Sécurité technologique Canada

Téléphones

Une note sur la langue

Dans cette trousse, nous utiliserons parfois le mot femme et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif de la violence facilitée par la technologie sur les femmes et les filles. Nous reconnaissons que la VFGFT a également un impact sur les personnes trans, non binaires et bispirituelles. Nous espérons que toutes les personnes touchées par la VFGFT trouveront ces documents utiles.

Traiter les appels, les SMS et les messages de harcèlement

Options légales

Selon la méthode et l'ampleur du harcèlement, des recours juridiques peuvent être disponibles. Vous pouvez entamer des démarches juridiques (par exemple, un tribunal peut accepter une demande d'engagement de ne pas troubler l'ordre public). Cette ordonnance peut «maintenir la paix» et empêcher l'auteur de vous approcher ou de vous appeler. (Notez que si un engagement de ne pas troubler l'ordre public est enfreint, cela peut être considéré comme un crime.) Il existe d'autres options juridiques, comme une enquête de police, pouvant aboutir à une accusation criminelle et à des poursuites. Vous devez vous adresser à la police ou obtenir des conseils juridiques si vous souhaitez explorer ces options.

Signalement à la police

Si vous signalez le harcèlement à la police, celle-ci mènera une enquête pour déterminer si un crime a été commis, comme le harcèlement criminel, la traque furtive, ou d'autres comportements violents. Lorsque la police enquête, elle recueille et évalue les preuves qu'elle peut obtenir afin de déterminer s'il y a lieu de porter une accusation criminelle.

Vous pouvez aider la police en fournissant des preuves du harcèlement. Gardez à l'esprit que ces documents sont des éléments qui peuvent démontrer qu'un crime a été commis. La police devra également mener sa propre enquête.

Documenter le harcèlement

Que vous demandiez un engagement de ne pas troubler l'ordre public ou que vous signaliez l'incident à la police, il peut être utile de disposer d'une certaine documentation (captures d'écran ou enregistrement de la date, de l'heure, et des notes relatives à l'abus). Les preuves de harcèlement sont très importantes et la survivante est parfois la seule à y avoir accès. En fonction de la manière dont le harcèlement se produit ou de la plateforme technologique sur laquelle il a eu lieu, les messages peuvent être irrémédiablement supprimés.

Parlez à la police, à un·e avocat·e ou à une intervenante antiviolence de votre communauté pour savoir quel type de preuves aurait le plus de valeur légale dans votre cas. Vous approfondirez ainsi votre connaissance des lois et des procédures policières et judiciaires.

Le fait de documenter le harcèlement peut constituer une validation pour certaines personnes, mais pour d'autres, cela peut être un traumatisme ou un facteur déclenchant. Faites ce qui vous semble le mieux. Pensez à contacter une intervenante antiviolence ou un·e avocat·e pour envisager les prochaines étapes.

Pour plus d'informations, consultez notre fiche sur la documentation des preuves et le modèle de journal. Si vous n'êtes pas prête à parler à quelqu'un, consultez le document Preserving Digital Evidence Toolkit pour obtenir plus d'informations et des suggestions sur la façon de documenter les preuves et ce qu'il faut y inclure.

Signaler le harcèlement à l'entreprise en technologie

Vous pouvez également signaler le harcèlement à l'entreprise de technologie. La plupart d'entre elles ont des politiques qui interdisent le harcèlement. S'il est confirmé qu'une personne enfreint leurs politiques en harcelant quelqu'un par l'intermédiaire de leur plateforme, ils peuvent supprimer les contenus néfastes, demander à la personne de cesser ce comportement et, dans de rares cas, la bannir de la plateforme.

Fournisseur de téléphonie

Si le harcèlement se produit par le biais d'appels téléphoniques ou de SMS par l'intermédiaire d'un fournisseur de services téléphoniques, envisagez de faire un signalement.

Le signalement à votre fournisseur peut être une solution si le harcèlement n'est pas suffisamment grave pour que la police puisse enquêter. Dans un tel cas, la personne qui passe les appels ou envoie des messages peut découvrir qui a porté plainte, à savoir vous. Si vous ne voulez pas que l'auteur de violence sache qui a déposé la plainte, ce n'est **peut être** pas la meilleure solution.

Médias sociaux

Si le message de harcèlement est passé par un média social ou une appli de messagerie (comme Snapchat ou Facebook Messenger), vous pouvez le signaler à l'entreprise de médias sociaux. L'entreprise réagira au harcèlement selon ses conditions d'utilisation ou ses directives communautaires; dans certains cas, votre situation ne tombe pas sous le coup d'une interdiction. Si le harcèlement est interdit, l'entreprise peut retirer le contenu offensant et vous

encourager à bloquer la personne qui harcèle. Dans de rares cas, l'entreprise peut suspendre le compte de l'auteur du harcèlement.

Astuce: Documentez toujours le message et les informations du profil de la personne qui l'envoie ou le publie avant de le signaler et que l'entreprise le supprime. Une fois le contenu supprimé par l'entreprise, il disparaît à jamais.

Stratégies pour gérer les messages et appels de harcèlement

Recevoir des appels et des messages de harcèlement peut être très difficile à vivre. Vous pouvez avoir l'impression que la personne est constamment présente, que vous ne pouvez pas lui échapper et que la seule solution consiste à vous désengager de toute technologie pour ne plus être contactée. Bien que vous ne puissiez pas obliger quelqu'un à cesser de vous harceler, vous pouvez prendre certaines mesures pour atténuer le bombardement constant de l'auteur.

Bloquez l'auteur de violence

Une stratégie consiste à empêcher l'auteur de violence de vous contacter. Vous pouvez bloquer quelqu'un sur votre appareil mobile, par l'intermédiaire de votre fournisseur téléphonique, ou sur une plateforme de médias sociaux. Le blocage fonctionne différemment selon la plateforme ou l'appareil mobile, il est donc important de faire des tests pour savoir à quoi s'attendre, se familiariser avec la fonction et s'assurer que le blocage est efficace la plupart du temps. Testez la fonction de blocage avec une personne de confiance pour vérifier comment elle fonctionne.

N'oubliez pas que le blocage a ses limites. Lorsque vous bloquez quelqu'un, vous l'empêchez de vous contacter par un numéro de téléphone ou un compte de médias sociaux en particulier. Ces personnes peuvent toujours utiliser un autre numéro ou un autre compte. Cela peut également vous empêcher de voir ce qui est publié à votre sujet.

- **Appareils mobiles**
  Selon le type de téléphone que vous possédez, vous pouvez modifier vos paramètres pour bloquer quelqu'un et l'empêcher de vous contacter. En général, une fois le numéro bloqué, les appels ou les SMS provenant de ce numéro n'aboutissent pas. Le blocage sera toutefois différent sur chaque téléphone; par exemple, l'appareil peut bloquer les appels entrants, mais pas les SMS, ou la personne bloquée peut toujours laisser un message vocal, mais vous ne recevrez pas de notification. Si vous ne savez pas comment procéder, recherchez «comment bloquer un numéro» pour la marque et le modèle de votre téléphone sur une plateforme comme Google et, si possible, testez le blocage pour voir comment il fonctionne.

- **Médias sociaux**
  Si l'auteur de violence vous harcèle par le biais d'une appli de messagerie ou de médias sociaux, vous pouvez le bloquer. Chaque plateforme possède sa propre fonction de blocage et ses propres processus. Si vous ne savez pas comment procéder, recherchez «comment bloquer quelqu'un» à partir du média social concerné sur un moteur de recherche comme Google. La plupart des entreprises de médias sociaux disposent de directives dans leurs centres d'aide.

