Sécurité technologique Canada

Conseils rapides pour la planification de sécurité technologique

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.

Êtes-vous la cible de violence technologique?

Il peut s'agir de violence technologique si quelqu'un:

- Contrôle votre téléphone
- Vous enlève votre téléphone
- Brise votre téléphone
- Vous oblige à partager votre téléphone
- Contrôle vos comptes en ligne
- Vous empêche d'utiliser vos comptes en ligne
- Utilise vos comptes en ligne sans votre consentement
- Partage des photos de vous sans votre consentement
- Exerce un chantage en vous disant qu'il va partager des photos de vous sans votre consentement, à moins que vous ne fassiez ce qu'il demande

Il peut s'agir de violence technologique si quelqu'un surveille ce que vous faites en utilisant:

- Votre téléphone
- Des caméras cachées
- Des applis

Il peut s'agir de violence technologique si quelqu'un utilise un ordinateur, un téléphone ou une tablette pour:

- Vous contacter de manière répétée et non souhaitée
- Publier des choses qui vous blessent
- Vous punir
- Menace de vous faire du mal ou s'en prend à des membres de votre famille

Il peut s'agir de violence technologique si quelqu'un utilise des applis ou des médias sociaux pour:

- Publier des choses qui vous mettent mal à l'aise
- Publier des choses qui portent attente à votre image ou à celle de votre famille
- Menacer de faire du tort, à vous ou à votre famille

Il peut s'agir de violence technologique si quelqu'un utilise la technologie pour:

- Découvrir où vous êtes contre votre gré
- Découvrir ce que vous faites à votre insu
- Vous suivre et vous surveiller

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, d'après leur ressource *Is Tech Abuse Happening to You*.

Plan de sécurité technologique, fiche-conseils

LA SÉCURITÉ D'ABORD

Envisagez d'utiliser un appareil plus sécuritaire. Si vous pensez que quelqu'un surveille votre ordinateur ou tout appareil mobile, essayez d'utiliser un autre appareil auquel l'auteur de violence n'a pas pu accéder physiquement ou à distance dans le passé et auquel il n'a pas présentement accès (comme un ordinateur à la bibliothèque ou le téléphone d'un·e ami·e). C'est une façon de réduire le risque de surveillance.

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 appeler une organisation antiviolence près de chez vous pour vous connecter avec une intervenante, ou consulter www.hebergementfemmes.ca.

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

Planifiez stratégiquement autour de votre technologie. Lorsque les auteurs de violence utilisent la technologie à mauvais escient, il est souvent naturel de vouloir jeter des appareils ou fermer des comptes en ligne pour que cela cesse. Cependant, certains individus violents peuvent intensifier le harcèlement et les comportements dangereux s'ils ont l'impression d'avoir perdu le contrôle de leur partenaire ou de leur ex-partenaire. Avant de retirer une caméra cachée ou un traceur GPS que vous avez trouvé, ou de désinstaller un logiciel de harcèlement, réfléchissez à la façon dont l'auteur pourrait réagir et planifiez votre sécurité. Par exemple, certaines femmes choisissent d'utiliser un appareil plus sûr pour certaines interactions, mais continuent également d'utiliser le dispositif surveillé afin de recueillir des preuves et d'éviter l'escalade.

IDENTIFIER LES ABUS

Cherchez des schémas. Prenez le temps de réfléchir au type de technologie qui pourrait être utilisé pour vous traquer, vous surveiller ou vous harceler. Par exemple, si l'auteur a laissé entendre qu'il vous surveille, pensez à ce qu'il sait.

Est-il au courant de ce que vous faites dans une pièce de votre maison en particulier? Si c'est le cas, il y a peut-être une caméra cachée dans cette pièce.

Si vous pensez être surveillée, est-ce seulement lorsque vous êtes dans votre voiture, ou également lorsque vous circulez à pied? Si c'est juste dans votre voiture, il y a peut-être un appareil caché dans votre véhicule. Si vous avez l'impression que c'est constant, il peut s'agir d'un objet que vous portez sur vous, comme votre téléphone, ou un traceur dans votre sac.

