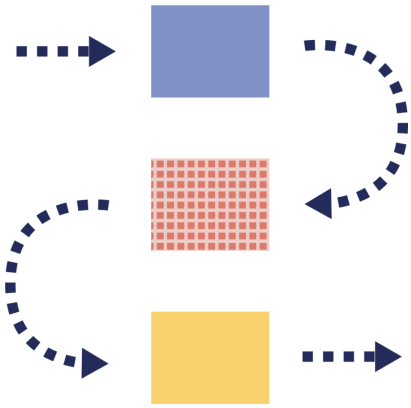
Sécurité technologique Canada

# Planification de la sécurité technologique



Cette trousse fournit aux femmes, aux jeunes, aux personnes d'une diversité de genres et au personnel de première ligne des informations sur l'intégration de la technologie dans la planification de sécurité, de manière à reprendre un certain contrôle en cas de harcèlement, de menaces, de surveillance ou d'abus par l'auteur de violence.

Les survivantes et le personnel antiviolence constatent de plus en plus souvent que les auteurs utilisent la technologie pour harceler les femmes. La violence fondée sur le genre facilitée par la technologie (VFGFT) se produit lorsque la technologie (comme un téléphone, un ordinateur, une montre intelligente ou un appareil connecté) sert à commettre des actes abusifs, tels que la violence conjugale, le harcèlement, la traque, les agressions sexuelles, l'usurpation d'identité, l'extorsion, ainsi que le tournage et le partage non consensuels d'images intimes.

Le contenu de cette trousse est à jour au moment de la publication, mais nous savons que la technologie évolue rapidement. Nous vous encourageons à consulter régulièrement notre site pour des informations actualisées et à contacter votre maison d'hébergement locale pour un soutien supplémentaire.

## 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.»

# Documenter la violence technologique

La façon dont la technologie est utilisée à des fins de harcèlement et de contrôle peut vous sembler invraisemblable. Cependant, il est important de faire confiance à votre instinct. Si vous pensez être surveillée ou harcelée par le biais de la technologie, c'est peut-être le cas. Le fait de préciser ce qui arrive, y compris les tactiques et les technologies utilisées, peut aider à déterminer s'il s'agit de violence fondée sur le genre facilitée par la technologie (VFGFT) et, le cas échéant, comment y remédier.

Voici quelques bonnes raisons de de documenter tout ce qui vous arrive:

- Vous aurez une vue d'ensemble de la situation, ce qui peut s'avérer utile si vous souhaitez engager une action en justice.
- Vous serez alertée de toute escalade dans la surveillance et le contrôle, ce qui peut signaler que le danger augmente.
- Cela vous aidera à repérer les schémas de VFGFT et à déterminer comment l'auteur de violence utilise une technologie ou une autre.

## Conseils pour la documentation

- **Tenez un journal de tous les incidents**, même si vous n'êtes pas certaine de vouloir faire appel à la police. Parmi les informations que vous pouvez inclure, citons la date, l'heure, le lieu, les coordonnées de l'agent·e de police (si l'incident a été signalé), les témoins (s'il y en a), la technologie présumée utilisée (téléphone, courriel, etc.), et enfin, une brève description des faits.
- **Prenez-en note tout ce qui concerne l'événement ou l'incident**. Si vous recevez un message menaçant par courriel, SMS ou messagerie vocale, assurez-vous de le sauvegarder. Prenez une photo ou une capture d'écran. Même s'il peut être tentant de les supprimer, sauvegarder les messages pourrait révéler des tendances utiles pour établir des stratégies de sécurité et fournir les preuves nécessaires.

- **Réfléchissez à la technologie que l'auteur pourrait utiliser**. Dans certains cas, les femmes ont de forts soupçons quant à la technologie utilisée par l'auteur de violence en fonction du type d'abus, des tactiques de l'auteur et de ce qu'elles savent de lui.
- **Pensez d'abord à votre sécurité**. Dans certains cas, lorsqu'un auteur apprend qu'une femme documente les abus, la surveillance, le contrôle et la violence physique peuvent s'intensifier. Vous êtes la mieux placée pour évaluer la situation et les différents scénarios possibles. Faites confiance à votre instinct et veillez au mieux à votre sécurité.
- **Ne documentez que les informations pertinentes**. Gardez à l'esprit que ces informations pourraient éventuellement servir de preuves ou être partagées par inadvertance avec l'auteur des faits. Par exemple, vous ne souhaitez peut-être pas documenter des photos personnelles qui ne sont pas utilisées dans le cadre de la violence numérique.

