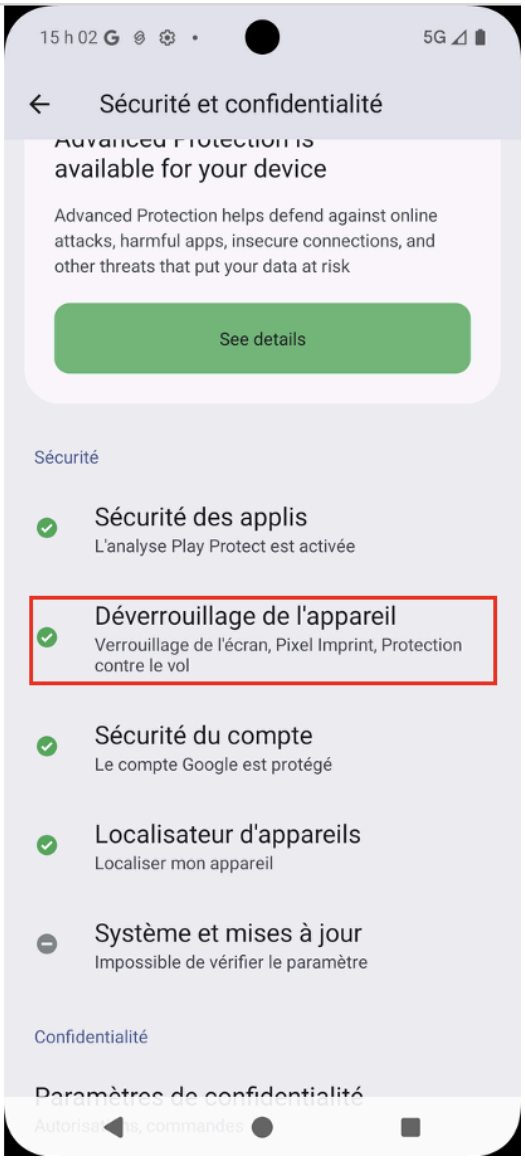


+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Android : Paramètres → Sécurité → Verrouillage de l'écran





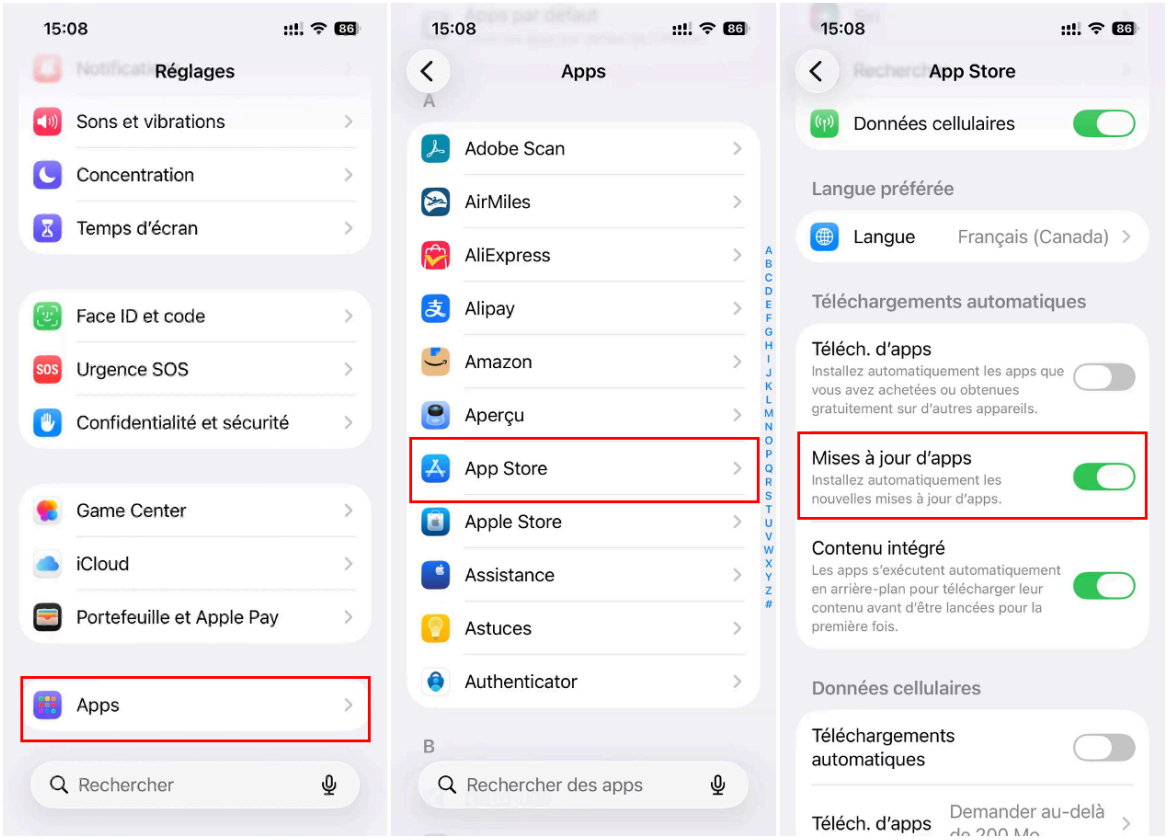
+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Étape 2 - Activez les mises à jour automatiques des applications

