Amorces de conversation pour la planification de sécurité technologique

Comment utiliser cette ressource

Ce document vise à aider le personnel antiviolence à soutenir les survivantes de violence fondée sur le genre facilitée par la technologie (VFGFT). Si elles ont subi la VFGFT, celle-ci doit faire partie de leur plan de sécurité.

Vous y trouverez des questions, des stratégies et des liens utiles pour guider vos conversations sur la planification de sécurité.

Pour obtenir un soutien supplémentaire, consultez les ressources suivantes: Êtes-vous la cible de violence technologique? et la Liste de contrôle pour la planification de la sécurité technologique.

Considérations initiales:

- Rencontrez la survivante là où elle se trouve et entamez une conversation pour mieux comprendre ce qu'elle subit.
- Lorsque vous planifiez la sécurité d'une victime de VFGFT, il est important de souligner que l'auteur peut avoir accès à ses appareils ou à ses comptes et qu'il surveille peut-être ses communications et ses déplacements.
- Le fait de modifier un appareil, un compte de médias sociaux, un courriel ou toute autre technologie peut alerter l'auteur sur le fait que la survivante cherche de l'aide et peut aggraver la violence.
- Il peut être nécessaire de prendre des précautions supplémentaires en matière de planification de sécurité dans ces situations.

Les questions ci-dessous ne constituent pas une liste de contrôle, mais plutôt des suggestions sur la manière d'intégrer la technologie dans les conversations relatives à la planification de sécurité. N'utilisez que les questions qui correspondent à l'expérience de la survivante.

Est-ce que quelqu'un:

Contrôle, prend, brise ou vous oblige à partager votre téléphone?

- Avez-vous votre propre téléphone? À quoi vous sert votre téléphone?
- Qui est propriétaire de votre téléphone et de votre compte?
- Est-ce que quelqu'un vous empêche de parler à votre famille ou à vos proches?
- Partagez-vous votre téléphone avec quelqu'un d'autre ou est-ce que quelqu'un d'autre regarde votre téléphone?
- Avez-vous déjà eu besoin d'utiliser votre téléphone sans pouvoir le faire? Pouvez-vous m'en dire plus sur ce qui s'est passé?
- Est-ce que quelqu'un sait comment déverrouiller votre téléphone, ou vous oblige à le déverrouiller?

Stratégies de sécurité technologique suggérées:

Si la survivante ne peut pas cesser d'utiliser en toute sécurité un téléphone que l'auteur surveille:

- Suggérez-lui de continuer à utiliser son téléphone comme d'habitude pour ne pas éveiller les soupçons, mais à se servir d'un autre appareil ou d'une autre méthode plus sûre pour les conversations privées et la planification de sécurité.
- Rappelez-lui de signaler en personne à ses contacts de confiance que son téléphone n'est pas privé.
- Aidez la survivante à créer un mot de code simple qu'elle peut utiliser pour signaler que quelqu'un écoute ses appels ou lit ses messages.
- Suggérez-lui de noter les numéros de contact importants et de les conserver dans un endroit sûr au cas où son téléphone serait volé ou détruit.
- Aidez-la à contacter l'opérateur de téléphonie mobile pour connaître les possibilités de fermer un compte contrôlé par l'auteur ou de configurer un nouveau téléphone ou un nouveau numéro.

Pour plus de conseils, consultez notre liste de contrôle pour la planification de la sécurité technologique.

Est-ce que quelqu'un:
Accède à vos comptes (courriel, banque, réseaux sociaux, etc.), les contrôle ou les verrouille?