  En général, les entreprises de médias sociaux n'informent pas l'autre personne qu'elle a été bloquée. Cependant, l'auteur de violence peut s'en rendre compte lorsqu'il ne peut plus voir votre contenu ou vous envoyer des messages.

Autres Stratégies

Vous pouvez vouloir garder un certain contact avec l'autre personne parce que vous souhaitez continuer à recueillir des preuves du harcèlement. Parfois, le fait de savoir ce que fait et dit l'auteur de violence peut vous aider à déterminer si son comportement va s'intensifier ou non. Dans certains cas, vous devrez rester en contact pour communiquer au sujet des enfants, des animaux de compagnie ou d'autres problèmes communs.

Utiliser une sonnerie spécifique pour la personne violente

Si vous avez besoin de rester en contact, mais que la sonnerie du téléphone en vient à vous perturber, une solution consiste à utiliser une sonnerie spécifique pour cette personne. Ainsi, lorsque vous recevez d'autres appels, votre téléphone sonnera normalement. Mais lorsque l'auteur de violence appelle, la sonnerie spéciale va vous alerter, et vous pourrez décider de répondre ou de mettre votre téléphone en sourdine et de l'ignorer.

Laisser l'appel aller à la messagerie vocale

Une stratégie courante consiste à laisser la messagerie vocale répondre à l'appel. Cela vous permet de recueillir des preuves de harcèlement. En utilisant cette stratégie et en attribuant à la personne sa propre sonnerie, vous saurez si vous devez prendre l'appel ou le laisser aller sur la messagerie vocale.

Se procurer un deuxième téléphone

Une autre stratégie consiste à se procurer un deuxième téléphone. Vous pouvez utiliser un appareil pour communiquer avec l'auteur, et un autre pour tout le reste. De cette façon, vous restez en contact avec votre entourage, vous êtes munie d'un téléphone plus sécuritaire et vous n'êtes pas constamment bombardée de messages de l'auteur de violence.

Renvoyer les appels provenant d'un numéro de téléphone spécifique

Certaines compagnies de téléphone proposent une fonction qui vous permet de transférer les appels d'un numéro vers un autre. Vous pouvez transférer tous les appels et messages de l'auteur de violence vers un autre numéro, ce qui signifie que même s'il compose votre numéro, votre téléphone ne sonnera pas et vous ne recevrez pas les SMS de harcèlement.

Obtenir un nouveau numéro de téléphone ou un nouveau compte de médias sociaux

Dans certains cas, vous pouvez simplement décider de vous procurer un nouveau numéro de téléphone ou un nouveau compte de médias sociaux. C'est la meilleure option si vous voulez couper tous les liens, ne pas communiquer, et si vous pensez que l'auteur ne découvrira pas le nouveau numéro ou l'existence du nouveau compte de médias sociaux. Cette solution ne convient pas à tout le monde, car changer de numéro ou créer un nouveau compte de médias sociaux peut représenter beaucoup de travail.

Cette option présente une autre faiblesse. Selon votre situation, il peut être assez facile pour l'auteur de violence de découvrir votre nouveau numéro ou compte – en particulier si vous avez des ami·e·s en commun ou par le biais de

membres de votre famille – ou s'il a accès à vos comptes (courriel, etc.), aux bureaux ou aux organisations (bureaux de soins de santé, écoles, etc.) où vous avez mis à fourni votre nouveau numéro.

Rendre votre numéro privé

Si vous devez appeler l'auteur de violence, mais ne voulez pas révéler votre nouveau numéro, pensez à désactiver l'identification de l'appelant dans les paramètres de votre téléphone pour demeurer anonyme. Le destinataire verra apparaître sur son téléphone «Numéro privé» ou «Identification de l'appelant non disponible» lorsque son appareil va sonner.

Si vous ne voulez pas que votre numéro soit masqué en permanence, une autre option consiste à le faire appel par appel. Chaque compagnie de téléphone dispose d'un code que vous pouvez entrer avant de composer un numéro. Vous pouvez contacter votre fournisseur pour connaitre son code de blocage de l'identification de l'appelant.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Tech Safety Project de WESNET, d'après leur ressource Dealing with Harassing Call, Texts and Messages.

Guide des téléphones pour les survivantes: Améliorer la protection de la vie privée et réagir aux abus

Partie 1: Votre téléphone est-il utilisé pour vous nuire?

Malheureusement, les conversations et les informations sur les téléphones peuvent être utilisées à mauvais escient pour vous surveiller, vous contrôler ou vous harceler. **Faites confiance à votre instinct**. Si vous soupçonnez que quelqu'un surveille votre téléphone, voici quelques questions à se poser.

Est-ce que vous repérez des schémas?

La personne semble-t-elle tout savoir – à qui vous avez parlé, le contenu des conversations que vous avez eues au téléphone ou à proximité de votre téléphone, le contenu des SMS que vous avez envoyés et reçus, les endroits où vous allez – ou seulement des bribes de telles informations? En sachant lesquelles de vos activités font l'objet d'une surveillance, vous pourrez déterminer les mécanismes et les stratégies à envisager.

Qu'est-ce que l'auteur semble savoir?

Si l'auteur sait que vous avez eu une conversation, mais pas précisément ce que vous avez dit, écrit ou partagé, il a peut-être accès à votre historique d'appels, vos relevés de facturation ou à ce genre d'information sur votre compte. Il a aussi peut-être parlé avec la personne que vous avez appelée.

Si l'auteur connaît le contenu de vos publications, il se peut qu'il utilise d'autres appareils liés à vos comptes ou surveille votre appareil, ou encore que la personne qui a envoyé les messages les ait partagés ou transférés.

Si l'auteur semble savoir ce qui a été échangé lors de conversations ou conférences vidéo, mais qu'il n'était pas sur place pour entendre la conversation, et qu'il n'a pas pu être informé de ce qui a été dit, cette personne utilise peut-être un stalkerware. Attention: tout ce que vous faites sur votre téléphone, y compris la recherche d'informations ou la recherche de stalkerware, peut être épié. En savoir plus sur les stalkerware et sur la sécurisation de votre appareil.

Est-ce que la personne qui vous surveille a eu accès à votre téléphone?

La surveillance nécessite souvent un accès physique. La personne peut parcourir régulièrement votre téléphone pour voir qui vous a appelé et envoyé des SMS, ou peut avoir installé un stalkerware sur le téléphone lui permettant de suivre vos activités depuis un autre téléphone ou ordinateur. En ayant un accès physique à votre téléphone, il est également possible de télécharger des applis ou modifier les fonctions de compte et de sécurité, rendant vos informations vulnérables.

La personne a-t-elle accès à l'un de vos comptes infonuagique ou autre?

Une autre façon pour quelqu'un de surveiller votre utilisation est d'avoir accès à votre compte de téléphone ou à un compte infonuagique (par exemple Google ou Apple). Si leur nom figure sur le compte ou s'ils peuvent se faire passer pour vous ou un titulaire de compte autorisé auprès de la compagnie de téléphone, ils peuvent activer des fonctions telles que les services de localisation, accéder à vos dossiers de facturation en ligne et consulter vos historiques d'appels et d'autres informations.

L'auteur a-t-il tendance à savoir où vous vous trouvez?

Les téléphones et les applis peuvent révéler l'endroit où vous vous trouvez. Vérifiez les paramètres de votre téléphone et des différentes applis pour empêcher le partage de votre localisation. La plupart des téléphones disposent également d'une fonction de recherche d'un téléphone perdu. Cela peut révéler votre position à quelqu'un qui a accès à votre téléphone ou à votre compte. En savoir plus sur le suivi de la localisation au-delà des téléphones.

