Sécurité technologique Canada

Stalkerware et géolocalisation

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.

Guide de sécurité: Stalkerware pour téléphones

Qu'est-ce qu'un stalkerware?

Le terme stalkerware désigne des outils – applis, logiciels et appareils – qui permettent à quelqu'un de surveiller secrètement votre activité téléphonique.

Les stalkerware peuvent surveiller presque tout ce que vous faites sur votre téléphone, y compris les photos et les vidéos que vous prenez, les sites Web que vous visitez, les messages que vous envoyez et recevez, l'historique de vos appels et votre localisation. Ils peuvent permettre d'activer la webcam ou le microphone, de faire des captures d'écran, de voir l'activité sur des applis tierces (comme Snapchat ou WhatsApp) et d'intercepter, de transférer ou d'enregistrer des appels téléphoniques.

Presque tous les stalkerware nécessitent un accès physique à l'appareil. Une fois installés, ils fonctionnent en mode furtif sans qu'aucune notification ou activité ne soient visibles, ce qui les rend difficiles à détecter ou à supprimer. Pour accéder à votre activité téléphonique, la personne qui vous surveille se connecte à un site Web ou à une appli sur un autre appareil. L'auteur peut également recevoir des notifications de certaines activités, telles que des copies de SMS ou une alerte indiquant que vous êtes en communication, afin de pouvoir se joindre secrètement et vous épier.

Comment savoir si un stalkerware est présent sur mon téléphone?

La détection peut être difficile. Il peut s'agir d'une batterie qui se vide rapidement, d'un appareil qui s'éteint et se rallume, ou d'augmentations soudaines dans l'utilisation des données. Le comportement suspect de l'auteur de violence est le signe le plus courant que votre activité est surveillée. Il peut en savoir trop sur vos activités téléphoniques, par exemple. Faites confiance à votre instinct et cherchez des schémas. Une vérification professionnelle de l'appareil est peut-être le seul moyen de détecter la présence d'un stalkerware.

Réagir aux Stalkerware

La sécurité avant tout. Avant de chercher ou d'essayer de supprimer un stalkerware, pensez à votre sécurité. Certains auteurs peuvent intensifier leur comportement violent lorsque le logiciel qui facilite le harcèlement est supprimé. Vous pouvez aborder la planification de la sécurité avec une intervenante antiviolence.

Si vous soupçonnez la présence d'un stalkerware, ce que vous faites sur votre téléphone pourrait être vu par d'autres personnes. Pour les appels ou les activités où vous souhaitez plus de confidentialité, utilisez un téléphone ou un autre appareil non surveillé. Il peut s'agir du téléphone d'une amie ou d'un ordinateur à la bibliothèque, à l'école ou au travail.

Documenter le Stalkerware

Vous pouvez prendre des notes sur ce que vous vivez. Notre fiche d'information sur la documentation de la violence numérique et notre exemple de journal de la violence facilitée par la technologie vous fourniront des informations utiles.

Sinon, en temps opportun, la police ou des spécialistes en criminalistique pourront rechercher des preuves sur votre appareil. Il peut également être utile de lire la trousse à outils de sauvegarde des preuves numériques d'HFC sur un appareil non surveillé pour obtenir des conseils utiles.

Supprimer le Stalkerware

Dans la plupart des cas, une remise à l'état initiale du fabricant peut supprimer le stalkerware. Cependant, la réinstallation d'applis ou de fichiers à partir d'une sauvegarde peut les réinstaller sur l'appareil. En plus de la remise à l'état initial, vous pouvez également créer un nouveau compte iCloud ou Google afin de repartir à zéro, sans possibilité de réinstallation du logiciel de harcèlement.

Prévenir les stalkerware

- **Pensez à l'accès.** Soyez prudente si quelqu'un veut mettre à jour ou utiliser votre téléphone. Un stalkerware est vite installé. Faites confiance à votre instinct. Méfiez-vous d'un nouveau téléphone ou d'une nouvelle tablette que vous offre l'auteur de violence, à vous ou à vos enfants.
- **Mettez vos comptes à jour.** Changez les mots de passe et mettez en place une vérification à deux facteurs. En savoir plus sur la sécurité des mots de passe.

