लेन-देन और खाता सुरक्षा

हमारे लिए खाते की सुरक्षा लिए ज़रूरी है और हमने आपके Remitly खाते से जुड़ी जानकारी की सुरक्षा के लिए कई कदम उठाए हैं. आप भी कुछ चीजें करके खाते और व्यक्तिगत जानकारी को सुरक्षित रखने में मदद पा सकते हैं.

खाते को सत्यापित करने की प्रक्रियाएं

आपका Remitly खाता उच्च स्तरीय सुरक्षा, विश्वास और बचाव को बनाए रखने के लिए सत्यापन प्रक्रियाओं के अधीन है.

अगर आप नए Remitly ग्राहक हैं और आपने Remitly वेबसाइट का उपयोग करके नया Remitly खाता बनाया है, तो आपको कुछ व्यक्तिगत जानकारी देनी होगी और ईमेल सत्यापन की प्रक्रिया पूरी करनी होगी

जब आपका खाता चालू हो जाता है और काम करने लगता है, तो हम अलग-अलग तरह की मैन्युअल और ऑटोमैटिक जोखिम प्रबंधन प्रक्रियाएं लागू करते हैं, जिससे हम खाते की संदिग्ध गतिविधि का प्रकटीकरण कर पाते हैं. हमारा मकसद आपके पिछले उपयोग से हटकर या असंगत लगने वाले लक्षणों की पहचान करना है. इस प्रक्रिया के एक हिस्से के तौर पर हम व्यक्तिगत और वित्तीय जानकारी को सत्यापित करने के लिए उद्योग के अग्रणी सेवा प्रदाताओं से अनुबंध करते हैं. ये सेवाएं कभी प्रत्यक्ष रूप से आपसे संपर्क नहीं करेंगी या आपकी जानकारी का उपयोग आपके इच्छित लेन-देन के सफलतापूर्वक समापन के अतिरिक्त किसी भी अन्य चीज़ के लिए नहीं करेंगी.

पासवर्ड सुरक्षा

जब आप अपने खाते में लॉग इन करते हैं, तो हम आपके खाते की सुरक्षा के लिए कुछ खास चीज़ें करते हैं सबसे पहले, जब भी आप अपने Remitly खाते को लॉग इन करें, तो किसी सुरक्षित सर्वर कनेक्शन (https://) का उपयोग करके लॉग इन करें. हम सर्वर को सुरक्षित रखने के लिए, उद्योग मानक 256-बिट एन्क्रिप्शन के साथ सिक्योर सॉकेट लेयर (SSL) का उपयोग करते हैं.

आपका खाता आपकी तरफ़ से बनाए गए यूनीक पासवर्ड से भी सुरक्षित रहता है. आपको अपने पासवर्ड में सामान्य शब्दों या वाक्यांशों का उपयोग नहीं करना चाहिए. इसकी जगह, अपने पासवर्ड में अपर और लोअर केस को उपयोग करते हुए संख्या और अक्षर, दोनों को मिलाकर कम से कम आठ अक्षर होने चाहिए. आपको इस पासवर्ड को गोपनीय रखना चाहिए. अपना पासवर्ड शेयर करने से आपके Remitly खाते की सुरक्षा में कमी आएगी.

इंटरनेट पर होने वाले स्कैम से सावधान रहें

लॉटरी या पुरस्कार जीतने का दावा करने के लिए या बड़ी राशि देने का वादा करने वालों को, किसी तरह का भुगतान न करें.

भुगतान न करें, क्योंकि आपको क्रेडिट कार्ड या ऋण की "गारंटी" दी जाती है.

किसी ऐसे इंटरनेट या फ़ोन ऑफ़र का जवाब न दें, जिसके बारे में आपको थोडी-सी भी शंका हो.

किसी ऐसे व्यक्ति को भुगतान न करें, जिसे आप नहीं जानते या जिसकी पहचान आप सत्यापित नहीं कर सकते.

