Protéger vos appareils

Cette ressource propose des mesures pratiques pour protéger les appareils contre les formes courantes de localisation et couvre notamment la désactivation de Bluetooth, le partage de la connexion Wi-Fi et de la localisation, le changement du nom de l'appareil, la vérification des logiciels espions et des autorisations des applications, et la réinitialisation.

Voici des conseils généraux pour protéger vos appareils. Les mesures exactes peuvent varier d'un appareil à l'autre et évoluer au fil du temps.

Sur les appareils iPhone et iPad, vous pouvez trouver un paramètre en appuyant sur l'icône des réglages, puis en faisant glisser l'écran vers le bas pour afficher la barre de recherche. (Pour obtenir de l'aide, consultez la page https://support.apple.com/fr-ca/iphone.)

Sur les appareils Android, faites glisser l'écran d'accueil vers le haut : une barre de recherche indiquant « Rechercher dans votre téléphone et plus encore » s'affichera. Saisissez le réglage que vous recherchez dans la barre de recherche.

Désactivez les fonctions Bluetooth et Wi-Fi lorsque vous ne les utilisez pas

Les fonctions Bluetooth et Wi-Fi rendent votre appareil visible à d'autres appareils. Lorsque vous ne les utilisez pas, désactivez ces fonctions en accédant aux **réglages** ou en appuyant sur les icônes **Bluetooth** et **Wi-Fi**.

Vous pouvez également accéder à vos paramètres Bluetooth (**icône d'engrenage** > **Bluetooth**) et rechercher les appareils qui sont jumelés à votre téléphone. Si vous ne reconnaissez pas certains des appareils énumérés, désactivez-les.

Désactivez le partage de localisation

Le partage de la localisation et les applications comme celle vous aidant à trouver votre téléphone fonctionnent même si votre téléphone est éteint. Vous devez donc les désactiver dans les réglages. Sur un iPhone, ouvrez **les réglages**, puis allez dans « Confidentialité et sécurité » et ensuite dans « Service de localisation », ou cherchez les termes « Service de localisation », et désactivez le partage de localisation.

Sur un appareil Android, ouvrez la fonction « **Cartes** », appuyez sur votre photo de profil, puis sur « Partage de localisation ». Appuyez sur la photo de profil de toutes les personnes qui *ne devraient pas* voir votre localisation, puis appuyez sur « Arrêter ».

Clé des icônes

- les réglages / l'icône d'engrenage
- Bluetooth
- Wi-Fi
- la bascule
- Cartes
- l'icône des trois points horizontaux

Protéger vos appareils

Renommez vos appareils

Même si vous n'avez jamais changé l'identité (nom) de votre téléphone, il a tout de même un nom. Sur un iPhone, ouvrez **les réglages**, puis allez dans « Général », puis sans « Informations » et « Nom », ou recherchez le mot « Nom », puis saisissez un nouveau nom et appuyez sur « Terminé ».

Sur un appareil Android, appuyez sur l'**icône d'engrenage**, puis allez dans « Informations du téléphone » et ensuite « Nom de l'appareil », ou recherchez le mot « Nom », puis entrez le nouveau nom et appuyez sur « Ok ».

Vérifiez la présence de logiciels espions

Les logiciels espions sont des applications qui permettent à une personne d'espionner votre appareil. Vérifiez s'il existe des applications que vous ne reconnaissez pas. Sur un iPhone, faites glisser vers la droite sur l'écran d'accueil jusqu'à la bibliothèque d'applications.

Appuyez sur la barre de recherche au haut de l'écran, puis parcourez la liste des applications et supprimez toutes celles que vous ne reconnaissez pas.

Sur un appareil Android, ouvrez **les réglages**, puis allez dans « Applications » et ensuite « Voir toutes les applications », ou recherchez le mot « Applications ».

Il existe également des applications comme *Certo* et *Incognito* qui analysent vos appareils pour trouver des logiciels espions, mais vous devez savoir qu'il est tout de même possible qu'un logiciel espion demeure sur votre téléphone.

Vérifiez les autorisations des applications

Vous pouvez également empêcher une application de recueillir ou de partager des informations comme votre localisation. Sur un iPhone, ouvrez **les réglages**, puis allez dans « Confidentialité et sécurité » et ensuite « Rapport de confidentialité des apps » pour voir ce que partage chaque application, ou recherchez les mots « Rapport de confidentialité ». Appuyez sur chaque application pour modifier les réglages.