# Ce qu'il faut documenter

## Courriels

- Les courriels contiennent des adresses IP qui pourraient révéler l'adresse IP d'origine et, par conséquent, l'identité de la personne qui a envoyé le message. Pour cette raison, il importe de ne pas supprimer le courriel et de ne pas le transférer.
- Si vous sauvegardez le contenu d'un courriel en l'imprimant ou en faisant des captures d'écran, veillez à sauvegarder également l'en-tête (souvent caché et pouvant être trouvé dans les paramètres). C'est là que sont stockées les informations IP. L'accès à l'en-tête peut varier en fonction de la messagerie que vous utilisez (Gmail, Outlook, Yahoo! Mail, etc.).
- Si vous craignez que l'auteur puisse accéder au compte et supprimer des courriels, il est suggéré d'imprimer ou de faire des captures d'écran du contenu, y compris des en-têtes. Les courriels transférés perdront les informations d'identification nécessaires à l'établissement de preuves.

## Messages texte

- Les messages texte (SMS) qui sont simplement stockés sur un téléphone peuvent être supprimés par inadvertance ou être automatiquement supprimés si vous manquez d'espace. Faites une capture d'écran ou une photo des SMS pour conserver les preuves.
- Faites également une capture d'écran de la page de contact pour montrer que les messages de harcèlement de l'auteur sont associés à son numéro de téléphone.
- Le contenu des SMS n'est conservé par le fournisseur de téléphonie mobile que pendant une durée limitée. Si vous travaillez avec les forces de l'ordre, demandez-leur d'envoyer une lettre au fournisseur de téléphonie dès que possible, pour l'aviser de ne pas détruire les données.

## Harcèlement dans les médias sociaux et sur Internet

- Pour conserver des preuves de harcèlement sur les médias sociaux, faites une capture d'écran du harcèlement ou de l'abus sur votre ordinateur ou appareil mobile.
- Certains sites proposent d'autres moyens de documenter l'activité sur le site ou sur votre page. Par exemple, en utilisant la fonction «Télécharger vos informations» (DYI) de Facebook, vous pouvez capturer tout le contenu et l'enregistrer pour plus tard.
- En cas de collaboration avec les forces de l'ordre, une lettre peut être envoyée à l'entreprise de médias sociaux ou au site Web pour leur demander de conserver les informations du compte, ou contactez l'équipe du Service d'entraide internationale du ministère de la Justice.

- Vous pouvez envisager de signaler le harcèlement à l'entreprise de médias sociaux ou au site web. N'oubliez pas de documenter d'abord si vous voulez avoir des preuves car, si cela enfreint les conditions d'utilisation du site ou les directives relatives au contenu, l'entreprise peut supprimer le contenu.

### Harcèlement téléphonique

- Vous pouvez envisager d'enregistrer vos conversations téléphoniques pour conserver des preuves de harcèlement ou de menaces, car le Canada autorise l'enregistrement avec le consentement d'une seule partie.

### Usurpation de numéro de téléphone ou d'identité

- Documentez vos journaux d'appels en prenant une photo de l'identifiant de l'appelant. N'oubliez pas d'indiquer la date et l'heure des appels.
- Conservez vos registres téléphoniques pour indiquer le numéro de l'appel d'origine, la date et l'heure.

Notre modèle de journal de la violence facilitée par la technologie peut vous aider à documenter ce qui vous arrive. Pour plus d'informations sur la manière de stocker vos preuves numériques, consultez notre fiche d'information «Comment sauvegarder et stocker les preuves de violence facilitée par la technologie».

*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 *Documenting Abuse*.

# Journal du harcèlement et des abus facilités par la technologie

## Qu'est-ce qu'un journal sur le harcèlement et les abus facilités par la technologie?

On parle de harcèlement et de violence fondée sur le genre facilitée par la technologie (TFGBV) lorsqu'un auteur de violence utilise la technologie comme outil pour surveiller une personne et lui causer du tort. Il peut s'agir de repérer l'endroit où vous vous trouvez, d'envoyer des SMS de harcèlement et de menacer de partager des images sans votre consentement. Parmi les technologies utilisées à mauvais escient figurent les appareils et les comptes.

