bitcoin PROFIT SECRETS

GUIDE 9:

Protect yourself against fraud and theft

How To Protect Yourself Against Fraud And Theft

Bitcoin and cryptocurrencies are hot commodities right now. Everyone wants a piece of the action, though with soaring prices, many can't afford to buy and invest out of their own pockets.

So they do the next best thing they can think of – scam and steal these precious digital coins from other people. In this guide, we'll show you some of the most common scams these con artists are running as well as how you can protect yourself against them.

Bitcoin And Cryptocurrencies Are Not Scams

Before we go into the main scams you should be aware of, we'd like to point out that these scams are all from outside forces, and not cryptocurrencies themselves. You might hear some people say that cryptocurrencies are nothing but a huge scam but it's 100% false, and we'll explain why.

The technology behind cryptocurrencies is called the blockchain. It is an incorruptible digital ledger that records all transactions in the network. No central body controls it. It is transparent, and anyone can track any transaction that has ever happened in the past.

No one can alter any transaction recorded on the blockchain because doing so would mean you'd have to alter the rest of the transactions or blocks that came after that particular transaction; this is virtually an impossible task to do.

The blockchain is so secure that many banks and startup companies are now experimenting, and starting to implement blockchain technology because they've seen just how well it works on Bitcoin and cryptocurrencies.

Now that you know you can trust the technology behind cryptocurrencies, let's discuss the most common scams that many people fall prey to.

Scam #1 – Fake Bitcoin Exchanges

There are plenty of reputable bitcoin exchanges today. The biggest and most popular platforms that have been around a few years are Coinbase, Kraken, CEX.io, Changelly, Bitstamp, Poloniex, and Bitfinex. With that being said, we cannot vouch for any company even if they're well known in the industry.

You will have to do your due diligence by researching the company's history, user reviews, and determine for yourself whether you want to spend your hard-earned fiat money with them.

Too Good To Be True Exchange Rates

Due to the highly volatile nature of cryptocurrencies (prices can go up and down by a huge spread in just a few hours!), many unsavory characters on the Internet are capitalizing on this volatility. They prey on unsuspecting beginners who can't spot the difference between a legitimate exchange and a fake one.

These fake bitcoin exchanges can easily put up nice-looking websites and impress people with their seemingly sophisticated look. They hook people

in with their promises of lower-than-market-rate prices and guaranteed returns. Simply put, they play on people's greed.

Imagine how ecstatic you'd feel if you found out about a website that offers bitcoins at 10% or 20% lower rates than the going rates on Coinbase or Kraken. If these large platforms are offering $15,000 for 1 bitcoin, and this other site is offering it at $12,000, wouldn't you jump at the chance?

You'd save so much ($3,000 per bitcoin!), and you can use your savings to buy even more bitcoins. See, that's them playing on greed! They know that people want to buy more bitcoins for less dollars. And who can blame those poor victims? If we didn't know any better, we might fall for the same scam too.

Receive Instant PayPal Payment For Your Bitcoins

Another method these fake bitcoin exchanges use to steal your bitcoins is they'll offer to buy your coins at higher-than-market-rates, and then send the equivalent dollar amount to your PayPal address.

To the unsuspecting bitcoin owner, he thinks he's getting the better end of the deal because he's going to get more money for his bitcoins, and he'll get the cash instantly in his PayPal account.

So, he enters the amount of bitcoins he wants to sell, confirms he's happy with the equivalent dollar amount, types in his PayPal address so they can send the money to him, then he waits. And waits. And waits some more.

He'll contact the website but, of course, they're not going to reply to him now because they have his bitcoins (remember, all bitcoin transactions are final and irreversible once validated).

At this point, he'll realize he's just been scammed. He can report the site and write bad reviews, but who's he kidding? These savvy scammers will just set up shop under a new domain name and wait for their next victim.

> *The key takeaway here is to stay away from 'exchanges' with too-good-to-be-true rates. As the saying goes, if it's too good to be true, it probably is.*

Scam #2 – Phishing Scams

There are so many kinds of phishing scams that run rampant today. Ever received an email from your 'bank' asking you verify or update your account details to make sure your details remain up to date? And that you have to click on the email link to update your details?

Many people are aware these types of emails are nothing more than a scam. Modern email services send these junk emails to the junk folder anyway, so you don't see them all that much nowadays.

But with Bitcoin and cryptocurrency being so new and so hot in the news right now, scammers are scrambling to find a way to steal your bitcoins by getting access to your digital wallets!

Email Phishing Scams

Scammers will send you an email designed to make it look like it came from your online wallet service (this is why we don't suggest storing large sums of virtual currency in your exchange wallets).

