Liste de contrôle pour une rupture numérique : Sécurité en ligne après une séparation

Cette liste de contrôle est destinée au personnel de première ligne qui soutient les survivantes de violence technologique. Elle présente quelques-unes des principales mesures que peut prendre une survivante après avoir quitté son partenaire pour s'assurer que ses applis et comptes en ligne sont protégés.

Avant de commencer, rappelez-vous les principes du soutien centré sur la survivante. Voir les 4 principes fondamentaux de la sécurité technologique.

Étape 1 : Identifier les comptes et applis en ligne

Pour obtenir un portrait complet des risques numériques, commencez par dresser avec la survivante une liste de ses comptes en ligne. Les survivantes peuvent avoir des comptes qu'elles n'utilisent pas régulièrement ou auxquels elles ne pensent même pas, mais ces comptes peuvent néanmoins contenir des données personnelles auxquelles leur partenaire ou ex-partenaire peut avoir accès. Servez-vous de la liste ci-dessous pour établir une liste complète avec la survivante.

Types de comptes à vérifier :

- **Courriels** (Gmail, Outlook, etc.)
    - Il est possible d'accéder aux courriels pour surveiller les activités d'une survivante.
    - Vérifiez si la survivante possède plusieurs adresses courriel qu'elle a peut-être oubliées. Par exemple, ont-elles un ancien courriel personnel ou un courriel professionnel qu'elles n'utilisent plus ?
- **Médias sociaux** (Facebook, Instagram, TikTok, Discord, etc.)
    - Les comptes de médias sociaux peuvent servir à localiser une personne, envoyer des menaces et des messages de harcèlement, usurper l'identité d'une survivante, publier des contenus humiliants ou surveiller ses activités.
    - Incitez les survivantes à réfléchir à toutes les plateformes de médias sociaux qu'elles utilisent ou ont utilisées au cours des dernières années, et pas seulement les principales. Ont-elles des comptes sur des plateformes telles que Pinterest, Snapchat, Reddit, WeChat, etc.

- **Comptes bancaires et financiers** (banque en ligne, PayPal, profils d'achat en ligne, etc.)
    - Il est possible d'accéder aux comptes bancaires et autres comptes financiers pour dépenser les fonds d'une survivante et ouvrir un crédit à son nom.
- **Services de diffusion continue et de jeux** (Netflix, Spotify, Xbox, Twitch, Discord, etc.)
    - Ces comptes peuvent servir à effectuer des achats avec les méthodes de paiement de la survivante, ou un auteur peut se faire passer pour un autre joueur afin de se rapprocher de la survivante.
- **Applications de santé et de conditionnement physique** (Apple Health, Fitbit, etc.)
    - Ces applis peuvent suivre la localisation et les données de santé d'une survivante.
- **Applis de voyage et de covoiturage** (Uber, Lyft, etc.)
    - Ces applis peuvent servir à localiser une survivante et savoir où elle se trouve.
- **Services de livraison de nourriture** (DoorDash, UberEats, etc.)
    - Ces applis/comptes peuvent être utilisés pour effectuer des achats avec le mode de paiement de la survivante ou pour se présenter à son adresse en se faisant passer pour un livreur.
- **Services de stockage en nuage** (Google Drive, iCloud, Dropbox, etc.)
    - Ces services peuvent servir à surveiller les courriels et les SMS, accéder aux photos ou télécharger des applis suspectes.

Remarques importantes sur la sécurité

- Des changements soudains, comme le blocage d'une personne, peuvent alerter l'auteur sur le fait que la survivante sait qu'il accède à

ses comptes. Cela pourrait aggraver le risque de violence ou permettre de détruire des preuves.

- Envisagez de prendre des mesures graduelles, d'élaborer un plan de sécurité ou de demander conseil avant d'agir.
- En cas de danger immédiat, conseillez à la survivante de contacter une organisation de soutien ou les services d'urgence.

Étape 2 : Sécuriser chaque compte et chaque appareil

Une fois les comptes identifiés, guidez la survivante à travers les étapes ci-dessous. Suivez ces étapes pour chaque compte/appli de la liste.

