Transaktions- und Kontosicherheit

Das Thema Kontosicherheit ist für Remitly äußerst wichtig und wir nutzen eine Vielzahl von Sicherheitsmaßnahmen, um die Sicherheit Ihrer Kontoinformationen zu gewährleisten. Auch Sie selbst können bestimmte Maßnahmen durchführen, um dabei zu helfen, Ihr Konto und Ihre persönlichen Daten zu schützen.

Verfahren zur Kontoverifizierung

Ihr Remitly-Konto unterliegt Überprüfungsverfahren, sodass ein hohes Maß an Sicherheit, Vertrauen und Schutz gewährleistet werden kann.

Wenn Sie ein neuer Remitly-Kunde sind und ein neues Remitly-Konto über die Remitly-Website erstellen, müssen Sie bestimmte persönliche Informationen angeben und den E-Mail-Verifizierungsprozess abschließen.

Sobald Ihr Konto eingerichtet wurde, setzen wir eine Vielzahl von manuellen und automatisierten Risikomanagementverfahren ein, die es uns ermöglichen, verdächtige Kontoaktivitäten zu identifizieren. Das Ziel ist es, auf all jene Charakteristika aufmerksam zu werden, die in Bezug auf Ihre bisherige Nutzung ungewöhnlich oder inkonsistent erscheinen. Im Rahmen dieses Prozesses beauftragen wir branchenführende Dienstleister, die persönliche und finanzielle Informationen überprüfen. Diese Dienstleister werden sich nie direkt mit Ihnen in Verbindung setzen oder Ihre Informationen für andere Zwecke verwenden als für jene, die für den erfolgreichen Abschluss Ihrer beabsichtigten Transaktion erforderlich sind.

Passwortsicherheit

Während Sie sich einloggen, führen wir bestimmte Maßnahmen durch, um Ihr Konto zu schützen. Wenn Sie sich in Ihr Remitly-Konto einloggen, nutzen Sie eine sichere Server-Verbindung (https://). Wir verwenden Secure Socket Layer (SSL) mit 256-Bit-Verschlüsselung, den Industriestandard für die Serversicherheit.

Ihr Konto ist auch durch das von Ihnen erstellte einzigartige Passwort geschützt. Sie sollten keine gängigen Wörter oder Phrasen als Passwort verwenden. Ihr Kennwort sollte stattdessen mindestens acht Zeichen lang sein und eine Kombination von Großbuchstaben, Kleinbuchstaben und Ziffern enthalten. Behandeln Sie dieses Passwort vertraulich. Das Teilen Ihres Passwortes mit anderen Personen gefährdet die Sicherheit Ihres Remitly-Kontos.

Schützen Sie sich vor Internet-Betrügern

- Leisten Sie KEINE Zahlungen, um Lotteriegewinne oder Preise in Anspruch zu nehmen oder um auf ein Versprechen zu reagieren, das große Geldsummen in Aussicht stellt.
- Leisten Sie KEINE Zahlungen aufgrund der Tatsache, dass Ihnen eine Kreditkarte oder ein Darlehen „zugesichert" wurden.
- Reagieren Sie NICHT auf ein Internet- oder Telefonangebot, von dem Sie nicht sicher sein können, dass es ehrlich gemeint ist.
- Leisten Sie KEINE Zahlungen an Personen, die Sie nicht kennen oder deren Identität Sie nicht verifizieren können.

Fordern Sie im Zweifelsfall einen potenziellen Empfänger dazu auf, Ihnen Informationen zum Zweck und zur Sicherheit der von ihm erbetenen Zahlung zu übermitteln. Übermitteln Sie die Zahlung erst dann, wenn Sie mit den Inhalten der Transaktion zufrieden sind.

Identifizieren von Phishing oder gefälschten E-Mails

Unter Umständen können Sie E-Mails erhalten, die so aussehen, als kämen sie von Remitly, aber in Wirklichkeit gefälscht sind. Eine solche E-Mail-Nachricht kann Sie ggf. zu einer Website weiterleiten, die der Remitly-Website ähnelt. Sie werden dann eventuell gebeten, bestimmte Kontoinformationen wie Ihre E-Mail-Adresse oder Ihr Passwort anzugeben.

Diese nicht authentischen Websites können sich aus betrügerischen Gründen Ihre sensiblen Konto- und Zahlungsinformationen aneignen. Betrügerische E-Mails können potenzielle Viren oder Malware enthalten, die Passwörter oder sensible Daten erkennen können. Wir empfehlen Ihnen daher, ein Anti-Viren-Programm zu installieren und dieses zu jeder Zeit auf dem neuesten Stand zu halten.