Activer cette option permet de s'assurer que vos applications restent à jour avec les derniers correctifs de sécurité sans que vous ayez à vous souvenir de les mettre à jour manuellement.

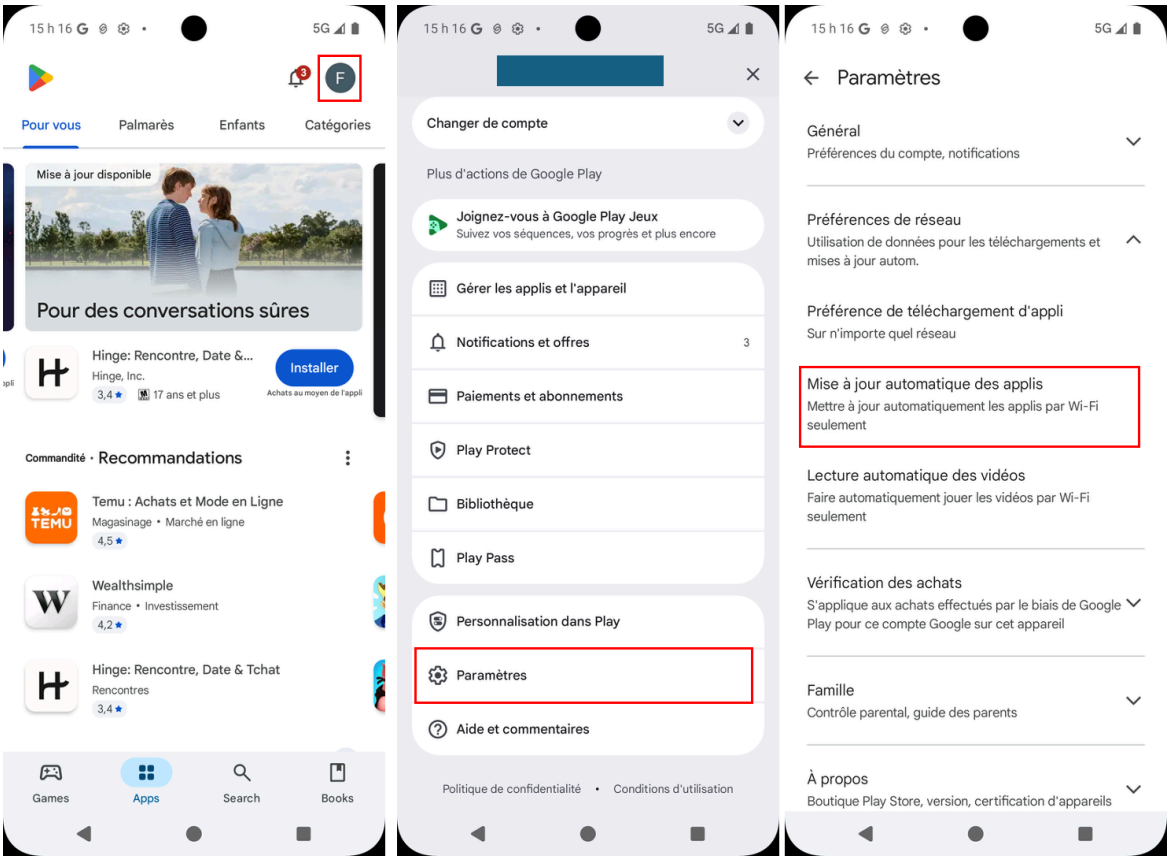
iPhone : Paramètres → App Store → Mises à jour des applications ACTIVÉES