- **Verrouillez votre téléphone.** Étant donné que la plupart des stalkerware ont besoin d'un accès physique pour être installés, mettez en place un code de sécurité sur votre téléphone (et ne le partagez pas) pour minimiser les risques. De nombreux appareils vous permettent de choisir entre un numéro, un motif, une empreinte digitale ou d'autres modalités pour la sécurité. Lire plus de conseils de sécurité téléphonique.
- **Utilisez un antivirus.** Téléchargez des applis de sécurité; elles peuvent contribuer à empêcher l'installation de stalkerware et détecter les malware.
- **Utilisez les fonctions de sécurité.** Consultez les paramètres de sécurité en détail, pour savoir tout ce que vous pouvez faire. Les téléphones Android autorisent les installations à partir de «sources inconnues»; assurez-vous que cette option est désactivée. Installez toujours les dernières mises à jour pour votre téléphone et vos applis. Ne pas le faire peut les rendre plus vulnérables aux problèmes de sécurité et de confidentialité.
- **Ne pas effectuer de «root» (Android) ou de «jailbreak» (iPhones) sur votre téléphone.** «Rooter» ou «jailbreaker» un appareil signifie supprimer les limitations du système d'exploitation pour permettre des installations tierces (celles qui ne figurent pas dans les App Store). Cela a un impact sur les fonctions de sécurité intégrées conçues pour protéger l'appareil et le rend vulnérable. La plupart des fonctions les plus invasives des stalkerware ne fonctionnent que si les protections mises en place par le fabricant sont contournées. Sur les iPhone, la plupart ne peuvent être installés que si l'appareil est jailbreaké. Un téléphone *rooté* ou *jailbreaké* sera plus vulnérable aux virus et aux logiciels malveillants, ce qui facilitera l'installation de stalkerware.

Quand ce n'est pas un stalkerware

Il existe de nombreuses autres méthodes pour accéder à des informations sur votre téléphone ou connaître vos activités sans installer de stalkerware. Si l'auteur de violence a un accès physique au téléphone ou à vos comptes en ligne, il n'aura peut-être pas besoin d'installer un stalkerware pour vous surveiller. Parfois, l'auteur passe par des proches et des membres de la famille pour recueillir des informations. Identifiez des schémas dans ce que la personne sait et les endroits d'où peuvent provenir ces informations pour vous aider à découvrir ses stratégies. Une intervenante antiviolence peut vous aider à comprendre ce qui vous arrive et à planifier les prochaines étapes.

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, selon leur ressource *Stalkerware: Phone Surveillance & Safety for Survivors*.

Logiciel espion ou stalkerware: Surveillance et sécurité sur l'ordinateur

Que sont les logiciels espions ou stalkerware?

Les logiciels espions ou stalkerware désignent des outils – applis, logiciels et appareils – qui permettent à une personne non autorisée (comme un auteur de violence) de surveiller et d'enregistrer secrètement des informations sur votre ordinateur. Le terme stalkerware est un terme plus récent qui attire l'attention sur l'utilisation abusive, intrusive et dangereuse de ces outils.

Les stalkerware peuvent suivre et enregistrer presque tout ce que vous faites sur votre ordinateur, y compris chaque frappe au clavier, chaque site web visité, le clavardage et les messages instantanés envoyés ou reçus, ainsi que chaque document ouvert. Certains stalkerware peuvent également permettre d'activer la webcam ou le microphone, de faire des captures d'écran, de faire parler l'ordinateur ou d'émettre d'autres bruits, ou encore d'éteindre ou de redémarrer l'ordinateur. L'auteur de violence peut voir vos activités ou les contrôler à distance, généralement via le tableau de bord d'un site web ou d'une appli.

La plupart des stalkerware peuvent être installés à distance, généralement par l'envoi d'un courriel ou d'un message contenant un fichier joint ou un lien. Le logiciel espion s'installe automatiquement lorsque vous cliquez sur le lien ou ouvrez la pièce jointe. Certains stalkerware peuvent être envoyés par le biais d'un message instantané, d'un jeu vidéo ou d'autres stratagèmes pour vous inciter, vous ou vos enfants, à ouvrir la pièce jointe ou à cliquer sur un lien. Une fois installé, il fonctionne en mode furtif sans aucune notification ni activité pouvant révéler son existence, ce qui le rend difficile à détecter ou à supprimer.

Si la plupart des stalkerware sont installés sous forme de logiciels, il existe également des dispositifs analogues d'espionnage appelés enregistreurs de frappe. Ces dispositifs peuvent ressembler à des composantes normales de l'ordinateur; par exemple, il peut s'agir d'un clavier spécial avec des capacités d'enregistrement des frappes ou d'un dispositif près du fil qui relie le clavier à l'ordinateur. Une fois branché sur l'ordinateur, il enregistre chaque touche tapée, ce qui peut inclure les mots de passe, les numéros d'identification personnels (NIP) et les sites web visités. Certains dispositifs analogues permettent l'espionnage à distance, tandis que d'autres exigent que l'auteur dispose d'un accès physique à l'ordinateur pour être en mesure de vous espionner.

