Sécurité technologique Canada

Guide de sécurité: Stalkerware pour 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.

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*.

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