+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Android : Play Store → Paramètres → Mise à jour automatique des applications



+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

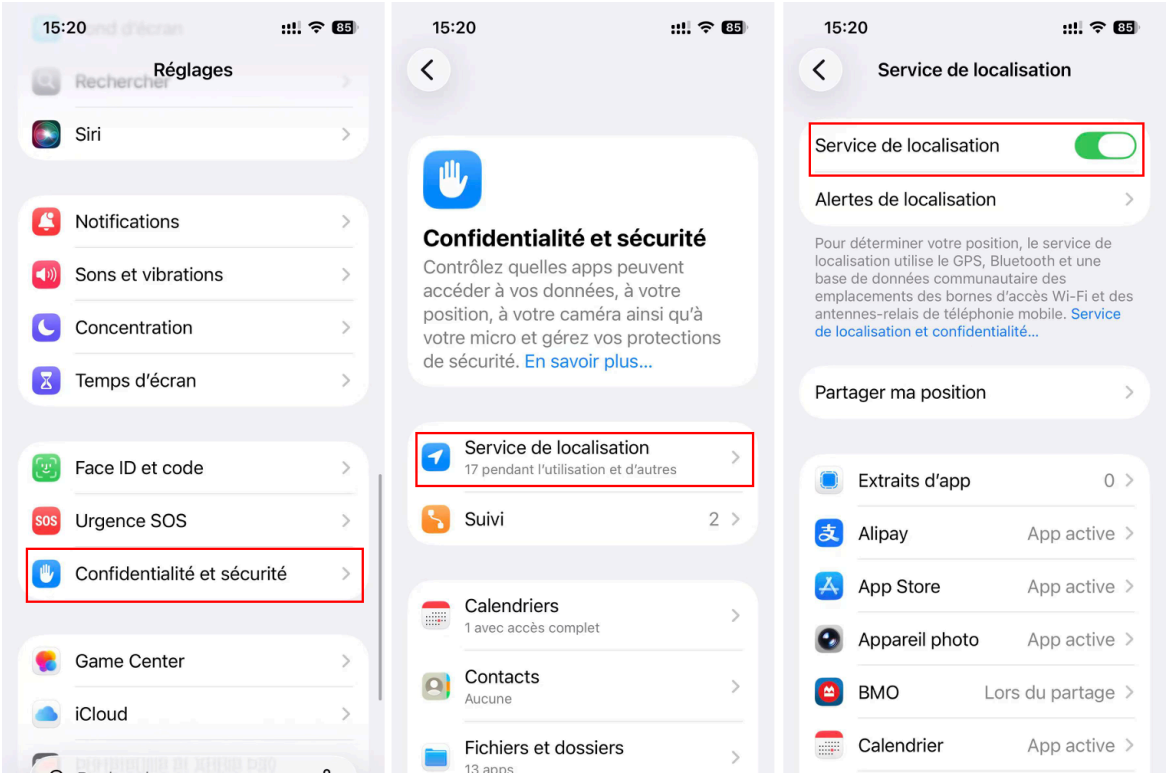
Connected Canadians
Canadiens Branchés

Étape 3 - Vérifiez les autorisations des applications

Parcourez la liste et demandez-vous si chaque application qui a accès à votre localisation en a vraiment besoin ? Plans de déplacements? Oui. Une application de lampe de poche? Non. Retirez l'accès à tout ce qui ne requiert pas une telle autorisation.