Partie 2: Si votre téléphone est surveillé

Il existe des mesures que vous pouvez prendre pour sécuriser votre téléphone, vos applis et vos comptes. Il n'y a pas une «meilleure» façon de réagir. Ce qui fonctionne pour certaines peut ne pas fonctionner ou être sécuritaire dans votre cas.

ATTENTION: Le fait d'apporter des changements attire souvent l'attention de l'auteur de violence. Il peut vous forcer à déverrouiller votre appareil ou à partager vos mots de passe. La violence peut s'intensifier. Les modifications apportées peuvent également effacer des preuves.

1. Réinitialisez le téléphone et les comptes. Une remise à l'état initial du téléphone peut désinstaller tout stalkerware installé contre votre gré ou à votre insu. Il est aussi important d'éviter de télécharger la sauvegarde d'un état précédent de l'appareil, afin que le stalkerware ne soit pas réinstallé.

Vous pouvez désinstaller toute appli inconnue et vérifier les applis et les paramètres qui autorisent le partage de la localisation. Appelez votre fournisseur de téléphonie mobile pour vous assurer que la géolocalisation est désactivée partout.

Réinitialisez les mots de passe (facturation du téléphone, nuage et autres comptes connectés) pour supprimer tout accès externe.

2. Remplacez votre téléphone. Si vous êtes en mesure de remplacer votre téléphone et que cela vous semble sécuritaire, faites-le ou procurez-vous un deuxième appareil. Voici quelques options:

- Achetez un nouveau téléphone, et envisagez de changer de fournisseur et d'obtenir un nouveau numéro. Demandez s'il existe des options supplémentaires pour renforcer la sécurité de votre compte, par exemple en clarifiant avec l'entreprise que vous êtes la seule titulaire autorisée du compte ou en configurant des notifications vous alertant de modifications à votre compte, notamment l'ajout ou la suppression de fonctionnalités.

- Achetez un téléphone à carte avec de l'argent liquide.

- Un proche ou un membre de la famille peut vous donner un ancien téléphone. Veillez à effacer la mémoire de l'appareil et à effectuer une remise à l'état initial pour supprimer toutes les informations.

Important: Ne connectez pas le nouveau téléphone à d'anciens comptes, en particulier les comptes infonuagiques comme Google ou iCloud, et n'utilisez pas votre ancien numéro. Ne transférez pas les données de votre ancien téléphone vers le nouveau en utilisant une carte mémoire, une carte SIM, votre compte infonuagique ou des sauvegardes précédentes. Cela pourrait réinstaller un stalkerware.

3. Soyez futée au sujet du téléphone surveillé. Certains auteurs de violence peuvent devenir plus agressifs lorsqu'ils n'ont plus accès à l'information et au contrôle. Vous pouvez envisager de garder le téléphone et de l'utiliser de manière stratégique pour ne pas éveiller les soupçons. Vous pouvez également conserver le téléphone surveillé comme preuve. Si vous gardez le téléphone, pensez à l'endroit où vous allez l'entreposer. Vous pouvez l'éteindre ou retirer la batterie. N'oubliez pas qu'une fois le téléphone rallumé, votre position sera visible si quelqu'un vous surveille par le biais d'un signal cellulaire ou Wi-Fi. Ce sont toutes des options à envisager et à aborder avec une intervenante antiviolence. Elle est là pour vous aider à planifier votre sécurité.

4. Parlez à vos proches et à votre famille. La famille et les proches peuvent partager l'endroit où vous êtes par inadvertance, ainsi que le nom des gens à qui vous parlez ou ce que vous faites dans les médias sociaux ou avec d'autres personnes. Si vous avez des enfants, apprenez-leur à ne pas partager votre localisation ou des informations sur vos activités personnelles.

5. Documentez ce qui se passe. Vous pouvez documenter les faits, si vous vous sentez en sécurité, en faisant des captures d'écran et en créant un journal des événements avant d'effectuer des changements. Vous avez la possibilité de partager toute information recueillie avec les forces de l'ordre ou un·e avocat·e, ou de les conserver. Le fait de documenter la violence peut également vous aider à créer ou mettre à jour un plan de sécurité. En savoir plus sur la documentation des abus.

Partie 3: Moyens d’accroître la sécurité et la confidentialité

1. **Utilisez un code d’accès sur votre téléphone.** La plupart des téléphones demandent un code d’accès à 4 chiffres, mais certains permettent de configurer un code plus complexe, un motif ou un verrouillage biométrique utilisant votre empreinte digitale ou la reconnaissance faciale. Si vous n’êtes pas en mesure de mettre un code d’accès sur votre téléphone ou si l’auteur de violence exige de le connaître, envisagez d’emprunter le téléphone d’une autre personne pour rechercher des informations sur la sécurité ou pour appeler une ligne d’urgence.

2. **Sécurisez les comptes de votre téléphone.** Vous avez généralement un compte avec la compagnie de téléphone et un compte infonuagique pour stocker les données personnelles (très probablement un compte Google ou iCloud). Passez en revue les paramètres de sécurité et envisagez de changer les mots de passe de votre téléphone et de vos comptes infonuagiques pour être la seule à pouvoir accéder à vos informations.

3. **Utilisez un logiciel antivirus et antispyware sur votre téléphone.** Vous pouvez rechercher des programmes réputés en ligne ou les trouver dans les magasins d’applis. Beaucoup ont des versions gratuites et peuvent vous protéger contre les stalkerware et autres applis malveillantes téléchargées sur votre appareil.

4. **Désactivez le partage de la localisation.** Les téléphones sont dotés d’un GPS intégré qui permet de localiser votre emplacement. Certains téléphones et applis partagent ces informations. Vous pouvez gérer le partage de votre localisation dans les réglages de votre téléphone, ou choisir les applis qui peuvent y accéder, ou vous pouvez désactiver complètement le partage de la localisation. Certaines applis vous permettent également de gérer le partage de votre localisation dans les paramètres.

5. **Vérifiez vos paramètres de sécurité et de confidentialité.** La plupart des téléphones disposent de paramètres qui vous aideront à gérer votre sécurité et votre confidentialité. Vous trouverez ces options dans les réglages du téléphone ou de l’appli. Pour en savoir plus, lisez nos conseils de sécurité et de confidentialité en ligne, et consultez nos guides concernant Facebook et Twitter pour en savoir plus sur leurs paramètres de sécurité et de confidentialité.

6. **Se déconnecter des applis et des comptes.** Pensez à vous déconnecter de vos comptes afin que l’on ne puisse pas y accéder si vous pensez que votre appareil est compromis. Il se peut que vous ne puissiez pas vous déconnecter de certaines applis sans les supprimer de votre téléphone. Il peut être moins commode d’accéder au compte par le biais d’un navigateur, mais prenez votre décision en fonction des risques pour votre sécurité et votre confidentialité.

7. **Passez en revue les applis téléchargées.** Si vous trouvez une appli inconnue, supprimez-la. Les applis sont faciles à télécharger et faciles à oublier, certaines d’entre elles peuvent aussi faire la collecte de vos informations personnelles. Toutefois, usez de prudence avant de supprimer une appli si vous craignez qu’il s’agisse d’un logiciel espion ou d’un stalkerware. Faites vos propres recherches sur les logiciels espions en utilisant un appareil plus sécuritaire.

8. **Évitez les téléphones débloqués (jailbreakés).** La suppression des restrictions imposées par le fabricant ou le fournisseur téléphonique rend les téléphones plus vulnérables aux logiciels espions et malveillants. Le fait de savoir si votre téléphone a été débloqué peut également indiquer que l’on a pu y installer une appli de surveillance.

