Seguridad de la transacción y de la cuenta

Para nosotros tiene una gran importancia la seguridad de la cuenta, por ello hemos adoptado varias medidas que protegen la información relativa a tu cuenta Remitly. También hay ciertas cosas que puedes hacer para ayudar a proteger tu cuenta y tu información personal.

Procesos de verificación de cuenta

Tu cuenta Remitly está sujeta a procedimientos de verificación que mantienen un alto nivel de seguridad, de confianza y de protección.

Si eres un nuevo cliente de Remitly y creas una nueva cuenta Remitly a través del sitio web de Remitly, debes indicar determinada información personal y completar el proceso de verificación de correo electrónico.

Una vez activada tu cuenta desplegamos diversos procedimientos de gestión de riesgo, tanto manuales como automáticos, que nos permiten detectar actividad de cuenta sospechosa. El propósito es identificar cualquier característica que parezca inhabitual o incoherente con tu uso en el pasado. Como parte del proceso contratamos a proveedores de servicio líderes en el sector para que verifiquen la información personal y financiera. Estos servicios nunca se pondrán en contacto directo contigo ni usarán tu información para otra cosa que no sea la realización con éxito de la transacción que desees.

Seguridad de la contraseña

Cuando inicias sesión en tu cuenta llevamos a cabo ciertas acciones para proteger tu cuenta. Primero, siempre que inicias sesión en tu cuenta Remitly, te conectas mediante una conexión segura al servidor (https://). Usamos el protocolo SSL (Secure Socket Layer, SSL) con cifrado de 256 bits, la norma de la industria en protección segura de servidores.

Tu cuenta también está protegida por una contraseña única que tú creas. No deberías usar como contraseña palabras o frases comunes. Al contrario, la contraseña debería constar al menos de ocho caracteres, incluido tanto números como letras, en mayúscula y en minúscula. Debes mantener la confidencialidad de contraseña. Compartir tu contraseña con alguien disminuirá la seguridad de tu cuenta Remitly.

Presta atención a las estafas de Internet

- NO realices pagos para reclamar premios de sorteos o de loterías, ni con la

promesa de recibir una gran cantidad de dinero.

- NO realices pagos porque se te "garantiza" una tarjeta de crédito o un préstamo.
- NO respondas a ofertas de Internet o telefónicas de cuya honestidad no estés seguro.
- NO realices pagos a nadie que no conozcas o cuya identidad no puedas comprobar.

En caso de duda, pregunta al destinatario previsto acerca del objeto y de la seguridad del pago solicitado. No envíes el pago hasta que estés seguro de la transacción.

Identificación de suplantación de identidad (Phishing) o correos electrónicos simulados

En ocasiones puedes recibir correos electrónicos que parecen proceder de Remitly, pero que no son auténticos. Estos correos electrónicos te remiten a un sitio web que se parece igualmente al de Remitly. Incluso es posible que se te solicite que indiques información de cuenta como tu dirección de correo electrónico y contraseña.

Estos sitios web falsos pueden robarte información sensible relativa a tu cuenta o a pagos, con el fin de cometer un posterior fraude. Estos falsos correos electrónicos pueden contener virus o software malicioso que es capaz de detectar contraseñas o datos sensibles. Así pues, te recomendamos que instales un programa antivirus y que lo mantengas actualizado en todo momento.

He aquí algunos puntos clave a tener en cuenta para defenderse de los correos electrónicos fraudulentos:

1. Conocer los datos que Remitly no te solicitará por correo electrónico

- Tu número completo de la Seguridad Social o la fecha de nacimiento
- Tu número de tarjeta de crédito, PIN o código de seguridad de la tarjeta (incluidas "actualizaciones" de cualquiera de lo anterior)
- **2. Presta atención a los adjuntos en correos electrónicos sospechosos**

Te recomendamos que no abras adjuntos de correos electrónicos procedentes de fuentes desconocidas o sospechosas. Los adjuntos de correos electrónicos pueden contener virus que infectarían tu ordenador al abrir el fichero. Si recibes un correo electrónico sospechosos aparentemente enviado por Remitly y que contiene un adjunto, te recomendamos que borres el correo electrónico sin abrir el fichero adjunto.

