Sécurité technologique Canada

Amorces de conversation 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.

Comment utiliser cette ressource

Cette ressource a pour but d'aider le personnel antiviolence à aborder la violence fondée sur le genre facilitée par la technologie (VFGFT) avec les survivantes. La VFGFT est largement utilisée par les auteurs de violence conjugale. Si la personne que vous soutenez est concernée par la VFGFT, il faut en tenir compte dans son plan de sécurité. Cette ressource contient des questions, des stratégies de sécurité technologique et des liens vers des documents pouvant guider vos conversations sur la planification de sécurité avec des survivantes de VFGFT.

Vous pouvez également consulter les ressources complémentaires: «Êtes-vous la cible de violence technologique?» et «Liste de contrôle pour la planification de sécurité technologique».

Quelques considérations:

- Les stratégies suivantes peuvent ne pas convenir à toutes les situations. Rencontrez votre cliente là où elle se trouve et demandez-lui de quel type d'abus technologiques elle soupçonne être la cible. Voici quelques suggestions sur la manière d'intégrer la technologie dans la planification de sécurité.
- Pour planifier la sécurité d'une personne en situation de VFGFT, il faut tenir compte de la possibilité que l'auteur de violence puisse avoir accès à ses appareils et ses comptes. Il pourrait donc être en mesure de surveiller ses communications et ses déplacements. Le fait de modifier un appareil, un compte de médias sociaux, un courriel ou toute autre technologie peut signaler à l'auteur que votre cliente recherche de l'aide et entrainer une escalade de la violence. Il peut s'avérer nécessaire de prendre des précautions additionnelles dans ce genre de situations

Est-ce que quelqu'un peut prendre le contrôle de votre téléphone, s'en emparer, le briser ou vous obliger à le partager?

- Avez-vous votre propre téléphone? À quoi vous sert votre téléphone?
- Est-ce que quelqu'un vous empêche de communiquer avec votre famille ou vos proches?
- Partagez-vous votre téléphone ou est-ce que quelqu'un d'autre y a accès?
- Avez-vous déjà eu besoin d'utiliser votre téléphone sans pouvoir le faire? Pouvez-vous m'en dire plus sur cette situation?
- Est-ce que quelqu'un sait comment débloquer votre téléphone ou pourrait vous obliger à le faire?

Stratégies de sécurité technologique suggérées:

- Si vous ne vous sentez pas en sécurité d'arrêter d'utiliser un téléphone que l'auteur surveille ou auquel il a accès, ne changez pas vos habitudes, mais trouvez un autre moyen de passer des communications en privé et planifiez votre sécurité.
- Faites savoir aux gens quand vous les rencontrez en personne que votre téléphone n'est pas privé. Convenez d'un code signalant à l'autre personne que quelqu'un écoute votre appel ou lit vos SMS.
- Faites une liste manuscrite de vos contacts et conservez-la en lieu sûr en cas de vol ou de bris de votre téléphone.
- Pour plus de conseils, consultez notre liste de contrôle pour la planification de sécurité technologique.

Est-ce que quelqu'un a accès à vos comptes (courriel, banque, réseaux sociaux, etc.), les contrôle ou vous empêche d'y accéder?

- Partagez-vous vos comptes avec quelqu'un? Qui l'a ouvert et qui prend des décisions concernant votre compte?
- Est que quelqu'un a accès à vos comptes de messagerie, bancaires, GooglePlay, Apple ID ou iCloud?
- Les choses que vous faites sur votre téléphone ou vos comptes sont-elles privées ou accessibles à quelqu'un d'autre?
- Est-ce que quelqu'un connait vos mots de passe ou consulte vos comptes?
- Est-ce qu'on vous a déjà privée de l'accès à vos comptes ou les a-t-on modifiés?
- Est-ce que quelqu'un pourrait ouvrir des comptes en votre nom, mentir ou se faire passer pour vous?
- Avez-vous un compte bancaire auquel vous seule avez accès?

Stratégies de sécurité technologique suggérées:

- Utilisez un mot de passe long, composé de chiffres et de symboles, difficile à deviner.
- Utilisez la vérification en deux étapes ou l'authentification multifactorielle si vous pouvez le faire en toute sécurité.
- Utilisez un mot de passe différent pour chaque compte.
- Envisagez de changer vos mots de passe ou de créer de nouveaux comptes.
- Créez de nouveaux comptes «sécuritaires» sur un téléphone non surveillé ou un ordinateur de la bibliothèque. Utilisez ces comptes uniquement sur un appareil auquel l'auteur de violence n'a pas accès.
- Pour plus de conseils, consultez notre liste de contrôle pour la planification de sécurité technologique

Est-ce que quelqu'un vous embarrasse, vous humilie, vous menace ou usurpe votre identité sur les médias sociaux, applis, SMS, courriel ou téléphone?

- Est-ce que quelqu'un dit du mal de vous sur les médias sociaux?
- Est-ce que d'autres personnes commencent à dire des choses pour vous blesser ou à «aimer» des publications censées vous déplaire?
- Est-ce que quelqu'un compromet votre sentiment de sécurité sur les médias sociaux? De quelle manière?
- Est-ce que quelqu'un vous a trompé ou s'est fait passer pour vous ou pour une de vos connaissances sur les médias sociaux?