Comment savoir si un stalkerware se trouve sur mon ordinateur?

La détection des stalkerware sur votre ordinateur peut être très difficile. Dans la plupart des cas, l'ordinateur va continuer de fonctionner (par exemple, votre ordinateur ne sera pas nécessairement ralenti ou figé). Toutefois, même sans que cela se produise, vous pouvez soupçonner que votre activité est surveillée en raison du comportement suspect de l'auteur. Faites confiance à votre instinct et identifiez des schémas. Si l'auteur de violence en sait trop sur votre activité numérique ou sait des choses que vous n'avez faites que sur votre ordinateur ou votre téléphone, il se peut qu'un stalkerware soit installé sur votre appareil.

Si un périphérique a été installé, vous pouvez voir un composant supplémentaire entre l'ordinateur et le fil du clavier, ou vous pouvez avoir reçu un nouveau clavier ou une nouvelle souris. Sur les ordinateurs portables, un dispositif analogue peut être plus difficile à détecter puisqu'il sera installé à l'intérieur de l'ordinateur, par le biais du panneau d'accès.

Réagir aux stalkerware

La sécurité avant tout. Avant de vous mettre à chercher ou à supprimer un stalkerware, il est important de prendre en compte la sécurité et de saisir l'occasion de recueillir des preuves. Étant donné que de nombreux auteurs de violence utilisent des stalkerware pour surveiller et contrôler les femmes, le harcèlement et la violence peuvent s'intensifier s'ils soupçonnent que la femme l'a retiré d'un appareil. Avant de le supprimer, réfléchissez à votre sécurité en envisageant des moyens de vous protéger. Parlez avec une intervenante antiviolence de la planification de votre sécurité. Pour trouver du soutien consultez le site www.hebergementfemmes.ca.

Rassembler les preuves

Les forces de l'ordre ou un spécialiste en criminologie informatique peuvent vous aider si vous souhaitez préserver les preuves nécessaires à une enquête criminelle ou à une action en justice civile. Les outils dont disposent les forces de l'ordre peuvent être seuls à pouvoir déterminer avec certitude la présence d'un stalkerware sur un ordinateur. Pour en savoir plus, consultez le document d'HFC intitulé Trousse à outils pour la sauvegarde des preuves numériques.

Utilisez des appareils non surveillés. Si vous soupçonnez la présence d'un stalkerware sur votre appareil, n'oubliez pas que toute activité, y compris les discussions en ligne, les courriels et les recherches sur Internet, peut être révélée à l'auteur des faits. Si vous le pouvez, utilisez un ordinateur ou un appareil plus sécuritaire – auquel l'auteur n'a pas d'accès physique ou à distance – lorsque vous recherchez de l'aide ou des informations. Il peut s'agir d'un ordinateur de bibliothèque publique ou de centre communautaire, ou de l'appareil d'une amie.

Supprimer les stalkerware

Les stalkerware peuvent être très difficiles à supprimer une fois installés. Vous pouvez envisager de nettoyer l'ordinateur et de le remettre à neuf, en commençant par réinstaller le système d'exploitation, bien que cela ne garantisse pas la suppression de logiciels malveillants. Une autre option consiste à remplacer le disque dur ou à vous procurer un nouvel ordinateur. Veillez à ne pas copier les fichiers ou les documents de l'ordinateur infecté sur le nouveau, ce qui pourrait réinstaller les stalkerware dissimulés dans des fichiers. Utilisez les services infonuagiques pour entreposer les documents de l'ordinateur infecté.

Mise à jour des comptes

Si vous pensez qu'un stalkerware a permis à l'auteur d'accéder à vos informations de connexion (comme pour ouvrir une session), envisagez de réinitialiser vos mots de passe sur un autre appareil et de cesser de vous connecter à certains comptes à partir de l'ordinateur que vous croyez surveillé. Veillez également à changer les mots de passe des comptes sensibles tels que les comptes bancaires et les comptes de médias sociaux. En savoir plus sur la sécurité des mots de passe.

Prévention des stalkerware

Pensez à l'accès. Méfiez-vous si quelqu'un vous propose d'utiliser un nouveau clavier, fil ou logiciel, ou encore, si l'on vous incite à mettre à jour ou «réparer» l'ordinateur ou le téléphone, surtout si cela coïncide avec une augmentation de la surveillance ou des abus. Méfiez-vous des cadeaux que l'auteur de violence vous offre, à vous ou à vos enfants, tels que de nouveaux téléphones, ordinateurs, claviers ou jeux.