9. **Utilisez des numéros de téléphone virtuels**. Envisagez d’utiliser un numéro de téléphone virtuel vous permettant de filtrer les appels, de recevoir des messages vocaux, de passer des appels ou d’envoyer des SMS sans partager le numéro de téléphone de votre appareil. Les numéros virtuels peuvent être liés à un compte infonuagique (par exemple, Google Voice). Assurez-vous que ce compte est également sécurisé.

10. Essayez de ne pas conserver d'informations sensibles sur votre téléphone. Moins vous avez d'informations sensibles sur votre téléphone, moins il est probable que l'on y ait accès. Il se peut que vous souhaitiez supprimer certains messages texte ou vocaux de votre téléphone et de comptes infonuagiques comme Google ou iCloud.

11. Si vous envisagez d'utiliser une appli de sécurité... Il existe de nombreuses «applis de sécurité personnelle» qui proposent d'améliorer la sécurité; certaines sont offertes spécialement aux victimes de violence. En savoir plus sur les applis de sécurité pour savoir si elles vous conviennent.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du *Safety Net Project* de NNEDV, d'après leur ressource *A Survivors Guide to Phones*.

Sécuriser un téléphone ou autre appareil lors de l'activation

Ce document vise à vous aider à configurer un appareil mobile avec un nouveau numéro. Parfois, les auteurs de violence détruisent les téléphones ou surveillent l'appareil «principal» d'une femme. De nombreuses femmes peuvent choisir de se procurer un deuxième téléphone pour appeler le 9-1-1 ou des services d'assistance en privé pendant qu'elles planifient ce qu'elles vont faire ensuite.

Il existe des situations uniques et des besoins de sécurité technologique qui ne sont pas couverts par ces conseils de base. Faites confiance à votre instinct. Si vous pensez avoir besoin de plus d'informations, notamment si l'auteur de violence s'y connait en technologie, consultez nos autres fiches d'information à www.techsafetycanada.ca.

Risques et avantages de la configuration et de l'activation d'un nouveau téléphone

Il est important de comprendre les risques et les avantages liés à l'acquisition d'un nouveau téléphone afin de planifier la meilleure manière de demeurer en sécurité. En voici quelques-uns.

Les risques comprennent:

- Un auteur trouve le nouveau téléphone et devient plus violent.
- Un nouveau compte de téléphonie peut être involontairement lié au compte d'un auteur de violence en raison de données similaires ou partagées (adresse, courriel, etc.). Il peut s'agir d'informations provenant d'un ancien appareil transférées sur le nouveau.
- Un auteur découvre qu'une survivante a fermé son compte de téléphone.
- Les abus financiers, qui peuvent affecter le crédit et rendre plus difficile l'accès à un téléphone.

Les avantages comprennent:

- Pouvoir appeler le 9-1-1, le personnel de soutien et les personnes de confiance sur un appareil sécuritaire
- Effectuer des recherches sur Internet ou d'autres activités sur l'appareil sans être surveillée
- Être capable de fuir et d'utiliser des services de localisation comme les cartes numériques
- Se sentir moins isolée

Si vous décidez de vous procurer un nouveau téléphone, voici quelques pistes de réflexion:

- Création de nouveaux comptes non liés (comme Google, iCloud ou Apple ID)
- Comment maintenir la batterie du téléphone chargée
- Comment conserver son crédit, et savoir quand il peut expirer
- Ce que vous pouvez dire et faire si un auteur de violence ou un enfant trouve le téléphone
- Utiliser les données du téléphone plutôt que le Wi-Fi de votre domicile, car il peut être surveillé
- Comment empêcher le téléphone de vibrer ou de sonner?

La principale chose à retenir lors de la configuration et de l'activation d'un nouveau téléphone, surtout si vous prévoyez continuer à utiliser votre appareil «principal», est de séparer tout ce qui concerne le nouveau téléphone et votre appareil «principal». Nous allons aborder certaines mesures de base que vous pouvez prendre. En fonction de votre situation et des connaissances technologiques de l'auteur ou de ses contacts, il peut être prudent de consulter nos guides plus détaillés pour Android ou iPhone avant d'acheter un nouveau téléphone.

En quoi la séparation des informations est une question de sécurité

Les histoires de sécurité technologique de Kristin et Joanna**

Kristin a acheté une nouvelle carte SIM ainsi qu'un nouveau téléphone et configuré le nouvel appareil avec le même fournisseur. Quelques jours plus tard, son partenaire l'a confrontée et lui a demandé avec colère pourquoi elle configurait un nouveau téléphone. Kristin n'avait pas réalisé que son mari était le titulaire légal de leur compte familial et qu'il était averti lorsqu'elle ajoutait un nouveau numéro de téléphone à son nom. Joanna a vécu une expérience semblable après avoir fourni son courriel à la compagnie de téléphone, sans se souvenir que son ex-mari violent pouvait accéder à son compte de messagerie et lire ses courriels entrants. Il a vu un message de la compagnie de téléphone l'informant que son nouveau compte avait été configuré avec succès.

**les noms ont été changés*

Processus simplifié, étape par étape, pour configurer et activer un nouveau téléphone en toute sécurité

1. Créez une nouvelle adresse courriel en utilisant un appareil auquel l'auteur n'a pas eu accès. Que le nouveau téléphone que vous vous procurez soit un iPhone ou un Android, cette adresse courriel peut être utilisée pour l'identifiant Apple, le compte iCloud, le compte Google, etc.

2. Mettez à jour les paramètres de sécurité et de confidentialité de votre nouveau compte courriel. Ajustez les paramètres en fonction de votre niveau de confort afin que vos contacts, votre localisation et d'autres informations personnelles ne soient pas collectés à votre insu. Protégez votre sécurité en étant sélective quant aux informations personnelles que vous partagez lors de l'installation.

3. Procurez-vous un nouveau téléphone qui ne soit pas un cadeau de l'auteur. Conservez les reçus, si possible.

4. Trouvez un nouveau fournisseur de services mobiles que l'auteur de violence n'utilise pas ou n'a pas utilisé, si possible. Séparez votre identité en insistant pour obtenir un nouveau numéro de compte et un nouveau numéro de téléphone pour cet appareil. Insistez auprès de la personne qui active le téléphone sur le fait que le compte est à votre nom et demandez que des mesures de sécurité supplémentaires soient activées, comme un code d'identification ou une vérification en deux étapes qu'un auteur ne peut pas deviner ou auxquels il ne peut pas accéder.

5. Obtenez un nouveau numéro de téléphone. Cela peut être difficile, et les besoins de chaque personne peuvent être différents. Le principal risque de conserver un ancien numéro et de le transférer sur un nouveau compte est que l'auteur de violence connait ce numéro. Cela peut entraîner du harcèlement ou même une usurpation d'identité pour reprendre le contrôle.

6. Obtenez une nouvelle carte SIM et une nouvelle carte SD. N'utilisez pas la nouvelle carte SIM ou SD de l'ancien téléphone ou l'ancienne carte SIM ou SD dans le nouveau téléphone. Gardez les appareils séparés. Cela peut nécessiter la saisie physique des contacts de l'ancien téléphone.

7. Explorez les fonctions de sécurité, de confidentialité et de connectivité de votre nouveau téléphone pouvant recueillir vos coordonnées, votre localisation ou toute autre information. Assurez-vous de vous entraîner à utiliser les fonctions du téléphone pour savoir comment le mettre en veilleuse, le recharger et y ajouter du crédit.

8. Utilisez de nouveaux verrous, codes d'accès et mots de passe complexes pour votre nouveau téléphone. Faites attention aux applis ou aux comptes auxquels vous accédez sur votre nouveau téléphone, car le titulaire d'un compte peut être averti d'une connexion à partir d'un appareil inconnu. Ne téléchargez des applis que sous votre nouvel identifiant Apple, votre compte iCloud, votre compte Google, etc.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Tech Safety Project de WESNET, d'après leur ressource Safely Setting Up and Activating A Phone or Other Device.

