KRYPTO-SCAMS UND WIE MAN SIE VERMEIDET

Veröffentlicht am 19.02.2024 um 10:02 von Redaktion AltkreisBlitz

Es ist ein weit verbreiteter Irrglaube, dass Krypto-Betrug
vor allem ältere oder leichtgläubige Menschen betrifft. Tatsächlich kann jeder Opfer von Online-Betrügern werden, die immer raffiniertere Überredungs- und Manipulationsmethoden einsetzen, um an Ihr Geld zu kommen - insbesondere im Bereich der Kryptowährungen. Im folgenden Artikel präsentieren wir Ihnen die gängigsten Krypto-Scams und wie man sie vermeidet.

Das sind die häufigsten Krypto-Scams

Es gibt eine gigantische Anzahl verschiedener Arten von Krypto-Betrug. Im Folgenden konzentrieren wir uns auf die am weitesten verbreiteten Scam-Methoden.

1. Wallet-Drainer - neue Gefahr im Krypto-Raum

Wallet-Drainer nutzen Sicherheitslücken in Kryptobörsen, digitalen Geldbörsen oder dezentralisierten Anwendungen (dApps) aus. Auch wenn Sie nur den aktuellen Bitvavo IOTA Kurs checken möchte, sollten Sie stets vorsichtig sein. Wenn ein Nutzer seine digitale Geldbörse mit einer manipulierten Webseite oder Plattform verbindet und einen Smart Contract über seine Wallet bestätigt, stimmt er damit allen Aktionen zu, die im Code des betrügerischen Smart Contracts festgelegt sind. Diese Zustimmung führt in der Regel dazu, dass alle in der Wallet befindlichen Kryptowährungen und NFTs auf eine von den Angreifern kontrollierte Wallet übertragen werden. Die Folgen solcher Angriffe können für die Betroffenen katastrophal sein, da die entwendeten Gelder aufgrund der Irreversibilität von Blockchain-Transaktionen nicht zurückgegeben werden können.Die Transparenz der Blockchain bietet jedoch die Möglichkeit, Transaktionen nachzuverfolgen. Wallets, die unter der Kontrolle von Kriminellen oder mit Geldern aus zweifelhaften Quellen in Verbindung stehen, können identifiziert und markiert werden. Dies kann es Kriminellen erschweren, gestohlene Kryptowährungen in traditionelle Währungen umzutauschen, insbesondere wenn sie durch Überwachungsinstrumente wie Chainalysis markiert sind. Dennoch sollten Sie bei der Autorisierung von Transaktionen auf Websites äußerste Vorsicht walten lassen und immer die URL einer Webpräsenz überprüfen, bevor Sie Ihre persönlichen Daten eingeben und Ihre Wallet verbinden.

2. ICO-Scams - die altbewährte Betrugsmasche

Initial Coin Offerings (ICOs) sind eine Methode der Kapitalbeschaffung, bei der Unternehmen eine neue Kryptowährung auf den Markt bringen und diese an Investoren verkaufen. Die Anleger kaufen diese digitalen Währungen in der Hoffnung, dass ihr Wert im Laufe der Zeit steigt. Einige Betrüger nutzen jedoch die Popularität von ICOs aus, um für gefälschte Projekte zu werben. Diese sogenannten ICO-Scams locken mit der Aussicht auf ein innovatives Blockchain-Projekt, hinter dem jedoch kein reales Produkt oder Unternehmen steht.Wenn eine Investitionsmöglichkeit zu gut klingt, um wahr zu sein, und die Projektverantwortlichen das Unmögliche versprechen: Sollten Sie vor einer Investition gründlich recherchieren. Ein hohes Maß an Skepsis und eine gründliche Recherche können Sie vor Betrug und Krypo-Scammern schützen.

3. SIM-Swap-Attacken - raffinierte Angriffe auf Smartphones

Bei der SIM-Swap-Attacke täuschen die Krypto-Scammer einen Mobilfunkanbieter vor, um die Telefonnummer eines Nutzers auf eine neue SIM-Karte zu kopieren. Dadurch erhält der Betrüger vollen Zugriff auf die Telefonnummer des Nutzers, einschließlich der Möglichkeit, SMS zu empfangen, die für die Zwei-Faktor-Authentifizierung (2FA) verwendet werden. Auf diese Weise kann sich der Angreifer Zugang zu Finanzkonten, sozialen Netzwerken und anderen Online-Diensten des Opfers verschaffen. Die Folgen eines solchen Betrugs sind schwerwiegend und können von finanziellen Verlusten über Identitätsdiebstahl bis hin zu emotionalen Schäden und Reputationsverlust reichen. Ein aktuelles Beispiel ist der gehackte

Twitter-Account der SEC, über den ein verfrühter Tweet über einen Bitcoin-Spot-ETF veröffentlicht wurde, der zu Marktschwankungen führte.Um sich vor solchen Gefahren zu schützen, sollten Sie die Strategien der Betrüger kennen und aktiv Maßnahmen zum Schutz der eigenen Telefonnummer und persönlichen Daten ergreifen. Statt Telefonnummern für die Zwei-Faktor-Authentifizierung zu verwenden, sollten Sie auf spezielle Apps setzen, wie zum Beispiel:Google AuthenticatorAuthy

Fazit

Der beste Schutz vor Krypto-Betrug ist eine sichere Wallet. Der Schlüssel ist der wichtigste Sicherheitsfaktor und sollte nur Ihnen bekannt sein.