What is 2FA (2-factor Authentication)?

By Nat Cole
BTC BOS LTD

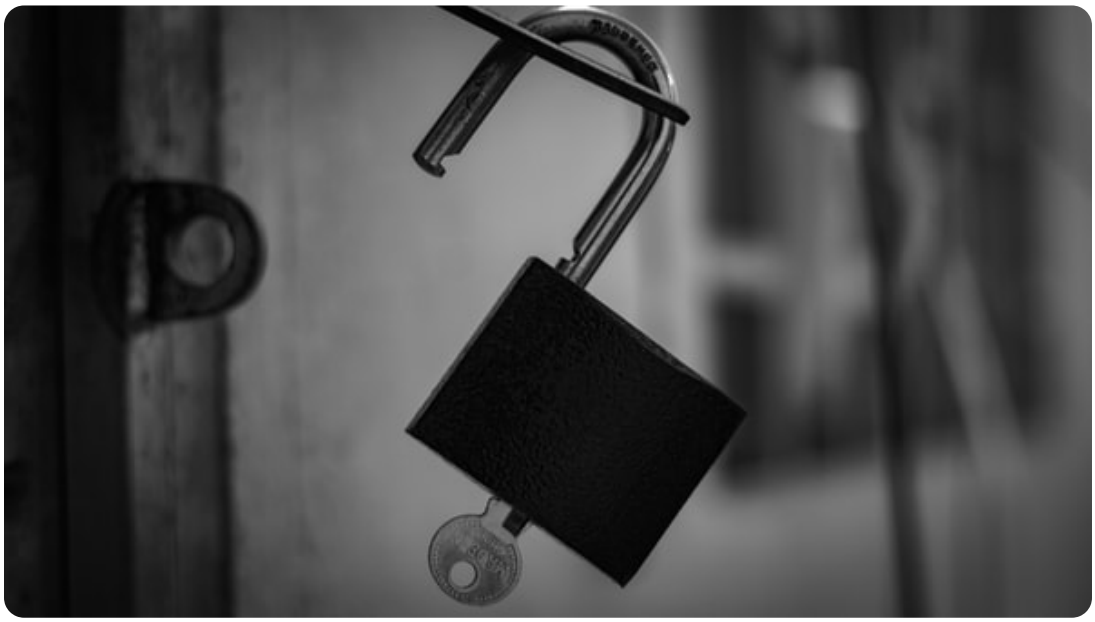
Regardless of whether you're securing, assets, funds or your Facebook account. 2FA is one of the most important steps in securing your data.

When creating a digital account on any platform it is important for users to employ extra methods of security, other than just a password. In 2021, most platforms offer at least one extra layer of security, beyond ensuring that users choose a **suitable** password. One such method attempts to ensure live verification from other devices that the user registered ownership of when creating their account. The most popular and trusted of these methods is 2FA.

What is 2FA and where did it come from?

The term 2 Factor Authentication, is actually derived from the term '**Multi-Factor Authentication**', an electronic authentication method, in which a user must present at least two pieces of 'evidence' to support them being the authorised user of a device or service. These evidences are referred to as 'factors'.

As far as its history, **Kim Dotcom** was known to have filed a patent claim in the year 2000 for 2-FActor Authentication. This was later revoked, by the European parliament on grounds that the U.S. based telecoms giant **AT&T** had already filed a 'too similar' patent in 1998.



So, how does it work?

Again, 2-FA works, by asking a user to present a second type of evidence to show that they are in fact the correct user of said device/service. To give you a better view let's describe some 2-FA scenarios:

- You attempt to login to your email account, with a correct username and password, you are automatically sent a text message with a 'verification code' **– 2FA**
- You call up you bank, get an automated system that asks you to confirm your account information, then passes you through to an advisor, who asks for your 'secret' word or phrase – **2FA**
- You go to a cash machine, enter your PIN, select your withdrawal amount and are asked for your PIN a second time – **NOT 2FA**
- You attempt to login to your crypto hardware wallet. You are asked for a PIN o your hardware's screen, then your computer screen prompts you to enter your private key **– 2FA**

We hope you can see how this works?
Now, you may be wondering why the cash machine example is NOT a 2-FA request, given that you were asked for your PIN twice?!

To put it simply, your PIN is the same information you entered the first time, so it does not count. If someone had stolen your card and PIN, then it's clear that they already know this info and can verify it a million times over. 2FA would ask you for a different piece of information on the second ask, as this is more likely to be information that a fraudster wouldn't know.

How important are your assets and your data?