1. Modifier les mots de passe en toute sécurité

- Utilisez un mot de passe fort et unique que l'auteur ne peut pas deviner, comme « $pringIsH3r3! ».
- Évitez les mots de passe liés aux anniversaires, aux animaux de compagnie ou à d'autres détails personnels.
- Utilisez un gestionnaire de mots de passe si vous avez du mal à vous souvenir.
- N'utilisez pas le même mot de passe pour plusieurs comptes.

2. Vérifier la récupération du mot de passe et les paramètres de sécurité

La plupart des comptes demandent un courriel ou un numéro de téléphone de récupération en cas d'oubli du mot de passe. Veillez à ce que les informations relatives à la récupération **ne soient accessibles qu'à la survivante**. Si un auteur y a accès, il peut réinitialiser le mot de passe et accéder au compte.

- Allez dans **Paramètres du compte > Sécurité > Options de récupération** (cela varie selon la plateforme).
- Mettez à jour l'adresse courriel et le numéro de téléphone du service de recouvrement pour qu'ils soient inaccessibles à l'auteur.
- Mettez à jour les questions de sécurité de l'appli ou désactivez les questions de sécurité si l'auteur peut connaître les réponses aux questions actuelles. Il s'agit de questions prédéfinies que les plateformes utilisent pour vérifier votre identité si vous oubliez votre mot de passe. Les réponses aux questions de sécurité ne doivent pas nécessairement être réelles.

3. Activer l'authentification à deux facteurs (2FA)

L'authentification à deux facteurs est un moyen de rendre les comptes plus sécuritaires. Cela signifie que deux étapes sont nécessaires pour se connecter – comme taper son mot de passe puis saisir un code envoyé à son téléphone ou à son courriel.

- Certains appareils permettent aux utilisateurs d'activer cette fonction sous **Paramètres > Sécurité > Authentification à deux facteurs.**
- Si possible, mettez en place une méthode de sauvegarde, comme une appli d'authentification.
- Les options comprennent les SMS, une appli d'authentification (Google Authenticator, Microsoft Authenticator, etc.), ou une clé de sécurité.
- Si la survivante choisit d'utiliser un SMS ou une autre adresse courriel pour s'authentifier, assurez-vous qu'elle utilise un numéro de téléphone ou un courriel auxquels l'auteur n'a pas accès.

4. Examiner et supprimer les dispositifs non autorisés

- Pour les comptes en nuage (iCloud, Google Drive, etc.), vous pouvez vous déconnecter à distance de tous les appareils connectés aux comptes en nuage à partir des paramètres de sécurité du compte. La survivante doit se connecter à son compte iCloud ou Google et aller dans **Paramètres > Sécurité > Appareils ou Sessions actives**. Supprimez tous les appareils inconnus ou partagés.
- La plupart des applis de médias sociaux vous permettent de voir où votre compte est connecté. Vous trouverez ces informations dans **Paramètres > Sécurité > Appareils ou Sessions actives.**
- Recherchez dans les paramètres du compte de courriel les règles de transfert de messages qui pourraient envoyer des copies des messages à l'auteur. Cette opération s'effectue généralement par le biais de **Paramètres > Transfert et filtres** dans les comptes de courriel.
- Pour les comptes qui peuvent avoir plusieurs utilisateurs ou être partagés (Netflix, Google Drive, configurations de partage familial, etc.), assurez-vous qu'aucun utilisateur supplémentaire n'est lié aux comptes.
- Vérifiez les plans familiaux des opérateurs de téléphonie mobile, Partage familial d'Apple et Google Play Family pour voir s'il y a des appareils ou des comptes inconnus qui accèdent aux comptes.

5. Désactiver le partage de la localisation

- Sur un téléphone : Allez dans les **paramètres** du téléphone **> Localisation** et vérifiez si la localisation est activée. Désactivez-la si elle n'est pas nécessaire. Une survivante peut également sélectionner les applis qui peuvent accéder à sa position.