संदेह होने पर, वांछित प्राप्तकर्ता से अनुरोधित भुगतान के उद्देश्य और सुरक्षा के बारे में अधिक जानकारी देने के लिए कहें. जब तक आप लेन-देन के लिए सहज ना महसूस करें, तब तक भुगतान न करें.

फ़िशिंग या फ़र्ज़ी ई-मेल को पहचानना

शायद कभी-कभार आपको ऐसा ईमेल आए, जो देखने में Remitly से आया प्रतीत होता हो, लेकिन असल में यह प्रामाणिक न हो. ऐसे ईमेल आपको Remitly जैसी दिखने वाली वेबसाइट तक ले जा सकते हैं. आपसे आपके ई-मेल पते और पासवर्ड जैसी खाता जानकारी भी देने के लिए कहा जा सकता है.

ये जाली वेबसाइट धोखाधड़ी करने के लिए आपके संवेदनशील खाते और भुगतान की जानकारी को चुरा सकती हैं. इन जाली ई-मेल में पासवर्ड या संवेदनशील डेटा का पता लगा सकने वाले संभावित वायरस या मैलवेयर हो सकते हैं. इसलिए हमारा सुझाव है कि आप एक एंटी-वायरस प्रोग्राम इंस्टॉल करें और इसे हर समय अपडेट रखें.

यहां पर धोखाधड़ी वाले ई-मेल से बचाव के हिस्से के तौर पर ध्यान में रखने योग्य कुछ अहम बिंदु दिए गए हैं:

जानें कि Remitly ई-मेल के माध्यम से क्या नहीं मांगेगा

आपका पूरा सोशल सिक्योरिटी नंबर या जन्मतिथि

आपका क्रेडिट कार्ड नंबर, पिन या क्रेडिट कार्ड सुरक्षा कोड (ऊपर दिए गए किसी भी "अपडेट" सहित)

संदिग्ध ई-मेल में होने वाले संलग्नक से सावधान रहें

हमारा सुझाव है कि आप संदिग्ध या अज्ञात स्त्रोतों से आए किसी भी ई-मेल अटैचमेंट को न खोलें. हो सकता है कि ई-मेल अटैचमेंट में वायरस हो, जो अटैचमेंट को खोले जाने पर आपके कंप्यूटर को संक्रमित कर दे. अगर आपको कथित तौर पर Remitly से भेजा गया अटैचमेंट वाला कोई संदिग्ध ई-मेल मिलता है, तो हम सुझाव देते हैं कि आप अटैचमेंट को खोले बिना ई-मेल को हटा दें.

व्याकरण या मुद्रण संबंधी त्रुटियां खोजें

खराब व्याकरण या मुद्रण संबंधी त्रुटियां खोजें कुछ फ़िशिंग ई-मेल अन्य भाषाओं से अनुवादित किए जाते हैं या बिना प्रूफरीड किए हुए भेजे जाते हैं और इसके नतीजन उनमें खराब व्याकरण पाया जाता है या टाइपोग्राफ़िकल त्रुटियां होती हैं.

रिटर्न एड्रेस को जांचें

[**क्या ई-मेल Remitly की ओर से आया है? हालांकि, फ़िशर जाली ई-मेल भेजकर इसे Remitly की ओर से भेजे जाने जैसा दिखावा कर सकते हैं, आप रिटर्न एड्रेस की जांच करके कभी-कभार इसकी प्रमाणिकता को निर्धारित कर सकते हैं. अगर ई-मेल की "from" वाली लाइन "remitly-security@hotmail.com" या "remitly-fraud@msn.com" जैसी लगती है या इसमें किसी अन्य इंटरनेट सेवा प्रदाता का नाम है, तो आप सुनिश्चित हो सकते हैं कि यह वास्तविक नहीं है.**](mailto:remitly-security@hotmail.com)

वेबसाइट का पता जांचें

[असली Remitly वेबसाइट हमेशा निम्नलिखित डोमेन पर होस्ट की जाती हैं: https://www.remitly.com/](https://www.remitly.com/)

नकली ई-मेल में होने वाला लिंक भी कभी-कभार असली Remitly पते जैसा लगता है. आप लिंक पर अपने माउस को फिराकर इस बात की जांच सकते हैं कि यह असल में कहां इशारा करता है - वास्तविक वेबसाइट जिसकी तरफ़ यह इशारा करता है वह आपके ब्राउज़र विंडो के नीचे स्टेटस बार में या पॉप-अप के तौर पर दिखाई देगी.

