Rappel - Pratiques de sécurité pour les déclarants par voie électronique

But

L'Agence du revenu du Canada (ARC) a remarqué une menace croissante de fraude financière et d'arnaques numériques. Nous jouons tous un rôle important pour protéger les renseignements et atténuer les risques en nous tenant au courant des pratiques exemplaires de sécurité et en étant vigilants.

Ce message comprend quelques **étapes simples** que vous pouvez suivre pour confirmer l'identité de vos clients et protéger vos comptes de l'ARC et votre réseau contre les cybermenaces. Il comprend aussi des façons de rester vigilant face aux dernières tendances en matière d'arnaque et de fraude. Ces conseils ne visent pas à remplacer les procédures de sécurité présentes dans votre organisation et doivent seulement être considérés comme des pratiques exemplaires qui peuvent compléter vos protocoles déjà existants.

En plus de ce qui suit, en respectant les responsabilités TED suivantes, vous aidez à vous protéger contre la fraude et à atténuer la divulgation de renseignements sur les contribuables à un utilisateur non autorisé ou à un acteur malveillant :

1. Un préparateur électronique doit traiter directement avec son client.
2. Un préparateur électronique doit valider l'identité de son client.
3. Un préparateur électronique respecte le fait que l'accès au service de transmission électronique de la TED est limité uniquement aux fins de la production électronique d'une déclaration de revenu. Toute autre utilisation est interdite, comme, sans s'y limiter, la récupération de documents à des fins de vérification des revenus.

Validez l'identité de votre client

Valider l'identité de votre client, surtout celle des nouveaux clients, avant toute transaction ou divulgation de renseignements, que l'interaction soit en personne, par téléphone ou en ligne, est l'une des nombreuses façons d'atténuer la fraude potentielle.

Cela aide à prévenir les conséquences indésirables, comme la divulgation de renseignements à des utilisateurs non autorisés ou le versement de fonds à des groupes ou à des personnes malveillantes. Il est également recommandé d'effectuer des validations complètes pour les clients plus anciens, car les acteurs de menace peuvent être patients lorsqu'ils planifient des stratagèmes plus complexes. Vous trouverez ci-dessous quelques façons de valider l'identité de vos clients.

En personne

- Pièce d’identité avec photo délivrée par le gouvernement, authentique, valide et à jour
- Questions de confidentialité complexes et appropriées liées aux renseignements au dossier ou dans le compte
- Vérification du dossier de crédit en temps réel pour comparer les renseignements contenus dans le rapport avec ceux fournis par le client

Téléphone

- Questions de confidentialité liées aux renseignements au dossier ou dans le compte
- Authentification multifacteur
- Système de numéro d’identification personnel pour les clients

En ligne

- Appel vidéo, au besoin, pour valider une pièce d’identité avec photo délivrée par le gouvernement, authentique, valide et à jour
- Logiciel de validation des documents
- Authentification multifacteur

Protégez vos renseignements et vos comptes de l’ARC

Il y a plusieurs choses que vous pouvez faire pour protéger vos renseignements et vos comptes en ligne contre le vol d’identité ou la fraude potentiels.

- **Surveillez vos comptes régulièrement :** cela aide à repérer et à traiter les activités suspectes.
- **Changez souvent vos ID utilisateur et vos mots de passe :** utilisez des mots de passe uniques et complexes.
- **Gardez vos coordonnées à jour :** si l’ARC remarque une activité suspecte dans votre compte, elle pourrait avoir besoin de vous contacter.
- **Tenez à jour les renseignements sur vos clients :** supprimez les renseignements obsolètes afin d’empêcher toute utilisation non autorisée à l’avenir.
- **Gérez les représentants associés à un ID Groupe de numéro d’entreprise :** cela prévient l’accès non autorisé aux renseignements sur le client.
- **Déconnectez-vous après chaque session :** cela atténue le risque d’accès non autorisé.

Certaines de ces pratiques peuvent également être appliquées pour sécuriser votre compte de la TED. Pour en savoir plus, consultez la page Web Protéger vos comptes de l’ARC. Si vous remarquez une activité suspecte dans votre compte, allez à la page Web de l’ARC Signaler une arnaque ou un vol d’identité.

Communiquer à l'ARC des informations sur les tendances et les stratagèmes de fraude peut l'aider l'Agence à cerner et à traiter les activités frauduleuses rapidement. Un effort collectif renforcera nos défenses contre la fraude et favorisera un environnement plus sécuritaire.

