Abus financiers numériques: Conseils de planification de sécurité Personnel antiviolence

Cette ressource vise à aider le personnel antiviolence à aborder la maltraitance financière numérique avec les survivantes. La technologie financière évoluant rapidement, les abus financiers numériques deviennent une tactique courante de la violence fondée sur le genre facilitée par la technologie (VFGFT).

Si la personne avec laquelle vous travaillez est en situation de maltraitance financière numérique, il convient d'en tenir compte dans son plan de sécurité.

Cette ressource contient:

- des questions,
- des stratégies de sécurité technologique, et
- des liens vers des documents qui peuvent guider vos conversations de planification de sécurité.

Ces ressources complémentaires sur la VFGFT et la planification de la sécurité peuvent également vous être utiles:

- Êtes-vous victime d'abus technologique?
- Êtes-vous victime d'abus financiers numériques?
- Liste de contrôle pour la planification de la sécurité technologique
- Amorces de conversation pour la planification de la sécurité technologique
- 6 conseils pour sécuriser vos informations financières en ligne

Planification de la sécurité touchant les informations d'identification personnelle

Un partenaire ou un ex-partenaire peut utiliser les informations d'identification personnelle (nom, date de naissance, NAS, adresse) à mauvais escient pour ouvrir des comptes, se connecter à des applis financières et restreindre l'accès à l'argent.

DEMANDEZ:

- Votre partenaire ou ex-partenaire a-t-il 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 des états financiers?

- Votre partenaire ou ex-partenaire connaît-il vos numéros de compte, mots de passe et codes PIN des services bancaires en ligne, d'autres applis financières et des comptes que vous possédez?
- Avez-vous accès à vos données d'identification personnelles et à celles de vos enfants (nom, date de naissance, NAS), à des documents ou à des états financiers?
- Votre accès à vos documents est-il limité?
    - Par exemple: Pas de Wi-Fi à la maison pour faire une demande de remplacement, le partenaire ou l'ex-partenaire vous a caché des documents.

STRATÉGIES SUGGÉRÉES:

- Rassemblez les documents, faites-en des copies et conservez-les en lieu sûr.
- Remplacez les documents manquants et envoyez-les à l'adresse d'une personne de confiance.
- Modifier mots de passe et choisissez-en qui comportent un mélange de chiffres, de lettres et de symboles et qui sont longs.
    - Par exemple: $ummer1$myFavouriteeaon.
- Changez de code PIN pour une nouvelle combinaison de chiffres que vous n'avez jamais utilisée.
    - Choisissez une séquence aléatoire de chiffres et évitez d'utiliser des chiffres que votre partenaire ou ex-partenaire pourrait deviner facilement.
    - Par exemple: N'utilisez pas votre date de naissance ou celle de vos enfants, votre chiffre préféré, l’adresse de votre maison, etc.

- N'enregistrez pas de nouveaux mots de passe et codes PIN sur votre appareil, à moins d'être certaine que votre appareil ou votre compte n'est pas surveillé ou utilisé par d'autres personnes.

Plan de sécurité concernant la propriété des comptes financiers et l'accès à ceux-ci

DEMANDEZ:

- D'une manière générale, qui contrôle les finances de votre ménage?
- Avez-vous un compte bancaire? Si oui, s'agit-il d'un compte conjoint ou individuel?
- 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 sécuritaire où mettre de l'argent de côté sans que votre partenaire ou ex-partenaire n'y ait accès?

STRATÉGIES SUGGÉRÉES:

- Modifiez les codes PIN, les adresses postales, les coordonnées et les mots de passe de vos comptes individuels.
- Ne modifiez pas les informations relatives à votre compte si vous ne pouvez pas le faire en toute sécurité.
    - Au lieu de cela, enregistrez ou prenez des captures d'écran ou des photos pour saisir régulièrement le solde du compte et l'historique des transactions.
    - Concentrez-vous sur la documentation des dates, des soldes et des transactions clés.

- Ouvrir un nouveau compte dans une banque différente dont l'auteur de violence ne connaît pas l'existence.
    - Pour en savoir plus sur la manière de le faire en toute sécurité, consultez notre ressource, Protection contre les abus financiers numériques lors de l'ouverture d'un nouveau compte bancaire.

Planification de la sécurité en cas de harcèlement et de menaces:

 DEMANDEZ:

- Avez-vous reçu des menaces par le biais de la section «message facultatif» lorsque vous recevez un virement électronique de votre partenaire ou ex-partenaire?
- Est-ce que votre partenaire ou ex-partenaire exige de connaître vos identifiants et mots de passe pour vos opérations bancaires en ligne?
- Est-ce que votre partenaire ou ex-partenaire vous demande constamment de l'argent?
- Votre partenaire ou ex-partenaire a-t-il porté atteinte à votre crédit en demandant des cartes de crédit, des prêts ou des prestations publiques à votre nom?
- Est-ce que votre partenaire ou ex-partenaire a pu vous localiser en se connectant à des comptes financiers en ligne?
- Est-ce que votre partenaire ou ex-partenaire a limité l’accès aux finances en annulant ou en suspendant vos cartes bancaires et cartes de crédit?

STRATÉGIES SUGGÉRÉES:

- Signalez tout abus ou toute activité suspecte à votre banque ou à la société émettrice de votre carte de crédit.
- Conserver les preuves du harcèlement, des menaces et de la surveillance en effectuant des captures d'écran ou vidéo d'écran.
- Si vous vous sentez à l'aise, contactez les forces de l'ordre.
- Retirez de l'argent à un guichet automatique plus éloigné de votre lieu de travail ou de résidence.
- Modifier vos mots de passe et codes PIN pour qu'ils soient difficiles à deviner.
- Demander un dossier de crédit gratuit auprès d'Equifax.

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 une personne de votre entourage êtes victime de VFGFT, vous n'êtes pas seule. Vous pouvez consulter https://hebergementfemmes.ca/ pour trouver une MH près de chez vous afin de discuter de vos options et élaborer un plan de sécurité. Il n'est pas nécessaire de résider dans une MH pour avoir accès à des services et à un soutien gratuits et confidentiels. Pour plus d'informations sur les abus financiers numériques, consultez notre trousse complète sur les abus financiers numériques.

Adapté pour le Canada à partir du New York City Domestic Violence Economic Justice Taskforce's Financial Development Subcommittee, sur la base de leur ressource Financial Safety Planning: Best Practices for Domestic Violence Service Providers.

Ce projet a été financé par le Groupe Banque TD, par l'entremise de sa plateforme de citoyenneté d'entreprise, La promesse TD Prêts à agir.