3. Revisa los errores gramaticales o tipográficos

Detecta una gramática incorrecta o errores tipográficos. Algunos correos electrónicos de suplantación de identidad se traducen de otros idiomas o se envían sin corregir y, por tanto, contienen una gramática errónea o fallos tipográficos.

4. Comprueba la dirección del remitente

¿El correo electrónico es de Remitly? Aunque los suplantadores pueden enviar un correo electrónico falsificado que parezca proceder de Remitly, a veces puedes discernir si es o no auténtico comprobando la dirección del remitente. Si la línea "de" del correo electrónico presenta una dirección del tipo "remitly-security@hotmail.com" o "remitly-fraud@msn.com", o contiene el nombre de otro proveedor de servicio de Internet, puedes estar seguro de que no es auténtico.

5. Comprueba la dirección del sitio web

Los sitios web auténticos de Remitly están siempre alojados en el dominio siguiente: https://www.remitly.com/

A veces el enlace incluido en los correos electrónicos falsos se parece a una dirección auténtica de Remitly. Puedes comprobar la dirección a la que lleva realmente pasando el ratón por encima del enlace--el sitio web al que realmente dirige se mostrará en la barra de estado en la parte inferior de la ventana de tu navegador o en una ventana emergente.

Nunca usamos una dirección web alojada en un dominio distinto de los indicados anteriormente. Por ejemplo, las variantes de dominio como "https://security-payments-remitly.com/" o una dirección IP (serie de números) seguida de directorios como "https://123.456.789.123/remitly.com/" no son sitios web válidos de Remitly.

Además, en ocasiones los correos electrónicos simulados están configurados de modo que si haces clic en algún punto del texto te traslada al sitio web fraudulento. Remitly nunca te enviará un correo electrónico que haga tal cosa. Si haces clic de forma accidental en un correo electrónico de este tipo y te lleva a un sitio web falso, no introduzcas ninguna información; simplemente cierra esa ventana del navegador.

6. Si un correo electrónico parece sospechoso, accede al sitio web de Remitly directamente.

Si tienes alguna duda, no hagas clic en el enlace dentro del correo electrónico. Ve directamente a https://www.remitly.com/ y haz clic en **Tu cuenta** en el menú de la parte superior derecha para ver las compras recientes o revisar tu información de cuenta. Si no puedes acceder a tu cuenta o ves algo sospechoso, infórmanos enseguida.

7. Protege la información de tu cuenta

Si ya has hecho clic en un correo electrónico simulado o sospechoso y has introducido información de tu cuenta Remitly, debes actualizar **inmediatamente** tu contraseña. Para ello puedes ir directamente a https://www.remitly.com/ y hacer clic en **Ajustes de cuenta**. En la página siguiente, haz clic en **Cambiar tu información personal, dirección de correo electrónico o contraseña**.

Si has enviado el número de tu tarjeta de crédito al sitio web al que lleva el correo electrónico falsificado, te recomendamos que adoptes medidas para proteger tu información. Puedes contactar con la empresa de tu tarjeta de crédito, por ejemplo, para informarles del asunto. Por último, deberías borrar esa tarjeta de crédito de tu cuenta Remitly para impedir que nadie obtenga un acceso indebido a tu cuenta.

8. Notificación de correo electrónico de suplantación de identidad

Si estás seguro de haber recibido un correo electrónico falso o si crees que has sido víctima de un ataque de suplantación de identidad o tienes dudas sobre tu cuenta Remitly, infórmanos de ello enseguida notificando un [correo electrónico de suplantación de identidad o simulado](https://www.remitly.com/es/es/home/contact).