Transactie- en Accountbeveiliging

De beveiliging van uw account is belangrijk voor ons en we hebben verschillende stappen ondernomen om de informatie in verband met uw Remitly-account te beschermen. Ook u kunt bepaalde zaken doen die bijdragen aan de bescherming van uw account en persoonlijke gegevens.

Account Verificatieprocessen

Uw Remitly-account is onderworpen aan verificatieprocedures om een hoog niveau van veiligheid, vertrouwen en bescherming te handhaven.

Als u een nieuwe Remitly-klant bent en via de Remitly-website een nieuwe Remitly-account aanmaakt, moet u bepaalde persoonlijke gegevens verstrekken en het e-mailverificatieproces voltooien.

Zodra uw account operationeel is, stellen we verscheidene handmatige en geautomatiseerde risicobeheerprocedures in werking waarmee we verdachte accountactiviteiten onder de aandacht kunnen brengen. Het doel is om alle kenmerken te identificeren die ongebruikelijk of inconsistent lijken met uw gebruik in het verleden. Als onderdeel van dit proces gaan we contracten aan met toonaangevende dienstverleners om persoonlijke en financiële informatie te verifiëren. Deze diensten zullen nooit rechtstreeks contact met u opnemen of uw gegevens gebruiken voor iets anders dan de succesvolle afronding van uw voorgenomen transactie.

Wachtwoordbeveiliging

Wanneer u inlogt bij uw account, doen we bepaalde dingen om uw account te beschermen. Ten eerste, wanneer u inlogt bij uw Remitly-account, logt u in via een beveiligde serververbinding (https://). We gebruiken Secure Socket Layer (SSL) met 256-bit encryptie, de industrienorm voor de beveiliging van servers.

Uw account wordt ook beschermd door een uniek wachtwoord dat u hebt aangemaakt. Gebruik geen veelvoorkomende woorden of zinnen als wachtwoord. In plaats daarvan moet uw wachtwoord bestaan uit ten minste acht tekens met zowel cijfers als letters met gebruik van hoofdletters en kleine letters. U dient dit wachtwoord vertrouwelijk te houden. Het delen van uw wachtwoord zal de beveiliging van uw Remitly-account verminderen.

Wees op uw Hoede voor Internetbedrog

- Voer NOOIT een betaling uit om loterij- of prijswinningen te claimen, of op

belofte van het ontvangen van een grote som geld.

- Voer NOOIT een betaling uit omdat u een creditcard of lening werd "gegarandeerd".
- Reageer NOOIT op een internet- of telefoonaanbod waarvan u niet zeker weet of het eerlijk is.
- Voer NOOIT een betaling uit aan iemand die je niet kent of wiens identiteit u niet kunt verifiëren.

Vraag bij twijfel de beoogde ontvanger om meer informatie over het doel en de veiligheid van de gevraagde betaling. Voer de betaling pas uit wanneer u zich gerust voelt bij de transactie.

Identificatie van Phishing of Gespoofte E-mails

U kunt op een bepaald moment een e-mail ontvangen die eruit ziet als afkomstig van Remitly, maar in feite niet echt is. Een dergelijke e-mail kan u doorverwijzen naar een website die eruitziet als de Remitly-website. U kunt zelfs worden gevraagd om accountgegevens te verstrekken, zoals uw e-mailadres en wachtwoord.

Deze valse websites kunnen uw gevoelige account- en betalingsgegevens stelen om fraude te plegen. Deze valse e-mails kunnen potentiële virussen of malware bevatten die wachtwoorden of gevoelige gegevens kunnen detecteren. Wij raden u daarom aan een antivirusprogramma te installeren en dit te allen tijde up-to-date te houden.

