CryptoCurrencies & Bitcoin Scams

The entire cryptocurrency market has reached a total traded capitalization of nearly $2 trillion dollars in just 10 years. The price of a single bitcoin reached $18,737.60 by 18 December 2017, with a global FOMO frenzy, but then the price of bitcoin tanked to as low as $3,209.76 by 15 December 2018. The volatility of the cryptocurrency has not however deterred investors trying to make a quick buck and this is where the scammers take advantage of innocent victims.

Although blockchain tech is a relatively safe technology, cybercriminals manage to find breaches and loopholes to break into the websites and compromise users' digital wallets and funds. It goes without saying that the laws protecting investors of ICO are far from perfect, so it's easy for founders to commit serious financial crime and get away with it. The term "Wild West" is often associated with cryptocurrencies and for the most part, it is true, as global regulation is still a work in progress, with governments struggling to keep up with the pace of innovation.

People often buy cryptocurrencies using a credit card/ wire transfer or any type of method to move funds to an exchange and in some cases directly through the scam websites, and this is where the liability can be attributed to the card issuers and banks, as they are supposed to safeguard customers funds.

Investment Scams will often get you to transfer cryptocurrencies as they are anonymous it is very difficult for an untrained to track and recover their funds. Below are two of the most prolific scams in recent history:

In 2015 Ruja Ignatova, along with her brother, Konstantin Ignatov, ran "OneCoin" which claimed to be a new and better version of the cryptocurrency Bitcoin and managed to steal an incredible $5 Billion from people around the world. They held elaborate and glamorous events where they pitched OneCoin to potential investors and claimed it was going to change the world and usher in a new world of financial freedom. Those who invested early were told they would be at the start of a revolution. However, nothing actually existed, OneCoin didn't have a blockchain, a cryptocurrency or wallet. Ruja Ignatova vanished in mid-2017 and is being charged with money laundering offenses in several countries.

Another well known MLM cryptocurrency scheme was a company called "Bitconnect" that had a total capitalization of trade in excess of $1.5 Billion just before the entire house of cards came tumbling down on 16 January 2018, and with it many thousands of people lost all of their investments to what turned out to be a global Ponzi scheme. The scammers were accused of fraud, misrepresentation, and misappropriation in connection with bitcoin/BCC trading. The crypto scammers are now being sought by law enforcement authorities in virtually every major country.

Common types of Cryptocurrency Scams

Cryptocurrency scammers are constantly inventing new ways to steal your coins & tokens many people have reportedly been a victim to one of these five types of scams below.

The Pump & Dump

The crypto scammers "pump up" or hype up (pump) a cryptocurrency that they own in bulk with the aim to sell it (dump) once the value peaks due to the increased demand that they themselves have generated. In most cases, however, they will actually convince newbie inexperienced investors into colluding with their scam with false promises of massive returns. Sadly these naive people often find out too late and are then left holding huge amounts of worthless cryptocurrencies.

Fake Investment Syndicates

Often the only people who profit from online "syndicates" are the scammers who run them. The sites look incredibly legitimate and, similar to binary options sites, they also feature photos of happy members with large houses, sports cars or in exotic locations, and claim to have made megabucks by investing with the hidden cryptocurrency pros who stand behind the curtain. The last time you see your money will be when you hand it over to the scammers and then suddenly the customer support is too busy to assist with your inquiries about returning investments or missed deadlines for dividends.

Fake Exchanges

They're all over cyberspace, and for first-time investors, they're hard to distinguish from the legitimate ones. In December 2017, Korean authorities closed down one of them, BitKRX. What was particularly pernicious was that BitKRX usurped the last three letters of its name from KRX, the Korean Stock Exchange, in order to purposely misrepresent itself.

Fake Wallet

This scam is custom-made for cryptocurrencies. Since "altcoins" are bytes of data, rather than metal, they have to be parked somewhere online in what is euphemistically called a "digital wallet." Innovative scammers with good marketing skills set up their own digital wallets advertise aggressively for customers to come along and once they deposit their cryptocurrency in them, it disappears forever.

Ponzi and Pyramid Schemes

If cryptocurrency investments are, as they say, guaranteed to quickly appreciate in value at a skyrocketing rate, why would someone offer you a higher interest than the market currently generates? The most obvious answer is because the offer is a red light for a cryptocurrency Ponzi or pyramid scheme. The phenomenon will continue, since other such online schemes employ the same 200%-in-90-days business model, and are bound to collapse as well. The main difference between the operators of these sites and Charles Ponzi, for whom the scheme is named, is that these guys, unlike Mr. Ponzi, are anonymous.

Telegram messaging

Using the 'Telegram messaging" platform has its risks also and it is often used by scammers to trick victims into thinking they are dealing with real "admins" just by changing their username so it looks official, essentially they will add a letter or even "admin" next to their username. Once they have started a conversation with you they will take time to gain trust and offer help and even appear to be very sympathetic to your needs. However, they will soon ask you to transfer cryptocurrency as part of an admin process to verify your details or they will try to get you to send the private keys to your wallet. Many people new to cryptocurrencies are very trusting in the beginning and are not sure about what to look for to spot the scams and the scammers rely on this and take full advantage to steal your money. Telegram is also full of bots and spam which often have links to fake sites or to sites that can install phishing links that scrape your data and allows the scammers to get more information about your online presence, so we recommend never to click on these links.