Créez des comptes d'utilisateur ou d'invité distincts. Vous pouvez créer des comptes d'invités ou un compte d'utilisateur dont les paramètres ne permettent pas d'installer des logiciels ou des applis sans la connexion de l'administrateur. Cela peut empêcher l'installation accidentelle de stalkerware ou d'autres logiciels malveillants si vous ou une autre personne utilisant votre ordinateur clique sur un lien ou ouvre un fichier.

Utilisez un antivirus sur votre téléphone. Installez des antivirus ciblant les stalkerware, assurez-vous qu'ils sont à jour et configurez-les pour qu'ils analysent régulièrement votre ordinateur. Ces programmes peuvent contribuer à empêcher l'installation de stalkerware, et ils obtiennent de meilleurs résultats avant que votre ordinateur ne soit compromis. En outre, avant de naviguer ou de cliquer sur des liens, faites appel à votre antivirus pour une protection supplémentaire. Notez que ces programmes ne vous protègent que des logiciels ou programmes espions, et non des périphériques tels qu'un clavier ou un dispositif d'enregistrement des frappes.

Pas un stalkerware?

Il existe de nombreuses autres méthodes permettant à quelqu'un d'accéder à des informations sur votre ordinateur sans installer de stalkerware. Si l'auteur a un accès physique à l'ordinateur, il n'a pas forcément besoin d'installer un stalkerware spécialisé dans la surveillance à distance.

Les auteurs peuvent également se connecter à des comptes tels que les courriels ou les médias sociaux pour savoir ce que vous faites. Il est possible d'accéder à ces comptes à partir d'un autre appareil si l'auteur de violence connaît le nom d'utilisateur ou l'adresse courriel et le mot de passe.

Parfois, des membres de votre famille ou des proches peuvent partager des informations sur vous, ce qui explique que la personne en sait trop sur ce que vous faites. La recherche de schémas et de l'origine de ces informations peut vous aider à comprendre les stratégies de l'auteur. Une intervenante antiviolence peut vous aider à comprendre ce qui vous arrive et à planifier les prochaines étapes.

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 *Spyware and Stalkerware: Computer Surveillance & Safety for Survivors*.

Guide de la survivante pour la surveillance des déplacements

La confidentialité de la localisation est essentielle à la sécurité. Les téléphones et les applis peuvent partager votre position avec d'autres personnes, parfois à votre insu. En outre, les dispositifs de localisation et les GPS intégrés aux voitures peuvent être utilisés à mauvais escient pour connaitre vos allées et venues. Les outils de localisation peuvent également servir à accroître la sécurité (savoir où se trouvent vos enfants ou vos animaux de compagnie), pour des raisons pratiques (retrouver des téléphones ou des clés) ou pour savoir si l'auteur de violence se trouve à proximité.

Vous pouvez souhaiter plus de confidentialité en matière de localisation, notamment si vous craignez que quelqu'un vous suive à la trace. Ce guide propose des informations et des stratégies pour déterminer si vous êtes surveillée et, le cas échéant, prendre une décision.

Étape 1: Accorder la priorité à votre sécurité

Renseignez-vous davantage. Il peut être très difficile et dangereux de faire face à la violence, aux abus et au harcèlement. Le personnel antiviolence de votre région peut vous informer des options et ressources locales, ainsi que vous aider à créer un plan de sécurité. Vous pouvez consulter www.hebergementfemmes.ca pour trouver des ressources.

Faites confiance à votre instinct. Les auteurs de violence sont souvent très déterminés à maintenir leur contrôle, et la technologie est l'un des nombreux outils qu'ils utilisent pour y parvenir. Si quelqu'un semble en savoir trop sur vous, des informations ont pu être obtenues par le biais de diverses sources, comme la surveillance de vos appareils, l'accès à vos comptes, la géolocalisation, ou en récoltant des renseignements vous concernant sur Internet.

Étape 2: Déterminer par quel moyen vous êtes localisée

- Pouvez-vous identifier des schémas dans ce que l'autre personne sait? Sait-elle où vous êtes en temps réel ou sait-elle seulement après coup où vous êtes allée?

- Partagez-vous votre compte téléphonique avec d'autres personnes? Est-ce que quelqu'un d'autre a accès à votre téléphone ou sait comment se connecter à l'un de vos comptes?

- Utilisez-vous des applis qui partagent votre position? Si oui, qui a accès à ces informations?

- Vos proches ou votre famille pourraient-ils partager l'endroit où vous êtes, par exemple, par le biais des médias sociaux?