Le fait d'identifier la technologie utilisée contre vous peut vous aider à créer un plan de sécurité et à documenter la violence. En savoir plus sur l'Évaluation de la violence facilitée par la technologie[JN1] .

Documentez les incidents. La documentation d'une série d'incidents peut montrer à la police ou au tribunal un schéma de comportement correspondant à la définition légale de la traque furtive ou du harcèlement. La documentation peut également vous aider à voir si les choses s'aggravent et planifier votre sécurité. Pour plus d'informations, consultez les Stratégies de documentation pour les femmes subissant la VFGFT[JN2] .

Signalez les incidents. Vous pouvez également signaler les incidents aux forces de l'ordre ou demander un engagement de ne pas troubler l'ordre public ou une ordonnance de protection familiale. Si le harcèlement se produit en ligne, vous pouvez également signaler l'abus au site web ou à l'application où le harcèlement a lieu. Si le comportement enfreint les conditions d'utilisation de la plateforme, le contenu peut être supprimé ou la personne peut être bannie. Il est important de reconnaître que le fait de signaler un contenu peut le faire disparaître complètement. Il faut donc documenter ces preuves avant de signaler l'abus.

[JN1]Link to 1.04

[JN2]Link to 1.05

MESURES À PRENDRE POUR AMÉLIORER LA SÉCURITÉ

Changez les mots de passe et les noms d'utilisateur. Si vous pensez que l'on accède à vos comptes en ligne, vous pouvez changer vos noms d'utilisateur et vos mots de passe à partir d'un appareil de confiance. Une fois que vous avez mis à jour les informations relatives à un compte, il est important de ne pas y accéder à partir d'un appareil que vous pensez être surveillé. Vous pouvez également envisager de créer de nouveaux comptes, par exemple une nouvelle adresse électronique avec un nom d'utilisateur non identifiable au lieu de votre nom réel ou de toute autre information personnelle. Il est important de ne pas lier ces nouveaux comptes à d'anciens comptes ou numéros, et de ne pas utiliser le même mot de passe pour tous vos comptes. Lire plus de conseils sur la sécurité des mots de passe[JN1] .

Vérifiez vos appareils et vos paramètres. Passez en revue votre appareil mobile, vos applications et vos comptes en ligne pour vérifier les paramètres de confidentialité et vous assurer que d'autres appareils ou comptes ne sont pas connectés au vôtre et que tout accès d'appareil à appareil, comme le Bluetooth, est désactivé lorsque vous ne l'utilisez pas. Assurez-vous de bien connaître chacune de vos applications et ce qu'elle fait. Supprimez de votre appareil toutes les applications qui ne vous sont pas familières ou que vous n'utilisez pas. Identifiez les augmentations soudaines d'utilisation des données — cela peut indiquer qu'un logiciel de surveillance est utilisé.

Procurez-vous un nouvel appareil. Si vous soupçonnez que votre appareil est surveillé, le plus sûr est peut-être d'en acquérir un nouveau avec un compte auquel l'auteur de violence n'a pas accès. Un téléphone à carte est une option moins coûteuse. Mettez un code d'accès sur le nouvel appareil et ne le reliez pas à vos anciens comptes infonuagiques comme iCloud ou Google auxquels la personne pourrait avoir accès. Pensez à désactiver le partage de localisation et le Bluetooth lorsqu'ils ne sont pas utilisés. Vous pouvez également conserver l'ancien appareil pour que l'auteur pense que vous l'utilisez toujours et n'essaie pas d'accéder au nouvel appareil.