Every person has some things that they would like to keep private. In a digital world, data, assets, funds, records and more are needed to be kept privately.

As with our previous statement, you would not want a fraudster or hacker to be able to access all of your private digital possessions. If any of your accounts or funds were hacked/stolen, you would all instantly blame the service which you were using, as such you would also be very mad if another person kept logging into whatever device/service and kept changing, deleting or adding things.

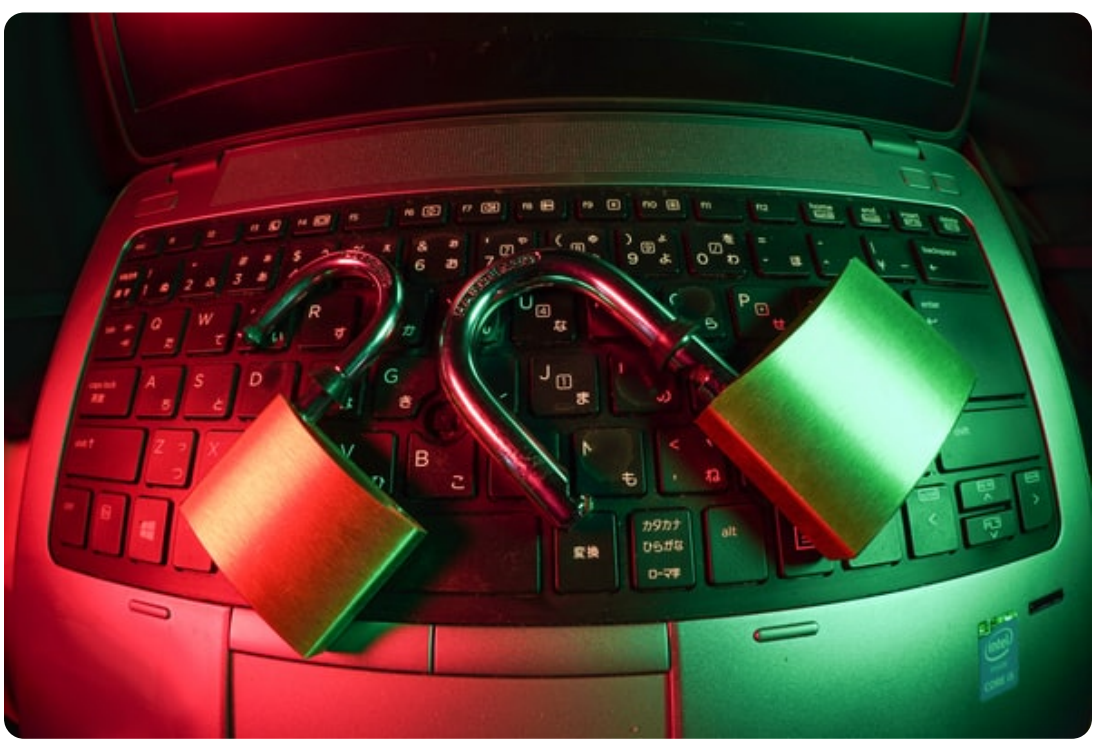
MFA attempts to resolve this, with the second step making it a 2FA method at minimum.

Make it secure

As we've pointed out, there are many ways to implement a 2FA method and it all depends on the scenario it's being used in as to how the method is implemented. Most of these methods use a TPA (Third Party Authenticator) to complete the process. TPA's present the user with a randomly generated 'verification code' which can be used to authenticate the user.

The most popular ways to complete 2FA are among the following:

- **SMS message**
- **Email**
- **Telephone Call**
- **2FA Application**



What TPA's can I trust?

Although many companies have already implemented 2FA, only a handful of actual companies are widely integrated and trusted for verification of this kind.

The most popular 2FA applications:

- **Google Authenticator**
- **Authy**

To learn more about these applications, just **click the link at the end of this guide to see our Security Tips and Tricks.**

Lucky for crypto enthusiast, most popular crypto exchanges, apps and services already have 2FA and MFA methods implemented, so please **keep your account secure!**

Fun fact! Google's GAUTH authentication codes can also be called upon, inside the the Authy app, as well as it's own native application.

By Nat Cole
BTC BROS LTD

Get 100's of Cryptocurrency guides to help your learning, or to Share with your Friends & Family.

Inspire yourself with easy to understand Blockchain and Cryptocurrency resources. Our Website and services include 100's of PDF's about Bitcoin, Blockchain and related Emerging Technologies.

GET MORE GUIDES >>