Ce document comporte un modèle de journal permettant de documenter la violence en détail. Deux journaux sont fournis, sous forme longue et brève; choisissez celui qui convient le mieux à votre situation.

## Je tiens un journal sur le harcèlement et les abus facilités par la technologie pour:

- Documenter les preuves au moment où les abus se produisent, ce qui les rend plus fiables devant un tribunal
- Étayer les preuves recueillies
- Percevoir les schémas et les escalades en vue de planifier ma sécurité
- Fournir des preuves à la police et au personnel antiviolence un aperçu des risques auxquels je suis confrontée afin de recevoir un soutien adapté à mes besoins
- Reprendre le contrôle de ma vie et être proactive
- Valider mon expérience. Cela peut être utile si l'auteur de violence minimise ou nie ses actions, ou *gaslight* la personne. Le *gaslighting* est une forme d'abus psychologique où l'auteur prétend que l'abus n'a pas eu lieu et accuse la victime de «devenir folle».
- Ne pas oublier le comportement d'un auteur de violence. Les souvenirs peuvent s'estomper avec le temps. Un journal peut renforcer une plaidoirie devant un tribunal ou aider une survivante à décider ce qu'elle doit faire si un partenaire violent tente de rétablir le contact.

# Demeurez en sécurité pendant la collecte des preuves

**Pensez à l'endroit où vous pouvez entreposer vos journaux en toute sécurité. Il peut s'agir d'un bureau fermé à clé au travail, de l'intervenante qui vous soutient ou d'un·e ami·e proche. Faites-vous confiance. C'est vous qui connaissez le mieux votre situation.**

Si vous décidez de fournir vos journaux à la police ou à d'autres services, on vous demandera peut-être des détails supplémentaires sur l'auteur de violence. Ces éléments peuvent inclure des informations sur la technologie utilisée, notamment:

- Informations sur le fournisseur Internet ou téléphonique, et sur le compte;
- Appareils, tels que téléphones, ordinateurs, tablettes, appareils photo, drones, disques durs externes, USB, appareils pour enfants, etc.;
- Comptes ou applis qui ont été utilisés dans le cadre de l'abus, tels les médias sociaux ou les comptes bancaires;
- Adresses courriel, numéros de téléphone, comptes infonuagiques, noms d'utilisateur, avatars, pseudonymes, identifiants en ligne, etc.
- Toute autre information relative aux technologies utilisées: mots de passe, associés en ligne, appareils de surveillance, adresses de fournisseurs Internet, vol d'identité ou fraude, etc.

**Note: Bien qu'il puisse être utile de recueillir les informations ci-dessus si vous pouvez le faire en toute sécurité, ces détails ne sont pas inclus dans le journal de harcèlement car ils ne s'appliquent pas forcément à toutes les situations, ni ne sont toujours susceptibles d'affecter la sécurité. Réfléchissez à une manière créative de documenter les événements, tout en tenant compte de votre sécurité.**

**Télécharger un journal sur le harcèlement et les abus facilités par la technologie**

*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 Tech Safety Project de WESNET, d'après leur ressource: Stalking and Tech-Facilitated Abuse Log.*

# Amorces de conversation pour la planification de sécurité technologique

## 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.*

# Évaluation de la violence technololgique: Conseils pour le personnel antiviolence

## Meilleures pratiques pour les programmes

La sécurité et la vie privée des femmes sont souvent compromises par des auteurs de violence qui utilisent la technologie et les informations personnelles des survivantes à mauvais escient. En tant qu'intervenante de première ligne, il est important de prendre le temps de s'informer pour mieux orienter les survivantes quant à la manière dont la technologie peut être utilisée pour faciliter le harcèlement et la surveillance.