Faites attention à la géolocalisation Si l'auteur de violence semble savoir où vous êtes en tout temps, il se peut qu'il surveille vos déplacements grâce à votre appareil mobile, votre véhicule ou en utilisant un appareil de géolocalisation. Vous pouvez vérifier votre appareil mobile, vos applications et vos comptes pour voir si la géolocalisation est activée et mettre à jour les paramètres selon vos besoins. Vous pouvez également appeler votre fournisseur de téléphonie mobile pour demander si la géolocalisation est activée, surtout en cas d'abonnement familial avec l'auteur. Pour la voiture, vos

allées et venues peuvent être tracées par le biais d'un service d'assistance routière ou de sécurité du conducteur. Si vous craignez qu'un appareil muni d'un GPS soit caché dans votre voiture ou tout autre bien, un organisme d'aide juridique, un détective privé ou un mécanicien automobile peut être en mesure de vous aider à le trouver. Il est important de planifier la sécurité et de documenter les preuves avant d'interrompre la géolocalisation par l'auteur de violence.

Pensez aux caméras et aux appareils audio. Si vous soupçonnez que vous êtes surveillée par des caméras ou des enregistreurs audio, il est possible que des appareils cachés soient en cause. Il peut s'agir d'un cadeau de l'auteur, ou d'un appareil de tous les jours comme une webcam, un assistant personnel (tels que Google Home ou Alexa), ou un système de sécurité. Si les caméras cachées vous préoccupent, envisagez d'utiliser un détecteur de caméras, bien que certains ne localisent que les caméras sans fil, et non les caméras câblées, et vice versa. Les appareils de tous les jours ou les cadeaux peuvent être sécurisés en modifiant les paramètres du compte ou les mots de passe. Les caméras web intégrées peuvent être recouvertes d'un morceau de ruban adhésif amovible (bien que cela ne concerne que la caméra, et non les logiciels espions présents sur l'ordinateur). N'oubliez pas d'établir un plan de sécurité et de documenter les preuves avant de retirer les appareils ou de couper l'accès à l'auteur de violence.

[JN1]Link to 1.24

MESURES POUR UNE CONFIDENTIALITÉ ACCRUE

Protégez votre adresse. Si vous craignez que quelqu'un découvre votre adresse personnelle, vous pouvez ouvrir une boîte postale (privée). Notez que cela est surtout utile si vous avez déménagé récemment ou si l'auteur ne connaît pas encore votre adresse. Dites à vos proches et à votre famille de ne pas partager votre adresse, et usez de prudence lorsque vous la donnez à des entreprises locales. Vérifiez quelles informations sont publiques dans votre communauté si vous prévoyez acheter une maison, afin de prendre une décision éclairée.

Limitez le partage de vos informations. De nos jours, presque toutes nos activités nécessitent des informations d'identification personnelle, que ce soit pour faire un achat, utiliser un coupon rabais ou créer un compte en ligne. Les informations que nous fournissons sont souvent vendues à des tiers et se retrouvent ensuite en ligne dans les moteurs de recherche et chez les courtiers en données. Lorsque cela est possible, refusez la collecte d'informations ou ne fournissez que le minimum nécessaire. Vous pouvez faire preuve de créativité. Par exemple, au lieu d'utiliser votre nom et votre prénom, utilisez vos initiales. Vous pouvez également utiliser un numéro de téléphone virtuel gratuit, tel que Google Voice, pour obtenir un autre numéro à partager au besoin.

Contrôlez votre vie privée en ligne et hors ligne. Notre Trousse à outils sur la sécurité et la confidentialité technologiques contient des conseils de sécurité et de confidentialité en ligne [JN1] qui incluent plus d'informations sur la modification des paramètres de vos appareils électroniques, de vos comptes de médias sociaux tels que Facebook et Twitter, et de votre réseau Wi-Fi[JN2] domestique. Suivez ces étapes pour mieux protéger votre vie privée et réduire les risques que l'auteur utilise ces technologies à mauvais escient, vous localise ou surveille vos activités.

[JN1]Link 1.18

[JN2]Link 1.26

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 êtes en situation de 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 des services gratuits et confidentiels.*

Adapté pour le Canada avec la permission du projet Safety Net de NNEDV, selon leur ressource «Technology Safety Plan: A Guide for Survivors and Advocates.»

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