Stratégies de sécurité technologique suggérées:

- Conservez une trace des publications sur les médias sociaux, de la personne qui les a mises en ligne et de celles qui les ont reçues (utilisez la fonction «télécharger les données», faites une capture d'écran ou une photo avec un appareil «sécuritaire», ou copiez, imprimez ou entreposez les données sur une clé USB).
- Réglez les paramètres de sécurité et de confidentialité (y compris les tags) sur les médias sociaux. Bloquez l'auteur si vous pouvez le faire en toute sécurité.
- Ces comportements peuvent être contraires à la loi et vous pouvez demander une assistance juridique ou celle de la police.
- Pour plus de conseils, consultez notre liste de contrôle pour la planification de sécurité technologique

Est-ce que quelqu'un vous harcèle, vous maltraite, vous punit ou vous menace par SMS, applis de communication (Whatsapp, Viber, Skype, Facetime), courriel ou téléphone?

- Est-ce que l'on vous a dit des choses au téléphone pour vous blesser ou vous effrayer?
- Devez-vous faire certaines choses avec votre téléphone pour ne pas avoir d'ennuis?
- Est-ce que quelqu'un vous envoie constamment des messages ou se met en colère si vous ne répondez pas?

Stratégies de sécurité technologique suggérées

- Prenez note des détails des conversations téléphoniques et conservez les journaux d'historique des appels, parfois appelés «récents» (capture d'écran, prise de photo avec un appareil «sécuritaire» ou imprimer). Les fournisseurs de téléphonie mobile permettent également d'accéder à l'historique des appels et des messages.
- Conservez les SMS (copie, capture d'écran, prise de photo avec un autre appareil «sécuritaire» ou sauvegarde sur une clé USB).
- Désactivez le Wi-Fi et le Bluetooth, puis mettez l'appareil en mode avion pour préserver l'historique des appels et les messages texte sur l'appareil.
- Apportez l'appareil et toutes les copies, captures d'écran, documents imprimés ou clé USB à votre avocat·e ou à la police pour que les preuves soient formellement documentées, car ces comportements peuvent être sujets à sanction.
- Pour plus de conseils, consultez notre liste de contrôle pour la planification de sécurité technologique

Est-ce que quelqu'un partage ou menace de partager des images sans votre consentement?

- Est-ce que quelqu'un possède des photos ou des vidéos privées de vous, obtenues avec ou sans votre consentement?
- Est-ce que ces photos ont été partagées ou est-ce que quelqu'un vous menace de les partager?
- Avez-vous reçu ces menaces en personne ou autrement?

Stratégies de sécurité technologique suggérées

- Demandez à la personne de retirer les images et de les supprimer.

- Signalez les images à l'entreprise de médias sociaux
- Le partage d'images intimes sans consentement est contraire à la loi et il est possible de demander de l'aide à une intervenante, un·e avocat·e ou à la police.
- Pour plus de conseils, consultez notre liste de contrôle pour la planification de sécurité technologique

Est-ce que quelqu'un sait où vous êtes, ce que vous faites, ou vous harcèle en utilisant des applis de localisation/GPS, de surveillance, de logiciels espions/enregistreurs de frappe ou des caméras cachées?

- Est-ce que quelqu'un utilise votre téléphone pour vous surveiller ou suivre vos déplacements?
- Est-ce qu'une personne sait des choses que vous ne lui avez pas confiées? D'après vous, comment ces informations ont-elles été obtenues?
- Est-ce que quelqu'un semble savoir certaines choses mais pas d'autres? Que sait-on sur vous? Quelle pourrait être la provenance de ces informations?
- Est-ce que des choses bizarres ou inexpliquées se produisent avec votre téléphone, votre voiture ou votre maison?
- Si votre cliente soupçonne d'être géolocalisée ou qu'elle est la cible de harcèlement, ses appareils, sa maison, sa voiture, ses biens ou les appareils ou biens de ses enfants peuvent être compromis.
- **Tout harcèlement doit être pris au sérieux**

Stratégies de sécurité technologique suggérées:

- Envisagez d'utiliser un appareil «sécuritaire» (un nouveau téléphone ou celui d'un membre de la famille ou d'un proche) pour les activités de planification de sécurité, ou de confier l'appareil à des personnes de confiance.
- Déterminez si des tendances peuvent être établies sur les informations qui sont découvertes. Sait-on où vous allez en tout temps, ou seulement lorsque vous utilisez votre voiture ou les transports publics? Envisagez de répertorier ce que la personne sait, et d'où peut venir cette information. Cela peut aider à en déterminer l'origine. Par exemple, si l'on découvre les endroits où vous vous rendez en utilisant une application de covoiturage, mais pas lorsque vous employez d'autres moyens de transport, c'est peut-être cette appli qui est compromise.
- Vérifiez les paramètres de localisation globale sur le téléphone et pour chaque appli, car certaines peuvent collecter et partager des informations de localisation. Vérifiez également les outils de localisation comme Tile ou AirTags.
- Les comportements de harcèlement peuvent être contraires à la loi et vous pouvez demander de l'aide d'un·e avocat·e ou de la police.
- Pour plus de conseils, consultez notre liste de contrôle pour la planification de sécurité technologique

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 ou appeler ou envoyer un message texte à Jeunesse, J'écoute pour discuter de vos options et 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 l'autorisation du Technology Safety Project de WESNET, d'après leur ressource Tech Abuse: Client Conversation Starters & Safety Planning.

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