Sécurité des transactions et des comptes

La sécurité des comptes est importante à nos yeux et nous avons pris plusieurs mesures pour protéger les informations liées à votre compte Remitly. Vous aussi, vous pouvez prendre certaines mesures qui aideront à protéger votre compte et vos informations personnelles.

Processus de vérification des comptes

Votre compte Remitly est soumis à des procédures de vérification afin de maintenir un niveau élevé de sécurité, de confiance et de protection.

Si vous êtes un nouveau client créant un nouveau compte Remitly à l'aide du site Remitly, vous devez fournir certaines informations personnelles et compléter le processus de vérification par e-mail.

Une fois que votre compte est opérationnel, nous déployons diverses procédures de gestion des risques, manuelles et automatisées, nous permettant de mettre en évidence les activités de compte suspectes. Le but est d'identifier toutes les caractéristiques qui semblent inhabituelles ou incompatibles avec votre utilisation passée. Dans le cadre de ce processus, nous avons passé des contrats avec des fournisseurs de services, leaders sur le marché, afin de vérifier les informations personnelles et financières. Ces fournisseurs de services ne vous contacteront jamais directement ni n'utiliseront jamais vos informations pour autres fins que la bonne exécution de la transaction envisagée.

Sécurité du mot de passe

Lorsque vous vous connectez à votre compte, nous prenons certaines mesures pour protéger votre compte. Tout d'abord, chaque fois que vous vous connectez à votre compte Remitly, vous vous connectez à l'aide d'une connexion de serveur sécurisée (https: //). Nous utilisons le protocole SSL (Secure Socket Layer) avec cryptage 256 bits, le standard de l'industrie en matière de protection de serveur sécurisée.

Votre compte est également protégé par un mot de passe unique que vous créez. Vous ne devez pas utiliser de mots ou d'expressions courants comme mot de passe. Votre mot de passe devrait plutôt comporter au moins huit caractères, comprenant des chiffres et des lettres, avec majuscules et minuscules. Vous devriez garder ce mot de passe confidentiel. Le partage de votre mot de passe diminuera la sécurité de votre compte Remitly.

Méfiez-vous des escroqueries sur Internet

- NE faites PAS de paiement pour réclamer des gains à la loterie ou un prix, ni sous la promesse de recevoir une grosse somme d'argent.
- NE faites PAS de paiement car vous êtes « assuré » d'une carte de crédit ou d'un prêt.
- NE répondez PAS à une offre par Internet ou par téléphone si vous n'êtes pas sûr que cette offre soit honnête.
- NE faites PAS de paiement à une personne que vous ne connaissez pas ou dont vous ne pouvez pas vérifier l'identité.

En cas de doute, demandez au destinataire prévu plus d'informations sur le but et la sécurité du paiement requis. N'envoyez pas le paiement tant que vous n'êtes pas à l'aise avec la transaction.

Identification des e-mails de phishing ou d'usurpation d'identité

Vous pouvez à un moment donné recevoir un e-mail qui semble provenir de Remitly, mais qui, en réalité, n'est pas authentique. Un tel e-mail peut vous diriger vers un site qui ressemble au site de Remitly. Vous pourriez même être invité à fournir des informations sur votre compte, telles que votre e-mail et votre mot de passe.

Ces faux sites peuvent voler vos informations de compte et de paiement sensibles afin de commettre des fraudes. Ces faux e-mails peuvent contenir des virus ou des logiciels malveillants susceptibles de détecter des mots de passe ou des données sensibles. Nous vous recommandons donc d'installer un programme anti-virus et de le maintenir à jour en permanence.

Voici quelques points essentiels à garder à l'esprit lors de la défense contre les e-mails frauduleux :

1. **Sachez que Remitly ne demandera jamais par e-mail**
   - Votre numéro de sécurité sociale complet ou date de naissance
   - Votre numéro de carte de crédit, code PIN ou code de sécurité de votre carte de crédit (y compris les « mises à jour » des éléments ci-dessus)
2. **Méfiez-vous des pièces jointes dans les e-mails suspects**

Nous vous recommandons de ne pas ouvrir de pièces jointes provenant de sources suspectes ou inconnues. Les pièces jointes peuvent contenir des virus qui infectent votre ordinateur lors de l'ouverture de la pièce jointe. Si vous recevez un e-mail suspect

qui aurait été envoyé de Remitly et qui contient une pièce jointe, nous vous recommandons de le supprimer sans ouvrir la pièce jointe.

