Transazione e sicurezza del Conto

La sicurezza del conto è per noi importante e abbiamo adottato diverse misure per proteggere le informazioni relative al conto Remitly. Anche tu puoi agire in modo da proteggere il tuo conto e le tue informazioni personali.

Processi di verifica del conto

Il tuo conto Remitly è soggetto a procedure di verifica per mantenere livelli di sicurezza elevati, affidabilità e protezione.

Se sei un nuovo cliente Remitly e crei un nuovo conto Remitly utilizzando il sito web Remitly, devi fornire alcune informazioni personali e completare il processo di verifica via posta elettronica.

Una volta che il tuo conto è attivo e funzionante, implementiamo una serie di procedure manuali e automatizzate di gestione del rischio che ci consentono di evidenziare le attività sospette del conto. L'obiettivo è di identificare le caratteristiche che sembrano insolite o incoerenti con il tuo uso passato. Come parte di questo processo, ci affidiamo a fornitori di servizi leader del settore per verificare le informazioni personali e finanziarie. Non verrai mai contattato direttamente da tali servizi né le tue informazioni verranno utilizzate per motivi diversi dal completamento della transazione prescelta.

Sicurezza della password

Quando accedi al tuo conto, ci adoperiamo per proteggere il tuo conto. Innanzitutto, ogni volta che accedi al tuo conto Remitly, accedi utilizzando una connessione server sicura (https://). Utilizziamo Secure Socket Layer (SSL) con crittografia a 256 bit, lo standard del settore per una protezione sicura del server.

Il tuo conto è inoltre protetto da una password unica creata da te. Non devi usare parole o frasi comuni come password. Piuttosto, la tua password deve contenere almeno otto caratteri, inclusi sia numeri che lettere, usando maiuscole e minuscole. Devi mantenere questa password riservata. La condivisione della password ridurrà la sicurezza del tuo conto Remitly.

Diffidare delle truffe su Internet

- NON effettuare un pagamento per ritirare vincite della lotteria o premi o con la promessa di ricevere ingenti quantità di denaro.

- NON effettuare un pagamento in "cambio" di una carta di credito o un prestito.
- NON rispondere ad un'offerta Internet o telefonica che non sei certo dell'onestà della stessa.
- NON effettuare pagamenti a persone che non conosci o di cui non puoi verificare l'identità.

In caso di dubbi, chiedi al destinatario designato maggiori informazioni sullo scopo e sulla sicurezza del pagamento richiesto. Non inviare il pagamento finché non si è soddisfatti della transazione.

Identificazione di e-mail di phishing o contraffatte

Potresti ricevere un'e-mail che sembra provenire da Remitly, ma in realtà non è autentica. Tale e-mail potrebbe indirizzarti a un sito web simile al sito web Remitly. Ti potrebbe anche venire richiesto di fornire informazioni sul conto, come il tuo indirizzo e-mail e la password.

Questi siti web falsi possono rubare le tue informazioni sensibili relative conto e al pagamento per commettere frodi. Queste e-mail false potrebbero contenere potenziali virus o malware in grado di rilevare password o dati sensibili. Pertanto, ti consigliamo di installare un programma antivirus e tenerlo aggiornato in ogni momento.

Ecco alcuni punti chiave da tenere a mente per difendersi da e-mail fraudolente:

1. Sapere ciò che Remitly non ti chiederà via e-mail

- Il tuo numero completo di previdenza sociale o la data di nascita
- Il numero di carta di credito, il PIN o il codice di sicurezza della carta di credito (compresi gli "aggiornamenti" di uno dei precedenti)

2. Diffidare degli allegati in e-mail sospette

Ti consigliamo di non aprire allegati di e-mail ricevute da fonti sospette o sconosciute. Gli allegati alle e-mail possono contenere virus che infettano il computer quando viene aperto l'allegato. Se ricevi un'e-mail sospetta inviata da Remitly che contiene un allegato, ti consigliamo di eliminare l'e-mail senza aprire l'allegato.

3. Verifica la presenza errori grammaticali o tipografici

Verificare la presenza di scorrettezze grammaticali o errori tipografici. Alcune e-mail di phishing sono tradotte da altre lingue o vengono inviate senza revisione e, di conseguenza, contengono errori grammaticali o tipografici.

4. Controlla l'indirizzo del mittente

Si tratta dell'e-mail di Remitly? Sebbene i phisher possano inviare una e-mail falsificata per far sembrare che provenga da Remitly, a volte puoi determinare la sua autenticità controllando l'indirizzo del mittente. Se nel campo del mittente "da" dell'e-mail appare ad es. "remitly-security@hotmail.com" o "remitly-fraud@msn.com" o il nome di un altro fornitore di servizi Internet, puoi essere certo che non è autentica.

5. Controlla l'indirizzo del sito web

I siti web originali Remitly sono sempre ospitati sul seguente dominio: https://www.remitly.com/

A volte il link incluso nelle e-mail falsificate sembra un vero indirizzo Remitly. Puoi controllare la destinazione effettiva posizionando il mouse sul link: il sito web effettivo di destinazione verrà mostrato nella barra di stato nella parte inferiore della finestra del browser o come popup.

Non usiamo mai un indirizzo web ospitato su un dominio diverso da quelli suelencati. Ad esempio, domini varianti come "http://security-payments-remitly.com/" o un indirizzo IP (stringa di numeri) seguito da directory come "http://123.456.789.123/remitly.com/" non sono validi siti web.

Inoltre, a volte l'e-mail falsificata è impostata in modo tale per cui cliccando su un punto qualsiasi del testo, si viene reindirizzati al sito web fraudolento. Remitly non invierà mai una e-mail con tale caratteristica. Se si clicca accidentalmente su tale e-mail e si accede a un sito web contraffatto, non immettere alcuna informazione; piuttosto chiudere semplicemente la finestra del browser.

6. Se un'e-mail sembra sospetta, andare direttamente sul sito web Remitly

In caso di dubbi, non cliccare su un collegamento incluso in un'e-mail. Vai direttamente a https://www.remitly.com/ e clicca su **Il tuo conto** nel

menu in alto a destra per visualizzare gli acquisti recenti o rivedere le informazioni del tuo conto. Se non riesci ad accedere al tuo conto o se vedi qualcosa di sospetto, informaci immediatamente.

7. Proteggi le informazioni del tuo conto

Se hai cliccato su un'e-mail falsa o sospetta e hai inserito le informazioni del tuo conto Remitly, devi **immediatamente** modificare la tua password. Puoi farlo andando direttamente su https://www.remitly.com/ e cliccando su **Impostazioni del conto**. Nella pagina successiva, clicca su **Cambia le tue informazioni personali, l'indirizzo e-mail o la password**.

Se hai inviato il numero della tua carta di credito al sito collegato al messaggio e-mail falsificato, ti consigliamo di prendere provvedimenti per proteggere le tue informazioni. Potresti volere contattare la società che gestisce tua carta di credito, ad esempio, per segnalare loro la questione. Infine, devi eliminare la carta di credito dal tuo conto Remitly per impedire a chiunque di riacquistare in modo improprio l'accesso al tuo conto.

8. Segnalazione di e-mail di phishing

Se hai ricevuto una e-mail certamente falsa, o se pensi di essere stato vittima di un attacco di phishing e sei preoccupato per il tuo conto Remitly, ti preghiamo di comunicarcelo immediatamente segnalando l'[e-mail di phishing o contraffatta](https://www.remitly.com/home/contact).v