Guide de conversation : Sécuriser vos comptes bancaires en ligne

Qu’est-ce qu’un abus financier numérique ?

L’abus financier numérique est l’utilisation abusive d’outils financiers en ligne, tels que les comptes bancaires, pour nuire financièrement à une survivante ou restreindre son accès à l’argent et aux ressources.

Cela pourrait ressembler à quelqu’un qui :

- Se connecte au compte bancaire de la survivante sans autorisation pour prendre de l’argent ou surveiller les transactions.
- Déplace de l’argent d’un compte à l’autre pour semer la confusion ou contrôler les finances de la survivante.
- Demande des cartes de crédit, contracte des prêts ou ouvre des comptes bancaires au nom de la survivante à son insu.

- Change les mots de passe ou les questions de sécurité pour empêcher la survivante d'accéder à son propre compte bancaire.
- Met en place des paiements ou des virements automatiques pour voler de l'argent.
- Désactive les alertes bancaires pour empêcher la survivante de voir ce qui se passe
- Retire la survivante d'un compte commun pour lui bloquer l'accès à son argent.
- Utilise des applis de paiement mobile ou de virements électroniques pour prendre de l'argent secrètement
- Menace de dénoncer une fausse fraude pour ruiner la réputation financière de la survivante
- Utilise des cryptomonnaies ou des portefeuilles numériques pour dissimuler de l'argent.

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 contrôle ou accède aux finances 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.

Pensez à poser la question :

- Est-ce que quelqu'un a accédé à vos comptes bancaires ou à vos cartes de crédit sans votre autorisation ?
- Qui contrôle les finances de votre ménage ? Avez-vous un compte conjoint ?
- Votre partenaire ou ex-partenaire peut-il accéder physiquement ou électroniquement à votre compte bancaire ou à vos relevés de compte ?
- Avez-vous un endroit sûr où mettre de l'argent de côté sans que votre partenaire ou ex-partenaire n'y ait accès ?
- Avez-vous remarqué que de l'argent a disparu, que des transactions étranges ont été effectuées ou que de nouveaux comptes ont été ouverts à votre nom ?
- Vos comptes bancaires ont-ils été bloqués ou vos mots de passe changés ?
- Recevez-vous des alertes ou des relevés concernant des comptes que vous ne reconnaissez pas ?
- Vous sentez-vous contrainte ou effrayée de prendre des décisions financières ?
- Si la survivante est incertaine, suggérez-lui de vérifier son historique bancaire en ligne, son rapport de crédit ou de s'adresser à sa banque pour identifier toute activité inhabituelle.

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 aviser 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 finances 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 souhaite sécuriser ses comptes en ligne, suggérez-lui de :

- Modifier les mots de passe et les questions de sécurité s'il est possible de le faire en toute sécurité (si cela ne risque pas d'aggraver le risque de préjudice). Éviter les réponses que l'auteur pourrait deviner.
- Activer la vérification en deux étapes pour plus de sécurité en activant l'option dans les paramètres.
- Examiner les paramètres du compte bancaire pour supprimer les utilisateurs ou dispositifs non autorisés.

Si la survivante souhaite surveiller et protéger ses finances, suggérez-lui de :

- Vérifier ses relevés bancaires et rapports de crédit pour détecter toute activité inhabituelle.

- Configurer des alertes de transaction pour être au courant de tout changement dans les paramètres du compte.
- Geler ou fermer les comptes compromis.
- Renforcer la protection de la vie privée et la sécurité.
- Utiliser une nouvelle adresse courriel et un nouveau numéro de téléphone pour ses opérations bancaires si l'auteur a accès à son compte courriel et son numéro de téléphone.
- Demander des relevés de compte papier ou changer l'adresse courriel du compte si l'auteur a accès au courriel de la survivante.
- Envisager d'ouvrir un compte bancaire séparé auprès d'une autre institution financière afin d'empêcher l'auteur d'y avoir accès.

Si la survivante a besoin de soutien supplémentaire, suggérez-lui de :

- Contacter le service des fraudes de la banque pour obtenir de l'aide afin d'annuler les frais ou de sécuriser les comptes.
- Discuter avec un conseiller financier des possibilités de rétablir son crédit ou consolider ses dettes.
- Si vous pouvez le faire en toute sécurité, signalez l'usurpation d'identité ou la fraude aux autorités.

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 de pouvoir s'en prévaloir en cas de besoin. 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.
- Prévoyez des mesures de sécurité, en particulier pour se rendre au poste de police, car l'auteur peut soupçonner que la survivante porte plainte si un traceur de localisation se trouve encore sur les effets personnels ou le véhicule de la survivante.
- Demandez l'aide d'une avocate civile ou d'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. Documenter toute activité suspecte.
- Conservez les preuves en lieu sûr. Sauvegardez-le 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: Sécuriser vos comptes bancaires en ligne pour interdire l'accès d'un partenaire violent - Vidéo pour les survivantes
- Êtes-vous la cible de violence technologique?
- Liste de contrôle pour la planification de sécurité technologique
- 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 consulter notre site securitetech.ca.

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