Guide de confidentialité et de sécurité pour iPhone

Veuillez noter: Ce document a été mis à jour en décembre 2022. Si vous avez un modèle ou un système d'exploitation plus récent, veuillez consulter le site d'Apple pour connaître les dernières fonctionnalités.

Apple ID:

La première fois que vous achetez un iPhone ou un iPad, vous devez créer un identifiant Apple. Cet identifiant est utilisé pour tout ce que vous faites avec Apple, y compris les achats dans iTunes ou l'App Store, l'accès aux services iCloud, l'utilisation d'iMessage ou de FaceTime, ou pour contacter l'assistance Apple. Votre identifiant Apple est généralement une adresse électronique – il peut s'agir d'une adresse courriel personnelle ou d'une adresse courriel se terminant par @icloud.com (également utilisée pour accéder à votre compte iCloud).

Il est possible d'ajouter d'autres identifiants Apple ou adresses courriel à votre compte. Pour voir quels courriels sont associés à votre compte, connectez-vous à l'aide de votre identifiant et de votre mot de passe Apple. Une fois connectée, vous pouvez supprimer les anciennes adresses courriel que vous n'utilisez plus et vous assurer qu'aucune autre adresse courriel n'a été ajoutée. Vous pouvez également mettre à jour vos mots de passe, vos questions de sécurité et autres informations de contact. Lorsque vous mettez à jour ou créez de nouveaux mots de passe, utilisez un mot de passe fort, que l'on ne peut pas deviner, et changez-le si vous soupçonnez que quelqu'un d'autre le connaît. Lire plus de conseils sur les mots de passe.

Services iCloud

La plupart des utilisateurs d'iPhone utilisent également les services iCloud d'Apple, un service infonuagique qui permet de stocker de la musique et d'autres fichiers, tels que des photos, des applis, des contacts, des courriels et des documents. Les documents créés dans des applis, tels que les présentations, les feuilles de calcul, les images et les PDF, peuvent également être enregistrés sur iCloud.

L'accès à iCloud peut se faire par le biais de tous les appareils Apple ou en se connectant au compte iCloud (généralement votre identifiant Apple) depuis un ordinateur. Si vous effectuez une sauvegarde de votre appareil sur iCloud, après avoir réinitialisé ou mis à jour votre téléphone, vous devez vous reconnecter à votre compte pour que toutes vos applis et tous vos paramètres soient automatiquement transférés sur votre appareil.

L'utilisation des services iCloud présente des avantages et des inconvénients. En revanche, si vous achetez un nouvel appareil ou si vous devez réinitialiser votre appareil, la connexion à l'aide de votre identifiant Apple mettra automatiquement à jour votre appareil, et va transférer vos applis tout en conservant vos paramètres habituels. Si vous utilisez iCloud Drive, vous pouvez également accéder à vos documents ou applis sur d'autres appareils en utilisant votre identifiant Apple. Toutefois, si vous configurez un nouvel appareil pour éviter d'être surveillée par un partenaire violent, la mise à jour de votre nouvel appareil avec les mêmes applis et paramètres peut s'avérer problématique. Voir Sécuriser un téléphone ou autre appareil lors de l'activation pour plus de détails.

D'autre part, l'utilisation d'iCloud signifie que vos informations sont accessibles à partir de plusieurs appareils plutôt qu'un seul. Les points d'accès multiples peuvent rendre vos informations plus faciles d'accès et par conséquent, plus vulnérables. Si quelqu'un connaît votre identifiant Apple ou votre nom d'utilisateur / mot de passe iCloud, cette personne il peut être en mesure d'accéder à vos données et informations.

Les mesures de sécurité et de confidentialité comprennent la modification du mot de passe de votre compte iCloud ou la restriction des informations que vous souhaitez rendre accessibles depuis le nuage. Pour accéder aux informations de votre iPhone ou iPad qui seront sauvegardées sur iCloud, allez dans Réglages / iCloud sur votre appareil et sélectionnez les données (Photos, Messagerie, Contacts, etc.) qui seront sauvegardées sur iCloud. Cette fonction vous permettra également de sélectionner ce que vous souhaitez enregistrer dans iCloud Drive.

Réglages de l’iPhone

L’iPhone lui-même comporte de nombreux réglages qui vous permettent de contrôler l’accès aux informations. Bien que cela prenne du temps, l’une des façons de s’assurer que votre téléphone est aussi privé et sécurisé que possible consiste à passer en revue chaque réglage. Cela vous permettra d’en connaître la fonction, le contrôle que vous avez réellement sur votre appareil et la quantité d’informations stockée sur votre appareil pouvant être surveillée. Il est préférable de passer en revue chaque réglage; voici quelques paramètres de confidentialité importants pour commencer.

Trouver mon iPhone

Si la fonction Trouver mon iPhone est activée, il est possible de localiser l’appareil en se connectant à iCloud. Cette fonction est destinée à vous aider à retrouver votre appareil s’il est perdu ou volé; toutefois, il est possible de l’utiliser pour localiser une autre personne. Les utilisatrices soucieuses de la confidentialité de leur localisation peuvent désactiver cette fonction sur leur appareil en allant dans Réglages / iCloud et en désactivant Trouver mon iPhone

Partage familial.

La fonction de partage familial permet à un maximum de 6 comptes différents de partager les achats iTunes, iBooks et App store, les photos et les vidéos, ainsi qu’un calendrier familial. Chaque personne doit être invitée et accepter l’invitation à faire partie du groupe de partage familial. L’organisateur familial est responsable du paiement des achats initiés par les autres membres de la famille et peut refuser des achats.

Le contenu acheté peut être partagé avec tous les membres du groupe.

Lorsque vous vous inscrivez au programme Partage familial, il vous sera demandé si vous souhaitez partager vos informations de localisation. Vous pouvez toujours désactiver cette fonction en allant dans Réglages / iCloud / Partager ma position; ce paramètre vous permet de déterminer quel membre de votre famille peut voir votre position.

Paramètres de localisation

De nombreuses applis demandent un accès à la localisation de votre iPhone/iPad. Dans la plupart des cas, vous pouvez contrôler les applis qui peuvent accéder à vos informations de localisation en allant dans Réglages / Confidentialité / Service de localisation. Vous pouvez y désactiver tous les services de localisation ou désactiver manuellement l’accès à la localisation pour certaines applis. Nous vous recommandons de désactiver l’accès à la localisation lorsque vous n’utilisez pas une appli. Vous pouvez toujours la réactiver au besoin.

Un autre réglage de localisation à examiner est celui des services système, dans lequel l’iPhone utilise vos informations de localisation pour d’autres fonctionnalités. Pour accéder aux services système, allez dans Réglages / Confidentialité / Service de localisation, faites défiler jusqu’en bas et sélectionnez «Services système». Minimiser l’accès aux informations de localisation de cette façon permettra également de préserver l’autonomie de la batterie.

Réglages de confidentialité

Certaines applis demandent d’accéder à vos contacts, calendriers, photos ou à votre appareil photo. Sous Réglages / Confidentialité, vous pouvez autoriser ou refuser l’accès des applis à d’autres informations sur votre appareil. Chaque

appli qui a demandé l'accès à des informations sur votre téléphone est répertoriée et vous pouvez contrôler les informations auxquelles elle a accès.

Réglages des applis

La liste de la plupart de vos applis se trouve à la fin de la rubrique Réglages de votre iPhone. Sous chaque appli, vous disposez de réglages de confidentialité additionnels. N'oubliez pas que la plupart des applis disposent de réglages de confidentialité, de sécurité ou de notification au sein même de l'appli. Passez en revue toutes les applis que vous avez téléchargées et assurez-vous que les paramètres sont réglés selon vos préférences.

