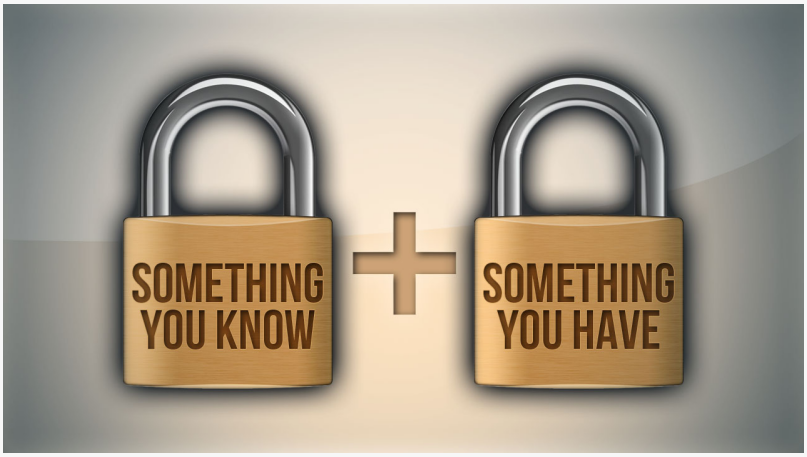
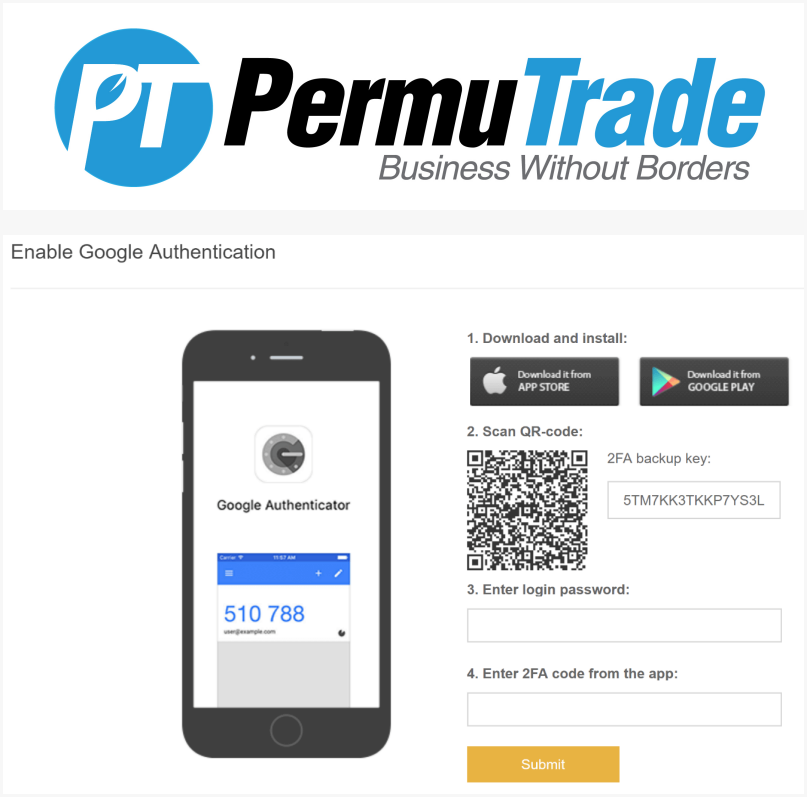
What Is Two-Factor Authentication & Why Should You Use It

Two-Factor Authentication is an extra security level where access to your account is granted after inputting something that you know and something you have.



2FA - Something You Know + Something You Have



2FA - Google Authentictor

WEST PALM BEACH, FLORIDA, UNITED STATES, January 15, 2018 /EINPresswire.com/ -- Newcomers to the world of cryptocurrency might have heard of two-factor authentication popularly called 2FA, the best way to protect your precious coins. Cryptocurrency security can be overwhelming to many people. You've got wallets, cold storage, public and private keys, two-factor authentication and more. I've broken down what 2FA is, how it works, the different kinds, and why you should use it.

Cryptocurrency investors have raked in eye-popping returns in the last year. If you bought Bitcoin for example on January 1st 2017, you would have seen massive returns in just one year. It makes the single digits earnable in an Individual Retirement Account (IRA) seem pretty inadequate. But with reward comes risk and nowhere is that more evident than in cryptocurrency. If someone swipes your credit card and buys a couple of plasma TVs, you can call your bank and fix things. If someone hacks your profile on an exchange and steals your coins, you'll never see that money again.