Pendant que vous y êtes, regardez qui a accès à votre microphone et à votre caméra. Tout ce qui semble inattendu devrait être désactivé.

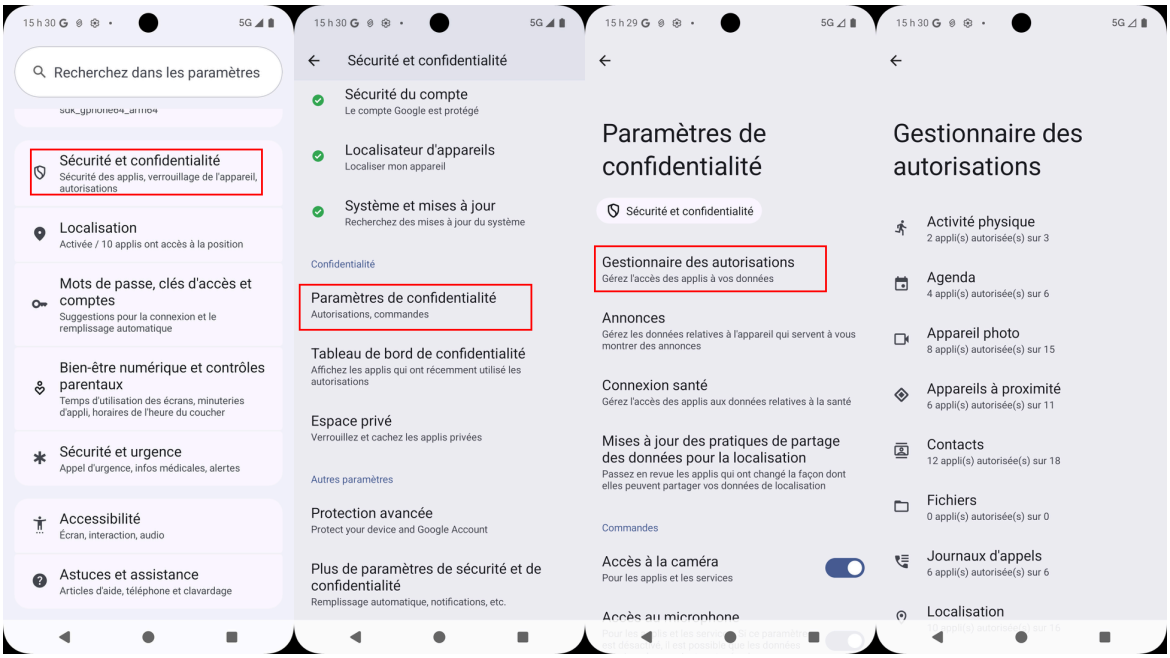
iPhone : Paramètres → Confidentialité → Services de localisation



+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Android : Paramètres → Confidentialité → Gestionnaire des autorisations