- Partagez-vous vos comptes avec d'autres personnes? Est-ce que ces personnes configurent votre appareil ou prennent des décisions pour vous concernant votre compte?
- Quelqu'un a-t-il accès à vos comptes courriel, bancaires, GooglePlay ou iCloud?
- Les choses que vous faites sur votre téléphone ou votre compte sont-elles privées?
- Est-ce que quelqu'un connaît vos mots de passe ou accède à vos comptes? Peut accéder à votre gestionnaire de mots de passe?
- Est-ce que quelqu'un vous a déjà bloqué l'accès à vos comptes ou y a apporté des modifications?
- Est-ce que quelqu'un ouvre des comptes à votre nom ou ment en prétendant que vous voulez ouvrir un compte?
- Avez-vous votre propre compte bancaire ou avez-vous un compte partagé?

Stratégies de sécurité technologique suggérées:

Pour améliorer la sécurité du compte:

- Aidez la survivante à créer des mots de passe longs et difficiles à deviner en utilisant un mélange de chiffres et de symboles.

- Si c'est possible, aidez-la à activer l'authentification en deux étapes ou multifactorielle.
- Encouragez l'utilisation d'un mot de passe différent pour chaque compte afin de réduire les risques si l'un d'entre eux est compromis.
- Demandez à la survivante si elle croit qu'il est plus sécuritaire de changer de mots de passe ou de créer de nouveaux comptes.
- Aidez-la à créer de nouveaux comptes à l'aide d'un appareil sécurisé, comme un ordinateur de la bibliothèque ou un téléphone auquel l'auteur n'a pas accès, et suggérez-lui d'éviter de se connecter à ces comptes sur un appareil surveillé.

Pour plus de conseils, consultez notre liste de contrôle pour la planification de la sécurité technologique.

Est-ce que quelqu'un:
Vous fait honte, vous humilie, vous menace ou usurpe votre identité sur des médias sociaux, applis, SMS, courriels ou sur le téléphone?

- Est-ce que quelqu'un dit du mal de vous sur les médias sociaux?
- Est-ce que d'autres personnes se mettent à dire des choses qui vous blessent ou à «aimer» des choses méchantes que d'autres ont publiées à votre sujet?
- Est-ce que quelqu'un vous fait craindre d'utiliser les médias sociaux? Que font-ils?
- Est-ce que quelqu'un vous a déjà piégée ou fait semblant d'être vous ou une personne que vous connaissez sur les médias sociaux?

Stratégies de sécurité technologique suggérées:

Si la survivante subit des abus sur les médias sociaux:

- Aidez-la à tenir un journal des messages nuisibles, avec les noms de l'auteur et des personnes qui ont vu ces messages.
- Si possible, utiliser la fonction «télécharger les données», faire une capture d'écran ou une photo avec un appareil sécuritaire, ou copier, imprimer ou enregistrer le contenu sur une clé USB.
- Aidez-la à ajuster les paramètres de confidentialité et de sécurité sur ses comptes de médias sociaux, y compris les paramètres de marquage.
- Si cela ne présente pas de danger, aidez-la à bloquer ou à mettre l'auteur en sourdine.
- Faites-lui savoir que certains de ces comportements peuvent être illégaux et qu'elle peut envisager d'en parler à la police ou à une avocate.

Pour plus de conseils, consultez notre liste de contrôle pour la planification de la sécurité technologique.

Est-ce que quelqu'un:

Vous harcèle, vous maltraite, vous punit ou vous menace par SMS, appli de communication (WhatsApp, FaceTime), courriel ou téléphone?

- Est-ce que quelqu'un vous a dit des choses par téléphone pour vous blesser ou vous effrayer?

- Devez-vous faire des choses avec votre téléphone pour que votre partenaire violent ne s'énerve pas ou ne se mette pas en colère?
- Est-ce que quelqu'un vous envoie constamment des messages ou se met en colère si vous ne lui répondez pas?