- Si vous utilisez Google : Accédez à **Google Maps > Partage de la position** et désactivez tout accès partagé.
- Si vous utilisez Apple : Ouvrir **Trouver mon iPhone > Personnes > Supprimer les contacts partagés**.
- Médias sociaux : Les survivantes peuvent vérifier les paramètres de localisation sur Snapchat, Facebook et Instagram en allant sur leur profil et en consultant les paramètres du compte.
- Désactiver le suivi en temps réel dans les applis de conditionnement physique et de covoiturage.

6. Ajuster les paramètres de confidentialité sur les médias sociaux

- Les survivantes doivent se rendre dans les paramètres de leur compte et régler leur profil sur **privé** afin de contrôler qui peut voir les messages et leurs informations personnelles.

- Supprimez tous les contacts susceptibles de partager des informations avec l'auteur, même des personnes auparavant dignes de confiance. Il peut s'agir d'amis communs, de membres de la famille ou de toute personne susceptible d'être encore en contact avec l'auteur et de lui donner accès au compte de la survivante, soit directement, soit en partageant des captures d'écran ou des mises à jour.
- Examinez les permissions des applis qui autorisent l'ouverture de sessions par des tiers.
- Envisagez de télécharger l'historique des médias sociaux s'il est nécessaire à des fins de preuve par le biais des paramètres de confidentialité.

Pour plus d'informations, voir Guide de conversation: Messages de harcèlement et de menace.

7. Supprimer les modes de paiement enregistrés dans les applis.

- Vous pouvez le faire sur la plupart des appareils en allant dans **Paramètres > Méthodes de paiement** et en supprimant les cartes de crédit ou PayPal sur l'appli. Faites de même pour chaque appli (covoiturage, livraison de nourriture, boutiques en ligne, etc.).

Étape 3 : Plan de sécurité permanent

Une fois ses comptes sécurisés, suggérez à la survivante de continuer à surveiller sa présence numérique :

- **Vérifiez régulièrement les activités suspectes** ou les tentatives de connexion par le biais des paramètres de compte et de confidentialité.
- **Mettez en place une méthode de récupération de secours en étant avertie de toute activité suspecte** par un second courriel ou numéro de téléphone.
- **Stockez vos fichiers en toute sécurité** à l'aide d'une clé USB, d'un dossier protégé par un mot de passe ou d'un compte courriel fiable.

Les survivantes peuvent ne pas vouloir impliquer les forces de l'ordre dans l'immédiat. Encouragez-les à conserver les preuves de l'accès d'appareils inconnus à leurs comptes, appareils et applis, afin d'avoir des preuves en cas de besoin. Voici quelques suggestions :

- Prendre des captures d'écran et des enregistrements d'écran vidéo de tout appareil inconnu accédant à des comptes, appareils et applis avant de les supprimer.
- Inclure le profil de la personne, y compris son numéro de téléphone et tout autre détail permettant de savoir qui elle est.

- Sauvegarder et imprimer toutes les transactions effectuées sur le compte de la survivante à son insu et sans son consentement.
- Conservez les preuves en lieu sûr (un appareil ou un compte auquel l'auteur n'a pas accès). Sauvegardez-les également ailleurs, au cas où.

La situation de chaque survivante est unique et ses choix doivent guider la réponse. En fournissant des informations, des options et un soutien, le personnel de première ligne peut aider les survivantes à reprendre le contrôle de leurs finances tout en accordant la priorité à leur sécurité.

Ressources suggérées

- Qu'est-ce que la violence fondée sur le genre facilitée par la technologie?
- Êtes-vous la cible de violence technologique (affiche)
- Liste de contrôle pour la planification de sécurité technologique
- Planification de la sécurité technologique: amorces de conversation pour le personnel antiviolence soutenant des survivantes autochtones
- Votre sécurité, votre voix: Les étapes d'une rupture numérique
- Liste de contrôle pour la planification de sécurité technologique
- Trousse à outils pour la préservation des preuves numériques
- Outil de rupture numérique

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. En tant que travailleuse de soutien, il est important de faire savoir aux survivantes qu'elles ne sont pas seules. Pour obtenir des conseils sur la VFGFT, vous pouvez consulter notre site securitetech.ca.

Ce projet a été soutenu par une subvention du programme Net Good de CIRA.