In the email, they'll ask you to click on a link which will lead you to a fake website. It will look exactly like your exchange or wallet website. Of course, it's not the same because the domain name will be different.

For example, if you're using Coinbase, they'll use a similar misspelled domain such as:

- Cooinbase
- Coiinbase
- Coinbasse
- Coinsbase
- Coinbase-Client-Update.com
- or something similar…

It will also most probably not have a security feature called SSL installed, which means the domain will start with HTTP and not HTTPS (modern browsers like Chrome and Firefox should warn you if it's a secure site or not).

If you fall for this phishing scam, and you log in to the fake wallet site, then the scammers now have your login details to your real wallet! They can easily lock you out of your account, and they'll then have the freedom to transfer every single bitcoin you own to their own wallets.

Malware Scams

In this type of scam, scammers will ask you to click on a link either via email, banner ad, forum ad, or anywhere they can post a link which will then download a type of malware to your computer.

Often, these malwares are keyloggers which will record everything you type on your computer, and send the information to the scammers. So, if you log in to your online wallet, like Coinbase for example, they will be able to see your username and your password, and they can then log in to your account and easily steal your coins from you!

> *The key takeaway for protecting yourself from these types of scams is to never click on links from untrustworthy sources.*

If you don't recognize the sender, or the website domain name is misspelled, it should raise a red flag, and you should report the email and/or leave the phishing site right away.

Furthermore, consider using offline storing methods such as paper wallets or hardware wallets so even if scammers get access to your online wallet, they'll have nothing to steal there.

Scam #3 – Cloud Mining Scams

Cloud mining is a popular way of becoming a bitcoin miner. You no longer need to invest in your own supercomputer and join a mining group to solve complex cryptographic hash problems. You don't even need to worry about expensive electricity bills.

You simply need to sign up to a cloud mining service (also known as a mining farm), rent mining equipment, and receive payments proportionate to your subscription.

While some cloud mining companies are legitimate, there are many fly-by-night websites which promise unrealistic returns for measly sums, whose sole purpose is to steal your money.

Some common red flags to watch out for when looking to join a cloud mining service is the absence of an About page, Terms of Use/Service page, physical address, and/or contact number.

They might also not have a secure domain (no HTTPS before their domain name). These details are all very important in figuring out which site is a scam and which is not. You can search Google for reviews and go through their website to get a feel if they're legitimate or not. More often than not, these sites would be anonymous with no names or faces behind them.

Some may appear legitimate at first but take a deeper look at what your investment's going to get you. You may pay eventually sign up for a contract which is going to cost you a few thousand dollars a year but what are you going to get in return? You'll have to do the math yourself and calculate if you're going to end up in the green.

The key takeaway here is before you spend any of your hard-earned fiat money, you should at least make sure you're dealing with a legitimate company and not some anonymous scammer who'll leave you in tears.

Do plenty of research, read reviews, and browse the crypto-mining communities for information on the best and most trustworthy cloud mining companies.

Scam #4 – Ponzi Scams

Ponzi scams are probably easier to spot than the other scams we've covered so far in this guide. This is because Ponzi scams are well known for guaranteeing outlandish returns on investments with little to no risk to the investors. People fall for these sorts of scams all the time because people want guaranteed returns on their investments.

With Bitcoin and cryptocurrency, any company that guarantees exponential returns on any investment should be viewed as a potential scammer. The cryptocurrency market is highly volatile, and one minute the price could be at an all-time high and the next, it's down by a few hundred or a few thousand dollars.

Because of this volatility, you should never believe anyone who tells you you're guaranteed a 10% return on your investment every single day, or whatever the scammer's terms may be.

Since Ponzi schemes rely on new members, a.k.a. victims, to pay off their early investors, they usually offer incentives for members to recruit new people to join their network.

It's very common for scams like this to offer some form of affiliate rewards. You refer someone to invest in the 'company,' and you get compensated for your efforts.

Some Ponzi schemes guarantee daily profits *forever*. If this seems impossible, it most certainly is. No one even knows if bitcoins will be around that long and guaranteeing daily returns is just crazy. Right off the bat, an intelligent investor will see that offers like these are nothing more than scams designed to rip you off your money or your bitcoins.

In fact, many of these scam sites prefer bitcoin payments because they know Bitcoin transactions can't be reversed or canceled once sent! Either way, whether they require fiat or cryptocurrency, know who you're sending your money to first.

The key takeaway here is if you know the company's offers are too good to be true, then you should run away in the opposite direction. Sometimes, there's just no point in even looking up reviews on the Internet when it comes to scams like these because most 'reviewers' are those who got in the game early and thus have already received some return on their investment.

And usually, when these users leave reviews they'll include their affiliate link so you know right away they have a vested interest for leaving glowing reviews for a company they may, or may not know, is a scam.