SICHERHEITSRISIKEN

Sicherheit der Kryptowährungs-Wallet/des Kryptowährungskontos des Kunden und der E-Mail-Konten des Kunden.

Der Kunde muss alle angemessenen Schritte unternehmen, um die Kryptowährungs-Wallet/das Konto, das Passwort und alle anderen Sicherheitsmerkmale des Kunden jederzeit sicher zu verwahren und sie niemals an Dritte weiterzugeben.

Der Kunde muss alle angemessene Sorgfalt walten lassen, um sicherzustellen, dass die E-Mail-Konten des Kunden sicher sind und nur der Kunde darauf zugreifen kann, da die E-Mail-Adresse des Kunden verwendet werden kann, um Sicherheitscodes zu erhalten, die für die Abhebung von Geldern von der Kryptowährungs-Wallet/dem Kryptowährungskonto des Kunden verwendet werden, um Passwörter zurückzusetzen oder um mit dem Kunden über die Sicherheit Ihrer Kryptowährungs-Wallet/Ihres Kryptowährungskontos zu kommunizieren. Für den Fall, dass eine der bei PTGR registrierten E-Mail-Adressen des Kunden kompromittiert wird, sollte der Kunde unverzüglich nach Bekanntwerden dieses Ereignisses PTGR und auch den E-Mail-Dienstleister des Kunden kontaktieren.

Unsere Mitarbeiter werden Sie niemals auffordern, Ihr E-Mail-Passwort und andere E-Mail-Sicherheitsfunktionen (z. B. OTP, 2FA usw.) an uns oder Dritte weiterzugeben. Der Kunde ist verpflichtet, seine E-Mails privat und vertraulich zu verwalten und zu verwenden, ohne jemandem Zugang zu gewähren, auch nicht mittels Fernsteuerungsdiensten (VPN, Nutzung desselben Geräts, TeamViewer usw.).

Jede Nachricht, die der Kunde erhält, oder jede Website, die nach dem Passwort des Kunden oder anderen Sicherheitsmerkmalen fragt, sollte an PTGR gemeldet werden. Wenn der Kunde Zweifel an der Echtheit einer Website hat, sollte er sich an PTGR wenden. Es ist ratsam, dass der Kunde das Passwort regelmäßig, d.h. mindestens alle drei Monate, ändert, um das Risiko einer Sicherheitsverletzung in Bezug auf die Kryptowährungs-Wallet/das Kryptowährungskonto des Kunden zu verringern. PTGR rät dem Client auch, kein Passwort zu wählen, das leicht aus Informationen zu erraten ist, die jemand über den Client kennen oder sammeln könnte, oder ein Passwort, das eine Bedeutung hat.

Unabhängig davon, ob der Kunde einen öffentlichen, einen gemeinsam genutzten oder einen eigenen Computer verwendet, um auf seine E-Mail und/oder Kryptowährungs-Wallet/sein Konto zuzugreifen, muss der Kunde immer sicherstellen, dass seine Anmeldedaten nicht vom Browser gespeichert oder zwischengespeichert oder anderweitig aufgezeichnet werden. Der Kunde sollte niemals Funktionen verwenden, die es ermöglichen, Anmeldedaten oder Passwörter auf dem von ihm verwendeten Computer zu speichern.

Der Kunde muss die Sicherheitsverfahren einhalten, über die PTGR den Kunden von Zeit zu Zeit informiert.

Der Kunde, nicht PTGR, ist für die Aufrechterhaltung einer angemessenen Sicherheit und Kontrolle aller IDs, Passwörter oder anderer Details verantwortlich, die der Kunde für den Zugriff auf seine Wallet/sein Konto und die Dienste verwendet. Der Kunde ist allein verantwortlich für den unbefugten Zugriff auf und/oder die unbefugte Nutzung der Wallet/des Kontos und/oder der E-Mail des Kunden sowie für Verlust, Diebstahl, Veruntreuung und/oder Missbrauch. Der Kunde haftet ausschließlich für alle Verluste und Kosten (vollständig und vollständig, ohne Beschränkungen, Beschränkungen und Ausschlüsse) im Zusammenhang mit einer unbefugten Nutzung der Kryptowährungs-Wallet/des Kryptowährungskontos und/oder der E-Mail-Konten des Kunden sowie in Fällen, in denen der Kunde betrügerisch handelt und/oder eine oder mehrere seiner Verpflichtungen in Bezug auf die korrekte und sichere Verwendung und sichere Aufbewahrung der Kryptowährungs-Wallet/des Kryptowährungskontos und/oder der E-Mail-Konten des Kunden nicht erfüllt.

In Anbetracht der Tatsache, dass sich die Technologien schnell und ständig weiterentwickeln und es derzeit unmöglich ist, alle möglichen zukünftigen Wege vorherzusehen, um illegalen Zugriff auf die Kryptowährungs-Wallet/das Kryptowährungskonto und/oder die E-Mail-Konten des Kunden zu erhalten, ist es unmöglich, alle Maßnahmen aufzulisten, die der Kunde ergreifen oder vermeiden muss, um die sichere Aufbewahrung und Nutzung der Kryptowährungs-Wallets/des Kryptowährungskontos und/oder der E-Mail-Konten des Kunden zu gewährleisten. Nichtsdestotrotz trägt der Kunde die volle Verantwortung dafür, alle angemessenen Vorsichtsmaßnahmen und Sicherheitsmaßnahmen zu ergreifen, um den Zugriff unbefugter Personen auf die Kryptowährungs-Wallet/das Kryptowährungskonto und/oder die E-Mail-Konten des Kunden und deren weitere Nutzung zu verhindern.