Protection contre les abus financiers numériques lors de l’ouverture d’un nouveau compte bancaire

Les survivantes d’abus financiers peuvent décider d’ouvrir un nouveau compte bancaire en ligne ou en personne, avant ou après avoir quitté une relation violente.

Cette fiche d’information fournit des conseils pour se protéger contre d’autres abus financiers numériques lors de l’ouverture d’un nouveau compte.

Modifications d’un compte bancaire existant – Alerter accidentellement un auteur de violence

Apporter des modifications pour améliorer la sécurité ou la confidentialité d’un compte bancaire existant peut mettre la puce à l’oreille d’un auteur, ce qui risque d’entraîner une escalade de la violence. Les auteurs de violence peuvent:

- Recevoir des notifications par courriel ou par SMS lorsque des modifications sont apportées aux comptes auxquels ils ont un accès partagé.
- Recevoir des appels du personnel de la banque confirmant des changements sur des comptes auxquels ils ont un accès partagé.
- Utiliser un stalkerware pour suivre l’activité des appareils de la survivante et voir quels sont les sites web ou les applis auxquels elle accède.
- Disposer des informations bancaires et des mots de passe de la survivante, leur permettant de se connecter à partir de leur propre appareil et de s’apercevoir qu’un mot de passe ne fonctionne plus.

Si l’on soupçonne l’une de ces situations, il faut ouvrir un nouveau compte bancaire sans fermer celui auquel l’auteur a accès.

Considérations de sécurité lors de l’ouverture d’un nouveau compte

Les survivantes peuvent contacter une MH locale ou une organisation antiviolence pour discuter de leurs options et élaborer un plan de sécurité avant d'ouvrir un nouveau compte bancaire. Cela peut s'avérer particulièrement important dans les situations suivantes:

- **L'auteur retient une pièce d'identité pour empêcher la survivante d'ouvrir un compte**. Les maisons d'hébergement peuvent appuyer une demande de carte d'identité temporaire ou recommander des banques qui ouvriront des comptes sans carte d'identité.
- **L'auteur a placé** des dispositifs de localisation sur la voiture de la survivante ou un traceur Bluetooth (par exemple airTag) ou un logiciel espion sur le téléphone de la survivante pour savoir quand elle va à la banque.
- Un logiciel espion **a été téléchargé sur l'appareil de la survivante** et permet à l'auteur de voir ce qu'elle fait, y compris lorsqu'elle ouvre un nouveau compte bancaire en ligne, ses informations de connexion et son mot de passe.

Considérations lors de l'ouverture d'un compte en ligne:

- Si vous ouvrez un compte bancaire en ligne via une appli ou un site web, utilisez un appareil sécuritaire que l'auteur ne surveille pas, par exemple celui d'une amie ou d'une personne en qui vous avez confiance, ou un appareil au travail ou à la bibliothèque locale.
- Déconnectez-vous des services bancaires en ligne sur l'ordinateur ou l'appareil que vous utilisez, surtout s'il s'agit d'un ordinateur partagé ou public.

- Utilisez un réseau Wi-Fi sécurisé et privé. Évitez d'utiliser le Wi-Fi public pour des opérations sensibles telles que l'ouverture d'un compte bancaire.
- Si vous devez utiliser un réseau Wi-Fi public, envisagez d'accéder à vos comptes via un VPN (Virtual Private Network) pour protéger vos données.
- Effacer l'historique du navigateur de recherche Internet ou ouvrir le compte dans un navigateur privé si l'auteur a encore accès aux appareils de la famille.
- Si vous devez saisir un courriel, un numéro de téléphone ou d'autres informations de contact, utilisez des comptes auxquels l'auteur n'a pas accès. Vous devrez peut-être ouvrir un nouveau courriel pour vos communications bancaires, surtout si les mises à jour du nouveau compte sont envoyées à un courriel que l'auteur surveille, car cela l'alertera sur le fait que vous avez ouvert un nouveau compte.

Ouverture d'un compte en personne:

- Si vous êtes suivie, envisagez de garer le véhicule plus loin de la banque ou de laisser votre appareil compromis dans la voiture si vous pouvez le faire en toute sécurité.

Conseils généraux de sécurité

- Utiliser un mot de passe fort composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.
- Ne réutilisez pas les mots de passe ou les codes PIN d'autres comptes; mieux encore, utilisez un gestionnaire de mots de passe pour les stocker en toute sécurité.

- Choisissez une banque qui propose l'authentification à deux facteurs (2FA) et activez-la. Cela ajoute une couche de sécurité en exigeant un deuxième type de vérification, tel qu'un code envoyé à un numéro de téléphone ou à un courriel. Lors de la mise en place de cette procédure, assurez-vous que le courriel ou le numéro de téléphone que vous utilisez pour la vérification n'est pas accessible à l'auteur.
- Ne mettez pas le nom d'une autre personne sur le compte et ne donnez pas l'accès à quelqu'un d'autre.
- Configurez des notifications pour un compte qui n'est pas surveillé pour toutes les transactions ou tentatives de connexion afin d'être averti en cas d'activité suspecte ou d'accès non autorisé.
- Vérifiez les paramètres de confidentialité pour savoir qui a accès à vos informations (en ligne ou lors de l'ouverture du compte à la banque).
- Assurez-vous que les réponses à vos questions de sécurité ne sont pas des informations que l'auteur connaît.
- Si vous habitez toujours avec l'auteur de violence, gardez les cartes de débit/crédit associées à vos nouveaux comptes ailleurs ou cachées.
- Envisagez d'utiliser une autre banque ou d'indiquer clairement à votre banque actuelle que vous souhaitez qu'il n'y ait aucun lien entre vos comptes existants et ce compte. Par exemple, si vous ouvrez un nouveau compte dans votre banque actuelle, il peut apparaître dans la liste des comptes de votre banque en ligne avec vos autres comptes, qui peuvent être liés au compte en ligne d'un auteur.
- Usez de prudence si vous transférez de l'argent d'un compte auquel l'auteur peut accéder vers votre nouveau compte, car il pourrait savoir, à partir des relevés et transactions, que vous avez un nouveau compte et dans quel établissement il se trouve.

- Usez de prudence lorsque vous mettez à jour votre carte de crédit ou vos informations bancaires dans d'autres applis/plateformes; si vous ajoutez vos nouvelles informations à un compte auquel l'auteur peut accéder, il verra alors vos nouvelles informations bancaires.

Ces précautions peuvent contribuer à protéger votre nouveau compte bancaire d'une utilisation abusive par un auteur de violence. Si vous avez besoin d'aide, contactez une maison d'hébergement locale, ou consultez notre fiche d'information, 6 Conseils pour sécuriser vos informations financières en ligne pour obtenir des conseils sur la façon de rester en sécurité.

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 www.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, veuillez consulter notre trousse complète.

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.