SEGURIDAD DE TRANSACCIONES Y CUENTA

La seguridad de las cuentas es importante para nosotros y hemos dado varios pasos para proteger la información relacionada con su cuenta Remitly. Usted también puede hacer determinadas cosas que lo ayudarán a proteger su cuenta y su información personal.

Acerca de los procesos de verificación

Su cuenta Remitly está sujeta a procedimientos de verificación para mantener altos niveles de seguridad, confianza y protección.

Si usted es un cliente nuevo de Remitly y crea una cuenta Remitly nueva mediante nuestro sitio web, debe proporcionar determinada información personal y completar el proceso de verificación por correo electrónico.

Una vez que su cuenta se ha configurado y está funcionando, implementamos diversos procedimientos de administración de riesgos manuales y automatizados que nos permiten resaltar actividad de cuenta sospechosa. El objetivo es identificar cualquier característica que parezca inusual o inconsistente con su uso pasado. Como parte de este proceso, tenemos contrato con proveedores de servicios líderes del sector para verificar información personal y financiera. Estos servicios nunca lo contactarán directamente ni usarán su información para nada que no sea la finalización correcta de su transacción.

Seguridad de contraseña

Cuando inicia sesión en su cuenta, hacemos algunas cosas para proteger su cuenta. Primero, siempre que inicie sesión en su cuenta Remitly, lo hace mediante una conexión de servidor protegida (https://). Usamos Secure Socket Layer (SSL) con cifrado de 256 bits, el estándar del sector en protección segura de servidores.

Su cuenta también está protegida por una contraseña única que usted crea. No debe usar palabras ni frases comunes como su contraseña. En su lugar, su contraseña debe tener al menos ocho caracteres incluidos números y letras en mayúsculas y minúsculas. Esta contraseña debe mantenerla como confidencial. Compartir su contraseña disminuirá la seguridad de su cuenta Remitly.

Esté atento a los fraudes por Internet

- NO realice pagos para reclamar ganancias de lotería o premios, ni tampoco bajo la promesa de recibir una gran cantidad de dinero.

- NO realice pagos porque se le ha "garantizado" una tarjeta de crédito ni un préstamo.
- NO responda a una oferta telefónica ni de Internet de la cual no esté seguro que sea honrada
- NO realice pagos a alguien que no conozca ni cuya identidad no pueda verificar.

Cuando tenga dudas, pida al destinatario más información acerca de la finalidad y la seguridad del pago solicitado. No envíe el pago hasta que esté cómodo con la transacción.

Identificación de phishing o correos electrónicos falsificados

Es posible que en algún momento reciba un correo electrónico que parezca que proviene de Remitly, pero que, en realidad, no es genuino. Tal correo electrónico puede dirigirlo a un sitio web que parecerá similar al sitio web de Remitly. Incluso es posible que se le pida proporcionar información de su cuenta como su dirección de correo electrónico y contraseña.

Estos sitios web falsos pueden robar su información confidencial de cuenta y pagos con el fin de cometer fraude. Estos correos electrónicos falsos pueden contener posibles virus o malware que pueden detectar contraseñas o datos confidenciales. Por lo tanto, le recomendamos que instale un programa antivirus y que lo mantenga actualizado en todo momento.

Estos son algunos puntos clave que se deben considerar como parte de una defensa contra correos electrónicos fraudulentos:

- Su número de seguro social completo o fecha de nacimiento
- Su número de tarjeta de crédito, PIN o código de seguridad de tarjeta de crédito (incluidas "actualizaciones" a cualquiera de los puntos anteriores)

Le recomendamos que no abra ningún adjunto de correo electrónico de fuentes sospechosas o desconocidas. Los adjuntos de correo electrónico pueden contener virus que infecten su computadora al momento de abrir tales archivos. Si recibe un correo electrónico sospechoso supuestamente enviado por Remitly que contiene un adjunto, le recomendamos que elimine el correo electrónico sin abrir el archivo.

Busque errores gramaticales o tipográficos garrafales. Algunos correos electrónicos de phishing se traducen de otros idiomas o se envían sin revisión y, como resultado, contienen errores gramaticales o tipográficos garrafales.

¿Es de Remitly el correo electrónico? Aunque los suplantadores de identidad

pueden enviar un correo electrónico falsificado para que parezca que proviene de Remitly, a veces puede determinar si es auténtico al comprobar la dirección de retorno. Si la línea "de" del correo electrónico se ve como "remitly-security@hotmail.com" o "remitly-fraud@msn.com", o contiene el nombre de otro proveedor de servicios de Internet, puede estar seguro de que no es genuino.

Los sitios web genuinos de Remitly siempre se hospedan en el siguiente dominio: https://www.remitly.com/

Algunas veces el vínculo incluido en correos electrónicos falsificados parece una dirección de Remitly genuina. Puede comprobar hacia adónde apunta al posar el mouse sobre el vínculo; el verdadero sitio web hacia adonde apunta aparecerá en la barra de estado en la parte inferior de la ventana del explorador o como un elemento emergente.

Nunca usamos una dirección web hospedada en un dominio que no sean los mostrados anteriormente. Por ejemplo, variaciones de dominios como "https://security-payments-remitly.com/. . ." o una dirección IP (cadena de números) seguida por directorios como "https://123.456.789.123/remitly.com/. . ." no son sitios web válidos de Remitly.

Además, a veces el correo electrónico falsificado está configurado de tal manera que si hace clic en cualquier parte del texto le llevará al sitio web fraudulento. Remitly nunca enviará un correo electrónico que haga esto. Si accidentalmente hizo clic en un correo electrónico semejante y va a un sitio web falsificado, no ingrese ninguna información; en su lugar, simplemente cierre esa ventana del explorador.

Cuando tenga dudas, no haga clic en el vínculo incluido en un correo electrónico. Vaya directamente a https://www.remitly.com/ y haga clic en **Su Cuenta** en el menú superior derecho para ver compras recientes o revisar la información de su cuenta. Si no puede acceder a su cuenta, o si ve algo sospechoso, comuníquenoslo de inmediato

Si hizo clic en un correo electrónico falsificado o sospechoso e ingresó la información de su cuenta Remitly, debe actualizar **inmediatamente** su contraseña. Puede hacerlo al ir directamente a https://www.remitly.com/ y hacer clic en **Configuración de cuenta**. En la página siguiente, haga clic en **Cambiar su información personal, dirección de correo electrónico o contraseña.**

Si envió el número de su tarjeta de crédito al sitio vinculado en el mensaje del correo electrónico falsificado, le aconsejamos que dé pasos para proteger su información. Es posible que desee contactarse con su compañía de tarjeta de crédito, por ejemplo, para notificarles sobre este asunto. Por último, debe eliminar esa tarjeta de crédito de su cuenta Remitly para evitar que alguien vuelva a tener acceso a su cuenta de manera incorrecta.

Si recibió un correo electrónico que sabe es falso, o si cree que ha sido víctima de un ataque de phishing y está preocupado por su cuenta Remitly, comuníquenoslo de inmediato al informarnos de [phishing o correo electrónico falsificado](/home/contact/).