Stratégies de sécurité technologique suggérées :

Pour aider à documenter les abus par téléphone et par SMS:

- Aidez la survivante à écrire ce qui a été dit pendant les appels et à conserver un journal (souvent répertorié sous la rubrique «Récents»).
- Si possible, elle peut faire une capture d'écran, prendre une photo avec un appareil sécuritaire, imprimer ou enregistrer les journaux sur une clé USB ou à une nouvelle adresse courriel.
    - Certains enregistrements d'appels et de SMS peuvent également être demandés aux opérateurs de téléphonie mobile.
- Aidez-la à conserver les messages violents en utilisant des méthodes similaires: copie, capture d'écran, photographie, impression ou sauvegarde.
- Pour protéger les données existantes, il est conseillé de désactiver le Wi-Fi et le Bluetooth, puis de mettre le téléphone en mode avion.
- Si la survivante décide de faire appel à la police ou à une avocate, elle peut apporter le téléphone et tous les enregistrements sauvegardés pour aider à documenter formellement la violence (qui peut s'avérer illégale).

Pour plus de conseils, consultez notre liste de contrôle pour la planification de la sécurité technologique.

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

- Est-ce que quelqu'un possède des photos ou des vidéos privées de vous, avec ou sans votre consentement?
- Est-ce que ces personnes ont partagé ces photos ou menacé de les partager?
- Vous ont-ils dit ces choses en personne ou vous les ont-ils envoyées?

Stratégies de sécurité technologique suggérées:

Si une image intime est partagée sans consentement:

- Aidez la survivante à demander à la personne qui a partagé l'image de la retirer et de la supprimer, si elle peut le faire en toute sécurité.
- Aidez-la à signaler l'image à la plateforme de médias sociaux ou au site web où elle a été partagée.
- Si elle craint que l'image soit partagée sur l'une de ces plateformes, vous pouvez déposer un dossier auprès de StopNCII.org
- Dites-lui que le partage d'images intimes sans consentement est illégal. Elle peut envisager de s'adresser à une avocate, à un service juridique ou à la police pour obtenir du soutien.

Pour plus de conseils, consultez notre liste de contrôle pour la planification de la sécurité technologique.

Est-ce que quelqu'un:
Sait où vous êtes, ce que vous faites, ou vous traque

à l'aide d'applis de localisation/GPS ou de caméras cachées?

- Est-ce que quelqu'un utilise votre téléphone pour vous surveiller ou savoir où vous allez?
- Est-ce que quelqu'un sait des choses que vous ne lui avez pas dites? Comment pensez-vous qu'ils l'ont appris?
- Est-ce que quelqu'un semble connaître certaines choses mais pas d'autres?
  Quelles sont les choses qu'ils savent? Quand savent-ils où vous êtes? D'où viennent ces informations?
- Si la survivante soupçonne que sa position est surveillée:
  - ses appareils, son domicile, sa voiture, ses biens ou ceux de ses enfants peuvent être compromis.

 Stratégies de sécurité technologique suggérées:

Si la survivante craint d'être traquée ou suivie:

- Aidez-la à utiliser un appareil «sécuritaire», comme un nouveau téléphone ou un téléphone emprunté à une amie ou une personne de confiance, pour planifier leur sécurité.
  - Elle peut également choisir de confier cet appareil à une personne de confiance.
- Aidez-la à repérer des schémas dans ce que la personne violente semble savoir. Par exemple, est-ce qu'elle sait toujours où se trouve la survivante ou seulement lorsqu'elle utilise certains moyens de transport?

    - L’inventaire de ce que semble savoir l’auteur et de l’origine de ces informations peut aider à identifier les sources possibles de surveillance.
    - Par exemple, si les données de localisation correspondent à des trajets en covoiturage mais pas à d’autres trajets, une appli de covoiturage peut être compromise.
- Consultez les paramètres de localisation du téléphone et les paramètres spécifiques à l’appli pour vérifier ce qui partage les informations de localisation.
    - Vérifiez également la présence de dispositifs de suivi physique tels que les AirTags ou les Tiles.
- Dites-lui que la traque et le suivi non autorisé peuvent être illégaux.
    - Elle peut envisager de s’adresser à la police ou à une avocate pour obtenir une aide supplémentaire.

Pour plus de conseils, consultez notre liste de contrôle pour la planification de la 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.