Les informations suivantes offrent un cadre pour soutenir les femmes, afin qu'elles soient en mesure d'identifier et de répondre aux différentes formes d'abus technologiques, et de planifier leur sécurité. Il faut penser stratégiquement au rôle de la technologie dans nos vies quotidiennes si on veut l'inclure dans un plan de sécurité. Lorsque les auteurs de violence utilisent la technologie pour arriver à leurs fins, il est tout à fait naturel de vouloir jeter des appareils ou fermer des comptes en ligne. Toutefois, certains individus violents peuvent intensifier leur comportement contrôlant et dangereux s'ils ont l'impression d'avoir perdu le contrôle de leur partenaire ou leur ex-partenaire. Les questions ci-dessous ont pour but d'effectuer une évaluation rapide; elles ne constituent pas une liste détaillée de tous les problèmes de sécurité liés à la technologie auxquels une femme pourrait être confrontée.

Les intervenantes antiviolence doivent éventuellement discuter plus en profondeur des préoccupations spécifiques de chaque femme, ainsi que des stratégies permettant d'accroître sa sécurité, de documenter les incidents et de chercher du soutien. Les autres ressources de notre Trousse d'outils sur la sécurité et la confidentialité technologiques peuvent vous être utiles dans ce processus. Gardez à l'esprit que les femmes participent souvent à des groupes de soutien ayant peu d'interactions directes avec le personnel antiviolence. Pour ce faire, envisagez d'incorporer cette information comme sujet de groupe de soutien.

## Étapes de l'évaluation du mauvais usage et de la sécurité des technologies

- *Donner la priorité à la planification de la sécurité: Quelles sont vos préoccupations actuelles en matière de sécurité?*
- *Réduire le nombre de technologies qui pourraient être utilisées:* Que s'est-il passé pour que vous soyez préoccupée ou vous sentiez en danger?
- *Évaluer les connaissances et la compréhension des femmes:* Comment pensez-vous que cela se produit?

Ces questions ouvrent une conversation qui permettra de donner la priorité à la sécurité. Il s'agit de discuter des types d'appareils ou d'applications susceptibles d'être utilisés à mauvais escient, et d'identifier la meilleure façon de répondre aux besoins et de partager un maximum de connaissances.

Vous trouverez ci-dessous des questions qui traitent d'abus technologiques pour vous aider à entreprendre le processus de réponse, une fois que vous aurez déterminé ce qui se passe:

### 1. Êtes-vous préoccupée par le fait que l'auteur de violence puisse savoir où vous êtes en permanence? Voici quelques méthodes courantes de surveillance:

- Par le biais de votre appareil mobile
- Par le biais d'applications qui utilisent votre GPS
- Par le biais des médias sociaux
- Par vos proches
- À travers votre voiture ou d'un appareil de surveillance sur le véhicule
- Grâce à un dispositif de localisation tel que Tile ou AirTag

## 2. Craignez-vous que l'auteur puisse avoir accès à vos communications avec d'autres personnes? Voici quelques communications qui peuvent être compromises:

- Par courriel
- Par appareil mobile (par exemple, SMS ou appels)
- Communication téléphonique
- Messages privés instantanés ou directs (MP et MD)

## 3. Êtes-vous préoccupée par des informations qui sont publiées à votre sujet en ligne? Voyons comment les informations vous concernant peuvent être partagées en ligne:

- Par le biais de vos comptes de médias sociaux
- Par les comptes de médias sociaux de l'auteur
- Par les comptes de médias sociaux de vos enfants/famille/ami·e·s
- Pouvez-vous préciser vos préoccupations au sujet de ces comptes?
  - L'auteur de violence publie des choses terribles.
  - L'auteur surveille les comptes de médias sociaux pour trouver des informations sur vous.
  - L'auteur accède à des comptes en ligne sans votre permission.
- Y a-t-il d'autres informations en ligne vous concernant qui vous préoccupent?
  - Sites web du travail ou de l'école
  - Forums et groupes communautaires
  - Applis

## 4. Avez-vous des préoccupations concernant l'utilisation de la technologie par votre entourage et la possibilité que cela compromette votre sécurité?

- Est-ce que vos proches utilisent des applications qui vous préoccupent sur leurs appareils (cellulaire, iPads, tablettes, etc.)?
- Est-ce que votre famille joue à des jeux qui vous inquiètent?
- Est-ce que l'auteur a accès à la technologie des enfants ou d'autres membres de la famille?