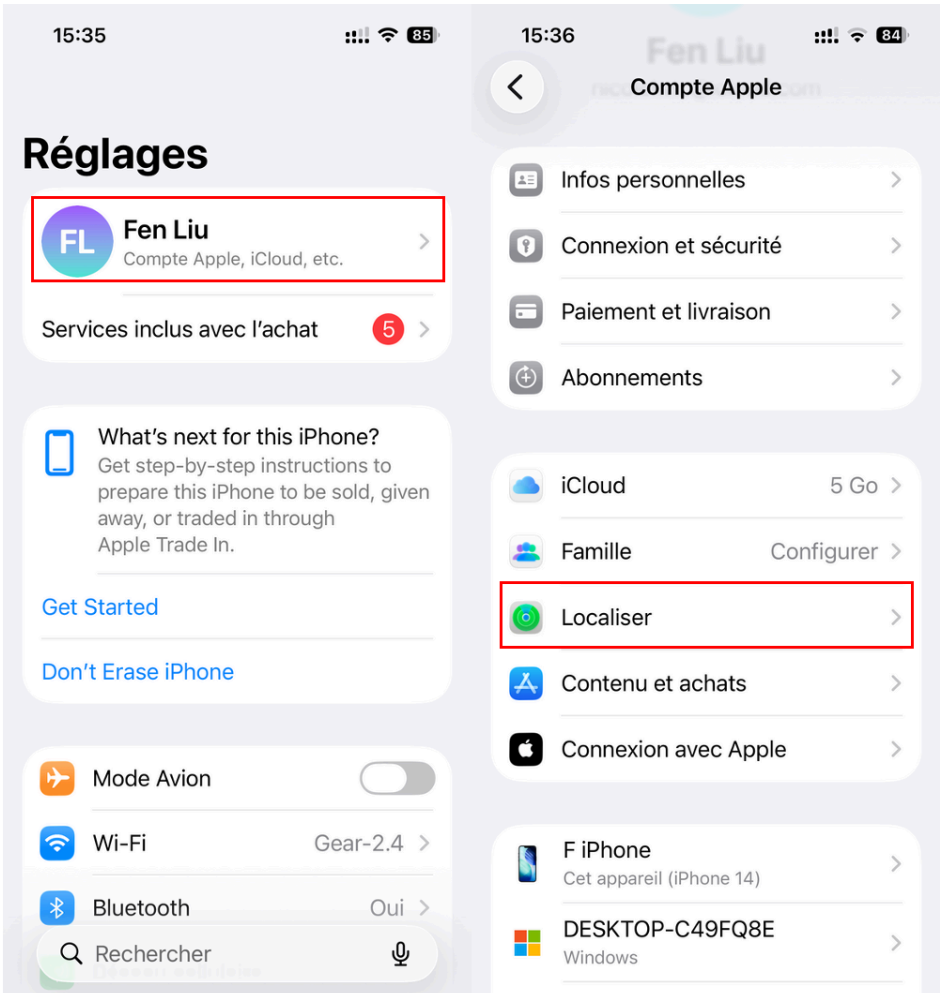
+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Étape 4 - Activez la fonction « Localiser mon appareil »

Activer « Localiser mon appareil » vous permet de localiser, verrouiller ou effacer votre appareil s'il est perdu ou volé. Vous protégez ainsi votre appareil et les informations personnelles qu'il contient.

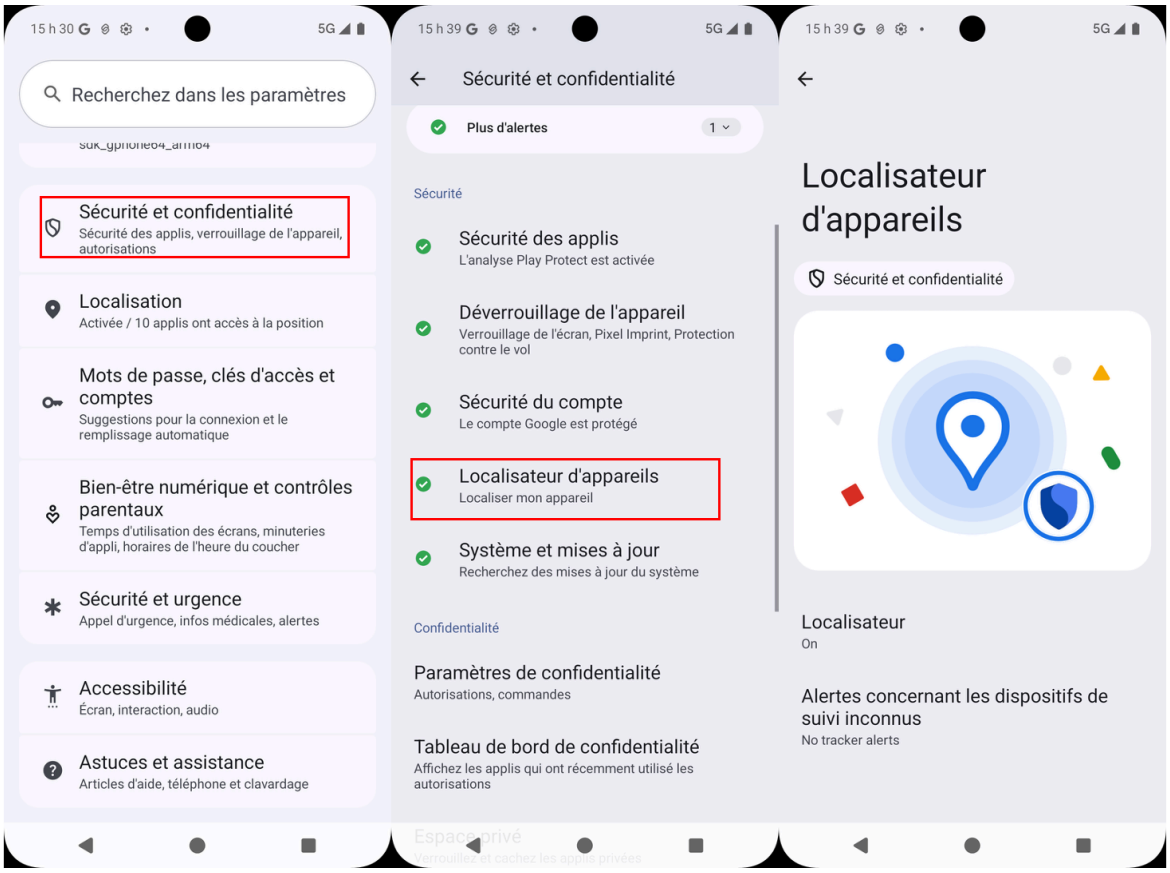
iPhone : Réglages → [Votre nom] → Localiser