Étape 3: En savoir plus sur le fonctionnement de cette technologie

Téléphones et appareils mobiles

- Les téléphones suivent votre position grâce au GPS intégré, aux connexions Wi-Fi qui peuvent servir à la localisation et aux tours de téléphonie cellulaire qui connectent votre téléphone au réseau. Vous pouvez désactiver certains partages de localisation, mais les services d'urgence et les compagnies de téléphone pourront accéder à votre position dès que le téléphone est allumé.

- Les téléphones connectés à votre compte Apple ou Google ont des fonctions conçues pour aider à retrouver les téléphones perdus. Toute personne ayant accès à votre compte peut suivre votre téléphone.

- Votre téléphone, votre tablette ou votre ordinateur portable enregistrera également tous les réseaux Wi-Fi auxquels vous vous êtes connectée. Il se peut que vous puissiez supprimer cet historique, en partie ou en entier.

Applis et médias sociaux

- Il se peut que vous partagiez votre position sur les médias sociaux et d'autres applis. Vérifiez les paramètres de localisation et de confidentialité de chaque appli.

- Les applis d'appareil photo stockent souvent l'endroit où une photo a été prise, et incluent cette information lorsque vous partagez une photo. Vous pouvez généralement désactiver cette fonction dans les paramètres de l'appareil photo et des applis photo. N'oubliez pas que le lieu peut également être révélé par la photo elle-même (points de repère).

- Vos proches peuvent partager votre position sur les médias sociaux en vous identifiant dans un certain lieu ou en mentionnant votre nom dans une publication qui cite un lieu spécifique. Si vous utilisez cette appli, vous pourrez peut-être configurer des notifications afin de savoir si d'autres personnes partagent votre position, ou modifier vos paramètres de confidentialité afin d'empêcher les autres de partager votre position ou d'indiquer votre nom dans une publication.

- Certaines applis demandent votre localisation. Les applis de commerce en ligne, les services de covoiturage ou les services de livraison de nourriture en sont des exemples. Quelqu'un ayant accès à ces comptes pourrait découvrir votre position.

- Les logiciels espions (également appelés stalkerware) installés sur votre téléphone, votre tablette ou votre ordinateur portable peuvent suivre votre localisation. Ce type d'appli peut être installé à votre insu sur votre téléphone et s'avérer difficile à détecter. En savoir plus sur les stalkerware pour appareils mobiles.

Dispositifs de système de positionnement global (GPS)

- De nombreuses voitures sont équipées de systèmes de navigation intégrés qui pourraient révéler l'historique de vos déplacements à toute personne ayant accès au système.

- Des dispositifs GPS peuvent également être placés dans un véhicule ou dans des effets personnels pour surveiller une personne. Ces appareils peuvent être peu coûteux, de petite taille et facilement dissimulés. Les appareils GPS doivent généralement être connectés à une source d'alimentation.

- Les informations relatives au suivi par GPS peuvent être en temps réel (données transmises directement à la personne qui a installé le GPS via un site web ou son téléphone) ou elles peuvent enregistrer l'historique de la localisation pour être examinées ultérieurement.

Traqueurs de localisation

- Les nouveaux dispositifs de localisation sont de petite taille et peuvent être dissimulés dans un sac à main, un sac à dos ou des cadeaux.

- Contrairement aux appareils GPS, ces traceurs n'ont pas besoin d'être connectés à une source d'alimentation et peuvent fonctionner pendant des mois sans être rechargés.

- Ces appareils de localisation sont connectés à une appli ou à un compte.

- Les localisateurs utilisent une combinaison de GPS, de RFID (identification par radiofréquence) active, de Bluetooth (basse énergie) et de réseaux Wi-Fi.

Étape 4: Stratégies de sécurité et de confidentialité

Vous pouvez prendre des mesures pour sécuriser votre localisation. 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 alerte souvent l'autre personne, qui risque de devenir plus violente. L'auteur peut essayer de vous surveiller d'une autre manière ou vous obliger à partager à nouveau votre position. Il peut aussi effacer des preuves. Envisagez de parler avec une intervenante antiviolence au sujet de la planification de sécurité. Si vous avez de soutien, consultez www.hebergementfemmes.ca.

Documenter votre expérience

Vous pouvez documenter ce qui se passe si cela vous semble sécuritaire. 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 à mettre à jour un plan de sécurité.

- Même sans savoir comment vos déplacements sont surveillés, vous pouvez documenter ce qui arrive. Que vous a dit l'auteur de violence qui indique qu'il sait où vous êtes? Quand et où s'est-il manifesté alors que vous ne vous y attendiez pas? Qu'est-ce que vous savez ou soupçonnez d'autre qui vous fait penser que vous êtes surveillée? Soyez aussi précise que possible.

