

## Welche Gefahren birgt der digitale Raum?

Sicherheit wird im digitalen Raum und gerade im Bereich Bitcoin immer eine große Rolle spielen. Oftmals ist es schwierig unseriöse Dienste oder betrügerische Techniken auf den ersten Blick zu erkennen. Eine große Gefahr ist es, dass mit einem falschen Download oder durch eine Anmeldung auf einer betrügerischen Website, sofort die gesamte eigene Sicherheit kompromittiert sein kann. Daten sind im digitalen Raum Gold wert und daher ist es immer wichtig, die persönlichen Daten zu schützen. Vor allem wenn es um den Bereich Bitcoin oder Geld im Allgemeinen geht.

## Welche Methoden werden von Angreifern genutzt?

Die wahrscheinlich gängigste Methode zum Stehlen von Informationen ist das sogenannte Phishing. Hierbei werden zum Beispiel seriös aussehende E-Mails versendet, welche die Aufforderung enthalten, die eigenen Benutzerdaten bei einem Bankkonto zu aktualisieren oder erneut über einen Link zu verifizieren. Der Link führt allerdings zu einem Nachbau der Website des Unternehmens und somit können Benutzerdaten in die falschen Hände geraten. Es können auch Dateien mit Malware versendet werden. Diese Malware kann verschiedene Zwecke haben und sich unbemerkt auf deinem Computer installieren.

Weiterhin gibt es ebenfalls verschiedene Betrugsmaschen, gerade rund um den Bereich Bitcoin. Es wird meistens mit hohen Renditen geworben. Betrüger geben sich als Broker aus oder eine Plattform verleiht Bitcoin und verspricht darüber einen Zins. Ebenso gibt es viele Schneeballsysteme oder Trading-Bots, welche durch einen Algorithmus angeblich hohe Gewinne erzielen. Von all diesen Dingen sollte man sich fernhalten, gerade wenn gefordert wird Bitcoin an die Plattform zu senden.

## Woran erkenne ich potenzielle Betrugsversuche?

Im Allgemeinen gilt: überprüfe alles detailliert und vertraue nicht blind.

Prüfe beispielsweise die Adresse des Absenders einer E-Mail, prüfe die URL eines weiterführenden Links, prüfe auch den Inhalt einer Nachricht auf Logik und generell auf die Rechtschreibung und Grammatik. Bei Webseiten von Unternehmen kann der Unternehmenssitz, das Impressum, die Geschäftsführer und das Geschäftsmodell geprüft werden. Es kann ebenfalls helfen, den Namen eines Unternehmens in Verbindung mit Schlagwörtern wie „Betrug“ oder „Erfahrungen“ über eine Online-Suchmaschine einzugeben. Wenn du E-Mails erhältst, vermeintlich von Unternehmen bei denen du Kunde bist, kontaktiere das Unternehmen direkt und frage nach, ob die Nachricht seriös ist.

Überlege genau, ob es sinnvoll ist, dass dich ein Unternehmen kontaktiert und die Ausführung bestimmter Schritte verlangt. Schau auf der Website des Unternehmens nach, melde dich bei deinem Kundenkonto an oder kontaktiere das Unternehmen direkt bevor du einen Link aus einer E-Mail anklickst.

## Was kann ich beachten, um mich zu schützen?

Der Empfang von Spam oder Phishing-E-Mails wird sich vermutlich kaum verhindern lassen. Im Allgemeinen kannst du aber, wie beschrieben, den Absender überprüfen, niemals unerwartete Anhänge öffnen, nicht auf Links klicken, wenn du selbst keinen angefordert hast. Weiterhin kannst du vor der Anmeldung bei Webseiten die Seriösität prüfen und selbst recherchieren. Im Zweifel kannst du auch immer das Unternehmen kontaktieren, um die Echtheit einer Nachricht zu verifizieren.

Lade niemals Software herunter, um den Bildschirm mit Fremden zu teilen oder Fernsteuerungssoftware, um den Zugang zu dem eigenen Gerät zu ermöglichen. Gerade im Bitcoin-Bereich gibt es viele Betrugsmaschen, welche sich diese Technik gerne zu Nutze machen. Vertraue nicht auf „Investitionsberater“, „Broker“ oder sonstige Personen, egal, wie seriös sie auch erscheinen mögen. Erst recht nicht, wenn sie dich per E-Mail oder Social-Media kontaktieren. Lasse dich nicht von Personen dazu verleiten, ein Konto bei einer Plattform zu eröffnen, die du nicht kennst und führe ebenfalls keine Transaktionen auf das Drängen von anderen aus.

Vertraue nur dir selbst und deiner eigenen Recherche. **„Don't trust, verify!“** - Vertraue nicht, verifiziere!

## Wie schütze ich meine Bitcoin?

Generell gilt im Bitcoin-Bereich: **„Not your keys, not your coins.“** - Nicht deine Private Keys, nicht deine Bitcoin. Dieses Mantra wird schon seit Jahren von Bitcoinern wiederholt. Es ist im Prinzip die wichtigste Regel in diesem Bereich. Du kannst nur sicher sein, Bitcoin im eigenen Besitz zu haben, wenn nur du alleine die Private Keys kennst. Verwende daher keine sog. Custody-Lösungen, bei denen Plattformen oder Börsen die Verwaltung der Private Keys übernehmen.

Bitcoin bedeutet Selbstbestimmung, aber dadurch auch Verantwortung. Lerne, wie du diese Verantwortung übernehmen kannst und deine Private Keys richtig absicherst.

## Interessiert?

Du findest unser Angebot unter: <https://bitcoinexplained.de/beratung/>

Mehr Informationen zur Sicherheit u. a. relevante Themen findest du unter: <https://bitcoinexplained.de/freie-inhalte/>