Clé des icônes

les réglages
l'icône d'engrenage

l'icône des trois points horizontaux

la bascule

Sur un appareil Android, téléchargez l'application *DuckDuckGo* à partir de l'application Play Store (boutique d'applications), puis ouvrez-la. Ouvrez **les réglages**, puis choisissez la fonction de protection contre le suivi des applications et faites glisser **la bascule** vers la droite.

Réinitialisation

Si vous avez fait tout ce qu'il fallait et que vous pensez tout de même qu'une personne pourrait suivre votre téléphone, vous pouvez procéder à une réinitialisation. Cependant, cette opération supprimera toutes les données, y compris toute preuve contenue dans votre téléphone que vous pourriez être amené à fournir à la police ou à un avocat. Si vous réinitialisez votre téléphone, vous *ne pouvez pas* le restaurer à partir d'une sauvegarde puisqu'une application qui vous suivait pourrait être retéléchargée. Vous devez recommencer à zéro.

Si vous êtes sûr de vouloir réinitialiser votre téléphone, vous pouvez ouvrir **les réglages** sur votre iPhone, allez dans le menu « Général », puis dans « Transférer ou réinitialiser l'iPhone » et ensuite « Effacer contenu et réglages ». Vous pouvez aussi rechercher le mot « réinitialiser » pour trouver ce réglage.

Si vous avez un iPhone, vous pouvez également activer le mode de confinement, qui vous protège contre la plupart des logiciels espions. Ce mode limite aussi l'utilisation d'applications comme FaceTime et Safari. Consultez la page https://support.apple.com/fr-ca/HT212650 pour en savoir plus sur le mode de confinement.

Sur un appareil Android, commencez par ouvrir **les réglages**, puis recherchez la fonction « Réinitialiser ». Recherchez une option indiquant « Réinitialisation » ou « Effacer toutes les données », et appuyez sur l'option.

Habilo Médias

Avec le financement de

Agence de la santé publique du Canada | Public Health Agency of Canada

Communiquer en toute sécurité

Cette ressource propose des étapes pratiques pour communiquer en ligne en toute sécurité afin d'éviter les formes courantes de suivi en ligne et couvre des actions comme : se déconnecter des comptes; désactiver le partage de localisation; revoir les paramètres de confidentialité; changer des mots de passe.

Voici des conseils généraux pour protéger vos appareils. Les mesures exactes peuvent varier d'un appareil à l'autre et évoluer au fil du temps.

Sur les appareils iPhone et iPad, vous pouvez trouver un paramètre en appuyant sur l'icône des réglages, puis en faisant glisser l'écran vers le bas pour afficher la barre de recherche. (Pour obtenir de l'aide, consultez la page https://support.apple.com/fr-ca/iphone.)

Sur les appareils Android, faites glisser l'écran d'accueil vers le haut : une barre de recherche indiquant « Rechercher dans votre téléphone et plus encore » s'affichera. Saisissez le réglage que vous recherchez dans la barre de recherche.

Déconnectez-vous de tous vos comptes

Vous êtes peut-être connecté à certaines applications sur plusieurs appareils. Pour vous déconnecter de *Facebook* sur tous les appareils, appuyez sur **les trois points horizontaux**, puis sur les paramètres [icône d'engrenage], ensuite sur « Mot de passe et sécurité », et enfin sur « Espace Comptes ». Appuyez sur « Mot de passe et sécurité » et ensuite sur « Appareils connectés ».

Vous verrez maintenant tous vos comptes *Facebook*, *Instagram* et *WhatsApp*. Appuyez sur chacun d'eux pour voir sur quels appareils vous êtes connecté, puis sélectionnez tous les appareils à déconnecter, sauf votre téléphone.

Clé des icônes

- l'icône des trois points horizontaux
- les paramètres l'icône d'engrenage
- l'icône des trois points verticaux
- la bascule

Désactivez le partage de localisation dans les médias sociaux

Cette action est importante si vous utilisez Snapchat, qui affiche votre localisation sur une carte. Pour désactiver cette fonction, ouvrez Snapchat et appuyez sur l'icône de votre profil. Appuyez ensuite sur l'**icône des trois points verticaux** dans le coin supérieur droit et faites défiler l'écran jusqu'à la section « Qui peut… ». Si vous appuyez sur « Voir ma position », une fenêtre contextuelle indiquant « Mode fantôme » s'affiche. Activez la fonction en faisant glisser **la bascule**.

Sur *Facebook* ou *Instagram*, vous pouvez désactiver la localisation en appuyant sur l'**icône d'engrenage**, puis sur « Confidentialité », ensuite sur « Services de localisation », et en faisant ensuite **basculer le bouton** situé à côté. La plupart des autres réseaux sociaux placent cette fonction à des endroits similaires, soit dans les paramètres de confidentialité ou de sécurité.