## 5. Êtes-vous préoccupée par votre capacité à continuer à utiliser la technologie tout en protégeant votre sécurité et votre vie privée?

- Y a-t-il des appareils spécifiques, tels que votre cellulaire ou votre ordinateur portable, que vous voulez que l'on examine pour votre sécurité?
- Devez-vous passer par vos comptes de réseaux sociaux pour connaître les paramètres de confidentialité et de sécurité

### 6. Quelles sont les autres préoccupations concernant votre vie privée et votre sécurité?

- Avez-vous besoin de vous référer à d'autres technologies pour comprendre les paramètres de confidentialité et de sécurité? Si oui, quelles sont-elles?

*La violence fondée sur le genre 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, sachez que 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 projet Safety Net de NNEDV, selon leur ressource «Assessing for Technology Abuse.»

# Liste de contrôle pour la planification de sécurité technologique

La planification de sécurité technologique doit toujours être effectuée en tandem avec la planification de sécurité plus conventionnelle. La violence en ligne et hors ligne sont interconnectées et la planification doit aussi tenir compte des risques qui ne sont pas directement associés à la technologie. La présente liste de contrôle se veut le complément d'un plan de sécurité en bonne et due forme, et non une liste indépendante.

Lorsque vous établissez un plan de sécurité avec une personne qui a vécu la VFGFT, il ne faut pas oublier 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 compte 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 est parfois nécessaire de prendre des précautions additionnelles dans ces situations.

Dans certains cas, vous pouvez avoir recours à un spécialiste informatique ou aux forces de l'ordre, par exemple pour la détection de stalkerware ou d'autres logiciels espions.

## Mots de passe

- [ ] Make a list of all devices (e.g. laptop, cell phone, Fitbit, AirTags, home security system, smart car, Internet-connected devices, Siri/Alexa, Bluetooth-connected sound systems, etc.) and accounts (e.g. social media, email, online shopping, online food services, transportation apps, cloud accounts, fitness trackers, games, etc.). See appendix A for a list of potential accounts.
- [ ] Note which of these the perpetrator has access to, knows the passwords to, or may know the passwords to.
- [ ] Think about what information is included on those accounts (e.g. home address, phone number, email address, credit card information, personal messages, Internet search history, communication about safety planning, etc.).

- [ ] Change all passwords to unique passphrases that the perpetrator would not be able to guess. Avoid using things like the names of children or pets, important dates, old addresses, or old phone numbers. A passphrase is a sentence that is easy to remember but would not be easy to guess. Adding symbols of numbers for letters can make it even more difficult to guess (e.g. L1tTl3R3dC0rV3Tt3).
- [ ] Do not use the same password for multiple accounts.
- [ ] Use a unique passphrase for each account or use a password manager.
- [ ] Change the password to your home Wi-Fi.
- [ ] For security questions on accounts, make up fake answers or do not use questions that the perpetrator would be able to guess; otherwise, they may be able to access the account (e.g. instead of using your mother's maiden name, make up an answer when they ask for your mother's maiden name and answer with something different. Just make sure you will remember your fake answer).
- [ ] Turn off all automatically saved passwords on all devices and accounts.
- [ ] Sign out of all accounts and devices when not using them.
- [ ] Use two-factor authentication on any app or account that allows for it. Two-factor authentication requires you to enter a password that is sent to your phone or email to confirm that it is actually you accessing the account.
    - [ ] For general information on two-factor authentication, see HackBlossom.
    - [ ] Use this website to see which common apps use two-factor authentication.
- [ ] Do not use social media accounts to sign in to other accounts (e.g. "Sign in with Facebook" or "Sign in with Google" options).
- [ ] Remove the perpetrator's email addresses or devices from shared accounts and as Trusted Devices on your accounts.