You've probably used 2FA before dabbling into cryptocurrency. It's the practice of backing up your login information through some other method, typically an app or phone number. When you login to a website, it'll ask you to use that other method to prove it's really you. This prevents someone from guessing your password and email to login. 2FA is used by everyone from Apple to Zendesk.

Security is critical in the crypto world so exchanges and wallets have adopted 2FA to protect users. Users download apps like Google Authenticator or Authy. When logging into an exchange, you'll pull up the app which has a code you must enter to login. The app constantly creates and discards codes adding considerable security to the login process. There's software-based 2FA, hardware-based 2FA, and Short Message Service (SMS) based 2FA. I'll get into them all in the coming paragraphs.

2FA - Ledger Nano S

2FA - Trezor

SMS 2FA is the simplest option. We've all had to enter our phone number somewhere on a website, read a text containing some number sequence, and enter it to prove it's really us. Unfortunately, this isn't quite secure enough in the world of crypto. Search YouTube and you can find videos of hackers calling phone companies and weaseling users personal information out of them. It's frighteningly easy to call, impersonate someone, and collect some of their personal information. If an attacker gets access to your email, it can be game over. They can reset the password from an exchange, login as you, and send the money to themselves.

Sometimes hackers will employ what's called phone porting. They'll call a phone company and persuade a customer service agent to swap your phone number to a different device with a different SIM card. As you can imagine, this isn't good. I recommend placing restrictions on your account to prevent any kind of change without complete verification of identity.

There are measures you can and should take to secure your phone account but the best option is using software or hardware based 2FA. The most popular software options are apps called Google Authenticator and Authy. When you create a profile on an exchange, you'll download one of these apps and enter your information. You'll then scan a QR code which looks like a barcode to link your app to the exchange.

Software-based 2FA works through a Temporary One Time Password (TOTP) protocol. The app and the exchange liaison to determine a one-time code that can be used to access the exchange. This code expires every 20 seconds so even if someone was looking over your shoulder and snooped your code, it wouldn't be useful for very long.

Google Authenticator and Authy are two free options with their own pros and cons. Google Authenticator is easy to use and many people's first 2FA choice when getting into crypto. Authy on the

other hand is my personal preference as it offers additional features such as the ability to use multiple devices. This can be very handy especially if you ever lose or break your phone. Authy also has an optional feature where it lets you encrypt and backup your data. This data is decrypted only on your device using a password that only you know.

Hardware-based 2FA can be another great option if you want to get even more security. Ledger Nano S and Trezor are two popular options. They essentially function like Google Authenticator or Authy but also operate as a wallet for your crypto coins.

So what happens if you lose your phone? It depends heavily on what app you're using. If you were using Google Authenticator, you're in for some tedious arguing with exchanges if you didn't save your original QR code. You'll have to disable 2FA on each exchange or service and then re-enable it. That's doable but it's not going to be fun with how slowly exchanges are replying to support tickets these days. Authy offers backups and multiple device usage so you can simply authenticate yourself via another device.

You can restore 2FA if you used proper diligence from the get-go. When setting up 2FA, printing copies of the QR code is a great security measure. You can just scan those over again to rebuild your 2FA profile. Usually you'll get a string of characters with the QR code which can be used in the same way. You'll want to keep all of this information in a safe place and copying the code down by hand is always safer than keeping it on your computer.

Of course, like everything else in life, 2FA isn't perfect. If you get sloppy and don't enable it on every exchange then you're still going to be in trouble. Also this solution cannot protect you from phishing websites. Creating mock websites that are identical to exchanges is a favorite tactic of hackers. Users enter their email, passwords, and 2FA to a phishing website. Their money can be gone in seconds. To combat this, I recommend you bookmark verified exchange sites rather than searching the web for them.

As a cryptocurrency investor, you should get serious about security and enable 2FA via app or hardware wallet. Don't empower hackers to access your accounts by being lazy. Crypto is still in its Wild West days so you can't be too careful about security.

Engr. AJ Jama, MBA
PermuTrade LLC
+1-561-228-4111
email us here