+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Android : Paramètres → Sécurité → Localiser mon appareil



+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Naviguer en toute sécurité

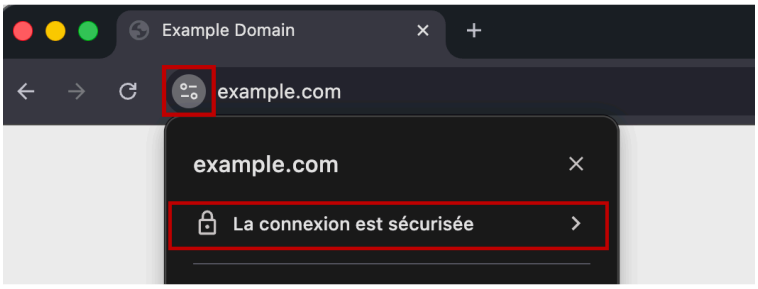
Le cadenas

Recherchez un 🔒 cadenas avant de saisir des mots de passe ou des numéros de carte.

Pas de cadenas = ne saisissez pas vos informations.

Remarque : Un cadenas ne garantit PAS qu'un site est légitime.

Vérifiez toujours l'orthographe de l'adresse Web.

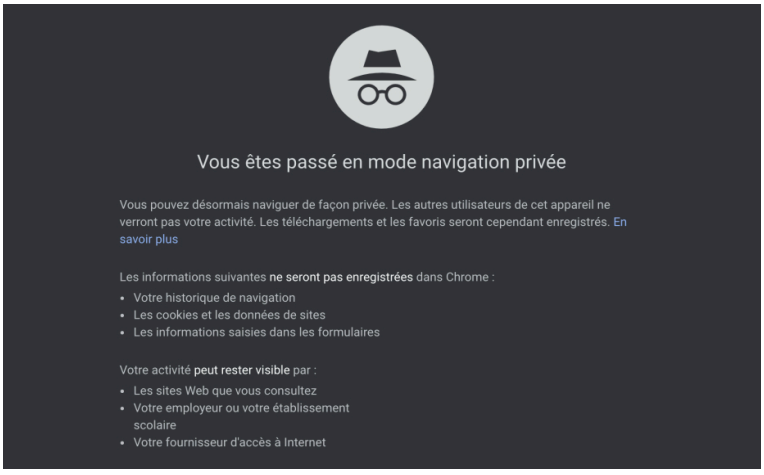


Mode privé / Navigation privée

Efface votre historique et vos connexions lorsque vous fermez la fenêtre.