Hier zijn enkele belangrijke punten om in gedachten te houden als onderdeel van een verdediging tegen frauduleuze e-mails:

1. Weet wat Remitly niet zal vragen via e-mail

- Uw volledige socialezekerheidsnummer of geboortedatum
- Uw creditcardnummer, PIN-code of beveiligingscode van uw creditcard (inclusief "updates" van een van de bovenstaande)

2. Wees op uw hoede voor bijlagen in verdachte e-mails

Wij raden u aan geen e-mailbijlagen te openen van verdachte of onbekende bronnen. E-mailbijlagen kunnen virussen bevatten die uw computer infecteren wanneer de bijlage wordt geopend. Als u een verdachte e-mail ontvangt die naar verluidt door Remitly werd verzonden en die een bijlage bevat, raden wij u aan de e-mail te verwijderen zonder de bijlage te openen.

3. Zoek naar grammaticale of tikfouten.

Zoek naar slechte grammatica of tikfouten. Sommige phishing e-mails worden uit andere talen vertaald of zonder proeflezen verzonden en bevatten daardoor grammaticale of tikfouten.

4. Controleer het retouradres

Is de e-mail van Remitly? Hoewel phishers een vervalste e-mail kunnen sturen om de schijn te creëren dat de e-mail afkomstig is van Remitly, kunt u soms door het retouradres te controleren bepalen of de e-mail authentiek is. Als de regel "van" in de e-mail eruit ziet als "remitly-security@hotmail.com" of "remitly-fraud@msn.com", of de naam van een andere internetprovider bevat, kunt u er zeker van zijn dat deze niet echt is.

5. Controleer het adres van de website

Echte Remitly-websites worden altijd gehost op het volgende domein: https://www.remitly.com/

Soms lijkt de link in gespoofte e-mails op een echt Remitly-adres. U kunt controleren waar de link daadwerkelijk naartoe verwijst door met de muis over de link te bewegen – de website waar de link naartoe verwijst wordt weergegeven in de statusbalk onderin uw browservenster of als een pop-up.

We gebruiken nooit een webadres dat gehost wordt op een ander domein dan de hierboven vermelde domeinen. Bijvoorbeeld variantdomeinen zoals "http://security-payments-remitly.com/" of een IP-adres (nummerreeks) gevolgd door directories zoals "http://123.456.789.123/remitly.com/" zijn geen geldige Remitly-websites.

Ook is de gespoofte e-mail soms zo opgezet dat als u ergens op de tekst klikt u naar de frauduleuze website wordt gebracht. Remitly stuurt nooit een e-mail die dit doet. Als u per ongeluk op een dergelijke e-mail klikt en naar een gespoofte website gaat, voer dan geen enkele informatie in maar sluit gewoon dat browservenster.

6. Als een e-mail er verdacht uitziet, ga dan direct naar de Remitly-website

Klik in geval van twijfel niet op de link in een e-mail. Ga direct naar https://www.remitly.com/ en klik op **Uw Account** in het menu rechtsboven om recente aankopen of uw accountgegevens te bekijken. Als u geen toegang hebt tot uw account of als u iets verdachts ziet, laat het ons dan meteen weten.

7. Bescherm uw accountgegevens

Als u toch vanuit een gespoofte of verdachte e-mail doorklikte en uw Remitly-accountgegevens hebt ingevoerd, dient u **onmiddellijk** uw wachtwoord bij te werken. U kunt dit doen door rechtstreeks naar https://www.remitly.com/ te gaan en te klikken op **Accountinstellingen**. Op de volgende pagina klikt u op **Wijzig uw persoonlijke gegevens, e-mailadres of wachtwoord**.

Als u uw creditcardnummer hebt verzonden naar de site waarnaar wordt gelinkt via het vervalste e-mailbericht, raden wij u aan stappen te ondernemen om uw gegevens te beschermen. U kunt bijvoorbeeld contact opnemen met uw creditcardmaatschappij om hen hiervan op de hoogte te stellen. Tot slot dient u die creditcard van uw Remitly-account te verwijderen om te voorkomen dat iemand ten onrechte weer toegang krijgt tot uw account.

8. Het melden van Phishing E-mail

Als u een e-mail hebt ontvangen waarvan u weet dat het een vervalsing is, of als u denkt dat u het slachtoffer bent geweest van een phishing-aanval en u maakt zich zorgen over uw Remitly-account, laat het ons dan meteen weten door een [phishing of gespoofde e-mail](https://www.remitly.com/home/contact) te melden.