This lecture is of much importance, as it sets the tone for why we are going to be covering what we’ll be covering in this lecture. The security of your cryptocurrencies, and further, your wallet.

Staying safe and secure is an inherent part of using cryptocurrencies. Cryptocurrencies allows you to hold your own money and secure it yourself, which is very empowering, but as you know, with great power, comes great responsibility.

Allow me to explain: if you lose your private keys, your money is gone - period. That’s the sad reality of it, and it’s better to understand this reality sooner rather than later. This is not only true for when someone else gets a hold of your keys, but also when you don’t back up your seed and lose your phone, or forget where you kept your backup, which today is by far the the most common way to lose your crypto.

Cryptocurrency has no customer service to call, there is no public relations department, there is no account insurance, or anything like that, so it’s absolutely key to secure your money. The Internet is filled with people who have lost their backups, which has resulted in them losing hundreds of thousands of dollars in cryptocurrencies.

Backing up your 12-word passphrase is imperative, so please do it if you haven’t already. Do it for any new wallet you open, and make sure you insist on it with everyone you bring into the cryptocurrency ecosystem.

Now a key feature of cryptocurrencies is that no one can take your money away from you if you don’t want to give it to them, but that certainly doesn’t prevent people from taking your money if you’ve been fooled into giving it to them. Irreversible anonymous money, which is what cryptocurrencies are, attracts a lot of scammers and thieves, from exchanges that run away with your money, to fake stores, ponzi schemes, and a whole host of other scams.

In fact, the first exchange to claim to get approved by the regulators in it’s home country of Cyprus, Neo & Bee, turned out to be an investment scam. people invested millions into it, and they just took the money and disappeared.

With bitcoin and other cryptocurrencies, you must always ask yourself: why should i trust these guys? Does what they say make sense? What are my guarantees? This kind of critical thinking could have saved friends of mine, and many others, a lot heartache and precious coins.

In the old days the bitcoin community was very small, and it was dispersed all around the world, with no resources available to help with most common issues. If you came across an issue you had to ask for help from strangers online, and in many cases it worked. But bitcoin users soon learned a couple of important lessons - always ask for help in a public space for example in a facebook group or forum, and never give, send or show your private keys online publicly.

When you ask for help in a public place, people are going to be able to point out mistakes and frauds on the answers you’re getting. It’ll also keep out casual fraudsters which don’t want their reputations ruined by publicly defrauding you - remember to always second check advice that is given to you, especially advice that involves your password or passphrase.

Now, hopefully, you have been adequately convinced of the importance of using security measures and common sense when it comes to cryptocurrencies, but in case you haven’t, here are a few prominent cases that will drive this point home.

On one occasion, a guest on a talkshow brought along a bitcoin paper wallet to the show the host. It turns out that a few seconds of video with the private key showing, was just enough exposure for a hacker to take the bitcoins that were in that wallet, and within minutes of the show airing, someone transferred it into a wallet they controlled.

Another memorable and highly referenced occasion in the short history of bitcoin is the mt.gox hack. Up until 2013, the vast majority of bitcoin trading was done on just one exchange, called mt.gox.

The site started off as an exchange trading cards for the video game, Magic: The Gathering Online, it had very few security measures, and simply wasn’t built for security. Then in 2013, the inevitable happened - Mt.gox was presumably hacked, and 400 million dollars worth of bitcoin were stolen.

Needless to say that all of the people that held their bitcoin in Mt.gox lost it, and to this day there’s a legal battle going in regards to the bitcoins that were lost. Maybe someday in the future these people will get some fraction of their coins.

And by the way, even if the exchange you’re dealing with isn’t hacked, that doesn’t mean that your coins are safe. I’d like to go into more detail on the story of a bitcoin user loosing approximately $8,000 within 15 minutes, because it’s an interesting one that shows that any weakness in your security ecosystem can cause a total breach of your safeguards. If any of the terms or security features I mention here are unfamiliar to you, don’t worry: we’re going to explain all of them, and do a play-by-play of how this all could be avoided, in the coming lectures.

So. The way that this hack worked is as follows:

In late may, 2017, Cody Brown reposted a friend’s Facebook post about being hacked by Coinbase, which this friend “thought” was secure. Mistake #1: Both Cody and Adam were keeping all of their cryptocurrencies in Coinbase’s so-called “wallet,” and not in their own secure wallets. Mistake #2: Cody announced to the whole world exactly where he was trading.

On May 24th, at 11:31PM, Cody got a text message from Verizon Wireless, saying that he was on the phone with them.

Since Cody was NOT on the phone with them, he then immediately calls Verizon… who, unfortunately, had just closed for the evening.

Cody frantically tweets to Verizon support, who writes back asking for more information, but it’s too little, too late. Cody’s phone number - which was linked to his GMail account in case he forgot his password - had been changed to another device besides his. This was Mistake #3: Using SMS as a form of authentication for a forgotten password, without realizing that someone can claim to be you and take control of your phone simply by knowing a few personal details such as your billing address.

You can probably imagine what happened next:

Within a few minutes, Cody’s Gmail signs out. The password had been changed. Mistake #5: Cody didn’t have any 2 Factor Authentication method enabled on his Gmail account.

Next, with access to his Gmail, the thieves were able to change his Coinbase.com password. Mistake #6: Not using a secure 2 Factor Authentication method on Coinbase.

What happened next is just painful to think about. Cody watched, in real time, as the thieves liquidated his account.

At 11:44PM, they sent themselves 1.18BTC. A minute later, 70.96LTC. And finally, one minute after that, 16.03 ETH. And just like that, Cody Brown lost over $8,000, all because of a few small mistakes. Had he enabled just one or two of the security features you’re going to learn about in the coming lectures, all of this could have been avoided.

With each of these horror stories, the lessons to be learnt are the same as you’ve already heard: First, don’t keep your cryptocurrencies in an exchange unless you’re actively trading with those funds, which we normally don’t recommend anyways. Remember, there’s no good reason to keep your money in other people’s hands.

While today’s cryptocurrency exchanges are among the most secure internet businesses out there, and some of them are leading the pack in regards to internet security in general, they’re still big honeypots, and they are vulnerable to “social engineering” hacks like the one that happened to Cody. Remember, we’re not dealing with financial institutions that have several decades worth of reputation to maintain, or government backing and insurance. Any entity that’s holding your crypto can theoretically disappear in one day with your money, and nothing will bring it back unless they decide to give it back - so rely on yourself, hold your own crypto.

You also already know that your cryptocurrencies aren’t truly yours unless you’re the only person with the keys to using them, so keep your bitcoins within your own wallet where you control the private keys, and use the advanced security measures that you’re about to learn about, without exception, on everything from your email account to your hardware wallet.

To conclude, though there are a lot of different ways to get scammed or become another cryptocurrency horror story, they all share one major similarity: they could all have been prevented by the users avoiding unnecessary third party services, and instead, relying on themselves and their own security measures. So the key here - pun intended - is to hold your own seed, and take the appropriate steps to secure it.

Now, let’s learn how to do it. I look forward to seeing you in the next lecture where we will go into how to begin safeguarding your cryptocurrency portfolio.