Utilisez-le sur les ordinateurs partagés ou publics. Il ne vous cache **pas** de votre fournisseur d'accès Internet.

Appuyez sur Ctrl+Maj+N (Windows) ou Cmd+Maj+N (Mac).



+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

Naviguer en toute sécurité

- **Configurer des alertes bancaires :** demandez à votre banque de vous envoyer un texto chaque fois qu'une transaction est effectuée. Vous serez informé d'une fraude en quelques secondes.
- **Avertissement concernant le virement Interac :** le virement Interac n'offre AUCUNE protection contre la fraude. Une fois envoyé, c'est parti. N'envoyez jamais rien à quelqu'un que vous n'avez pas rencontré en personne.
- **Alerte à la fraude gratuite :** appelez Equifax Canada et TransUnion Canada pour placer une alerte à la fraude gratuite. Les prêteurs doivent prendre des mesures supplémentaires avant d'ouvrir des comptes en votre nom.
- **Utilisez le crédit, pas le débit en ligne :** les cartes de crédit offrent une meilleure protection contre la fraude. En cas de fraude, la banque se bat pour vous. Avec le débit, votre argent est parti pendant qu'ils enquêtent.

Sauvegardez vos données — La règle 3-2-1

Un virus, un vol ou un téléphone qui tombe peut tout effacer. Une sauvegarde est votre filet de sécurité.
La **règle de sauvegarde 3-2-1** est un moyen simple de protéger vos données contre la perte.

Cela signifie:

- conserver **trois copies de vos données** (l'original plus deux sauvegardes),
- stockées sur **deux types de stockage différents** (par exemple, votre ordinateur et un disque dur externe),
- avec **une copie stockée hors site** (comme dans un stockage en nuage).

Ainsi, si un appareil tombe en panne, est volé ou est infecté par un logiciel malveillant, vous disposez toujours d'autres copies en sécurité.

Sites à explorer

- **Centre antifraude du Canada** - Base de données canadienne des alertes à la fraude. Consultez les dernières arnaques ciblant les Canadiens en ce moment. cafc.ca

+1 (877) 304 5813
info@canadiensbranches.org
www.canadiensbranches.org
78 George St #204, Ottawa, ON K1N 5W1

Connected Canadians
Canadiens Branchés

- **Pensez cybersécurité** (Gouvernement du Canada)- Conseils officiels du gouvernement du Canada en matière de cybersécurité — en langage clair et fiable. pensezcybersecurite.gc.ca
- **Gestionnaire de mots de passe Bitwarden** - Gratuit et à code source ouvert. Fonctionne sur téléphone, tablette et ordinateur. Commencez par ici. bitwarden.com
- **Alertes aux arnaques de la FTC** - Basé aux États-Unis, mais pertinent — la plus grande base de données de signalement d'arnaques au monde. Utile pour les tendances. consumer.ftc.gov/scams
- **Have I Been Pwned** - Vérifiez si votre courriel figure dans une violation connue. Inscrivez-vous aux alertes gratuites. haveibeenpwned.com
- **Votre rapport de crédit gratuit** - Vérifiez les comptes que vous n'avez pas ouverts. Gratuit une fois par an auprès de chaque bureau. equifax.ca transunion.ca canada.ca/fr/agence-consommation-matiere-financiere/services/dossier-pointage-credit/commander-dossier-credit.html
- **CheckFirst.ca (OSC)** - Vérifiez si un conseiller en placement ou une société est enregistré au Canada avant d'investir. checkfirst.ca
- **Restez en sécurité en ligne (NCSA)** - Guides en langage clair sur tous les sujets de sécurité numérique. Idéal à partager avec la famille. staysafeonline.org

Si vous avez des questions ou si vous souhaitez du soutien concernant l'un des sujets abordés ici, veuillez communiquer avec Canadiens Branchés par courriel à: www.canadiensbranches.org.
Nos personnes bénévoles sont prêtes à vous aider, à s'assurer que vous vous sentiez en confiance et à vous accompagner dans votre parcours numérique.