Passez en revue les paramètres de confidentialité

Tous vos comptes de réseaux sociaux proposent des paramètres de confidentialité, auxquels vous pouvez généralement accéder en appuyant sur l'**icône d'engrenage**, puis sur une option comme « Confidentialité », « Confidentialité et sécurité » ou « Public ». Assurez-vous d'activer seulement les publications que vos amis peuvent voir.

Modifiez vos mots de passe du stockage infonuagique

Si vous utilisez un système de stockage infonuagique pour vos photos ou vidéos, comme *iCloud* ou *Google Drive*, assurez-vous d'avoir modifié le mot de passe afin que personne d'autre ne puisse y accéder.

Habilo Médias

Avec le financement de

Agence de la santé publique du Canada | Public Health Agency of Canada

Naviguer en toute sécurité

Cette ressource fournit des conseils pratiques pour naviguer en ligne en toute sécurité afin d'éviter les formes courantes de traçage en ligne et couvre des actions comme : utiliser des navigateurs respectueux de la vie privée; naviguer en privé ou incognito; effacer l'historique; et se connecter à l'aide de courriels anonymes et de mots de passe fiables.

Voici des conseils généraux pour protéger vos appareils. Les mesures exactes peuvent varier d'un appareil à l'autre et évoluer au fil du temps.

Sur les appareils iPhone et iPad, vous pouvez trouver un paramètre en appuyant sur l'icône des réglages, puis en faisant glisser l'écran vers le bas pour afficher la barre de recherche. (Pour obtenir de l'aide, consultez la page https://support.apple.com/fr-ca/iphone.)

Sur les appareils Android, faites glisser l'écran d'accueil vers le haut : une barre de recherche indiquant « Rechercher dans votre téléphone et plus encore » s'affichera. Saisissez le réglage que vous recherchez dans la barre de recherche.

Utilisez un navigateur respectueux de la vie privée

Les navigateurs comme *Firefox* et *DuckDuckGo* ont été conçus dans le respect de la vie privée, de sorte qu'ils suivent vos activités le moins possible. Essayez l'un d'entre eux plutôt que le navigateur fourni avec votre appareil.

Naviguez de façon privée ou incognito

La plupart des navigateurs disposent d'un mode **privé** ou **incognito**. Ce mode empêche le navigateur lui-même d'enregistrer les sites que vous visitez, mais il n'empêche pas ces sites (ou votre fournisseur de service Internet ou d'autres applications sur votre appareil) d'enregistrer ce que vous faites.

Clé des icônes

mode privé ou incognito

l'icône d'engrenage

Naviguer en toute sécurité

Effacez votre historique

Recherchez l'historique sur votre appareil. Si vous disposez d'un compte Google, vous pouvez également effacer l'historique de Google et de YouTube. Consultez le site **https://myactivity.google.com** et désactivez les activités du Web et des applications, ainsi que l'historique de localisation et de YouTube.

Pour effacer l'historique de votre navigateur sur Safari, appuyez sur l'**icône d'engrenage**, puis sur « Safari » et « Effacer l'historique et les données des sites Web », ou recherchez les mots « Données des sites Web ».

Clé des icônes

mode privé ou incognito

l'icône d'engrenage

Connectez-vous à l'aide d'un courriel anonyme

Bon nombre de sites Web et de services vous demandent de fournir une adresse électronique pour vous inscrire. Si vous n'avez pas besoin de cliquer sur un lien de vérification, vous pouvez utiliser une fausse adresse électronique créée sur **www.sharklasers.com**.

Vous pouvez également créer une adresse *Proton Mail* gratuite, privée et sécurisée afin de ne pas avoir à utiliser une adresse que quelqu'un d'autre pourrait reconnaître.

Utilisez des mots de passe fiables

Vous pouvez créer un mot de passe fiable en commençant par une phrase facile à mémoriser (comme « J'aime les bananes »), puis en remplaçant certaines lettres par des chiffres ou des caractères spéciaux (comme des astérisques ou des points d'exclamation).

N'utilisez pas le même mot de passe pour différents comptes. Il est particulièrement important d'utiliser un mot de passe fiable et différent pour votre compte de messagerie principal puisque c'est là que seront envoyés les courriels de récupération de compte. Vous pouvez également utiliser un gestionnaire de mots de passe comme *1Password*. Assurez-vous alors que le mot de passe que vous utilisez est fiable et différent de tous vos autres mots de passe.

Habilo Médias

Avec le financement de

Agence de la santé publique du Canada | Public Health Agency of Canada