Guide de conversation : Sécuriser vos informations personnelles en ligne

Qu’est-ce qu’une information d’identification personnelle ?

Les informations d’identification personnelle sont toutes les informations qui peuvent être utilisées pour créer des comptes ou vérifier l’identité d’une personne. Il importe de conserver ce type d’informations personnelles en lieu sûr, car un partenaire ou un ex-partenaire peut s’en servir pour accéder aux

comptes de la survivante, ou se faire passer pour elle dans le but de créer de nouveaux comptes en son nom.

Voici ce à quoi peut ressembler l'utilisation abusive d'informations d'identification personnelle :

- Ouvrir des comptes bancaires ou contracter des emprunts au nom de la survivante
- Se connecter aux applis financières de la survivante pour obtenir des informations sur ses finances ou virer de l'argent de ses comptes
- Restreindre l'accès d'une survivante à l'argent en bloquant ou en fermant des comptes
- Ces informations peuvent servir aux partenaires violents pour localiser la nouvelle adresse d'une survivante, la contacter après qu'elle a changé de numéro, ou même découvrir des choses personnelles sur sa vie.

Voici quelques exemples d'informations d'identification personnelle :

- Nom complet
- Adresse du domicile
- Numéro de téléphone
- Courriel
- Date de naissance
- Nom de l'école
- Les noms d'utilisateur des médias sociaux (par exemple, des noms d'utilisateur tels que « Kate1981 » peuvent révéler des détails personnels tels que le nom et l'année de naissance d'une personne)
- Les informations relatives aux cartes de crédit ou aux opérations bancaires, telles que les numéros de compte, les codes d'accès et les mots de passe.

- Le numéro d'assurance sociale

Amorces de conversation avec les survivantes :

Avant de commencer, rappelez-vous les principes fondamentaux du soutien à la sécurité technologique centrée sur la survivante.

Étape 1 : Comprendre ce qui se passe

Commencez par poser des questions pour savoir comment l'auteur utilise les informations personnelles de la survivante. Cela permet de déterminer le niveau de risque et de préjudice et d'identifier les mesures les plus efficaces pour résoudre le problème. Vous pouvez poser les questions suivantes :

- Est-ce que votre partenaire ou ex-partenaire a accès à vos données d'identification personnelle (nom, date de naissance, NAS, adresse) et à celles de vos enfants, ainsi qu'à des documents ou à des états financiers ?
- Avez-vous accès à vos données d'identification personnelles et à celles de vos enfants (nom, date de naissance, NAS), ainsi qu'à des documents ou à des états financiers qui vous concernent ?
- Est-ce que votre partenaire ou ex-partenaire connaît les numéros de compte, les mots de passe et les codes PIN des services bancaires en ligne, d'autres applis financières et des comptes que vous possédez ?
- Est-ce que votre partenaire ou ex-partenaire a déjà accédé à vos comptes financiers ou ouvert un compte à votre nom

- Votre accès à vos documents est-il limité (par exemple, pas de Wi-Fi à la maison pour demander le remplacement d'une pièce d'identité, le partenaire ou l'ex-partenaire vous a dérobé les documents, etc.)

Étape 2 : Comprendre ce que veut faire la survivante

Les besoins et les objectifs de chaque survivante sont différents. Au lieu de supposer ce qui doit se passer ensuite, posez la question:

- Que souhaiteriez-vous voir se produire ? Que voulez-vous ?
- Voulez-vous impliquer l'institution financière ?
- Voulez-vous que les forces de l'ordre soient impliquées ?
- Souhaitez-vous conserver une trace de ce qui s'est passé ?

Étape 3 : Identifier les stratégies qui correspondent aux objectifs de la survivante

Une fois que les objectifs de la survivante sont clairs, aidez-la à élaborer un plan pour sécuriser ses comptes en ligne et réduire les méfaits. Nous nous concentrons ici sur les stratégies et les réponses technologiques. Vous devez également prendre toute autre mesure que vous recommanderiez normalement si, par exemple, un auteur enfreint un engagement de ne pas troubler l'ordre public ou une décision de justice, ou si vous avez des

inquiétudes immédiates ou urgentes concernant la sécurité de la survivante.