# Blocage, suppression d'amis

- Envisagez de bloquer ou de supprimer de votre liste d'amis l'adresse courriel, le numéro de téléphone ou l'identifiant sur les médias sociaux de l'auteur de violence. Assurez-vous d'abord d'avoir recueilli toutes les preuves nécessaires. Certains programmes suppriment ou empêchent l'accès aux conversations et aux informations de l'autre personne une fois que son compte a été supprimé de la liste d'amis, ou bloqué.
- Lorsque vous décidez de bloquer ou de supprimer des amis, demandez-vous si cela pourrait aggraver la situation. L'accès aux médias sociaux de l'auteur peut présenter des avantages (comme le fait de savoir où il se trouve) qui méritent d'être pris en compte.
- Réfléchissez aux proches et membres de votre famille qui pourraient avoir votre partenaire violent comme «ami» sur leurs comptes. Demandez-leur de ne pas publier d'informations ou de photos vous concernant et de ne rien divulguer à votre sujet à l'auteur des faits.

# Harcèlement, traque et surveillance

- Utilisez un cache-caméra sur tous vos appareils lorsque vous n'utilisez pas la caméra.
- Si l'auteur surveille votre appareil ou vos comptes, envisagez d'utiliser un autre appareil (l'ordinateur d'un proche, un appareil au travail ou un ordinateur à la bibliothèque) pour rechercher des informations et commencez à planifier la sécurité de vos appareils.
- Demandez-vous quelles informations personnelles sont publiées en ligne (adresse du domicile sur une invitation à un anniversaire, numéro de téléphone dans une publication Facebook, nouveau lieu de travail sur LinkedIn, etc.) et déterminez si vous souhaitez supprimer ces informations ou les rendre privées. N'oubliez pas que d'autres personnes pourraient partager ces informations avec l'auteur de violence, même si vous les avez bloquées.

- Désactiver ou limiter les fonctions de localisation sur vos appareils lorsqu'ils ne sont pas utilisés.
- Désactivez les fonctions de localisation comme Trouver mon téléphone ou Trouver mes amis.
- Supprimez l'historique des lieux visités, en particulier avant et après votre arrivée dans une maison d'hébergement ou dans un autre endroit sécuritaire.
- Ne vous «enregistrez» pas sur les médias sociaux lorsque vous participez à un événement.
- Modifiez les paramètres de confidentialité des applis et des médias sociaux pour qu'ils soient privés dans la mesure du possible.
- Ne publiez pas sur les médias sociaux de photos contenant des métadonnées ou des informations de fond qui pourraient révéler où vous êtes allée. Une façon de supprimer les métadonnées de localisation d'une photo consiste à publier une capture d'écran plutôt que la photo originale qui contient les métadonnées.
- Supprimez les adresses courriel ou les appareils de l'auteur de vos comptes partagés et supprimez son téléphone des Appareils de confiance sur tous vos comptes. Voir l'annexe A pour une liste des comptes.
- Vérifiez l'activité du compte pour voir si des adresses IP inconnues y accèdent.
- Si vous craignez que l'auteur ait accès à vos comptes, envisagez d'utiliser une boîte postale pour les comptes et livraisons en ligne. Considérez le risque que l'auteur accède aux informations des cartes de crédit ou utilise le compte à votre détriment s'il y a accès.
- Déconnectez votre téléphone ou d'autres appareils de ceux de l'auteur (la stéréo Bluetooth dans sa voiture ou chez lui, les notifications de fitness sur sa montre intelligente, etc.)
- Fouillez vos effets personnels (sacs à main, voitures, vestes, etc.) à la recherche de dispositifs GPS ou d'autres appareils d'enregistrement.
- Examinez tous les cadeaux ou les objets inhabituels de la maison, y compris les articles pour enfants, à la recherche de caméras cachées ou de dispositifs d'enregistrement.
- Réfléchissez aux informations qui se trouvent sur les appareils et les comptes de vos enfants (téléphones, consoles de jeux, médias sociaux, etc.) et à celles qui pourraient fournir des informations à l'auteur.
- Demandez-vous si l'auteur peut accéder aux informations sur le système de sécurité du domicile, comme l'accès aux caméras ou des informations sur les personnes qui sortent ou entrent dans la maison.
- Envisagez d'utiliser un dispositif ou un programme (scanners de réseau, scanners de port, détecteurs de signaux RF, etc.) capable de détecter certaines caméras cachées pour scanner votre Wi-Fi ou votre maison.
- Faites l'inventaire des applis sur votre téléphone et supprimez celles qui ne vous sont pas familières
- Si vous craignez que l'auteur ait installé un logiciel espion sur vos appareils, vous pouvez demander à un spécialiste informatique ou aux forces de l'ordre de vérifier l'appareil. N'oubliez pas que si un logiciel espion est installé, l'auteur peut être en mesure de voir toutes les activités sur l'appareil, ce qui peut aggraver la violence.
    - The Clinic To End Tech Abuse propose également des ressources pour aider à identifier les logiciels espions sur un appareil.
    - Signes qu'un appareil peut contenir un logiciel espion:
        - L'appareil fonctionne lentement
        - La batterie se décharge rapidement
        - Les données s'épuisent rapidement
        - L'appareil chauffe
        - L'appareil s'allume lorsqu'il n'est pas utilisé
        - Clics ou sons bizarres lors des appels
        - Prends beaucoup de temps pour s'éteindre
- Maintenez les systèmes d'exploitation de vos appareils à jour. Ces mises à jour corrigent souvent les éventuelles failles du système d'exploitation dont les pirates et les logiciels espions peuvent tirer parti. Vérifiez à nouveau vos paramètres de confidentialité après une mise à jour pour vous assurer qu'ils n'ont pas été modifiés.

