In this lecture I’m going to show you how to safeguard your cryptocurrency portfolio, ensuring as you build your cryptocurrency portfolio going forward, you are not prone to amateur mistakes which could jeopardise your investments.

To start with, I want to discuss passwords. So passwords are generally broken in one two ways: when they are leaked and aren’t a secret anymore, or by “brute force” - basically, guessed after a huge number of attempts, generally using a specialized computer program.

So how do we keep a password from being broken by brute force, and how can we prevent someone - or some computer - from guessing your password?

The name of the game here is Entropy, which, in cryptography, means lack of predictability.

To achieve that, we want to make the amount of guesses one has to go through to figure out our password as large as possible. Luckily, the numbers are on our side: let me explain.

For a one digit PIN, I only need to remember one digit, and an attacker needs 10 guesses to cover the entire range of possible passwords.

Now, for a 2 digit PIN, I’ll need to remember 2 digits, but the attacker would need 100 attempts. 3 digits give us 1000 attempts, 4 is 10,000 attempts, and so on. So for every digit I add i need to remember just one more digit, but bruteforcing my PIN becomes 10 times harder.

However, computers today are very, very good at doing this guesswork, and can go through huge numbers of attempts given enough time, so we need very long passwords.

Now I know what you’re thinking, I’m probably safe because my password has my dog's name, my birthday, and my mother’s car manufacturer in it, that’s like 22 characters, so i’m probably good, right?

That’s actually not the right way to do it, on two levels. The first level is, by saying “my password”, it implies you have one password, which is a bad practice to begin with. We’ll talk about why in the next lecture.

The second, more interesting, and mathematical part that makes it bad, is that words, even though they are made of several characters, aren’t actually adding as much entropy as several characters. There are softwares out there that can get all of your social media data online, and try breaking your passwords with your dogs name as one component. They can also take entire lists of common words or phrases, and plug those in as variables.

Such techniques drastically reduce the number of attempts needed to break our passwords. Also, as it turns out, humans aren’t very good at generating unpredictable patterns, and so our attempts to do so often end up punching the keyboard in highly common and predictable areas.

So what can we do?

For most passwords, randomly generating them is the answer. Computers are much better than us at generating randomness to create long and unpredictable strings. A good rule of thumb is that a password should be hard to remember and pronounce.

This means that for all but your master password, you should use a password manager. We’ll cover that in another lecture, though.

For now, let’s talk about this master password, used to unlock all of your other passwords, because if you follow the recommendations in this lecture, you will hopefully never try to create your own passwords, except for that one.

For your secure master password, it needs to be something that is highly memorable - so you won’t forget - but hard to brute force.

Unfortunately, as we said, over the last 20 years, we’ve managed to train people to create passwords that are easy for computers to guess, but hard for us to remember.

In fact, some of the strongest and most memorable passwords you can create are actually similar to a Bitcoin seed.. Just a bunch of random words, put together.

For example, “correct horse battery staple” would be many orders of magnitude more difficult to guess than some attempt at a random password. If you add in some punctuation and capitalizations, such as capitalizing names or adding in dates, the password gets even more challenging.

Before choosing any master password, we recommend that you run it through the website “HowSecureIsMyPassword.net".You might just be surprised to find that your idea for a random password is already on the list of brute force variables, whereas something that would be easy for you to remember, such as a completely random list of 5 words from https://xkpasswd.net/s/, would take 188 Octillion years to crack.

Play around with the links and come up with a secure master password.

This leads me nicely onto two factor authentication, or 2FA in short, which is a second method by which a provider, like a bitcoin exchange, or your email provider, can authenticate your identity in addition to your password.

So why is it important?

First, someone could have gotten your password in any number of ways, like a keylogger or simply looking while you type it, which of course would not work because by now you ARE using a password manager and not typing your passwords, or by hacking into a website that you use.  If such an attacker would like to access your 2FA enabled account, they would be prompted to also give a 2FA code, which they will not have, because the password they obtained is only the first factor of authentication.