- Si vous savez comment vous êtes surveillée, prenez des photos ou des captures d'écran si possible. Certaines technologies laisseront des traces ou des enregistrements de l'accès de quelqu'un d'autre à vos informations de localisation.

- Si vous expliquez à quelqu'un d'autre ce qui se passe, notez son nom, la date et l'heure.

Trouver l'appareil ou le service

- Vérifiez si des dispositifs GPS ou d'autres services de localisation sont cachés dans vos biens ou votre véhicule.

- Dans votre voiture, vérifiez dans le coffre, sous le capot, à l'intérieur du pare-chocs, ainsi que sous et entre les sièges. Vous pouvez demander à un mécanicien de confiance ou aux forces de l'ordre de voir s'ils peuvent trouver ce genre de dispositifs.

- Dans vos affaires, cherchez tout objet qui ne vous appartient pas; n'oubliez pas qu'un appareil peut être aussi petit qu'une pièce de 25 cents. Pour les cadeaux qui ne sont pas électroniques (comme un jouet), recherchez les pièces électroniques qui semblent ne pas faire partie du jouet.

Signaler la violence

- Les prestataires de services aux victimes peuvent vous aider à explorer les options de signalement aux forces de l'ordre ou à discuter des recours civils.

- Envisagez de prévenir les forces de l'ordre, si vous vous sentez assez en sécurité pour le faire. Leur capacité à enquêter sur votre plainte peut varier en fonction de leurs ressources et de leurs connaissances.

- Demandez l'aide d'un·e avocat·e au civil ou d'une organisation d'aide juridique. Vous pouvez également envisager de demander une ordonnance civile de protection par vous-même ou avec le soutien d'une intervenante ou d'un·e avocat·e.

- Vous pouvez également contacter le fabricant pour demander que l'accès de l'auteur de violence à votre position soit supprimé ou obtenir plus d'informations sur la manière de mieux contrôler le partage de votre localisation.

Suppression, blocage ou brouillage

- Si cela ne présente aucun danger, vous pouvez retirer le dispositif de suivi ou désactiver le partage de la localisation.

- Vous pouvez décider quand le suivi de la localisation doit être activé ou désactivé dans le cadre de votre plan de sécurité.

- Certains équipements de contre-surveillance «brouillent» ou bloquent la communication d'un appareil de localisation, mais cela peut aussi bloquer d'autres signaux, comme les communications téléphoniques.

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 le *Survivors Guide to Location Tracking*.

Logiciels espions pour appareils mobiles: Identification, suppression et prévention

Le contenu de cette fiche d'information ne constitue pas un avis juridique. Les informations contenues ci-dessous ont été mises à jour en février 2023 et traitent de ce qui peut être fait au Canada si vous pensez qu'un logiciel espion a été placé sur votre téléphone ou appareil mobile.

Si vous pensez que votre téléphone ou appareil mobile est surveillé, remplacez-le par un appareil que vous jugez sécuritaire lorsque vous recherchez des informations ou que vous demandez de l'aide. Il peut s'agir de l'ordinateur d'une bibliothèque publique ou d'une organisation de lutte contre la violence, ou encore du téléphone ou de l'ordinateur d'un membre de la famille ou d'une personne de confiance.

Si vous soupçonnez que quelqu'un vous surveille en utilisant la technologie, l'auteur peut également vous effrayer d'autres manières. Si vous souhaitez explorer les options de soutien disponibles, vous pouvez contacter un programme antiviolence dans votre région à partir d'un appareil sécuritaire. Consultez une intervenante antiviolence, pour discuter de la surveillance et de la violence facilitées par la technologie, ce qui vous permettra d'intégrer une réponse dans votre plan de sécurité.

Plan de sécurité

Avant d'agir, réfléchissez à la réaction de l'auteur des faits si vous l'empêchez de vous surveiller. Lorsque vous élaborez un plan de sécurité, vous pouvez aborder avec une intervenante antiviolence les répercussions possibles de la suppression de l'accès à l'auteur, et intégrer des mesures de sécurité concrètes dans votre plan. Pour des informations sur les stratégies permettant d'améliorer les plans de sécurité en cas de violence facilitée par la technologie, consultez la trousse à outils de planification de la sécurité en matière de technologie d'HFC.

Je suis inquiète qu'un logiciel espion soit installé sur mon téléphone. Est-ce possible?

L'installation d'un logiciel espion ou stalkerware sur votre téléphone exige un accès physique à l'appareil, ou la connaissance de votre identifiant et de votre mot de passe infonuagique.