- Envisagez de remplacer les appareils. Dans ce cas, vous ne devez pas effectuer de sauvegarde des données d'appareils précédents. Cela pourrait transférer un logiciel espion sur le nouvel appareil.
- Recherchez les dispositifs inhabituels fixés aux ordinateurs de bureau (les enregistreurs de frappe sont souvent fixés entre le clavier et l'ordinateur).
- Il convient de noter que les pirates et les ingénieurs informatiques expérimentés peuvent accéder à la localisation d'un appareil, même si cette fonction est désactivée dans les paramètres. Si l'auteur de violence a une formation informatique, votre sécurité technologique peut demander des efforts supplémentaires en fonction de ses compétences. Si tel est le cas, vous pouvez vous adresser à un spécialiste informatique ou aux forces de l'ordre.

# Comptes alternatifs

- Si l'auteur a accès à vos comptes et que vous n'avez pas d'autres options (par exemple, s'il vous oblige à partager vos mots de passe en vous menaçant de vous faire du mal autrement), créez un nouveau compte courriel ou de médias sociaux à son insu et auquel il n'a pas accès pour vos communications sensibles.
- Ne vous connectez pas à ce compte sur vos appareils personnels ou partagés. Utilisez un ordinateur au travail, à la bibliothèque ou celui d'un proche pour y accéder.

# Stockage en nuage, comptes partagés, accès non autorisé

- Retirez l'auteur de tous les comptes, appareils ou plans partagés, si vous pouvez le faire sans danger.
- Supprimez les connexions Bluetooth des appareils de l'auteur (ceux qui sont connectés à la chaîne stéréo de son domicile, à sa voiture, etc.)
- Réfléchissez au contenu automatiquement téléchargé ou connecté (calendriers, stockage iCloud pour les photos et les textes, Fitbit, montres intelligentes, etc.) et demandez-vous si l'auteur pourrait avoir accès à ces comptes ou informations.
- Assurez-vous que seuls vos appareils figurent dans la liste des Appareils de confiance sur tous vos comptes.
- Vérifiez la dernière activité sur tous vos comptes pour voir si une adresse IP ou un appareil inhabituel a accédé au compte.

# Historique de recherche

- Si l'auteur a accès à l'appareil ou au compte, il peut vérifier votre historique de recherche.
- Si vous cherchez de l'aide ou des ressources, utilisez un ordinateur sécuritaire (ordinateur public, d'un proche, au travail, etc.).
- Supprimez sélectivement l'historique des recherches sur Internet.
- Utilisez les modes «privé» ou «incognito» pour que l'historique des recherches ne soit pas enregistré.
- Désactivez les cookies dans les paramètres du navigateur.

# Images intimes ou «pornographie de vengeance»

- Dressez de mémoire une liste des images et des vidéos qui peuvent exister.
- Envisagez d'utiliser le programme de Facebook qui empêche d'autres personnes de télécharger des images sexuelles qui ont été enregistrées et «hachées» auprès de l'entreprise. Cependant, vous devrez envoyer ces photos à

Facebook pour que le programme puisse reconnaître et supprimer les images de Facebook et Instagram.

