6 conseils pour sécuriser vos informations financières en ligne

Si vous tentez de protéger vos finances d'un partenaire ou ex-partenaire, voici six conseils pour sécuriser votre identité financière en ligne.

1. Vérifier les paramètres

Vérifiez les paramètres de votre compte bancaire en ligne et de tout autre compte ou appli qui stocke des informations financières.

Si vous craignez qu'un partenaire ou un ex-partenaire n'accède à votre compte, envisagez:

- De renforcer la sécurité en modifiant votre mot de passe sur un appareil qui n'est pas surveillé.
- En mettant en place une authentification multifactorielle.

Vous pouvez également vous familiariser avec les mesures à prendre en plus du changement de mot de passe, telles que:

- restriction de l'accès aux cartes,
- verrouillage des cartes de crédit, et
- mise en place d'alertes pour être informée par SMS ou par courriel des achats, soldes inhabituels, tentatives de connexion infructueuses ou d'autres changements.

Contactez votre banque ou la société émettrice de votre carte de crédit pour obtenir des conseils.

2. Sécuriser vos comptes, appareils et réseaux

Utilisez des comptes, des appareils et des réseaux sécurisés, comme l'ordinateur de la bibliothèque ou l'appareil d'une amie, pour accéder à vos informations financières.

Si vous craignez que l'auteur de violence surveille vos appareils, vous pourrez ainsi vous assurer qu'il n'est pas au courant des nouveaux mots de passe, comptes ou autres modifications que vous apportez à vos comptes financiers, à condition que son courriel ne soit pas configuré pour être informé des changements.

Pour éviter tout accès non autorisé:

- sécurisez vos comptes à l'aide d'un NIP ou un mot de passe connu de vous seule et
- veillez à être la seule à avoir accès à votre courriel pour l'authentification.

3. Vérifier les informations d'identification personnelle accessibles au public

Vérifiez, sécurisez ou supprimez les informations d'identification personnelle (nom, date de naissance, NAS, adresse, etc.) accessibles au public en ligne.

Les informations d'identification personnelle telles que votre nom, votre adresse, votre courriel, votre numéro de téléphone et d'autres données peuvent se retrouver en ligne de différentes manières.

Par exemple:

- vous pouvez les partager volontairement,
- quelqu'un d'autre peut les partager en votre nom, ou
- elles peuvent provenir d'une fuite de données.

Il existe différents moyens de gérer votre empreinte digitale, certains gratuits, d'autres nécessitant un paiement unique ou un abonnement mensuel.

Pour savoir ce qui est publiquement accessible à votre sujet en ligne, vous pouvez simplement utiliser un moteur de recherche (Safari, Firefox, Chrome, etc.) pour rechercher votre nom et voir quelles informations apparaissent dans les résultats. Vous trouverez les informations que vous ou quelqu'un

d’autre avez partagées, car celles divulguées dans le cadre d’une fuite de données ne sont généralement pas facilement accessibles par le biais de recherches en ligne.

Il existe plusieurs options gratuites et payantes pour déterminer si vos informations ont été compromises dans le cadre d’une fuite de données et quelles sont les informations susceptibles d’être exposées. have i been pwned? est une option gratuite qui recherchera votre courriel et vous pourrez vous inscrire pour recevoir des notifications en cas de violations futures.

Mesures à prendre si vous trouvez vos informations personnelles en ligne:

Informations partagées par vous:

- Si vous trouvez des informations que vous avez partagées et que vous souhaitez supprimer, vous pouvez les gérer ou les supprimer vous-même si vous avez toujours accès au compte.
- Si vous n’avez plus accès au compte, des mesures peuvent être prises pour rétablir l’accès au compte à partir duquel vous avez partagé les informations.

Informations partagées par quelqu’un d’autre:

- Si vous voulez supprimer des informations que quelqu’un a partagées à votre sujet, consultez la ressource National Network to End Domestic Violence sur la suppression d’informations sensibles sur Internet.

Informations partagées lors d’une fuite de données:

- Dès que vous savez que vos informations ont fait l'objet d'une violation de données, il est essentiel de:
    - mettre à jour les mots de passe,
    - sécuriser vos comptes actuels, et
    - ne pas réutiliser un mot de passe impliqué dans une fuite pour d'autres comptes.

Ne partagez vos informations financières sensibles qu'avec des applis et des organisations en lesquelles vous avez confiance.

- Vos données sont un bien précieux pour de nombreux sites web et applis qui demandent des informations sensibles sur votre identité financière pour diverses raisons.
- Certains vous permettront d'importer des informations bancaires à des fins diverses, telles que le traitement des paiements, les demandes de location et le suivi des dépenses.
- Le partage de ces informations peut vous aider à atteindre plus rapidement vos objectifs financiers, mais il peut aussi mettre votre vie privée en danger si l'appli ou l'institution ne protège pas vos informations de manière adéquate.
- Le partage d'informations peut également présenter un risque si un auteur de violence a accès à un compte non financier contenant des informations financières que vous ne souhaitez pas qu'il possède, tel que des cartes de crédit et des informations bancaires.

Questions à se poser

Pour décider à quels sites web ou applis confier vos informations, voici quelques questions essentielles à se poser:

Avec qui vos informations sont-elles partagées?

- Vos informations seront-elles communiquées à d'autres personnes une fois que vous les aurez partagées avec cette institution ou cette appli?
- Pouvez-vous choisir les autres personnes avec qui ces informations sont partagées?

Pensez-y pour vos comptes bancaires et de crédit, ainsi que pour les applis avec lesquelles vous partagez ces informations. Des directives sont inscrites dans la politique de confidentialité régissant l'utilisation de votre compte ou appli, mais ces documents sont souvent trop longs pour être lus et compris en une seule fois.