[हम ऊपर सूचीबद्ध डोमेन के अतिरिक्त किसी अन्य डोमेन पर होस्ट किए गए वेब पते का कभी भी उपयोग नहीं करते हैं. उदाहरण के लिए, भिन्न डोमेन जैसे "https://security-payments-remitly.com/..." या एक आईपी पता (स्ट्रिंग की संख्याएं) जिसके साथ "https://123.456.789.123/remitly.com/..." जैसी डायरेक्टरीज़ होती हैं, जो मान्य Remitly वेबसाइट नहीं हैं.](https://security-payments-remitly.com/)

साथ ही, कभी-कभार नकली ई-मेल इस तरह से तैयार किया जाता है कि अगर आप टेक्स्ट पर कहीं भी क्लिक करें तो आपको धोखाधड़ी वाली वेबसाइट पर ले जाए. Remitly कभी भी ऐसे ईमेल नहीं भेजेगा. अगर आप गलती से ऐसे किसी ई-मेल पर क्लिक करके किसी फ़र्ज़ी वेबसाइट पर चले जाएं, तो कोई भी जानकारी ना डालें; इसके बजाय, बस उस ब्राउज़र विंडो को बंद कर दें.

अगर कोई ई-मेल संदिग्ध लगे तो सीधे Remitly की वेबसाइट पर जाएं

[जब संदेह हो, तो ई-मेल में दिए गए लिंक पर क्लिक न करें. सीधे https://www.remitly.com/ पर जाएं और हालिया खरीदारी को देखने या अपने खाते की जानकारी की समीक्षा करने के लिए सबसे ऊपर दाईं ओर दिए गए मेन्यू से अपने खाते पर क्लिक करें. अगर आप अपने खाते तक नहीं पहुंच सकते या आपको कुछ भी संदिग्ध दिखाई देता है, तो हमें तुरंत बताएं.](https://www.remitly.com/)

अपने खाते की जानकारी को सुरक्षित रखें

[अगर आपने किसी फ़र्ज़ी या संदिग्ध ई-मेल पर क्लिक किया है और आपने अपने Remitly खाते की जानकारी डाली है, तो आपको तुरंत अपने पासवर्ड को अपडेट कर देना चाहिए. आप सीधे https://www.remitly.com/ पर जाकर खाता सेटिंग्स पर क्लिक करके, ऐसा कर सकते हैं. अगले पेज पर 'अपनी

व्यक्तिगत जानकारी, ई-मेल पता या पासवर्ड बदलें' पर क्लिक करें.](https://www.remitly.com/)

अगर आपने अपना क्रेडिट कार्ड नंबर फ़र्ज़ी ई-मेल संदेश से जुड़ी साइट पर डाला है, तो हमारी सलाह है कि आप अपनी जानकारी की सुरक्षा के लिए कदम उठाएं. शायद आप अपनी क्रेडिट कार्ड कंपनी से संपर्क करके उन्हें इस मामले के बारे में सूचित करना चाहें. आखिर में, आपको अपने Remitly खाते से उस क्रेडिट कार्ड को हटा देना चाहिए, ताकि किसी को भी आपके खाते को अनुचित तरीके से फिर से ऐक्सेस करने से रोका जा सके.

फ़िशिंग ई-मेल की रिपोर्ट करना

[**अगर आपको कोई ऐसा ई-मेल मिलता है, जिसकी जालसाज़ी के बारे में आपको पता है या अगर आपको लगता है कि आप फ़िशिंग का शिकार हो गए हैं और आपको अपने Remitly खाते की चिंता है, तो कृपया हमें फ़िशिंग या फ़र्ज़ी ई-मेल की रिपोर्ट करके तुरंत बताएं.**](https://www.remitly.com/il/hi/home/contact/)