FaceID, Touch ID et Code d'accès

Selon le modèle de votre iPhone, il y aura des options pour FaceID, Touch ID et le code d'accès sous Réglages généraux. Vous pouvez y mettre à jour votre FaceID, Touch ID et votre code d'accès. Vous devriez toujours utiliser un code d'accès afin d'empêcher que l'on fouille dans vos appareils lorsqu'ils sont sans surveillance. L'iPhone 5s ou ultérieur, l'iPad Pro, l'iPad Air 2 et l'iPad mini 3 ou ultérieur sont tous dotés de Touch ID, qui utilise votre empreinte digitale pour accéder à votre appareil. L'iPhone X ou ultérieur disposera de l'option FaceID, qui utilise un modèle mathématique de votre visage pour accéder à votre appareil. Outre les fonctions Face ID et Touch ID, vous pouvez également configurer un code d'accès personnalisé qui est soit un code numérique à 4-6 chiffres, soit un code numérique personnalisé (plus long que 4 chiffres), soit un code alphanumérique personnalisé (combinaison de chiffres et de lettres). Plus le code d'accès est complexe, plus il sera difficile à deviner.

Déverrouillage des iPhone

Certaines personnes vont débloquer leur iPhone (jailbreak), un processus qui supprime les restrictions imposées par Apple ou le fournisseur téléphonique sur l'appareil lui-même (le terme équivalent pour les appareils Android est «rooting»). Cela permet de télécharger des logiciels et des applications qui ne sont pas disponibles dans l'App Store d'Apple. Ce processus rendra le téléphone plus vulnérable aux malware et aux stalkerware. La plupart, sinon la totalité, des stalkerware dans le commerce nécessitent un iPhone débloqué pour être installés.

Une façon de savoir si votre iPhone est débloqué est d'accéder à la page de recherche Spotlight (balayez l'écran vers le bas) et de rechercher l'appli Cydia, qui est une indication possible que votre appareil pourrait être débloqué. Si votre téléphone est débloqué ou si vous soupçonnez que ce soit le cas, effectuez une restauration et assurez-vous que vous exécutez la dernière version d'iOS. Cela supprimera les logiciels qui ont été téléchargés en dehors de l'App Store d'Apple.

Conseils supplémentaires

Employez des mots de passe forts. Assurez-vous d'avoir un mot de passe fort et ne le partagez pas. Si quelqu'un apprend votre mot de passe, changez-le dès que possible.

Limitez l'accès à vos informations. Les appareils mobiles permettent d'accéder très facilement à vos informations à partir de plusieurs appareils. Mettez en balance la commodité et la confidentialité pour déterminer l'option la plus sécuritaire pour vous.

Déconnecter des comptes. Si vous n'utilisez pas une appli en particulier, pensez à vous déconnecter. Il peut être ennuyeux de devoir se reconnecter chaque fois que vous voulez l'utiliser, mais cela empêchera l'accès à vos comptes.

Ne partagez pas vos appareils. L'option la plus sécuritaire consiste à ne pas utiliser l'appareil d'une autre personne et à ne pas partager son propre appareil. Si vous devez emprunter l'appareil de quelqu'un, demandez à ce que vos informations soient supprimées une fois que vous avez terminé, par exemple le numéro que vous avez composé ou le SMS que vous avez envoyé. Si vous devez utiliser une carte virtuelle, accédez-y via un navigateur web et activez la fonction de mode privé. N'oubliez pas de vous déconnecter de tous les comptes auxquels vous avez accédé en utilisant l'appareil d'une autre personne.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. *Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.*
Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource iPhone Safety and Privacy Guide.

Guide de confidentialité et de sécurité pour appareil Android

Veuillez noter: Ce document a été mis à jour en décembre 2022. Si vous avez un modèle ou un système d'exploitation plus récent, veuillez *consulter le site d'Android pour connaître les dernières fonctionnalités.*

Les appareils mobiles stockent de nombreuses informations personnelles, notamment des comptes courriel ou de médias sociaux, des rappels et des notifications, le nombre de pas que vous faites chaque jour, et même des données biométriques personnelles comme les empreintes digitales et la reconnaissance faciale. Si tout cela peut faciliter la vie, les auteurs de violence et de harcèlement peuvent aussi utiliser ces informations pour surveiller, contrôler et harceler les victimes.

Ce guide vous aidera à renforcer la sécurité et la confidentialité lorsque vous utilisez un appareil Android. Bien que tous les appareils Android utilisent le même système d'exploitation (Samsung, Google, LG, Huawei, Motorola), les réglages de chaque marque peuvent être très différents. Ce document vise à servir de guide général, et non de marche à suivre détaillant chaque étape.

Il y a deux domaines à prendre en compte pour améliorer la sécurité et la confidentialité de votre appareil mobile: (1) les mécanismes de sécurité et de confidentialité intégrés à votre appareil (qui peuvent être légèrement différents selon la marque) et (2) le compte Google associé au téléphone (indispensable à tous les téléphones Android).

Réglages des appareils Android

Bien que chaque téléphone Android ait des réglages légèrement différents, il existe des paramètres de sécurité et de confidentialité standard vous permettant de mieux contrôler les informations contenues dans votre appareil. Même si cela prend du temps, l'une des façons de s'assurer que votre téléphone est aussi privé et sécurisé que possible consiste à passer en revue chaque réglage. Cela vous permettra d'en connaître la fonction, le contrôle que vous avez réellement sur votre appareil et la quantité d'informations pouvant être surveillée. Voici les principaux paramètres de sécurité et de confidentialité à utiliser pour commencer.

Verrouillage d'écran et codes d'accès

Le paramètre de sécurité le plus évident – et le plus important – par lequel vous devriez commencer est la sécurisation de votre téléphone Android avec un code d'accès. Cela empêchera quiconque de s'accaparer votre appareil à votre insu et de le fouiller. En fonction du modèle, vous aurez probablement le choix entre plusieurs options de code d'accès. Le plus courant est un code à 4 ou 6 chiffres. Les autres options comprennent un code numérique personnalisé, un code alphanumérique (combinaison de chiffres et de lettres) ou un motif. Certains appareils Android utilisent des options telles que la reconnaissance des visages ou des empreintes digitales pour le déverrouillage. Sur la plupart des Android, vous pouvez trouver les options de code d'accès sous Paramètres / Écran de verrouillage et sécurité.

D'autres disposeront de paramètres supplémentaires, permettant par exemple de décider si les notifications ou les raccourcis doivent être visibles lorsque votre téléphone est verrouillé. Le choix d'afficher ou non ces informations dépend de votre niveau de confort au cas où quelqu'un verrait ces informations sur votre appareil. Vous pouvez les trouver sous Paramètres / Écran de verrouillage et sécurité.

Smart Lock

Utilisez l'option Smart Lock pour déverrouiller votre téléphone si:

- Vous vous trouvez dans un «lieu de confiance», tel que votre domicile
- L'appareil mobile veut se connecter à un «périphérique de confiance», comme votre enceinte Bluetooth
- Vous portez le téléphone sur vous
- La personne qui regarde votre téléphone est reconnue comme un «visage de confiance»
- Votre appareil reconnaît votre voix comme une «voix de confiance»

Dans ces circonstances, votre téléphone se déverrouillera sans que vous ayez besoin de saisir un code d'accès. Si le verrouillage intelligent peut être pratique à utiliser – par exemple, lorsque vous jonglez avec des sacs et ouvrez une porte pendant que vous déverrouillez votre téléphone – il peut également permettre l'accès à une autre personne que vous. Réfléchissez à vos préoccupations en matière de protection de la vie privée et trouvez un équilibre entre la commodité, la sécurité et la confidentialité. Vous pouvez généralement trouver ce réglage sous Paramètres / Écran de verrouillage et sécurité / Paramètres de verrouillage sécurisé / Smart Lock.