Sécurisez vos réseaux

Vos réseaux sont la clé maîtresse de vos appareils et de vos données les plus importantes. Il est essentiel de mettre en œuvre, de promouvoir et de surveiller les pratiques exemplaires en cybersécurité pour protéger votre posture en matière de sécurité. Tenez compte de ce qui suit :

- **Réseaux privés :** utilisez une phrase ou un mot de passe complexe, limitez la zone de couverture et mettez à jour les appareils.
- **Segmentez votre réseau :** empêchez le trafic de circuler vers les zones sensibles ou restreintes.
- **Réseaux privés virtuels (RPV) :** envisagez ce type de connexion sécurisée entre deux points, cela vous permet d'envoyer et de recevoir des données de façon plus sécuritaire.
- **Pare-feu :** veillez à contrôler qui peut accéder à votre appareil en utilisant un pare-feu matériel, en installant une protection à partir d'une source crédible et en gardant le logiciel à jour.
- **Surveillez les passerelles Internet et d'appareils mobiles, le trafic sur le réseau et les points d'accès sans fil :** vérifiez les registres pour détecter les anomalies.
- **Mettez en œuvre un système de noms de domaine (DNS) :** cela protège les utilisateurs contre la visite par inadvertance de domaines malveillants sur Internet.
- **Formez votre personnel (s'il y a lieu) aux outils et aux programmes de sécurité du réseau :** un personnel informé peut réduire la probabilité d'incidents de cybersécurité.
- **Ne communiquez pas vos mots de passe :** protéger les mots de passe aide à prévenir les atteintes au réseau.

Restez vigilant

Être au courant des dernières arnaques et techniques que les personnes malveillantes utilisent pour commettre des fraudes vous aidera à vous protéger, vous et vos clients, contre le vol de renseignements et les pertes financières. La page Web Arnaques et fraudes et les plateformes de médias sociaux de l'ARC présentent des renseignements et les dernières nouvelles sur les arnaques et les activités frauduleuses. Voici quelques-unes des arnaques les plus récentes.

- **Arnaque de paiement de l'ARC par message texte :** Un message texte avec une image du logo du gouvernement du Canada prétend provenir de l'ARC et offre un dépôt par virement Interac® frauduleux. Un autre message texte

apparaît. Il contient un lien vers un faux portail de connexion pour les institutions financières.

- **Messages contenant des renseignements personnels :** Un message prétendant provenir de l'ARC et exigeant un paiement ou contenant un lien comprend des renseignements personnels, comme votre nom, votre date de naissance ou votre numéro d'assurance sociale.
- **Arnaque de remboursement ou de crédit de TPS/TVH :** Une personne malveillante se faisant passer pour l'ARC vous envoie un message texte ou un courriel pour vous remettre un remboursement ou un crédit de TPS/TVH. On vous demande de fournir des renseignements personnels pour aller de l'avant.
- **Arnaque pour accéder aux comptes de l'ARC :** L'acteur de menace envoie un message texte prétendant provenir de l'ARC afin d'avoir accès à vos comptes de l'ARC. Le message indique qu'il y a une erreur dans votre compte et qu'il devra être mis à jour. On vous demande de répondre « AIDE » au message texte, puis de fournir des renseignements personnels.
- **Vol d'identité et déclarations de revenus frauduleuses :** Les acteurs de menace obtiennent des renseignements personnels (comme un ID utilisateur et un mot de passe) et produisent de fausses déclarations de revenus à votre nom.
- **Documents d'impôt frauduleux :** Soyez vigilants avec des feuillets indiquant des déductions anormalement élevées par rapport au revenu ou dépassant les plafonds annuels. Soyez également attentifs aux incohérences dans les antécédents d'emploi ou de revenu d'un contribuable, comme des hausses soudaines des revenus déclarés ou des demandes qui ne correspondent pas aux années précédentes. Ces éléments peuvent indiquer des tentatives d'obtenir des remboursements ou des prestations injustifiés.

Ressources supplémentaires

Pour d'autres pratiques de sécurité, consultez les ressources suivantes :

Agence du revenu du Canada
Sécurité et protection de vos renseignements à l'ARC

Centre antifraude du Canada
Protégez-vous contre les fraudes

Centre canadien pour la cybersécurité
Information pour les petites et moyennes entreprises

Comptables professionnels agréés du Canada
Ressources en matière de cybersécurité

Centre d'analyse des opérations et déclarations financières du Canada
Méthodes pour vérifier l'identité de personnes et d'entités
À quel moment vérifier l'identité des personnes et des entités – Comptables