Comment vos informations sont-elles utilisées?

- Quel est le but de la collecte?
    - Avant de partager vos informations, demandez-vous si elles sont nécessaires pour atteindre votre but.
- Est-ce possible d'atteindre ce but sans partager ces informations?
    - Par exemple, un locateur éventuel pourrait-il examiner des bulletins de salaire ou une autre forme de vérification des revenus plutôt que de demander des informations bancaires sensibles?

Quelles sont les protections ou les mesures pour protéger vos informations personnelles une fois qu'elles ont été saisies dans l'appli?

- Si une appli demande l'accès à des informations financières sensibles, elle doit être transparente sur la manière dont ces informations sont utilisées et protégées.

    - Les magasins d'applis d'Apple et de Google fournissent un aperçu de la manière dont chaque appli traite les données écrites par le développeur, qui peut être consulté avant de télécharger l'appli.
- Vous pouvez aussi consulter les évaluations des utilisateurs pour savoir si d'autres personnes signalent des problèmes de sécurité.
- En outre, des programmes antivirus tels que Norton 360 peuvent vous aider à déterminer si une appli est digne de confiance, quelles sont les informations récoltées et avec qui elles sont partagées.
    - Ces programmes peuvent servir à déterminer si une appli répond à vos besoins en matière de protection de la vie privée, mais ils sont généralement payants et ne sont pas forcément accessibles à toutes les survivantes.

4. Utiliser une carte de crédit

Si vous avez accès au crédit, un moyen de protéger vos finances consiste à **utiliser une carte de crédit plutôt qu'une carte de débit pour les achats courants**. L'utilisation d'une carte de crédit protège les liquidités contre un retrait instantané si quelqu'un accède à votre carte et l'utilise pour un achat non autorisé.

De plus, la plupart des cartes de crédit offrent un certain niveau de protection contre les achats non autorisés. Elles ne tiendront pas le titulaire de la carte responsable des frais frauduleux, bien qu'il faille parfois du temps pour les contester et les faire disparaître d'un compte. Idéalement, utilisez une carte de crédit dont l'auteur ignore l'existence afin que vos achats ne puissent pas être contrôlés.

Si vous possédez plusieurs cartes de crédit, le fait d'utiliser des cartes spécifiques pour des types d'achats spécifiques (courses, essence, etc.) peut

faciliter la détection des fraudes ou autres dépenses non autorisées si elles se produisent.

5. Surveiller votre dossier de crédit

Surveillez votre dossier de crédit et repérez toute nouvelle demande de renseignements ou tout changement dans votre dossier de crédit.

Il existe plusieurs options gratuites et payantes pour surveiller les modifications apportées à votre dossier de crédit. Certaines agences de renseignements sur les consommateurs vous permettent de créer un compte et de recevoir des copies supplémentaires de leur rapport. Les rapports de crédit indiquent les comptes de crédit actifs et fermés, le niveau d'endettement et l'historique des paiements, mais ils peuvent également inclure un score de crédit. Les scores de crédit sont déterminés sur la base des informations contenues dans vos rapports de crédit. Par conséquent, si vous trouvez des activités frauduleuses ou des erreurs dans votre rapport de crédit, cela peut avoir un impact sur votre score de crédit.

Si vous constatez une activité frauduleuse dans votre dossier de crédit:

- Contestez le problème auprès de l'agence ou des agences d'évaluation du crédit (p. ex. Equifax Canada, TransUnion Canada) qui affichent des informations incorrectes.
- Informez la banque, la société de cartes de crédit ou l'institution qui a signalé l'erreur.
    - Elles sont légalement tenues d'enquêter et de corriger les inexactitudes.

- Déposez une alerte à la fraude ou un gel de crédit auprès d'Equifax et de TransUnion pour avertir les prêteurs qu'ils doivent prendre des mesures supplémentaires pour vérifier votre identité.
- Pensez à demander un gel de crédit pour éviter que de nouveaux comptes soient ouverts à votre nom sans votre consentement.

6. 6. Utiliser les alertes à la fraude

Utilisez les alertes à la fraude pour protéger votre identité financière et votre crédit.

Les alertes à la fraude informent les créanciers potentiels que vous avez été ou pourriez être victime d'une fraude et les encouragent à prendre des mesures additionnelles pour vérifier votre identité avant de vous accorder une nouvelle ligne de crédit.

Il existe deux types d'alertes à la fraude: Les alertes initiales et Les alertes étendues.

Les alertes initiales

- Vous pouvez demander une première alerte à la fraude pour n'importe quelle raison, et elle restera sur votre dossier de crédit pendant un an.
- Les alertes à la fraude peuvent être renouvelées chaque année si nécessaire.

Les alertes étendues

- L'alerte à la fraude étendue n'est accessible qu'aux victimes de fraude disposant de certains types de documents, tels qu'un rapport de police ou un affidavit confirmant la fraude ou l'usurpation d'identité.

- Ce type d'alerte:
    - restera sur votre dossier de crédit pendant sept ans, sauf si vous y renoncez plus tôt, et
    - vous empêchera de recevoir des offres présélectionnées de cartes de crédit et d'assurance pendant cinq ans.

Les deux types d'alertes à la fraude vous permettent de demander gratuitement des copies additionnelles de votre dossier de crédit à des fins de contrôle de la solvabilité. Il vous suffit de demander une alerte à la fraude à l'un des trois bureaux de crédit nationaux (Experian, TransUnion et Equifax), qui communiquera ensuite avec les deux autres en votre nom.

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, consultez notre trousse complète sur les abus financiers numériques.

Adapté pour le Canada avec la permission du projet Safety Net du NNEDV, sur la base de leur ressource Financial Abuse and Technology.

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.