Paramètres de localisation

La localisation est un autre paramètre que vous devez vérifier sur votre Android. Vous pouvez généralement le trouver sous la rubrique «Confidentialité et sécurité». Sous Paramètres de localisation, vous avez la possibilité d'activer ou de désactiver votre localisation pour toutes les applis. Grâce à ce paramètre, vous pourrez également voir quelles applis ont récemment demandé votre position. Si vous ne voulez pas que certaines applis aient accès à votre localisation, vous devrez les passer en revue et désactiver manuellement la localisation. Pour une plus grande confidentialité, n'activez la localisation que si nécessaire. Désactivez l'appli lorsque vous avez terminé, vous pourrez toujours la réactiver au besoin.

Dans vos paramètres de localisation, vous pouvez également décider de la manière dont votre position est accessible, que ce soit par GPS, Wi-Fi, réseaux mobiles, toutes ces options ou une combinaison de ces options. En général, c'est lorsque toutes les options de localisation sont activées que votre position est la plus précise. Cela peut s'avérer important si vous utilisez des applis de sécurité qui ont besoin de connaître votre position exacte. Certaines personnes peuvent choisir le GPS ou les réseaux mobiles uniquement, pour économiser leur batterie.

Paramètres Bluetooth

Un autre paramètre à désactiver si vous ne l'utilisez pas est le Bluetooth. Si vous vous êtes déjà connectée à un appareil Bluetooth, qui peut être votre voiture, des haut-parleurs portables ou même une imprimante, il peut se connecter automatiquement dès que vous êtes à portée. La désactivation du Bluetooth empêchera la connexion automatique et vous pourrez la réactiver lorsque nécessaire. Ce paramètre se trouve généralement sous Paramètres / Bluetooth.

Accès au contenu de l'appareil par les applis

Lorsque vous téléchargez une appli, vous recevez un message qui vous indique à quel contenu de votre appareil l'appli pourra avoir accès, comme les contacts, les calendriers, les photos, l'appareil photo, le microphone, les SMS, les capteurs, le stockage, etc. Sur la dernière version d'Android, vous pouvez sélectionner et choisir le contenu auquel une appli particulière peut avoir accès sous Paramètres / Applications / Permissions des applications. Sous chaque catégorie, vous verrez quelle appli veut accéder à quel contenu et vous pourrez activer ou désactiver l'accès. Sur les téléphones fonctionnant avec des versions plus anciennes, vous devrez peut-être accéder au gestionnaire d'applis et passer en revue chaque appli manuellement.

Dans certains cas, il se peut que vous n'ayez pas la possibilité de refuser l'accès d'une appli particulière au contenu de votre appareil, ou que l'appli puisse ne pas fonctionner correctement sans autorisation. Par exemple, Google Maps doit avoir accès à votre position pour vous donner des indications. Dans un tel cas, déterminez si cela en vaut vraiment la peine, en considérant l'utilité de l'appli.

Installation d'applis de sources inconnues

Un autre paramètre à activer est l'interdiction d'installer sur votre appareil des applis ne provenant pas du Google Play Store. Contrairement à l'iPhone, votre téléphone Android vous permet d'installer des applis en dehors du Google Play Store, par exemple à partir d'un site web ou via votre ordinateur. C'est souvent de cette manière que les malware et les stalkerware sont installés, il est donc important de désactiver cette fonction. Vous pouvez trouver ce paramètre sous Écran verrouillage et sécurité / Sources inconnues.

Cryptage

Votre appareil est probablement déjà crypté par le fabricant si vous utilisez Android version Marshmallow ou ultérieure. Sinon, vous pouvez toujours accroitre votre sécurité en activant le cryptage, sous Paramètres / Sécurité / Cryptage. Avec un téléphone crypté, il sera plus difficile pour quelqu'un d'accéder à vos données, à moins de disposer de la clé de cryptage, qui est généralement votre code d'accès.

Vous pouvez également choisir de crypter votre carte SD (même si votre téléphone est déjà crypté). Vous pouvez généralement trouver ce paramètre sous Écran verrouillage et sécurité / Cryptage de la carte SD. Notez que les cartes SD cryptées ne peuvent être lues que sur l'appareil utilisé pour les crypter.

Sauvegarde et réinitialisation

Les téléphones Android offrent de nombreux moyens de sauvegarder vos données. La fonction Sauvegarde et restauration de Google ne se contente pas de sauvegarder le contenu de votre téléphone. Elle sauvegarde également toutes les données de vos applis Google, telles que l'agenda, le navigateur Chrome, les contacts et les photos. Une fois les données sauvegardées, en cas de configuration d'un nouveau téléphone, il vous suffit de vous connecter avec votre compte Google et toutes vos données seront synchronisées. Bien qu'incroyablement pratique, il importe de s'assurer que votre compte Google est sécurisé. Profitez de la vérification en deux étapes de Google pour recevoir une notification si quelqu'un se connecte à votre compte.

Une autre méthode pour sauvegarder les données de votre compte consiste à utiliser des services en ligne, tels que Google Drive ou Dropbox pour sauvegarder vos photos ou vos vidéos. Là encore, bien que ces services soient pratiques et utiles pour libérer de l'espace sur votre Android, assurez-vous que votre compte est sécurisé avant de les utiliser.

Compte et services Google

Le système d'exploitation mobile Android étant conçu par Google, votre appareil Android est intimement lié à la plateforme Google. Pour acheter des applis via le Google Play Store, vous devez disposer d'un compte Google. Ce compte sera également utilisé pour tous les autres produits et services Google sur l'appareil, notamment Gmail, l'agenda, les contacts, le navigateur Chrome et YouTube. Avoir tous ces services reliés à un seul compte peut être pratique. Par exemple, lorsque vous consultez un site web sur le navigateur Chrome de votre Android, le navigateur Chrome de votre ordinateur personnel s'en souviendra dans son historique. L'historique de votre navigateur est enregistré sur votre compte, ainsi que sur l'appareil en tant que tel.

En fonction de votre situation, vous pouvez souhaiter qu'un seul compte relie vos informations sur plusieurs appareils, ou vous pouvez exiger plus de confidentialité et ne pas vouloir que vos informations soient mémorisées ou synchronisées sur plusieurs appareils. Si tous ces services sont regroupés sous un seul compte Google et que quelqu'un y accède, une quantité considérable d'informations sur votre téléphone seront à sa portée. La bonne nouvelle est que Google offre de nombreuses options de confidentialité. Vous trouverez ci-dessous quelques suggestions pour augmenter la confidentialité et réduire les connexions.

Passez par les paramètres de Google

Les paramètres Google vous offrent plusieurs options pour améliorer votre sécurité et votre confidentialité lors de l'utilisation de ces produits. Vous pouvez accéder aux paramètres sur votre Android en allant dans Paramètres / Google. Vous pouvez également y accéder en ligne via un navigateur web à l'adresse https://myaccount.google.com. Nous vous suggérons de passer en revue tous les paramètres. C'est la meilleure façon d'accroitre la sécurité et la confidentialité de vos informations. Un moyen simple consiste à passer par le Check Up Sécurité de Google ainsi que par le Check Up Confidentialité (les deux peuvent être effectués à partir des paramètres de votre téléphone ou via votre navigateur). Vous trouverez ci-dessous quelques paramètres à parcourir, mais n'oubliez pas que cette liste n'est pas exhaustive. Nous vous encourageons vivement à passer en revue tous vos paramètres Google afin de satisfaire vos besoins en matière de sécurité et de confidentialité.