Si quelqu'un a un accès physique à votre appareil, et qu'il connait votre mot de passe, il est concevable qu'un logiciel espion ait été placé sur votre téléphone. Cette fiche d'information vous aidera à en évaluer la probabilité, et les mesures à prendre pour identifier et remédier à la surveillance par des logiciels espions.

Qu'est-ce qu'un logiciel espion et que peut-il faire?

Un «logiciel espion pour appareil mobile» désigne une appli ou un programme placé délibérément sur l'appareil d'une personne pour la surveiller. Il s'agit d'une catégorie de stalkerware. Un logiciel espion est défini comme «tout logiciel explicitement vendu ou autorisé pour faciliter la violence, les abus ou le harcèlement entre partenaires intimes, y compris l'intrusion délétère dans la vie privée d'un des partenaires par le biais d'actions physiques ou numériques».

En fonction du type de logiciel espion pour appareil mobile, il va surveiller:

- Historique des appels, y compris le numéro de téléphone, la date et la durée de l'appel
- SMS, y compris le numéro de téléphone et le contenu
- Frappes de touches
- Contacts
- Navigation sur Internet, y compris l'historique et les signets
- Position ou localisation du téléphone
- Photos prises sur le téléphone
- Courriels téléchargés sur le téléphone

Si le téléphone a été «jailbreaké» (c'est-à-dire que des restrictions matérielles imposées par Apple et l'opérateur sans fil ont été appliquées à un iPhone) ou «rooté» (c'est-à-dire que le code du logiciel d'exploitation Android a été modifié et que d'autres logiciels bloqués par le fabricant ont été installés), les logiciels espions peuvent surveiller:

- Certaines applications de messagerie, telles que WhatsApp, Viber et Skype

- Les conversations téléphoniques

- L'utilisation du microphone pour enregistrer l'environnement du téléphone

Il peut être difficile de repérer la présence d'un logiciel espion. Comme la plupart fonctionnent en mode «furtif» ou caché, ils sont difficilement détectés.

Une fois installé, l'auteur peut surveiller toutes les activités susmentionnées via un site Web ou une appli.

Si ce n'est pas un logiciel espion, qu'est-ce que ça peut être d'autre?

Il existe plusieurs moyens de traquer ou de surveiller les activités d'une autre personne à l'aide de différentes technologies, par exemple:

- Surveiller des informations sur Facebook

- Se connecter au compte iCloud ou Google associé au téléphone, ce qui permet d'accéder à des informations sensibles, notamment la localisation
- Utiliser les fonctions du téléphone telles que Trouver mon téléphone. Ces capacités intégrées, populaires pour leur côté pratique, peuvent également permettre le suivi de la localisation dans le contexte du harcèlement criminel (traque furtive), par exemple.

Je possède un iPhone. Quels sont les risques liés aux logiciels espions sur les iPhone?

Si vous possédez un iPhone 6 ou supérieur et que vous avez régulièrement mis à jour l'iOS (système d'exploitation), il est peu probable qu'un logiciel espion inconnu se trouve sur votre téléphone.

Si vous possédez un modèle d'iPhone plus ancien, ou si vous n'avez pas mis à jour votre iOS régulièrement, il est possible que des logiciels espions inconnus se trouvent sur votre iPhone dans le cas où: (a) quelqu'un a été en contact physique avec votre appareil; (b) cette personne connaissait le mot de passe de votre appareil, ainsi que de votre identifiant et votre mot de passe Apple ID; et (c) votre iOS ne peut pas accéder à la mise à jour la plus récente.

Si quelqu'un que vous soupçonnez a été en contact physique avec votre appareil, connait le mot de passe ou les détails de connexion de l'Apple ID, et si vous pensez qu'un logiciel espion est installé sur votre appareil, veuillez contacter votre organisation locale de lutte contre la violence pour élaborer un plan de sécurité.

Je possède un Android. Quels sont les risques liés aux logiciels espions sur les téléphones utilisant le système d'exploitation Android?

Cela inclut les téléphones de Samsung, Sony, Google Pixel, Huawei, LG, HTC et Nokia.

Le système d'exploitation Android est plus vulnérable aux logiciels espions placés sur l'appareil. Il est également facile de dissimuler les traces de logiciels espions sur les appareils Android. Si quelqu'un que vous soupçonnez a été en contact physique avec votre appareil, connait le mot de passe ou les détails, et si vous pensez qu'un logiciel espion est installé sur votre appareil, veuillez contacter votre organisation locale de lutte contre la violence depuis un appareil sécuritaire pour obtenir de plus amples informations sur les logiciels espions et la planification de sécurité.

Puis-je apporter mon téléphone au magasin où il a été acheté ou à un «spécialiste en technologie» à proximité pour vérifier la présence de logiciels espions?