Hier sind einige wichtige Punkte, die Sie vor betrügerischen E-Mails schützen sollen:

1. Sie sollten wissen, welche Details Remitly nicht per E-Mail von Ihnen abfragt

- Ihre vollständige Sozialversicherungsnummer oder Ihr Geburtsdatum
- Ihre Kreditkartennummer, PIN oder Ihren Kreditkarten-Sicherheitscode (einschließlich „Updates" zu einem der oben genannten Punkte)

2. Vorsicht vor Anhängen in verdächtigen E-Mails

Wir empfehlen Ihnen, keine E-Mail-Anhänge aus verdächtigen oder unbekannten

Quellen zu öffnen. Anlagen können Viren enthalten, die Ihren Computer infizieren, sobald Sie sie öffnen. Wenn Sie verdächtige E-Mails erhalten, die angeblich von Remitly gesendet wurden und einen Anhang enthalten, empfehlen wir Ihnen, diese E-Mails zu löschen, ohne den Anhang zu öffnen.

3. Achten Sie auf grammatikalische oder typografische Fehler

Achten Sie auf schlechte Grammatik oder typografische Fehler. Einige Phishing-Mails wurden aus anderen Sprachen übersetzt oder ohne vorherige Korrekturlesung versandt, was schlechte Grammatik oder typografische Fehler zur Folge haben kann.

4. Überprüfen Sie die Absenderadresse

Stammt die E-Mail von Remitly? Während Phisher zwar gefälschte E-Mails versenden können, die so aussehen, als kämen sie von Remitly, können Sie eventuell feststellen, ob diese authentisch sind, indem Sie die Absenderadressen überprüfen. Wenn der Absender (die „Von"-Zeile) der E-Mail wie „remitly-security@hotmail.com" oder „remitly-fraud@msn.com" aussieht oder den Namen eines anderen Internet-Dienstanbieters enthält, können Sie sicher sein, dass die Nachricht nicht authentisch ist.

5. Überprüfen Sie die Adresse der Website

Echte Remitly-Websites werden immer auf folgender Domain gehostet: https://www.remitly.com/

Manchmal sieht der Link in gefälschten E-Mails wie eine echte Remitly-Adresse aus. Sie können überprüfen, worauf der Link tatsächlich verweist, indem Sie die Maus über den Link bewegen – die eigentliche Website, auf die Sie weitergeleitet werden, wird dann in der Statusleiste am unteren Rand Ihres Browserfensters oder als Pop-up angezeigt.

Wir verwenden niemals Web-Adressen, die auf einer anderen Domain als den oben aufgeführten gehostet werden. Zum Beispiel sind Domains wie „http://security-payments-remitly.com/" oder eine IP-Adresse (Zahlenfolge), gefolgt von Verzeichnissen wie „http://123.456.789.123/remitly.com/", keine gültigen Remitly-Websites.

Manchmal ist die gefälschte E-Mail auch so eingerichtet, dass Sie, sobald Sie irgendwo auf den Text klicken, auf die betrügerische Website weitergeleitet werden. Remitly

würde nie eine solche E-Mail versenden. Wenn Sie versehentlich auf eine solche E-Mail klicken und zu einer gefälschten Website gelangen, geben Sie keine Informationen ein; schließen Sie stattdessen einfach das Browserfenster.

6. Erscheint Ihnen eine E-Mail-Nachricht verdächtig, gehen Sie direkt zur Remitly-Website

Klicken Sie im Zweifelsfall nicht auf einen Link, der in einer E-Mail enthalten ist. Gehen Sie direkt zu https://www.remitly.com/ und klicken Sie auf **Ihr Konto** im Menü oben rechts, in dem die letzten Einkäufe eingesehen werden können, oder überprüfen Sie Ihre Account-Informationen. Wenn Sie nicht auf Ihr Konto zugreifen können oder wenn Sie etwas Verdächtiges sehen, lassen Sie es uns sofort wissen.

7. Schützen Sie Ihre Kontoinformationen

Wenn Sie von einer gefälschten oder verdächtigen E-Mail aus weiterklicken und Ihre Remitly-Kontoinformationen eingegeben haben, sollten Sie Ihr Passwort **sofort** ändern. Sie können dies tun, indem Sie direkt auf https://www.remitly.com/ gehen und auf **Kontoeinstellungen** klicken. Klicken Sie auf der nächsten Seite auf **Ändern Ihrer persönlichen Informationen, Ihrer E-Mail-Adresse oder Ihres Passwortes**.

Wenn Sie Ihre Kreditkartennummer auf der Seite, die mit der gefälschten E-Mail-Nachricht verlinkt ist, eingegeben haben, empfehlen wir Ihnen, Schritte zum Schutz Ihrer Daten zu unternehmen. Sie sollten sich dann beispielsweise mit Ihrer Kreditkartenfirma in Verbindung setzen, um diese über diese Angelegenheit zu informieren. Sie sollten in weiterer Folge diese Kreditkarte von Ihrem eigenen Konto löschen, um zu verhindern, dass jemand unrechtmäßig Zugriff auf Ihr Konto erlangt.

8. Meldung von Phishing-E-Mails

Wenn Sie eine E-Mail erhalten haben, von der Sie wissen, dass es sich um eine Fälschung handelt, oder wenn Sie denken, dass Sie Opfer eines Phishing-Angriffs geworden sind und Sie in Bezug auf Ihr Remitly-Konto besorgt sind, teilen Sie uns dies bitte sofort mit, indem Sie diesen Vorfall unter [Phishing oder gefälschte E-Mails](https://www.remitly.com/home/contact) melden.