Réduire la collecte de l'activité des périphériques par Google

Une façon d'empêcher Google de collecter vos informations est de passer par «ne collecte pas votre activité» en vous rendant sur Paramètres / Google / Infos personnelles et confidentialité / Contrôles d'activité. Vous pouvez y définir vos préférences concernant les activités dont Google se souvient et qu'il enregistre sur votre compte (Activité Web et applications, Historique de la localisation, Informations sur les appareils, Activité vocale et audio, Historique des recherches sur YouTube et Historique des visionnements sur YouTube). Choisissez «pause» pour empêcher Google de collecter ces informations. Gardez toutefois à l'esprit que l'interruption du suivi de l'une des activités susmentionnées ne supprime pas les activités précédemment enregistrées. Vous devez les supprimer séparément dans les paramètres de l'activité de révision. Vous pouvez y accéder en allant dans Paramètres / Google / Infos personnelles et confidentialité / Mon activité. N'oubliez pas que, même si le paramètre est désactivé, Google peut continuer à suivre temporairement certaines de vos activités (par exemple, les recherches sur Internet afin d'améliorer la qualité de votre session de recherche actuelle).

Accordez une attention particulière à l'historique de localisation

Un autre élément à désactiver est l'historique de localisation. Lorsque cette option est activée, Google suivra tous vos déplacements via votre appareil mobile (ce qui est différent de l'utilisation de Google Maps). L'objectif est de permettre à Google d'optimiser les recommandations en matière de recherches cartographiques, entre autres. Cependant, si quelqu'un accédait à votre compte Google, il pourrait voir tout ce que vous avez fait (et éventuellement prédire où vous irez). Déterminez si les risques que représente le fait que l'on puisse savoir où vous allez l'emportent sur la commodité d'une recherche rapide sur une carte ou d'une recommandation de Google basée sur votre position actuelle. Désactivez l'historique des positions en allant dans Paramètres / Infos personnelles et confidentialité / Vos informations personnelles / Partage des positions.

Trouver mon Téléphone

De nombreuses personnes utilisent la fonction «Trouver mon téléphone» pour localiser leur appareil en cas de perte ou de vol. Toutefois, une personne ayant accès à votre compte Google pourrait s'y connecter et savoir où se trouve votre téléphone grâce à cette fonctionnalité. C'est à vous de décider si vous voulez utiliser ce paramètre. Considérez la sécurité de votre compte Google et la probabilité que l'on puisse l'utiliser pour vous localiser, par rapport au réconfort de savoir que votre téléphone peut être retrouvé en cas de vol ou de perte.

Supprimer les applis et les appareils connectés

Vous pouvez vous connecter à votre compte Google à partir de plusieurs appareils (un appareil Android, un ordinateur portable, etc.). Pour vous aider à gérer ces différentes connexions, Google vous indique les appareils présentement connectés, ou ceux qui ont accédé à votre compte au cours des 28 derniers jours. Vous trouverez cette information dans les paramètres de votre téléphone, sous Google / Connexion et sécurité / Appareils récemment utilisés. S'il y a des appareils que vous ne reconnaissez pas ou si vous vous êtes connectée quelque part et avez oublié de vous déconnecter, c'est ici que vous pouvez interrompre l'accès de ces appareils. Cette fonction est également utile si vous perdez votre Android et devez déconnecter l'appareil de votre compte Google.

N'oubliez pas que votre compte Google peut également être connecté à d'autres comptes, comme des applis ou d'autres services en ligne. À moins de savoir que votre compte Google est sécurisé et que vous êtes à l'aise de vous connecter à d'autres comptes, il est généralement préférable de créer un nouveau nom d'utilisateur et de nouveaux mots de passe lorsque vous accédez à d'autres comptes en ligne. Toutefois, si vous choisissez d'utiliser votre compte Google, vous pouvez vérifier à quelles applis ou quels comptes il est connecté. Allez dans Paramètres / Connexion et sécurité / Apps et sites connectés pour vérifier ou supprimer l'accès à des applis ou des comptes.

Se déconnecter des produits Google sur votre Android

Si certains services Google, tels que Gmail ou le Google Play Store, exigent que vous vous connectiez pour y accéder, ce n'est pas le cas de tous les produits Google. Lorsque vous êtes déconnectée, ce que vous faites sur ces applis ne sera pas enregistré dans votre compte Google. Cependant, souvenez-vous que si votre compte Google n'enregistre pas vos activités, l'appli sur votre Android s'en souviendra. Par exemple, si vous n'êtes pas connectée lorsque vous utilisez l'appli Chrome sur votre Android, votre compte Google ne retiendra pas les sites Web que vous avez visités, mais votre historique de navigation sera enregistré à même l'appli Chrome de votre Android. Si vous ne voulez pas laisser de traces, pensez à supprimer l'historique de navigation dans Chrome ou à utiliser le mode Incognito.

Sécurité supplémentaire pour Android

Applications de sécurité

Bien que le téléphone Android lui-même dispose de paramètres de sécurité intégrés, vous pouvez également télécharger une appli de sécurité. Les applis de sécurité provenant de tierces parties offrent un large éventail de fonctionnalités, notamment la protection contre les malware et les virus, la localisation de votre téléphone en cas de perte ou de vol, ou la suppression à distance de toutes les données de votre téléphone.

Vous pouvez également télécharger des applis antimalware qui protégeront votre téléphone contre les virus ou empêcheront l'installation de logiciels malveillants. Selon le type d'appareil Android que vous possédez, il est possible qu'il soit déjà muni d'une protection antivirus. Si ce n'est pas le cas (ou si vous souhaitez explorer d'autres options), vous pouvez vous rendre sur le Google Play Store et rechercher des applis qui vous protègent des malware. Une autre façon de trouver de bons antivirus consiste à chercher sur Google «les meilleurs antivirus pour Android» et de lire les commentaires.

Lorsque vous téléchargez des applis depuis le Google Play Store, lisez les critiques. Plus la note est proche de 5 étoiles, mieux c'est, mais regardez aussi combien de personnes ont téléchargé l'appli et lisez quelques critiques.

«Rooter» votre Android

Certaines personnes «rootent» leur Android, un processus qui permet de modifier le code du système d'exploitation et d'installer d'autres logiciels bloqués par le fabricant (le terme équivalent pour les appareils Apple est déblocage ou «jailbreaking»). Malheureusement, un téléphone *rooté* peut être plus vulnérable aux malware et aux stalkerware, annuler votre garantie et rendre impossibles les mises à jour de votre système d'exploitation. Ces mises à jour sont importantes, car elles peuvent inclure des correctifs de sécurité et rendre votre téléphone moins vulnérable au piratage. Une façon de savoir si votre Android est *rooté* consiste à télécharger une appli de vérification (root-checker) depuis le Google Play Store. Pour «*dérooter*» votre téléphone, recherchez les directives en ligne sur Google, car il existe plus d'une façon de faire.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project de WESNET, selon leur ressource *Android Safety and Privacy Guide*.

Ce document fait partie du projet Sécurité technologique Canada d'Hébergement femmes Canada. Nous vous encourageons à visiter le site www.securitetech.ca pour trouver des informations et des ressources supplémentaires sur la violence facilitée par la technologie, la planification de la sécurité technologique et la préservation des preuves numériques. Ce document, ou toute partie de celui-ci peut être reproduit ou utilisé à condition de citer la source. Si vous souhaitez adapter le contenu, veuillez contacter Hébergement femmes Canada à l'adresse info@endvaw.ca.

© copyright 2023 Hébergement femmes Canada | Tous droits réservés

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).