Certaines formes de logiciels espions peuvent être facilement identifiées dans un point de vente au détail. Mais d'autres logiciels nécessitent un examen plus approfondi qui dépasse la compétence du personnel des magasins d'ordinateurs ou d'appareils mobiles.

En fonction de votre situation, si la surveillance par le biais d'un logiciel espion n'est qu'une partie de la violence que vous subissez, vous pouvez demander l'aide d'un service de lutte contre la violence familiale pour mettre en place un plan de sécurité**.**

Je pense qu'un logiciel espion est utilisé sur mon téléphone ou l'un de mes appareils en ce moment. Que puis-je faire pour me protéger?

Si vous n'avez pas la possibilité de contacter une organisation antiviolence, mais que vous avez des raisons de croire qu'un logiciel espion vous surveille, voici quelques mesures temporaires que vous pouvez prendre pour vous protéger:

- Envisagez d'utiliser un autre téléphone ou un appareil sécuritaire pour les communications privées ou d'autres activités telles que la recherche de services de soutien. Continuez à utiliser le téléphone suspect pour des activités «publiques» jusqu'à ce qu'il soit possible de vérifier si l'appareil est infecté par un logiciel espion. Cette stratégie peut être utile si vous ne voulez pas que l'auteur sache que vous soupçonnez la présence d'un tel logiciel sur le téléphone.
- Par précaution, tenez vos conversations privées sur un autre appareil ou préconisez les échanges en personne, hors de portée d'enregistrements suspects pouvant provenir de logiciels espion.
- N'oubliez pas que les logiciels espions peuvent surveiller la localisation, alors faites attention aux endroits où vous allez avec votre téléphone. Par exemple, si vous apportez le téléphone à la police, l'auteur peut alors savoir que le téléphone se trouve au poste de police. Réfléchissez à tous les risques et à la manière de planifier votre sécurité.
- Les logiciels espions ne communiquent des informations que lorsque le téléphone est allumé et connecté à Internet. Le fait de l'éteindre ou d'activer le mode avion permet de s'affranchir temporairement du suivi par GPS ou de tout risque de capture d'images, de sons ou de vidéos par l'appareil photo.

Dans le meilleur des cas, activer le mode avion ou éteindre le téléphone constitue une mesure temporaire pour empêcher les logiciels espions de vous suivre. Une fois le téléphone rallumé, il reprend ses activités, par exemple, accéder à une photo prise pendant que le téléphone était en mode avion ou déconnecté. Il faut réfléchir au moment où vous pouvez rallumer votre appareil en toute sécurité.

- Vous pouvez réinitialiser votre appareil, vous assurer que le système d'exploitation est à jour et modifier votre identifiant Apple/iCloud ou vos mots de passe Google pour débarrasser votre appareil des logiciels espions. Cela fonctionne pour de nombreux types de logiciel espion, mais pas tous. Il est conseillé de demander des informations à votre organisation antiviolence. Une organisation antiviolence pourra vous montrer: 1) comment préserver les preuves si nécessaire; 2) comment pourrait réagir l'auteur si vous lui retirez la possibilité de vous surveiller; et 3) comment élaborer un plan de sécurité.
- Pensez à utiliser un antivirus réputé pour détecter et supprimer les logiciels espions. Certains peuvent être détectés et supprimés à l'aide de ces programmes.

- En dernier recours, l'achat d'un nouveau téléphone devrait éliminer la menace. Toutefois, si vous achetez un nouvel appareil Android, évitez d'utiliser la sauvegarde complète de l'ancien lorsque vous configurez le nouveau, et changez vos mots de passe de connexion Google sur un appareil sécuritaire. Si vous avez un iPhone, changer votre mot de passe iCloud devrait suffire, à moins que l'auteur de violence ne dispose d'autres moyens (ordinateur de bureau et enregistreur de frappe) pour vous surveiller.
    - Note: Sur les téléphones Android, vérifiez les paramètres de sécurité, désactivez l'option «autoriser l'installation à partir de sources inconnues» et sélectionnez «vérifier les applications» pour empêcher l'installation de logiciels espions.

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.*

Remerciements particuliers à Christopher Parsons, Citizen Lab, Munk School of Global Affairs & Public Policy; Dr Diarmaid Harkin, Université Deakin; et Dr Adam Molnar et Mme Erica Vowles, Université Deakin.

Adapté pour le Canada avec la permission du WESNET's Technology Safety project, d'après leur ressource Mobile Spyware: Identification, Removal and Prevention.

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.

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

Femmes et Égalité des genres Canada | Women and Gender Equality Canada | Canada