- Si vous pouvez le faire en toute sécurité, demandez à vos ex-partenaires de supprimer toute image intime et spécifiez que vous ne leur accordez pas la permission de les publier. Documentez cette communication.
- Demandez-vous si l'auteur a pu capturer des images sans consentement (caméra cachée, capture d'écran via Zoom ou Skype, etc.).
- Faites une recherche inversée d'images sur Google.
- Cherchez votre nom sur des sites pornographiques courants. Les gens sont souvent victimes de doxing et d'atteinte à leur réputation lorsque leurs images sont partagées.
- Créez une alerte Google pour votre nom. Vous serez avertie lorsque votre nom est mentionné en ligne et affiché avec vos images.
- Envisagez d'alerter la famille, les proches et les collègues de travail susceptibles de recevoir les images afin de réduire les préjudices.
- Si l'image a été partagée sans consentement, voir le Cyber Civil Rights Initiative Guide pour obtenir le retrait de contenu de l'Internet.
- Faites un signalement aux entreprises de médias sociaux ou pornographiques, car la plupart ont des politiques qui interdisent les images de nudité partagées sans consentement.
- Si vous partagez des images intimes, envisagez des stratégies de réduction des risques:
  - Évitez les images qui montrent votre visage ou des marques d'identification (tatouages, taches de naissance, etc.)
  - Évitez les images dans des lieux identifiables (par exemple, une pièce reconnaissable)
  - Utilisez des programmes comme Signal qui permettent de faire disparaître les messages
- Si des images ont été diffusées, envisagez d'utiliser un service réputé pour vous aider à faire retirer le contenu.

# Alertes Google

- Créez une alerte Google pour votre nom afin d'être avertie lorsqu'il apparaît en ligne. Cela peut vous alerter dans certains cas.
- Créez une alerte Google pour toutes les versions de votre nom (par exemple, Victoria Chan, Vickie Chan, Vicky Chan).

# Signaler les contenus préjudiciables aux entreprises de médias sociaux

- Rassemblez des preuves (par exemple, des captures d'écran) du contenu préjudiciable avant de le signaler, car il peut être supprimé par l'entreprise de médias sociaux s'il enfreint ses politiques.
- Voir les Media Safety Guides de HeartMob pour obtenir des conseils sur les politiques et les mécanismes de signalement des entreprises de médias sociaux.

# Mises à jour des logiciels, pare-feu et antivirus

- Mettez régulièrement à jour vos logiciels. Cela inclut vos appareils mobiles. Ces mises à jour corrigent souvent les failles de sécurité que les pirates pourraient exploiter.
- Activez les pare-feu et les antivirus sur tous les appareils.

# Collecte des preuves

- Créez un journal de toutes les expériences de VFGFT et incluez des informations telles que l'heure, la date, l'auteur, les preuves et d'autres informations utiles. Voir le modèle de journal de la violence facilitée par la technologie d'HFC ici
- Prenez des captures d'écran ou faites des enregistrements des comportements violents.
- Vérifiez si l'appli peut alerter l'auteur lorsque vous faites une capture d'écran. Si oui, il peut être préférable de prendre une photo ou une vidéo avec un autre appareil.
- Veillez à inclure le profil et les autres informations d'identification de l'auteur dans les preuves.
- Assurez-vous que la date des actes abusifs y figure.
- En cas de courriel violent, conservez le courriel original, car il contient des métadonnées telles que l'adresse IP de l'expéditeur.
- En cas de publication de contenu préjudiciable, capturez-le avant que la personne ait le temps de le supprimer.
- Conservez des copies des preuves dans un endroit sécuritaire. Sauvegardez ces informations dans au moins un autre endroit.
- Si l'auteur a accès à l'appareil ou au service infonuagique où se trouvent les preuves, il peut les supprimer.
- Conservez à la fois des copies imprimées et des copies numériques des preuves.

**Télécharger l'annexe a: Appareils et comptes à considérer**

*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 utiliser 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.*

*Nous remercions Suzie Dunn, doctorante à l'Université d'Ottawa, pour la création de cette fiche d'information.*

*Adapté du projet Technology Safety de la BCSTH, d'après leur ressource Technology Safety Planning Checklist.*

*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).