Secondly, the vast majority of attacks online do not happen in real time. Which means, attackers typically deploy some malware, or send out some phishing mail or site, and after a while, when they get a bunch of results, they try and access the accounts they were able to get passwords to. Since 2FA is generated at or near the moment that you’re trying to access your account, such static forms of attacks don’t work when 2FA is required.

2FA does not protect you from an online, live man-in-the-middle attack, which is someone pretending to be your service provider in real time, and using the credentials you type in to sign into the real site. However, these attacks are more expensive to execute, as well as more rare, and since most people don’t use 2FA, why bother? When you enable 2FA, hackers realize that there are easier fish to catch than you, and indeed it’s one of those things that require just a little bit of extra effort to protect you from 95% of the threats out there.

Now, please note that as we learned from Cody Brown, using your phone number and getting an SMS 2FA code is not secure, as anyone can use social engineering to take over your phone number, or even just see the contents of the authentication message on your phone’s lock screen. Plus, if you have your phone and your computer synchronized with something like iCloud, they might not even need your second device to receive and read that confirmation SMS. Furthermore, SMS are sent unencrypted in a wide network, and are proven to be very easy to intercept.

For these reasons and many more, we like the Google Authenticator app, since it’s easy to use, intuitive, open source, and does not require any sketchy permissions.

Here’s a two minute guide to enabling 2FA on your accounts. It should pretty similar for any site that has 2FA functionality, and if a site doesn’t offer 2FA, then you should consider it insecure.

Start by installing the Google Authenticator app on your device

Then, on the website you’re using,

Go to account settings->security-> 2nd Factor Authentication

When you click “Enable” a QR Code and oftentimes a code shows up, print these. It’ll serve you if you lose your phone and need to authenticate yourself, and will save you a couple of weeks of emailing back and forth with customer support.

Then, go to Google Authenticator and Hit “+” or “Add Account”

A Camera Scanner opens up. Simply point it at the QR code until it scans it.

You can see now that a 6 digit code with a little 30 second clock next to it is showing on your app. This is because this code changes every 30 seconds.

Go back to the site, on the page with the QR code, it should ask for the temporary code, type it in.

Then you’re done!

Now, every time you’d want to log into the site, and possibly even before you complete other sensitive actions on the site that require 2FA - like withdrawing bitcoins, you’ll be prompted to provide this temporary code. Your account is now significantly more secure.

It’s important to note that this is by no means part of the Bitcoin protocol, and no matter how well your 2FA is set up and on which wallet, your 12-word passphrase, the seed backup, is still the final and ultimate control over your wallet.

2FA is merely a security feature on the website you’re using. Which means if you lose your seed, you lose your crypto, but it also means that if you lose your 2FA, you don’t necessarily lose access to your account. You’ll need to contact the site’s support, possibly verify who you are in another manner, like a passport scan or a recent utility bill, and most likely wait anywhere from a few days up to a couple of months. It’s not an inherent cryptographic impossibility to recover your account without it, though. In that sense, it’s very much like your password, just that they don’t send you a new one to your email address if you lose it, because that would defeat the whole purpose.

One last note is that if you choose a Hardware Wallet, such as Trezor or Ledger, it can also act as an automated 2FA tool any time that it’s plugged in to your computer. This can speed things up, by eliminating the need to type in codes, but can be inconvenient if you don’t plan on carrying your hardware wallet with you everywhere.

So give some thought to 2FA, and maybe do an assessment of all of the sites that you log in to that work with it. We recommend that at the very least, you enable 2FA for your Gmail account, any exchanges you work with, your bank account, and your LastPass or password manager. It’s a bit inconvenient, but again, will prevent at least 95% of attacks on your security.

I hope this in-depth lecture was of huge use. I look forward to seeing you in the next lecture where we will be discussing the difference between hot and cold wallets in detail.