3. Soyez à l'affût des erreurs grammaticales ou typographiques

Soyez à l'affût d'une grammaire déficiente ou d'erreurs typographiques. Certains e-mails de phishing sont traduits d'autres langues ou sont envoyés sans correction d'épreuve et, par conséquent, contiennent des erreurs de grammaire ou de typographie.

4. Vérifiez l'adresse de retour

Cet e-mail provient-t-il bien de Remitly? Bien que les phishers puissent envoyer un e-mail frauduleux en faisant croire qu'il provient de Remitly, vous pouvez parfois déterminer s'il est authentique en vérifiant l'adresse de retour. Si la ligne « de » de l'e-mail ressemble à « remitly-security@hotmail.com » ou « remitly-fraud@msn.com » ou contient le nom d'un autre fournisseur de services Internet, vous pouvez être sûr que cet e-mail n'est pas authentique.

5. Vérifiez l'adresse du site

Les sites Remitly authentiques sont toujours hébergés sur le domaine suivant : https://www.remitly.com/

Parfois, le lien inclus dans les e-mails frauduleux ressemble à une adresse Remitly authentique. Vous pouvez vérifier où il pointe en passant votre souris sur le lien - le site réel vers lequel il pointe sera affiché dans la barre d'état en bas de la fenêtre de votre navigateur, ou sous forme de fenêtre contextuelle.

Nous n'utilisons jamais une adresse Web hébergée sur un domaine autre que ceux énumérés ci-dessus. Par exemple, les variantes de domaines telles que « http://security-payments-remitly.com/». . Ou une adresse IP (chaîne de nombres) suivis des répertoires tels que « http://123.456.789.123/remitly.com/ ». . ne sont pas des sites Remitly valides.

De plus, l'e-mail frauduleux est parfois configuré de telle sorte que si vous cliquez n'importe où sur le texte, vous accédez au site frauduleux. Remitly n'enverra jamais un e-mail de la sorte. Si vous cliquez accidentellement sur un tel e-mail et accédez à un site frauduleux, ne saisissez aucune information. Au lieu de cela, fermez cette fenêtre du

navigateur.

6. Si un e-mail semble suspect, accédez directement au site de Remitly

En cas de doute, ne cliquez pas sur le lien inclus dans un e-mail. Accédez directement à [https://www.remitly.com/] et cliquez sur **Votre compte** dans le menu en haut à droite pour afficher les derniers achats ou consulter les informations de votre compte. Si vous ne pouvez pas accéder à votre compte, ou si vous voyez quelque chose de suspect, contactez-nous immédiatement.

7. Protégez les informations de votre compte

Si vous avez cliqué sur un e-mail frauduleux ou suspect et que vous avez entré les informations de votre compte Remitly, vous devez **immédiatement** mettre à jour votre mot de passe. Vous pouvez le faire en allant directement à [https://www.remitly.com/] et en cliquant sur **Paramètres du compte.** Sur la page suivante, cliquez sur **Modifier vos informations personnelles, votre e-mail ou votre mot de passe**.

Si vous avez saisi votre numéro de carte de crédit sur le site lié à l'e-mail frauduleux, nous vous conseillons de prendre des mesures pour protéger vos informations. Vous devriez contacter votre société de carte de crédit pour l'informer de ce problème. Enfin, vous devez supprimer cette carte de crédit de votre compte Remitly afin d'empêcher quiconque de récupérer indûment l'accès à votre compte.

8. Signaler un e-mail de phishing

Si vous avez reçu un e-mail que vous savez être frauduleux, ou si vous pensez que vous avez été victime d'une attaque de phishing et que vous êtes inquiet au sujet de votre compte Remitly, veuillez nous en informer immédiatement en signalant un [e-mail frauduleux ou de phishing](https://github.com/Remitly/legal-markup/blob/master/home/contact).