Voici quelques stratégies pour différents scénarios :

Si la survivante n'a pas accès à ses documents ou informations ou craint de ne plus y avoir accès, suggérez-lui de :

- Rassembler les documents relatifs aux comptes financiers, en faire des copies et les conserver en lieu sûr.
- Remplacer les documents manquants et les envoyer à l'adresse d'une personne de confiance.

Si l'auteur a déjà eu accès à des comptes ou possède les informations pour y accéder à l'avenir, suggérez à la survivante de :

- Remplacer les mots de passe par des combinaisons longues, composées de chiffres, de lettres et de symboles, comme $ummer1$myFavouriteeaon, sur un appareil auquel le partenaire ou l'ex-partenaire n'a pas accès, s'il est possible de le faire en toute sécurité.
- Changer de code PIN pour une nouvelle combinaison de chiffres que l'auteur n'a jamais utilisée. Choisir une séquence aléatoire de chiffres et éviter d'utiliser des chiffres que le partenaire ou ex-partenaire pourrait deviner facilement. Par exemple, ne pas utiliser la date de naissance des enfants, leur chiffre préféré, l'adresse de la maison, etc.
- Mettre à jour les réponses aux questions de sécurité des comptes (celles utilisées pour réinitialiser un mot de passe en cas d'oubli) avec de nouvelles réponses que l'auteur ne pourra pas deviner. Les réponses n'ont pas besoin d'être véridiques, les survivantes doivent simplement s'en souvenir.
- Ne pas enregistrer de nouveaux mots de passe et codes PIN sur leur appareil à moins d'avoir la certitude que leur appareil ou leur compte n'est pas surveillé ou utilisé par d'autres personnes.

Pour plus d'informations, consultez notre fiche Que faire si vous êtes victime d'une fraude financière.

Si la survivante souhaite intenter une action en justice :

Les survivantes peuvent ne pas vouloir impliquer les forces de l'ordre dans l'immédiat. Mais si les preuves ne sont pas conservées au moment où l'abus se produit, elles risquent de disparaitre. Encouragez-les à conserver les preuves afin d'en disposer en cas de besoin. Voici quelques suggestions :

Voici quelques suggestions :

- Envisagez de prévenir les forces de l'ordre si vous vous sentez en sécurité pour le faire. Faites savoir à la survivante que le fait de signaler l'incident à la police pourrait donner lieu à une enquête visant à déterminer si l'auteur a enfreint la loi.
- Prévoir des mesures de sécurité, en particulier pour se rendre au poste de police, car l'auteur peut soupçonner qu'elles sont en train de porter plainte si un traceur de localisation se trouve encore sur les effets personnels ou le véhicule de la survivante.
- Chercher un soutien juridique. Les survivantes peuvent s'adresser à une avocate civile ou à une organisation d'aide juridique. La survivante peut également envisager de demander une ordonnance civile de protection de manière indépendante ou avec le soutien d'une avocate ou d'une intervenante.
- Conservez une trace des documents financiers, faites-en des copies et conservez-les en lieu sûr. Voir le modèle d'Hébergement femmes Canada (HFC) Journal du harcèlement et des abus facilités par la technologie pour obtenir des conseils.
- Vérifiez si les comptes en ligne permettent de savoir où et quand une personne s'est connectée à vos comptes et recoupez ces informations avec votre localisation et votre emploi du temps. La plupart des comptes en ligne offrent la possibilité de télécharger ces informations qui peuvent servir de preuves.

- Conservez les preuves en lieu sûr. Sauvegardez-le également ailleurs, au cas où.

Pour accompagner les survivantes de VFGFT, il faut savoir ce que sont les informations d'identification personnelle (IIP) et la manière dont elles peuvent être utilisées à mauvais escient. En ayant des conversations informées, en identifiant des stratégies de sécurité et en préservant les preuves numériques, le personnel antiviolence peut aider les survivantes à reprendre le contrôle de leurs informations personnelles et de leur sécurité financière. Chaque situation est unique et une approche centrée sur la survivante garantit que ses choix, ses besoins et sa sécurité demeurent la priorité absolue.

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: Protéger ses informations personnelles en ligne - Vidéo pour les survivantes
- Mots de passe: Des moyens simples pour renforcer votre sécurité
- Liste de contrôle pour la planification de sécurité technologique
- Trousse à outils sur les abus financiers numériques
- Trousse à outils pour la préservation des preuves numériques

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 vous consulter notre site securitetech.ca.

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